ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI THỊ HOÀNG YẾN

SỐ P-ADIC

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - Năm 2012

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI THỊ HOÀNG YẾN

SỐ P-ADIC

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. NÔNG QUỐC CHINH

Thái Nguyên - Năm 2012

Mục lục

Mở đầu

Số p-adic để mã hóa thông tin, có ứng dụng mạnh mẽ trong lý thuyết số. Giải tích p-adic là một trong các hướng mới và đang phát triển nhanh trong ngành đại số và lý thuyết số. Mục tiêu chính của luận văn là giới thiệu những khái niệm cơ bản nhất về số p-adic và giải tích p-adic.

Luận văn gồm có phần Mở đầu, 4 chương tiếp theo và phần kết luận.

Chương 1. Trình bày những kiến thức về đồng dư thức và phương trình modulo.

Chương 2. Xây dựng các khái niệm chuẩn, chuẩn Archimedean, chuẩn phi−Archimedean trên một vành giao hoán có đơn vị. Cấp p-adic, chuẩn p-adic của một số hữu tỉ; Khái niệm dãy hội tụ, dãy Cauchy; Khái niệm vành đầy đủ đối với một chuẩn N; Xây dựng vành các số p-adic và một vài tính chất của nó.

Chương 3. Giới thiệu sơ lược một số khái niệm và tính chất cơ bản của giải tích p-adic.

Chương 4. Một số bài tập tham khảo.

Mỗi chương đều có ví dụ và phần bài tập liên quan.

Luận văn này được hoàn thành tại Trường Đại học Khoa học, Đại học Thái Nguyên dưới sự hướng dẫn của PGS.TS. Nông Quốc Chinh. Tác giả xin bày tỏ lòng kính trọng và biết ơn sâu sắc tới thầy về sự tận tình hướng dẫn trong suốt thời gian tác giả làm luận văn.

Trong quá trình học tập và làm luận văn, thông qua các bài giảng và

xêmina, tác giả thường xuyên nhận được sự quan tâm giúp đỡ và đóng góp những ý kiến quý báu của các giáo sư trong Viện Toán học thuộc Viện Khoa học và Công nghệ Việt Nam cùng các thấy cô giáo trong trường Đại học Khoa học - Đại học Thái Nguyên. Từ đáy lòng mình, tác giả xin bày tỏ lòng biết ơn sâu sắc đến các thầy các cô.

Tác giả xin bày tỏ lòng biết ơn tới các thầy, các cô, Ban Giám hiệu Nhà trường, phòng Đào tạo Khoa học và Quan hệ Quốc tế, Khoa Toán - Tin Trường Đại học Khoa học - Đại học Thái Nguyên đã quan tâm và giúp đỡ tác giả trong thời gian học tập và làm luận văn cao học.

Cuối cùng, tác giả xin gửi lời cảm ơn tới gia đình, bạn bè, đồng nghiệp đã luôn theo sát, động viên tác giả vượt qua những khó khăn để có được điều kiện tốt nhất khi học tập và nghiên cứu.

Mặc dù đã hết sức cố gắng, song do năng lực và thời gian còn hạn chế nên chắc chắn luận văn không thể tránh khỏi thiếu sót. Vì vậy tác giả rất mong được sự góp ý, chỉ bảo của các Thầy cô, bạn bè đồng nghiệp và các độc giả quan tâm.

Xin chân thành cảm ơn!

Thái Nguyên, 19 tháng 10 năm 2012.

Tác giả

Bùi Thị Hoàng Yến

Chương 1

Đồng dư thức và phương trình modulo

Cho $n \in \mathbb{N}^*$.

Định nghĩa 1.1. *Cho $x, y \in \mathbb{Z}$, ta viết $x \underset{n}{\equiv} y$ nếu và chỉ nếu $n \,|(x-y)$. Ta thường viết $x \equiv y(\mathrm{mod} n)$ và đọc là x đồng dư với y theo modulo n.*

Chú ý rằng khi $n = 0$, $x \equiv y(\mathrm{mod} n)$ nếu và chỉ nếu $x = y$, vì vậy trường hợp $\underset{0}{\equiv}$ thực ra là đẳng thức.

Mệnh đề 1.1. *Quan hệ $\underset{n}{\equiv}$ là một quan hệ tương đương trên $\mathbb{Z}$.*

Chứng minh : Cho $x, y, z \in \mathbb{Z}$. Rõ ràng $\underset{n}{\equiv}$ có tính chất phản xạ vì $n \,|(x-x) = 0$. Nó có tính chất đối xứng vì nếu $n \,|(x-y)$ thì $x - y = kn$ với mỗi $k \in \mathbb{Z}$, suy ra $y - x = (-k)n$ và vì vậy $n \,|(y-x)$. Có tính chất bắc cầu, giả sử rằng $n \,|(x-y)$ và $n \,|(y-z)$, khi đó vì $x - z = (x-y) + (y-z)$ nên ta có $n \,|(x-z)$.

