ĐỒNG DƯ

Đồng dư là một khái niệm Toán học cơ bản, đơn giản và sơ cấp. Nó thường được giảng dạy ngay từ chương trình THCS. Đó cũng làm khuôn khổ để phát biểu và chứng minh một trong những định lý Toán học thực sự đầu tiên mà học sinh được học, đó là định lý Fermat nhỏ. Lần đầu tiên tôi được nghe giảng về định lý Fermat nhỏ có lẽ là vào thời gian học lớp sáu, đó cũng là lần đầu tiên tôi nhận ra được cái mà người ta gọi là vẻ đẹp Toán học, một thứ rất khó định nghĩa, nhưng cũng là cái mà bao nhiêu người vẫn miệt mài, thầm lặng theo đuổi.

Mục đích của bài viết nhỏ này là thuật lại sự xuất hiện của khái niệm đồng dư từ nền văn minh cổ đại, và rồi nhấn mạnh một khía cạnh mà có lẽ ít người để ý đến, đó là tính xúc tác của nó trong sự hình thành các cấu trúc đại số trong Toán học hiện đại. [1]

1. Euclid và Tôn Tử

Chương VI và IX của quyển sách "Cơ Sở" của Eudlid có nhắc đến tính chất chia hết, khái niệm số chẵn và số lẻ, nhưng chưa phát biểu tường minh khái niệm đồng dư.

Hai số nguyên a_1, a_2 được coi là đồng dư theo modulo b nếu mà $a_1 - a_2$ chia hết cho b, hay nói cách khác a_1 và a_2 có cùng một phần dư Euclid trong phép chia cho b. Ta ký hiệu

$$a_1 \equiv a_2 \pmod{b}.$$

Khái niệm đồng dư xuất hiện khá rõ nét trong định lý phần dư Trung Hoa. Người Trung Hoa gọi nó là bài toán Hàn Tín điểm binh: Một nhóm không quá một trăm binh lính xếp hàng bảy thì dư ra một người, xếp hàng năm thì dư ra ba người, xếp hàng ba thì không dư ra ai. Tướng quân giỏi nhẩm sẽ tính ra rằng số binh linh bằng đúng bảy mươi tám.

Dựa theo tra cứu thì thấy định lý này được phát biểu lần đầu trong sách Toán pháp Tôn Tử (thế kỷ thứ $III - V$ sau Công nguyên), không liên quan gì đến Binh pháp Tôn Tử (thế kỷ thứ V trước Công nguyên). Vì vậy có thể đặt câu hỏi gán ghép bài toán đồng dư với tên của Hàn Tín có phải là một nhầm lẫn lịch sử hay không ?

Định lý phần dư Trung Hoa phát biểu với ký hiệu hiện đại như sau:

Cho m là số nguyên dương. Nếu $n_1, n_2, \ldots, n_m$ là các số nguyên đôi một nguyên tố cùng nhau và $r_1, r_2, \ldots, r_m$ là các số nguyên thoả mãn $0 \leqslant r_i < n_i$ với $i \in \{1, 2, \ldots, m\}$ thì tồn

[1] Tác giả chân thành cảm ơn thầy Trần Nam Dũng đã giúp biên tập bài viết này.

tại duy nhất một số nguyên r thoả mãn $0 \leqslant r < \prod_{i=1}^{m} n_i$ sao cho r đồng dư với $r_i \bmod n_i$ với mọi $i \in \{1, 2, \ldots, m\}$, hay là

$$r \equiv r_i \pmod{n_i}. \tag{1}$$

Giả thiết quan trọng trong định lý phần dư Trung Hoa là giả thiết nguyên tố cùng nhau. Hai số nguyên a và b được coi là nguyên tố cùng nhau nếu như ước số chung lớn nhất của chúng là 1. Nếu a và b là hai số nguyên dương, ta ký hiệu $(a;\ b)$ là ước số chung lớn nhất của chúng. Như vậy, a và b là nguyên tố cùng nhau khi và chỉ khi $(a;\ b) = 1$.

Sách Cơ sở của Euclid, chương VI, có khảo sát khá kỹ khái niệm nguyên tố cùng nhau.

