

BỘ GIÁO DỤC VÀ ĐÀO TẠO  
TRƯỜNG ĐẠI HỌC VINH

TRẦN THỊ THU HƯƠNG

ĐỊNH LÝ THẶNG DƯ TRUNG HOA  
TRÊN VÀNH VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Nghệ An - 2024

BỘ GIÁO DỤC VÀ ĐÀO TẠO  
TRƯỜNG ĐẠI HỌC VINH

TRẦN THỊ THU HƯỜNG

ĐỊNH LÝ THẶNG DƯ TRUNG HOA  
TRÊN VÀNH VÀ ỨNG DỤNG

*Chuyên ngành:* ĐẠI SỐ VÀ LÝ THUYẾT SỐ

Mã số: 846 01 04

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học

PGS. TS. NGUYỄN THỊ HỒNG LOAN

Nghệ An - 2024

# MỤC LỤC

|                                                                                                                |           |
|----------------------------------------------------------------------------------------------------------------|-----------|
| <b>Mục lục</b>                                                                                                 | <b>1</b>  |
| <b>Mở đầu</b>                                                                                                  | <b>3</b>  |
| <b>1 Sự hình thành và phát triển của Định lý thặng dư Trung Hoa</b>                                            | <b>5</b>  |
| 1.1. Lịch sử phát triển . . . . .                                                                              | 5         |
| 1.2. Định lý Thặng dư Trung Hoa cho số nguyên . . . . .                                                        | 8         |
| 1.3. Code thuật toán thặng dư Trung Hoa . . . . .                                                              | 13        |
| 1.4. Ứng dụng của Định lý thặng dư Trung Hoa trong việc giải hệ phương trình đồng dư bậc nhất một ẩn . . . . . | 16        |
| <b>2 Các phát biểu khác của Định lý Thặng dư Trung Hoa</b>                                                     | <b>26</b> |
| 2.1. Định lý Thặng dư Trung Hoa cho vành . . . . .                                                             | 26        |
| 2.2. Định lý Thặng dư Trung Hoa trên vành đa thức . . . . .                                                    | 31        |
| <b>3 Ứng dụng của Định lý Thặng dư Trung Hoa</b>                                                               | <b>35</b> |
| 3.1. Dãy số nguyên hữu hạn . . . . .                                                                           | 35        |
| 3.2. Sử dụng Định lý Thặng dư Trung Hoa để chứng minh một tính chất của miền Dedekind . . . . .                | 37        |
| 3.3. Sử dụng Định lý Thặng dư Trung Hoa để giải một số bài toán sơ cấp                                         | 39        |
| 3.4. Sơ đồ mật mã . . . . .                                                                                    | 42        |

|                           |           |
|---------------------------|-----------|
| <b>Kết luận</b>           | <b>48</b> |
| <b>Tài liệu tham khảo</b> | <b>49</b> |

## MỞ ĐẦU

Bài toán số dư xuất hiện lần đầu tiên trên thế giới vào khoảng thế kỷ III sau công nguyên trong cuốn sách của nhà toán học Tôn Tử - một nhà toán học người Trung Quốc. Ngày nay, bài toán số dư được phổ biến rộng rãi với tên gọi Định lý Thặng dư Trung Hoa.

Trong cuốn sách của Tôn Tử, định lý này xuất hiện ở Chương 3, Bài 26 như sau: "Chúng ta có một số đồ vật biết rằng số đó chia cho 3 dư 2, chia cho 5 dư 3 và chia cho 7 thì dư 2. Tìm số lượng đồ vật đó". Bên cạnh phát biểu bài toán, tác giả cũng đưa ra đáp án và lời giải cụ thể.

Từ thời cổ đại, định lý này đã được sử dụng trong việc tính toán lịch, đếm số lượng binh lính và xây dựng. Sử dụng thuật ngữ đồng dư, sau này định lý được phát biểu như sau: "Cho  $k$  số nguyên dương đôi một nguyên tố cùng nhau  $m_1, m_2, \dots, m_k$  và  $a_1, a_2, \dots, a_k$  là  $k$  số nguyên tùy ý. Khi đó hệ phương trình đồng dư tuyến tính

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

có nghiệm duy nhất theo modulo  $M = m_1.m_2...m_k$ ".

Trải qua một thời gian dài, người ta đã mở rộng Định lý thặng dư Trung Hoa lên vành. Hơn thế nữa, Định lý thặng dư Trung Hoa còn được ứng dụng rộng rãi trong khoa học máy tính, lập trình và lý thuyết mật mã.

Nội dung của luận văn là trình bày lại Định lý thặng dư Trung Hoa liên

quan đến số nguyên, sau đó mở rộng lên vành và một số ứng dụng của định lý này.

Ngoài phần mở đầu, kết luận và danh mục tài liệu tham khảo, nội dung của luận văn được viết thành ba chương. Chương 1 trình bày về lịch sử phát triển, nội dung của Định lý thặng dư Trung Hoa và code thuật toán. Chương 2 trình bày mở rộng của Định lý thặng dư Trung Hoa lên vành. Chương 3 trình bày một số ứng dụng của Định lý thặng dư Trung Hoa.

Luận văn này được hoàn thành dưới sự hướng dẫn của PGS. TS. Nguyễn Thị Hồng Loan. Tác giả xin được bày tỏ lòng biết ơn sâu sắc tới Cô - người đã giảng dạy, hướng dẫn, chỉ bảo tận tình và chu đáo trong quá trình tác giả học tập và thực hiện luận văn. Tác giả cũng xin được gửi lời cảm ơn tới Ban giám hiệu Trường THPT Chuyên Phan Bội Châu, các đồng nghiệp, gia đình và người thân đã luôn quan tâm giúp đỡ và tạo mọi điều kiện thuận lợi để tác giả có thể học tập, nghiên cứu và hoàn thành luận văn.

*Nghệ An, tháng 9 năm 2024*

**Tác giả**

## CHƯƠNG 1

# SỰ HÌNH THÀNH VÀ PHÁT TRIỂN CỦA ĐỊNH LÝ THẶNG DƯ TRUNG HOA

## 1.1 Lịch sử phát triển

Trong lịch sử, đã có một số bài toán liên quan đến việc tìm số lượng (chẳng hạn như số giỏ, số khối gạch hoặc số binh sĩ trong một nhóm) thỏa mãn một số điều kiện nhất định, được tính thông qua số dư. Một ví dụ như sau: "Chúng ta có một số đồ vật biết rằng số đó chia cho 3 dư 2, chia cho 5 dư 3 và chia cho 7 thì dư 2. Tìm số lượng đồ vật đó."

Bài toán trên đã được nêu ra trong các tác phẩm toán học kinh điển của nhà toán học Trung Quốc cổ đại - Tôn Tử. "Sun Zi Suanjing" và "Sổ tay toán học của Tôn Tử" có niên đại vào khoảng đầu thời Hy Lạp - La Mã, năm 100 - 500 sau Công nguyên. Tác phẩm toán học kinh điển lâu đời nhất của Trung Quốc là "Chou Pei Suanjing", có niên đại khoảng 1000 năm trước Công nguyên. Cuốn sách này ghi lại các tính toán toán học trong thiên văn. Đặc biệt trong cuốn sách này, Định lý Pythagore đã được sử dụng. Mặc dù cuốn sách của Tôn Tử không phải là tác phẩm toán học kinh điển lâu đời nhất ở Trung Quốc nhưng Định lý thặng dư Trung Hoa lần đầu tiên xuất hiện trong cuốn sách này.

Cách tính lịch Trung Hoa cổ đại là nguồn gốc của Định lý thặng dư. Vào năm 237, các nhà thiên văn học Trung Quốc đã xác định thời điểm bắt đầu của lịch là "Thượng Nguyên". Nếu ngày Đông chí của một năm nào đó xảy

ra  $r_1$  ngày sau thượng nguyên và  $r_2$  ngày sau ngày trăng non thì năm đó là  $N$  năm sau thượng nguyên. Vì vậy ta có hệ phương trình đồng dư:

$$\begin{cases} xN \equiv r_1 \pmod{60} \\ xN \equiv r_2 \pmod{y} \end{cases}$$

cho biết số năm  $N$  sau Thượng Nguyên, trong đó  $x$  là số ngày trong một năm nhiệt đới,  $y$  là số ngày trong một tháng âm lịch.

Ví dụ này được xem như là ứng dụng đầu tiên của Định lý thặng dư Trung Hoa. Kiểu tính toán này cũng được sử dụng trong việc xây một bức tường hoặc phần móng của một tòa thành, chẳng hạn như việc xây dựng Vạn Lý Trường Thành trong thời phong kiến năm 475 - 221 trước Công nguyên. Để xây dựng một nền móng hình chữ nhật cho một tòa thành, có bốn loại vật liệu có sẵn: khối vật liệu lập phương lớn mỗi cạnh dài 130 đơn vị; khối vật liệu lập phương nhỏ mỗi cạnh dài 110 đơn vị; gạch "thành phố" dài 120 đơn vị, rộng 60 đơn vị và dày 25 đơn vị; và gạch "sáu cửa" dài 100 đơn vị, rộng 50 đơn vị và dày 20 đơn vị. Bốn loại vật liệu này được sử dụng để xây dựng các phần móng mà không làm hỏng bất kỳ viên nào. Do đó, ta có một hệ phương trình đồng dư khi tính toán các vật liệu khác nhau cho mỗi lần sử dụng một loại vật liệu xây móng. Nếu sử dụng khối lập phương lớn, chiều dài móng thừa 60 đơn vị, nhưng chiều rộng cần thêm 60 đơn vị. Nếu sử dụng khối lập phương nhỏ, chiều dài móng thừa 20 đơn vị, nhưng chiều rộng cần thêm 30 đơn vị. Nếu tính theo chiều dài của gạch "thành phố", chiều dài móng thừa 30 đơn vị, nhưng chiều rộng cần thêm 10 đơn vị. Nếu tính theo chiều rộng của gạch "thành phố", chiều dài móng thừa 30 đơn vị, nhưng chiều rộng cần thêm 10 đơn vị. Nếu tính theo độ dày của gạch "thành phố", chiều dài móng thừa 5 đơn vị, nhưng chiều rộng cần thêm 10 đơn vị. Nếu tính theo chiều dài, chiều rộng và độ dày của gạch "sáu cửa", chiều dài móng tương ứng thừa 30, 30 và 10 đơn vị; chiều rộng móng lần lượt thừa 10, 10 và 10 đơn vị. Mục tiêu là tìm chiều dài  $X$  và chiều rộng  $Y$  của móng.



Ví dụ trên được đơn giản hóa thành hệ phương trình đồng dư:

$$\begin{cases} X \equiv 60 \pmod{130} \\ X \equiv 30 \pmod{120} \\ X \equiv 20 \pmod{110} \\ X \equiv 30 \pmod{100} \\ X \equiv 30 \pmod{60} \\ X \equiv 30 \pmod{50} \\ X \equiv 5 \pmod{25} \\ X \equiv 10 \pmod{20} \end{cases}$$

và

$$\begin{cases} Y \equiv 60 \pmod{130} \\ Y \equiv 10 \pmod{120} \\ Y \equiv 30 \pmod{110} \\ Y \equiv 10 \pmod{100} \\ Y \equiv 10 \pmod{60} \\ Y \equiv 10 \pmod{50} \\ Y \equiv 10 \pmod{25} \\ Y \equiv 10 \pmod{20}. \end{cases}$$

Bên cạnh đó, cách tính này cũng được sử dụng để tính toán số lượng binh sĩ ra trận. Để tránh kẻ thù biết số lượng binh lính mình có, một vị tướng đã nghĩ ra cách đếm binh lính của mình theo cách sau đây. Đầu tiên ông ta yêu cầu binh lính nhóm thành các hàng gồm 11 người, sau đó là hàng gồm 17, 29 và 31 người. Tương ứng, mỗi lần ông ta được báo cáo còn dư 8, 5, 16 và 24 người. Sau đó, vị tướng sẽ tự mình tính toán số lượng binh lính. Vì không có nhiều người biết về cách tính toán bí mật này nên vị tướng có thể che giấu số lượng binh lính của mình. Ví dụ này có thể đơn giản hóa bởi một hệ phương

trình đồng dư với các modulo đôi một nguyên tố cùng nhau, trong đó  $x$  là số lượng binh lính:

$$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 5 \pmod{17} \\ x \equiv 16 \pmod{29} \\ x \equiv 24 \pmod{31}. \end{cases}$$

Ta sẽ giải ba bài toán trên ở phần cuối chương này.

## 1.2 Định lý Thặng dư Trung Hoa cho số nguyên

Bây giờ ta sẽ xem xét các dạng phát biểu khác nhau của Định lý thặng dư Trung Hoa. Định lý này cung cấp một phương pháp để giải quyết bài toán đã được trình bày ở phần mở đầu.

Cho  $m_1, \dots, m_r$  là các số nguyên lớn hơn 1. Ta ký hiệu  $M$  là tích của các  $m_i$ .

Định lý thặng dư Trung Hoa được trình bày theo ngôn ngữ đồng dư như sau:

**1.2.1 Định lý. (*Dạng phát biểu thứ nhất*)** Cho  $m_1, m_2, \dots, m_r$  là các số nguyên dương đôi một nguyên tố cùng nhau và  $a_1, \dots, a_r$  là số nguyên bất kỳ. Khi đó, hệ phương trình đồng dư

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

có nghiệm duy nhất theo modulo  $M = m_1 m_2 \dots m_r$ .

*Chứng minh.* Đặt  $M_k = \frac{M}{m_k} = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$ . Ta có  $(M_k, m_k) = 1$  vì  $(m_j, m_k) = 1, \forall j \neq k$ . Do đó với mỗi  $k$ , tồn tại các số nguyên  $x_k, y_k$  sao

cho  $m_k x + M_k y_k = 1$ . Suy ra  $M_k y_k \equiv 1 \pmod{m_k}$ . Vậy  $y_k$  là phần tử nghịch đảo của  $M_k$  theo  $\text{mod } m_k$ . Ta xét

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_r M_r y_r.$$

Khi đó  $x$  sẽ là nghiệm của hệ phương trình đồng dư nói trên.

Thật vậy, vì  $m_k \mid M_j, \forall j \neq k$ , nên  $M_j \equiv 0 \pmod{m_k}$ . Do đó ta có

$$a_j M_j y_j \equiv 0 \pmod{m_k}, \forall j \neq k.$$

Suy ra  $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$  vì  $M_k y_k \equiv 1 \pmod{m_k}$ .

