

**Đại Học Thái Nguyên
Trường Đại Học Khoa Học**

Đỗ Cao Sơn

CÁC HÀM SỐ HỌC VÀ ỨNG DỤNG

**Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
MÃ SỐ: 60.46.40**

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học: GS.TSKH. HÀ HUY KHOÁI

Thái Nguyên - 2011

**Công trình được hoàn thành tại
Trường Đại Học Khoa Học - Đại Học Thái Nguyên**

Người hướng dẫn khoa học: GS.TSKH. HÀ HUY KHOÁI

Phản biện 1: PGS.TS. Lê Thị Thanh Nhàn

Phản biện 2: TS. Nguyễn Văn Ngọc

**Luận văn được bảo vệ trước hội đồng chấm luận văn họp tại:
Trường Đại Học Khoa Học - Đại Học Thái Nguyên
*Ngày 09 tháng 09 năm 2011***

**Có thể tìm hiểu tại
Thư Viện Đại Học Thái Nguyên**

Mục lục

Mục lục	1
Mở đầu	3
1 Các hàm số học cơ bản	5
1.1. Phi - hàm Ô-le	5
1.1.1. Định nghĩa	5
1.1.2. Các tính chất	6
1.2. Hàm tổng các ước số dương của n	9
1.2.1. Định nghĩa	9
1.2.2. Các tính chất	10
1.3. Hàm tổng các chữ số của số tự nhiên n	12
1.3.1. Định nghĩa	12
1.3.2. Các tính chất	12
1.4. Hàm số các ước $\tau(n)$	15
1.4.1. Định nghĩa	15
1.4.2. Các tính chất	15
1.5. Hàm phần nguyên $[x]$	16
1.5.1. Định nghĩa	16
1.5.2. Các tính chất	16
2 Một số ứng dụng của các hàm số học	18
2.1. Ứng dụng của Phi - hàm Ô-le	18
2.1.1. Xét đồng dư môđulô của một số nguyên tố	18
2.1.2. Chứng minh phép chia với dư	19
2.1.3. Giải phương trình đồng dư	20
2.1.4. Tìm nghiệm nguyên của phương trình	21

2.1.5.	Tìm cấp của số nguyên	22
2.1.6.	Tìm số tự nhiên thỏa mãn tính chất hàm số $\varphi(n)$	23
2.2.	Ứng dụng của hàm tổng các ước số dương của số tự nhiên n	24
2.2.1.	Chứng minh một số là hợp số	24
2.2.2.	Chứng minh một số là số hoàn hảo	25
2.2.3.	Chứng minh bất đẳng thức liên quan tới $\sigma(n)$. .	29
2.3.	Ứng dụng của hàm $S(n)$	32
2.3.1.	Tìm n bởi $S(n)$ thỏa mãn một hệ thức cho trước .	32
2.3.2.	Tính giá trị $S(n)$	35
2.3.3.	Chứng minh một số biểu thức liên quan tới $S(n)$.	37
2.3.4.	Xét tính bị chặn của hàm số chứa $S(n)$	39
2.4.	Ứng dụng của hàm số các ước $\tau(n)$	40
2.4.1.	Tìm n thỏa mãn một điều kiện cho trước của $\tau(n)$	40
2.4.2.	Một số bất đẳng thức liên quan tới hàm $\tau(n)$. .	43
2.4.3.	Tìm số nghiệm của phương trình bằng phương pháp sử dụng $\tau(n)$	45
2.5.	Ứng dụng của hàm phần nguyên $[x]$	46
2.5.1.	Bài toán định tính	46
2.5.2.	Bài toán định lượng	50
Kết luận		54
Tài liệu tham khảo		55

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, có 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 nhiều ứng dụng, đặc biệt trong lĩnh vực bảo mật thông tin. Vì thế, việc trang bị những kiến thức cơ bản về số học ngay từ trường phổ thông là hết sức cần thiết. Không như nhiều ngành khác của toán học, có rất nhiều thành tựu hiện đại và quan trọng của Số học có thể hiểu được chỉ với những kiến thức phổ thông được nâng cao một bước. Do đó, đây chính là lĩnh vực thuận lợi để đưa học sinh tiếp cận nhanh với khoa học hiện đại. Tuy nhiên, trong chương trình Số học ở trường phổ thông hiện nay, môn Số học chưa được giành nhiều thời gian. Cũng vì thế mà học sinh thường rất lúng túng khi giải bài toán Số học, đặc biệt là trong các kì thi chọn học sinh giỏi.

Trong phần Số học, các hàm số học đóng vai trò quan trọng trong việc hình thành và nghiên cứu lí thuyết để hoàn thiện. Đây là một vấn đề cổ điển và quan trọng của Số học. Các bài tập ứng dụng các hàm số học cơ bản được đề cập nhiều trong các kì thi chọn học sinh giỏi cấp tỉnh (thành phố), Quốc gia, Quốc tế.

Mục đích chính của luận văn là nêu ra được một số ứng dụng cơ bản của các hàm số học cơ bản (Phi-hàm Ô-le, hàm tổng các ước dương của n , số các ước dương của n , tổng các chữ số của số tự nhiên n , hàm phần nguyên). Cụ thể là phân loại được các dạng bài tập của các hàm số học thông qua hệ thống bài tập sử dụng các hàm số học và các định lí cơ

bản của Số học.

Nội dung của luận văn gồm 2 chương

Chương 1: Trình bày các kiến thức cơ bản của các hàm số học.

Chương 2: Một số ứng dụng của các hàm số học.

Luận văn này được hoàn thành với sự hướng dẫn và chỉ bảo tận tình của GS.TSKH. Hà Huy Khoái - Viện Toán Học Hà Nội. Thầy đã dành nhiều thời gian hướng dẫn và giải đáp các thắc mắc của tôi trong suốt quá trình làm luận văn. Tôi xin được bày tỏ lòng biết ơn sâu sắc đến Thầy.

Tôi xin cảm ơn tới Sở Nội Vụ, Sở Giáo dục và Đào tạo tỉnh Bắc Ninh, trường THPT Thuận Thành 1, tổ Toán trường THPT Thuận Thành 1 đã tạo điều kiện giúp đỡ tôi hoàn thành khóa học này.

Tôi xin gửi tới các Thầy Cô khoa Toán, phòng Đào tạo sau Đại học Trường Đại Học Khoa Học - Đại Học Thái Nguyên, cũng như các Thầy cô tham gia giảng dạy khóa Cao học 2009-2011 lời cảm ơn sâu sắc về công lao dạy dỗ trong suốt quá trình giáo dục, đào tạo của nhà trường. Đồng thời tôi xin gửi lời cảm ơn tới tập thể lớp Cao Học Toán K3A Trường Đại Học Khoa Học đã đồng viên giúp đỡ tôi trong quá trình học tập và làm luận văn này.

Tuy nhiên do sự hiểu biết của bản thân và khuôn khổ của luận văn thạc sĩ, nên chắc rằng trong quá trình nghiên cứu không tránh khỏi những thiếu sót, tôi rất mong được sự đóng góp ý kiến của các Thầy Cô và độc giả quan tâm tới luận văn này.

Thái Nguyên, ngày 31 tháng 07 năm 2011

Tác giả

Đỗ Cao Sơn

Chương 1

Các hàm số học cơ bản

1.1. Phi - hàm Ô-le

1.1.1. Định nghĩa

Định nghĩa 1.1. Giả sử n là một số nguyên dương. Phi-hàm Ô-le của n là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n .

Kí hiệu Phi-hàm Ô-le là $\varphi(n)$.

Ví dụ 1.1. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$.

Định nghĩa 1.2. Cho n là số nguyên dương. Nếu a là số nguyên với $(a, n) = 1$ thì luôn tồn tại số nguyên dương k để $a^k \equiv 1 \pmod{n}$. Số nguyên dương k bé nhất thỏa mãn $a^k \equiv 1 \pmod{n}$ được gọi là cấp của số nguyên $a \pmod{n}$.

Định nghĩa 1.3. Một hệ thặng dư thu gọn môđulô n là một tập hợp gồm $\varphi(n)$ số nguyên sao cho mỗi phần tử của tập hợp đều nguyên tố cùng nhau với n và không có hai phần tử khác nhau nào đồng dư môđulô n .

Ví dụ 1.2. Tập hợp $\{1, 3, 5, 7\}$ là một hệ thặng dư thu gọn môđulô 8. Tập hợp $\{-3, -1, 1, 3\}$ cũng vậy.

Định nghĩa 1.4. Một tập hợp A nào đó được gọi là một hệ thặng dư đầy đủ $\pmod{n}$ nếu với bất kỳ số $x \in \mathbb{Z}$ tồn tại một $a \in A$ để $x \equiv a \pmod{n}$.

Ví dụ 1.3. $A = \{0, 1, 2, \dots, n-1\}$ là một hệ thặng dư đầy đủ theo môđulô n .

Chú ý 1.1. Dễ thấy một tập $A = \{a_1, a_2, \dots, a_n\}$ gồm n số sẽ là một hệ thặng dư đầy đủ theo môđulô n khi và chỉ khi $a_i \not\equiv a_j \pmod{n}$ (ta kí hiệu "không đồng dư" là $\not\equiv$) với $i \neq j$ và $i, j \in \{1, 2, \dots, n\}$.

1.1.2. Các tính chất

Tính chất 1. Giả sử $\{r_1, r_2, \dots, r_{\varphi(n)}\}$ là một hệ thặng dư thu gọn môđulô n , a là số nguyên dương và $(a, n) = 1$. Khi đó, tập hợp $\{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$ cũng là hệ thặng dư thu gọn môđulô n .

Chứng minh. Trước tiên ta chứng tỏ rằng, mỗi số nguyên ar_j là nguyên tố cùng nhau với n . Giả sử ngược lại, $(ar_j, n) > 1$ với j nào đó. Khi đó tồn tại ước nguyên tố p của (ar_j, n) . Do đó, hoặc $p|a$, hoặc $p|r_j$, tức là hoặc $p|a$ và $p|n$, hoặc $p|r_j$ và $p|n$. Tuy nhiên, không thể có $p|r_j$ và $p|n$ vì r_j và n là nguyên tố cùng nhau. Tương tự, không thể có $p|a$ và $p|n$. Vậy, ar_j và n nguyên tố cùng nhau với mọi $j = 1, 2, \dots, \varphi(n)$.

Còn phải chứng tỏ hai số ar_j, ar_k ($j \neq k$) tùy ý không đồng dư môđulô n . Giả sử $ar_j \equiv ar_k \pmod{n}$, $j \neq k$ và $1 \leq j \leq \varphi(n)$; $1 \leq k \leq \varphi(n)$. Vì $(a, n) = 1$ nên ta suy ra $r_j \equiv r_k \pmod{n}$. Điều này mâu thuẫn vì r_j, r_k cùng thuộc một hệ thặng dư thu gọn ban đầu môđulô n .

Ví dụ 1.4. Tập hợp $\{1, 3, 5, 7\}$ là một hệ thặng dư thu gọn môđulô 8. Do $(3, 8) = 1$ nên $\{3, 9, 15, 21\}$ cũng là một hệ thặng dư môđulô 8.

Tính chất 2. (Định lý Ô-le) Giả sử m là số nguyên dương và a là số nguyên với $(a, m) = 1$. Khi đó $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Chứng minh. Giả sử $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ là một hệ thặng dư thu gọn gồm các số nguyên dương không vượt quá m và nguyên tố cùng nhau với m . Do Tính chất 1 và do $(a, m) = 1$, tập hợp $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ cũng là một hệ thặng dư thu gọn môđulô m . Như vậy, các thặng dư dương bé nhất của $ar_1, ar_2, \dots, ar_{\varphi(m)}$ phải là các số nguyên $r_1, r_2, \dots, r_{\varphi(m)}$ xếp theo thứ tự nào đó. Vì thế, nếu ta nhân các vế từ trong hệ thặng dư thu gọn trên đây, ta được: $ar_1.ar_2...ar_{\varphi(m)} \equiv r_1.r_2...r_{\varphi(m)} \pmod{m}$.

Do đó, $a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod{m}$.

Vì $(r_1, r_2, \dots, r_{\varphi(m)}, m) = 1$ nên $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Ta có thể tìm nghịch đảo môđul n bằng cách sử dụng Định lý Ô-le. Giả sử a, m là các số nguyên tố cùng nhau, khi đó:

$$a \cdot a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Vậy $a^{\varphi(m)-1}$ là nghịch đảo của a môđul m .

Ví dụ 1.5. $2^{\varphi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod{9}$ là một nghịch đảo của 2 môđul 9.

Hệ quả 1.1. $(a, b) = 1$ thì $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

Hệ quả 1.2. Với $(a, b) = 1$ và n, v là hai số nguyên dương nào đó thì

$$a^{n\varphi(b)} + b^{v\varphi(a)} \equiv 1 \pmod{ab}.$$

Hệ quả 1.3. Giả sử có k ($k \geq 2$) số nguyên dương $m_1, m_2, \dots, m_k$ và chúng nguyên tố với nhau từng đôi một. Đặt $M = m_1 \cdot m_2 \dots m_k = m_i \cdot t_i$ với $i = 1, 2, \dots, k$ ta có:

$$t_1^n + t_2^n + \dots + t_k^n \equiv (t_1 + t_2 + \dots + t_k)^n \pmod{M} \text{ với } n \text{ nguyên dương.}$$

Bây giờ ta sẽ cho công thức tính giá trị của phi-hàm Ô-le tại n khi biết phân tích của n ra thừa số nguyên tố.

Tính chất 3. Với số nguyên tố p ta có $\varphi(p) = p - 1$. Ngược lại, nếu p là số nguyên dương sao cho $\varphi(p) = p - 1$ thì p là số nguyên tố.

Chứng minh. Nếu p là số nguyên tố thì với mọi số nguyên dương nhỏ hơn p đều nguyên tố cùng nhau với p . Do có $p - 1$ số nguyên dương như vậy nên $\varphi(p) = p - 1$.

Ngược lại, nếu p là hợp số thì p có các ước $d, 1 < d < p$. Tất nhiên p và d không nguyên tố cùng nhau. Như vậy, trong các số $1, 2, \dots, p - 1$ phải có những số không nguyên tố cùng nhau với p , nên $\varphi(p) \leq p - 2$. Theo giả thiết, $\varphi(p) = p - 1$. Vậy p là số nguyên tố.

Tính chất 4. Giả sử p là số nguyên tố và a là số nguyên dương. Khi đó:

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

Chứng minh. Các số nguyên dương nhỏ hơn p^a không nguyên tố cùng nhau với p là các số không vượt quá p^{a-1} và chia hết cho p . Có đúng p^{a-1} số như vậy. Do đó tồn tại $p^a - p^{a-1}$ số nguyên nhỏ hơn p^a và nguyên tố cùng nhau với p^a . Vậy, $\varphi(p^a) = p^a - p^{a-1}$.

Ví dụ 1.6. $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$; $\varphi(2^{10}) = 2^{10} - 2^9 = 512$.

Tính chất 5. Nếu m, n là các số nguyên dương nguyên tố cùng nhau thì $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Chứng minh. Ta viết các số nguyên dương không vượt quá mn thành bảng sau:

1	$m + 1$	$2m + 1$	...	$(n - 1)m + 1$
2	$m + 2$	$2m + 2$	...	$(n - 1)m + 2$
3	$m + 3$	$2m + 3$	...	$(n - 1)m + 3$
...	...	...	...	...
m	$2m$	$3m$	...	mn

Bây giờ giả sử r là một số nguyên không vượt quá m . Giả sử $(m, r) = d > 1$. Khi đó, không có số nào trong dòng thứ r nguyên tố cùng nhau với mn , vì mỗi phần tử của dòng đó đều có dạng $km + r$, trong đó $1 \leq k \leq n - 1$, $d \mid (km + r)$, vì $d \mid m, d \mid r$.

Vậy, để tìm các số trong bảng mà nguyên tố cùng nhau với mn , ta chỉ cần xem các dòng thứ r với $(m, r) = 1$. Ta xét một dòng như vậy, nó chứa các số $r, m + r, \dots, (n - 1)m + r$. Vì $(r, m) = 1$ nên mỗi số nguyên trong dòng đều nguyên tố cùng nhau với n . Như vậy, n số nguyên trong dòng lập thành hệ thặng dư đầy đủ môđulô n . Do đó có đúng $\varphi(n)$ số trong hàng đó nguyên tố cùng nhau với n . Do các số đó cũng nguyên tố cùng nhau với m nên chúng nguyên tố cùng nhau với mn .