Mệnh đề số 2 trong chương VI đưa ra một thuật Toán hiệu quả cho việc tìm ước số chung lớn nhất của hai số nguyên dương và đồng thời xác định xem hai số nguyên cho trước có nguyên tố cùng nhau hay không:

Cho a và b là hai số nguyên dương. Xét (x, y) là một cặp biến nguyên với giá trị ban đầu là $(x, y) = (a, b)$. Ta thực hiện phép chia Euclid $x = yq + r$ với $q, r \in \mathbb{Z}$, $0 \leqslant r < y$. Nếu $r = 0$, ước số chúng lớn nhất của a và b bằng y. Nếu $r > 0$, ta thực hiện vòng lặp với giá trị mới $(x, y) := (b, r)$ thay cho cặp số $(x, y) = (a, b)$ ban đầu. Thuật toán dừng khi mà phép chia Euclid không còn phần dư. Thuật toán hiển nhiên phải dừng sau một số hữu hạn bước vì $b > r$ và biến y không thể giảm mãi trong tập các số nguyên dương.

Để giải thích cho thuật toán Euclid, ta cần nhận xét rằng $\gcd(a, b) = \gcd(b, r)$, tức là ước số chung lớn nhất của cặp số (a, b) đúng bằng ước số chung lớn nhất của cặp số (b, r). Thật vậy, từ quan hệ $a = bq + r$, ta rút ra rằng một số nguyên d là ước của cả a và b khi và chỉ khi nó là ước của cả b và r. Ở bước cuối cùng, khi mà phần dư bằng 0, hiển nhiên ước số chung lớn nhất của x và y đúng bằng y.

Một nhận xét rất quan trọng là trong tiến trình của thuật toán Euclid với cặp số biến thiên $(x, y) = (a, b)$ ở bước thứ nhất, rồi $(x, y) = (b, r)$ ở bước thứ hai, các giá trị nhận được của x và y luôn là các tổ hợp tuyến tính nguyên của a và b, hay nói cách khác, ở mọi thời điểm, giá trị của x và y luôn có dạng $ma + bn$ với m, n là những số nguyên nào đó. Ta có thể rút ra kết luận rằng ước số chung lớn nhất $\gcd(a, b)$ bắt buộc phải có dạng này, tức là tồn tại những số nguyên m, n sao cho

$$\gcd(a, b) = ma + nb. \tag{2}$$

Đây cũng chính là tổ hợp tuyến tính có giá trị tuyệt đối dương nhỏ nhất của hai số nguyên dương (a, b) cho trước. Trong ngôn ngữ Đại số hiện đại, ta sẽ nói rằng tập hợp các số ở dạng $ma + nb$ với $m, n \in \mathbb{Z}$ là ideal sinh bởi a và b. Ideal này là ideal chính, nó có phần tử sinh là ước số chúng lớn nhất $\gcd(a, b)$. Tất nhiên, ngày xưa, Euclid không có khái niệm ideal chính trong hành trang lý thuyết của mình, nhưng khái niệm này đã tiềm ẩn trong thuật toán mà ông nghĩ ra.

Cũng cần bổ sung thêm rằng chứng minh định lý phần dư Trung Hoa cho hai số nguyên n_1, n_2 nguyên tố cùng nhau, có thể qui về việc chỉ ra hai số nguyên m_1, m_2 thoả mãn $m_1 n_1 + m_2 n_2 = 1$.

2. Fermat và Euler

Nếu p là một số nguyên tố và a là một số nguyên dương không chia hết cho p thì khi đó, ta có phương trình đồng dư

$$a^{p-1} \equiv 1 \pmod{p}. \tag{3}$$

Đây là phát biểu của định lý nhỏ của Fermat, một trong những định lý quan trọng nhất trong Số học sơ cấp.

Euler mở rộng định lý của Fermat cho trường hợp đồng dư modulo một số nguyên không nhất thiết nguyên tố. Nếu n là một số nguyên dương, ta ký hiệu $\phi(n)$ là số các số nguyên a với $0 < a \leqslant n$ sao cho $(a; n) = 1$. Với một số nguyên tố, ta có $\phi(p) = p - 1$. Số $\phi(n)$ được gọi là chỉ số Euler của n. Định lý Fermat được Euler mở rộng ra như sau

$$a^{\phi(n)} \equiv 1 \pmod{n}, \tag{4}$$

với mọi cặp số nguyên (a, n) nguyên tố cùng nhau.