Để chứng minh tính duy nhất của nghiệm theo modulo  $M$ , ta giả sử  $x_1$  và  $x_2$  là hai nghiệm của hệ phương trình đồng dư. Khi đó  $x_1 \equiv x_2 \equiv a_k \pmod{m_k}, \forall k = \overline{1, r}$ . Vì vậy  $m_k \mid (x_2 - x_1) \forall k = \overline{1, r}$ . Suy ra  $M \mid (x_2 - x_1)$  hay  $x_1 \equiv x_2 \pmod{M}$ .  $\square$

Định lý này còn có thể được phát biểu dưới dạng phép chia có dư như dưới đây.

**1.2.2 Định lý. (Dạng phát biểu thứ hai)** Nếu các số nguyên  $m_i$  đôi một nguyên tố cùng nhau và  $a_1, \dots, a_r$  là các số nguyên sao cho  $0 \leq a_i < m_i$  với mọi  $i$ , thì tồn tại duy nhất một số nguyên  $x$  sao cho  $0 \leq x < M$  và phần dư của phép chia  $x$  cho  $m_i$  là  $a_i$  với mọi  $i$ .

Cho hai số nguyên  $k, m$  nguyên tố cùng nhau. Đặt  $n = km$ . Khi đó  $\forall a, b \in \mathbb{Z}$ , theo Định lý 1.2.1 hệ phương trình đồng dư

$$\begin{cases} x \equiv a \pmod{k} \\ x \equiv b \pmod{m} \end{cases}$$

có nghiệm duy nhất theo modulo  $n$ . Điều này có nghĩa là ánh xạ

$$\begin{aligned} \phi : \mathbb{Z} &\rightarrow \mathbb{Z}_k \oplus \mathbb{Z}_m \\ r &\mapsto (\bar{r}, \bar{r}) \end{aligned}$$

là một toàn cấu vành với  $\ker \phi = n\mathbb{Z}$ . Do đó trong Đại số hiện đại, Định lý 1.2.1 có thể được phát biểu như sau:

**1.2.3 Định lý. (*Dạng phát biểu thứ ba*)** Cho  $k$  và  $m$  là hai số nguyên nguyên tố cùng nhau và  $n = km$ . Khi đó ta có đẳng cấu vành

$$\mathbb{Z}_n \cong \mathbb{Z}_k \oplus \mathbb{Z}_m.$$

*Tổng quát*, cho  $k_1, \dots, k_r$  là  $k$  số nguyên đôi một nguyên tố cùng nhau và  $n = k_1 \cdots k_r$ . Khi đó ta có đẳng cấu vành

$$\mathbb{Z}_n \cong \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_r}.$$

Đặc biệt, nếu số nguyên dương  $n$  có phân tích tiêu chuẩn là  $n = p_1^{e_1} \cdots p_r^{e_r}$  thì vành cyclic  $\mathbb{Z}_n$  có thể xem như là tổng trực tiếp của các vành cyclic  $\mathbb{Z}_{p_i^{e_i}}$ , nghĩa là:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{e_r}}.$$

*Chứng minh.* Khẳng định thứ ba là trường hợp đặc biệt của khẳng định thứ hai.

Khẳng định thứ hai sẽ chứng minh được bằng phương pháp quy nạp và dựa trên khẳng định thứ nhất.

Do đó ta chỉ cần chứng minh khẳng định đầu tiên. Ta sẽ sử dụng Định lý đồng cấu vành để chứng minh khẳng định này. Gọi  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_k \oplus \mathbb{Z}_m$  là tương ứng được xác định bởi

$$\phi(r) = (\bar{r}, \bar{r}).$$

•  $\phi$  là một ánh xạ. Thật vậy, cho  $r, s \in \mathbb{Z}$  và  $r = s$ . Khi đó  $\phi(r) = (\bar{r}, \bar{r})$  và  $\phi(s) = (\bar{s}, \bar{s})$ . Vì  $r = s$ , nên ta có  $\bar{r}_k = \bar{s}_k$  và  $\bar{r}_m = \bar{s}_m$ . Do đó,  $(\bar{r}, \bar{r}) = (\bar{s}, \bar{s})$ . Vậy  $\phi(r) = \phi(s)$ .

- $\phi$  là một đồng cấu vành. Thật vậy, với mọi  $a, b \in \mathbb{Z}$  ta có

$$\begin{aligned}\phi(a + b) &= (\overline{a + b}, \overline{a + b}) = (\overline{a} + \overline{b}, \overline{a} + \overline{b}) \\ &= (\overline{a}, \overline{a}) + (\overline{b}, \overline{b}) = \phi(a) + \phi(b)\end{aligned}$$

và

$$\begin{aligned}\phi(ab) &= (\overline{ab}, \overline{ab}) = (\overline{a}\overline{b}, \overline{a}\overline{b}) \\ &= (\overline{a}, \overline{a})(\overline{b}, \overline{b}) = \phi(a)\phi(b).\end{aligned}$$

- $\phi$  là toàn ánh. Thật vậy, cho  $(\overline{a}, \overline{b}) \in \mathbb{Z}_k \oplus \mathbb{Z}_m$ . Khi đó  $(\overline{a}, \overline{b}) = (a + uk, b + vm)$  với  $a, b, u, v \in \mathbb{Z}$ . Vì  $(k, m) = 1$ , nên tồn tại các số nguyên  $x, y$  sao cho  $xk + ym = 1$ . Khi đó ta có  $a = axk + aym$  và  $b = bxx + bym$ . Xét  $(aym + bxx) \in \mathbb{Z}$ . Ta có  $\phi(aym + bxx) = (\overline{aym}, \overline{bxx})$ . Tuy nhiên,  $(\overline{a}, \overline{b}) = (\overline{axk + aym}, \overline{bxx + bym}) = (\overline{axk} + \overline{aym}, \overline{bxx} + \overline{bym}) = (\overline{aym}, \overline{bxx})$ . Vậy  $\phi(aym + bxx) = (\overline{a}, \overline{b})$ . Do đó  $\phi$  là toàn ánh.

Theo Định lý đồng cấu vành, ta có  $\mathbb{Z}/\ker \phi \cong \phi(\mathbb{Z})$  mà  $\phi(\mathbb{Z}) = \mathbb{Z}_k \oplus \mathbb{Z}_m$  do  $\phi$  là toàn cấu. Vì vậy  $\mathbb{Z}/\ker \phi \cong \mathbb{Z}_k \oplus \mathbb{Z}_m$ .

- $\ker \phi = n\mathbb{Z}$ . Thật vậy,

$$\begin{aligned}\ker \phi &= \{a \in \mathbb{Z} \mid \overline{a} = \overline{0} \in \mathbb{Z}_k, \overline{a} = \overline{0} \in \mathbb{Z}_m\} \\ &= \{a \in \mathbb{Z} \mid k|a, m|a\} \text{ mà } (k, m) = 1 \\ &= \{a \in \mathbb{Z} \mid (mk)|a\} \\ &= \{a \in \mathbb{Z} \mid n|a\} \\ &= n\mathbb{Z}.\end{aligned}$$

Do đó  $\ker \phi = n\mathbb{Z}$ . Vậy ta có  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_k \oplus \mathbb{Z}_n$  hay  $\mathbb{Z}_n \cong \mathbb{Z}_k \oplus \mathbb{Z}_n$ . Như vậy định lý được chứng minh.  $\square$

Từ Định lý 1.2.3, để thực hiện một chuỗi các phép tính trong  $\mathbb{Z}_n$ , ta có thể thực hiện các phép tính tương tự một cách độc lập trên mỗi  $\mathbb{Z}_{k_i}$  và kết quả nhận được bằng cách áp dụng đẳng cấu (từ phải sang trái). Bằng cách này ta có thể tính toán nhanh hơn nhiều so với tính toán trực tiếp khi  $n$  và

số phép tính lớn. Phương pháp này được gọi là tính toán đa môđun và được sử dụng rộng rãi trong đại số tuyến tính trên các số nguyên hoặc số hữu tỉ.

Bây giờ, ta sẽ sử dụng cách xây dựng nghiệm trong chứng minh Định lý 1.2.1 để giải bài toán được đề cập đến trong phần mở đầu.

**1.2.4 Ví dụ.** "Có một số đồ vật biết rằng số đó chia cho 3 dư 2, chia cho 5 dư 3 và chia cho 7 thì dư 2. Tìm số lượng đồ vật đó".

### Giải

Giả sử  $x$  là số đồ vật chưa biết. Khi đó  $x$  là nghiệm của hệ phương trình đồng dư:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7}. \end{cases}$$

Đặt  $M = 3 \cdot 5 \cdot 7 = 105$ . Vậy  $M_1 = \frac{105}{3} = 35$ ,  $M_2 = \frac{105}{5} = 21$  và  $M_3 = \frac{105}{7} = 15$ . Khi đó  $M_1 y_1 \equiv 1 \pmod{3}$  tương đương với  $35y_1 \equiv 1 \pmod{3}$  hay  $2y_1 \equiv 1 \pmod{3}$ . Suy ra  $y_1 = 2 \pmod{3}$ . Tương tự,  $M_2 y_2 \equiv 1 \pmod{5}$  trở thành  $21y_2 \equiv 1 \pmod{5}$ . Ta thu được  $y_2 \equiv 1 \pmod{5}$ . Và  $M_3 y_3 \equiv 1 \pmod{7}$  trở thành  $15y_3 \equiv 1 \pmod{7}$ . Ta thu được  $y_3 \equiv 1 \pmod{7}$ .

Vậy  $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233 \equiv 23 \pmod{105}$  là nghiệm của hệ phương trình.

Kiểm tra lại, dễ thấy  $23 \equiv 2 \pmod{3}$ ,  $23 \equiv 3 \pmod{5}$ ,  $23 \equiv 2 \pmod{7}$ .

Như vậy hệ phương trình đồng dư

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

có nghiệm duy nhất  $x \equiv 23 \pmod{105}$ .

Ta sẽ giải quyết bài toán đếm số lượng binh lính được đề cập trong Mục 1.1.

**1.2.5 Ví dụ.** Để tránh kẻ thù biết số lượng binh lính mình có, một vị tướng đã nghĩ ra cách đếm binh lính của mình theo cách sau đây. Đầu tiên ông ta yêu cầu binh lính nhóm thành các hàng gồm 11 người, sau đó là hàng gồm 17, 29 và 31 người. Tương ứng, mỗi lần ông ta được báo cáo còn dư 8, 5, 16, và 24 người. Sau đó, vị tướng sẽ tự mình tính toán số lượng binh lính.

Như ở Mục 1.1, ta có hệ phương trình đồng dư về số lượng quân ra trận:

$$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 5 \pmod{17} \\ x \equiv 16 \pmod{29} \\ x \equiv 24 \pmod{31}. \end{cases}$$

Vì tất cả các modulo đều đôi một nguyên tố cùng nhau nên ta sử dụng Định lý Thặng dư Trung Hoa để tìm  $x$ . Ta có  $M = 11 \cdot 17 \cdot 29 \cdot 31 = 168113$ , vì vậy  $M_1 = \frac{168113}{11} = 15283$ ,  $M_2 = \frac{168113}{17} = 9889$ ,  $M_3 = \frac{168113}{29} = 5797$  và  $M_4 = \frac{168113}{31} = 5423$ . Ta xác định  $y_1$  bằng cách giải phương trình đồng dư  $15283y_1 \equiv 1 \pmod{11}$ , tương đương với  $4y_1 \equiv 1 \pmod{11}$ . Như vậy  $y_1 \equiv 3 \pmod{11}$ . Bằng cách giải  $9889y_2 \equiv 1 \pmod{17}$ , tương đương với  $12y_2 \equiv 1 \pmod{17}$ , ta tìm được  $y_2 \equiv 10 \pmod{17}$ . Tương tự,  $5797y_3 \equiv 1 \pmod{29}$ , tương đương với  $26y_3 \equiv 1 \pmod{29}$ . Ta nhận được  $y_3 \equiv 19 \pmod{29}$ . Cuối cùng, ta giải  $5423y_4 \equiv 1 \pmod{31}$  hay  $29y_4 \equiv 1 \pmod{31}$  thu được  $y_4 \equiv 15 \pmod{31}$ .

Do đó, ta tính số lượng binh lính ra trận bằng

$$\begin{aligned} x &= 8 \cdot 15283 \cdot 3 + 5 \cdot 9889 \cdot 10 + 16 \cdot 5797 \cdot 19 + 24 \cdot 5423 \cdot 15 \\ &\equiv 36759 \pmod{168113}. \end{aligned}$$

Vì vậy, số lượng binh sĩ đồng dư với  $36759 \pmod{168113}$ .

### 1.3 Code thuật toán thặng dư Trung Hoa

Dưới đây là chương trình code dựa trên Định lý thặng dư Trung Hoa cho số nguyên. Đầu vào (Input) lần lượt nhập số phương trình trong hệ phương

trình đồng dư, các modulo và các số dư tương ứng. Kết quả (Output) thu được là nghiệm của hệ phương trình đồng dư đã nhập.

```
main.cpp
1  #include <bits/stdc++.h>
2  using namespace std;
3  int tích = 1;
4  // thuật toán euclid mở rộng
5  int uclnExtended(int a, int b, int* x, int* y)
6  {
7
8      // th cơ bản
9      if (a == 0) {
10         *x = 0, *y = 1;
11         return b;
12     }
13
14     int x1, y1;
15     int ucln = uclnExtended(b % a, a, &x1, &y1);
16
17     *x = y1 - (b / a) * x1;
18     *y = x1;
19
20     return ucln;
21 }
22 // Hàm tìm nghịch đảo của A theo modun M
23 int nghichdaomodun(int A, int M)
24 {
25     int x, y;
26     int g = uclnExtended(A, M, &x, &y);
27     if (g != 1)
28         return -1;
29     else {
30
31         //đề phòng th x âm, cộng thêm M.
32         int res = (x % M + M) % M;
33         return res;
34     }
35 }
36 int findMinX(int modun[], int du[], int k)
37 {
38
```



```

39     int result = 0;
40
41     // theo công thức nghiệm định lí thặng dư trung hoa
42     for (int i = 0; i < k; i++) {
43         int pp = tích / modun[i];
44         result += du[i] * nghichdaomodun(pp, modun[i]) * pp;
45     }
46
47     return result % tích;
48 }
49
50 int main(void)
51 {
52     cout<<"Nhập số phương trình của hệ đồng dư k=";
53     int k;
54     cin>>k;
55
56     int modun[k];
57     int du[k];
58     cout<<"Nhập các modun";
59     for (int i=0;i<k;i++) cin>>modun[i];
60     cout<<"Nhập các số dư tương ứng";
61     for (int i=0;i<k;i++) cin>>du[i];
62
63     // tính tích tất cả các modulo
64     for (int i = 0; i < k; i++)
65         tích *= modun[i];
66     cout << "nghiệm x đồng dư với "
67     << findMinX(modun, du, k)<<" theo modun "<<tích;
68     return 0;
69 }
70
71

```

Một ví dụ minh họa khi chạy chương trình code.

```

Nhập số phương trình của hệ đồng dư k=4
Nhập các modun 11 17 29 31
Nhập các số dư tương ứng 8 5 16 24
nghiệm x đồng dư với 36759 theo modun 168113

```

## 1.4 Ứng dụng của Định lý thặng dư Trung Hoa trong việc giải hệ phương trình đồng dư bậc nhất một ẩn

Bằng việc giải các phương trình đồng dư bậc nhất, ta có thể đưa các hệ phương trình đồng dư bậc nhất về hệ phương trình có dạng sau:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k}. \end{cases} \quad (1)$$

Ở thế kỷ XIII, trong cuốn “Cửu Mục Toán Học” (The Mathematical Treatise in Nine Sections - 1247), Tần Cửu Tiêu (Quin Jiushao) đã mô tả phương pháp “tổng hợp DaYan”, đây là phiên bản tổng quát của Định lý Thặng dư Trung Hoa. Phương pháp này nhằm mục đích đưa hệ phương trình đồng dư dạng (1) không hạn chế các môđun  $m_i$  đôi một nguyên tố cùng nhau về dạng thông thường (tức là các môđun đôi một nguyên tố cùng nhau)

$$\begin{cases} x \equiv a_1 \pmod{c_1} \\ x \equiv a_2 \pmod{c_2} \\ \dots \\ x \equiv a_k \pmod{c_k} \end{cases} \quad (2)$$

với  $c_1, c_2, \dots, c_k$  là các số nguyên dương đôi một nguyên tố cùng nhau. Từ đó áp dụng Định lý thặng dư Trung Hoa để tìm lời giải phù hợp.