Vì có $\varphi(m)$ dòng, mỗi dòng chứa $\varphi(n)$ số nguyên tố cùng nhau với mn nên ta suy ra $\varphi(mn) = \varphi(m)\varphi(n)$.

Kết hợp hai tính chất trên, ta được tính chất sau:

Tính chất 6. Giả sử $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ là phân tích n ra thừa số nguyên tố. Khi đó:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Chứng minh. Vì φ là hàm có tính chất nhân nên nếu n có phân tích như trên, ta được: $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\dots\varphi(p_k^{a_k})$.

Mặt khác: $\varphi(p_j^{a_j}) = p_j^{a_j} - p_j^{a_j-1} = p_j^{a_j} \left(1 - \frac{1}{p_j}\right), j = 1, 2, \dots, k$.

Vậy

$$\begin{aligned}\varphi(n) &= p_1^{a_1} \left(1 - \frac{1}{p_1}\right) p_2^{a_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{a_k} \left(1 - \frac{1}{p_k}\right) \\ &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

Tính chất 7. Giả sử n là một số nguyên dương. Khi đó:

$$\sum_{d|n} \varphi(d) = n.$$

Chứng minh. Tổng trên đây được lấy theo các ước số của n . Ta phân chia tập hợp các số tự nhiên từ 1 đến n thành các lớp sau đây. Lớp C_d gồm các số nguyên $m, 1 \leq m \leq n$, mà $(m, n) = d$. Như vậy m thuộc C_d nếu và chỉ nếu d là ước chung của m, n và $(m/d, n/d) = 1$. Như vậy, số phần tử của C_d là các số nguyên dương không vượt quá n/d và nguyên tố cùng nhau với n/d ; tức là C_d gồm $\varphi(n/d)$ phần tử. Vì mỗi số nguyên m từ 1 đến n thuộc một và chỉ một lớp C_d nào đó ($d = (m, n)$) nên n bằng tổng của số các thành phần trong các lớp C_d, d là ước số của n . Ta có $n = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$.

1.2. Hàm tổng các ước số dương của n

1.2.1. Định nghĩa

Định nghĩa 1.1. Hàm tổng các ước dương của số tự nhiên n được kí hiệu là $\sigma(n)$.

Ví dụ 1.7. $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$.

Chú ý 1.2. Ta có thể biểu diễn hàm $\sigma(n)$ dưới dạng: $\sigma(n) = \sum_{d|n} d$

1.2.2. Các tính chất

Bổ đề 1.1. Giả sử m, n là các số nguyên dương nguyên tố cùng nhau. Khi đó, nếu d là ước chung của mn thì tồn tại cặp duy nhất các ước dương d_1 của m và d_2 của n sao cho $d = d_1.d_2$. Ngược lại, nếu d_1 và d_2 là các ước dương tương ứng của m và n thì $d = d_1.d_2$ là ước dương của mn .

Chứng minh. Giả sử m, n có phân tích ra thừa số nguyên tố như sau:

$$m = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} ; \quad n = q_1^{n_1} q_2^{n_2} \dots q_t^{n_t}.$$

Vì $(m, n) = 1$ nên tập hợp số nguyên tố $p_1, p_2, \dots, p_s$ và tập hợp các số nguyên tố $q_1, q_2, \dots, q_t$ không có phần tử chung. Do đó phân tích ra thừa số của mn có dạng: $mn = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} . q_1^{n_1} q_2^{n_2} \dots q_t^{n_t}$.

Như vậy, nếu d là một ước chung của mn thì $d = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} . q_1^{f_1} q_2^{f_2} \dots q_t^{f_t}$, trong đó $0 \leq e_i \leq m_i (i = 1, 2, \dots, s) ; 0 \leq f_i \leq n_i (i = 1, 2, \dots, t)$.

Đặt: $d_1 = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$, $d_2 = q_1^{f_1} q_2^{f_2} \dots q_t^{f_t}$. Rõ ràng $d = d_1 d_2$ và $(d_1, d_2) = 1$.

Ngược lại, giả sử d_1 và d_2 là các ước dương tương ứng của m và n . Khi đó:

$$\begin{aligned} d_1 &= p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} \text{ trong đó, } 0 \leq e_i \leq m_i (i = 1, 2, \dots, s) \\ d_2 &= q_1^{f_1} q_2^{f_2} \dots q_t^{f_t} \text{ trong đó, } 0 \leq f_i \leq n_i (i = 1, 2, \dots, t). \end{aligned}$$

Số nguyên $d = d_1 d_2 = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} . q_1^{f_1} q_2^{f_2} \dots q_t^{f_t}$.

Rõ ràng là ước của $mn = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} . q_1^{n_1} q_2^{n_2} \dots q_t^{n_t}$

vì lũy thừa của mỗi số nguyên tố xuất hiện trong phân tích ra thừa số nguyên tố của d bé hơn hoặc bằng lũy thừa của số nguyên tố đó trong phân tích của mn .

Bổ đề 1.2. Giả sử p là số nguyên tố, a là số nguyên dương. Khi đó:

$$\begin{aligned} \sigma(p^a) &= (1 + p + p^2 + \dots + p^a) = \frac{p^{a+1} - 1}{p - 1} \\ \tau(p^a) &= a + 1 \end{aligned}$$

Chứng minh. Các ước của p^a là $1, p, p^2, \dots, p^a$. Do đó, p^a có đúng $a + 1$ ước dương, $\tau(p^a) = a + 1$. Mặt khác, $\sigma(p^a) = 1 + p + p^2 + \dots + p^a = \frac{p^{a+1} - 1}{p - 1}$.

Định lý 1.1. Giả sử f là một hàm có tính chất nhân. Khi đó hàm $F(n) = \sum_{d|n} f(d)$ cũng có tính chất nhân.

Chứng minh. Ta sẽ chỉ ra rằng nếu m, n là các số nguyên dương nguyên tố cùng nhau thì $F(mn) = F(m).F(n)$. Giả sử $(m, n) = 1$, ta có:

$$F(mn) = \sum_{d|mn} f(d).$$

Vì $(m, n) = 1$ nên theo bổ đề 1.1, mỗi ước số của mn có thể viết duy nhất dưới dạng tích các ước d_1 của m và d_2 của n và d_1, d_2 nguyên tố cùng nhau, đồng thời mỗi cặp ước số d_1 của m và d_2 của n tương ứng với ước $d_1.d_2$ của mn . Do đó ta có thể viết: $F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1.d_2)$.

Vì f là hàm có tính chất nhân và $(d_1, d_2) = 1$ nên

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) = \sum_{d_1|m} f(d_1) \cdot \sum_{d_2|n} f(d_2) = F(m).F(n)$$

Tính chất 1. Hàm $\sigma(n)$ là hàm nhân tính, tức là: Với mọi số tự nhiên n_1, n_2 nguyên tố cùng nhau thì $\sigma(n_1.n_2) = \sigma(n_1).\sigma(n_2)$

Chứng minh. Từ Định lý 1.1 suy ra hàm số $\sigma(n)$ có tính chất nhân. Vì thế ta có thể viết công thức của chúng khi biết phân tích thành thừa số nguyên tố của n .

Tính chất 2. Nếu p là số nguyên tố thì $\sigma(p) = 1 + p$

Chứng minh. Được suy ra từ Bổ đề 1.2.

Tính chất 3. Giả sử n là số nguyên dương và có khai triển chính tắc $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ thì $\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$

Chứng minh. Do hàm σ có tính chất nhân nên ta có

$$\sigma(n) = \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) \dots \sigma(p_k^{\alpha_k}).$$

1.3. Hàm tổng các chữ số của số tự nhiên n

1.3.1. Định nghĩa

Định nghĩa 1.1. Giả sử n là một số tự nhiên. Ta định nghĩa $S(n)$ là hàm tổng các chữ số của n , khi biểu diễn trong hệ thập phân.

1.3.2. Các tính chất

Với n là số nguyên dương. Ta có:

Tính chất 1. $S(n) \equiv n \pmod{9}$.

Chứng minh. Giả sử trong biểu diễn thập phân, số nguyên dương n có dạng: $n = \overline{\alpha_k \alpha_{k-1} \dots \alpha_2 \alpha_1 \alpha_0} |_{10}$

Khi ấy

$$\begin{aligned} n &= \alpha_0 + 10\alpha_1 + 10^2\alpha_2 + \dots + 10^{k-1}\alpha_{k-1} + 10^k\alpha_k \\ S(n) &= \alpha_0 + \alpha_1 + \alpha_2 + \dots + \alpha_{k-1} + \alpha_k \end{aligned}$$

Vì thế

$$n - S(n) = 9\alpha_1 + 99\alpha_2 + \dots + \underbrace{99\dots9}_{(k-1) \text{ số } 9} \alpha_{k-1} + \dots + \underbrace{99\dots9}_{k \text{ số } 9} \alpha_k. \quad (1.1)$$

Từ (1.1) suy ra $[n - S(n)] : 9$ hay $S(n) \equiv n \pmod{9}$, suy ra điều phải chứng minh.

Tính chất 2. $0 < S(n) \leq n$

Tính chất 3. $S(n) = n \Leftrightarrow 1 \leq n \leq 9$

Chứng minh. Ta có $n = \overline{\alpha_k \alpha_{k-1} \dots \alpha_2 \alpha_1 \alpha_0} |_{10}$. Vì $n > 0$ nên $\alpha_k > 0$. Ngoài ra $\alpha_i \in \{0, 1, 2, \dots, 9\}$ với mọi $i = 1, 2, \dots, k$.

Từ đó, do $S(n) = \alpha_k + \alpha_{k-1} + \dots + \alpha_1 + \alpha_0$ suy ra $S(n) > 0$.

Lại thấy từ (1.1) thì $S(n) \leq n$ và $S(n) = n \Leftrightarrow \alpha_1 = \alpha_2 = \dots = \alpha_k = 0 \Leftrightarrow \alpha_0 > 0 \Leftrightarrow \alpha_0 \in \{1, 2, \dots, 9\}$. Đó là điều phải chứng minh.

Tính chất 4. $S(m+n) \leq S(m) + S(n)$, với mọi m, n nguyên dương.

Chứng minh. Giả sử trong hệ thập phân, n và m lần lượt có dạng:

$$\begin{aligned} n &= \overline{\alpha_k \alpha_{k-1} \dots \alpha_1 \alpha_0} |_{10} \\ m &= \overline{\beta_k \beta_{k-1} \dots \beta_1 \beta_0} |_{10} \end{aligned}$$

Không giảm tổng quát, ta có thể cho là $n \geq m \Rightarrow k \geq s$. Ta có thể viết lại m dưới dạng sau đây $m = \overbrace{00\dots 0}^{(k-s) \text{ số } 0} \beta_s \beta_{s-1} \dots \beta_1 \beta_0 |_{10}$

$$\text{Đặt } \beta_i' = \begin{cases} \beta_i & \text{với } i = 0, 1, 2, \dots, s \\ 0 & \text{với } i = s + 1, \dots, k. \end{cases}$$

Vì thế luôn luôn có thể coi n và m có cùng loại biểu diễn sau:

$$\begin{aligned} n &= \overline{\alpha_k \alpha_{k-1} \dots \alpha_2 \alpha_1 \alpha_0} |_{10} \\ m &= \overline{\beta_k \beta_{k-1} \dots \beta_2 \beta_1 \beta_0} |_{10} \end{aligned}$$

trong đó $0 \leq \alpha_i, \beta_i \leq 9$, với mọi $i = 0, 1, 2, \dots, k$ và α_i, β_i nguyên.

Ta sẽ chứng minh bất đẳng thức $S(m+n) \leq S(m) + S(n)$ với mọi m, n nguyên dương bằng phép quy nạp theo k .

- Nếu $k = 0$, khi đó $n = \alpha_0, m = \beta_0$ suy ra $S(n) + S(m) = \alpha_0 + \beta_0$

Ta có $m+n = \alpha_0 + \beta_0$, do vậy

$$S(m+n) = \begin{cases} \alpha_0 + \beta_0 & \text{nếu } \alpha_0 + \beta_0 \leq 9 \\ (\alpha_0 + \beta_0 - 10) + 1 & \text{nếu } \alpha_0 + \beta_0 > 9 \end{cases}$$

Chú ý rằng do $0 < \alpha_0 \leq 9; 0 < \beta_0 \leq 9$ nên $\alpha_0 + \beta_0 \leq 18$, suy ra $\alpha_0 + \beta_0 - 9 \leq 9 < \alpha_0 + \beta_0$ (khi $\alpha_0 + \beta_0 > 9$)

Tóm lại, ta luôn chứng minh được $S(m+n) \leq S(m) + S(n)$, trong trường hợp $k = 0$. Vậy điều khẳng định đúng khi $k = 0$.

- Giả sử điều khẳng định đã đúng đến $k-1$, tức là với mọi biểu diễn trong hệ thập phân: $n = \overline{\alpha_{k-1} \dots \alpha_2 \alpha_1 \alpha_0} |_{10}$, $m = \overline{\beta_{k-1} \dots \beta_2 \beta_1 \beta_0} |_{10}$ (trong đó ít nhất một trong hai số $\alpha_{k-1}, \beta_{k-1}$ phải lớn hơn 0), ta luôn có: $S(m+n) \leq S(m) + S(n)$

- Xét trường hợp với k , tức là khi n và m biểu diễn như sau:

$$n = \overline{\alpha_k \alpha_{k-1} \dots \alpha_2 \alpha_1 \alpha_0} |_{10}, m = \overline{\beta_k \beta_{k-1} \dots \beta_2 \beta_1 \beta_0} |_{10}$$

ở đây ít nhất một trong hai số α_k, β_k phải lớn hơn 0.

Ta có thể viết lại: $n = 10.\overline{\alpha_k \alpha_{k-1} \dots \alpha_1 \alpha_0}$; $m = 10.\overline{\beta_k \beta_{k-1} \dots \beta_1 \beta_0}$

Vì $10.\overline{\alpha_k \alpha_{k-1} \dots \alpha_1} = \overline{\alpha_k \alpha_{k-1} \dots \alpha_1 0}$ nên suy ra $S(n) = S(n')$,

ở đây $n' = \overline{\alpha_k \alpha_{k-1} \dots \alpha_1}$

Tương tự: $10.\overline{\beta_k \beta_{k-1} \dots \beta_1} = \overline{\beta_k \beta_{k-1} \dots \beta_1 0}$ nên suy ra $S(m) = S(m')$,

ở đây $m' = \overline{\beta_k \beta_{k-1} \dots \beta_1}$

Rõ ràng ta có: $S(n) = \alpha_0 + S(n')$ và $S(m) = \beta_0 + S(m')$.

Áp dụng giả thiết quy nạp, ta thấy ngay: $S(m' + n') \leq S(m') + S(n')$.

Mặt khác, ta có: $m + n = 10(m' + n') + \alpha_0 + \beta_0$ nên

$$S(m + n) \leq S(m') + S(n') + \alpha_0 + \beta_0.$$

suy ra $S(m + n) \leq S(m') + S(n') + \alpha_0 + \beta_0 = S(m) + S(n)$.

Vậy điều khẳng định cũng đúng đến k . Từ đó suy ra điều phải chứng minh.

Nhận xét 1.1. Bằng quy nạp dễ dàng chứng minh được:

Nếu $a_1, a_2, \dots, a_k$ là các số nguyên dương thì:

$$S(a_1 + a_2 + \dots + a_k) \leq \sum_{i=1}^k S(a_i)$$

$$S(a_1 a_2 \dots a_k) \leq S(a_1) \cdot S(a_2) \dots S(a_k).$$

Tính chất 5. $S(mn) \leq S(m) \cdot S(n)$, với mọi m, n nguyên dương.