Fermat phát biểu định lý nhỏ trong một bức thư cho de Bessy vào năm 1640. Ông nói rằng không viết ra chứng minh vì nó hơi dài. Euler tỏ ra nghi ngờ về chứng minh mà Fermat không công bố, nhưng ông rõ ràng rất thích định lý này và công bố ít nhất hai chứng minh khác nhau. Chứng minh đầu tiên dùng công thức nhị thức Newton còn chứng minh thứ hai dùng tác động của nhóm $(\mathbb{Z}/n)^\times$ lên chính nó. Chứng minh thứ hai của Euler thực sự đi trước lịch sử và bản thân chúng ta sẽ phải tiếp tục xuôi dòng lịch sử trước khi quay lại bình luận về chứng minh của Euler.

3. Disquisitiones của Gauss

Trong chương IX sách "Cơ Sở" của Euclid có ít nhất 5 mệnh đề về cộng và nhân các số chẵn lẻ, ví dụ như tích của hai số lẻ luôn là số lẻ. Chương đầu của quyển Disquisiotiones của Gauss cũng dành vào việc chứng minh tập $\mathbb{Z}/n$ các lớp đồng dư modulo n tạo thành một vành. Đáng chú ý rằng, người ta chưa phát biểu một cách tổng quát thế nào là một vành giao hoán vào thời của Gauss, nhưng ông hoàng của Toán học đã biết rõ thế nào là một vành, và hiểu tầm quan trọng của việc $\mathbb{Z}/n$ tạo thành một vành.

Ông cũng chứng minh rằng vành $\mathbb{Z}/n$ là một trường khi và chỉ khi n là một số nguyên tố.

Định lý phần dư Trung Hoa có thể được làm mạnh lên như sau:

Nếu $n = \prod_{i=1}^{m} n_i$ với $n_1, n_2, \ldots, n_m$ là các số nguyên dương đôi một nguyên tố cùng nhau thì ánh xạ

$$\mathbb{Z}/n \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z} \tag{5}$$

là đẳng cấu vành.

Định lý phần dư Trung Hoa sau này xuất hiện dưới nhiều hình hài khác nhau trong Toán học hiện đại, tường minh nhất là trong đại số như trong chương một quyển cẩm nang Đại số giao hoán của Matsumura, ẩn hơn trong khái niệm adele của Số học hiện đại.

Với mọi vành giao hoán R, ta ký hiệu $R^\times$ tập con các phần tử khả nghịch của R : $a \in R$ được gọi là khả nghịch nếu tồn tại $b \in R$ sao cho $ab = 1$. Tập $R^\times$ là một nhóm giao hoán đối với phép nhân. Sử dụng (2), ta thấy rằng lớp đồng dư của a là một phần tử khả nghịch trong $\mathbb{Z}/n$ khi và chỉ khi a và n nguyên tố cùng nhau. Như vậy, chỉ số Euler $\phi(n)$ chính là số phần tử của nhóm $(\mathbb{Z}/n)^\times$ các phần tử khả nghịch của $\mathbb{Z}/n$. Thể hiện chỉ số Euler như số phần tử khả nghịch của vành $\mathbb{Z}/n$ cho phép ta giải thích những tính chất cơ bản của chỉ số Euler.

Nếu $n = \prod_{i=1}^{m} n_i$ với $n_1, n_2, \ldots, n_m$ đôi một nguyên tố cùng nhau thì từ (5), ta suy ra rằng ánh xạ

$$(\mathbb{Z}/n)^\times \to \prod_{i=1}^{m} (\mathbb{Z}/n_i)^\times \tag{6}$$

là một đẳng cấu nhóm. Đẳng cấu này kéo theo đẳng thức

$$\phi(n) = \prod_{i=1}^{m} \phi(n_i), \tag{7}$$

đúng dưới giả thiết các số nguyên dương $n_1, n_2, \ldots, n_m$ đôi một nguyên tố cùng nhau.

