ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN TRỌNG NAM

LÝ THUYẾT ĐỒNG DƯ VÀ ỨNG DỤNG TRONG MÃ SỬA SAI

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2009

Số hóa bởi Trung tâm Học liệu – Đại học Thái Nguyên http://www.Lrc-tnu.edu.vn

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN TRỌNG NAM

LÝ THUYẾT ĐỒNG DƯ VÀ ỨNG DỤNG TRONG MÃ SỬA SAI

Chuyên ngành: TOÁN SƠ CẤP

Mã số: 60.46.40

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học: PGS.TS TẠ DUY PHƯỢNG

THÁI NGUYÊN - 2009

Số hóa bởi Trung tâm Học liệu – Đại học Thái Nguyên http://www.Lrc-tnu.edu.vn

MỤC LỤC

LỜI NÓI ĐẦU 1

Chương 1: LÝ THUYẾT ĐỒNG DƯ 3

§ 1. Quan hệ đồng dư 3

1.1. Định nghĩa đồng dư 3

1.2. Các tính chất của quan hệ đồng dư 4

§ 2. Thặng dư 7

2.1. Tập các lớp thặng dư 7

2.2. Các tính chất của lớp thặng dư 7

2.3. Tập các lớp thặng dư nguyên tố với môđun 9

2.4. Vành các lớp thặng dư 9

§ 3. Hệ thặng dư đầy đủ - Hệ thặng dư thu gọn 11

3.1. Hệ thặng dư đầy đủ 11

3.2. Hệ thặng dư thu gọn 13

3.3. Các định lí quan trọng 16

§ 4. Phương trình đồng dư 17

4.1. Các khái niệm chung 17

4.2. Phương trình và hệ phương trình đồng dư bậc nhất một ẩn 23

4.2.1. Phương trình đồng dư bậc nhất một ẩn 23

4.2.2. Hệ phương trình đồng dư bậc nhất một ẩn 26

4.3. Phương trình đồng dư bậc cao theo môđun nguyên tố 31

4.3.1. Nhận xét 31

4.3.2. Phương trình bậc cao theo môđun nguyên tố 32

Chương 2: ỨNG DỤNG CỦA LÝ THUYẾT ĐỒNG DƯ TRONG MÃ SỬA SAI 36

§ 1. Khái niệm mã 36

§ 2. Những ví dụ về mã 39

2.1. Mã lặp 39
2.2. Mã chẵn lẻ 41
2.3. Mã vạch 44
§ 3. Khoảng cách Hamming 48
§ 4. Mã tuyến tính 53
4.1. Mã nhị phân tuyến tính 53
4.2. Biểu diễn ma trận của các mã nhị phân 55
4.3. Thuật toán hội chứng giải mã cho các mã nhị phân 65
4.4. Mã nhị phân Hamming 67
4.5. Các tính chất của mã nhị phân Hamming [n,k] 70
4.6. Các p-mã Hamming 71
4.7. Các tính chất của p-mã Hamming [n,k] 74
§ 5. Mã thập phân 77
5.1. Mã số sách tiêu chuẩn quốc tế (ISBN) 77
5.2. Mã sửa lỗi đơn 82
5.3. Mã sửa lỗi kép 84
KẾT LUẬN 88
TÀI LIỆU THAM KHẢO 89

LỜI NÓI ĐẦU

Có thể nói, số học, lý thuyết số là một trong những kiến thức toán học lâu đời nhất. Từ trước tới nay, người ta thường coi lý thuyết số như một lĩnh vực đẹp, nhưng thuần túy lý thuyết, của toán học. Với sự phát triển của khoa học máy tính và công nghệ thông tin, lý thuyết số đã đóng góp những ứng dụng thực tế bất ngờ và quan trọng, đặc biệt trong lĩnh vực mã hóa thông tin.

Nhiều khía cạnh khác nhau của mã hóa thông tin được các nhà toán học và tin học quan tâm. Thường thường thông tin được mã hóa qua dãy các chữ số trong hệ đếm cơ số 2, cơ số 10, hoặc cơ số p nào đó. Trong quá trình truyền tin hoặc nhận tin, vì nhiều lý do, thông tin có thể bị sai lệch. Thí dụ, một tin nhắn được mã hóa trong cơ số 2 khi truyền đi bị sai một lỗi (lỗi đơn) thì điều này có nghĩa là chữ số 1 tại vị trí nào đó đã bị đổi thành chữ số 0 hoặc ngược lại. Một trong những vấn đề cần giải quyết là phát hiện ra các lỗi sai và sửa chúng.