Ký hiệu  $m = [m_1, \dots, m_k]$  là bội chung nhỏ nhất của các số nguyên  $m_1, \dots, m_k$ .  $d_{ij} = (m_i, m_j)$ ,  $1 \leq i, j \leq k$  là ước chung lớn nhất của hai số nguyên  $m_i, m_j$ .

**1.4.1 Định lý.** *Nếu hệ phương trình đồng dư bậc nhất (1) có nghiệm thì hệ này có một nghiệm duy nhất theo modulo  $m$ .*

*Chứng minh.* Giả sử hệ (1) có các nghiệm  $x \equiv x_1 \pmod{m}$  và  $x \equiv x_2 \pmod{m}$ , khi đó

$$x_1 \equiv a_i \pmod{m_i}, x_2 \equiv a_i \pmod{m_i}, \forall i = 1, 2, \dots, k.$$

Theo tính chất bắc cầu của quan hệ đồng dư ta có

$$x_1 \equiv x_2 \pmod{m_i}, \forall i = 1, 2, \dots, k.$$

Từ đó thu được  $x_1 \equiv x_2 \pmod{m}, \forall i = 1, 2, \dots, k$ . Như vậy, các nghiệm  $x \equiv x_1 \pmod{m}$  và  $x \equiv x_2 \pmod{m}$  của hệ phương trình đồng dư đang xét là trùng nhau.  $\square$

**1.4.2 Định lý.** Nếu hệ phương trình đồng dư bậc nhất (1) có nghiệm thì hiệu  $a_i - a_j$  chia hết cho  $d_{ij}$  với mọi  $i, j = 1, \dots, k$ .

*Chứng minh.* Giả sử hệ phương trình (1) có nghiệm, khi đó tồn tại một số nguyên  $x_0$  sao cho  $x_0 \equiv a_i \pmod{m_i}, \forall i = 1, 2, \dots, k$ . Với  $1 \leq i, j \leq k$  ta xét hai đồng dư thức

$$x_0 \equiv a_i \pmod{m_i},$$

$$x_0 \equiv a_j \pmod{m_j}.$$

Khi đó, tồn tại một số nguyên  $t_0$  nào đó sao cho  $x_0 = a_j + m_j t_0$ . Từ đó  $a_j + m_j t_0 \equiv a_i \pmod{m_i}$  hay  $m_j t_0 \equiv a_i - a_j \pmod{m_i}$ . Từ định lý về điều kiện có nghiệm của phương trình đồng dư bậc nhất suy ra  $d_{ij} = (m_i, m_j)$  là ước của  $a_i - a_j$ . Định lý được chứng minh.  $\square$

**Phương pháp của Tần Cửu Tiêu chuyển hệ phương trình dạng (1) về hệ phương trình dạng (2) được mô tả như sau:**

Cho các số nguyên  $m_1, m_2, \dots, m_k$  và  $m = [m_1, \dots, m_k]$  là bội chung nhỏ nhất của  $m_1, \dots, m_k$ . Ta tìm các số nguyên  $c_1, c_2, \dots, c_k$  thỏa mãn:

1.  $c_i$  là ước của  $m_i, i = 1, 2, \dots, k$ ;
2.  $\gcd(c_i, c_j) = 1$  với mọi  $i \neq j$ ;
3.  $c_1 c_2 \dots c_k = m = [m_1, \dots, m_k]$ .

Khi đó hệ phương trình đồng dư

$$x \equiv a_i \pmod{m_i} \text{ với } i = 1, \dots, k$$

được chuyển đổi thành hệ phương trình đồng dư

$$x \equiv a_i \pmod{c_i} \text{ với } i = 1, \dots, k,$$

trong đó các modulo  $c_i$  là các số đôi một nguyên tố cùng nhau.

Để tìm tập hợp các số nguyên  $c_i$  với  $i = 1, \dots, k$  ta phải thực hiện quy trình sau.

Xét trường hợp đầu tiên với  $k = 2$  :

**B1.** Đặt  $(m_1, m_2) = d_1$ . Nếu  $(m_1/d_1, m_2) = 1$ , thì lấy

$$c_1 = \frac{m_1}{d_1}, c_2 = m_2.$$

**B2.** Nếu  $(m_1, m_2/d_1) = 1$ , thì lấy

$$c_1 = m_1, c_2 = \frac{m_2}{d_1}.$$

**B3.** Nếu  $(m_1, m_2/d_1) = d_2 > 1$ , thì tính  $d_3 = (m_1/d_2, m_2d_2/d_1)$  trong đó  $d_2$  là ước của  $d_1$  và  $d_3$  là ước của  $d_1/d_2$ . Nếu  $d_3 = 1$  thì lấy  $c_1 = m_1/d_2$  và  $c_2 = m_2d_2/d_1$ , nếu không thì tính  $d_4 = (m_1/d_2d_3, m_2d_2d_3/d_1)$ . Tiếp tục quá trình này cho đến khi tồn tại một số nguyên  $s$  sao cho  $d_{s+1} = 1$ . Số  $s$  như vậy tồn tại vì  $d_1 > d_2 > \dots \geq 0$ . Khi đó lấy

$$c_1 = \frac{m_1}{d_2d_3\dots d_s}, c_2 = \frac{m_2d_2d_3\dots d_s}{d_1}.$$

Vậy  $(c_1, c_2) = 1$ .

Đối với trường hợp  $k > 2$ , đầu tiên ta áp dụng thuật toán trên cho  $m_k$  và  $m_{k-1}$  để thu được  $c_k^{(1)}, c'_{k-1}$ . Sau đó, áp dụng thuật toán tương tự cho  $c_k^{(1)}$  và  $m_{k-2}$  sẽ thu được  $c_k^{(2)}, c'_{k-2}$ . Tiếp tục quá trình này và cuối cùng áp dụng thuật toán cho  $c_k^{(k-2)}$  và  $m_1$ , thu được  $c_k, c'_1$ . Khi đó các số

nguyên  $c'_1, c'_2, \dots, c'_{k-1}, c_k$  thỏa mãn  $(c_k, c'_i) = 1$  với  $i = 1, 2, \dots, k-1$  và  $[c_1, c_2, \dots, c_k] = [c'_1, c'_2, \dots, c'_{k-1}, c_k] = c_k \cdot [c'_1, c'_2, \dots, c'_{k-1}]$ .

Như vậy, trường hợp  $k$  modulo đã được quy về trường hợp  $k-1$  modulo. Nếu lặp lại quá trình này, ta sẽ thu được các số  $c_1, \dots, c_k$  như mong muốn.

Sau đây là một số ví dụ minh họa cho điều vừa trình bày.

**1.4.3 Ví dụ.** Cho  $m_1 = 12$  và  $m_2 = 20$  là cặp số nguyên không nguyên tố cùng nhau. Khi đó  $[12, 20] = 60$ . Vì  $(12, 20) = 4$  và  $\left(\frac{12}{4}, 20\right) = 1$  nên theo bước 1, lấy  $c_1 = 3$  và  $c_2 = 20$  thì  $(c_1, c_2) = 1$ . Do đó, ta có  $c_1 c_2 = 3 \cdot 20 = 60 = [m_1, m_2]$ . Nếu ta có một hệ phương trình đồng dư được cho bởi

$$\begin{cases} x \equiv a_1 \pmod{12} \\ x \equiv a_2 \pmod{20} \end{cases}$$

thì nó sẽ trở thành

$$\begin{cases} x \equiv a_1 \pmod{3} \\ x \equiv a_2 \pmod{20} \end{cases}$$

trong đó 3 và 20 là các số nguyên nguyên tố cùng nhau.

**1.4.4 Ví dụ.** Cho  $m_1 = 12$  và  $m_2 = 18$  trong đó  $m_1$  và  $m_2$  không nguyên tố cùng nhau. Sử dụng thuật toán, tính được  $d_1 = (m_1, m_2) = (12, 18) = 6$ ;  $d_2 = \left(m_1, \frac{m_2}{d_1}\right) = (12, 3) = 3$ ;  $d_3 = \left(\frac{m_1}{d_2}, \frac{m_2 d_2}{d_1}\right) = (4, 9) = 1$ . Vì  $d_3 = 1$  nên ta lấy  $c_1 = \frac{m_1}{d_2} = 4$  và  $c_2 = \frac{m_2 d_2}{d_1} = 9$ .

Khi đó hệ phương trình đồng dư

$$\begin{cases} x \equiv a_1 \pmod{12} \\ x \equiv a_2 \pmod{18} \end{cases}$$

sẽ trở thành

$$\begin{cases} x \equiv a_1 \pmod{4} \\ x \equiv a_2 \pmod{9}. \end{cases}$$

Trong tính toán ứng dụng lịch nêu ở Mục 1.1, thuật toán được sử dụng với 2 modulo.

**1.4.5 Ví dụ.** Nếu ngày Đông chí của một năm nào đó xảy ra  $r_1$  ngày sau thượng nguyên và  $r_2$  ngày sau ngày trăng non thì năm đó là  $N$  năm sau thượng nguyên. Hệ phương trình đồng dư:

$$\begin{cases} xN \equiv r_1 \pmod{60} \\ xN \equiv r_2 \pmod{y} \end{cases}$$

cho biết số năm  $N$  sau Thượng Nguyên, trong đó  $x$  là số ngày trong một năm nhiệt đới,  $y$  là số ngày trong một tháng âm lịch.

Giả sử số ngày trong một năm nhiệt đới là 365 và số ngày trong một tháng âm lịch là 30. Khi đó  $x = 365$  và  $y = 30$ . Ngày đông chí diễn ra sau thượng nguyên  $r_1$  ngày và sau ngày trăng non  $r_2$  ngày. Ta có hệ phương trình đồng dư:

$$\begin{cases} 365N \equiv r_1 \pmod{60} \\ 365N \equiv r_2 \pmod{30} \end{cases}$$

được chuyển đổi thành

$$\begin{cases} 5N \equiv r_1 \pmod{60} \\ 5N \equiv r_2 \pmod{30} \end{cases}$$

trong đó  $N$  là số năm sau Thượng Nguyên. Theo thuật toán đã trình bày trên đây, ta có  $d_1 = (60, 30) = 30$ ;  $d_2 = (60, 1) = 1$ . Vì vậy, lấy  $c_1 = 60$  và  $c_2 = 1$  thì hệ phương trình đồng dư mới sẽ là:

$$\begin{cases} 5N \equiv r_1 \pmod{60} \\ 5N \equiv r_2 \pmod{1} \end{cases}$$

hay  $5N \equiv r_1 \pmod{60}$ .

Cuối cùng ta sẽ sử dụng thuật toán trên để minh họa ví dụ về việc xây móng đã nêu ở Mục 1.1 theo  $k$  modulo với  $k > 2$ .

**1.4.6 Ví dụ.** Để xây dựng một nền móng hình chữ nhật cho một tòa thành, có bốn loại vật liệu có sẵn: khối vật liệu lập phương lớn mỗi cạnh dài 130 đơn vị; khối vật liệu lập phương nhỏ mỗi cạnh dài 110 đơn vị; gạch "thành phố" dài 120 đơn vị, rộng 60 đơn vị và dày 25 đơn vị; và gạch "sáu cửa" dài 100 đơn vị, rộng 50 đơn vị và dày 20 đơn vị. Bốn loại vật liệu này được sử dụng để xây dựng các phần móng mà không làm hỏng bất kỳ viên nào. Do đó, ta có một hệ phương trình đồng dư khi tính toán các vật liệu khác nhau cho mỗi lần sử dụng một loại vật liệu cụ thể. Nếu sử dụng khối lập phương lớn, chiều dài móng thừa 60 đơn vị, nhưng chiều rộng cần thêm 60 đơn vị. Nếu sử dụng khối lập phương nhỏ, chiều dài móng thừa 20 đơn vị, nhưng chiều rộng cần thêm 30 đơn vị. Nếu tính theo chiều dài của gạch "thành phố", chiều dài móng thừa 30 đơn vị, nhưng chiều rộng cần thêm 10 đơn vị. Nếu tính theo chiều rộng của gạch "thành phố", chiều dài móng thừa 30 đơn vị, nhưng chiều rộng cần thêm 10 đơn vị. Nếu tính theo độ dày của gạch "thành phố", chiều dài móng thừa 5 đơn vị, nhưng chiều rộng cần thêm 10 đơn vị. Nếu tính theo chiều dài, chiều rộng và độ dày của gạch "sáu cửa", chiều dài móng tương ứng thừa 30, 30 và 10 đơn vị; chiều rộng móng lần lượt thừa 10, 10 và 10 đơn vị. Mục tiêu là tìm chiều dài  $X$  và chiều rộng  $Y$  của móng.

Bài toán này được đơn giản hóa thành hệ phương trình đồng dư:

$$\begin{cases} X \equiv 60 \pmod{130} \\ X \equiv 30 \pmod{120} \\ X \equiv 20 \pmod{110} \\ X \equiv 30 \pmod{100} \\ X \equiv 30 \pmod{60} \\ X \equiv 30 \pmod{50} \\ X \equiv 5 \pmod{25} \\ X \equiv 10 \pmod{20} \end{cases}$$

và

$$\left\{ \begin{array}{l} Y \equiv 60 \pmod{130} \\ Y \equiv 10 \pmod{120} \\ Y \equiv 30 \pmod{110} \\ Y \equiv 10 \pmod{100} \\ Y \equiv 10 \pmod{60} \\ Y \equiv 10 \pmod{50} \\ Y \equiv 10 \pmod{25} \\ Y \equiv 10 \pmod{20}. \end{array} \right.$$

. Ta sẽ sử dụng thuật toán để biến đổi các modulo đã cho thành các modulo đôi một nguyên tố cùng nhau.

