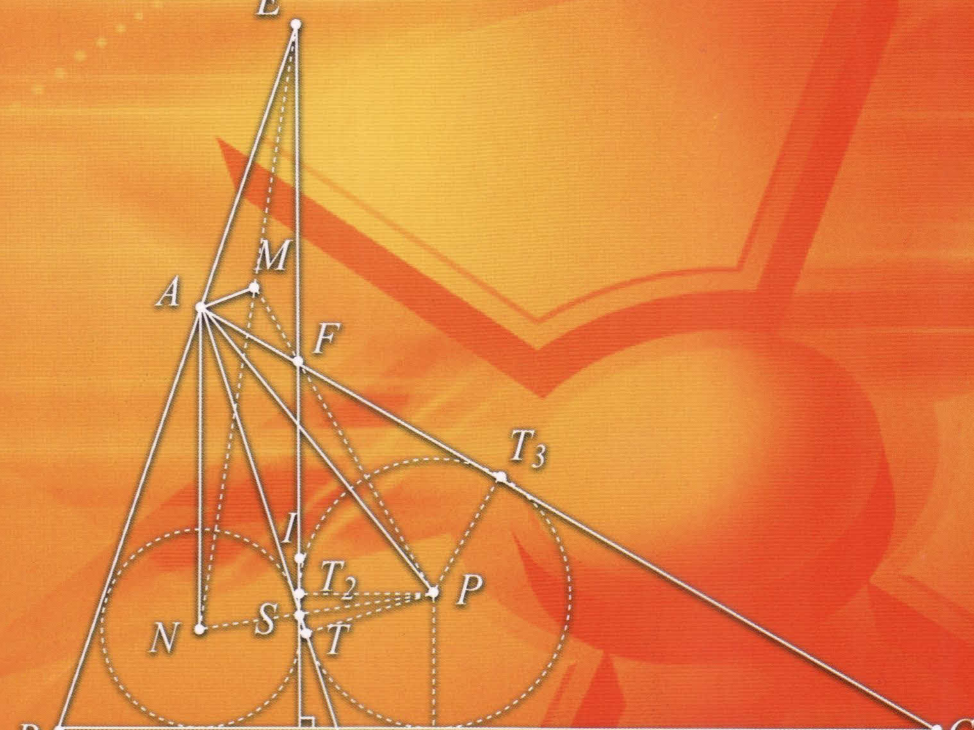
TRẦN NAM DŨNG (Chủ biên)

CÁC CHUYÊN ĐỀ BỒI DƯỠNG HỌC SINH GIỎI TOÁN



TP.HCM, tháng 8/2011

TRẦN NAM DŨNG (Chủ biên)

CÁC CHUYÊN ĐỀ BỒI DƯỠNG

HỌC SINH GIỎI TOÁN

TP. HỒ CHÍ MINH, 08/2011

LỜI NÓI ĐẦU

Tài liệu này được biên soạn dành cho chương trình "Gặp gỡ Toán học lần thứ III" được tổ chức tại thành phố Hồ Chí Minh từ ngày 8/8 đến ngày 14/8 năm 2011 dành cho các học sinh, sinh viên và giáo viên chuyên Toán. Tuy vậy, đây không hẳn là tập hợp các bài giảng sẽ được trình bày tại các lớp học của chương trình mà là tuyển tập các bài viết hoàn chỉnh của các chuyên gia, các thầy giáo, các sinh viên và học viên cao học về các chủ đề bồi dưỡng học sinh giỏi Toán. Vì thế, có thể coi tài liệu này là một cuốn sách độc lập dành cho học sinh và giáo viên chuyên Toán. Ban biên tập đã nhận được những bài viết có chất lượng tốt được gửi từ khắp mọi miền đất nước. Chủ đề của các chuyên đề lần này rải đều tất cả các phân môn: Số học, Tổ hợp, Giải tích, Đại số, Hình học và tuổi của các tác giả cũng rải đều từ 20 đến 65. Điều này một lần nữa cho thấy sự ủng hộ của những người yêu toán dành cho chương trình "Gặp gỡ Toán học" nói riêng và phong trào chuyên Toán nói chung không bao giờ cạn và luôn ở mức cao nhất.