Định lý Fermat nhỏ và mở rộng của nó là định lý Euler cũng có thể suy ra từ cấu trúc nhóm của $(\mathbb{Z}/n)^\times$. Thật vậy, với mọi nhóm hữu hạn G với m phần tử, với mọi $g \in G$, ta có $g^m = 1$. Đây là một hệ quả của định lý Lagrange khẳng định rằng số phần tử của mọi nhóm con H của G luôn là một ước số của số phần tử của G. Áp dụng mệnh đề này vào trường hợp của nhóm con sinh ra bởi một phần tử $a \in (\mathbb{Z}/n)^\times$, ta suy ra đẳng thức $a^{\phi(n)} = 1$ trong vành $\mathbb{Z}/n$.

Nhìn từ quan điểm cấu trúc đại số, định lý nhỏ của Fermat và mở rộng của Euler đơn thuần là tính chất đơn giản nhất của nhóm $(\mathbb{Z}/n)^\times$ các phần tử khả nghịch của vành $\mathbb{Z}/n$ các lớp đồng dư mod n. Tuy vậy, cần lưu ý rằng Fermat và Euler dường như không nhận thức về điều này.

Nên lưu ý rằng phải chờ đến thời Galois, Sylvester thì khái niệm về nhóm trừu tượng mới hình thành. Tra cứu chứng minh thứ hai của Euler, ta thấy tuy rằng ông chưa có khái niệm nhóm trừu tượng nhưng ông ta đã biết cho nhóm $(\mathbb{Z}/n)^\times$ tác động lên chính nó và chứng minh định lý Fermat nhỏ mở rộng dựa vào tác động này. Qua đây, ta thấy rằng khái niệm nhóm tác động lên một tập hợp xuất hiện trước khái niệm nhóm trừu tượng.

4. Định lý nhóm nhân và mật mã

Sylvester đã chỉ ra rằng mọi nhóm Abel hữu hạn đều có dạng

$$A = \mathbb{Z}/d_1 \times \mathbb{Z}/d_2 \times \cdots \times \mathbb{Z}/d_m, \tag{8}$$

với $d_1|d_2|\cdots|d_m$ là một dãy số nguyên dương, số sau là bội của số trước. Dãy số $d_1|d_2|\cdots|d_m$, hoàn toàn được xác định bởi A, được gọi là kiểu của A. Số m là số tối thiểu các phần tử lập thành một hệ sinh của A. Nhóm A được gọi là nhóm xích nếu $m = 1$, nói cách khác A có một phần tử sinh.

Ta có thể đặt ra câu hỏi xác định kiểu của nhóm nhân $(\mathbb{Z}/n)^\times$. Định lý nhóm nhân khẳng định rằng trong trường hợp $n = p$ là một số nguyên tố thì $(\mathbb{Z}/p)^\times$ là nhóm xích.

Giả sử $(\mathbb{Z}/p)^\times = \mathbb{Z}/d_1 \times \mathbb{Z}/d_2 \times \cdots \times \mathbb{Z}/d_m$ với $m > 1$ và q là một số nguyên tố ước của $d_1, d_2, \ldots d_m$. Khi đó, có đúng q^m phần tử $x \in (\mathbb{Z}/p)^\times$ thoả mãn $x^q = 1$. Những phần tử này là nghiệm của phương trình $x^q - 1 = 0$ trong trường $\mathbb{F}_p = \mathbb{Z}/p$. Vì không thể có quá q nghiệm của phương trình bậc q, ta có $m = 1$.

Định lý nhóm nhân có nhiều ứng dụng trong lý thuyết số sơ cấp. Ví dụ thứ nhất liên quan đến việc tính toán ký hiệu Legendre.