Xét hệ phương trình đồng dư:

$$\left\{ \begin{array}{l} X \equiv 60 \pmod{130} \\ X \equiv 30 \pmod{120} \\ X \equiv 20 \pmod{110} \\ X \equiv 30 \pmod{100} \\ X \equiv 30 \pmod{60} \\ X \equiv 30 \pmod{50} \\ X \equiv 5 \pmod{25} \\ X \equiv 10 \pmod{20}. \end{array} \right.$$

Ta bắt đầu từ dưới lên. Trước hết, cho  $m_i, i = 1, 2, \dots, 8$  như sau:  $m_1 = 130, m_2 = 120, m_3 = 110, m_4 = 100, m_5 = 60, m_6 = 50, m_7 = 25$  và  $m_8 = 20$ . Ta bắt đầu với  $m_8 = 20$  và  $m_7 = 25$ . Khi đó,  $d_1 = (20, 25) = 5$ ;  $d_2 = \left(20, \frac{25}{5}\right) = 5$ ;  $d_3 = \left(\frac{20}{5}, \frac{25 \cdot 5}{5}\right) = 1$ . Vậy  $\alpha_8^{(1)} = \frac{20}{5} = 4$  và  $\alpha'_7 = 25$ .

Bây giờ hãy áp dụng thuật toán cho  $\alpha_8^{(1)} = 4$  và  $m_6 = 50$ . Tương tự, ta có  $d_1 = (4, 50) = 2$ . Khi đó  $d_2 = \left(4, \frac{50}{2}\right) = 1$ . Vậy  $\alpha_8^{(2)} = 4$  và  $\alpha'_6 = 25$ .



Tiếp tục quá trình này, áp dụng thuật toán cho  $\alpha_8^{(2)} = 4$  và  $m_5 = 60$ . Khi đó  $d_1 = (4, 60) = 4$ ;  $d_2 = \left(4, \frac{60}{4}\right) = (4, 15) = 1$ . Ta có  $\alpha_8^{(3)} = 4$  và  $\alpha'_5 = 15$ .

Tiếp theo, áp dụng quy trình cho  $\alpha_8^{(3)} = 4$  và  $m_4 = 100$ . Khi đó  $d_1 = (4, 100) = 4$ ;  $d_2 = \left(4, \frac{100}{4}\right) = (4, 25) = 1$ . Vậy  $\alpha_8^{(4)} = 4$  và  $\alpha'_4 = 25$ .

Cặp tiếp theo là  $\alpha_8^{(4)} = 4$  và  $m_3 = 110$ . Vậy  $d_1 = (4, 110) = 2$ ;  $d_2 = \left(4, \frac{110}{2}\right) = (4, 55) = 1$ . Do đó,  $\alpha_8^{(5)} = 4$  và  $\alpha'_3 = 55$ .

Tiếp tục với  $\alpha_8^{(5)} = 4$  và  $m_2 = 120$ . Ta nhận được  $d_1 = (4, 120) = 4$ ;  $d_2 = \left(4, \frac{120}{4}\right) = (4, 30) = 2$ ;  $d_3 = \left(\frac{4}{2}, \frac{120 \cdot 2}{4}\right) = (2, 60) = 2$ ;  $d_4 = \left(\frac{4}{2 \cdot 2}, \frac{120 \cdot 2 \cdot 2}{4}\right) = (1, 120) = 1$ . Do đó,  $\alpha_8^{(6)} = 1$  và  $\alpha'_2 = 120$ .

Cuối cùng là cặp  $\alpha_8^{(6)} = 1$  và  $m_1 = 130$ . Rõ ràng, hai số này nguyên tố cùng nhau nên ta thu được  $\alpha_8 = 1$  và  $\alpha'_1 = 130$ .

Lúc này ta đã giảm 8 modulo thành 7 modulo với modulo cuối cùng nguyên tố cùng nhau với các modulo còn lại. Ta có 7 modulo theo thứ tự: 130, 120, 55, 25, 15, 25, 25. Áp dụng lại quy trình này, ta có  $d_1 = (\alpha'_7, \alpha'_6) = (25, 25) = 25$ ;  $d_2 = \left(25, \frac{25}{25}\right) = 1$ . Vậy lấy  $\beta_7^{(1)} = 25$  và  $\beta'_6 = 1$ .

Tiếp theo,  $d_1 = (25, 15) = 5$ ;  $d_2 = \left(25, \frac{15}{5}\right) = 1$ . Do đó,  $\beta_7^{(2)} = 25$  và  $\beta'_5 = 3$ .

Một lần nữa,  $d_1 = (25, 25) = 25$ , sau đó  $d_2 = \left(25, \frac{25}{25}\right) = 1$ . Do đó, lấy  $\beta_7^{(3)} = 25$  và  $\beta'_4 = 1$ .

Tương tự,  $d_1 = (25, 55) = 5$  và  $d_2 = \left(25, \frac{55}{5}\right) = 1$ . Lấy  $\beta_7^{(4)} = 25$  và  $\beta'_3 = 11$ .

Bây giờ ta có  $d_1 = (25, 120) = 5$ ;  $d_2 = \left(25, \frac{120}{5}\right) = 1$ . Lấy  $\beta_7^{(5)} = 25$  và  $\beta'_2 = 24$ .

Cuối cùng,  $d_1 = (25, 130) = 5$ ;  $d_2 = \left(25, \frac{130}{5}\right) = 1$ . Do đó  $\beta_7 = 25$  và

$$\beta'_1 = 26.$$

Các modulo mới là 26, 24, 11, 1, 3, 1, 25. Ta có thể thấy rằng các modulo đôi một nguyên tố cùng nhau ngoại trừ hai modulo 26 và 24. Vì vậy, ta sẽ sử dụng thuật toán một lần nữa để chuyển đổi chúng thành cặp số nguyên tố cùng nhau.

Đặt  $d_1 = (26, 24) = 2$ ;  $d_2 = \left(26, \frac{24}{2}\right) = 2$ ;  $d_3 = \left(\frac{26}{2}, \frac{24 \cdot 2}{2}\right) = 1$ . Do đó, hai modulo 26 và 24 bây giờ trở thành 13 và 12. Tuy nhiên, điều này tạo ra một cặp không nguyên tố cùng nhau là 12 và 3. Một lần nữa, ta áp dụng thuật toán cho hai modulo này.

Ta có  $d_1 = (12, 3) = 3$ ;  $d_2 = (12, 1) = 1$ . Vì vậy, hai modulo mới là 12 và 1. Bây giờ ta có một hệ phương trình đồng dư mới với các modulo đôi một nguyên tố cùng nhau:

$$\begin{cases} X \equiv 60 \pmod{13} \\ X \equiv 30 \pmod{12} \\ X \equiv 20 \pmod{11} \\ X \equiv 30 \pmod{1} \\ X \equiv 30 \pmod{1} \\ X \equiv 30 \pmod{1} \\ X \equiv 5 \pmod{25} \\ X \equiv 10 \pmod{1} \end{cases}$$

hay

$$\begin{cases} X \equiv 8 \pmod{13} \\ X \equiv 6 \pmod{12} \\ X \equiv 9 \pmod{11} \\ X \equiv 5 \pmod{25} \end{cases}$$

Sử dụng Định lý Thặng dư Trung Hoa, ta thu được  $M = 13 \cdot 12 \cdot 11 \cdot 25 = 42900$ . Do đó,  $M_1 = \frac{42900}{13} = 3300$ ,  $M_2 = \frac{42900}{12} = 3575$ ,  $M_3 = \frac{42900}{11} =$

3900 và  $M_4 = \frac{42900}{25} = 1716$ .

Khi đó  $3300y_1 \equiv 1 \pmod{13}$  trở thành  $11y_1 \equiv 1 \pmod{13}$ , do đó  $y_1 \equiv 6 \pmod{13}$ . Tương tự,  $3575y_2 \equiv 1 \pmod{12}$ , tức là  $11y_2 \equiv 1 \pmod{12}$ . Vậy  $y_2 \equiv 11 \pmod{12}$ . Tương tự,  $3900y_3 \equiv 1 \pmod{11}$  trở thành  $6y_3 \equiv 1 \pmod{11}$ , do đó  $y_3 \equiv 2 \pmod{11}$ . Cuối cùng,  $1716y_4 \equiv 1 \pmod{25}$ , hay  $16y_4 \equiv 1 \pmod{25}$ . Vậy  $y_4 \equiv 11 \pmod{25}$ . Do đó,  $x = 8 \cdot 3300 \cdot 6 + 6 \cdot 3575 \cdot 11 + 9 \cdot 3900 \cdot 2 + 5 \cdot 1716 \cdot 11 = 558930 \pmod{42900} \equiv 1230 \pmod{42900}$ . Vậy chiều dài móng của bức tường đồng dư với  $12300 \pmod{42900}$ .

Để tìm chiều rộng đáy tường, ta thiết lập hệ phương trình đồng dư tương tự như trên với các modulo nguyên tố cùng nhau.

$$\begin{cases} Y \equiv 60 \pmod{13} \\ Y \equiv 10 \pmod{12} \\ Y \equiv 30 \pmod{11} \\ Y \equiv 10 \pmod{1} \\ Y \equiv 10 \pmod{1} \\ Y \equiv 10 \pmod{1} \\ Y \equiv 10 \pmod{25} \\ Y \equiv 10 \pmod{1} \end{cases}$$

hay

$$\begin{cases} Y \equiv 8 \pmod{13} \\ Y \equiv 10 \pmod{12} \\ Y \equiv 8 \pmod{11} \\ Y \equiv 10 \pmod{25} \end{cases}$$

Theo Định lý thặng dư Trung Hoa  $Y = 8 \cdot 3300 \cdot 6 + 10 \cdot 3575 \cdot 11 + 8 \cdot 3900 \cdot 2 + 10 \cdot 1716 \cdot 11 = 802220 \pmod{49000} \equiv 18220 \pmod{49000}$ . Vậy chiều rộng móng của bức tường đồng dư với  $18220 \pmod{42900}$ .

## CHƯƠNG 2

## CÁC PHÁT BIỂU KHÁC CỦA ĐỊNH LÝ THẶNG DƯ TRUNG HOA

### 2.1 Định lý Thặng dư Trung Hoa cho vành

Trong vành số nguyên  $\mathbb{Z}$ , cho hai ideal  $I = (a)$  và  $J = (b)$ . Ta có  $I + J = \mathbb{Z}$  khi và chỉ khi tồn tại  $u, v \in \mathbb{Z}$  sao cho  $au + bv = 1$  hay  $a$  và  $b$  là hai số nguyên tố cùng nhau. Từ nhận xét này người ta mở rộng khái niệm hai số nguyên tố cùng nhau trên vành  $\mathbb{Z}$  thành khái niệm hai ideal nguyên tố cùng nhau trên một vành giao hoán bất kỳ như sau.

**2.1.1 Định nghĩa.** Trong vành giao hoán  $R$ , hai ideal  $A$  và  $B$  được gọi là *nguyên tố cùng nhau* nếu  $A + B = R$ .

**2.1.2 Mệnh đề.** Cho  $R$  là một vành giao hoán có đơn vị.

1. Cho  $I, J$  là các ideal của  $R$ . Nếu  $I + J = R$  thì  $IJ = I \cap J$ .
2. Cho  $I_1, I_2, \dots, I_n$  là các ideal của  $R$ . Nếu  $I_1, I_2, \dots, I_n$  đôi một nguyên tố cùng nhau thì  $I_1 I_2 \cdots I_n = \bigcap_{i=1}^n I_i$ .

*Chứng minh.*

1. Giả sử  $r \in IJ$ . Khi đó tồn tại  $n \in \mathbb{N}, a_i \in I$  và  $b_i \in J$  sao cho  $r = \sum_{i=1}^n a_i b_i$ . Vì vậy  $r \in J$  và  $r \in I$  vì  $I$  và  $J$  là các ideal. Do đó  $r \in I \cap J$ .  
Vậy  $IJ \subseteq I \cap J$ .

Mặt khác, ta có

$$(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) = II \cap IJ + JI \cap JJ \subseteq IJ.$$

Vì  $I + J = R$  nên  $(I + J)(I \cap J) = (I \cap J)$ . Do đó  $I \cap J \subseteq IJ$ .

2. Ta sẽ tiến hành quy nạp theo  $n$ .

Trường hợp  $n = 2$  được chứng minh ở phần (1).

Giả sử  $n > 2$  và  $\prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$  (hay  $I_1 I_2 \cdots I_{n-1} = \bigcap_{i=1}^{n-1} I_i$ ).

Đặt  $J = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$ . Vì  $I_i + I_n = R$  với  $1 \leq i \leq n-1$ , nên tồn tại  $x_i \in I_i$  và  $y_i \in I_n$  sao cho  $x_i + y_i = 1$ . Do đó  $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{I_n}$ . Vậy  $I_n + J = R$ . Do đó,  $\prod_{i=1}^n I_i = JI_n = J \cap I_n = \bigcap_{i=1}^n I_i$ .

□

Sử dụng khái niệm idêan nguyên tố cùng nhau, người ta có thể mở rộng Định lý thặng dư Trung Hoa (Định lý 1.2.3) lên một vành bất kỳ. Trước hết ta xét trường hợp hai idêan.

### 2.1.3 Định lý. (Định lý Thặng dư Trung Hoa cho hai idêan)

Giả sử  $R$  là một vành giao hoán có đơn vị,  $I$  và  $J$  là các idêan thực sự của  $R$ . Nếu  $I + J = R$  thì  $R/(I \cap J)$  đẳng cấu với  $R/I \oplus R/J$ .

*Chứng minh.* Ta sẽ sử dụng Định lý đồng cấu vành để chứng minh định lý này. Gọi  $\phi : R \rightarrow R/I \oplus R/J$  là tương ứng được xác định bởi

$$\phi(r) = (r + I, r + J).$$

•  $\phi$  là một ánh xạ. Thật vậy, cho  $r, s \in R$  và  $r = s$ . Khi đó  $\phi(r) = (r + I, r + J)$  và  $\phi(s) = (s + I, s + J)$ . Vì  $r = s$ , nên ta có  $r + I = s + I$  và  $r + J = s + J$ . Do đó,  $(r + I, r + J) = (s + I, s + J)$ . Vậy,  $\phi(r) = \phi(s)$ .