Chúng tôi trân trọng đưa vào tài liệu những tài liệu đã trở thành kinh điển: chương Hàm số số học trích từ cuốn sách "Số học Thuật toán" của GS Hà Huy Khoái và TS Phạm Huy Điển, bài giảng về Tổ hợp của thầy Nguyễn Khắc Minh trình bày tại khóa bồi dưỡng giáo viên Toán mùa Đông năm 1996. Xin cảm ơn GS Hà Huy Khoái và thầy Nguyễn Khắc Minh đã nhận lời tham gia giảng bài tại trường hè để truyền lửa cho các bạn học sinh ở phía Nam nói riêng và phong trào dạy và học Toán ở phía Nam nói chung.

Rất tiếc là chúng tôi không kịp đưa bài viết của GS Ngô Bảo Châu vào cuốn kỷ yếu lần này. Tuy nhiên chúng tôi sẽ gửi tặng bạn đọc bản viết tay của GS dành cho trường hè. Sự ủng hộ của GS Ngô Bảo Châu cũng như sự khích lệ của GS Ngô Việt Trung, GS Nguyễn Văn Mậu, GS Lê Tuấn Hoa là một nguồn cổ vũ lớn lao cho các thành viên BTC.

Chúng tôi trân trọng cảm ơn trường Đại học Khoa học Tự nhiên, đặc biệt là PGS TS Dương Anh Đức và PGS TS Đặng Đức Trọng đã ủng hộ và hỗ trợ mọi mặt cho những người thực hiện chương trình. Cảm ơn nhà in Đại học Quốc gia thành phố Hồ Chí Minh đã hoàn thành tốt công việc của mình với tinh thần trách nhiệm cao nhất. Ban biên tập chân thành cảm ơn các bạn Lê Phúc Lữ (sinh viên năm 2 trường Đại học FPT) và bạn Lê Việt Hải (học sinh lớp 12 trường Phổ thông Năng khiếu) đã có nhiều đóng góp cho việc biên tập.

Cuối cùng chúng tôi muốn cảm ơn Công ty cổ phần Giáo dục Titan đã tạo những điều kiện tốt nhất và hỗ trợ tối đa để Ban biên tập có thể hoàn thành cuốn tài liệu này.

BAN BIÊN TẬP

MỤC LỤC

VỀ CÁC HÀM SỐ HỌC

Hà Huy Khoại – Phạm Huy Điển[1,2]

Khi nghiên cứu các số nguyên, ta thường làm việc với các đại lượng như: số các ước của một số nguyên tố cho trước, tổng các ước của nó, tổng các lũy thừa bậc k của các ước, ... Ngoài những ví dụ đó còn có nhiều hàm số học quan trọng khác. Trong bài viết này, ta sẽ đi qua một vài hàm quan trọng, đặc biệt là hàm Euler, một trong những hàm số học quan trọng nhất.

1 Định nghĩa

Định nghĩa 1. *Hàm số học tức là hàm xác định trên tập hợp các số nguyên dương.*

Định nghĩa 2. *Một hàm số học f được gọi là nhân tính nếu với mọi m, n nguyên tố cùng nhau, ta có đẳng thức*

$$f(mn) = f(m)f(n).$$

Trong trường hợp đẳng thức trên đúng với mọi m, n (không nhất thiết nguyên tố cùng nhau), hàm f được gọi là nhân tính mạnh.

Những ví dụ đơn giản nhất về hàm nhân tính (mạnh) là $f(n) = n$ và $f(n) = 1$.

Dễ chứng minh tính chất sau đây: nếu f là một hàm nhân tính, n là số nguyên dương có khai triển thành thừa số nguyên tố dạng $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, thì $f(n)$ được tính theo công thức

$$f(n) = f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_k^{a_k}).$$

2 Phi-hàm Euler

Trong các hàm số học, hàm Euler mà ta định nghĩa sau đây có vai trò rất quan trọng.

Định nghĩa 3. *Phi-hàm Euler $\phi(n)$ là hàm số học có giá trị tại n bằng số các số không vượt quá n và nguyên tố cùng nhau với n.*

Ví dụ. Từ định nghĩa ta có $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$, $\phi(9) = 6$, $\phi(10) = 4$.

Từ định nghĩa trên đây, ta có ngay hệ quả trực tiếp: *Số p là nguyên tố khi và chỉ khi $\phi(p) = p-1$.*

Nếu định lý Fermat bé cho ta công cụ nghiên cứu đồng dư modulo một số nguyên tố, thì Phi-hàm Euler được dùng để xét đồng dư modulo một tập hợp số. Trước khi đi vào vấn đề đó, ta cần một số định nghĩa sau.