Chứng minh. Giả sử B có biểu diễn dưới dạng thập phân là:

$$B = \overline{b_1 b_2 \dots b_k}$$

Do đó $B = b_k + 10b_{k-1} + 10^2 b_{k-2} + \dots + 10^{k-1} b_1$

Trước hết ta có nhận xét sau:

Nếu N là số tự nhiên thì với mọi số p nguyên dương, ta có:

$$S(10^p N) = S(N)$$

(Nhận xét này quá hiển nhiên dựa vào trực tiếp từ định nghĩa của hàm

$S(n)$). Ta có: $AB = Ab_k + 10Ab_{k-1} + 10^2 Ab_{k-2} + \dots + 10^{k-1} Ab_1$

Theo chứng minh của Tính chất 4, suy ra:

$$\begin{aligned} S(AB) &= S(Ab_k + 10Ab_{k-1} + \dots + 10^{k-1} Ab_1) \\ &\leq S(Ab_k) + S(10Ab_{k-1}) + \dots + S(10^{k-1} Ab_1) \end{aligned} \quad (1.2)$$

Lại theo Tính chất 4, ta có

$$S(Ab_k) = S(\underbrace{A + A + \dots + A}_{b_k \text{ số hạng } A}) \leq S(A) + S(A) + \dots + S(A) = b_k S(A)$$

Tương tự, ta có

$$\begin{aligned} S(10Ab_{k-1}) &\leq b_{k-1}S(10A) = b_{k-1}S(A); \\ S(10^2Ab_{k-2}) &\leq b_{k-1}S(10^2A) = b_{k-2}S(A); \\ &\dots\dots\dots \\ S(10A^{k-1}b_1) &\leq b_1S(10^{k-1}A) = b_1S(A). \end{aligned}$$

Vì vậy, thay vào (1.2), ta có: $S(AB) \leq (b_1 + b_2 + \dots + b_k) \cdot S(A)$
Do $S(B) = b_1 + b_2 + \dots + b_k$ nên từ đẳng thức trên ta thu được

$$S(AB) \leq S(A) \cdot S(B)$$

Đó là điều phải chứng minh.

Chú ý 1.3. Theo nguyên lí quy nạp, ta suy ra kết quả sau:

Nếu $A_1, A_2, \dots, A_n$ là các số nguyên dương thì

$$S(A_1A_2\dots A_n) \leq S(A_1) \cdot S(A_2) \cdot \dots \cdot S(A_n).$$

1.4. Hàm số các ước $\tau(n)$

1.4.1. Định nghĩa

Định nghĩa 1.1. Số các ước dương của của số tự nhiên n được kí hiệu là $\tau(n)$.

Ví dụ 1.8. $\tau(1) = 1, \tau(2) = 2, \tau(12) = 6$.

1.4.2. Các tính chất

Tính chất 1. Hàm $\tau(n)$ là hàm có tính chất nhân.

Chứng minh. Dựa trực tiếp vào Định lí (1.1)

Tính chất 2. Nếu p là số nguyên tố thì $\tau(p) = 2$.

Tính chất 3. Giả sử số nguyên dương n có khai triển chính tắc $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ thì $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$.

Chứng minh. Được suy ra trực tiếp từ Bổ đề 1.2

1.5. Hàm phần nguyên $[x]$

1.5.1. Định nghĩa

Định nghĩa 1.1. Hàm phần nguyên $[x]$ của một số nguyên x là số nguyên lớn nhất không vượt quá x .

Ví dụ 1.9. $[2.33] = 2$, $[-2.33] = -3$

1.5.2. Các tính chất

Tính chất 1. Cho x, y là các số thực, khi đó:

1. $[x] \leq x < x + 1$; $x - 1 < [x] \leq x$; $0 \leq x - [x] < 1$
2. Với mọi số nguyên m , $[x + m] = [x] + m$
3. $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$
4. $[x] + [-x] = \begin{cases} 0 & \text{nếu } x \text{ là một số nguyên} \\ -1 & \text{nếu trái lại} \end{cases}$
5. $-[-x]$ là số nguyên nhỏ nhất lớn hơn hoặc bằng x .
6. Nếu m là một số nguyên thì $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$
7. Nếu a, m là các số nguyên dương thì $\left[\frac{x}{m}\right]$ là số các bội số của a nằm trong khoảng $[1, m]$.

Chứng minh.

1. Hiển nhiên suy ra từ định nghĩa.
2. Chỉ cần chứng minh cho $0 \leq x < 1$. Khi đó, $m \leq x + m < m + 1$ nên theo định nghĩa, $[x] = 0$, $[x + m] = m = [x] + m$.
Tức là $[x + m] = [x] + m$
3. Do $f(x) = [x]$ là một hàm không giảm và $[y] \leq y < [y] + 1$ nên từ 2) ta có $[x] + [y] = [x + [y]] \leq [x + y] \leq [x + ([y] + 1)]$
Tức là $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$
4. Nếu $x = m$ là một số nguyên thì $[x] = m$, $[-x] = -m$
nên $[x] + [-x] = 0$.
Nếu x không là một số nguyên, $x = m + h$ với m là một số nguyên và $0 < h < 1$ thì $-x = -m - 1 + (1 - h)$ với $0 < 1 - h < 1$ nên theo định nghĩa $[x] = m$ và $[-x] = -m - 1$. Do đó, $[x] + [-x] = -1$.

5. Chỉ cần chứng minh cho trường hợp x không phải là một số nguyên. Giả sử $x = m + h$ với m là một số nguyên và $0 < h < 1$, Khi đó như chứng minh trên ta có $[-x] = -m - 1$ nên $-[-x] = m + 1$ chính là số nguyên nhỏ nhất lớn hơn hoặc bằng x .

6. Giả sử $\left[\frac{x}{m}\right] = k$. Khi đó, $k \leq \frac{x}{m} < k + 1$ nên $km \leq x < k(m + 1)$.

Do $[x]$ là số nguyên dương lớn nhất không vượt quá x nên

$$km \leq [x] \leq x < m(k + 1).$$

Do đó $km \leq [x] < m(k + 1)$,

suy ra $k \leq \frac{[x]}{m} < k + 1$, tức là $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$

7. Giả sử $a, 2a, \dots, na$ là tất cả các bội số của a nằm trong khoảng $[1, m]$, ta cần chứng minh $[m/a] = n$. Thật vậy, do $a, 2a, \dots, na$ là tất cả các bội số của a nằm trong khoảng $[1, m]$ nên $na \leq m < (n + 1)a$. Do đó, $n \leq m/a < (n + 1)$. Theo định nghĩa ta có: $[m/a] = n$.

Định lí được chứng minh.

Tính chất 2 (Công thức Polignac). Cho p là một số nguyên tố, khi đó số mũ lớn nhất k sao cho p^k là ước của $n!$ là $k = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$

Chứng minh. Gọi e_i là các số chia hết cho p^i trong khoảng $[1, n]$. Khi đó số các số trong khoảng $[1, n]$ chia hết cho p^i mà không chia hết cho p^{i+1} là $f_i = e_i - e_{i+1}$ và số mũ lớn nhất k sao cho p^k là ước số của $n!$ có dạng $k = \sum_{i=1}^{\infty} if_i$. Theo tính chất 1) ta có $e_i = \left[\frac{n}{p^i}\right]$, $f_i = \left[\frac{n}{p^i}\right] - \left[\frac{n}{p^{i+1}}\right]$

Do đó $k = \sum_{i=1}^{\infty} if_i = \sum_{i=1}^{\infty} i \left(\left[\frac{n}{p^i}\right] - \left[\frac{n}{p^{i+1}}\right] \right) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$

Điều phải chứng minh.

Chương 2

Một số ứng dụng của các hàm số học

Trong chương trình phổ thông, các bài toán về số học đóng vai trò quan trọng trong việc hình thành tư duy toán học. Việc sử dụng các hàm số học đã giải quyết được những lớp bài toán cơ bản trong các bài toán sơ cấp.

Trong chương này trình bày một số ứng dụng của các hàm số học cơ bản trong việc giải các bài toán sơ cấp. Ngoài ra, còn có những bài toán tổng hợp sử dụng một số hàm số khác.

2.1. Ứng dụng của Phi - hàm Ơ-le

2.1.1. Xét đồng dư môđulô của một số nguyên tố

Ví dụ 2.1. Giả sử p nguyên tố, r là số tự nhiên nhỏ hơn p sao cho:

$$(-1)^r r! \equiv 1 \pmod{p} \quad (2.1)$$

Chúng minh rằng:

$$(p - r - 1)! + 1 \equiv 0 \pmod{p} \quad (2.2)$$

Lời giải. Theo định lí Wilson ta có

$$(p - 1)! + 1 \equiv 0 \pmod{p}. \quad (2.3)$$

Mặt khác, $(p - 1)(p - 2) \dots (p - r) \equiv (-1)^r r! \pmod{p}$. Suy ra

$$(p - 1)! \equiv (p - r - 1)!(-1)^r r! \pmod{p} \equiv (p - r - 1)! \pmod{p}. \quad (2.4)$$

Từ (2.3) và (2.4) suy ra các đồng dư (2.1) và (2.2) là tương đương nhau.

Ví dụ 2.2. Xét dãy $U_k = \frac{k(k+1)}{2}$ với $k = 1, 2, \dots, n$. Chứng minh rằng nếu $n = 2^s (s > 1)$ thì trong dãy trên có thể chọn được một hệ thặng dư đầy đủ môđulo n .

Lời giải. Xét n số U_{2k-1} với $k = 1, 2, \dots$. Ta chỉ cần chứng minh với mọi $1 \leq i < j \leq n$ thì $U_{2i-1} \not\equiv U_{2j-1} \pmod{n}$

Giả sử ngược lại tồn tại $1 \leq i < j \leq n$ mà $U_{2i-1} \equiv U_{2j-1} \pmod{n}$

$$\begin{aligned} &\Leftrightarrow (2i-1)i \equiv (2j-1)j \pmod{n} \\ &\Leftrightarrow (j-i)(2j+2i-1) \equiv 0 \pmod{n} \end{aligned} \quad (2.5)$$

Do $n = 2^s (s > 1)$ nên n không có ước lẻ.

Từ (2.5) $\Rightarrow j \equiv i \pmod{n}$ (vô lý) suy ra điều phải chứng minh.

2.1.2. Chứng minh phép chia với dư

Ví dụ 2.3. Chứng minh rằng: nếu a nguyên tố với 7 thì $a^{2010} - 1$ chia hết cho 7.

Lời giải. Do 7 là số nguyên tố nên $\varphi(7) = 7 - 1 = 6$.

Do đó theo định lý Ô-le ta có $a^{\varphi(7)} = a^6 \equiv 1 \pmod{7}$.

Từ đó $a^{2010} = (a^6)^{335} \equiv 1 \pmod{7}$ hay $a^{2010} - 1 \equiv 0 \pmod{7}$.

Vậy $a^{2010} - 1$ chia hết cho 7.

Ví dụ 2.4. Chứng minh rằng: $20^{15} - 1$ chia hết cho 11.31.61

Lời giải.

Chứng minh $20^{15} - 1$ chia hết cho 11.

Do $(20, 11) = 1$ và $\varphi(11) = 10$. Theo định lý Ô-le ta có

$$20^{\varphi(11)} \equiv 20^{10} \equiv 1 \pmod{11}$$

Do đó $20^{15} \equiv 20^5 \equiv (-2)^5 \equiv 1 \pmod{11}$

Vậy $20^{15} - 1$ chia hết cho 11.

Chứng minh tương tự, ta có: $20^{15} - 1$ chia hết cho 31 và 61.

mà 11, 31, 61 là các số nguyên tố cùng nhau.

Vậy $20^{15} - 1$ chia hết cho 11.31.61

Ví dụ 2.5. Chứng minh rằng: $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$ với $m, n > 1$ và $(m, n) = 1$.

Lời giải. Do $(m, n) = 1$ nên theo định lí Ô-le ta có

$$\begin{cases} m^{\varphi(n)} \equiv 1 \pmod{n} \\ n^{\varphi(m)} \equiv 1 \pmod{m} \end{cases} \Rightarrow \begin{cases} m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{n} \\ n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{m} \end{cases}$$

Suy ra $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$.

2.1.3. Giải phương trình đồng dư

Ví dụ 2.6. Tìm ít nhất 4 nghiệm của phương trình:

$$x^3 + y^7 \equiv 1 \pmod{30}.$$

Lời giải. Do $30 = 5 \times 6$ và $(5, 6) = 1$ nên theo hệ quả (1.1) có

$$5^{\varphi(6)} + 6^{\varphi(5)} \equiv 1 \pmod{30}$$

Vì $\varphi(6) = \varphi(2) \cdot \varphi(3) = 2$ và $\varphi(5) = 4$; $6^2 \equiv 6 \pmod{30}$ nên ta có

$$5^2 + 6^4 \equiv (25 + 6) \equiv 1 \pmod{30}$$

Ta thấy $25^3 \equiv 25 \pmod{30}$; $6^2 \equiv 6 \pmod{30}$ nên theo hệ quả (1.2) có

$$25^3 + 6^7 \equiv 25 + 6 \equiv 1 \pmod{30}$$

Tương tự có $25^7 \equiv 25 \pmod{30}$; $6^3 \equiv 6 \pmod{30}$ nên

$$6^3 + 25^7 \equiv 1 \pmod{30}$$

Nếu phân tích $30 = 3 \times 10$ với $(3, 10) = 1$ thì theo hệ quả (1.1) có

$$3^{\varphi(10)} + 10^{\varphi(3)} \equiv 1 \pmod{30}$$

Tính toán tương tự trên ta có $3^4 + 10^3 \equiv 1 \pmod{30}$

Vì $3^4 = 81 \equiv 21 \pmod{30}$; $10^2 \equiv 10 \pmod{30}$ nên theo hệ quả (1.3) có

$$(3^4)^3 + (10^2)^7 \equiv 1 \pmod{30} \text{ và } (3^4)^7 + (10^2)^3 \equiv 1 \pmod{30}$$

Suy ra phương trình có ít nhất 4 nghiệm (x, y) là:

$$(25, 6), (6, 25), (21, 10), (10, 21).$$

Ví dụ 2.7. Chứng minh rằng phương trình đồng dư sau có nghiệm (x, y, z, t) khác $(0, 0, 0, 0)$: $x^3 + y^3 + z^3 \equiv t^3 \pmod{210}$.

Lời giải. Do $210 = 5 \times 6 \times 7$ và $(5, 6) = (5, 7) = (6, 7) = 1$ nên ta đặt

$$m_1 = 5, t_1 = 42, m_2 = 6, t_2 = 35, m_3 = 7, t_3 = 30.$$

Theo hệ quả (1.3) ta có

$$42^3 + 35^3 + 30^3 \equiv (42 + 35 + 30)^3 \equiv 107^3 \pmod{210}.$$

Vậy phương trình có nghiệm (x, y, z, t) là $(42, 35, 30, 107)$.

Nếu phân tích $210 = 3 \times 7 \times 10$ thì tương tự như thế ta thấy phương trình có nghiệm (x, y, z, t) là $(70, 30, 21, 121)$.

2.1.4. Tìm nghiệm nguyên của phương trình

Ví dụ 2.8. Tìm nghiệm nguyên của phương trình:

$$12x - 19y + 21 = 0.$$

Lời giải. Phương pháp này dựa trên mệnh đề sau:

Mệnh đề. Xét phương trình $ax + by + c = 0$, trong đó a, b là các số nguyên dương, $(a, b) = 1, c$ là số nguyên. Khi đó phương trình này có

một nghiệm riêng sau đây:
$$\begin{cases} x_0 = -ca^{\varphi(b)-1} \\ y_0 = c \cdot \frac{a^{\varphi(b)} - 1}{b} \end{cases}$$

Do a, c là các số nguyên, còn $\varphi(b) \geq 1$ là số nguyên nên hiển nhiên x_0 là số nguyên. Theo định lý Ô-le thì

$$a^{\varphi(b)} \equiv 1 \pmod{b} \Rightarrow (a^{\varphi(b)} - 1) : b.$$

Từ đó y_0 là số nguyên. Mặt khác

$$ax_0 + by_0 + c = -aca + ca - c + c = -ca^{\varphi(b)} + ca^{\varphi(b)} = 0$$

Vậy (x_0, y_0) là nghiệm riêng của phương trình $ax + by + c = 0$, suy ra điều phải chứng minh.

Trở lại phương trình đã cho

$$\begin{aligned} 12x - 19y + 21 &= 0 \\ \Leftrightarrow 12x + 19(-y) + 21 &= 0 \\ \Leftrightarrow 12x + 19z + 21 &= 0, \text{ với } z = -y. \end{aligned}$$

Do 19 là số nguyên tố nên $\varphi(19) = 19 - 1 = 18$. Do đó

$$\begin{cases} x_0 = -21.12^{17} \\ z = 21. \frac{12^{18} - 1}{19} \end{cases}$$

là một nghiệm riêng của phương trình $12x + 19z + 21 = 0$.

