ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN HỮU BẠN

ĐỊNH LÝ THẶNG DƯ TRUNG HOA

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN HỮU BẠN

ĐỊNH LÝ THẶNG DƯ TRUNG HOA

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
MÃ SỐ: 60.46.01.13

LUẬN VĂN THẠC SỸ TOÁN HỌC

Người hướng dẫn khoa học:
PGS TS. Nông Quốc Chinh

Thái Nguyên - 2014

Mục lục

LỜI MỞ ĐẦU

Trong các kỳ thi chọn học sinh giỏi Quốc gia và Quốc tế, các bài toán về số học thường đóng vai trò quan trọng. Khi nhắc đến số học hay lý thuyết số, ta không thể không nhắc tới định lý thặng dư Trung Hoa. Các bài toán sử dụng định lý này thường là những bài toán hay và khó.

Định lý Thặng dư Trung Hoa là tên người phương Tây đặt cho định lý này. Người Trung Quốc gọi nó là *Bài toán Hàn Tín điểm binh*. Tục truyền rằng khi Hàn Tín điểm quân số, ông cho quân lính xếp hàng 3, hàng 5, hàng 7 rồi báo cáo số dư. Từ đó, căn cứ vào lượng quân thì ông tính được chính xác quân số đến từng người.

Luận văn này được chia làm hai chương:

• Chương 1. Kiến thức chuẩn bị

Trong chương này, tác giả trình bày những kết quả đã biết trong số học như quan hệ đồng dư, hệ đồng dư, các định lý: Fermat, Euler, Wilson, ... Những kiến thức này sẽ được sử dụng trong việc giải các bài toán trong chương 2.

• Chương 2. Định lý thặng dư Trung Hoa

Nội dung chương này được chia làm hai phần. Phần đầu, tác giả nêu và chứng minh định lý thặng dư Trung Hoa và định lý thặng dư Trung Hoa dạng mở rộng. Phần thứ hai, tác giả trình bày những ứng dụng của định lý thặng dư Trung Hoa vào giải toán.

Luận văn được thực hiện và hoàn thành tại trường Đại học Khoa học - Đại học Thái Nguyên dưới sự hướng dẫn khoa học của PGS. TS. Nông Quốc Chinh. Qua đây, tác giả xin được gửi lời cảm ơn sâu sắc đến thầy giáo, người hướng dẫn khoa học của mình, PGS. TS. Nông Quốc Chinh, người đã đưa ra đề tài và tận tình hướng dẫn trong suốt quá trình nghiên cứu của tác giả. Đồng thời tác giả cũng chân thành cảm ơn các thầy cô trong trường Đại học Khoa học, Đại học Thái Nguyên, đã tạo mọi điều kiện cho tác giả về tài liệu và thủ tục hành chính để tác giả hoàn thành bản luận văn này. Tác giả cũng gửi lời cảm ơn đến gia đình, các đồng nghiệp đã động viên giúp đỡ tác giả trong quá trình học tập và làm luận văn.

Thái Nguyên, ngày 19 tháng 08 năm 2014

Tác giả

Chương 1

Kiến thức chuẩn bị

1.1 Định nghĩa đồng dư và các tính chất

1.1.1 Định nghĩa

Định nghĩa 1.1.1. Cho a, b, m là các số nguyên, m khác 0. Nếu $a - b$ chia hết cho m thì a được gọi là đồng dư với b modulo m, ký hiệu là $a \equiv b \pmod{m}$.

1.1.2 Các tính chất của đồng dư

Cho a, b, c, d là các số nguyên. Khi đó, ta có các tính chất sau đây

1) Nếu $a \equiv b \pmod{m}$ thì $b \equiv a \pmod{m}$.

2) Nếu $a \equiv b \pmod{m}$ và $b \equiv c \pmod{m}$ thì $a \equiv c \pmod{m}$.

3) Nếu $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$ thì $a + c \equiv b + d \pmod{m}$.

4) Nếu $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$ thì $ac \equiv bd \pmod{m}$.

