ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

ĐỒNG THỊ HUYỀN TRANG

PHƯƠNG TRÌNH ĐỒNG DƯ

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - Năm 2012

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

ĐỒNG THỊ HUYỀN TRANG

PHƯƠNG TRÌNH ĐỒNG DƯ

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số : 60.46.40

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS ĐÀM VĂN NHỈ

Thái Nguyên - Năm 2012

Mục lục

LỜI NÓI ĐẦU

Trong số học, thường ta phải xác định tất cả các số với tính chất p cho trước. Có thể có những số thỏa mãn tính chất p, nhưng có nhiều khi không có. Nếu ta xét tất cả các số thuộc tập $\mathbb{Z}$ thì đây là một công việc không thể thực hiện được. Nhưng nếu ta xét trên một tập hữu hạn nào đấy thì việc kiểm tra có thể thực hiện được. Lý thuyết đồng dư chính là việc chuyển những bài toán xét trên tập vô hạn $\mathbb{Z}$ về một tập hữu hạn những lớp đồng dư theo một môđun m nào đấy. Chẳng hạn:
Xác định x, y nguyên thỏa mãn: $x^2 + 1 = 3y$. Giả sử phương trình có nghiệm nguyên. Lấy modun 3 ta có $x^2 + 1 \equiv 0 (\mathrm{mod}\ 3)$. Biểu diễn $x = 3k$ hoặc $x = 3k \pm 1$. khi đó $x^2 + 1 = 3h + 1$ hoặc $3h + 2$. Vậy $x^2 + 1 \not\equiv 0 \pmod 3$: Mâu thuẫn. Tóm lại phương trình vô nghiệm.
Xác định x, y nguyên thỏa mãn: $x^2 + 2 = 5y$. Giả sử phương trình có nghiệm nguyên. Lấy modun 5 ta có $x^2 + 2 \equiv 0 (\mathrm{mod}\ 5)$. Biểu diễn $x = 5k$ hoặc $x = 5k \pm 1$hoặc $x = 5k \pm 2$. Khi đó $x^2 + 2 = 5h + 2$ hoặc $5h + 3$ hoặc $5h + 6$. Vậy $x^2 + 2 \not\equiv 0 \pmod 5$: Mâu thuẫn. Tóm lại phương trình vô nghiệm.
Qua ví dụ trên thay cho việc x, y thuộc tập $\mathbb{Z}$ vô hạn thì ta chỉ việc kiểm tra $\overline{x}$ nhận $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$.
Nội dung luận văn được chia thành ba chương:

Chương 1 **" Lý thuyết đồng dư"** bao gồm 5 mục. Mục 1.1 được dành trình bày về *Phép chia trong vành* $\mathbb{Z}$, kết quả chính trình bày lại thuật toán Euclid dể tìm ƯCLN và định lý cơ bản của số học. Mục 1.2 được dành trình bày về *Quan hệ đồng dư và tính chất* kết quả chính đã chỉ ra

được những tính chất cơ bản của quan hệ đồng dư. Mục 1.3 *Vành $\mathbb{Z}_m$ các lớp thặng dư môđun m* chứng minh được $\mathbb{Z}$ là vành giao hoán, chứng minh được $\mathbb{Z}_m^*$ là nhóm nhân. Mục 1.4 *Định lý Euler và Định lý Fermat* . Mục 1.5 *Một số ví dụ tổng hợp.*

Chương 2 **"Phương trình đồng dư"** bao gồm 6 mục. Mục 2.1 *Phương trình đồng dư một ẩn.* Mục 2.2 *Phương trình dồng dư bậc nhất.* Mục 2.3 *Hệ phương trình đồng dư một ẩn.* Mục 2.4 *Phương trình đồng dư một ẩn bậc cao.* Mục 2.5 *Phương trình đồng dư một ẩn bậc cao theo môđun p.* Mục 2.6 *Phương trình đồng dư bậc hai.* Kết quả chính của chương là trình bày chi tiết việc giải một số dạng phương trình đồng dư và trình bày lại chứng minh định lý Wilson.