Vậy mọi nghiệm của phương trình này có dạng

$$\begin{cases} x = -21.12^{17} + 19t \\ z = 21. \frac{12^{18} - 1}{19} - 12t \end{cases}$$

Nói cách khác, phương trình $12x - 19y + 21 = 0$ có nghiệm là:

$$\begin{cases} x = -21.12^{17} + 19t \\ y = -21. \frac{12^{18} - 1}{19} + 12t \end{cases}$$

Nhận xét 2.1. Cách giải này hoàn toàn mang tính chất lí thuyết. Trong thực tế, chúng ta sẽ không sử dụng cách này.

2.1.5. Tìm cấp của số nguyên

Ví dụ 2.9. Tìm cấp (mod 101) của 2.

Lời giải. Đặt $n = 101$ và $a = 2$. Gọi h là cấp của $a \pmod{101}$.

Vì $2^{\varphi(101)} \equiv 1 \pmod{101}$ nên ta có

$$\varphi(101) : h \tag{2.6}$$

Do 101 là số nguyên tố nên dễ thấy $\varphi(101) = 101 - 1 = 100$. Như vậy từ (2.6), ta có

$$101 : h$$

Nếu $h < 100$ thì do các ước nhỏ hơn 100 của 100 chỉ có thể là 2, 4, 10, 20, 25, 50 nên suy ra hoặc là $50 : h$ hoặc là $20 : h$.

Vì h là cấp của $2 \pmod{101}$ nên ta có

$$2^{50} \equiv 1 \pmod{101} \text{ hoặc } 2^{20} \equiv 1 \pmod{101} \quad (2.7)$$

Mặt khác, $2^{50} = (2^{10})^5 = 1024^5$. Vì $1024 \equiv 14 \pmod{101}$ nên ta đi đến

$$\begin{aligned} 1024^5 &\equiv 14^5 \pmod{101} \\ &\equiv 19.196.14 \pmod{101} \\ &\equiv (-6)(-6).14 \pmod{101} \\ &\equiv 504 \pmod{101} \\ &\equiv -1 \pmod{101} \end{aligned}$$

Vì thế ta có

$$2^{50} \equiv -1 \pmod{101} \quad (2.8)$$

Lại thấy

$$2^{20} \equiv 1024^2 \equiv 14^2 \equiv 196 \equiv -6 \pmod{101} \quad (2.9)$$

Từ (2.7), (2.8) và (2.9) suy ra mâu thuẫn. Vậy giả thiết phản chứng $h < 100$ là sai. Vì thế từ $100 : h$ suy ra $h = 100$.

Vậy 100 là cấp $\pmod{101}$ của 2.

2.1.6. Tìm số tự nhiên thỏa mãn tính chất hàm số $\varphi(n)$

Ví dụ 2.10. Tìm tất cả các số tự nhiên n có tính chất n chia hết cho $\varphi(n)$, trong đó φ là hàm Ô-le.

Lời giải. Hiển nhiên nếu $n = 1$ thì $\varphi(n) | n$. Ta xét $n > 1$. Giả sử n có phân tích thành thừa số nguyên tố dưới dạng $n = p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}$.

Ta có $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_i}\right)$.

Từ điều kiện $\varphi(n) | n$, chẳng hạn $n = x \cdot \varphi(n)$, suy ra

$$p_1 p_2 \dots p_i = x(p_1 - 1)(p_2 - 1) \dots (p_i - 1).$$

Như vậy, phải có p_j nào đó bằng 2 (nếu ngược lại thì vô lí, vì về trái là số lẻ, về phải là số chẵn). Giả sử $p_1 = 2$, ta có

$$2p_2 \dots p_i = x(p_2 - 1) \dots (p_i - 1).$$

Do $p_2, \dots, p_i$ khác 2 nên từ đẳng thức trên suy ra rằng n có nhiều nhất là một ước nguyên tố lẻ, chẳng hạn p_2 .

Đặt $p_2 = 2y + 1$. Ta có: $2p_2 = x(2y)$.

Do p_2 nguyên tố nên suy ra $x = p_2, y = 1$. Vậy $p_2 = 3$ và n có dạng

$$n = 2^k 3^m, \quad k \geq 1, m \geq 0.$$

Dễ thử lại rằng, các số n có dạng nói trên thỏa mãn điều kiện: $\varphi(n) | n$

Ví dụ 2.11. Chứng minh rằng với mọi số tự nhiên $n \geq 2$, ta có

$$\sigma(n) + \varphi(n) \geq 2n.$$

Lời giải. Giả sử các ước của n là $1 = d_1 < d_2 < \dots < d_k = n$.

Trong các số tự nhiên không vượt quá n , có $\frac{n}{d_i}$ số là bội của d_i . Mỗi số không vượt quá n và không nguyên tố cùng nhau với n phải là bội của một ước nào đó (lớn hơn 1) của n . Vì thế ta có

$$n - \varphi(n) \leq \frac{n}{d_2} + \frac{n}{d_3} + \dots + \frac{n}{d_k}.$$

Mặt khác, $\frac{n}{d_2} + \frac{n}{d_3} + \dots + \frac{n}{d_k} = d_{k-1} + d_{k-2} + \dots + d_1 = \sigma(n) - n$.

Vậy $n - \varphi(n) \leq \sigma(n) - n$, tức là $\sigma(n) + \varphi(n) \geq 2n$.

Khi n nguyên tố, ta có đẳng thức: $\sigma(n) + \varphi(n) = 2n$.

2.2. Ứng dụng của hàm tổng các ước số dương của số tự nhiên n

2.2.1. Chứng minh một số là hợp số

Ví dụ 2.12. Chứng minh rằng n là hợp số khi và chỉ khi:

$$\sigma(n) > n + \sqrt{n}.$$

Lời giải. Giả sử n là hợp số. Khi đó ngoài ước của 1 và n ra, n còn ít nhất một ước $d(1 < d < n)$. Lúc này $\frac{n}{d}$ cũng là một ước của n (rõ ràng $1 < \frac{n}{d} < n$). Có hai khả năng xảy ra:

1) Nếu $\frac{n}{d} \neq d$. Khi đó có ít nhất 4 ước là 1, n , d , $\frac{n}{d}$. Vì thế

$$\sigma(n) \geq 1 + n + d + \frac{n}{d} \quad (2.10)$$

Ta có

$$d + \frac{n}{d} \geq 2\sqrt{n} > \sqrt{n}. \quad (2.11)$$

Từ (2.10) và (2.11) suy ra trong trường hợp này ta có $\sigma(n) > n + \sqrt{n}$.

2) Nếu $\frac{n}{d} = d$ (tức là $d = \sqrt{n}$). Lúc này n có ít nhất 3 ước là 1, $\sqrt{n}$, n . Vì thế $\sigma(n) \geq 1 + n + \sqrt{n} > n + \sqrt{n}$.

Tóm lại khi n là hợp số ta luôn có $\sigma(n) > n + \sqrt{n}$.

Đảo lại, giả sử

$$\sigma(n) > n + \sqrt{n}. \quad (2.12)$$

Rõ ràng $n \neq 1$. Vì $\sigma(1) = 1$, suy ra

$$\sigma(1) < 1 + \sqrt{1}. \quad (2.13)$$

Từ (2.12) và (2.13) suy ra nếu n thỏa mãn (2.11) thì n không thể bằng 1.

Rõ ràng n không thể là số nguyên tố. Thật vậy, nếu p là số nguyên tố thì $\sigma(p) = p + 1 < p + \sqrt{p}$ (chú ý $p \geq 2$)

Vì thế, nếu n thỏa mãn (2.12) thì n cũng không thể là số nguyên tố. Vì lí do đó suy ra nếu n thỏa mãn (2.12) thì n là hợp số.

Tóm lại n là hợp số khi và chỉ khi $\sigma(n) > n + \sqrt{n}$. Đó là điều phải chứng minh.

2.2.2. Chứng minh một số là số hoàn hảo

Ví dụ 2.13. Số nguyên dương n gọi là số hoàn hảo nếu $\sigma(n) = 2n$. Chứng minh rằng số nguyên dương chẵn n là số hoàn hảo khi và chỉ

khi n có biểu diễn: $n = 2^{m-1}(2^m - 1)$, trong đó m là số nguyên sao cho $m \geq 2$ và $2^m - 1$ là số nguyên tố.

Lời giải.

1) Giả sử n là số nguyên dương chẵn và có dạng $n = 2^{m-1}(2^m - 1)$ trong đó m là số nguyên, mà $m \geq 2$ và $2^m - 1$ là số nguyên tố.

Rõ ràng $(2^{m-1}, 2^m - 1) = 1$, mà $\sigma(n)$ là hàm nhân tính nên ta có

$$\sigma(n) = \sigma(2^{m-1}).\sigma(2^m - 1) \quad (2.14)$$

Do $2^m - 1$ là số nguyên tố nên dựa vào công thức $\sigma(p) = p + 1$ khi p là số nguyên tố, ta có

$$\sigma(2^m - 1) = (2^m - 1) + 1 = 2^m.$$

Mặt khác 2^{m-1} có các ước dương là $1, 2, 2^2, \dots, 2^{m-1}$ và có tổng các ước là

$$1 + 2 + 2^2 + \dots + 2^{m-1} = \frac{2^m - 1}{2 - 1} = 2^m - 1.$$

Từ đó theo (2.14) suy ra

$$\sigma(n) = (2^m - 1).2^m = 2.2^{m-1}(2^m - 1) \Rightarrow \sigma(n) = 2n.$$

Vậy n là số hoàn hảo.

2) Đảo lại, giả sử n là số hoàn hảo chẵn. Biểu diễn n dưới dạng sau: $n = 2^s.t$, trong đó s và t là các số nguyên dương và t là số lẻ.

Do $\sigma(n)$ là hàm nhân tính và vì $(2^s, t) = 1$ nên

$$\sigma(n) = \sigma(2^s).\sigma(t) = (2^{s+1} - 1).\sigma(t) \quad (2.15)$$

(Chú ý, lập luận như trên, suy ra $\sigma(2^s) = 2^{s+1} - 1$).

Do n là số hoàn hảo nên theo định nghĩa thì

$$\sigma(n) = 2n = 2^{s+1}.t \quad (2.16)$$

Từ (2.15) và (2.16) ta có

$$2^{s+1}.t = (2^{s+1} - 1).\sigma(t) \quad (2.17)$$

Từ (2.17) suy ra

$$\{(2^{s+1} - 1) \sigma(t)\} : 2^{s+1} \quad (2.18)$$

Vì $(2^{s+1}, 2^{s+1}) = 1$ nên từ (2.18) ta có

$$2^{s+1} : \sigma(t) \quad (2.19)$$

Từ (2.19) ta có biểu diễn sau

$$\sigma(t) = 2^{s+1} \cdot q \quad (2.20)$$

Thay (2.20) vào (2.17) ta thu được

$$(2^{s+1} - 1)2^{s+1}q = 2^{s+1} \cdot t \Rightarrow (2^{s+1} - 1)q = t \quad (2.21)$$

Từ (2.21) suy ra $t : q$. Rõ ràng $t \neq q$ (vì nếu $t = q \Rightarrow 2^{s+1} - 1 = 1 \Rightarrow 2^{s+1} = 2 \Rightarrow s = 0 \Rightarrow n = t \Rightarrow n$ lẻ, do t lẻ. Đó là điều vô lí vì n là số nguyên dương chẵn). Ta lại thấy $t + q = (2^{s+1} - 1)q + q = 2^{s+1}q = \sigma(t)$ (theo (2.20)). Ta chứng minh rằng $q = 1$.

Thật vậy, nếu ngược lại $q > 1$ thì t có ít nhất 3 ước khác nhau là: $1, t, q$ (chú ý $t : q, t \neq q$). Theo định nghĩa thì $\sigma(t) \geq 1 + t + q$. Như vậy ta thu được hệ phi lí sau

$$\begin{cases} \sigma(t) = t + q \\ \sigma(t) \geq t + q + 1 \end{cases}$$

Vì thế $q = 1$. Do vậy $\sigma(t) = 2^{s+1} \Rightarrow t = \sigma(t) - 1 = 2^{s+1} - 1$. Từ đó

$$n = 2^s(2^{s+1} - 1).$$

Chú ý rằng cũng từ $q = 1$, ta có $\sigma(t) = t + 1 \Rightarrow t$ là số nguyên tố. $\Rightarrow 2^{s+1} - 1$ là số nguyên tố.

Đặt $m = s + 1$, thì $m \geq 2$ và $n = 2^{m-1}(2^m - 1)$, trong đó $2^m - 1$ là số nguyên tố. Bài toán đã được giải hoàn toàn.

Nhận xét 2.2. 1) Từ bài tập trên suy ra để tìm các số hoàn hảo, ta chỉ cần tìm số các số nguyên tố có dạng $2^m - 1$ (vì khi đó số $2^{m-1}(2^m - 1)$ là số hoàn hảo).

2) Giả sử m là số nguyên dương, khi đó số $M_m = 2^m - 1$ được gọi là số Mersenne thứ m . Nếu p là số nguyên tố và M_p cũng là số nguyên tố thì M_p được gọi là số nguyên tố Mersenne.

Ví dụ: M_2, M_3, M_5, M_7 là các số nguyên tố Mersenne, còn M_{11} là hợp số.

Ví dụ 2.14. Cho n là số hoàn hảo và là số lẻ. Chứng minh rằng n có ít nhất 3 ước nguyên tố khác nhau.

Lời giải. Giả sử n là số hoàn hảo, và gọi $\sigma(n)$ là tổng tất cả các ước số của n . Khi đó: $\sigma(n) = 2n$.

Bây giờ giả sử n là số hoàn hảo và là số lẻ nhưng kết luận của bài toán không đúng. Khi đó chỉ có hai khả năng sau xảy ra:

1) Nếu n chỉ có một ước số nguyên tố, tức là số n có dạng $n = p^k$ với p là số nguyên tố lẻ (chú ý do n là số lẻ). Ta có

$$\begin{aligned} 2 &= \frac{\sigma(n)}{n} = \frac{1 + p + p^2 + \dots + p^k}{p^k} = 1 + \frac{1}{p} + \frac{1}{p^2} + \dots + \frac{1}{p^k} \\ &= \frac{1 - \frac{1}{p^{k+1}}}{1 - \frac{1}{p}} < \frac{1}{1 - \frac{1}{p}} = \frac{p}{p-1} < 2 \end{aligned}$$

$(\frac{p}{p-1} < 2 \Leftrightarrow p < 2p - 2 \Leftrightarrow p > 2)$. Do p là số nguyên tố lẻ nên $p > 2$ là đúng).

Từ $2 < 2$ suy ra điều vô lí. Vậy ở trường hợp này giả thiết phản chứng là sai.

2) Nếu n có 2 ước số nguyên tố lẻ khác nhau p và q sao cho $n = p^a q^b$ (có thể cho là $p < q$). Lúc này ta có

$$\begin{aligned} 2 &= \frac{\sigma(n)}{n} = \frac{\sigma(p^a q^b)}{p^a q^b} = \frac{\sigma(p^a)}{p^a} \cdot \frac{\sigma(q^b)}{q^b} \\ &= \frac{1 + p + p^2 + \dots + p^a}{p^a} \cdot \frac{1 + q + q^2 + \dots + q^b}{q^b} \end{aligned}$$

Lập luận như trên suy ra

$$2 < \frac{1}{1 - \frac{1}{p}} \cdot \frac{1}{1 - \frac{1}{q}} \quad (2.22)$$

Vì p và q là hai số nguyên tố lẻ và $p < q$ nên $p \geq 3, q \geq 5$. Vì vậy

$$\frac{1}{1 - \frac{1}{p}} \cdot \frac{1}{1 - \frac{1}{q}} \leq \frac{1}{1 - \frac{1}{3}} \cdot \frac{1}{1 - \frac{1}{5}} = \frac{15}{8} < 2.$$

Thay vào (2.22) ta có $2 < 2$. Điều vô lí này chứng tỏ giả thiết phản chứng trong trường hợp này cũng sai.

Tóm lại giả thiết cho là kết luận của bài toán không đúng là giả thiết sai. Đó chính là điều phải chứng minh.

2.2.3. Chứng minh bất đẳng thức liên quan tới $\sigma(n)$

Ví dụ 2.15. Chứng minh rằng bất đẳng thức: $\sigma(n) > 3n$ đúng với một tập hợp vô hạn các số tự nhiên n .

Lời giải. Rõ ràng nếu d là ước của n thì $\frac{n}{d}$ cũng là một ước số của n . Vì

$$\text{vậy: } \sigma(n) = d_1 + d_2 + \dots + d_k = n \left(\frac{1}{d_1} + \frac{1}{d_2} + \dots + \frac{1}{d_k} \right)$$

ở đây $d_1, d_2, \dots, d_k$ là tất cả các ước tự nhiên của n .