•  $\phi$  là một đồng cấu. Thật vậy, với mọi  $a, b \in R$  ta có

$$\begin{aligned} \phi(a + b) &= (a + b + I, a + b + J) = (a + I + b + I, a + J + b + J) \\ &= (a + I, a + J) + (b + I, b + J) = \phi(a) + \phi(b) \end{aligned}$$

và

$$\begin{aligned}\phi(ab) &= (ab + I, ab + J) = ((a + I)(b + I), (a + J)(b + J)) \\ &= (a + I, a + J)(b + I, b + J) = \phi(a)\phi(b).\end{aligned}$$

•  $\phi$  là toàn ánh. Thật vậy, cho  $(\bar{a}, \bar{b}) \in R/I \oplus R/J$ . Khi đó  $(\bar{a}, \bar{b}) = (a + I, b + J)$  với  $a, b \in R$ . Vì  $R = I + J$ , nên ta có  $a = x + y$  và  $b = s + t$  với  $x, s \in I$  và  $y, t \in J$ . Xét  $y + s$ . Ta có  $\phi(y + s) = (y + s + I, y + s + J) = (y + I, s + J)$  vì  $s \in I, y \in J$ . Tuy nhiên,  $(\bar{a}, \bar{b}) = (a + I, b + J) = (x + y + I, s + t + J) = (y + I, s + J)$  vì  $x \in I$  và  $t \in J$ . Vậy  $\phi(y + s) = (\bar{a}, \bar{b})$ . Do đó  $\phi$  là toàn ánh.

Theo Định lý đồng cấu vành, ta có  $R/\ker \phi \cong \phi(R)$  mà  $\phi(R) = R/I \oplus R/J$  do đó  $\phi$  là toàn cấu. Vì vậy  $R/\ker \phi \cong R/I \oplus R/J$ .

•  $\ker \phi = I \cap J$ . Thật vậy, lấy  $r \in I \cap J$ . Do đó  $r \in I$  và  $r \in J$ . Khi đó  $\phi(r) = (r + I, r + J) = (I, J)$ . Vì vậy  $r \in \ker \phi \Rightarrow I \cap J \subseteq \ker \phi$ .

Giả sử  $b \in \ker \phi$ . Khi đó  $(b + I, b + J) = \phi(b) = (I, J)$ . Vậy  $b \in I$  và  $b \in J$ . Do đó  $b \in I \cap J \Rightarrow \ker \phi \subseteq (I \cap J)$ .

Do đó  $\ker \phi = I \cap J$ . Vậy ta có  $R/(I \cap J) \cong R/I \oplus R/J$ .  $\square$

Ví dụ sau đây cho thấy điều kiện  $I, J$  nguyên tố cùng nhau trong định lý trên là cần thiết, không thể bỏ đi được.

**2.1.4 Ví dụ.** Nếu  $R = \mathbb{Z}, I = (6)$  và  $J = (4)$  thì ánh xạ

$$\phi : R/(I \cap J) \rightarrow R/I \oplus R/J$$

không phải là toàn ánh.

*Chứng minh.* Vì  $\gcd(6, 4) = 2$  nên 6 và 4 không nguyên tố cùng nhau. Vì vậy các ideal  $(6)$  và  $(4)$  không nguyên tố cùng nhau. Ta có  $(6) + (4) = (2)$  nên  $I + J \neq \mathbb{Z}$  vì  $1 \notin (2)$ . Ngoài ra,  $\mathbb{Z}/((6) \cap (4)) \cong \mathbb{Z}/(2) = \mathbb{Z}_2$ , nhưng  $\mathbb{Z}_2 \not\cong \mathbb{Z}_4 \oplus \mathbb{Z}_6$ , vì  $\mathbb{Z}_2$  chỉ có 2 phần tử còn  $\mathbb{Z}_4 \oplus \mathbb{Z}_6$  có 24 phần tử. Vậy  $\phi$  không là toàn ánh.  $\square$

Định lý sau đây là một mở rộng của Định lý thặng dư Trung Hoa cho vành giao hoán đối với trường hợp  $n$  idêan.

**2.1.5 Định lý.** (*Định lý Thặng dư Trung Hoa cho  $n$  idêan*)

Cho  $R$  là một vành giao hoán có đơn vị và  $I_1, \dots, I_n$  là các idêan của  $R$  đôi một nguyên tố cùng nhau, tức là  $I_i + I_j = R$  với mọi  $i \neq j$ . Đặt  $I = \bigcap_{i=1}^n I_i$ . Khi đó vành  $R/I$  đẳng cấu với  $R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_n$ .

*Chứng minh.* Bằng quy nạp, với  $n = 1$ , ta có  $R/I \cong R/I$ .

Giả sử rằng  $I_1, \dots, I_n, I_{n+1}$  là các idêan của  $R$  đôi một nguyên tố cùng nhau và  $R/I$  đẳng cấu với  $R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_n$  trong đó  $I = \bigcap_{i=1}^n I_i$ .

Khi đó, bằng cách cho  $J = I_{n+1}$  và sử dụng Định lý 2.1.3, ta có

$$R/(I \cap J) \cong R/I \oplus R/J \cong R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_n \oplus R/J.$$

Vì  $I \cap J = \bigcap_{i=1}^{n+1} I_i$  nên  $R/(\bigcap_{i=1}^{n+1} I_i)$  đẳng cấu với  $R/I_1 \oplus R/I_2 \oplus \dots \oplus R/I_{n+1}$ . Định lý được chứng minh. □

**2.1.6 Hệ quả.** Nếu số nguyên  $m$  có phân tích tiêu chuẩn là  $m = p_1^{k_1} \dots p_i^{k_i}$  ( $k_i > 0, p_i$  là các số nguyên tố phân biệt), thì ta có đẳng cấu vành

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_i^{k_i}}.$$

*Chứng minh.* Vì tất cả các số  $p_i$  đều là các số nguyên tố phân biệt nên chúng là đôi một nguyên tố cùng nhau và  $\mathbb{Z}_m \cong \mathbb{Z}/(m)$ . Do đó, theo Định lý 2.1.5 và Mệnh đề 2.1.2, ta có  $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p_i^{k_i}}$ . □

**2.1.7 Định nghĩa.** Cho  $I$  là một idêan trong vành  $R$ ,  $a, b \in R$ . Ta nói  $a$  đồng dư với  $b$  theo modulo  $I$  nếu  $a - b \in I$  và kí hiệu là  $a \equiv b \pmod{I}$ .

Định lý Thặng dư Trung Hoa trên một vành giao hoán được phát biểu lại theo ngôn ngữ đồng dư như định lý dưới đây. Đây là phát biểu tổng quát cho Định lý 1.2.1.

### 2.1.8 Định lý. (Định lý Thặng dư Trung Hoa tổng quát trên vành)

Cho  $I_1, \dots, I_n$  là các ideal trong vành  $R$ ,  $I_i, I_j$  đôi một nguyên tố cùng nhau, tức là  $I_i + I_j = R$  với mọi  $i \neq j$ . Nếu  $b_1, \dots, b_n \in R$  thì tồn tại  $b \in R$  sao cho

$$b \equiv b_i \pmod{I_i} \text{ với } i = 1, 2, \dots, n.$$

Hơn nữa,  $b$  được xác định duy nhất theo modulo  $I_1 \cap I_2 \cap \dots \cap I_n$ .

Chứng minh. Vì  $I_1 + I_2 = R$  và  $I_1 + I_3 = R$ , nên

$$R = R^2 = (I_1 + I_2)(I_1 + I_3) = I_1^2 + I_1I_3 + I_2I_1 + I_2I_3 \subseteq I_1 + I_2I_3 \subseteq I_1 + (I_2 \cap I_3) \subseteq R.$$

Do đó,  $R = I_1 + (I_2 \cap I_3)$ . Giả sử quy nạp rằng

$$R = I_1 + (I_2 \cap I_3 \cap \dots \cap I_{k-1}).$$

Khi đó

$$R = R^2 = (I_1 + (I_2 \cap \dots \cap I_{k-1}))(I_1 + I_k) \subseteq I_1 + (I_2 \cap I_3 \cap \dots \cap I_k) \subseteq R.$$

Do đó,  $R = I_1 + (I_2 \cap \dots \cap I_k)$  hay  $R = I_1 + (\cap_{i \neq 1} I_i)$ . Tương tự, với mỗi  $k = 1, 2, \dots, n$ ,  $R = I_k + (\cap_{i \neq k} I_i)$ . Như vậy, với mỗi  $k$  tồn tại các phần tử  $a_k \in I_k$  và  $r_k \in \cap_{i \neq k} I_i$  sao cho  $b_k = a_k + r_k$ . Hơn nữa  $r_k \equiv b_k \pmod{I_k}$  và  $r_k \equiv 0 \pmod{I_i}$  với  $i \neq k$ .

Đặt  $b = r_1 + r_2 + \dots + r_n$ . Khi đó  $b \equiv r_i \pmod{I_i}$  và do đó  $b \equiv b_i \pmod{I_i}$  với mọi  $i$ . Cuối cùng, nếu  $c \in R$  sao cho  $c \equiv b_i \pmod{I_i}$  với mọi  $i$ , thì  $b \equiv c \pmod{I_i}$  với mọi  $i$  hay  $b - c \in I_i$  với mọi  $i$ . Do đó,  $b - c \in \cap_{i=1}^n I_i$  và  $b \equiv c \pmod{\cap_{i=1}^n I_i}$ .  $\square$

**2.1.9 Ví dụ.** Cho (2) và (3) là các ideal trong vành  $\mathbb{Z}$ . Khi đó ta có thể thấy rằng  $(2) + (3) = \mathbb{Z}$ . Với mọi  $a_1$  và  $a_2 \in \mathbb{Z}$ , tồn tại một  $a \in \mathbb{Z}$  sao cho  $a \equiv a_1 \pmod{2}$  và  $a \equiv a_2 \pmod{3}$ . Khi đó  $a \equiv m \pmod{(2) \cap (3)}$ , hay  $a \equiv m \pmod{6}$ . Kết quả này đưa ta trở lại định lý Thặng dư Trung Hoa cho số nguyên (Định lý 1.2.1).



## 2.2 Định lý Thặng dư Trung Hoa trên vành đa thức

Bây giờ ta sẽ xem xét Định lý số dư Trung Hoa được áp dụng như thế nào trên vành đa thức.

**2.2.1 Định nghĩa.** Cho  $D$  là một miền nguyên. Một đa thức  $f(x) \in D[x]$  khác 0 và không khả nghịch trong  $D[x]$  được gọi là *bất khả quy trên  $D$*  nếu không có hai đa thức không khả nghịch  $g(x), h(x) \in D[x]$  sao cho  $f(x) = g(x)h(x)$ .

Các phần tử  $a$  và  $b$  của miền nguyên  $D$  được gọi là *liên kết* nếu  $a = ub$  trong đó  $u$  là phần tử khả nghịch của  $D$ .

**2.2.2 Bổ đề.** Cho  $f(x)$  và  $g(x)$  là các đa thức bất khả quy trên trường  $F$ . Nếu  $f(x)$  và  $g(x)$  không liên kết, thì

$$F[x]/\langle f(x)g(x) \rangle \cong F[x]/\langle f(x) \rangle \oplus F[x]/\langle g(x) \rangle.$$

*Chứng minh.* Theo Định lý 2.1.3 và Định lý đồng cấu vành,  $F[x]/\langle f(x)g(x) \rangle$  đẳng cấu với  $F[x]/\langle f(x) \rangle \oplus F[x]/\langle g(x) \rangle$ . Ta chỉ cần kiểm tra xem nếu  $f(x)$  và  $g(x)$  không liên kết thì

$$\langle f(x)g(x) \rangle = \langle f(x) \rangle \langle g(x) \rangle = \langle f(x) \rangle \cap \langle g(x) \rangle.$$

Đặt  $r(x) \in \langle f(x)g(x) \rangle$ , thì  $r(x) = f(x)g(x)h(x)$  với  $h(x) \in F[x]$ . Khi đó  $r(x) = [f(x)h(x)]g(x)$  vì  $F$  là một trường. Do đó,  $r(x) \in \langle f(x) \rangle \cap \langle g(x) \rangle$  dẫn tới  $\langle f(x)g(x) \rangle \subseteq \langle f(x) \rangle \cap \langle g(x) \rangle$ .

Ngược lại, đặt  $s(x) \in \langle f(x) \rangle \cap \langle g(x) \rangle$ , do đó  $s(x) \in \langle f(x) \rangle$  và  $s(x) \in \langle g(x) \rangle$ . Khi đó,  $s(x) = f(x)h(x)$  và  $s(x) = g(x)r(x)$  với  $h(x), r(x) \in F[x]$ . Do đó, ta có  $f(x)h(x) = g(x)r(x)$ . Bởi vì  $f(x), g(x)$  là bất khả quy,  $\langle f(x) \rangle + \langle g(x) \rangle = F[x]$ , nên  $f(x)u(x) + g(x)v(x) = 1$ . Vì vậy

$$s(x)f(x)u(x) + s(x)g(x)v(x) = s(x).$$

Do đó,

$$s(x) = g(x)r(x)f(x)u(x) + f(x)h(x)g(x)v(x) = g(x)f(x)(r(x)u(x) + h(x)v(x))$$

nên  $s(x) \in \langle f(x)g(x) \rangle$ . Vậy  $\langle f(x) \rangle \cap \langle g(x) \rangle \subseteq \langle f(x)g(x) \rangle$ .  $\square$

Định lý thặng dư Trung Hoa tổng quát cho vành đa thức được phát biểu như sau.

**2.2.3 Định lý.** Cho  $F$  là một trường và  $b_1(x), \dots, b_n(x)$  là các đa thức tùy ý của  $F[x]$ .  $m_1(x), \dots, m_n(x)$  và  $a_1(x), \dots, a_n(x)$  là các đa thức của  $F[x]$  sao cho

$$\begin{cases} \gcd(m_i(x), m_j(x)) = 1, \forall i \neq j \\ \gcd(a_i(x), m_i(x)) = 1, i = 1, 2, \dots, n. \end{cases}$$

Khi đó hệ phương trình đồng dư

$$a_i(x)u(x) = b_i(x) \pmod{m_i(x)}, i = 1, 2, \dots, n$$

có nghiệm duy nhất theo modulo  $m(x) = m_1(x)m_2(x) \cdots m_n(x)$ .