Chương 3 **" Phương trình Mordell"** bao gồm 5 mục. Mục 3.1 *Chuẩn trong vành $\mathbb{Z}[\sqrt{d}]$ và số học.* Mục 3.2 *Khái niệm phương trình Mordell.* Mục 3.3 *Một vài phương trình có nghiệm.* Mục 3.4 *Một vài phương trình vô nghiệm.* Mục 3.5 *Ứng dụng của thặng dư bậc 3.* Kết quả chính của chương là trình bày được phương trình Mordell. Đã chỉ ra một số dạng phương trình có nghiệm hoặc vô nghiệm. Trình bày được thặng dư bậc ba.

Do thời gian và kiến thức còn hạn chế nên trong quá trình viết luận văn cũng như trong xử lý văn bản chắc chắn không tránh khỏi những sai sót nhất định. Tác giả luận văn rất mong nhận được sự góp ý của các thầy cô và các bạn đồng nghiệp để luận văn được hoàn thiện hơn.

Nhân dịp này, tác giả xin bày tỏ lòng biết ơn sâu sắc đến thầy hướng dẫn PGS.TS Đàm Văn Nhỉ đã tận tình giúp đỡ trong suốt quá trình làm luận văn.

Tác giả xin trân trọng cảm ơn các thầy, cô giáo Trường Đại học Khoa học- Đại học Thái Nguyên đã giảng dạy và tạo mọi điều kiện thuận lợi trong quá trình tác giả học tập và nghiên cứu.

Tác giả cũng xin chân thành cảm ơn tập thể bạn bè đồng nghiệp và gia đình đã quan tâm giúp đỡ, động viên tác giả hoàn thành tốt luận văn này.

Thái Nguyên, tháng 07 năm 2012.

Tác giả luận văn

Đồng Thị Huyền Trang

Chương 1

Lý thuyết đồng dư

Phương pháp đồng dư do Gauss đề xuất là một phương pháp hữu ích trong việc giải quyết nhiều vấn đề có liên quan đến tính chia hết của các số nguyên.

1.1 Phép chia trong vành $\mathbb{Z}$

Định lý 1.1.1. *Với mỗi cặp số nguyên a và $b \neq 0$, luôn tồn tại duy nhất một cặp số nguyên q, r với $0 \leq r < |b|$ để $a = qb + r$.*

Chứng minh: Sự tồn tại: Đặt $T = \{n\,|b|\ sao\,cho\,n\,|b| \leq a, n \in \mathbb{Z},\}$. Vì $|b| \geq 1$ nên

$$-|a|\,|b| \leq -|a| \leq a$$

Do đó $-|a|\,|b| \in T$. Vậy $T \neq 0$. Vì T là tập bị chặn triên T có một số lớn nhất $m\,|b|$. Từ $m\,|b| \leq a$ ta suy ra $r = a - m\,|b| \geq 0$. Ta lại có

$$(m+1)\,|b| = m\,|b| + |b| > m\,|b|\,.$$

Do $m\,|b|$ lớn nhất trong T nên $(m+1)\,|b|$. Như vậy $|b| > a - m\,|b| = r$ và ta có $a = qb + r$ với $0 \leq r < |b|$. Bây giờ ta chứng minh tính duy nhất. Giả sử có hai biểu diễn $a = qb + r$ với $0 \leq r < |b|$ và $a = q_1 b + r_1$ với $0 \leq r_1 < |b|$. Trừ từng vế, ta có $r - r_1 = b(q_1 - q)$. Từ $|r - r_1| < |b|$ ta

suy ra $|q_1 - q|\,|b| < |b|$. Vậy $q = q_1$ và do đó $r = r_1$.

Giả sử $a = qb + r, 0 \leq r < |b|$. Khi đó nếu $r = 0$ thì q được gọi là thườn của phép chia a cho b.., nếu $r \leq 0$ thì q gọi là thương hụt, còn gọi r là số dư của phép chia a cho b.