Lấy n là số tùy ý sao cho nó là bội số của số $16! = 1.2.3...15.16$. Dĩ nhiên số những số n như vậy là vô hạn (đó là các số có dạng $k.16!$ với $k = 1, 2, \dots$).

Nói riêng trong các ước của n có $1, 2, 3, \dots, 16$. Vì thế lúc này

$$\sigma(n) = n \left(\frac{1}{d_1} + \frac{1}{d_2} + \dots + \frac{1}{d_k} \right) \geq n \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{16} \right) \quad (2.23)$$

Để ý rằng

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{16} = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4} \right) + \left(\frac{1}{5} + \frac{1}{6} + \dots + \frac{1}{8} \right) + \left(\frac{1}{9} + \frac{1}{10} + \dots + \frac{1}{16} \right)$$

Mặt khác, hiển nhiên ta có

$$\begin{aligned} \frac{1}{3} + \frac{1}{4} &> 2 \cdot \frac{1}{4} = \frac{1}{2}; \\ \frac{1}{5} + \frac{1}{6} + \dots + \frac{1}{8} &> 4 \cdot \frac{1}{8} = \frac{1}{2}; \\ &\dots\dots\dots \\ \frac{1}{9} + \frac{1}{10} + \dots + \frac{1}{16} &> 8 \cdot \frac{1}{16} = \frac{1}{2}. \end{aligned}$$

Do vậy

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{16} > 3 \quad (2.24)$$

Bây giờ từ (2.23) và (2.24) ta đi đến $\sigma(n) > 3n$. Như vậy ta đã chứng minh được rằng tồn tại vô hạn số tự nhiên n , sao cho ta có bất đẳng thức $\sigma(n) > 3n$. Đó là điều phải chứng minh.

Ví dụ 2.16. Cho số tự nhiên $n \geq 1$. Chứng minh rằng ta luôn có bất đẳng thức sau: $\sigma(n) < n\sqrt{n}$.

Lời giải. Xét hai trường hợp sau:

1) Nếu $n = 2^\alpha$. Do $n > 2$ nên α là số nguyên lớn hơn hoặc bằng 2. Rõ ràng lúc này

$$\sigma(n) = \sigma(2^\alpha) = 2^0 + 2^1 + 2^2 + \dots + 2^\alpha = \frac{2^{\alpha+1} - 1}{2 - 1} = 2^{\alpha+1} - 1 \quad (2.25)$$

Vì $\alpha \geq 2$ nên ta có $\sigma(n) = 2^{\alpha+1} - 1 < 2^{\alpha+1} \leq 2^{\alpha+\frac{\alpha}{2}} = 2^\alpha \cdot 2^{\frac{\alpha}{2}} = n\sqrt{n}$

Vậy bất đẳng thức đã cho khi $n > 2$ và n có dạng $n = 2^\alpha$ là đúng.

2) Nếu n không có dạng 2^α (tức n không phải là lũy thừa của 2). ta sẽ chứng minh bằng quy nạp trong trường hợp này.

Do $n > 2$ nên số nhỏ nhất không có dạng 2^α là số 3.

Lúc này $\sigma(3) = 1 + 3 = 4 < 3\sqrt{3}$. Vậy bất đẳng thức đúng khi $n = 3$.

Giả thiết quy nạp $\sigma(k) < k\sqrt{k}$ đã đúng với mọi k , $3 \leq k < n$ và k không có dạng 2^α . Ta sẽ chứng minh:

$$\sigma(n) < n\sqrt{n} \quad (2.26)$$

Vì n không chia hết cho 2 nên n có dạng $n = mp$ trong đó m nguyên dương, p là số nguyên tố lẻ. Dễ thấy

$$1 + p < p\sqrt{p} \quad (2.27)$$

Thật vậy, khi $p = 3$ thì $1 + 3 < 3\sqrt{3}$, còn khi $p \geq 5$, ta có

$$\frac{1+p}{p} = 1 + \frac{1}{p} \leq 1 + \frac{1}{5} < 2.$$

Mặt khác $\sqrt{p} \geq \sqrt{5} > 2 \Rightarrow \frac{1+p}{p} < \sqrt{p}$ hay $1+p < p\sqrt{p}$.

Vậy (2.27) đúng.

Chỉ có các khả năng sau xảy ra:

a) Nếu $m = 1 \Rightarrow n = p$, khi đó p nguyên tố nên $\sigma(n) = \sigma(p) = 1 + p$.
 Từ (2.26) suy ra trong trường hợp này ta có: $\sigma(n) = 1+p < p\sqrt{p} = n\sqrt{n}$.

Vậy (2.26) đúng trong trường hợp này.

b) Nếu $m = 2 \Rightarrow n = 2p$. Do p nguyên tố nên lúc này

$$\sigma(n) = \sigma(2p) = 1 + 2 + p + 2p = 3(1 + p).$$

Vì p là nguyên tố lẻ nên $p \geq 3$. Ta có

$$\begin{aligned} 3 + \frac{3}{p} &\leq 3 + \frac{3}{3} \\ \Rightarrow 3 + \frac{3}{p} &\leq 4. \end{aligned}$$

Lại có: $2\sqrt{2} \cdot \sqrt{p} \geq 2\sqrt{6} > 4$. Vì thế

$$\begin{aligned} 3 + \frac{3}{p} &< 2\sqrt{2} \cdot \sqrt{p} \\ \Rightarrow 3(1+p) &< 2\sqrt{2} \cdot p\sqrt{p} = 2p\sqrt{2p} = n\sqrt{n} \\ \Rightarrow \sigma(n) &< n\sqrt{n}. \end{aligned}$$

Vậy (2.26) đúng trong trường hợp này.

c) Nếu $m \geq 3$. Vì m không có dạng 2^α , nên $m \geq 3$ và $m < n$, nên theo giả thiết quy nạp ta có: $\sigma(m) < m\sqrt{m}$. Ta thấy rằng các ước số của $n = mp$ chỉ có dạng d hoặc dp với d là ước số của m . Vì thế

$$\begin{aligned} \sigma(n) &= \sigma(m) + p\sigma(m) \\ &= (p+1)\sigma(m). \end{aligned}$$

Từ đó đi đến $\sigma(n) < (p+1)m\sqrt{m}$

Lại áp dụng (2.27), ta có $\sigma(n) < p\sqrt{p} \cdot m\sqrt{m} = mp\sqrt{mp} = n\sqrt{n}$.

Vậy (2.26) cũng đúng trong trường hợp này.

Tóm lại khi n không có dạng 2^α , ta cũng luôn có $\sigma(n) < n\sqrt{n}$. Vì lẽ ấy bất đẳng thức $\sigma(n) < n\sqrt{n}$ được chứng minh hoàn toàn.

2.3. Ứng dụng của hàm $S(n)$

2.3.1. Tìm n bởi $S(n)$ thỏa mãn một hệ thức cho trước

Ví dụ 2.17. Tìm số tự nhiên n sao cho $S(n) = n^2 - 2003n + 5$.

Lời giải. Ta có

$$0 < S(n) \leq n \quad (2.28)$$

Giả sử n là số nguyên dương thỏa mãn yêu cầu đề bài, tức là

$$S(n) = n^2 - 2003n + 5.$$

Từ (2.28) đi đến hệ bất phương trình sau (ẩn n)

$$\begin{cases} n^2 - 2003n + 5 > 0 \\ n^2 - 2003n + 5 \leq n \end{cases} \Leftrightarrow \begin{cases} n^2 - 2003n + 5 > 0 & (a) \\ n^2 - 2004n + 5 \leq 0 & (b) \end{cases}$$

Từ (a) suy ra, nói riêng $(n - 1)(n - 2002) > 0$ và tương tự từ (b) ta có $n(n - 2004) < 0$. Vì lẽ đó ta đi đến

$$2002 < n < 2004 \quad (2.29)$$

Từ (2.29) và từ tính nguyên của n ta thu được $n = 2003$.

Đảo lại, nếu $n = 2003$ thì $S(2003) = 2 + 3 = 5$.

Mặt khác, rõ ràng $2003^2 - 2003 \cdot 2003 + 5 = 5$.

Nói cách khác $S(n) = n^2 - 2003n + 5 \Leftrightarrow n = 2003$.

Điều đó có nghĩa là $n = 2003$ là giá trị duy nhất của n thỏa mãn yêu cầu bài toán.

Ví dụ 2.18. Tìm số tự nhiên n sao cho: $n + S(n) = 2003$.

Lời giải. Ta có

$$n + S(n) = 2003 \Leftrightarrow n = 2003 - S(n) \quad (2.30)$$

Vì $S(n) > 0$ và $S(n)$ nguyên, nên $S(n) \geq 1$. Do đó từ (2.30) ta có

$$n \leq 2002 \quad (2.31)$$

Chú ý rằng trong các số không vượt quá số 2002, thì số 1999 có tổng các chữ số lớn nhất. như vậy ta có bất đẳng thức sau

$$S(n) \leq S(1999) = 28 \quad (2.32)$$

đúng với mọi số tự nhiên $n \leq 2002$.

Thay (2.32) vào (2.30) ta có: $n \geq 1975$, kết hợp với (2.31) ta đi đến

$$1975 \leq n \leq 2002. \quad (2.33)$$

Do $S(2002) = 4$; $S(2001) = 3$; $S(2000) = 2$, nên $n = 2002, 2001, 2000$ dĩ nhiên không thỏa mãn hệ thức (2.30), vì thế kết hợp với (2.33), ta có:

$$1975 \leq n \leq 1999 \quad (2.34)$$

Vì lẽ ấy, ta có thể biểu diễn n dưới dạng

$$n = \overline{19ab} \ (a, b \in N), \ 0 \leq a \leq 9, \ 0 \leq b \leq 9.$$

Khi đó hệ thức $n + S(n) = 2003$ có dạng: $1900 + 10a + b + 10 + a + b = 2003$ hay

$$11a + 2b = 93. \quad (2.35)$$

Từ (2.35) ta có $b = \frac{93 - 11a}{2} = 46 - 5a + \frac{1 - a}{2}$

Do b nguyên nên $\frac{1 - a}{2} = t$ hay $a = 1 - 2t$ và $b = 11t + 41$, trong đó t nguyên. Vì a, b là các số nguyên không âm, nhưng không vượt quá 9 nên suy ra hệ thức sau để xác định t

$$\begin{cases} 9 \geq 1 - 2t \geq 0 \\ 9 \geq 11t + 41 \geq 0 \\ t \in \mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} -4 \leq t \leq \frac{1}{2} \\ -\frac{41}{11} \leq t \leq -\frac{32}{11} \\ t \in \mathbb{Z} \end{cases} \Leftrightarrow t = -3$$

Khi $t = -3$ thì $a = 7, b = 8$.

Như vậy nếu n thỏa mãn yêu cầu bài toán thì $n = 1978$.

Đảo lại, nếu $n = 1978$ thì $S(n) = 1 + 9 + 7 + 8 = 25$.

Rõ ràng $n + S(n) = 1978 + 25 = 2003$.

Tóm lại $n = 1978$ là giá trị duy nhất của n thỏa mãn yêu cầu đề ra.

Ví dụ 2.19. *Tìm tất cả các số tự nhiên n thỏa mãn:*

$$n + S(n) + S(S(n)) = 2001.$$

Lời giải. Ta có

$$n < 2001 \implies S(n) \leq S(1999) = 28 \implies S(S(n)) \leq S(28) = 10.$$

Suy ra $n \geq 2001 - 28 - 10 = 1963$.

Từ đó $S(n) \geq S(1970) = 17$ và $S(S(n)) \geq 2$

nên $n \leq 2001 - 17 - 2 = 1982$.

Mặt khác $3n \equiv n + S(n) + S(S(n)) \equiv 2001 \equiv 3 \pmod{9}$

nên $n \equiv 1 \pmod{3}$. Từ đó $n \in \{1963, 1966, 1969, 1972, 1975, 1978, 1981\}$.

Bằng cách thử trực tiếp ta thấy chỉ có các số 1969, 1972, 1975 thỏa mãn.

Như vậy, đáp số của bài toán là $n \in \{1969, 1972, 1975\}$.

Ví dụ 2.20. *Tìm số n nhỏ nhất sao cho trong n số tự nhiên liên tiếp tùy ý luôn chọn được một số N mà $S(N)$ chia hết cho 13.*

Lời giải. Ta chứng minh số cần tìm là 79.

Trước hết ta chứng minh trong 79 số liên tiếp thì luôn chọn được một số N mà $S(N)$ chia hết cho 13. Xét 2 trường hợp:

1) Nếu trong 79 số có số M chia hết cho 100. Khi đó nếu trong 79 số đó có ít nhất 39 số lớn hơn M thì trong 13 số liên tiếp trong các số sau: $S(M), S(M+1), \dots, S(M+9), S(M+19), S(M+29), S(M+39)$ phải có một số chia hết cho 13, còn nếu có ít nhất 40 số nhỏ hơn M thì trong 13 số liên tiếp

$$S(M-40), S(M-39), \dots, S(M-31), S(M-21), S(M-11), S(M-1)$$

cũng phải có một số chia hết cho 13.

2) Nếu trong 79 số không có số nào chia hết cho 100 thì gọi M là số chia hết cho 10 nhỏ nhất trong 79 số. Khi đó trong 13 số liên tiếp

$$S(M), S(M+1), \dots, S(M+9), S(M+19), S(M+29), S(M+39)$$

phải có một số chia hết cho 13.

Cuối cùng có thể kiểm tra 78 số liên tiếp bắt đầu từ 9 999 999 961 không có số N nào để $S(N)$ chia hết cho 13.

2.3.2. Tính giá trị $S(n)$

Ví dụ 2.21. (IMO-1975). Đặt $A = S(4444^{4444})$, và $B = S(A)$. Tìm $S(B)$.

Lời giải. Đặt $N = 4444^{4444}$. Do $N < 10000^{4444}$ nên N có không quá $4444.4 < 20000$ số. Từ đó: $A < 9.20000 = 180000$

$$\Rightarrow B \leq S(99999) = 45 \Rightarrow S(B) \leq 39 = 12 \quad (2.36)$$

Mặt khác $4444 \equiv (-2)(\text{mod } 9)$ nên

$$N \equiv 2^{4444} = 8^{1431}.2 \equiv (-2)(\text{mod } 9) \text{ và do đó } S(B) \text{ chia } 9 \text{ dư } 7. \quad (2.37)$$

Từ (2.36) và (2.37) suy ra $S(B) = 7$.

Ví dụ 2.22. Đặt $a = S\left((2^9)^{1999}\right)$; $b = S(a)$; $c = S(b)$. Tìm c .

Lời giải. Đặt $n = (2^9)^{1999}$ thì $n = (2^3)^{3.1999} = 8^{5997} < 10^{5997}$. Vậy n là một số có không quá 5997 số. Do $\underbrace{99\dots9}_{5997 \text{ số } 9}$ là số lớn nhất có 5997 chữ số.

Từ đó suy ra $a = S(n) \leq S(\underbrace{99\dots9}_{5997 \text{ số } 9}) = 9.5997 = 53973$

Như thế ta có

$$a \leq 53973 \quad (2.38)$$

Trong các số không vượt quá 53973, chữ số 49999 là số có tổng các chữ số lớn nhất. Vì thế từ (2.38) suy ra

$$b = S(a) \leq S(49999) = 40$$

Do vậy

$$b \leq 40 \quad (2.39)$$

Trong các số không vượt quá 40 thì số 39 lại là số có tổng các chữ số lớn nhất. Vì lẽ ấy, từ (2.39) ta thu được: $c = S(b) \leq S(39) = 12$.

Như vậy

$$c \leq 12 \quad (2.40)$$

Theo cách xác định trên thì $n = (2^3)^{5997}$. Do $2^3 \equiv (-1) \pmod{9}$ nên $n \equiv (-1)^{5997} \pmod{9}$ hay $n \equiv (-1) \pmod{9}$, cũng tức là

$$n \equiv 8 \pmod{9} \quad (2.41)$$

Ta có với mọi m tự nhiên thì $m \equiv S(m) \pmod{9}$.

Vì lẽ ấy, từ (2.41) suy ra: $c \equiv b \equiv a \equiv S(n) \equiv n \equiv 8 \pmod{9}$

Tóm lại ta có $0 < c \leq 12$ và $c \equiv 8 \pmod{9}$ nên $c = 8$.

