ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

TẠ VĂN TRUNG

CÁC HÀM SỐ HỌC VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - NĂM 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

TẠ VĂN TRUNG

CÁC HÀM SỐ HỌC VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số 60.46.01.13

Người hướng dẫn khoa học
PGS.TS. ĐÀM VĂN NHỈ

THÁI NGUYÊN - NĂM 2014

Mục lục

Lời mở đầu

Số học là một trong những lĩnh vực cổ xưa nhất của Toán học, và cũng là lĩnh vực tồn tại nhiều nhất những bài toán, những giả thuyết chưa có câu trả lời. Trên con đường tìm kiếm lời giải cho những giả thuyết đó, nhiều tư tưởng lớn, nhiều lí thuyết lớn của toán học đã nảy sinh. Hơn nữa trong những năm gần đây, Số học không chỉ là một lĩnh vực của toán học lí thuyết, mà còn là lĩnh vực có rất nhiều ứng dụng trực tiếp vào các vấn đề của đời sống như kinh tế, xã hội, kỹ thuật máy tính, đặc biệt trong lĩnh vực bảo mật thông tin. Chính vì thế, số học-một khoa học "ai cũng biết và nên biết chút ít". Mục đích của luận văn giới thiệu Các hàm số học và ứng dụng. Những ứng dụng của các hàm số học là rất nhiều, nhưng vì giới hạn trong phương pháp toán sơ cấp và hạn chế trong một luận văn thạc sĩ nên bản luận văn chỉ nêu ra một số ứng dụng cơ bản.

Bản luận văn gồm 2 chương:

Chương I: Lý thuyết chia hết trong vành $\mathbb{Z}$.

Nội dung của chương I trình bày về: Quan hệ chia hết, Phép chia với dư, Ước chung lớn nhất, Bội chung nhỏ nhất, Số nguyên tố và định lý cơ bản của số học, Biểu diễn số tự nhiên theo một cơ số.

Chương II: Các hàm số học và ứng dụng.

Phần đầu chương này trình bày về các hàm số học cơ bản. Phần cuối chương là vận dụng lý thuyết về các hàm số học vào giải một số bài toán.

Lời cảm ơn

Hoàn thành được luận văn này, ngoài sự nỗ lực của bản thân, tôi đã nhận được sự chỉ bảo, giúp đỡ của các thầy cô, gia đình và bạn bè.

Tôi xin bày tỏ lòng biết ơn sâu sắc nhất tới người thầy kính mến PGS.TS Đàm Văn Nhỉ, người đã trực tiếp truyền thụ kiến thức, quyết định hướng nghiên cứu và tận tình hướng dẫn cho tôi hoàn thành bản luận văn.

Tôi xin chân thành cảm ơn các thầy, cô giáo Khoa Toán, Trường Đại học Khoa học - Đại học Thái Nguyên, và các thầy cô tham gia giảng dạy khóa Cao học 2012-2014, những người đã trực tiếp giảng dạy và giúp đỡ tôi trong quá trình học tập tại trường cùng toàn thể bạn bè và người thân đã đóng góp ý kiến, giúp đỡ, động viên tôi trong quá trình học tập, nghiên cứu và hoàn thành luận văn này.

Số học là một lĩnh vực rộng lớn, nhưng vì giới hạn trong phương pháp toán sơ cấp và hạn chế trong một luận văn thạc sĩ nên bản luận văn mới chỉ trình bày được một phần nào đó. Do thời gian có hạn và năng lực có phần hạn chế nên chắc chắn luận văn không tránh khỏi những thiếu sót. Vì vậy, tôi mong nhận được những ý kiến đóng góp của các thầy cô và bạn bè đồng nghiệp để bản luận văn được hoàn chỉnh hơn.

Xin chân thành cảm ơn!

Thái Nguyên, ngày 19 tháng 04 năm 2014

Học viên

Tạ Văn Trung

Về ký hiệu:

$\mathbb{N}$ được ký hiệu cho tập các số tự nhiên.

$\mathbb{N}^*$ được ký hiệu cho tập các số tự nhiên dương.

$\mathbb{Z}$ được ký hiệu cho vành các số nguyên.

$\mathbb{Q}$ được ký hiệu cho trường các số hữu tỷ.