Định lý 1.1.2. [Định lý cơ bản của số học] *Mọi số tự nhiên lớn hơn 1 đều phân tích được thành một tích hữu hạn thừa số nguyên tố, và phân tích này là duy nhất nếu không kể đến thứ tự các thừa số.*

Chứng minh: Xét tập F gồm tất cả các số nguyên lớn hơn 1 không biểu diễn thành tích một số hữu hạn các thừ số nguyên tố. Ta chỉ cần chỉ ra $F \neq \phi$. Thật vậ, giả sử $F \neq \phi$. Khi đó có hai sô nguyên dương $q_1, q_2 > 0$ để $m = q_1 q_2$. Vì $q_1, q_2 < m$ nên $q_1, q_2 \notin F$. Như vậy ta có phân tích $q_1 = t_1, t_2, ..., t_h$ và $q_2 = u_1, u_2, ..., u_k$, ở đó các t_i, u_j đều là các số nguyên tố. Khi đó

$$m = q_1 q_2 = t_1 t_2 ... t_h u_1 u_2 ... u_k.$$

Điều này mâu thuẫn với giả thiết $m \in F$. Như vậy F là tập rỗng. Do đó mọi số tự nhiên lớn hơn 1 đều phân tích được thành tích của hữu hạn thừa số nguyên tốt. Bây giờ giả sử một số được phân tích thành hai tích dạng A và B các thừa số nguyên tố . Khi đó $A = B$. Bằng cách lược bỏ các tất cả các thừa số nguyên tố xuất hiện trong cả A và B, ta nhận được đẳng thức tương đương $C = D$. Ta cần phải chứng minh $C = D = 1$. Thật vậy giả sử trái lại $C = D \leq 1$. Gọi p là thừa số nguyên tố xuất hiện trong C. Khi đó p không thể là thừa số xuất hiện trong biểu thức tích của D. Có nghĩa là D không là bội của p, và do đó C cũng không là bội của p (mâu thuẫn!). Vậy $C = D = 1$. Điều này chứng tỏ rằng sự phân tích ra các thừa số nguyên tố của một số nguyên >1 là duy nhất nếu không kể đến thứ tự các thừa số.

Khi phân tích các số tự nhiên $q > 1$ thành tích các thừa số nguyên tố, có thể một số nguyên tố xuất hiện nhiều lần. Nếu các số nguyên tố $p_1, ..., p_s$

xuất hiện theo thứ tự $\alpha_1, ..., \alpha_s$ lần, ta viết $q = p_1^{\alpha_1} p_2^{\alpha_2} ... p_s^{\alpha_s}$ và ta gọi tích này là dạng phân tích tiêu chuẩn hay dạng phân tích chính tắc của q.
Khi hai số nguyên dương a, b ở dạng phân tích tiêu chuẩn, có thừa số nguyên tố pcủa a nhưng không là của b, thì ta có thể bổ sung vào phân tích của b thừa số p^0 (và ngược lại). Khi đó ta luôn viết được

$$a = p_1^{u_1} p_2^{u_2} ... p_s^{u_s}$$

và

$$b = p_1^{v_1} p_2^{v_2} ... p_s^{v_s},$$

trong đó có thể có những số mũ 0. Như vậy với hai số nguyên dương a, b luôn tồn tại các số nguyên tố $p_1, p_2, ..., p_s$ để

$$a = p_1^{u_1} p_2^{u_2} ... p_s^{u_s}$$

và

$$b = p_1^{v_1} p_2^{v_2} ... p_s^{v_s},$$

với các số mũ nguyên không âm. Khi đó dễ thấy rằng:

$$(a, b) = p_1^{\min(u_1, v_1)} p_2^{\min(u_2, v_2)} ... p_s^{\min(u_s, v_s)}$$

$$[a, b] = p_1^{\max(u_1, v_1)} p_2^{\max(u_2, v_2)} ... p_s^{\max(u_s, v_s)}.$$

Thuật toán Euclid: Giả sử a và b là hai số nguyên dương với $a \geq b$ và đặt $r_0 = a, r_1 = b$. Bằng cách áp dụng liên tiếp thuật toán chia, ta được:

$$r_0 = r_1 q_0 + r_2,\ r_1 = r_2 q_2 + r_3, ...,\ r_{n-2} = r_{n-1} q_{n-1} + r_2,\ r_{n-1} = r_n q_n$$

Với $r_1 > r_2 > ... > r_0 > 0$. Cuối cùng, số 0 sẽ xuất hiện trong dãy phép chia liên tiếp, vì dãy các số dư $b = r_1 > r_2 > ... \geq 0$ không chứa quá b số