Ta kí hiệu lớp tương đương của $x \in \mathbb{Z}$ là $[x]_n$ hoặc chỉ là $[x]$ nếu n xác định, ta sử dụng chung kí hiệu $\bar{x}$ nếu giá trị của n là rõ ràng từ dữ kiện. Bằng định nghĩa

$[x]_n = \left\{ y \in \mathbb{Z} : y \underset{n}{\equiv} x \right\} = \{ y \in \mathbb{Z} : y = x + kn, \forall k \in \mathbb{Z} \}$, với mỗi số tự nhiên khác không có đúng n lớp thặng dư, cụ thể là

$$[0]_n, [1]_n, ..., [n-1]_n.$$

Định nghĩa 1.2. *Tập hợp gồm tất cả các lớp thặng dư của* $\mathbb{Z}$ *theo modulo* n *là tập thương:*

$$\mathbb{Z}/n\mathbb{Z} = \{[x]_n : x = 0, 1, ..., n-1\} = \mathbb{Z}_n$$

Nếu $n = 0$ ta có $\mathbb{Z}_n = \mathbb{Z}$.

Xét hàm $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$; $\pi_n(x) = [x]_n$.

Đây là một toàn ánh thỏa mãn

$$\pi_n^{-1}(\alpha) = \{x \in \mathbb{Z} : x \in \alpha\}$$

Ta có thể định nghĩa phép cộng $\underset{n}{+}$ và phép nhân $\underset{n}{\times}$ trên $\mathbb{Z}_n$ bởi công thức

$[x]_n + [y]_n = [x+y]_n$;$[x]_n \times [y]_n = [xy]_n$

Điều này ta có thể dễ dàng nhìn thấy từ định nghĩa, tức là chúng không phụ thuộc vào việc chọn các phần tử đại diện x và y.

Mệnh đề 1.2. *Tập* $\mathbb{Z}_n$ *với các phép toán* $\underset{n}{+}$ *và* $\underset{n}{\times}$ *là một vành giao hoán và hàm* $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ *là một đồng cấu vành, nó là một toàn ánh và có hạt nhân*

$$k\text{er}\pi_n = [0]_n = \{x \in \mathbb{Z} : x \equiv 0(\text{mod}n)\}$$

Cho R là một vành giao hoán với phần tử đơn vị 1.

Định nghĩa 1.3. *Phần tử* $u \in R$ *được gọi là một phần tử khả nghịch nếu tồn tại một phần tử* $v \in R$ *thỏa mãn* $uv = vu = 1$. *Phần tử* v *là duy nhất xác định và được gọi là nghịch đảo của* u *và thường được kí hiệu là* u^{-1}.

Định nghĩa 1.4. *Phần tử khác không* $z \in R$ *được gọi là một ước của không nếu tồn tại ít nhất một phần tử* $\text{w} \in R$ *với* $\text{w} \neq 0$ *và* $z\text{w} = 0$.

Ta quy ước phần tử 0 là ước của chính nó.

Ví dụ 1. Cho $n = 6$, khi đó $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, ..., \bar{5}\}$. Các phần tử khả nghịch là $\bar{1}, \bar{5}$ với $\bar{1}^{-1} = \bar{1}$ và $\bar{5}^{-1} = \bar{5}$ vì $5^2 = 25 \underset{6}{\equiv} 1$. Các ước của không là $\bar{0}, \bar{2}, \bar{3}, \bar{4}$.

Ta đã biết nếu $a, b \in \mathbb{Z}$ thì ước chung lớn nhất của a và b là số nguyên dương lớn nhất đồng thời là ước của cả a và b. Ta thường viết là $\gcd(a, b)$.

Định lí 1.1. *Cho $n > 0$, khi đó ta có*

i, Các phần tử của $\mathbb{Z}_n$ hoặc là khả nghịch, hoặc là ước của không.

ii, $\bar{z}$ là một ước của không trong $\mathbb{Z}_n$ nếu và chỉ nếu $\gcd(z, n) > 1$.

iii, $\bar{u}$ là một phần tử khả nghịch trong $\mathbb{Z}_n$ nếu và chỉ nếu $\gcd(u, n) = 1$.

Chứng minh : Lấy $\bar{u}$ tùy ý trong $\mathbb{Z}_n$, giả sử $\bar{u}$ không phải là phần tử khả nghịch. Suy ra $\gcd(u, n) \neq 1$ vậy $\exists v : u = u_1.v; n = n_1.v$, trong đó $n_1 < n$ và $\bar{n}_1 \neq \bar{0}$.

Xét tích $\bar{u}.\bar{n}_1$ ta có

$$\bar{u}.\bar{n}_1 = \bar{u}_1.\bar{v}.\bar{n}_1 = \bar{u}_1.\bar{n} = \bar{0}$$

Suy ra $\bar{u}$ là ước của không trong $\mathbb{Z}_n$.

Ta đã biết nếu $a, b \in \mathbb{Z}$ với $b \neq 0$, khi đó $\exists! q, r \in \mathbb{Z}$ sao cho $a = bq + r$ với $0 \leq r < |b|$.