Vì yêu cầu thực tiễn đó, lý thuyết mã sửa sai đã ra đời, phát triển và có những ứng dụng thực tiễn quan trọng. Để xây dựng lý thuyết mã sửa sai, các nhà toán học và khoa học máy tính đã sử dụng nhiều thành tựu của toán học hiện đại (số học, toán rời rạc, đại số tuyến tính,...,) đặc biệt là số học trên tập số nguyên, trong đó có lý thuyết đồng dư.

Luận văn này có mục đích tìm hiểu và trình bày những kiến thức cơ bản nhất của lý thuyết mã sửa sai trên cơ sở lý thuyết đồng dư và lý thuyết trường hữu hạn.

Luận văn gồm hai chương.

Chương 1 trình bày các kiến thức cơ bản nhất của lý thuyết đồng dư và lý thuyết trường hữu hạn, chủ yếu dựa theo tài liệu [2], có tham khảo thêm các tài liệu [4] và [6].

Số hóa bởi Trung tâm Học liệu – Đại học Thái Nguyên http://www.Lrc-tnu.edu.vn

Chương 2 trình bày một số vấn đề cơ bản của mã sửa sai: khoảng cách Hamming; phát hiện và sửa lỗi; các thuật toán giải mã; mã hoàn hảo; mã tuyến tính và ma trận kiểm tra, xây dựng mã tuyến tính,...

Nội dung của Chương 2 trình bày chủ yếu dựa theo tài liệu [6], có tham khảo thêm các tài liệu [1] và [7]. Ngoài ra, chúng tôi cũng quan tâm đến khía cạnh thực tế của vấn đề: mã vạch, mã hàng hóa, mã sách tiêu chuẩn quốc tế,.... Chúng tôi cũng cố gắng tìm hiểu, tuy chưa được đầy đủ, các mã hàng hóa, mã văn hóa phẩm của Việt Nam và kiểm nghiệm các tiêu chuẩn giải mã cho các ví dụ cụ thể của các mã này.

Luận văn được hoàn thành dưới sự hướng dẫn khoa học của PGS TS Tạ Duy Phượng. Xin được tỏ lòng cám ơn chân thành nhất tới Thầy.

Tác giả xin cám ơn chân thành tới Trường Đại học Khoa học Thái Nguyên, nơi tác giả đã nhận được một học vấn sau đại học căn bản.

Và cuối cùng, xin cám ơn gia đình, bạn bè, đồng nghiệp đã cảm thông, ủng hộ và giúp đỡ trong suốt thời gian tác giả học Cao học và viết luận văn.

Hà Nội, ngày 19 tháng 9 năm 2009

Tác giả

Nguyễn Trọng Nam

Chương 1
LÝ THUYẾT ĐỒNG DƯ

§1. Quan hệ đồng dư

1.1. Định nghĩa đồng dư

Kí hiệu $\mathbb{Z}$ là tập hợp các số nguyên.

Định nghĩa

Cho *m* là một số nguyên dương, *a* và *b* là hai số nguyên. Ta nói *a* và *b* *đồng dư* với nhau theo môđun *m* nếu trong phép chia *a* và *b* cho *m* ta được cùng một số dư, nghĩa là có các số nguyên q_1, q_2, r với $0 \le r < m$ sao cho

$$a = mq_1 + r \text{ và } b = mq_2 + r.$$

Khi *a* và *b* đồng dư với nhau theo môđun *m*, ta viết $a \equiv b \pmod{m}$.

Nếu *a* không đồng dư với *b* theo môđun *m* thì ta viết $a \not\equiv b \pmod{m}$.

Định lý

Các mệnh đề sau là tương đương.

i. *a* và *b* đồng dư với nhau theo môđun *m*;

ii. a – b chia hết cho *m* (kí hiệu là $m \mid (a-b)$);

iii. Tồn tại số nguyên *t* sao cho *a* = *b*+*mt*.