Định nghĩa 4. *Hệ thặng dư thu gọn modulo n là tập hợp $\phi(n)$ số nguyên sao cho mỗi phần tử của tập nguyên tố cùng nhau với n, và không có 2 phần tử nào đồng dư với nhau modulo n.*

---

[1] Viện Toán học.

[2] Bài viết được trích trong cuốn sách "Số học Thuật toán" của các tác giả xuất bản năm 2003 tại Nhà xuất bản Đại học Quốc gia Hà Nội.

Nói cách khác từ hệ thặng dư đầy đủ modulo n, để lập hệ thặng dư thu gọn, ta chỉ giữ lại những giá trị nào nguyên tố cùng nhau với n.

Ví dụ. Các số 1, 2, 3, 4, 5, 6 lập thành hệ thặng dư thu gọn modulo 7. Đối với modulo 8, ta có thể lấy 1, 3, 5, 7.

Định lý 1. *Nếu $r_1, r_2, \ldots, r_{\phi(n)}$ là một hệ thặng dư thu gọn modulo n, và a là số nguyên dương, $(a, n) = 1$, thì tập hợp $ar_1, ar_2, \ldots, ar_{\phi(n)}$ cũng là hệ thặng dư thu gọn modulo n.*

Chứng minh. Chúng tôi dành chứng minh định lý này cho độc giả. □

Định lý trên đây được dùng để chứng minh mở rộng của định lý Fermat bé.

Định lý 2 (Euler). *Nếu m là số nguyên dương và a là số nguyên tố cùng nhau với m, thì*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Chứng minh. Ta lập luận hoàn toàn tương tự như trong định lý Fermat bé. Giả sử $r_1, r_2, \ldots, r_{\phi(m)}$ là thặng dư thu gọn mod m, lập nên từ các số nguyên dương không vượt quá m và nguyên tố cùng nhau với m. Theo định lý 1, $ar_1, ar_2, \ldots, ar_{\phi(m)}$ cũng là một hệ thặng dư thu gọn. Khi đó thặng dư dương bé nhất của hệ này sẽ là tập hợp $r_1, r_2, \ldots, r_{\phi(m)}$ sắp xếp theo một thứ tự nào đó. Ta có

$$(ar_1)(ar_2)\cdots(ar_{\phi(m)}) \equiv r_1r_2\cdots r_{\phi(m)} \pmod{m}.$$

Như vậy,

$$a^{\phi(m)}r_1r_2\cdots r_{\phi(m)} \equiv r_1r_2\cdots r_{\phi(m)} \pmod{m}.$$

Từ đó suy ra định lý. □

Định lý Euler có thể dùng để tìm nghịch đảo modulo m. Chẳng hạn nếu a và m là các số nguyên tố cùng nhau, ta có $a \cdot a^{\phi(m)-1} \equiv 1 \pmod{m}$, tức là $a^{\phi(m)-1}$ chính là nghịch đảo của a modulo m. Từ đó cũng suy ra nghiệm của phương trình đồng dư tuyến tính $ax \equiv b \pmod{m}$, với $(a, m) = 1$ là

$$x \equiv a^{\phi(m)-1}b \pmod{m}.$$

Định lý 3. *Phi-hàm Euler là hàm nhân tính.*

Chứng minh. Giả sử m, n là hai số dương nguyên tố cùng nhau. Ta cần chứng tỏ rằng

$$\phi(mn) = \phi(m)\phi(n).$$

Ta sắp xếp tất cả các số nguyên dương không vượt quá mn thành bảng sau

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
r & m+r & 2m+r & \ldots & (n-1)m+r \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
m & 2m & 3m & \ldots & mn
\end{array}$$

Giả sử r là số nguyên không vượt quá m, và $(r, m) = d > 1$. Khi đó trong hàng thứ r không có số nguyên nào nguyên tố cùng nhau với mn. Vì thế để tính $\phi(mn)$, ta chỉ cần quan tâm các số trong hàng thứ r với $(r, m) = 1$. Các số trong hàng này đều nguyên tố cùng nhau với m. Mặt khác dễ thấy rằng các số trong hàng này lập thành một hệ thặng dư đầy đủ modulo n. Do đó có đúng $\phi(n)$ số trong hàng nguyên tố cùng nhau với n, tức là trong hàng có $\phi(n)$ số nguyên tố cùng nhau với mn. Cả thảy có $\phi(n)$ hàng như vậy, định lý được chứng minh. □

Nhờ tính chất này ta có ngay công thức Phi-hàm Euler.