*Chứng minh.* Vì  $\gcd(a_i(x), m_i(x)) = 1$  với  $1 \leq i \leq n$  nên ta có thể tìm một đa thức  $c_i(x) \in F[x]$  sao cho  $c_i(x)a_i(x) = 1 \pmod{m_i(x)}$  với mọi  $i$ . Do đó,  $a_i(x)u(x) = b_i(x) \pmod{m_i(x)}$ ,  $i = 1, 2, \dots, n$  trở thành  $u(x) = c_i(x)b_i(x) \pmod{m_i(x)}$  với  $1 \leq i \leq n$ . Sử dụng Định lý Thặng dư Trung Hoa, ta có thể tìm  $M(x) = \prod_{i=1}^n m_i(x)$ , và  $M_1(x) = \frac{M(x)}{m_1(x)}$ ,  $M_2(x) = \frac{M(x)}{m_2(x)}$ ,  $\dots$ ,  $M_n(x) = \frac{M(x)}{m_n(x)}$ . Sau đó, tiếp tục như Định lý thặng dư Trung Hoa, lời giải được đưa ra như sau:

$$\begin{aligned} u(x) = & b_1(x)c_1(x)M_1(x)y_1(x) + b_2(x)c_2(x)M_2(x)y_2(x) + \\ & \dots + b_n(x)c_n(x)M_n(x)y_n(x) \pmod{M(x)}, \end{aligned}$$

trong đó  $y_i(x)$  là nghịch đảo của  $M_i(x) \pmod{m_i(x)}$  với  $i = 1, 2, \dots, n$ .  $\square$

**2.2.4 Ví dụ.** Trong vành đa thức  $\mathbb{R}[x]$  cho  $m_1 = x^2 + 1, m_2 = x^2 + 2, a_1 = x^2, a_2 = x^2 + 1, b_1 = 4x + 4, b_2 = 4x + 8$ .

Vì  $(-1).x^2 + (x^2 + 1) = 1$  nên  $(-1).x^2 \equiv 1 \pmod{(x^2 + 1)}$ . Do đó  $c_1(x) = -1$ .

Vì  $(-1).(x^2 + 1) + x^2 + 2 = 1$  nên  $(-1).(x^2 + 1) \equiv 1 \pmod{(x^2 + 2)}$ . Do đó  $c_2(x) = -1$ .

Khi đó hệ phương trình đồng dư:

$$\begin{cases} x^2 u(x) \equiv 4x + 4 \pmod{(x^2 + 1)} \\ (x^2 + 1)u(x) \equiv 4x + 8 \pmod{(x^2 + 2)} \end{cases}$$

trở thành

$$\begin{cases} u(x) \equiv -(4x + 4) \pmod{(x^2 + 1)} \\ u(x) \equiv -(4x + 8) \pmod{(x^2 + 2)}. \end{cases}$$

Đặt  $M(x) = (x^2 + 1)(x^2 + 2)$  thì  $M_1(x) = (x^2 + 2)$  và  $M_2(x) = (x^2 + 1)$ . Mặt khác do  $-1(x^2 + 1) + (x^2 + 2) = 1$  nên  $y_1(x) = 1$  và  $y_2(x) = -1$ . Vậy hệ phương trình đồng dư có nghiệm duy nhất

$$u(x) = -1(4x + 4)(x^2 + 2).1 + (-1)(4x + 8)(x^2 + 1)(-1) \pmod{M(x)}$$

hay  $u(x) = 4x^2 - 4x \pmod{M(x)}$ .

**2.2.5 Ví dụ.** Cho  $f(x)$  là một đa thức có hệ số nguyên, với mỗi số nguyên dương  $m$ , đặt  $N_m = |\{x \in \mathbb{Z} \mid f(x) \equiv 0 \pmod{m}\}|$ . Khi đó, nếu  $m_1, \dots, m_s$  là các số nguyên đôi một nguyên tố cùng nhau thì  $N_{m_1 \dots m_s} = N_{m_1} \dots N_{m_s}$ .

*Chứng minh.* Ta chỉ cần chứng minh với trường hợp  $s = 2$ .

Đặt  $m = m_1.m_2$ .  $S = \{0 \leq x < m \mid f(x) \equiv 0 \pmod{m}\}$  và  $S_i = \{0 \leq x < m_i \mid f(x) \equiv 0 \pmod{m_i}\}$  với  $i = 1, 2$ .

Ta sẽ chỉ ra có sự tương ứng một-một giữa  $S$  và  $S_1 \times S_2$ . Thật vậy, lấy  $x \in S$  bất kỳ, nghĩa là  $0 \leq x < m$  và  $m \mid f(x)$ . Ta có  $x = q_i m_i + x_i$  trong đó  $q_i$  là một số nguyên và  $0 \leq x_i < m_i$ . Dẫn tới  $m_i \mid (x - x_i)$ . Mà  $(x - x_i) \mid f(x) - f(x_i)$  nên  $m_i \mid f(x) - f(x_i)$ . Mặt khác  $m_i \mid m$  và  $m \mid f(x)$  nên  $m_i \mid f(x)$ . Do đó  $m_i \mid f(x_i)$  tức là  $x_i \in S_i$ . Vậy  $(x_1, x_2) \in S_1 \times S_2$ .

Ngược lại, lấy bất kỳ  $(y_1, y_2) \in S_1 \times S_2$  tức là  $m_1 \mid f(y_1), m_2 \mid f(y_2)$ . Theo Định lý thặng dư Trung Hoa, tồn tại một số nguyên  $y$  duy nhất sao cho  $0 \leq y < m_1 m_2 = m$  và thỏa mãn

$$\begin{cases} y \equiv y_1 \pmod{m_1} \\ y \equiv y_2 \pmod{m_2}. \end{cases}$$

Vì  $m_i \mid (y - y_i)$  và  $(y - y_i) \mid f(y) - f(y_i)$  nên  $m_i \mid f(y) - f(y_i)$ . Mặt khác  $m_i \mid f(y_i)$  do đó  $m_i \mid f(y)$ . Mà  $m_1, m_2$  nguyên tố cùng nhau nên  $m_1 \cdot m_2 \mid f(y)$ , tức là  $m \mid f(y)$  hay  $y \in S$ . Điều này chứng tỏ  $N_{m_1 m_2} = |S| = |S_1 \times S_2| = N_{m_1} N_{m_2}$ .

Áp dụng phương pháp quy nạp, ta có điều phải chứng minh. □

## CHƯƠNG 3

# ỨNG DỤNG CỦA ĐỊNH LÝ THẶNG DƯ TRUNG HOA

## 3.1 Dãy số nguyên hữu hạn

Đầu tiên ta sẽ xem xét ứng dụng của Định lý Thặng dư Trung Hoa đối với dãy số nguyên hữu hạn. Cho trước một dãy số nguyên hữu hạn bất kỳ, ta đều có thể tìm thấy hai số nguyên khác để biểu diễn nó.

Cho  $a, b$  là hai số nguyên. Ta sẽ kí hiệu số dư  $r$  trong phép chia  $a$  cho  $b$  là  $a \bmod b = r$ .

**3.1.1 Định lý.** Cho  $a_i, 0 \leq i \leq t$  là một dãy hữu hạn gồm các số nguyên không âm. Khi đó tồn tại các số nguyên  $u$  và  $v$  sao cho

$$u \bmod (1 + (i + 1)v) = a_i$$

với mọi  $i = 0, 1, \dots, t$ .

*Chứng minh.* Giả sử  $a$  là số nguyên lớn nhất của dãy  $a_i, 0 \leq i \leq t$  và đặt  $v = 2a \cdot t!$ ,  $m_i = 1 + v(i + 1), 0 \leq i \leq t$ . Ta sẽ chứng minh các số nguyên  $m_i, 0 \leq i \leq t$  là các số đôi một nguyên tố cùng nhau. Phản chứng, giả sử  $p$  là ước chung lớn nhất của  $m_i$  và  $m_j$ , với  $i > j$ . Khi đó  $p$  là ước của hiệu  $(i + 1)m_j - (j + 1)m_i = i - j \leq t$ . Ta có  $v$  chia hết cho tất cả các số nguyên nhỏ hơn hoặc bằng  $t$  hay  $v$  chia hết cho  $i - j$ , do đó  $v$  chia hết cho  $p$ . Vì  $p$  là ước của  $m_i$  và  $v$  chia hết cho  $p$  nên  $p$  phải là ước của 1. Từ đó ta thu được  $p = 1$  hay  $m_i$  và  $m_j$  nguyên tố cùng nhau. Vì vậy, các số nguyên  $m_i$  được coi

là modulo trong Định lý thặng dư Trung Hoa. Do đó tồn tại một số  $u$  sao cho

$$u \equiv a_i \pmod{m_i}, i = 0, 1, \dots, t.$$

Khi đó,  $u \pmod{m_i} = a_i \pmod{m_i}$  với mọi  $0 \leq i \leq t$ . Tuy nhiên, vì  $a_i < v < m_i$ , nên ta có thể kết luận rằng  $a_i \pmod{m_i} = a_i$  với  $0 \leq i \leq t$ . Do đó,  $u \pmod{m_i} = a_i$  với  $0 \leq i \leq t$ .  $\square$

Dưới đây là ví dụ áp dụng với một dãy gồm 4 số nguyên. Đối với dãy này, ta có thể tìm thấy hai số nguyên đại diện cho các số hạng trong dãy.

**3.1.2 Ví dụ.** Xét  $\{2, 3, 5, 6\}$  là một dãy hữu hạn với  $a_0 = 2, a_1 = 3, a_2 = 5$  và  $a_3 = 6$ . Khi đó theo Định lý 3.1.1, tồn tại các số nguyên  $u$  và  $v$  sao cho

$$u \pmod{1 + (i + 1)v} = a_i.$$

Ta sẽ chỉ ra cách tìm  $u$  và  $v$ . Số nguyên lớn nhất là 6, do đó, theo chứng minh của định lý, ta có  $v = 2 \cdot 6 \cdot 3! = 72$ , và:  $m_0 = 1 + 72 = 73, m_1 = 1 + 144 = 145, m_2 = 1 + 216 = 217, m_3 = 1 + 288 = 289$ . Khi đó ta thu được hệ phương trình đồng dư

$$u \equiv 2 \pmod{73}$$

$$u \equiv 3 \pmod{145}$$

$$u \equiv 5 \pmod{217}$$

$$u \equiv 6 \pmod{289}.$$

Hệ phương trình đồng dư này có một nghiệm. Sử dụng Định lý thặng dư Trung Hoa, ta thu được  $M = 663817105, M_0 = 9093385, M_1 = 4578049, M_2 = 3059065$  và  $M_3 = 2296945$ . Tiếp theo, ta có  $9093385y_0 = 1 \pmod{73}$ , dẫn tới  $y_0 = 12 \pmod{73}$ ;  $4578049y_1 = 1 \pmod{145}$  dẫn tới  $y_1 = 4 \pmod{145}$ ,  $3059065y_2 = 1 \pmod{217}$  hay  $y_2 = 95 \pmod{217}$ ; cuối cùng  $2296945y_3 =$

$1 \bmod 289$  thu được  $y_3 = 107 \bmod 289$ . Do đó,

$$\begin{aligned} u &= 2 \cdot 9093385 \cdot 12 + 3 \cdot 4578049 \cdot 4 + 5 \cdot 3059065 \cdot 95 + 6 \cdot 2296945 \cdot 107 \\ &= 545603973 \bmod 663817105. \end{aligned}$$

Như vậy, ta có thể biểu diễn các số hạng của dãy bằng cách sử dụng hai số nguyên 72 và 545603973 như sau:

$$2 = 545603973 \bmod (1 + 72 \cdot 1)$$

$$3 = 545603973 \bmod (1 + 72 \cdot 2)$$

$$5 = 545603973 \bmod (1 + 72 \cdot 3)$$

$$6 = 545603973 \bmod (1 + 72 \cdot 4).$$

## 3.2 Sử dụng Định lý Thặng dư Trung Hoa để chứng minh một tính chất của miền Dedekind

Trong lý thuyết số, Định lý cơ bản của số học phát biểu rằng mọi số tự nhiên lớn hơn 1 đều có thể được viết một cách duy nhất dưới dạng tích của các số nguyên tố. Trong đại số hiện đại, miền Dedekind có tính chất tương tự.

**3.2.1 Định nghĩa.** *Miền Dedekind* là một miền nguyên trong đó mỗi idêan có thể được viết dưới dạng tích của một số hữu hạn các idêan nguyên tố.

**3.2.2 Định nghĩa.** Cho  $R$  là một miền nguyên và  $I$  là một idêan của  $R$ . Đặt  $I^{-1} = \{x \in K \mid xI \subset R\}$  trong đó  $K$  là trường các thương của  $R$ . Nếu  $II^{-1} = R$  thì  $I$  được gọi là một *idêan khả nghịch*.

**3.2.3 Mệnh đề.** *Trong miền Dedekind, mọi idêan nguyên tố khác 0 đều là idêan cực đại.*

*Chứng minh.* Cho  $R$  là miền Dedekind và  $p$  là idêan nguyên tố khác 0 và  $p$  không cực đại. Giả sử  $a$  là một idêan khác của  $R$  sao cho  $p \subset a$ . Khi đó

$a^{-1}p \subset a^{-1}a = R$  nên  $a^{-1}p$  là một idêan của  $R$ . Vì  $a(a^{-1}p) = p$  nên  $a \subset p$  hoặc  $a^{-1}p \subset p$ . Nếu  $a^{-1}p \subset p$  thì  $a^{-1} \subset pp^{-1} = R$  dẫn tới  $R \subset a$  nên  $a = R$ . Mặt khác, nếu  $a \subset p$  và theo giả thiết,  $p \subset a$  thì  $p = a$ . Do đó  $p$  là idêan cực đại.  $\square$

**3.2.4 Ví dụ.** Vành các số nguyên  $\mathbb{Z}$  là một ví dụ về miền Dedekind. Thật vậy, giả sử  $I$  là một idêan của vành  $\mathbb{Z}$ . Khi đó tồn tại một số nguyên  $a$  sao cho  $I = (a)$ . Nếu  $a = 0$  thì  $I = (0)$  là idêan nguyên tố. Nếu  $a \neq 0$  thì  $a$  có phân tích tiêu chuẩn  $a = p_1^{k_1} \cdots p_n^{k_n}$ . Do đó  $(a) = (p_1^{k_1}) \cdots (p_n^{k_n})$  hay  $(a)$  có thể được viết dưới dạng tích của một số idêan hữu hạn. Vậy vành  $\mathbb{Z}$  là một miền Dedekind.

Mỗi vành chính là một miền Dedekind. Tuy nhiên, điều ngược lại không đúng. Định lý sau đây sẽ phát biểu điều kiện để một miền Dedekind là vành chính. Sử dụng Định lý Thặng dư Trung Hoa ta sẽ chứng minh được định lý này.