$\mathbb{Q}^*$ được ký hiệu cho tập các số hữu tỷ dương.

$\mathbb{R}$ được ký hiệu cho trường các số thực.

$\mathbb{C}$ được ký hiệu cho trường các số phức.

K được ký hiệu cho một trong ba trường $\mathbb{Q}, \mathbb{R}$ hoặc $\mathbb{C}$.

Chương 1

Lý thuyết chia hết trong vành $\mathbb{Z}$

Khái niệm nhóm, vành và trường không nhắc lại trong chuyên đề này. Tập $\mathbb{Z}$ là một miền nguyên, $\mathbb{Q}$ là một trường đặc số 0.

1.1 Quan hệ chia hết

Định nghĩa 1.1.1. Cho hai số nguyên $a, b \in \mathbb{Z}, b \neq 0$. Số a được gọi là *chia hết cho* số b hay b *chia hết* a nếu có $c \in \mathbb{Z}$ thỏa mãn $a = bc$.

Trong nhiều trường hợp, thay cho việc nói a chia hết cho b ta viết $a \vdots b$ hoặc nói b chia hết a và viết $b|a$. Khi $a = bc$ thì b được gọi là *một ước* của a. Các tính chất cơ bản sau đây về quan hệ chia hết là hiển nhiên.

(i) $1 \mid a$ với mọi $a \in \mathbb{Z}$.

(ii) $a \mid a$ với mọi $a \in \mathbb{Z}, a \neq 0$.

(iii) Nếu $a \mid b$ và $b \mid c$ thì $a \mid c$ với mọi $a, b, c \in \mathbb{Z}, a, b \neq 0$.

(iv) Nếu $a \mid b$ thì $|a| \leqslant |b|$ với mọi $a, b \in \mathbb{Z}, a, b \neq 0$.

(v) Nếu $a \mid b_i$ với $a, b_i \in \mathbb{Z}, i = 1, \ldots, n$, thì $a \mid \sum_{i=1}^{n} b_i x_i$ với $x_i \in \mathbb{Z}$.

(vi) Nếu $a \mid b$ và $b \mid a$ thì $a = b$ hoặc $a = -b$ với $a, b \in \mathbb{Z}, a, b \neq 0$.

Hiển nhiên, quan hệ chia hết trong $\mathbb{Z}$ có tính phản xạ, nhưng không có tính bắc cầu, chẳng hạn $0 \vdots 5$, nhưng $5 \not\vdots 0$ và không có tính phản đối

xứng, chẳng hạn $5 \mid -5, -5 \mid 5$, nhưng $5 \neq -5$. Do đó quan hệ chia hết không là quan hệ tương đương, cũng không là quan hệ thứ tự trong $\mathbb{Z}$.

1.2 Phép chia với dư

Định lý 1.2.1. Với mỗi cặp số nguyên $a, b \in \mathbb{Z}, b \neq 0$, luôn tồn tại duy nhất một cặp số nguyên $q, r \in \mathbb{Z}$ sao cho $a = qb + r$, với $0 \leqslant r < |b|$.

Chứng minh: Sự tồn tại: Đặt $T = \{n|b| \text{ sao cho } n|b| \leqslant a, n \in \mathbb{Z}\}$. Vì $|b| \geqslant 1$ nên $-|a||b| \leqslant -|a| \leqslant a$. Do đó $-|a||b| \in T$. Vậy $T \neq \emptyset$. Vì T là tập bị chặn trên nên T có một số lớn nhất $m|b|$. Từ $m|b| \leqslant a$ ta suy ra $r = a - m|b| \geqslant 0$ và $r \in \mathbb{Z}$. Ta lại có $(m+1)|b| = m|b| + |b| > m|b|$. Do tính lớn nhất của $m|b|$ trong T nên $(m+1)|b| > a$. Như vậy $|b| > a - m|b| = r$ và ta có $a = qb + r$ với $0 \leqslant r < |b|$.
Tính duy nhất: Giả sử có hai sự biểu diễn $a = qb + r$ với $0 \leqslant r < |b|$ và $a = q_1 b + r_1$ với $0 \leqslant r_1 < |b|$. Trừ vế cho vế, ta có $r - r_1 = b(q_1 - q)$. Từ $|r - r_1| < |b| \Rightarrow |q_1 - q||b| < |b|$. Vậy $q = q_1$ và hiển nhiên $r = r_1$. □

Biểu diễn $a = qb + r, 0 \leqslant r < |b|$. Nếu $r = 0$ thì q được gọi là *thương* của a chia cho b. Nếu $r \neq 0$ thì q gọi là *thương hụt,* còn r là *số dư* trong phép chia a cho b.