Định lí 1.2. *(Thuật toán Euclid tìm ước chung lớn nhất)*

Cho $a, b \in \mathbb{Z}$, khi đó có những dãy duy nhất các số nguyên q_i, r_i thỏa mãn

$$a = bq_1 + r_1$$

$$r_0 = b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

.

.

.

$$0 \neq r_{N-1} = q_N + 1.r_N$$

Trong đó ta có $0 \leq r_i < r_{i-1}$ với mỗi i, $r_N = \gcd(a, b)$ và tìm được $s, t \in \mathbb{Z}$ sao cho

$$r_N = sa + tb$$

Ví dụ 2. Nếu $a = 6, b = 5$ thì $r_0 = 5$ và ta có

$6 = 1.5 + 1$ vì vậy $q_1 = 1, r_1 = 1$.

$5 = 1.5$ vì vậy $q_2 = 5, r_2 = 0$.

Suy ra ta có $\gcd(6, 5) = 1$ và có thể viết $1 = 1.6 + (-1).5$.

Định nghĩa 1.5. *Ký hiệu $(\mathbb{Z}_n)^\times$ là tập các phần tử khả nghịch trong $\mathbb{Z}_n$. Ta có $(\mathbb{Z}_n)^\times$ là một nhóm Abel với phép nhân $\underset{n}{\times}$.*

Cho $\varphi(n) = \left|(\mathbb{Z}_n)^\times\right|$ = cấp của $(\mathbb{Z}_n)^\times$. Từ định lý 1.1, suy ra $\left|(\mathbb{Z}_n)^\times\right|$ bằng số các số nguyên $0, 1, 2, ..., n-1$ mà không có ước chung với n. Hàm φ này được biết đến là φ - hàm Euler.

Ví dụ 3. Với $n = 6$; $|\mathbb{Z}_6| = 6$ và $\mathbb{Z}_6$ có các phần tử khả nghịch là $\bar{1}, \bar{5}$, suy ra $\varphi(6) = 2$.

Ví dụ 4. Với $n = 12$; $|\mathbb{Z}_{12}| = 12$ và $\mathbb{Z}_{12}$ có các phần tử khả nghịch là $\bar{1}, \bar{5}, \bar{7}, 1\bar{1}$, suy ra $\varphi(12) = 4$.

Ta sẽ nghiên cứu xác định giá trị của $\varphi(n)$ qua n. Khi n là một số nguyên tố ta có kết quả sau:

Ví dụ 5. Cho p là một số nguyên tố. Khi đó p chỉ có ước tầm thường là 1 và p vì vậy $\varphi(p) = p - 1$. Hơn nữa: xét một lũy thừa của p, p^r với $r > 0$, khi đó các số nguyên trong $0, 1, 2, ..., p^r - 1$ có nhân tử chung với p^r đều được biểu diễn dưới dạng kp với $0 \leq k \leq p^{r-1} - 1$, suy ra có p^{r-1} phần tử. Vì vậy ta có

$$\varphi(p^r) = p^{r-1}(p - 1)$$

Ví dụ 6. Khi $p = 2$, ta có các nhóm

$$(\mathbb{Z}_2)^\times = \{\bar{1}\},$$

$$(\mathbb{Z}_{2^2})^\times = \{\bar{1}, \bar{3}\} \cong \mathbb{Z}_2,$$

$$(\mathbb{Z}_{2^3})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Và tổng quát lên ta có

$$(\mathbb{Z}_{2^{r+1}})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{r-1}}$$

Với mọi $r \geq 1$.

Giả sử n là một số tự nhiên tùy ý, ta biểu diễn $n = p_1^{r_1} p_2^{r_2} ... p_s^{r_s}$, trong đó với mỗi i, p_i là một số nguyên tố thỏa mãn $2 \leq p_1 < p_2 < ... < p_s$ và $r_i \geq 1$. Khi đó những số p_i, r_i được xác định duy nhất bởi n.

Định lí 1.3. *Có duy nhất một đẳng cấu vành*

$$\Psi : \mathbb{Z}_n \cong \mathbb{Z}_{p_1}^{r_1} \times \mathbb{Z}_{p_2}^{r_2} \times ... \times \mathbb{Z}_{p_s}^{r_s}$$

Và một đẳng cấu nhóm

$$\Psi : (\mathbb{Z}_n)^\times \cong \left(\mathbb{Z}_{p_1}^{r_1}\right)^\times \times \left(\mathbb{Z}_{p_2}^{r_2}\right)^\times \times ... \times \left(\mathbb{Z}_{p_s}^{r_s}\right)^\times$$

Do đó ta có $\varphi(n) = \varphi\left(p_1^{r_1}\right) \varphi\left(p_2^{r_2}\right) ... \varphi\left(p_s^{r_s}\right)$.

Chứng minh : Giả sử a, b là hai số nguyên tố cùng nhau, trước hết ta sẽ chứng minh có một đẳng cấu vành:

$$\Psi : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$$

Theo định lý 1.2, $\exists u, v \in \mathbb{Z}$ sao cho $ua + vb = 1$.

Hiển nhiên $\gcd(a, u) = \gcd(b, v) = 1$

Xét tương ứng

$$\Psi : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$$