**3.2.5 Định lý.** *Nếu miền Dedekind  $R$  chỉ có một số hữu hạn các idêan nguyên tố khác không  $P_1, \dots, P_n$  thì  $R$  là vành chính.*

*Chứng minh.* Với mỗi  $i$  chọn  $b_i \in P_i - P_i^2$ . Ta sẽ chứng minh rằng  $(b_i) = P_i$  từ đó suy ra rằng mọi idêan nguyên tố đều là idêan chính, do đó  $R$  là vành chính. Vì  $R$  là một miền Dedekind và nó chỉ có một số hữu hạn các idêan nguyên tố khác không  $P_i, 1 \leq i \leq n$ , nên các idêan nguyên tố này cũng là các idêan cực đại và do đó  $P_i + P_j = R, i \neq j$ . Vì  $R$  là miền Dedekind,  $(b_i) = I_1 I_2 \dots I_m$ , trong đó  $I_i = P_j$ . Theo Định lý thặng dư Trung Hoa 2.1.8, ta có  $b_i \equiv i_i \pmod{P_i}$  và  $b_i \equiv 1 \pmod{P_j}$ . Vì  $b_i \in P_i$  nên  $(b_i) \subseteq P_i$  hay  $I_1 I_2 \dots I_m \subseteq P_i$ . Do đó tồn tại số  $j$  nào đó để  $I_j = P_i$ . Như vậy ta có thể sắp xếp lại các idêan sao cho  $(b_i) = P_i I_1 \dots I_{m-1}$ . Nếu có một số  $r$  khác sao cho  $I_r = P_i$  thì  $(b_i) = P_i^2 I_1 \dots I_{m-2}$ , nhưng điều này mâu thuẫn với  $b_i \notin P_i^2$ . Vì vậy, tiếp tục quá trình này, ta có  $(b_i) = P_i I_1 \dots I_{m-1} = P_i \cap I_1 \cap \dots \cap I_{m-1}$  với  $I_1, \dots, I_{m-1}$



là các ideal nguyên tố phân biệt. Khi đó  $b_i \in I_1$  mà  $b_i \equiv 1 \pmod{I_1}$  hay  $b_i - 1 \in I_1$  nên  $1 \in I_1$  và do đó  $I_1 = R$ . Vậy  $(b_i) = P_i$ .  $\square$

### 3.3 Sử dụng Định lý Thặng dư Trung Hoa để giải một số bài toán sơ cấp

**3.3.1 Ví dụ.** Chứng minh rằng với mọi số tự nhiên  $n$ , luôn tồn tại  $n$  số tự nhiên liên tiếp mà một trong số  $n$  số tự nhiên đó có ít nhất một ước số là số chính phương.

*Chứng minh.* Xét hệ phương trình đồng dư  $x \equiv -i \pmod{p_i^2}$  với  $p_i$  là số nguyên tố  $i = \overline{1, n}$ . Áp dụng Định lý thặng dư Trung Hoa, hệ có một nghiệm nên  $x + i$  là bội của  $p_i^2$ . Bài toán đã được chứng minh.  $\square$

**3.3.2 Ví dụ. (IMO 1989)** Chứng minh rằng với mọi số nguyên dương  $n$  bất kì, tồn tại  $n$  số nguyên dương liên tiếp mà trong đó không có số nào là lũy thừa của một số nguyên tố.

*Chứng minh.* Bài toán này cũng tương tự như bài toán trước nên ta chọn hệ phương trình đồng dư tương tự bài toán trên và sử dụng Định lý Thặng dư Trung Hoa để chứng minh. Ta biết rằng nếu một số chia hết cho  $p$  nhưng không chia hết cho  $p^2$  thì số này không phải là lũy thừa của  $p$ . Điều này đưa ta đến việc lựa chọn hệ sau:  $x \equiv -i + p_i \pmod{p_i^2}$  với  $i \in \{1, 2, \dots, n\}$  ( $p_1, p_2, \dots, p_n$  là những số nguyên tố phân biệt). Áp dụng Định lý thặng dư Trung Hoa, tồn tại  $x$  thỏa mãn hệ. Dễ dàng thấy được  $x + i$  chia hết cho  $p_i$  nhưng không chia hết cho  $p_i^2$ . Như vậy dãy  $x + 1, x + 2, \dots, x + n$  gồm  $n$  số nguyên dương liên tiếp mà trong đó không có số nào là lũy thừa của một số nguyên tố.  $\square$

**3.3.3 Ví dụ. (Olympic Toán học Thành phố St. Petersburg)** Cho  $P(x)$  là một đa thức có hệ số nguyên. Cho các số nguyên  $a_1, a_2, \dots, a_n$  thỏa

mãn: Với mọi số nguyên  $x$ , tồn tại một  $i \in \{1, 2, \dots, n\}$  sao cho  $P(x)$  chia hết cho  $a_i$ . Chứng minh rằng tồn tại  $i_0 \in \{1, 2, \dots, n\}$  sao cho  $a_{i_0}$  là ước của  $P(x)$  với mọi số nguyên  $x$ .

*Chứng minh.* Ta chứng minh bằng phương pháp phản chứng. Giả sử khẳng định trên là sai. Khi đó với mỗi  $i = 1, 2, \dots, n$  tồn tại một số nguyên  $x_i$  sao cho  $P(x_i)$  không chia hết cho  $a_i$ . Do đó, tồn tại một lũy thừa của số nguyên tố  $p_i^{k_i}$  là ước của  $a_i$  và không là ước của  $P(x_i)$ . Một số lũy thừa  $p_1^{k_1}, p_2^{k_2}, \dots, p_n^{k_n}$  có thể có cùng cơ số. Nếu vậy, hãy loại bỏ tất cả các lũy thừa cùng cơ số trừ cái có số mũ nhỏ nhất. Không mất tính tổng quát, giả sử rằng dãy thu được là  $p_1^{k_1}, p_2^{k_2}, \dots, p_m^{k_m}$ ,  $m \leq n$  và  $p_1, p_2, \dots, p_m$  là các số nguyên tố phân biệt. Lưu ý rằng mỗi  $a_i$  có thể chia hết cho một vài số hạng của dãy này.

Vì  $p_1^{k_1}, p_2^{k_2}, \dots, p_m^{k_m}$  đôi một nguyên tố cùng nhau, nên áp dụng Định lý Thặng dư Trung Hoa ta có nghiệm của hệ phương trình đồng dư:

$$x \equiv x_1 \pmod{p_1^{k_1}}, x \equiv x_2 \pmod{p_2^{k_2}}, \dots, x \equiv x_m \pmod{p_m^{k_m}}.$$

Mặt khác vì  $P(x)$  là một đa thức có hệ số nguyên, nên từ  $x \equiv x_j \pmod{p_j^{k_j}}$  dẫn tới  $P(x) \equiv P(x_j) \pmod{p_j^{k_j}}$  với mọi  $j = 1, 2, \dots, m$ . Theo định nghĩa của  $p_j^{k_j}$ , số  $P(x_j)$  không chia hết cho  $p_j^{k_j}$ ,  $j = 1, 2, \dots, m$ . Do đó, đối với nghiệm  $x$  tìm được theo Định lý Thặng dư Trung Hoa,  $P(x)$  không chia hết cho bất kỳ lũy thừa  $p_j^{k_j}$  nào. Và bởi vì mỗi  $a_i$  chia hết cho một số  $p_j^{k_j}$ ,  $j = 1, 2, \dots, m$ , nên cũng không có  $a_i$  nào là ước  $P(x)$ , điều này mâu thuẫn với giả thiết ban đầu.  $\square$

**3.3.4 Ví dụ. (Olympic Toán học Séc và Slovakia năm 1997)** Chứng minh rằng tồn tại một dãy số tự nhiên  $\{a_n\}_{n=1}^{\infty}$  tăng dần sao cho với mọi  $k \geq 0$  thì dãy  $\{k + a_n\}$  chỉ chứa hữu hạn số nguyên tố.

*Chứng minh.* Gọi  $p_k$  là số nguyên tố thứ  $k$ ,  $k \geq 1$ . Đặt  $a_1 = 2$ . Với  $n \geq 1$ , đặt  $a_{n+1}$  là số nguyên nhỏ nhất lớn hơn  $a_n$  và thỏa mãn hệ phương trình đồng

dư:

$$x \equiv -k \pmod{p_{k+1}} \text{ với mọi } k \leq n.$$

Một số nguyên như vậy tồn tại theo Định lý Thặng dư Trung Hoa. Vì vậy, với mọi  $k \geq 0, k + a_n \equiv 0 \pmod{p_{k+1}}$  với  $n \geq k + 1$ . Khi đó, có nhiều nhất  $k + 1$  giá trị trong dãy  $\{k + a_n\}$  có thể là số nguyên tố; từ số hạng thứ  $k + 2$  trở đi, các giá trị là bội số không tầm thường của  $p_{k+1}$  và phải là hợp số. Bài toán đã được chứng minh.  $\square$

**3.3.5 Định nghĩa.** Số tự nhiên  $n$  được gọi là *lũy thừa hoàn hảo* nếu tồn tại hai số nguyên  $m > 1$  và  $k > 1$  sao cho  $m^k = n$ .

**3.3.6 Ví dụ.** Với mọi tập hợp số nguyên dương  $\{a_1, a_2, \dots, a_n\}$  tồn tại một số nguyên dương  $b$  sao cho tập hợp  $\{ba_1, ba_2, \dots, ba_n\}$  chứa các lũy thừa hoàn hảo.

*Chứng minh.* Giả sử  $p_1, p_2, \dots, p_k$  là tất cả các số nguyên tố có mặt trong phân tích tiêu chuẩn của  $a_1, a_2, \dots, a_n$ . Khi đó ta có thể viết:

$$a_i = p_1^{\alpha_{i1}} p_2^{\alpha_{i2}} \dots p_k^{\alpha_{ik}} \text{ với } i = 1, 2, \dots, n$$

trong đó  $\alpha_{ij}$  có thể bằng 0. Một số nguyên dương với phân tích tiêu chuẩn  $p_1^{u_1} p_2^{u_2} \dots p_k^{u_k}$  là lũy thừa hoàn hảo bậc  $q$  khi và chỉ khi tất cả số mũ  $u_j$  đều chia hết cho  $q$ . Vì vậy, chỉ cần tìm các số nguyên dương  $q_1, q_2, \dots, q_n$  lớn hơn 1 và các số nguyên không âm  $l_1, l_2, \dots, l_k$  sao cho

$$l_1 + \alpha_{11}, l_2 + \alpha_{12}, \dots, l_k + \alpha_{1k} \text{ chia hết cho } q_1,$$

$$l_1 + \alpha_{21}, l_2 + \alpha_{22}, \dots, l_k + \alpha_{2k} \text{ chia hết cho } q_2,$$

...

$$l_1 + \alpha_{n1}, l_2 + \alpha_{n2}, \dots, l_k + \alpha_{nk} \text{ chia hết cho } q_n.$$

Rõ ràng là ta có rất nhiều cách lựa chọn. Ví dụ: giả sử  $q_i$  là số nguyên tố thứ  $i$ . Đối với  $l_1$ , các điều kiện trên chuyển thành

$$l_1 \equiv -\alpha_{j1} \pmod{q_j}, \quad j = 1, 2, \dots, n.$$

Hệ phương trình đồng dư này có nghiệm theo Định lý Thặng dư Trung Hoa, bởi vì  $q_1, q_2, \dots, q_n$  đôi một nguyên tố cùng nhau. Tương tự, mỗi hệ phương trình đồng dư

$$l_2 \equiv -\alpha_{j2} \pmod{q_j}, \quad j = 1, 2, \dots, n,$$

$$l_3 \equiv -\alpha_{j3} \pmod{q_j}, \quad j = 1, 2, \dots, n,$$

...

$$l_k \equiv -\alpha_{jk} \pmod{q_j}, \quad j = 1, 2, \dots, n$$

cũng có nghiệm. Lấy  $l_1, l_2, \dots, l_k$  sao cho tất cả các đồng dư này đều được thỏa mãn. Nhân mỗi  $a_i$  với  $b = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$  thu được một tập hợp  $\{ba_1, ba_2, \dots, ba_n\}$  bao gồm các lũy thừa hoàn hảo (nói cách khác,  $ba_i$  là lũy thừa hoàn hảo bậc  $q_i$ ).  $\square$

Bài toán sau là hệ quả trực tiếp của kết quả trên.

**3.3.7 Ví dụ. (Đề xuất của Hàn Quốc về 33<sup>rd</sup> IMO)** Chứng minh rằng với mọi số nguyên dương  $n$  tồn tại một tập hợp  $n$  số nguyên dương sao cho tổng các phần tử của mỗi tập con khác rỗng của nó là một lũy thừa hoàn hảo.

*Chứng minh.* Giả sử  $\{x_1, x_2, \dots, x_m\}$  là một tập hợp hữu hạn các số nguyên dương và  $S_1, S_2, \dots, S_r$  tổng phần tử của các tập con khác rỗng của nó ( $r = 2^m - 1$ ). Chọn  $b$  sao cho  $bS_1, bS_2, \dots, bS_r$  đều là lũy thừa hoàn hảo. Khi đó tập  $\{bx_1, bx_2, \dots, bx_m\}$  là một tập hợp cần tìm.  $\square$

## 3.4 Sơ đồ mật mã

Định lý thặng dư Trung Hoa được áp dụng trong chia sẻ bí mật - một chủ đề quan trọng của mật mã học. Bản thân Định lý thặng dư Trung Hoa là một sơ đồ chia sẻ bí mật mà không cần bất kỳ sửa đổi nào. Ta sẽ xem xét

ứng dụng của Định lý thặng dư Trung Hoa trong sơ đồ chia sẻ bí mật và sơ đồ ngưỡng.

**Ý tưởng áp dụng Định lý thặng dư Trung Hoa trong sơ đồ chia sẻ bí mật như sau:**

Cho  $m_1, m_2, \dots, m_t$  là  $t$  số nguyên dương đôi một nguyên tố cùng nhau và  $m = \prod_{i=1}^t m_i$ . Giả sử bí mật là một số nguyên  $s$  sao cho  $0 \leq s < m$  và có  $t$  đối tượng  $P_1, P_2, \dots, P_t$  được chia sẻ bí mật. Khi đó  $P_i$  có số dư  $s_i = s \bmod m_i$  là thông tin mà chỉ  $P_i$  mới biết. Theo Định lý thặng dư Trung Hoa, có đủ  $t$  mảnh thông tin  $s_i$  sẽ xác định được bí mật  $s$  ban đầu, nhưng bất kì tập nào ít hơn  $t$  mảnh thông tin thì không thể tìm được  $s$ .

**Sơ đồ ngưỡng chia sẻ bí mật  $(k, t)$  được định nghĩa như sau.**

$t$  đối tượng tham gia  $P_i$  cùng chia sẻ một bí mật  $s$  thỏa mãn các điều kiện:

1. Mỗi bên có một phần thông tin  $s_i$  về bí mật  $s$  mà các bên khác không biết.
2. Bí mật  $s$  có thể được tính toán từ bất kỳ  $k$  phần  $s_i$  nào.
3. Không có  $k - 1$  phần  $s_i$  nào cung cấp đủ thông tin về bí mật  $s$ .