Chứng minh

i$\Rightarrow$ii. Ta có $a \equiv b \pmod{m} \Leftrightarrow a = mq_1 + r$, $b = mq_2 + r$ với $q_1, q_2, r \in \mathbb{Z}$, $0 \le r < m$. Suy ra $a - b = m(q_1 - q_2)$. Do $q_1 - q_2 \in \mathbb{Z}$ nên $m \mid (a-b)$.

ii$\Rightarrow$iii. Giả sử $m \mid (a-b)$. Khi ấy tồn tại số $t \in \mathbb{Z}$ sao cho $a - b = mt$, tức là *a* = *b* + *mt*.

iii$\Rightarrow$i. Giả sử có số $t \in \mathbb{Z}$ sao cho *a* = *b* + *mt*. Gọi *r* là số dư trong phép chia *a* cho *m*, nghĩa là *a* = mq_1 + *r* với q_1, $r \in \mathbb{Z}$, $0 \le r < m$. Khi ấy:

$b+mt=a=mq_1+r$ hay $b=m(q_1-t)+r$, trong đó $q_1-t\in\mathbb{Z}$, $0\le r<m$.

Chứng tỏ số dư trong phép chia b cho m cũng là r, tức là $a\equiv b(\bmod m)$.

1.2. Các tính chất của quan hệ đồng dư

a. Quan hệ đồng dư là một quan hệ tương đương trên tập $\mathbb{Z}$:

i. Với mọi $a\in\mathbb{Z}$: $a\equiv a(\bmod m)$;

ii. Với mọi $a,b\in\mathbb{Z}$: $a\equiv b(\bmod m)$ khi và chỉ khi $b\equiv a(\bmod m)$;

iii. Với mọi $a,b,c\in\mathbb{Z}$: $a\equiv b(\bmod m)$, $b\equiv c(\bmod m)$ suy ra $a\equiv c(\bmod m)$.

Chứng minh

i. Vì $a-a$ chia hết cho m nên $a\equiv a(\bmod m)$.

ii. Từ $a\equiv b(\bmod m)$ ta có $m|(a-b)$. Do đó $m|(b-a)\Rightarrow b\equiv a(\bmod m)$.

iii. Ta có $a\equiv b(\bmod m)$ và $b\equiv c(\bmod m)$ nên $m|(a-b)$ và $m|(b-c)$.

Khi đó $m|((a-b)+(b-c))$ hay $m|(a-c)$. Vậy $a\equiv c(\bmod m)$.

b. Ta có thể cộng hoặc trừ từng vế của nhiều đồng dư thức theo cùng một môđun. Cụ thể là, nếu $a_1\equiv b_1(\bmod m)$ và $a_2\equiv b_2(\bmod m)$ thì ta có:

$$a_1\pm a_2\equiv b_1\pm b_2(\bmod m).$$

Chứng minh

Từ $a_1\equiv b_1(\bmod m)$, $a_2\equiv b_2(\bmod m)$ suy ra tồn tại $t_1,t_2\in\mathbb{Z}$ sao cho $a_1=b_1+mt_1$, $a_2=b_2+mt_2$. Do đó $a_1\pm a_2\equiv b_1\pm b_2+m(t_1\pm t_2)$ với $t_1\pm t_2\in\mathbb{Z}$. Vậy $a_1\pm a_2\equiv b_1\pm b_2(\bmod m)$.

c. Ta có thể nhân từng vế của nhiều đồng dư thức theo cùng một môđun. Cụ thể là, nếu $a_1\equiv b_1(\bmod m)$, $a_2\equiv b_2(\bmod m)$ thì $a_1a_2\equiv b_1b_2(\bmod m)$.

Chứng minh

Từ $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$ suy ra tồn tại $t_1, t_2 \in \mathbb{Z}$ sao cho $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$.

Do đó $a_1a_2 = b_1b_2 + m(b_2t_1 + b_1t_2 + mt_1t_2)$, $b_2t_1 + b_1t_2 + mt_1t_2 \in \mathbb{Z}$.

Vậy $a_1a_2 - b_1b_2$ chia hết cho m hay $a_1a_2 \equiv b_1b_2 \pmod{m}$.

d. Hệ quả

1. $a \equiv b \pmod{m}$ khi và chỉ khi $a \pm c \equiv b \pm c \pmod{m}$.

Thật vậy, ta có $a \equiv b \pmod{m}$ và $c \equiv c \pmod{m}$.

Vậy $a \pm c \equiv b \pm c \pmod{m}$.

2. $a + c \equiv b \pmod{m}$ khi và chỉ khi $a \equiv (b - c) \pmod{m}$.