Định lý 4. *Giả sử $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ là phân tích của n thành thừa số nguyên tố. Khi đó ta có*

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

Chứng minh. Do Phi-hàm Euler là hàm nhân tính nên ta chỉ cần chứng minh rằng, với mọi số nguyên tố p, thì

$$\phi(p^k) = p^k - p^{k-1}.$$

Thật vậy, các số nguyên dương không vượt quá p^k và không nguyên tố cùng nhau với p phải có dạng sp với s nguyên dương nào đó. Có đúng p^{k-1} số như vậy. Do đó, số các số không vượt quá p^k và nguyên tố cùng nhau với p^k đúng bằng $p^k - p^{k-1}$. □

Tính chất quan trọng sau đây của Phi-hàm thường được sử dụng về sau.

Định lý 5. *Giả sử n là một số nguyên dương. Khi đó*

$$\sum_{d\,|\,n} \phi(d) = n,$$

trong đó tổng được lấy theo mọi ước của n.

Chứng minh. Ta phân các số nguyên từ 1 đến n thành từng nhóm C_d sao cho $m \in C_d$ khi và chỉ khi $(m, n) = d$, tức là khi và chỉ khi $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Như vậy, số phần tử của C_d đúng bằng số các số nguyên không vượt quá $\frac{n}{d}$ và nguyên tố cùng nhau với $\frac{n}{d}$, tức là bằng $\phi\left(\frac{n}{d}\right)$. Ta có

$$n = \sum_{d\,|\,n} \phi\left(\frac{n}{d}\right).$$

Khi d chạy qua mọi ước của n thì $\frac{n}{d}$ cũng chạy qua mọi ước của n, định lý được chứng minh. □

Nhận xét. Các tính chất của Phi-hàm Euler được sử dụng để tính đồng dư của những lũy thừa rất lớn. Chẳng hạn, ta cần tính $a^n \bmod k$, trong đó n là một số nguyên lớn. Giả sử ta có

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

Khi đó $a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$. Từ đây suy ra nếu N là bội chung nhỏ nhất của các số $\phi(p_i^{\alpha_i})$ thì $a^N \equiv a \pmod{k}$. Do đó, viết $n = Nq + r$ với $r < N$, ta được

$$a^n \equiv a^r \pmod{k}.$$

Ví dụ. Để tính $2^{1000000} \bmod 77$, ta thực hiện như sau: Ta có

$$77 = 11 \cdot 7, \quad \phi(7) = 6, \quad \phi(11) = 10.$$

Bội chung nhỏ nhất của 6 và 10 là 30, do đó

$$2^{30} \equiv 1 \pmod{77}.$$

Mặt khác, dễ dàng kiểm tra được $1000000 = 30 \cdot 33333 + 10$. Vì vậy,

$$2^{1000000} \equiv 2^{10} \equiv 23 \pmod{77}.$$

3 Số hoàn hảo và số nguyên tố Mersenne

Mục này dành để mô tả một dạng đặc biệt của số nguyên tố, có vai trò quan trọng trong lý thuyết và ứng dụng. Ta bắt đầu bằng một số hàm số học quan trọng.

Định nghĩa 5. *Hàm $\tau(n)$, số các ước, có giá trị tại n bằng số các ước dương của n. Hàm $\sigma(n)$, tổng các ước, có giá trị tại n bằng tổng các ước dương của n. Nói cách khác, ta có*

$$\tau(n) = \sum_{d\,|\,n} 1, \quad \sigma(n) = \sum_{d\,|\,n} d.$$

Ví dụ. Nếu p là một số nguyên tố thì $\tau(p) = 2$, $\sigma(p) = p + 1$.

Định lý 6. *$\tau(n)$ và $\sigma(n)$ là các hàm nhân tính.*

Dễ thấy rằng, định lý trên suy ra từ bổ đề sau.

Bổ đề 1. *Nếu f là hàm nhân tính, thì*

$$F(n) = \sum_{d\,|\,n} f(d)$$

cũng là hàm nhân tính.

Chứng minh. Giả sử m, n là các số nguyên dương nguyên tố cùng nhau. Ta có

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

Vì $(m, n) = 1$, mỗi ước d của mn có thể viết duy nhất dưới dạng $d = d_1 d_2$ trong đó d_1, d_2 tương ứng là ước của m, n, và d_1, d_2 nguyên tố cùng nhau, do vậy ta có

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

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

$$F(mn) = \sum_{d_1\,|\,m,\, d_2\,|\,n} f(d_1)f(d_2) = \left[\sum_{d_1\,|\,m} f(d_1)\right]\left[\sum_{d_2\,|\,n} f(d_2)\right] = F(m)F(n).$$

Bổ đề được chứng minh. □

Sử dụng định lý , ta có ngay công thức sau đây cho các hàm $\tau(n)$ và $\sigma(n)$.