Ví dụ 2.23. (Đề thi QG 2004). Tìm giá trị nhỏ nhất của $S(n)$ khi n chạy trên các bội của 2003.

Nhận xét 2.3. 1) Cho p là số nguyên tố lẻ và có dạng $p = 4k \pm 1$, ta có:

$$2^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}. \quad (2.42)$$

2) 2 là số chính phương $\pmod{p}$, với p nguyên tố lẻ thì điều kiện cần và đủ là

$$p = 8t \pm 1. \quad (2.43)$$

Lời giải.

Đặt $p = 2003$, thì p là số nguyên tố. Rõ ràng n không thể có dạng $100\dots 0$. Thật vậy, khi đó $n = 10^k$ và 10^k không chia hết cho 2003 với mọi k . Vì lẽ đó khi n chạy trên các bội của 2003 thì $S(n) > 1$.

Giả sử tồn tại n là bội của p mà $S(n) = 2$. Vì $S(n) = 2$, nên chỉ có thể xảy ra hai trường hợp sau:

1) Hoặc là $n = 200\dots 0$. Trường hợp này không thể có vì $200\dots 0 = 2 \cdot 10^k$ không chia hết cho 2003.

2) Hoặc là $n = \overline{1a_{q-1}a_{q-2}\dots a_1a_0}$, trong đó các hệ số $a_0, a_1, \dots, a_{q-1}$ có đúng một số bằng 1, còn lại đều bằng 0, tức là n có dạng $n = 10^q + 10^j$ với $0 \leq j < q$.

Theo giả thiết ta có $n : 2003$, tức là

$$10^q \equiv -10^j \pmod{p} \Rightarrow 10^{q-j} \equiv -1 \pmod{p}.$$

Đặt $k = q - j$, thì $10^k \equiv -1 \pmod{p}$

Dễ thấy $2^{10} = 1024 \equiv 10^7 \pmod{p}$ suy ra

$$(2^{5k})^2 = 2^{10k} \equiv 10^{7k} \equiv -1 \pmod{p}$$

Vậy -1 là số chính phương $\pmod{p}$. Theo (2.42), thì p phải có dạng $4k + 1$, suy ra $2003 = 4k + 1 \Rightarrow k = \frac{1001}{2} \notin \mathbb{Z}$

Ta thu được điều vô lí (do $k \notin \mathbb{Z}$).

Vậy $S(n)$ không thể bằng 2, suy ra $S(n) > 2$.

Bây giờ ta sẽ chỉ ra rằng tồn tại n là bội của 3 mà $S(n) = 3$. Ta có

$$10^7 \equiv 2^{10} \pmod{p} \Rightarrow 2 \cdot 10^{700} \equiv 2^{1001} = 2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

(do $p = 2003 \neq 8t \pm 1$) (áp dụng (2.43): 2 là số chính phương $\pmod{p} \Leftrightarrow p$ phải có dạng $8t \pm 1$). Vì $2003 \neq 8t \pm 1$, nên 2 không phải là số chính phương $\pmod{p}$. Theo nhận xét trên, suy ra: $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Từ đó suy ra $(2 \cdot 10^{700} + 1) : p$.

Đặt $n = 2 \cdot 10^{700} + 1$, thì n là bội của 2003 và $S(n) = 3$.

Tóm lại, $\min_{n \in D} S(n) = 3$, ở đây

$$D = \{n : n \text{ nguyên dương và là bội của } 2003\}.$$

Nhận xét 2.4. Ta đã áp dụng các kết quả về số chính phương $\pmod{p}$ để giải bài toán trên.

2.3.3. Chứng minh một số biểu thức liên quan tới $S(n)$

Ví dụ 2.24. Cho n là số tự nhiên bất kỳ. Chứng minh rằng:

$$\frac{S(8n)}{S(n)} \geq \frac{1}{8}.$$

Lời giải. Trước hết ta có nhận xét sau: Nếu n là số nguyên dương thì với mọi số nguyên dương p , ta có hệ thức:

$$S(n) = S(10^p n) \tag{2.44}$$

Thật vậy, giả sử $n = \overline{\alpha_1 \alpha_2 \dots \alpha_k}$ thì $10^p n = \overline{\alpha_1 \alpha_2 \dots \alpha_k \underbrace{00 \dots 0}_{p \text{ số } 0}}$.

Vì thế $S(n) = S(10^p n)$ (vì cùng bằng $\alpha_1 + \alpha_2 + \dots + \alpha_k$), tức là (2.44)

đúng.

Từ (2.44) nói riêng ta có

$$S(n) = S(1000n) = S(125.8n). \quad (2.45)$$

Áp dụng tính chất của hàm $S(n)$ thì

$$S(125.8n) \leq S(125).S(8n) = 8.S(8n) \quad (2.46)$$

Từ (2.45) và (2.46) ta đi đến $S(n) \leq 8S(8n) \Rightarrow \frac{S(8n)}{S(n)} \geq \frac{1}{8}$.

Ví dụ 2.25. Cho số nguyên dương n . Gọi A là tập hợp tất cả các số nguyên a trong $[10^n, 10^{n+1})$ mà $S(a)$ chẵn và B là tập hợp tất cả số nguyên b trong $[10^n, 10^{n+1})$ mà $S(b)$ lẻ. Chứng minh rằng:

$$\sum_{a \in A} a^m = \sum_{b \in B} b^m \text{ với mọi số tự nhiên } m \leq n. \quad (2.47)$$

Lời giải.

Kí hiệu $A(n), B(n)$ là các tập A, B ở đề bài với $n > 0$ và $A(0) = C \setminus \{0\}$, $B(0) = L \setminus \{1\}$ với $C = \{0, 2, 4, 6, 8\}$ và $L = \{1, 3, 5, 7, 9\}$.

Ta chứng minh (2.47) quy nạp với $n \geq 0$.

Với $n = 0$ thì $m = 0$ và (2.47) hiển nhiên đúng. Giả sử (2.47) đã đúng tới với n , ta chứng minh nó cũng đúng với $n + 1$.

Ta có

$$\sum_{a \in A(n+1)} a^m = \sum_{a \in A(n)} \sum_{x \in C} (10a + x)^m + \sum_{b \in B(n)} \sum_{y \in L} (10b + y)^m$$

Từ đó, nếu $m = 0$ thì ta có ngay điều phải chứng minh.

Nếu $0 < m \leq n + 1$ thì

$$\sum_{a \in A(n)} \sum_{x \in C} (10a + x)^m = \sum_{a \in A(n)} 10^m a^m + \sum_{i=0}^{m-1} \left(C_m^i \cdot 10^i \cdot S_i \cdot \sum_{x \in C} x^{m-1} \right)$$

với

$$S_i = \sum_{a \in A(n)} a^i = \sum_{b \in B(n)} b^i \quad \forall i \leq n.$$

$$\sum_{a \in A(n+1)} a^m = \sum_{a \in A(n)} 10^m a^m + \sum_{b \in B(n)} 10^m b^m + \sum_{i=0}^{m-1} \left(C_m^i \cdot 10^i \cdot S_i \cdot \sum_{z \in C \cup L} z^{m-1} \right)$$

Do tính đối xứng nên suy ra $\sum_{a \in A(n+1)} a^m = \sum_{b \in B(n+1)} b^m$.

Theo nguyên lý quy nạp ta có điều phải chứng minh.

Nhận xét 2.5. Có thể phát biểu lại kết quả **Bài toán 2.25** như sau:
 "Cho số nguyên dương n . Gọi A là tập hợp tất cả các số nguyên a trong khoảng $(1, 10^n)$ mà $S(a)$ chẵn và B là tập hợp tất cả các số nguyên b trong khoảng $(1, 10^n)$ mà $S(b)$ lẻ. Chứng minh rằng:

$$\sum_{a \in A} a^m = \sum_{b \in B} b^m \text{ với mọi số tự nhiên } m \leq n.$$

2.3.4. Xét tính bị chặn của hàm số chứa $S(n)$

Ví dụ 2.26. Xét tính bị chặn của hàm số $f(n) = \frac{S(a)}{S(a.n)}$ với $a \in \mathbb{Z}^+$ cho trước.

Lời giải. Đặt $a = 2^\alpha \cdot 5^\beta \cdot b$; $(b, 10) = 1$

$$\text{Nếu } b = 1 \text{ thì } f(n) = \frac{S(n)}{S(a.n)} = \frac{S(10^\alpha \cdot 10^\beta \cdot n)}{S(2^\alpha \cdot 5^\beta \cdot n)} \leq S(5^\alpha \cdot 2^\beta) = \text{const}$$

Nếu $b > 1$ thì gọi p là một ước nguyên tố của b . Ta có

$$f(n) = \frac{S(n)}{S(a.n)} \geq \frac{S(n)}{S(pn) \cdot S(a/p)} \geq \frac{S(n)}{S(pn) \cdot a/p}.$$

Ta chọn dãy $x_n = \frac{10^{n(p-1)}}{p}$ với $0 < c < p$ và $(c+10):p$. Khi đó với n đủ lớn thì $S(x_n \cdot p) = 1 + S(c) = \text{const}$ và để chứng tỏ hàm $f(n)$ không bị chặn ta chỉ cần có $S(x_n) \rightarrow +\infty$ khi $n \rightarrow +\infty$. Do $x_n \rightarrow +\infty$ khi $n \rightarrow +\infty$ nên ta chỉ cần chứng minh trong biểu diễn thập phân của x_n không có chữ số 0 nào.

Thật vậy, nếu ngược lại, dễ thấy rằng px_n có ít nhất 3 chữ số khác 0.

Vậy hàm $f(n)$ bị chặn khi và chỉ khi a không có ước nguyên tố nào ngoài 2 và 5.

Ví dụ 2.27. Cho a là số chẵn nhưng không chia hết cho 5. Chứng minh rằng: $\lim_{n \rightarrow +\infty} S(a^n) = +\infty$.

Lời giải. Lấy $n > 8$, đặt $a^n = \overline{a_k a_{k-1} \dots a_1}$

Ta chứng minh nếu $1 \leq i \leq \frac{n}{4}$ thì trong các chữ số $a_{i+1}, \dots, a_{4i}$ phải có ít nhất một số khác 0.

Thật vậy, vì nếu không thì đặt $c = \overline{a_i a_{i-1} \dots a_1}$ và ta có

$$(a^n - c) : 10^{4i} \Rightarrow c : 2^{4i} \text{ (vì } a \text{ chẵn)}$$

nhưng $0 < c < 10^i < 2^{4i}$ nên mâu thuẫn.

Từ đó lấy $n > 4^m$ thì

$$S(a^n) > (a_2 + a_3 + a_4) + \dots + (a_{4^m+1} + a_{4^m+2} + \dots + a_{4^m+m}) \geq m.$$

Vậy ta có điều phải chứng minh.

2.4. Ứng dụng của hàm số các ước $\tau(n)$

2.4.1. Tìm n thỏa mãn một điều kiện cho trước của $\tau(n)$

Ví dụ 2.28. Tìm n nhỏ nhất để $\tau(n) = 1$. (Giải bài toán khi thay 1 bởi một trong các số sau: 2, 3, 6, 14 và 100).

Lời giải. Ta biết rằng trong các ước dương của n luôn có mặt 1 và n .

1) Xét khi $\tau(n) = 1$. Vì n chỉ có một ước dương nên từ nhận xét trên suy ra $n = 1$. $\tau(n) = 1 \iff n = 1$. Dĩ nhiên số n nhỏ nhất cũng là $n = 1$.

2) Xét khi $\tau(n) = 2$. n chỉ có hai ước khi và chỉ khi n là số nguyên tố. Vậy khi $\tau(n) = 2$ thì n nhỏ nhất là 2 (vì 2 là số nguyên tố bé nhất).

3) Xét khi $\tau(n) = 3$. Ta có nếu trong khai triển ra thừa số nguyên tố $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, ở đây α_i nguyên và lớn hơn 0 ($i = 1, 2, \dots, k$) thì $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$. Vì thế $\tau(n) = 3$ nên suy ra $n = p^2$, với p là số nguyên tố. Do đó khi $\tau(n) = 3$ thì n nhỏ nhất là $2^2 = 4$.

4) Xét khi $\tau(n) = 6$. Ta có $6 = 2.3$, vì thế nên khi $\tau(n) = 6$ thì n có dạng $n = p_1 p_2^2$, trong đó p_1, p_2 là các số nguyên tố. Vậy khi $\tau(n) = 6$ thì n nhỏ nhất là $2^2.3 = 12$.

5) Xét khi $\tau(n) = 14$. Ta có $14 = 2.7$, vì thế khi $\tau(n) = 14$ thì n có dạng

$n = p_1 p_2^6$, trong đó p_1, p_2 là các số nguyên tố. Vậy khi $\tau(n) = 14$ thì n nhỏ nhất là $n = 26.3 = 64.3 = 192$.

6) Xét khi $\tau(n) = 100$. Ta có $100 = 2.50 = 4.25 = 2.2.25 = 2.2.5.5 = 10.10$. Vì vậy $n = p_1 p_2^{49} = p_1^3 p_2^{24} = p_1 p_2 p_3^{24} = p_1 p_2 p_3^4 p_4^4 = p_1^9 p_2^9$, trong đó p_1, p_2, p_3, p_4 là các số nguyên tố.

Số nhỏ nhất trong các số $p_1 p_2^{49}$ là $2^{49}.3$

Số nhỏ nhất trong các số $p_1^3 p_2^{24}$ là $2^{24}.3^3$

Số nhỏ nhất trong các số $p_1 p_2 p_3^4 p_4^4$ là $2^4.3^4.5.7$

Số nhỏ nhất trong các số $p_1^9 p_2^9$ là $2^9.3^9$

Dễ thấy $\min\{3.2^{49}; 3^3.2^{24}; 2^4.3^4.5.7; 2^9.3^9\} = 2^4.3^4.5.7 = 35.6 = 45360$

Vậy khi $\tau(n) = 100$ thì n nhỏ nhất là 45360.

Ví dụ 2.29. Tìm tất cả các số nguyên dương n sao cho $(\tau(n))^3 = 4n$.

Lời giải. Giả sử n là số nguyên dương thỏa mãn điều kiện:

$$(\tau(n))^3 = 4n \quad (2.48)$$

Giả sử trong khai triển ra thừa số nguyên tố của n , ta có

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \dots$ ở đây $p_1 < p_2 < \dots < p_s < \dots$ là tất cả các số nguyên tố, còn $\alpha_i, i = 1, 2, \dots$ là các số nguyên không âm. Khi đó ta có

$$\tau(n) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_s) \dots \quad (2.49)$$

Ta có $4n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \dots$ Do $p_1 = 2$ nên

$$4n = p_1^{2+\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \dots \quad (2.50)$$

Từ (2.48) suy ra $4n$ là lập phương của một số nguyên. Vì thế từ (2.50)

và do p_i là các số nguyên tố nên ta có $\begin{cases} \alpha_1 = 1 + 3\beta_1 \\ \alpha_i = 3\beta_i, i = 2, 3, \dots \end{cases}$

ở đây $\beta_1, \beta_2, \dots$ là các số nguyên lớn hơn hoặc bằng 0. Thay vào (2.49) ta có

$$\tau(n) = (2 + 3\beta_1)(1 + 3\beta_2)(1 + 3\beta_3) \dots (1 + 3\beta_s) \dots \quad (2.51)$$

Từ (2.51) suy ra $\tau(n)$ không chia hết cho 3 (vì $\tau(n) \equiv 2 \pmod{3}$).

Mặt khác, lại có $4n = (\tau(n))^3$ nên suy ra n không chia hết cho 3.

