ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

PHAN THỊ MỪNG

THẶNG DƯ TOÀN PHƯƠNG VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

PHAN THỊ MỪNG

THẶNG DƯ TOÀN PHƯƠNG VÀ ỨNG DỤNG

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 8 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
GS.TSKH. ĐẶNG HÙNG THẮNG

THÁI NGUYÊN - 2019

Mục lục

Bảng ký hiệu

(a, b): Ước chung lớn nhất của a và b

$[a, b]$: Bội chung lớn nhất của a và b

$a|b$: a là ước của b

$a \not| b$: a không là ước của b

$[x]$: Phần nguyên của số thực x

$\sum_{i=1}^{n} a_i$: $a_1 + ... + a_n$

$\prod_{i=1}^{n} a_i$: $a_1...a_n$

$a \equiv b(mod n)$: a đồng dư với b modulo n

$a \not\equiv b(mod n)$: a không đồng dư với b modulo n

$ord_m a$: cấp của a modulo m

F_n: Số Fermat thứ n

$\phi(n)$: Hàm Euler

$\left(\frac{a}{p}\right)$: Ký hiệu Legendre

$\left(\frac{a}{n}\right)$: Ký hiệu Jacobi

Mở đầu

Lý thuyết thặng dư - lý thuyết đặc biệt quan trọng trong số học và đã được nhiều nhà Toán học nghiên cứu, vận dụng trong việc giải nhiều bài toán hay, khó và có ứng dụng thực tế.

Trong các kì thi Olympic Toán học ở Việt Nam và các nước trên thế giới thì lý thuyết thặng dư là phần được quan tâm đáng kể, vì thế việc có những hiểu biết ban đầu về thặng dư sẽ giúp ta giải nhiều bài toán khó trong số học một cách nhẹ nhàng, ngắn gọn và đẹp.

Tuy nhiên, trong nhà trường phổ thông thì thời lượng giảng dạy cho phần lý thuyết thặng dư chưa nhiều nên học sinh thường thấy phần kiến thức này rất khó, vượt ra hiểu biết của các em. Vì vậy để giúp bản thân có những hiểu biết sâu sắc hơn về lý thuyết thặng dư, phục vụ tốt hơn cho công tác bồi dưỡng học sinh giỏi, tôi chọn đề tài "Thặng dư toàn phương và ứng dụng" để nghiên cứu.

Ngoài phần mở đầu và kết luận, nội dung chính của luận văn được trình bày trong ba chương:

Chương 1. Đồng dư và phương trình đồng dư
1.1. Đồng dư thức
1.2. Hệ thặng dư và lớp thặng dư
1.3. Định lý Euler và định lý Fermat
1.4. Phương trình đồng dư một ẩn

Chương 2. Thặng dư toàn phương
2.1. Thặng dư toàn phương
2.2. Ký hiệu Legendre
2.3. Định luật tương hỗ
2.4. Ký hiệu Jacobi

Chương 3. Một số ứng dụng của thặng dư toàn phương
3.1. Kiểm tra tính chất nguyên tố của số Fermat
3.2. Khái niệm số giả nguyên tố Euler
3.3. Giải một số bài toán khó trong Số học phổ thông

Để hoàn thành bản luận văn này, tôi xin được bày tỏ lòng biết ơn sâu sắc tới GS. TSKH Đặng Hùng Thắng, người thầy nhiệt huyết đã truyền thụ kiến thức, đã chỉ ra hướng đề tài và tận tình hướng dẫn trong suốt quá trình làm luận văn. Đồng thời, tôi xin chân thành cảm ơn các thầy, cô phản biện đã dành thời gian đọc và đóng góp những ý kiến quý báu cho bản luận văn này.

Tôi xin chân thành cảm ơn toàn thể các thầy cô trong Khoa Toán - Tin, Trường Đại học Khoa học - Đại học Thái Nguyên đã tận tình hướng dẫn, truyền đạt kiến thức trong suốt thời gian theo học, thực hiện và hoàn thành luận văn. Qua luận văn này, tôi cũng muốn gửi lời cảm ơn tới gia đình, bạn bè đã luôn động viên, giúp đỡ tôi trong thời gian làm luận văn.