5) Nếu $a \equiv b \pmod{m}$ và k là số nguyên dương thì $a^k \equiv b^k \pmod{m}$.

6) Nếu $a \equiv b \pmod{m}$ và $d|m$ thì $a \equiv b \pmod{d}$.

7) Nếu $a \equiv b \pmod{m}$ thì $ac \equiv bc \pmod{m}$ với mọi c khác 0.

8) Nếu $ab \equiv ac \pmod{m}$ và $(a, m) = 1$ thì $b \equiv c \pmod{m}$.

9) $a \equiv b \pmod{m_i}$ $(i = 1, 2, ..., n) \Leftrightarrow a \equiv b \pmod{[m_1, m_2, ..., m_n]}$.

1.2 Một vài định lý cần dùng

Định lý 1.2.1. Định lý Fermat nhỏ

Giả sử p nguyên tố, a là một số nguyên dương, $(a,p)=1$. Khi đó $a^{p-1} \equiv 1 \pmod{p}$.

Chứng minh. Xét dãy gồm $p-1$ số: $a, 2a, 3a, ..., (p-1)a$. Ta chứng minh rằng trong dãy không tồn tại hai số đồng dư với nhau trong phép chia cho p.

Giả sử $ka \equiv la \pmod{p}$ với $k, l \in \{1, 2, ..., p-1\}$ và k khác l. Khi đó $a(k-l) \vdots p \Rightarrow k-l \vdots p \Rightarrow k = l$ (mâu thuẫn). Vậy khi chia $p-1$ số trong dãy trên cho p ta nhận được $p-1$ số dư khác nhau từ $1, 2, ..., p-1$. Suy ra

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \Leftrightarrow (p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

Do $((p-1)!, p) = 1$ nên ta có điều phải chứng minh. □

Nhận xét 1.2.2. • Từ định lý trên ta có $a^p \equiv a \pmod{p}$ (với p nguyên tố).

• Định lý đảo của định lý nhỏ Fermat không đúng. Ví dụ như ta có thể kiểm tra được rằng với mọi số nguyên dương a mà $(a, 561) = 1$ thì

$$a^{560} \equiv 1 \pmod{561}.$$

Nhưng $561 = 3 \cdot 11 \cdot 17$ không phải là số nguyên tố. Những số có tính chất đặc biệt như vậy gọi là số giả nguyên tố với mọi cơ sở, hoặc số Carmichael. Ta có một định lý quan trọng về số Carmichael như sau: "*Nếu n là số giả nguyên tố với mọi cơ sở, tức là $\forall a \in \mathbb{N}^*$, $(a,n)=1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$, thì $n = p_1 p_2 ... p_k$ với p_i là các số nguyên tố sao cho $p_i - 1 | n$ với mọi i.*

Bằng định lý Thặng dư Trung Hoa, ta đã xác định được dạng phân tích cơ sở của các số Carmichael. Tuy nhiên các số này rất hiếm. Hai số Carmichael đầu tiên là 561 và 41041.

Định lý 1.2.3. Định lý Euler

Nếu m là số nguyên dương và $(a,m)=1$, thì

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

trong đó $\phi(m)$ là số các số nguyên dương nhỏ hơn m và nguyên tố cùng nhau với m.

Định lý 1.2.4. Định lý Wilson

p là số nguyên tố khi và chỉ khi $(p-1)!+1$ chia hết cho p.

Chứng minh.

• Nếu $(p-1)!+1$ chia hết cho p thì hiển nhiên p là số nguyên tố. Vì khi đó p sẽ nguyên tố cùng nhau với các số từ 1 đến $p-1$. Do đó nó không có ước nào khác ngoài 1 và chính nó.

• Ngược lại, nếu p là số nguyên tố thì ta chứng minh $(p-1)!+1$ chia hết cho p.

Xét đa thức

$$g(x) = (x-1)(x-2)...(x-(p-1))$$

và

$$f(x) = g(x) - (x^{p-1} - 1).$$

Rõ ràng phương trình $g(x) \equiv 0 \pmod{p}$ có $p-1$ nghiệm là $1, 2, ..., p-1$.