Vì $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \dots$, ở đây $p_2 = 3$. Do n không chia hết cho 3 nên $\alpha_2 = 0$ (vì nếu $\alpha_2 > 0$ thì $p_2^{\alpha_2}$ chia hết cho 3, tức là n chia hết cho 3, dẫn đến vô lí). Vì lẽ đó từ (2.51), lại có

$$\tau(n) = (2 + 3\beta_1)(1 + 3\beta_3) \dots (1 + 3\beta_s) \dots$$

Bây giờ phương trình

$$\begin{aligned} (\tau(n))^3 = 4n &\Leftrightarrow (2 + 3\beta_1)^3 (1 + 3\beta_3)^3 \dots (1 + 3\beta_s)^3 \dots = 2^{3(1+\beta_1)} p_3^{3\beta_3} \dots p_s^{3\beta_s} \dots \\ &\Leftrightarrow \frac{2 + 3\beta_1}{2^{1+\beta_1}} = \frac{p_3^{\beta_3} \dots p_s^{\beta_s} \dots}{(1 + 3\beta_3) \dots (1 + 3\beta_s) \dots} \end{aligned} \quad (2.52)$$

Vì $5 = p_3 < p_4 < \dots < p_s < \dots$ nên với mọi $i \geq 3$ thì

$$p_i^{\beta_i} \geq 5^{\beta_i} = (1 + 4)^{\beta_i} \geq 1 + 4^{\beta_i}$$

(theo bất đẳng thức Bernoulli, thì $(1 + a)^n \geq 1 + na$ với mọi n nguyên dương). Từ đó suy ra vế phải của (2.52) lớn hơn hoặc bằng 1, và đẳng thức xảy ra khi và chỉ khi $\beta_i = 0$ với mọi $i \geq 3$. Vì lẽ đó từ (2.52), ta có

$$\frac{2 + 3\beta_1}{2^{1+\beta_1}} \geq 1 \quad (2.53)$$

Từ (2.53) suy ra

$$2 + 3\beta_1 \geq 2^{1+\beta_1} \quad (2.54)$$

Mặt khác

$$2^{1+\beta_1} = 2(1 + 1)^{\beta_1} \geq 2(1 + C_{\beta_1}^1 + C_{\beta_1}^2) = 2 \left(1 + \beta_1 + \frac{\beta_1(\beta_1 - 1)}{2} \right)$$

hay từ (2.54) ta có $2 + 3\beta_1 \geq 2 + \beta_1 + 2\beta_1^2$ (ở đây đã sử dụng công thức khai triển nhị thức Newton). Từ đó ta có $2\beta_1 \geq \beta_1^2$ hay $\beta_1 \leq 2$. Từ tính nguyên của β_1 , có $\beta_1 = 0, 1$ hay 2 . Xét các trường hợp sau:

a) Nếu $\beta_1 = 0$ hay $\beta_1 = 2$ thì: $\frac{2 + 3\beta_1}{2^{1+\beta_1}} = 1$

Do đó suy ra cả hai vế của (2.52) bằng 1, vì lẽ đó từ lập luận trên suy ra 2 là ước số nguyên duy nhất của n . Từ đó:

- Nếu $\beta_1 = 0$, ta được nghiệm $n = 2^{1+3\beta_1} = 2$.
- Nếu $\beta_1 = 2$, ta được nghiệm $n = 2^{1+3\beta_1} = 2^7 = 128$.

b) Nếu $\beta_1 = 1$ thì $\frac{2+3\beta_1}{2^{1+\beta_1}} = \frac{5}{4}$

Khi đó từ (2.52) ta có $\beta_3 > 0$ nhưng $\beta_3 > 1$ không thể có. Thật vậy, khi đó $\frac{5^{\beta_3}}{1+3\beta_3} > \frac{5}{4}$, suy ra vế phải của (2.52) $> \frac{5}{4}$ và mâu thuẫn so với

(2.52). Vì lẽ đó $\beta_3 = 1$, thế thì $\frac{5^{\beta_3}}{1+3\beta_3} = \frac{5^1}{1+3} = \frac{5}{4}$ (và dĩ nhiên để (2.52) đúng thì $\beta_4 = \beta_5 = \dots = 0$). Từ đó ta có

$$\begin{cases} \alpha_1 = 1 + 3\beta_1 = 1 + 3.1 = 4 \\ \alpha_2 = 0 \\ \alpha_3 = 3\beta_3 = 3 \\ \alpha_i = 0, \forall i \geq 4 \end{cases}$$

Như vậy $n = 2^4.5^3 = 16.125 = 2000$.

Tóm lại các số nguyên dương cần tìm là $n = 2, n = 128$ và $n = 2000$.

2.4.2. Một số bất đẳng thức liên quan tới hàm $\tau(n)$

Ví dụ 2.30. Giả sử $\tau(n)$ là số tất cả các ước số tự nhiên của n . Chứng minh rằng với mọi $n = 1, 2, \dots$ ta có bất đẳng thức: $\tau^2(n) < 4n$.

Lời giải. Giả sử a là ước số của n , thì số $b = \frac{n}{a}$ cũng là ước của n . Do đó tất cả các ước số của n được chia thành từng cặp, khi đặt tương ứng với mỗi ước $a < \sqrt{n}$ và $b = \frac{n}{a}$. Ngoài ra, có thể thêm $\sqrt{n}$ nếu $\sqrt{n}$ là số nguyên (tức là khi n là số chính phương). Số nhỏ trong hai số của cặp gọi là số thứ nhất, còn lại số lớn gọi là số thứ hai. Xét hai khả năng sau:

1) Nếu n không phải là số chính phương.

Khi đó tất cả các số thứ nhất sẽ nhỏ hơn $\sqrt{n}$. Cũng vì lẽ đó nếu gọi d^* là số lớn nhất trong các số thứ nhất thì $d^* < \sqrt{n} \Rightarrow d^* < [\sqrt{n}]$, ở đây qua $[\alpha]$ để chỉ phần nguyên của số α .

Vì mọi số thứ nhất thuộc tập $\{1, 2, \dots, [\sqrt{n}]\}$, từ đó suy ra số các số thứ nhất $\leq [\sqrt{n}] < \sqrt{n}$ (do n không phải là số chính phương). Vì n không phải là số chính phương nên $\tau(n)$ bằng hai lần các số thứ nhất. Do vậy

ta có bất đẳng thức: $\tau(n) < 2\sqrt{n} \Rightarrow \tau^2(n) < 4n$.

2) Nếu n là số chính phương.

Khi đó $\sqrt{n}$ là ước của n , và tất cả các ước thứ nhất $\leq \sqrt{n} - 1$. Ký hiệu d^* như trong phần 1), ta có

$$d^* \leq \sqrt{n} - 1 \Rightarrow d^* \leq [\sqrt{n} - 1]$$

Lập luận như trên ta có số các số thứ nhất $\leq [\sqrt{n} - 1] \leq \sqrt{n} - 1$.

Khi n là số chính phương, thì $\tau(n)$ bằng hai lần số các số thứ nhất cộng thêm 1. Vì lẽ đó suy ra

$$\tau(n) < 2(\sqrt{n} - 1) + 1 \Rightarrow \tau(n) < 2\sqrt{n} - 1 < 2\sqrt{n} \Rightarrow \tau^2(n) < 4n.$$

Tóm lại, ta luôn luôn chứng minh được rằng với mọi $n = 1, 2, \dots$ thì $\tau^2(n) < 4n$. Đó là điều phải chứng minh.

Ví dụ 2.31. Chứng minh rằng, tồn tại n thỏa mãn: $\tau(n^2) = k\tau(n)$ khi và chỉ khi k là số lẻ.

Lời giải. Trước tiên, ta chỉ ra rằng, nếu tồn tại n để

$$\tau(n^2) = k\tau(n) \tag{2.55}$$

khi k là số lẻ.

Nếu $n = 1$ thì $\tau(n) = \tau(n^2) = 1 \Rightarrow k = 1$.

Giả sử $n > 1$, $n = p_1^{r_1} \dots p_s^{r_s}$ là khai triển n thành thừa số nguyên tố. Khi đó: $n^2 = p_1^{2r_1} \dots p_s^{2r_s}$.

Phương trình (2.55) cho ta

$$(2r_1 + 1) \dots (2r_s + 1) = k(r_1 + 1) \dots (r_s + 1) \tag{2.56}$$

Vậy k là số lẻ.

Ngược lại, giả sử $k = 2m + 1$. Ta chứng minh sự tồn tại n thỏa mãn (2.55) bằng quy nạp theo m . Sự tồn tại n tương đương với sự tồn tại $(r_1, \dots, r_s)$ thỏa mãn (2.56).

Với $m = 1$, ta có $2m + 1 = 3 = \frac{(2 \cdot 4 + 1)(2 \cdot 2 + 1)}{(4 + 1)(2 + 1)}$.

Giả sử với mọi $m < M$, mỗi số $k = 2m + 1$ đều có thể biểu diễn dưới dạng (2.56). Ta chứng minh $k = 2M + 1$ cũng có dạng đó.

Giả sử $k + 1 = 2^l \cdot t$, trong đó t lẻ. Khi đó ta có: $t = \frac{k+1}{2^l} \leq \frac{k+1}{2} < k$ vì $l \geq 1, k > 1$. Xét các số $r_1, \dots, r_l$ như sau

$$\begin{aligned} r_1 &= 2^l \cdot t - 2^0 \cdot t - 2^0 \\ r_2 &= 2^{l+1} \cdot t - 2^1 \cdot t - 2^1 \\ &\dots \\ r_l &= 2^{l+l-1} \cdot t - 2^{l-1} \cdot t - 2^{l-1}. \end{aligned}$$

Xét $n_1 = p_1^{r_1} \dots p_l^{r_l}$. Khi đó ta có

$$\begin{aligned} k &= \frac{\tau(n_1^2)}{\tau(n_1)} = \frac{(2^{l+1} \cdot t - 2^1 \cdot t - 2^1 + 1) \dots (2^{l+1} \cdot t - 2^l \cdot t - 2^l + 1)}{(2^l \cdot t - 2^0 \cdot t - 2^0 + 1) \dots (2^{l+l-1} \cdot t - 2^{l-1} \cdot t - 2^{l-1} + 1)} \\ &= \frac{2^{2l} \cdot t - 2^l \cdot t - 2^l + 1}{2^l \cdot t - 2^0 \cdot t - 2^0 + 1} = \frac{(2^l - 1)(2^l \cdot t - 1)}{(2^l - 1)t} = \frac{2^l \cdot t - 1}{t} \end{aligned}$$

Vì $1 < k$ nên theo giả thiết quy nạp, tồn tại số $n_2 = q_1^{a_1} \dots q_s^{a_s}$ sao cho

$$t = \frac{\tau(n_2^2)}{\tau(n_2)}.$$

Bằng cách chọn các số $q_1, \dots, q_s, p_1, \dots, p_l$ là các số nguyên tố khác nhau và đặt $n = n_1 \cdot n_2$, ta có: $\frac{\tau(n^2)}{\tau(n)} = \frac{\tau(n_1^2)}{\tau(n_1)} \cdot \frac{\tau(n_2^2)}{\tau(n_2)} = k_1 \cdot t = 2^l \cdot t - 1 = k$.

2.4.3. Tìm số nghiệm của phương trình bằng phương pháp sử dụng $\tau(n)$

Ví dụ 2.32. Chứng minh rằng với mọi $k > 1$, phương trình $\tau(n) = k$ có vô số nghiệm.

Lời giải. Ta có công thức: $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$, nếu $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, trong đó p_i là các số nguyên tố và α_i nguyên ≥ 1 , $\forall i = 1, 2, \dots, k$.

Xét hai khả năng sau:

1) Nếu k là số nguyên tố.

Khi đó từ $\tau(n) = k$ suy ra $n = p^{k-1}$, ở đây p là số nguyên tố. Do tập

hợp số nguyên tố là vô hạn, nên tồn tại vô hạn số nguyên dương có dạng $n = p^{k-1}$. Điều đó có nghĩa là phương trình $\tau(n) = k$ có vô số nghiệm khi k là số nguyên tố.

2) Nếu k là hợp số.

Khi đó ta có biểu diễn $k = k_1 \cdot k_2$, trong đó $k_1 > 1, k_2 > 1$. Từ $\tau(n) = k$, nên suy ra một trong các dạng của n là $n = p_1^{k_1-1} \cdot p_2^{k_2-1}$, ở đây p_1, p_2 là các số nguyên tố. Do tập hợp các số nguyên tố p_1, p_2 là vô hạn nên tồn tại vô hạn các số nguyên dương có dạng $n = p_1^{k_1-1} \cdot p_2^{k_2-1}$.

Tóm lại với mọi k nguyên dương lớn hơn 1, thì phương trình $\tau(n) = k$ có vô số nghiệm. Đó là điều phải chứng minh.

2.5. Ứng dụng của hàm phần nguyên $[x]$

2.5.1. Bài toán định tính

Ví dụ 2.33. Chứng minh rằng với mọi số nguyên n ,

$$\left[\frac{n+2}{4} \right] + \left[\frac{n+4}{4} \right] + \left[\frac{n-1}{2} \right] = n.$$

Lời giải. Xét $n = 4k$ ta có

$$\left[\frac{n+2}{4} \right] = k; \left[\frac{n+4}{4} \right] = k+1; \left[\frac{n-1}{2} \right] = 2k-1.$$

Do đó

$$\left[\frac{n+2}{4} \right] + \left[\frac{n+4}{4} \right] + \left[\frac{n-1}{2} \right] = n$$

Xét $n = 4k+1$ ta có

$$\left[\frac{n+2}{4} \right] = k; \left[\frac{n+4}{4} \right] = k+1; \left[\frac{n-1}{2} \right] = 2k$$

Do đó

$$\left[\frac{n+2}{4} \right] + \left[\frac{n+4}{4} \right] + \left[\frac{n-1}{2} \right] = n$$

Tương tự với $n = 4k+2, 4k+3$ ta cũng có điều phải chứng minh.

Ví dụ 2.34. Cho m, n là các số nguyên, c là một số vô tỷ dương và $d = \frac{1}{c}$. Chứng minh rằng:

$$\sum_{j=0}^{[m+nc]} [n+1+(m-j)d] = \sum_{j=0}^{[n+md]} [m+1+(n-j)c].$$

Lời giải. Trong mặt phẳng Oxy xét hai điểm $A(0, m+nc)$ và $B(n+md, 0)$. Xét số điểm nguyên nằm trong tam giác OAB theo hai cách.

Cách thứ nhất, với mỗi số nguyên j , $0 \leq j \leq [n+md]$ ta tính số các số nguyên i sao cho điểm (j, i) nằm trong tam giác OAB (coi j tương ứng với điểm $(j, 0)$ trên OB). Đặt $x_0 = n+md, y_0 = m+nc$, khi đó đường thẳng có phương trình $x = j$ cắt đoạn AB tại điểm có tung độ bằng

$$\begin{aligned} \frac{(x_0 - j)y_0}{x_0} &= \frac{(n+md-j)(m+nc)}{n+md} \\ &= \frac{(n + \frac{m}{c} - j)(n + \frac{m}{c})c}{n + \frac{m}{c}} \\ &= m + (n-j)c. \end{aligned}$$

Do đó, số các số nguyên i để điểm (j, i) nằm trong tam giác OAB là:

$$1 + [m + (n-j)c] = [m+1+(n-j)c]$$

Từ đó suy ra số điểm nguyên (j, i) nằm trong tam giác OAB là:

$$N = \sum_{0 \leq j \leq [n+md]} [m+1+(n-j)c].$$

Cách thứ hai, với mỗi số nguyên i , $0 \leq i \leq [m+nc]$ ta tính số các số nguyên j sao cho điểm (j, i) nằm trong tam giác OAB (coi i tương ứng với điểm $(0, i)$ trên OA). Bằng cách tính hoàn toàn tương tự ta có số các điểm nguyên (j, i) nằm trong tam giác OAB là

$$N = \sum_{0 \leq i \leq [m+nc]} [n+1+(m-j)d].$$

Từ đó suy ra điều phải chứng minh.

Ví dụ 2.35. Cho n là số nguyên dương thỏa mãn $n!$ có đúng 2002 chữ số 0 tận cùng. Chứng minh rằng: $n \leq 8024$.

Lời giải. Giả sử $n! = 2^\alpha 5^\beta q$, trong đó $(q, 2) = (q, 5) = 1$. Theo công thức Polignac, ta có: $\alpha = \sum_{i=1}^{\infty} \left[\frac{n}{2^i} \right] > \beta = \sum_{i=1}^{\infty} \left[\frac{n}{5^i} \right]$.

Do đó $n! : 10^\beta$, $n!$ không chia hết cho $10^{\beta+1}$ nên số chữ số 0 đứng tận cùng trong biểu diễn thập phân của n là β . Vậy ta cần tìm n nhỏ nhất sao cho

$$\beta = \sum_{i=1}^{\infty} \left[\frac{n}{5^i} \right] = 2002.$$

Với mỗi n đặt $p(n) = \sum_{i=1}^{\infty} \left[\frac{n}{5^i} \right]$. Ta có $p(n) \leq p(n+1)$ với mọi $n \geq 1$ và

$$\begin{aligned} p(8024) &= \left[\frac{8024}{5} \right] + \left[\frac{8024}{25} \right] + \left[\frac{8024}{125} \right] + \left[\frac{8024}{625} \right] + \left[\frac{8024}{3125} \right] \\ &= 1604 + 320 + 64 + 12 + 2 = 2002. \end{aligned}$$

Do đó $n \leq 8024$, điều phải chứng minh.