Ví dụ 1.2.2. Đặt $a_n = 1^{2011} + 2^{2011} + \cdots + n^{2011}$ với $n \in \mathbb{N}^*$. Chứng minh rằng a_n không chia hết cho $n + 2$.

Bài giải: Ta có

$$2a_n = [n^{2005} + 2^{2005}] + [(n-1)^{2005} + 3^{2005}] + \cdots + [2^{2005} + n^{2005}] + 2.$$

Vậy $2a_n = (n+2)d + 2, d \in \mathbb{N}^* \Rightarrow a_n$ không chia hết cho $n + 2$. □

Ví dụ 1.2.3. Giả sử x_1, x_2 là hai nghiệm của phương trình $x^2 - 38x + 1 = 0$. Đặt $a_n = x_1^n + x_2^n$ với $n = 0, 1, 2, \ldots$. Chứng minh rằng a_n là số nguyên và tìm dư của phép chia a_{1000} cho 19.

Bài giải: Có $a_0 = 1 + 1 = 2, a_1 = x_1 + x_2 = 38$. Vì $x_1^2 - 38x_1 + 1 = 0, x_2^2 - 38x_2 + 1 = 0$ nên $x_1^{n+2} - 38x_1^{n+1} + x_1^n = 0, x_2^{n+2} - 38x_2^{n+1} + x_2^n = 0$. Do đó $a_{n+2} = 38a_{n+1} - a_n$ với mọi $n \geqslant 0$. Bằng phương pháp quy nạp theo n ta suy ra a_n nguyên với mọi $n \geqslant 0$. Ta có $a_{n+2} + a_n \vdots 19$ với mọi số nguyên $n \geqslant 0$. Từ $a_{n+2} + a_n \vdots 19$ và $a_{n+4} + a_{n+2} \vdots 19$ suy ra $a_{n+4} - a_n \vdots 19$ với mọi $n \geqslant 0$ và nhận được bảng chia hết cho dưới đây:

$$\begin{aligned} a_4 - a_0 &\vdots 19 \\ a_8 - a_4 &\vdots 19 \\ a_{12} - a_8 &\vdots 19 \\ &\dots \\ a_{1000} - a_{996} &\vdots 19. \end{aligned}$$

Như vậy $a_{1000} - a_0 \vdots 19$ hay a_{1000} chia cho 19 dư 2. □

1.3 Ước chung lớn nhất

Định nghĩa 1.3.1. Cho các số nguyên $a_1, \dots, a_n \in \mathbb{Z}$ không đồng thời bằng 0. Số nguyên d được gọi là *ước chung* của các a_i nếu $d \mid a_i$ với mọi $i = 1, \dots, n$.

Hiển nhiên $+1, -1$ là ước chung của mọi tập hữu hạn các số nguyên. Ký hiệu tập tất cả các ước chung của $a_1, \cdots, a_n \in \mathbb{Z}$ là $\mathrm{C}(a_1, \cdots, a_n)$ và thấy ngay tập này khác rỗng. Ví dụ $\mathrm{C}(18, -15, 21) = \{1, -1, 3, -3\}$.

Định nghĩa 1.3.2. Cho các số nguyên $a_1, \dots, a_n \in \mathbb{Z}$ không đồng thời bằng 0. Số nguyên d được gọi là *ước chung lớn nhất* của các a_i nếu d là một ước chung của các a_i và d chia hết cho mọi ước chung của chúng.