Mặc dù đã có nhiều cố gắng hoàn thiện luận văn bằng tất cả sự nhiệt tình và năng lực của mình. Tuy nhiên, luận văn không thể tránh khỏi những thiếu sót, tôi rất mong nhận được những đóng góp quý báu của thầy cô và các bạn.

Thái Nguyên, ngày 29 tháng 12 năm 2019
Tác giả luận văn

Phan Thị Mừng

Chương 1

Đồng dư và phương trình đồng dư

1.1 Đồng dư thức

1.1.1 Khái niệm đồng dư

Cho trước số tự nhiên m lớn hơn 1. Ta nói các số nguyên a, b đồng dư với nhau theo modulo m nếu khi chia a và b cho m ta được cùng một số dư. Kí hiệu:

$$a \equiv b(\mathrm{mod} m) \tag{1.1}$$

Nói cách khác, a đồng dư với b theo modulo m nếu a và b biểu diễn được dưới dạng:

$$\begin{aligned} a &= pm + r \\ b &= qm + r \\ (0 &\leq r < m) \end{aligned}$$

Từ đó suy ra:

$$a \equiv b(\mathrm{mod} m)$$

khi và chỉ khi

$$m/a - b.$$

khi và chỉ khi tồn tại số nguyên t sao cho

$$a = b + mt.$$

Hệ thức (1.1) được gọi là một đồng dư thức.

1.1.2 Tính chất của đồng dư thức

a) • $a \equiv a(\mathrm{mod}m) \forall a$.

• Nếu $\begin{matrix} a \equiv b(\mathrm{mod}m) \\ b \equiv c(\mathrm{mod}m) \end{matrix}$ thì $a \equiv c(\mathrm{mod}m)$

• Nếu $\begin{matrix} a_1 \equiv b_1(\mathrm{mod}m) \\ a_2 \equiv b_2(\mathrm{mod}m) \end{matrix}$ thì $a_1 \pm a_2 \equiv b_1 \pm b_2(\mathrm{mod}m)$

Chứng minh. Ta chỉ chứng minh với phép toán cộng, phép trừ hoàn toàn tương tự.

Từ giả thiết ta có:

$$a_1 = b_1 + mt_1$$
$$a_2 = b_2 + mt_2$$

Cộng từng vế của hai đẳng thức ta có:

$$(a_1 + a_2) = (b_1 + b_2) + m(t_1 + t_2)$$

Chứng tỏ

$$a_1 + a_2 \equiv b_1 + b_2(\mathrm{mod}m).$$

Từ tính chất này ta suy ra:
* Có thể thêm, bớt cùng một số ở hai vế của một đồng dư thức. Nghĩa là: Nếu $a \equiv b(\mathrm{mod}m)$ thì $a + c \equiv b + c(\mathrm{mod}m)$ với c là số nguyên tùy ý.
* Có thể chuyển vế (phải đổi dấu) các số hạng của một đồng dư thức. Nghĩa là:

$$a + c \equiv b(\mathrm{mod}m)$$

khi và chỉ khi

$$a \equiv b - c(\mathrm{mod}m)$$

* Có thể thêm, bớt một vế của đồng dư thức một bội số của m. Nghĩa là:

$$a \equiv b(\mathrm{mod}m)$$

thì

$$a + tm \equiv b(\mathrm{mod}m)$$

b) Nếu

$$a_1 \equiv b_1(\mathrm{mod}m)$$
$$a_2 \equiv b_2(\mathrm{mod}m)$$

thì

$$a_1.a_2 \equiv b_1.b_2(\mathrm{mod}m)$$

Chứng minh. Từ giả thiết ta có:

$$\begin{aligned} &a_1 = b_1 + mt_1 \\ &a_2 = b_2 + mt_2 \\ &(t_1, t_2 \in \mathbb{Z}) \end{aligned}$$

