ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THÚY HẰNG

HÀM SINH BỞI CÁC ƯỚC SỐ VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN, NĂM 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THÚY HẰNG

HÀM SINH BỞI CÁC ƯỚC SỐ VÀ ỨNG DỤNG

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số: 60.46.01.13

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học:
PGS.TS NÔNG QUỐC CHINH

THÁI NGUYÊN, NĂM 2015

Mục lục

Mở đầu

Trong toán học và đặc biệt là trong lý thuyết số, hàm sinh bởi các ước số là một hàm số học liên quan đến tính toán các ước của một số nguyên. Hàm này gắn với phép đếm số các ước số của một số nguyên và các dạng toán liên quan đến biểu diễn các ước số. Các kết quả này gắn với các nghiên cứu gần đây của nhà toán học Ấn Độ Ramanujan.

Luận văn này nhằm mục đích tìm hiểu chi tiết các tính chất của hàm sinh bởi các ước số và xét các ứng dụng của nó trong việc giải các bài toán liên quan trong số học.

Ngoài phần Mở đầu và Kết luận, luận văn được chia thành ba chương đề cập đến các vấn đề sau đây:

Chương 1 trình bày về ước số và các tính chất liên quan.

Chương 2 trình bày các giá trị trung bình của hàm sinh bởi các ước số.

Chương 3 trình bày một số bài toán ứng dụng trong số học.

Tôi xin bày tỏ lòng biết ơn sâu sắc đối với Phó Giáo sư, Tiến sĩ Nông Quốc Chinh, người thầy đã trực tiếp hướng dẫn, cung cấp tài liệu và truyền đạt những kinh nghiệm nghiên cứu cho tôi.

Tôi xin chân thành cảm ơn các thầy, cô giáo trong khoa Toán - Tin, phòng Đào tạo trường Đại học Khoa học - Đại học Thái Nguyên, Trường THPT Hòn Gai và bạn bè đồng nghiệp đã giúp đỡ tạo điều kiện cho tôi hoàn thành bản luận văn này.

Chương 1

Hàm đếm các ước số $d(n)$

1.1 Một số kiến thức cơ bản của số học

1.1.1 Phép chia trong tập số nguyên

Định nghĩa 1.1. Cho hai số nguyên a và b , với $b \neq 0$. Nếu có một số nguyên q sao cho $a = bq$ thì ta nói rằng b chia hết a hay a chia hết cho b hoặc b là ước của a và ký hiệu là $b \mid a$ hay $a \vdots b$.

Tính chất 1.1.

1. $\pm 1 \mid a$ với $a \in \mathbb{Z}$.
2. $0 \vdots a$ với $a \in \mathbb{Z}$, $a \neq 0$.
3. $a \vdots a$ với $a \in \mathbb{Z}$, $a \neq 0$.
4. $b \mid a$ và $a \mid b$ khi và chỉ khi $a = \pm b$.
5. $b \mid a$ và $c \mid b$ kéo theo $c \mid a$.
6. Với mọi $i \in \{1; 2; \ldots; n\}$, $\forall x_i \in \mathbb{Z}$, $b \mid a$ kéo theo $b \mid \sum\limits_{i=0}^{n} a_i x_j$.

Định lý 1.1. (Định lý chia Euclid). Với các số nguyên a và b, $b \neq 0$, tồn tại duy nhất các số nguyên q, r sao cho

$$a = bq + r; 0 \leq r < |b|. \tag{1.1}$$

Chứng minh.

a) Sự tồn tại: Gọi M là tập hợp các bội của số b không vượt quá a:

$M = \{bx \mid x \in \mathbb{Z}, bx \leq a\}$.
Ta có $M \subset \mathbb{Z}$ và $M \neq \varnothing$ vì chẳng hạn $-|b|.|a| \in M$.
M bị chặn trên, vậy nó có số lớn nhất, ta gọi đó là bq. Số nguyên $bq + |b|$ là một bội của b và $bq + |b| \notin M$, do đó ta có $bq \leq a < bq + |b|$, từ đó suy ra $0 \leq a - bq < |b|$.
Đặt $r = a - bq$ ta được $a = bq + r$, $0 \leq a - bq < |b|$.

b) Tính duy nhất: Giả sử có q, r và q_1, r_1 thỏa mãn các điều kiện trên, tức là

$$\begin{aligned} a &= bq + r, \qquad 0 \leq r < |b|, \\ a &= bq_1 + r_1, \qquad 0 \leq r_1 < |b|, \end{aligned}$$

Khi đó ta được

$$bq + r = bq_1 + r_1 \Rightarrow r - r_1 \leq b(q - q_1).$$

Nhưng $|r - r_1| < |b|$, cho nên $|b||q - q_1| < |b|$, nghĩa là $|q - q_1| < 1$. Hệ thức này buộc $q - q_1 = 0$ nghĩa là $q = q_1$, từ đó suy ra $r = r_1$(điều phải chứng minh).