Thật vậy, ta có $a \equiv b \pmod{m}$, $c \equiv c \pmod{m}$. Vậy $a \equiv (b - c) \pmod{m}$.

3. $a \equiv b \pmod{m}$ khi và chỉ khi $a \pm km \equiv b \pmod{m}$ với mọi $k \in \mathbb{Z}$.

Thật vậy, $a \equiv b \pmod{m}$, $km \equiv 0 \pmod{m}$. Vậy $a \pm km \equiv b \pmod{m}$.

4. $a \equiv b \pmod{m}$ khi và chỉ khi $ac \equiv bc \pmod{m}$.

Ta có $a \equiv b \pmod{m}$, $c \equiv c \pmod{m}$. Vậy $ac \equiv bc \pmod{m}$.

5. $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ $\forall n \in \mathbb{Z}$, $n > 0$.

Ta có $a \equiv b \pmod{m}$; $a \equiv b \pmod{m}$; ...; $a \equiv b \pmod{m}$

Suy ra $a^n \equiv b^n \pmod{m}$.

6. Giả sử $f(x)$ là một đa thức với hệ số nguyên và $\alpha \equiv \beta \pmod{m}$. Khi ấy

$$f(\alpha) \equiv f(\beta) \pmod{m}$$

Đặc biệt, nếu $f(\alpha) \equiv 0 \pmod{m}$ thì $f(\alpha + km) \equiv 0 \pmod{m}$ với mọi $k \in \mathbb{Z}$.

Chứng minh

Thật vậy, giả sử $f(x) = a_0 + a_1x + ... + a_nx_n$. Từ giả thiết $\alpha \equiv \beta \pmod{m}$ suy ra $a_i\alpha^i \equiv a_i\beta^i \pmod{m}$, $i = 1, 2,...., n$. Do đó

$$a_0 + a_1\alpha + ... + a_n\alpha^n \equiv a_0 + a_1\beta + ... + a_n\beta^n \pmod{m},$$

nghĩa là $f(\alpha) \equiv f(\beta) \pmod{m}$.

Đặc biệt, vì $\alpha \equiv (\alpha + km) \pmod{m}$ $\forall k \in \mathbb{Z}$ nên $f(\alpha) \equiv f(\alpha + km) \pmod{m}$.

Nhưng $f(\alpha) \equiv 0 \pmod{m}$ nên ta có $f(\alpha + km) \equiv 0 \pmod{m}$ với mọi $k \in \mathbb{Z}$.

e. Ta có thể chia hai vế của một đồng dư thức cho một ước chung của chúng nguyên tố với môđun m:

$$ac \equiv bc \pmod{m} \text{ và } UCLN(c,m) = 1 \Rightarrow a \equiv b \pmod{m}.$$

Chứng minh

Ta có $ac \equiv bc \pmod{m} \Rightarrow m|(ac - bc)$ hay $m|c(a - b)$. Nhưng $(m,c) = 1$ nên ta có $m|(a-b) \Rightarrow a \equiv b \pmod{m}$.

f. Có thể chia hai vế và môđun của một đồng dư thức cho một ước chung dương của chúng:

$$a \equiv b \pmod{m},\ 0 < \delta \in \mathbb{Z},\ \delta | UCLN(a,b,m) \Rightarrow \frac{a}{\delta} \equiv \frac{b}{\delta} \left(\bmod \frac{m}{\delta}\right).$$

Chứng minh

Từ giả thiết $\delta|(a, b, m)$, ta đặt $a = \delta a_1$, $b = \delta b_1$, $m = \delta m_1$ với a_1, b_1, $m_1 \in \mathbb{Z}$, $m_1 > 0$. Mặt khác, $a \equiv b \pmod{m} \Rightarrow a = b + mt$, $t \in \mathbb{Z}$. Ta có:

$$\delta a_1 = \delta b_1 + \delta m_1 \Rightarrow a_1 = b_1 + m_1 t \Rightarrow a_1 \equiv b_1 \pmod{m_1} \text{ hay } \frac{a}{\delta} \equiv \frac{b}{\delta} \left(\bmod \frac{m}{\delta}\right).$$

g. Nếu hai số đồng dư với nhau theo một môđun thì chúng cũng đồng dư theo môđun là ước của môđun ấy:

$$a \equiv b \pmod{m},\ \delta | m,\ \delta > 0 \Rightarrow a \equiv b \pmod{m}.$$

Chứng minh