Nhân từng vế của hai đẳng thức ta được:

$$a_1.a_2 \equiv b_1.b_2 + mT$$

trong đó T là một số nguyên.

$$\Rightarrow a_1.a_2 \equiv b_1.b_2 (\mathrm{mod} m)$$

Từ tính chất này ta có thể suy ra các tính chất sau:
* Có thể nhân cả hai vế của một đòng dư thức với cùng một số nguyên. Chính xác hơn:

Nếu $a \equiv b (\mathrm{mod} m)$ thì $ak \equiv bk (\mathrm{mod} m)$
* Có thể nâng lên lũy thừa nguyên dương hai vế của một đồng dư thức. Tức là:

Nếu $a \equiv b (\mathrm{mod} m)$ thì $a^n \equiv b^n (\mathrm{mod} m)$ trong đó n nguyên dương bất kì.

c) Đặc biệt khi $m = p$ là số nguyên tố,

$$a = a_1.a_2.$$

Ta có khẳng định sau:

$$a \equiv 0 (\mathrm{mod} p)$$

khi và chỉ khi:

$$\left[\begin{array}{l} a_1 \equiv 0 (\mathrm{mod} p) \\ a_2 \equiv 0 (\mathrm{mod} p) \end{array} \right.$$

Chứng minh.

$$\begin{aligned} &a \equiv 0 (\mathrm{mod} p) \\ &\Leftrightarrow p/a \\ &\Leftrightarrow p/a_1 a_2 \\ &\Leftrightarrow \left[\begin{array}{l} p/a_1 \\ p/a_2 \end{array} \right. \\ &\Leftrightarrow \left[\begin{array}{l} a_1 \equiv 0 (\mathrm{mod} p) \\ a_2 \equiv 0 (\mathrm{mod} p) \end{array} \right. \end{aligned}$$

d) Nếu $a \equiv b(\mathrm{mod}m)$, $d/a, d/b, (d,m) = 1$ thì

$$\frac{a}{d} = \frac{b}{d}(\mathrm{mod}m)$$

Chứng minh. Giả sử $a = a_1 d, b = b_1 d$. Ta có:

$$\begin{aligned} & a \equiv b(\mathrm{mod}m) \\ & \Rightarrow m/a - b \\ & \Rightarrow m/d(a_1 - b_1), \end{aligned}$$

mà $(d,m) = 1$ nên $m/a_1 - b_1$. $\Rightarrow a_1 \equiv b_1(\mathrm{mod}m)$.

e) $a \equiv b(\mathrm{mod}m)$ khi và chỉ khi $ak \equiv bk(\mathrm{mod}mk)$ trong đó k nguyên dương bất kì.

Chứng minh.

$$\begin{aligned} & a \equiv b(\mathrm{mod}m) \\ & \Leftrightarrow a = b + mt \\ & \Leftrightarrow ak = bk + mkt \\ & \Leftrightarrow ak \equiv bk(\mathrm{mod}mk) \end{aligned}$$

g) Nếu $\begin{cases} a \equiv b(\mathrm{mod}m_1) \\ a \equiv b(\mathrm{mod}m_2) \end{cases}$ thì $a \equiv b(\mathrm{mod}m)$ trong đó $m = [m_1, m_2]$

Chứng minh. Từ giả thiết ta có:

$$\begin{cases} m_1/a - b \\ m_2/a - b \end{cases}$$

tức là $a - b$ là bội chung của m_1 và m_2.

Theo định nghĩa bội chung nhỏ nhất ta có

$$\begin{aligned} & m/a - b \\ & \Rightarrow a \equiv b(\mathrm{mod}m) \end{aligned}$$

h) Nếu $a \equiv b(\mathrm{mod}m)$ thì $a \equiv b(\mathrm{mod}d)$ trong đó d là ước số của m với $d > 1$.

Chứng minh.

$$\begin{aligned} & a \equiv b(\mathrm{mod}m) \\ & \Rightarrow m/a - b, \end{aligned}$$