Ví dụ 2.36. Cho $a_1, a_2, \dots, a_k$ là các số nguyên dương không vượt quá n thỏa mãn điều kiện: $[a_i, a_j] > n$ với mọi $1 \leq i \neq j \leq k$.

Chứng minh rằng: $\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_k} < 2$.

Lời giải. Phân hoạch tập $S = \{1, 2, \dots, n\}$ thành k tập $S_1, S_2, \dots, S_k$ thỏa mãn: $S_i = \left\{ s \in S \mid s : a_i \right\}$ với mọi $i = 1, 2, \dots, k$.

Ta sẽ chứng minh $S_i \cap S_j = \emptyset$ với mọi $1 \leq i \neq j \leq k$. Thật vậy, giả sử tồn tại $s \in S_i \cap S_j$ khi đó $s : a_i$ và $s : a_j$ nên $a : [a_i, a_j] > n$ vô lý. Vậy các tập $S_1, S_2, \dots, S_k$ đôi một rời nhau. Do đó: $\sum_{i=1}^k |S_i| = \sum_{i=1}^k \left[\frac{n}{a_i} \right] < n$.

$$\text{Từ đó, } \sum_{i=1}^k \frac{n}{a_i} < \sum_{i=1}^k \left(\left[\frac{n}{a_i} \right] + 1 \right) < n + k < 2n$$

Điều phải chứng minh.

Ví dụ 2.37. (Taiwan 1998). Chứng minh rằng với mọi số nguyên dương m và n , ta luôn có: $(m, n) = 2 \sum_{k=0}^{m-1} \left[\frac{kn}{m} \right] + m + n - mn$.

Lời giải. Đặt $d = (m, n)$, $m = dm'$, $n = dn'$ ta có m', n' là các số nguyên dương nguyên tố cùng nhau. Ta có

$$\left[\frac{kn}{m} \right] + \left[n - \frac{kn}{m} \right] = \begin{cases} n - 1 & \text{nếu } \frac{kn}{m} \text{ không là một số nguyên} \\ n & \text{nếu } \frac{kn}{m} \text{ là một số nguyên} \end{cases}$$

Mặt khác $\frac{kn}{m} = \frac{kn'}{m'}$ là một số nguyên khi và chỉ khi k chia hết cho m' .

Do đó, trong tập hợp $\{1, 2, \dots, m-1\}$ có $\left[\frac{m-1}{m'} \right] = \left[d - \frac{1}{m'} \right] = d-1$ giá trị của k sao cho $\frac{kn}{m}$ là một số nguyên. Ta có

$$\begin{aligned} 2 \sum_{k=0}^{m-1} \left[\frac{kn}{m} \right] &= 2 \sum_{k=1}^{m-1} \left[\frac{kn}{m} \right] \\ &= \sum_{k=1}^{m-1} \left(\left[\frac{kn}{m} \right] + \left[n - \frac{kn}{m} \right] \right) \\ &= mn - m - n + d. \end{aligned}$$

Suy ra $(m, n) = d = 2 \sum_{k=0}^{m-1} \left[\frac{kn}{m} \right] + m + n - mn$.

Điều phải chứng minh.

Ví dụ 2.38. (Vô địch toán quốc tế, 1972). Với số nguyên dương m, n .

Chứng minh rằng: $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ là một số nguyên.

Lời giải. Trước tiên, ta chứng minh:

$$[2\alpha] + [2\beta] \geq [\alpha] + [\beta] + [\alpha + \beta] \quad (2.57)$$

với α, β là các số thực.

Thật vậy, ta có

$$\begin{aligned} [2\alpha] &= [2[\alpha] + 2\{\alpha\}] = 2[\alpha] + [2\{\alpha\}] \\ [2\beta] &= [2[\beta] + 2\{\beta\}] = 2[\beta] + [2\{\beta\}] \\ [\alpha + \beta] &= [\alpha] + [\beta] + [\{\alpha\} + \{\beta\}] \end{aligned}$$

Bất đẳng thức (2.57) tương đương với bất đẳng thức

$$[2\{\alpha\}] + [2\{\beta\}] \geq [\{\alpha\} + \{\beta\}] \quad (2.58)$$

Vì $0 \leq \{\alpha\} + \{\beta\} < 2$ nên xảy ra hai trường hợp sau:

1) Nếu $0 \leq \{\alpha\} + \{\beta\} < 1$ thì (2.58) luôn đúng vì vế trái lớn hơn hoặc bằng 0.

2) Nếu $1 \leq \{\alpha\} + \{\beta\} < 2$ thì $[\{\alpha\} + \{\beta\}] = 1$. Khi đó $\{\alpha\} \geq \frac{1}{2}$ hoặc $\{\beta\} \geq \frac{1}{2}$, giả sử $\{\alpha\} \geq \frac{1}{2}$. Suy ra $2\{\alpha\} \geq 1 \Rightarrow [2\{\alpha\}] + [2\{\beta\}] \geq 1$.

Vậy (2.57) được chứng minh.

Bây giờ, Ta chứng tỏ rằng với mọi số nguyên tố p , số các thừa số p chứa trong tích $(2m)!(2n)!$ không nhỏ hơn các thừa số p chứa trong tích $m!n!(m+n)!$.

Gọi S_1, S_2 lần lượt là các số thừa số p chứa trong tích $(2m)!(2n)!$ và $m!n!(m+n)!$. Ta có

$$S_1 = \left[\frac{2m}{p} \right] + \left[\frac{2m}{p^2} \right] + \dots + \left[\frac{2n}{p} \right] + \left[\frac{2n}{p^2} \right] + \dots$$

$$S_2 = \left[\frac{m}{p} \right] + \left[\frac{m}{p^2} \right] + \dots + \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \dots + \left[\frac{m+n}{p} \right] + \left[\frac{m+n}{p^2} \right] + \dots$$

Để chứng tỏ $S_1 \geq S_2$ ta phải chứng minh với k tự nhiên bất kỳ ta có

$$\left[\frac{2m}{p^k} \right] + \left[\frac{2n}{p^k} \right] \geq \left[\frac{m}{p^k} \right] + \left[\frac{n}{p^k} \right] + \left[\frac{m+n}{p^k} \right]$$

Bất đẳng này được suy ra từ bất đẳng thức (2.57) ở trên với $\alpha = \frac{m}{p^k}$ và $\beta = \frac{n}{p^k}$.

2.5.2. Bài toán định lượng

Ví dụ 2.39. Cho $M = 19871987$, dãy $\{x_n\}_{n \geq 1}$ là các số nguyên thỏa

$$\text{mãn: } x_1 = M, x_{n+1} = \left\lfloor \frac{x_n + \left\lfloor \frac{M}{x_n} \right\rfloor}{2} \right\rfloor, \text{ với mọi } n = 1, 2, \dots$$

Tính $\min \{x_n : 1 \leq n \leq M\}$.

Lời giải. Đặt $\left[\sqrt{M} \right] = \alpha$, khi đó $\alpha \in \mathbb{Z}^+, \alpha^2 \leq M < (\alpha + 1)^2$.

Ta có: $\left[\frac{a + [b]}{2} \right] = \left[\frac{a + b}{2} \right]$ nên $x_{n+1} = \left[\frac{x_n + \frac{M}{x_n}}{2} \right] \geq \left[\sqrt{M} \right] = \alpha$.

do $M < (\alpha + 1)^2$ nên nếu $x_n \geq \alpha + 1$ thì

$$M/x_n < x_n \text{ và } x_{n+1} = \left[\frac{x_n + \frac{M}{x_n}}{2} \right] < \left[\frac{x_n + x_n}{2} \right] = x_n$$

Tức là, nếu $x_n \geq \alpha + 1$ thì $x_{n+1} \leq x_n - 1$. Từ đó suy ra

$$\min \{x_n : 1 \leq n \leq M\} = \alpha.$$

Ví dụ 2.40. *Tìm số nguyên dương n lớn nhất sao cho $2003!$ chia hết cho 5^n .*

Lời giải. Hiển nhiên số n cần tìm chính là số mũ của 5 trong phân tích $2003!$ thành tích các thừa số nguyên tố. Theo công thức Polignac,

$$\begin{aligned} n &= \sum_{i=1}^{\infty} \left[\frac{2003}{5^i} \right] = \left[\frac{2003}{5} \right] + \left[\frac{2003}{25} \right] + \left[\frac{2003}{125} \right] + \left[\frac{2003}{625} \right] \\ &= 400 + 80 + 16 + 3 = 499 \end{aligned}$$

Vậy $n = 499$ là số cần tìm.

Ví dụ 2.41. *(Canada 1998). Tìm số các nghiệm thực của phương trình:*

$$\left[\frac{a}{2} \right] + \left[\frac{a}{3} \right] + \left[\frac{a}{5} \right] = a.$$

Lời giải. Vì vế phải là một số nguyên nên a cũng phải là một số nguyên. Đặt $a = 30q + r$ trong đó q, r là các số nguyên, $0 \leq r \leq 29$. Ta có phương trình đã cho tương đương với phương trình sau

$$31q + \left[\frac{r}{2} \right] + \left[\frac{r}{3} \right] + \left[\frac{r}{5} \right] = 30q + r.$$

hay $q = r - \left(\left\lfloor \frac{r}{2} \right\rfloor + \left\lfloor \frac{r}{3} \right\rfloor + \left\lfloor \frac{r}{5} \right\rfloor \right)$.

Như vậy, với mỗi giá trị của r tồn tại duy nhất một giá trị của q sao cho $a = 30q + r$ thỏa mãn phương trình đã cho. Do r có thể nhận 30 giá trị (từ 0 đến 29) nên phương trình đã cho có 30 nghiệm.

Ví dụ 2.42. (Czeck-Slovak 1998). Tìm tất cả các số thực x thỏa mãn:

$$x[x[x[x]]] = 88.$$

Lời giải. Đặt $f(x) = x[x[x[x]]]$ với mọi số thực x .

Trước hết ta chứng minh rằng: $|f(a)| > |f(b)|$ với mọi $a, b \in \mathbb{R}$ thỏa mãn $ab > 0, |a| > |b| > 1$.

Thật vậy, từ $ab > 0, |a| > |b| > 1$ suy ra $[a] \geq [b] \geq 1$

Nhân $|a| > |b| > 1$ vào ta có $[a[a]] \geq [b[b]] \geq 1$

Dễ thấy $a[a]$ cùng dấu với $b[b]$, $a[a[a]]$ cùng dấu với $b[b[b]]$ nên tương tự như trên ta có

$$[a[a[a]]] \geq [b[b[b]]] \geq 1, [a[a[a[a]]]] \geq [b[b[b[b]]]] \geq 1$$

Từ đó suy ra $|f(a)| > |f(b)|$.

Vì $f(x) = 0$ với mọi $|x| < 1$, $f(\pm 1) = 1$ nên nếu $f(x_0) = 88$ thì $|x_0| > 1$.

Xét hai trường hợp sau:

Trường hợp 1: $x_0 > 1$. Từ chứng minh trên $f(x)$ đơn điệu tăng trên khoảng $(1, \infty)$ nên nếu tồn tại thì x_0 là duy nhất. Ta có

$$f(3) = 81 < 88 = f(x_0) < f(4) = 256$$

nên $3 < x_0 < 4$ và $[x_0] = 3$. Từ đó, $f(x_0) = x_0[x_0[3x_0]] = 88$.

Mặt khác $f(3) = 81 < 88 = f(x_0) < f\left(\frac{10}{3}\right) = 110$

nên $3 < x_0 < 10/3$ suy ra $[x_0[x_0]] = 9$.

Tiếp tục, $f(3) = 81 < 88 = f(x_0) < f\left(\frac{29}{9}\right) = \frac{29^2}{9}$ nên $3 < x_0 < 29/9$.

Do đó $27 < [x_0[x_0[x_0]]] = [9x_0] < 29 = \left\lceil 9\frac{29}{9} \right\rceil$

suy ra $[x_0[x_0[x_0]]] = 28$. Từ đó $f(x_0) = 28x_0 = 88$ nên $x_0 = 22/7$

Trường hợp 2: $x_0 < -1$. Từ chứng minh trên, $f(x)$ đơn điệu giảm trên khoảng $(-\infty, -1)$. Tương tự trường hợp 1, ta có

$$|f(-3)| = 81 < 88 = f(x_0) < \left| f\left(\frac{-112}{37}\right) \right| = 112$$

nên $-3 > x_0 > -112/37$ và $[x_0 [x_0 [x_0]]] = -37$.

Từ đó suy ra $x = -\frac{88}{37} > -3$, vô lý. Vậy không tồn tại nghiệm $x_0 < -1$.

Tóm lại, tồn tại duy nhất nghiệm $x_0 = \frac{22}{7}$.

Ví dụ 2.43. (Korea 1997). Biểu diễn $\sum_{k=1}^n [\sqrt{k}]$ theo n và $a = [\sqrt{n}]$.

Lời giải. Dễ dàng thấy rằng $[\sqrt{k}] = \sum_{j=1}^a [j^2 \leq k]$

vì nếu $1 \leq k \leq n$ thì $[\sqrt{k}] \leq [\sqrt{n}] = a$. Từ đó, ta có

$$\sum_{k=1}^n [\sqrt{k}] = \sum_{k=1}^n \sum_{j=1}^a [j^2 \leq k] = \sum_{j=1}^a \sum_{k=1}^n [j^2 \leq k]$$

Vì $\sum_{k=1}^n [j^2 \leq k]$ chứa số các số $k \in \{1, 2, \dots, n\}$ thỏa mãn $k \geq j^2$, và do $j \leq a$ kéo theo $j^2 \leq n$ nên số các số này là $n + 1 - j^2$. Theo đẳng thức trên ta có

$$\sum_{k=1}^n [\sqrt{k}] = \sum_{j=1}^a (n + 1 - j^2) = (n + 1)a - \frac{a(a + 1)(2a + 1)}{6}.$$

Trên đây là một số dạng bài toán cơ bản của số học trong chương trình phổ thông. Việc phân chia các bài toán qua các ứng dụng cơ bản giúp cho việc hình thành tư duy về số học một cách thuận lợi hơn.

Kết luận

Luận văn trình bày một số ứng dụng cơ bản của các hàm số học.

Luận văn đã trình bày và đạt được một số kết quả sau thông qua 2 chương.

1. Chương 1 đã trình bày được những lý thuyết cơ bản của các hàm số học.
2. Chương 2 đã nêu được các ứng dụng của các hàm số học cơ bản. Và qua đó tạo được tư duy trong việc phân hoạch các dạng toán của các hàm số học. Sự phân hoạch đó đem lại một cách tư duy cho người học bằng cách tự mình có thể phân chia lại các ứng dụng hoặc bổ sung hoàn chỉnh cho phần ứng dụng đó.
3. Thông qua phần lý thuyết và các ứng dụng cơ bản của các hàm số học đem lại cách nhìn cụ thể hơn đối với các hàm số học trong các bài toán sơ cấp ở phổ thông.

Tài liệu tham khảo

- [1] Phan Huy Khải - *Chuyên đề 3: Các bài toán về hàm số học* - NXB Giáo dục, tháng 3 năm 2009.
- [2] Phan Huy Khải - *Chuyên đề 4: Các bài toán về hàm số học* - NXB Giáo dục, tháng 3 năm 2009.
- [3] Hà Huy Khoái - *Chuyên đề bồi dưỡng học sinh giỏi toán trung học phổ thông Số học* - NXB Giáo dục, 2003.
- [4] Nguyễn Vũ Lương - Nguyễn Lưu Sơn - Nguyễn Ngọc Thắng - Phạm Văn Hùng - *Các bài giảng về số học* - NXB Đại học Quốc Gia Hà Nội, Quý 4 năm 2006.
- [5] *Tài liệu tập huấn phát triển chuyên môn giáo viên trường THPT Chuyên môn Toán*, tháng 07/2011.
- [6] Đặng Hùng Thắng - Nguyễn Văn Ngọc - Vũ Kim Thủy - *Bài giảng số học* - Xí nghiệp in đường sắt Hà Nội, tháng 05/1997.
- [7] Nguyễn Vũ Thanh - *Chuyên đề bồi dưỡng Chuyên môn toán Số học* - NXB Tiền Giang, tháng 09/1992.
- [8] Peter Vandendriessche - Hojoo Lee - *Problems in Elementary Number Theory*, 07/2007.