Theo định lý Fermat nhỏ, $x^{p-1}-1 \equiv 0 \pmod{p}$ có $p-1$ nghiệm là $1, ..., p-1$.

Suy ra đa thức $f(x) \equiv 0 \pmod{p}$ cũng có $p-1$ nghiệm. Nhưng đa thức $f(x)$ có bậc nhỏ hơn $p-1$, nên theo định lý Lagrange, các hệ số của $f(x)$ đồng dư 0 theo modulo p. Hơn nữa, $(p-1)!+1$ lại là hệ số tự do trong $f(x)$. Vậy $(p-1)!+1$ chia hết cho p. □

1.3 Hệ thặng dư đầy đủ

• Tập hợp $x_1, x_2, ..., x_n$ được gọi là một *hệ thặng dư đầy đủ modulo m* nếu với mỗi số nguyên y tồn tại duy nhất một số x_i sao cho $y \equiv x_i \pmod{m}$.

• Tập $\{1, 2, ..., m-1, m\}$ là một hệ thặng dư đầy đủ modulo m.

• Mọi hệ thặng dư đầy đủ modulo m đều có đúng m phần tử.

• Một tập gồm m phần tử là một hệ thặng dư đầy đủ modulo m nếu và chỉ nếu hai phần tử khác nhau bất kỳ của nó không đồng dư với nhau theo modulo m.

• Cho số nguyên a và $m > 0$. Tập hợp tất cả các số nguyên x thỏa mãn $x \equiv a \pmod{m}$ được gọi là một lớp đồng dư modulo m, ký hiệu $\overline{a} = \{a + mt : t \in \mathbb{Z}\}$. Có m lớp đồng dư phân biệt modulo m thu được bằng cách lấy lần lượt $a = 1, 2, ..., m$.

• Một tập hợp $\{r_1, r_2, ..., r_n\}$ được gọi là một hệ thặng dư thu gọn modulo m nếu $(r_i, m) = 1$, $r_i \neq r_j$ với mọi $i \neq j$, $1 \leq i, j \leq n$ và với mọi số nguyên x nguyên tố cùng nhau với m thì tồn tại r_i sao cho $r_i \equiv x \pmod{m}$.

Định lý 1.3.1. *Cho $(a, m) = 1$ và $\{r_1, r_2, ..., r_n\}$ là một hệ thặng dư thu gọn (đầy đủ) modulo m. Khi đó $ar_1, ar_2, ..., ar_n$ cũng là một hệ thặng dư thu gọn (đầy đủ) modulo m.*

1.4 Nghịch đảo modulo m

Định nghĩa 1.4.1. Giả sử a, m là các số nguyên, $m > 1$. Nghiệm của phương trình $ax \equiv 1 \pmod{m}$ được gọi là nghịch đảo của a modulo m.

Định lý 1.4.2. *Nghịch đảo của a modulo m tồn tại $\Leftrightarrow (a, m) = 1$.*

Hệ quả 1.4.3. *Nếu p nguyên tố thì mỗi phần tử của tập hợp $\{1, 2, ..., p-1\}$ đều có nghịch đảo duy nhất modulo p.*

Chương 2

Định lý Thặng dư Trung Hoa và ứng dụng

Định lý Thặng dư Trung Hoa là tên người phương Tây đặt cho định lý này. Người Trung Quốc gọi nó là *Bài toán Hàn Tín điểm binh*. Tục truyền rằng khi Hàn Tín điểm quân số, ông cho quân lính xếp hàng 3, hàng 5, hàng 7 rồi báo cáo số dư. Từ đó ông tính được chính xác quân số đến từng người.

Trong chương này, chúng tôi sẽ trình bày nội dung của định lý Thặng dư Trung Hoa và một số ứng dụng của định lý này.

2.1 Định lý thặng dư Trung Hoa

2.1.1 Một số kết quả bổ trợ

Bổ đề 2.1.1. *Giả sử rằng m, n là các số nguyên khác 0 thỏa mãn $(m, n) = 1$. Giả sử a là một số nguyên tùy ý. Khi đó $mn|a \Leftrightarrow m|a$ và $n|a$.*

Chứng minh. • Nếu $mn|a$ thì $a = mnt = m(nt) = n(mt)$ với số nguyên t nào đó, và do vậy $m|a$ và $n|a$.