1.1.2 Ước số chung lớn nhất (ƯSCLN)

Định nghĩa 1.2. Cho hai số nguyên a, b trong đó ít nhất một số khác 0. Số dương d được gọi là ƯSCLN của a, b và được ký hiệu là $d := (a, b)$ nếu

1. $d \mid a$ và $d \mid b$ (d là ước số chung của a và b).
2. Nếu $c \mid a$ và $c \mid b$ thì $c \mid d$.
   Nói cách khác, d là ƯSCLN của hai số a và b nếu d là ước chung của a và b đồng thời d là số lớn nhất trong các ước số chung của a và b. Nếu $(a, b) = 1$ thì ta nói hai số a và b nguyên tố cùng nhau.

Nhận xét 1.1. Trong trường hợp a, b có một số bằng 0 thì hiển nhiên ƯSCLN của chúng chính là số kia.

Tính chất 1.2.

1. $(ac, bc) = (a, b).c$ với $c \neq 0$.
2. $\left(\dfrac{a}{c}; \dfrac{b}{c}\right) = \dfrac{(a, b)}{c}$ với c là một ước chung của a,b.
3. Nếu $(a, b) = 1$ thì $(ac, b) = (c, b)$.
4. Nếu $(a, b) = 1$ và $b \vdots ac$ thì $b \vdots c$.
5. $(b, a_1) = (b, a_2) = 1 \Rightarrow (b, a_1a_2) = 1$.
6. Nếu $a \vdots c_1$, $a \vdots c_2$ mà $(c_1, c_2) = 1$ thì $a \vdots c_1c_2$.

Thuật toán tìm ƯSCLN của hai số nguyên

Chú ý 1.1. *Nếu giữa các số nguyên a, b, q, r có hệ thức $a = bq + r$ thì ta có*

$$(a, b) = (b, r).$$

a) Cho $a, b \in \mathbb{Z}$. Nếu một trong hai số là ước của số kia, chẳng hạn $b \mid a$ thì hiển nhiên.

b) Nếu không xảy ra trường hợp trên thì ta có các hệ thức sau biểu thị một dãy các phép chia có dư:

$$\begin{aligned}
&a = bq_0 + r_1, && 0 < r_1 < |b| \\
&b = r_1q_1, && 0 < r_2 < r_1 \\
&r_1 = r_2q_2 + r_3, && 0 < r_3 < r_2 \\
&\dots \qquad \dots && \\
&r_{n-2} = r_{n-1}q_{n-1} + r_n, && 0 < r_n < r_{n-1} \\
&r_{n-1} = r_nq_n. &&
\end{aligned}$$

Dãy phép chia có dư liên tiếp này được gọi là thuật toán Euclid thực hiện trên hai số a, b. Dãy này phải là dãy hữu hạn và thuật toán Euclid phải kết thúc với một số dư $r_{n+1} = 0$.

Theo chú ý ta có

$$(a, b) = (b, r_1) = \ldots = (r_{n-1}, r_n) = r_n.$$

Như vậy, ƯSCLN của hai số a, b là số dư cuối cùng khác 0 trong thuật toán Euclid thực hiện trên hai số a, b.

1.1.3 Số nguyên tố

Định nghĩa 1.3. Số nguyên tố là một số tự nhiên lớn hơn 1 và không có ước nào khác ngoài 1 và chính nó.

Định lý 1.2. Ước nhỏ nhất khác 1 của một số tự nhiên lớn hơn 1 là một số nguyên tố.

Định lý 1.3. Cho a là một số tự nhiên và p là một số nguyên tố, thế thì hoặc a nguyên tố cùng nhau với p, hoặc a chia hết cho p.

Định lý 1.4. Nếu số nguyên tố p là ước của một tích nhiều số thì nó phải là ước của ít nhất một trong các thừa số đó.

Định lý 1.5. Nếu một số nguyên tố p là ước của một tích nhiều số nguyên tố thì p phải trùng với một trong các số nguyên tố đó.

Định lý 1.6. (Về phân tích chính tắc của một số tự nhiên). Mọi số tự nhiên lớn hơn 1 đều phân tích được thành một tích các thừa số nguyên tố và sự phân tích đó là duy nhất (không kể thứ tự các thừa số).