Ta sẽ xem xét hai phương án chia sẻ bí mật; một liên quan đến các số nguyên và một liên quan đến đa thức.

## Sơ đồ ngưỡng 1

Cho  $m_i, i = 1, 2, \dots, t$ , là  $t$  số nguyên đôi một nguyên tố cùng nhau và không nhỏ hơn 2. Ta định nghĩa:

$$\min(k) = \min \{m_{i_1} m_{i_2} \cdots m_{i_k} \mid 1 \leq i_1 \leq \dots \leq i_k \leq t\},$$

$$\max(k - 1) = \max \{m_{i_1} m_{i_2} \cdots m_{i_{k-1}} \mid 1 \leq i_1 < i_2 < \dots < i_{k-1} \leq t\},$$

trong đó  $1 < k \leq t$ . Nói cách khác,  $\min(k)$  là tích nhỏ nhất của  $k$  số nguyên  $m_i$  và  $\max(k - 1)$  là tích lớn nhất của  $k - 1$  số nguyên  $m_i$ . Chọn  $w$  là số nguyên dương lớn nhất sao cho

- $w < \frac{\min(k)}{\max(k - 1)},$

- $\gcd(w, m_i) = 1, i = 1, 2, \dots, t.$

Đặt  $m = \min(k).$

Bí mật là số nguyên  $s$  sao cho  $0 \leq s < w$ . Vì vậy, ta giả sử rằng bí mật có khả năng là bất kỳ số nguyên nào trong khoảng từ 0 đến  $w - 1$ .

Ta tính toán các phần thông tin cho  $t$  đối tượng như sau.

Chọn  $a \in \mathbb{Z}$  sao cho  $0 \leq s + aw < m$ , và đặt  $s' = s + aw$ . Sau đó, các mảnh thông tin được cho bởi  $s_i = s' \bmod m_i, i = 1, 2, \dots, t$ , trong đó  $s_i$  là phần của đối tượng  $P_i$ . Ta sẽ chứng minh rằng  $k - 1$  phần hoặc ít hơn  $k - 1$  phần thì không có thông tin về bí mật nhưng bất kỳ  $k$  phần nào trở lên đều xác định được bí mật.

Không mất tính tổng quát ta giả sử  $s_1, s_2, \dots, s_h$  đã biết và  $1 \leq h < t$ . Đặt  $M = \prod_{i=1}^h m_i$  và  $M_j = \frac{M}{m_j}$  với  $j = 1, 2, \dots, h$ . Khi đó  $(M_j, m_j) = 1$ . Theo thuật toán Euclide, tồn tại  $u_j, v_j \in \mathbb{Z}$  sao cho  $M_j u_j + m_j v_j = 1$ . Điều này có thể được thực hiện bằng cách giải  $M_j u_j \equiv 1 \bmod m_j$  và  $m_j v_j \equiv 1 \bmod M_j$ . Khi đó, theo Định lý thặng dư Trung Hoa, hệ phương trình đồng dư

$$x \equiv s_i \bmod m_i \text{ với } 1 \leq i \leq h$$

có nghiệm duy nhất theo modulo  $M$  cho bởi

$$x = s_1 M_1 u_1 + s_2 M_2 u_2 + \dots + s_h M_h u_h.$$

Đặt  $s'' = \sum_{j=1}^h M_j u_j s_j \bmod M$  với  $0 \leq s'' < M$ , thì  $s'' \equiv s_i \bmod m_i$ . Ta có hai trường hợp:

### Trường hợp 1:

Nếu  $h \geq k$  thì  $M \geq \min(k) = m > w$ . Theo Định lý thặng dư Trung Hoa  $s'' = s'$  vì  $s' \equiv s_i \bmod m_i, s' < m \leq M$  và nghiệm của hệ  $x \equiv s_i \bmod m_i$  là duy nhất theo modulo  $M$ . Lại có  $s' \bmod w = (s + aw) \bmod w = s$  nên bí mật xác định được bởi  $s = s'' \bmod w$ .

### Trường hợp 2:

Nếu  $h = k - 1$  thì  $M \leq \max(k - 1) < \frac{m}{w}$ , vì  $w < \frac{\min(k)}{\max(k - 1)}$  hay  $\frac{\max(k - 1)}{\min(k)} < \frac{1}{w}$  do đó  $\max(k - 1) < \frac{\min(k)}{w}$ . Vậy  $w < \frac{m}{M}$  vì  $w > 0$ . Vì nghiệm của hệ phương trình đồng dư  $x \equiv s_i \pmod{m_i}$  là duy nhất theo modulo  $M$  nên ta có  $s' = s'' + bM$  với  $b$  nào đó. Lại có  $0 \leq s' < m$  hay  $0 \leq s'' + bM < m$ , vì vậy  $-s'' \leq bM < m - s''$  dẫn đến  $\frac{-s''}{M} \leq b < \frac{m - s''}{M}$ . Do đó,  $0 \leq b \leq \left\lfloor \frac{m - s''}{M} \right\rfloor$ . Mặt khác,  $\frac{m - s''}{M} > \frac{m - M}{M} = \frac{m}{M} - 1 > w - 1$ . Khi đó  $s \equiv s' \pmod{w} \equiv (s'' + bM) \pmod{w}$  mà  $b$  nằm trong phạm vi từ 0 đến  $\left\lfloor \frac{m - s''}{M} \right\rfloor$  và  $w - 1 \leq \left\lfloor \frac{m - s''}{M} \right\rfloor$ ,  $s$  có khả năng nhận  $0, 1, \dots, w - 1$ .

Do đó, bất kỳ  $k - 1$  mảnh thông tin trở xuống đều không thể tìm được bí mật  $s$ .

Bây giờ ta hãy xem một ví dụ để biết sơ đồ ngưỡng hoạt động như thế nào.

**3.4.1 Ví dụ.** Cho  $k = 3, t = 4, m_1 = 5, m_2 = 7, m_3 = 11$  và  $m_4 = 13$ . Khi đó  $m = \min(k) = 5 \cdot 7 \cdot 11 = 385$ , và  $\max(k - 1) = 11 \cdot 13 = 143$ . Vì vậy, tồn tại một số nguyên  $w$  sao cho  $w < \frac{\min(k)}{\max(k - 1)} = \frac{385}{143}$  và  $\gcd(w, m_i) = 1$ . Ta lấy  $w = 2$ . Bí mật  $s$  là một số nguyên thỏa mãn  $0 \leq s < w$ . Vậy  $s$  là 0 hoặc 1. Vì  $t = 4$  nên ta cần tính 4 phần chia sẻ thông tin. Ta chọn một số  $a$  thỏa mãn  $0 \leq s + aw < m$ . Do đó  $0 \leq aw < m - s$  dẫn tới  $0 \leq a < \frac{m - s}{w} = \frac{385 - 1}{2} = 192$ . Ví dụ chọn  $a = 30$ . Đặt  $s' = s + aw = s + 60$ . Bốn phần thông tin được cho bởi  $s_i = s' \pmod{m_i}$ . Khi đó  $s_1 = (s + 60) \pmod{5}, s_2 = (s + 60) \pmod{7}, s_3 = (s + 60) \pmod{11}$  và  $s_4 = (s + 60) \pmod{13}$ . Là người giữ bí mật, ta cho  $s = 1$  thì  $s_1 = 1$  và  $s_2 = 5$ . Khi đó  $M = m_1 m_2 = 35, M_1 = 7$  và  $M_2 = 5$ . Theo Thuật toán Euclide, ta nhận được  $7 \cdot (-2) + 5 \cdot 3 = 1$ . Do đó,  $u = -2$  và  $v = 3$ . Khi đó, theo Thuật toán thặng dư Trung Hoa, ta có

$s'' = M_1 u_1 s_1 + M_2 u_2 s_2$  vì  $h = 2$  hay  $s'' = (7 \cdot (-2) \cdot s_1 + 5 \cdot 3 \cdot s_2) \bmod 35 = (-14 + 75) \bmod 35 = 61 \bmod 35 = 26 \bmod 35$ . Vì  $h = 3 - 1 = 2$  nên ta có  $s' = s'' + bM = 26 + 35b$  trong đó  $0 \leq b \leq \frac{385 - 26}{35} = 10$ . Theo đó  $s = s' \bmod 2 = b \bmod 2$ . Vì  $b \in [0, 10]$  nên  $s$  có khả năng bằng 1 hoặc 0. Vì vậy, hai mảnh thông tin không xác định được bí mật.

Nếu ta có ba phần chia sẻ, ta có thể tính được bí mật  $s$ . Xét với ví dụ trên, giả sử ta có ba phần  $s_1 = 1, s_2 = 5$  và  $s_3 = 6$ . Khi đó  $M = m_1 m_2 m_3 = 5 \cdot 7 \cdot 11 = 385$ , do đó  $M_1 = 77, M_2 = 55$  và  $M_3 = 35$ . Do đó, bằng Thuật toán Euclide, ta có thể tìm  $u_j$  và  $v_j$ , với  $j = 1, 2, 3$  sao cho:

$$77u_1 + 5v_1 = 1$$

$$55u_2 + 7v_2 = 1$$

$$35u_3 + 11v_3 = 1.$$

Giải ba phương trình, ta được:

$$77 \cdot (-2) + 5 \cdot 31 = 1$$

$$55 \cdot (-1) + 7 \cdot 8 = 1$$

$$35 \cdot 6 + 11 \cdot (-19) = 1.$$

Do đó,  $s'' = 77 \cdot (-2) \cdot s_1 + 55 \cdot (-1) \cdot s_2 + 35 \cdot 6 \cdot s_3 = 831 \bmod 385 = 61 \bmod 385$ . Khi đó, bí mật  $s$  sẽ là  $s = 61 \bmod 2 = 1 \bmod 2$ . Vì vậy, bí mật  $s$  là 1.

## Sơ đồ ngưỡng 2

Sơ đồ chia sẻ bí mật này gần giống với sơ đồ 1, nhưng áp dụng cho đa thức.

Giả sử  $F$  là một trường hữu hạn và  $m_i(x), i = 1, \dots, t$  là  $t$  đa thức đôi một nguyên tố cùng nhau của  $F[x]$  với bậc lớn hơn hoặc bằng 1. Khi đó:

$$\min[k] = \min \{ \deg(m_{i_1} m_{i_2} \cdots m_{i_k}) \mid 1 \leq i_1 < \cdots < i_k < t \},$$

$$\max[k-1] = \max \{ \deg(m_{i_1} m_{i_2} \cdots m_{i_{k-1}}) \mid 1 \leq i_1 < \cdots < i_{k-1} < t \},$$

trong đó  $1 < k \leq t$ . Đặt  $w$  là số nguyên dương lớn nhất sao cho



- tồn tại một đa thức  $W(x)$  bậc  $w$  trên  $F$  với  $(W(x), m_i(x)) = 1$  với  $i = 1, 2, \dots, t$  và

- $w \leq \frac{\min[k]}{\max[k-1]}.$

Bí mật là một đa thức  $s(x) \in F[x]$  bậc nhỏ hơn  $w$ . Các phần của  $t$  đối tượng được tính như sau.

Chọn  $a(x) \in F[x]$  sao cho  $\deg(s(x) + a(x)W(x)) < \min[k]$ . Đặt  $s'(x) = s(x) + a(x)w(x)$ . Các mảnh thông tin được cho bởi  $s_i(x) = s'(x) \bmod m_i, i = 1, 2, \dots, t$ . Do đó,  $(k, t)$  là một sơ đồ ngưỡng.

Giả sử  $k$  phần  $s_1(x), s_2(x), \dots, s_k(x)$  đã cho. Đặt  $M(x) = \prod_{i=1}^k m_i(x)$  và  $M_j(x) = \frac{M(x)}{m_j(x)}$  với  $j = 1, \dots, k$ . Khi đó  $M_j(x)$  và  $m_j(x)$  là nguyên tố cùng nhau. Theo Thuật toán Euclide, tồn tại hai đa thức  $u_j(x)$  và  $v_j(x)$  trong  $F[x]$  sao cho  $M_j(x)u_j(x) + m_j(x)v_j(x) = 1$ . Theo Định lý thặng dư Trung Hoa, ta có  $s'(x) = \sum_{j=1}^k M_j(x)u_j(x)s_j(x) \bmod M(x)$ . Khi đó bí mật được đưa ra bởi  $s(x) = s'(x) \bmod W(x)$ .

## KẾT LUẬN

Dựa vào các tài liệu tham khảo, luận văn đã trình bày các nội dung sau đây:

1. Sự hình thành và phát triển của Định lý thặng dư Trung Hoa.
2. Các dạng phát biểu khác nhau của Định lý thặng dư Trung Hoa và đưa ra một chương trình code thuật toán dựa trên Định lý thặng dư Trung Hoa cho số nguyên.
3. Sự mở rộng của Định lý thặng dư Trung Hoa lên vành.
4. Một số ứng dụng của Định lý thặng dư Trung Hoa như: giải hệ phương trình đồng dư bậc nhất một ẩn và giải một số bài toán sơ cấp khác, ứng dụng đối với dãy số nguyên hữu hạn, miền Dedekind, ứng dụng trong chia sẻ bí mật của lý thuyết mật mã.

Từ đó có thể thấy Định lý thặng dư Trung Hoa có vai trò quan trọng trong đại số cũng như các lĩnh vực khác. Với sự phát triển liên tục của đại số hiện đại, việc mở rộng định lý này sẽ được tiếp tục quan tâm và nghiên cứu.

## TÀI LIỆU THAM KHẢO

- [1] Carol S. Jackson (2021), *The Chinese Remainder Theorem*, Master Thesis, Governors State University.
- [2] C. Ding, D. Pei, and A. Salomaa (1996), *Chinese remainder theorem, application in computing, coding, cryptography*, World Scientific Publishing.
- [3] Jacquelyn Ha Lac (2008), *Chinese remainder theorem and its applications*, Master Thesis, California State University, San Bernardino.
- [4] J. Grossschadl (2000), The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip, *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00)*, 384 - 393
- [5] Law Huong lng (2003), *The History of The Chinese Remainder Theorem*, Reading, Universiti Putro Malaysia.  
[https://sms.math.nus.edu.sg/smsmedley/Vol30](https://sms.math.nus.edu.sg/smsmedley/Vol30/The%20History%20of%20the%20Chinese%20Reminder%20Theorem%20(Law%20Huang%20lng).pdf) -  
[/The%20History%20of%20the%20Chinese%20Reminder%20Theorem%20\(Law%20Huang%20lng\).pdf](https://sms.math.nus.edu.sg/smsmedley/Vol30/The%20History%20of%20the%20Chinese%20Reminder%20Theorem%20(Law%20Huang%20lng).pdf)