Cho a và b là hai số nguyên nguyên tố cùng nhau, ta đặt

$$\left(\frac{a}{b}\right) = \begin{cases} 1 & \text{nếu tồn tại } x \in \mathbb{Z} \text{ sao cho } x^2 \equiv a \pmod{b} \\ -1 & \text{nếu không tồn tại } x \in \mathbb{Z} \text{ sao cho } x^2 \equiv a \pmod{b} \end{cases} \tag{9}$$

Xét ví dụ đơn giản nhất với $a = -1$ và $b = p$ là một số nguyên tố lẻ. Do $(\mathbb{Z}/p)^\times$ đẳng cấu với $\mathbb{Z}/(p-1)$ nên để cho -1 là một bình phương, điều kiện cần và đủ là $(-1)^{\frac{p-1}{2}} = 1$.

Vì vậy, ta có công thức

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{nếu } p \equiv 1 \pmod 4 \\ -1 & \text{nếu } p \equiv -1 \pmod 4 \end{cases} \tag{10}$$

Tổng quát hơn, Gauss chứng minh luật thuận nghịch bậc hai, một trong những định lý quan trọng nhất trong Disquisitiones. Luật này có thể xem như một thuật toán để tính ký hiệu Legendre. Bên cạnh ý nghĩa thuật toán, nó là khởi nguồn của của một mạch chính trong số học hiện đại bao gồm luật thuận nghịch Artin, giả thuyết Langlands. Chúng ta sẽ để dành chủ đề rộng lớn này cho những bài khác.

Ứng dụng thứ hai liên quan đến lý thuyết mật mã. Cho n là một số tự nhiên rất lớn và lấy tập hợp $\mathbb{Z}/n$ làm tập hợp các chữ cái. Mã hoá sẽ là một hàm số $\xi : \mathbb{Z}/n \to \mathbb{Z}/n$. Ta sẽ giả sử rằng ξ là một song ánh và gọi hàm ngược ξ^{-1} là giải mã. Nếu n là một số lớn và ξ là một hoán vị bất kỳ, việc xác định ξ^{-1} có độ phức tạp rất lớn, vượt ra ngoài khả năng tính toán của các máy tính hiện nay.

Xét trường hợp đặc biệt $\xi(x) = x^a$ với a là một số nguyên dương lớn hơn 1. Để ánh xạ $\xi : \mathbb{Z}/n \to \mathbb{Z}/n$ là song ánh, điều kiện cần, nhưng không đủ, là n không có ước chính phương, tức là $n = p_1 \cdot p_2 \cdots p_m$ là tích các số nguyên tố khác nhau. Trong trường hợp này, ta có thể suy ra từ định lý Euler rằng với mọi số nguyên m thoả mãn $m \equiv 1 \pmod{\phi(n)}$ ta có

$$x^m \equiv x \pmod n. \tag{11}$$

Nếu b là một số nguyên dương sao cho $ab \equiv 1 \pmod{\phi(n)}$ thì hàm $\xi' : \mathbb{Z}/n \to \mathbb{Z}/n$ cho bởi $x \mapsto x^b$ là hàm ngược của ξ. Như vây để giải mã ξ ta chỉ cần tìm số nguyên dương b sao cho $ab \equiv 1 \mod \phi(n)$. Với giả thiết a nguyên tố cùng nhau với $\phi(n)$, để tìm được b, ta có thể dùng thuật tuán chia Euclid. Nói cách khác để nghịch đảo ánh xạ ξ ta chỉ cần biết chỉ số Euler $\phi(n)$.

Từ suy luận này, ta thấy rằng để mã hoá, ta chỉ cần biết n và a; trong khi đó để giải mã, ta cần biết $\phi(n)$ và b. Biết $\phi(n)$ gần như tương đương với việc phân tích n thành tích các thừa số nguyên tố. Vì phân tích một số nguyên dương lớn thành tích các số nguyên tố có độ phức tạp tính toán cao cho nên trên nguyên tắc việc giải mã là rất khó ngay cả khi việc thông tin về mã hoá có thể hoàn toàn công khai.

5. Tham khảo

Về chủ đề này, bạn đọc có thể tìm đọc thêm quyển kinh điển "Course in Arithmetic" của Serre, hoặc quyển "A Computational Introduction to Number Theory and Algebra" của Shoup, cũng rất tốt và có thể tải về hợp pháp từ trên trang mạng của tác giả. Bạn đọc quan tâm đến lịch sử toán học nên bắt đầu từ Disquisitiones của Gauss.