Chú ý 1.2. Nói chung, một thừa số nguyên tố trong phân tích có thể lặp lại, bởi vậy để cho gọn, các thừa số lặp lại được viết dưới dạng lũy thừa:

$$a = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_k^{\alpha_k}. \tag{1.2}$$

Trong đó $p_i \neq p_j$, $\forall i \neq j$, còn $\alpha_i \in \mathbb{N}, \alpha_i \geq 1, 1 \leq i \leq k$. Và (1.2) được gọi là phân tích tiêu chuẩn của số tự nhiên a.

1.2 Hàm đếm các ước

Định nghĩa 1.4. Hàm số học là hàm số có miền xác định là tập các số nguyên dương và miền giá trị là tập các số phức.

Ví dụ 1.1.

a) Hàm $d(n)$ đếm các ước khác nhau của một số tự nhiên $n \geq 1$ là hàm số học.

b) Hàm phi-Euler $\varphi(n)$ là hàm số học.

c) Hàm $\delta : \mathbb{Z}^+ \to \mathbb{C}, \delta(n) = \begin{cases} 1 & \text{nếu } n = 1 \\ 0 & \text{nếu } n \geq 2 \end{cases}$ là hàm số học.

d) Hàm $O : \mathbb{Z}^+ \to \mathbb{C}$, $O(n) = 0$ là hàm số học.

Định nghĩa 1.5. Một hàm số học f được gọi là *hàm nhân tính* nếu với mọi cặp số m, n nguyên tố cùng nhau, ta có $f(n.m) = f(n).f(m)$. Trong từng trường hợp đẳng thức đúng với mọi m, n (không nhất thiết nguyên tố cùng nhau) hàm f gọi là hàm nhân tính mạnh.

Ví dụ 1.2. Ta có

$$\mu(1) = 1, \quad \mu(6) = 1, \quad \mu(2) = -1, \quad \mu(7) = -1, \quad \mu(3) = -1$$
$$\mu(8) = 0, \quad \mu(4) = 0, \quad \mu(9) = 0, \quad \mu(5) = -1, \quad \mu(10) = 1$$

Định nghĩa 1.6. Hàm số học xác định số các ước dương của một số nguyên dương n được gọi là hàm đếm các ước và kí hiệu là $d(n)$.

Như vậy

$d(1) = 1 \qquad d(6) = 4,$
$d(2) = 2 \qquad d(7) = 2,$
$d(3) = 2 \qquad d(8) = 4,$
$d(4) = 3 \qquad d(9) = 3.$

Giả sử

$$n = \prod_{p|n} p^{\nu_p(n)}.$$

Mọi ước của n có dạng:

$$d = \prod_{p|n} p^{a_p},$$

với a_p là số nguyên thỏa mãn:

$$0 \leq a_p \leq \nu_p(n).$$

Vì mỗi số mũ a_p có thể nhận $v_p(n)+1$ giá trịn khác nhau nên ta có

$$d(n) = \prod_{p|n} (\nu_p(n)+1).$$

Định lý 1.7. Hàm $d(n)$ là hàm nhân tính.

Chứng minh.

Cho m và n là hai số nguyên tố cùng nhau,

$$m = \prod_{p|m} p^{\nu_p}(m),$$

và

$$n = \prod_{q|n} q^{\nu_q}(n).$$

Vì $(m,n)=1$ nên tập hợp các số nguyên tố là ước của m và tập hợp các số nguyên tố là ước của n là rời nhau. Vì vậy

$$mn = \prod_{p|m} p^{\nu_p}(m) \prod_{q|n} q^{\nu_q}(n)$$

là sự phân tích thành nhân tử của mn, và

$$d(mn) = \prod_{p|m} (\nu_p(m)+1) \prod_{q|n} (\nu_q(n)+1) = d(m)d(n).$$

Vậy định lý đã được chứng minh.

Ví dụ 1.3. Tính $d(n)$ với $11 \leq n \leq 20$.

Lời giải.

$$\begin{aligned}
d(11) &= d(11^1) = 1+1 = 2 \\
d(12) &= d(2^2.3^1) = (2+1)(1+1) = 6 \\
d(13) &= d(13^1) = 1+1 = 2 \\
d(14) &= d(2^1.7^1) = (1+1)(1+1) = 4 \\
d(15) &= d(3^1.3^1) = (1+1)(1+1) = 4 \\
d(16) &= d(2^4) = 4+1 = 5
\end{aligned}$$