Như vậy, số nguyên d là ước chung lớn nhất của $a_1, \dots, a_n \in \mathbb{Z}$ khi và chỉ khi $d \mid a_i, i = 1, \dots, n$, và nếu $c \mid a_i, i = 1, \dots, n$, thì $c \mid d$. Khi số nguyên d là ước chung lớn nhất của $a_1, \dots, a_n$ thì $-d$ cũng là ước chung lớn nhất của $a_1, \dots, a_n$. Người ta ký hiệu ước chung lớn nhất của $a_1, \dots, a_n$ qua $(a_1, \dots, a_n)$ và chọn nó là $|d|$. Dễ thấy rằng, $(a_1, \dots, a_n)$ là số nguyên dương lớn nhất nằm trong tập $\mathrm{C}(a_1, \dots, a_n)$.

Định lý 1.3.3. Cho các số nguyên $a_1, \ldots, a_n \in \mathbb{Z}$ không đồng thời bằng 0. Khi đó luôn tồn tại ước chung lớn nhất $(a_1, \ldots, a_n)$.

Chứng minh: Đặt $I = \{y = \sum_{j=1}^{n} a_j x_j \mid x_j \in \mathbb{Z}, j = 1, \ldots, n\}$. Dễ dàng chỉ ra I là một iđêan của vành $\mathbb{Z}$. Từ $a_i = 1.a_i + \sum_{i \neq j=1}^{n} 0.a_j$ ta suy ra các a_i đều thuộc I. Vậy $I \neq \{0\}$. Nếu $y \in I$ thì $-y \in I$. Vậy có số dương thuộc I. Gọi d là số nguyên dương nhỏ nhất thuộc I. Ta chỉ ra $d = (a_1, \ldots, a_n)$. Trước tiên ta chỉ ra $d \in \mathrm{C}(a_1, \ldots, a_n)$: Giả sử $a_i = q_i d + r_i, 0 \leqslant r_i < d$ theo Định lý 1.2.1. Ta có biểu diễn $d = \sum_{j=1}^{n} a_j x_j, x_j \in \mathbb{Z}$ do $d \in I$ và từ $r_i = a_i - q_i d = a_1(-q_i x_1) + \cdots + a_i(1 - q_i x_i) + \cdots + a_n(-q_i x_n) \in I$ suy ra $r_i \in I$ với mọi $i = 1, \ldots, n$. Bởi vì d là số nguyên dương nhỏ nhất thuộc I và các $r_i \in I, 0 \leqslant r_i < d$, nên $r_1 = \cdots = r_n = 0$.
Tiếp theo, nếu $c \in \mathrm{C}(a_1, \ldots, a_n)$ thì $c|d$. Thật vậy, nếu $c \in \mathrm{C}(a_1, \ldots, a_n)$ thì có $b_j \in \mathbb{Z}$ để $a_j = b_j c$ với $j = 1, \ldots, n$. Do vậy $d = \sum_{j=1}^{n} a_j x_j = c(\sum_{j=1}^{n} b_j x_j)$ hay $c|d$. Tóm lại $d = (a_1, \ldots, a_n)$. □

Thuật toán Euclid để tìm ước chung lớn nhất

Bây giờ chúng ta sẽ sử dụng Định lý 1.2.1 để tìm ước chung lớn nhất của một số số nguyên không đồng thời bằng 0, nhưng thực ra chỉ cần cho hai số.
Để tìm ước chung lớn nhất của $a, b \in \mathbb{Z}, b \neq 0$, ta sẽ sử dụng Định lý 1.2.1 vào việc xây dựng lại Thuật toán Euclid như sau: Biểu diễn $a = q_0 b + r$ với $0 \leqslant r < |b|$. Nếu $r = 0$ thì $(a, b) = b$. Nếu $r \neq 0$, ta biểu diễn $b = q_1 r + r_1$ với $0 \leqslant r_1 < r$. Nếu $r_1 = 0$ thì ta dừng lại và ta có $r = (b, r) = (a, b)$ theo tính chất (vii). Nếu $r_1 \neq 0$, ta tiếp tục như trên. Đến bước thứ n ta có $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$ với $0 \leqslant r_{n-1} < r_{n-2}, \ldots$ Sau mỗi bước ta có $|b| > r > r_1 > \cdots \geqslant 0$ và các $r_i \in \mathbb{N}$. Như vậy quá trình trên không thể tiếp tục mãi được. Đến bước thứ m xác định nào đó quá trình trên phải