Định lý 7. *Giả sử n có phân tích ra thừa số nguyên tố là $n = p_1^{a_2} p_2^{a_2} \cdots p_k^{a_k}$. Khi đó ta có*

$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{a_j+1} - 1}{p_j - 1}, \quad \tau(n) = (a_1+1)(a_2+1)\cdots(a_k+1) = \prod_{j=1}^{k}(a_j+1).$$

Chứng minh. Chúng tôi dành chứng minh này cho độc giả. □

Do các quan niệm thần bí, người cổ Hy Lạp quan tâm đến các số nguyên bằng tổng tất cả các ước dương thực sự của nó. Họ gọi các số đó là các *số hoàn hảo*.

Định nghĩa 6. *Số nguyên dương n được gọi là số hoàn hảo nếu*

$$\sigma(n) = 2n.$$

Ví dụ. Các số 6, 28 là các số hoàn hảo vì

$$\sigma(6) = 1 + 2 + 3 + 6 = 12, \quad \sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56.$$

Định lý sau đây được biết từ thời Hy Lạp.

Định lý 8. *Số nguyên dương chẵn n là số hoàn hảo khi và chỉ khi $n = 2^{m-1}(2^m - 1)$, trong đó m là một số nguyên sao cho $m \geqslant 2$ và $2^m - 1$ là số nguyên tố.*

Chứng minh. Trước tiên, giả sử rằng, n có dạng như trên. Vì σ là hàm nhân tính, ta có

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

Từ công thức của hàm σ và giả thiết $2^m - 1$ là số nguyên tố, dễ thấy rằng $\sigma(2^{m-1}) = 2^m - 1$, $\sigma(2^m - 1) = 2^m$, và do đó $\sigma(n) = 2n$. Điều này chứng tỏ n là số hoàn hảo.

Ngược lại, giả sử n là số hoàn hảo chẵn. Viết n dưới dạng $n = 2^s t$, trong đó s, t là các số nguyên dương, t lẻ, ta được

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

Vì n là số hoàn hảo nên $\sigma(n) = 2n = 2^{s+1}t$. Như vậy, $2^{s+1} \mid \sigma(t)$. Giả sử $\sigma(t) = 2^{s+1}q$, thì

$$(2^{s+1} - 1)2^{s+1}q = 2^{s+1}t,$$

tức là $q \mid t$ và $q \neq t$. Mặt khác ta có

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

Ta sẽ chứng tỏ rằng $q = 1$. Thật vậy, nếu ngược lại, t có ít nhất 3 ước khác nhau là $1, t, q$, do đó $\sigma(t) \geqslant t + q + 1$, mâu thuẫn với đẳng thức vừa chứng minh. Vậy $\sigma(t) = t + 1$, có nghĩa t là số nguyên tố. Định lý được chứng minh. □

Như vậy để tìm các số hoàn hảo, ta cần tìm các số nguyên tố có dạng $2^m - 1$.

Định nghĩa 7. *Giả sử m là một số nguyên dương, khi đó $M_m = 2^m - 1$ được gọi là số Mersenne thứ m. Nếu p là số nguyên tố, và M_p cũng 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, trong khi M_{11} là hợp số.

Có nhiều định lý khác nhau dùng để xác định số nguyên tố Mersenne. Chẳng hạn nhờ định lý sau đây, ta có thể kiểm tra nhanh chóng dựa vào dạng của các ước nguyên tố của số Mersenne.

Định lý 9. *Nếu p là một số nguyên tố lẻ, thì mọi ước nguyên tố của số Mersenne M_p đều có dạng $2kp + 1$, trong đó k là số nguyên dương.*

Chứng minh. Giả sử q là một ước nguyên tố của M_q. Theo định lý Fermat bé, $q \mid (2^{q-1} - 1)$. Lại có $(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1$. Ước chung này lớn hơn 1, vì nó là một bội của q. Do đó, $(p, q - 1) = p$, vì p là một số nguyên tố. Ta có $q = mp + 1$, và vì q lẻ nên $m = 2k$, định lý được chứng minh. □