• Ngược lại, nếu $m|a$ thì ta có $a = mb$ với số nguyên b nào đó. Do $n|mb$ và $(n, m) = 1$ nên chúng ta có $n|b$. Do vậy $b = nc$ với số nguyên c nào đó. Từ đó $a = mb = mnc \Rightarrow mn|a$. □

Hệ quả 2.1.2. *Giả sử rằng m, n là các số nguyên dương thỏa mãn $(m, n) = 1$ và $a, b \in \mathbb{Z}$. Khi đó $a \equiv b \pmod{mn} \Leftrightarrow a \equiv b \pmod{m}$ và $a \equiv b \pmod{n}$.*

Chứng minh. $a \equiv b \pmod{mn} \Leftrightarrow mn|(a-b) \Leftrightarrow m|(a-b)$ và $n|(a-b)$ (theo Bổ đề 2.1.1) $\Leftrightarrow a \equiv b \pmod{m}$ và $a \equiv b \pmod{n}$. □

Bổ đề 2.1.3. *Giả sử rằng $m_1, m_2, ..., m_t, m$ là các số nguyên khác 0 thỏa mãn $(m, m_i) = 1$ với $i = 1, 2, ..., t$. Khi đó $(m, m_1 \cdots m_t) = 1$.*

Chứng minh. Ta dùng phản chứng. Giả sử rằng $(m, m_1 \cdots m_t) > 1$. Khi đó tồn tại một số nguyên tố p thỏa mãn $p|m$ và $p|m_1 \cdots m_t$. Do p nguyên tố, $p|m_i$ với i nào đó nên (m, m_i) khác 1 (trái với giả thiết). Vậy ta có điều phải chứng minh. □

Bổ đề 2.1.4. *Giả sử rằng $m_1, m_2, ..., m_t$ là các số nguyên dương thỏa mãn $(m_i, m_j) = 1$ nếu i khác j (Chúng ta gọi điều này là tập các số nguyên đôi một nguyên tố cùng nhau). Đặt $m = m_1 \cdots m_t$. Nếu $a, b \in \mathbb{Z}$ thì*

$$a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{m_i} \text{ với mọi } i = 1, 2, ..., t.$$

Chứng minh.

• Nếu $a \equiv b \pmod{m}$ thì dễ dàng suy ra $a \equiv b \pmod{m_i}$ với mọi $i = 1, 2, ..., t$.

• Ngược lại, giả sử $a \equiv b \pmod{m_i}$ với mọi $i = 1, 2, ..., t$, ta sẽ chứng minh $a \equiv b \pmod{m}$ bằng cách quy nạp theo t.

Nếu $t = 2$ thì đó chính là Hệ quả 2.1.2.

Giả sử kết quả đúng với t, và $m_1, m_2, ..., m_t, m_{t+1}$ là các số đôi một nguyên tố cùng nhau cho trước.

Đặt $m = m_1 \cdots m_2 \cdots m_{t+1}$. Do $(m_{t+1}, m_i) = 1$ với mọi $i = 1, 2, ..., t$ nên suy ra rằng $(m_{t+1}, m_1 \cdots m_t) = 1$ (theo Bổ đề 2.1.3). Ta viết $m = (m_1 \cdots m_t) \cdot m_{t+1}$. Khi đó

$$\begin{aligned} a \equiv b \pmod{m} \\ &\Leftrightarrow a \equiv b \pmod{m_1 \cdots m_t} \text{ và } a \equiv b \pmod{m_{t+1}} \text{ (theo Hệ quả 2.1.2)} \\ &\Leftrightarrow a \equiv b \pmod{m_i} \text{ với mọi } i \leq t \text{ và } a \equiv b \pmod{m_{t+1}} \\ &\Leftrightarrow a \equiv b \pmod{m_i} \text{ với mọi } i \leq t+1. \square \end{aligned}$$