

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
ĐẠI HỌC QUỐC GIA HÀ NỘI
*
*
*

BÀI TẬP LỚN

MÔN THỰC HÀNH TÍNH TOÁN

Sinh Viên Thực Hiện : **Nguyễn Xuân Bách**

Lớp : **K58A1T**

MỘT LỊCH SỬ CỦA LÝ THUYẾT SỐ

Từ <https://en.wikipedia.org/wiki/Numbertheory>

Mục lục

1	Lý thuyết số là gì?	4
2	Buổi đầu của lý thuyết số	4
3	Hy Lạp cổ điển và thời kì tiền Hellenistic	7
4	Diophantus	8
5	Aryabhata, Brahmagupta, Bhaskara	9
6	Số học trong thời kì vàng Islamic	10
7	Tây Âu trong Thời Trung Cổ	10
8	Lý thuyết số tiền hiện đại	11
8.1	Fermat	11
8.2	Euler	12
9	Lagrange, Legendre và Gauss	14
10	Phát triển và chia thành các lĩnh vực con	16
11	Lý thuyết số giải tích	17
12	Lý thuyết số đại số	18
13	Hình học Diophantine	19
14	Tài liệu	20
15	Giải thưởng	21

1 Lý thuyết số là gì?



Hình 1: Một sàng Lehmer, nó là một máy tính số gốc từng được sử dụng để tìm các số nguyên tố và giải các phương trình Diophantine đơn giản.

Lý thuyết số hay số học là một nhánh của toán học thuần túy cơ bản nghiên cứu các số tự nhiên và các số nguyên. Đôi khi được gọi là 'Nữ hoàng của toán học' bởi vị trí nền tảng của nó. Các nhà lý thuyết số nghiên cứu các số nguyên tố cũng như các đối tượng được tạo ra bởi các số nguyên (số hữu tỉ) hoặc được định nghĩa như tổng quát hóa của các số nguyên (số nguyên đại số).

Các số nguyên có thể được quan tâm trong chính chúng hoặc như lời giải của các phương trình (hình học Diophantine). Các câu hỏi trong lý thuyết số thường được hiểu tốt nhất thông qua nghiên cứu các đối tượng giải tích (hàm zeta Riemann) mở ra các tính chất của các số nguyên, số nguyên tố hoặc các đối tượng liên quan số khác theo một phong cách nào đó (lý thuyết số giải tích). Người ta cũng có thể nghiên cứu các số thực trong mối quan hệ với các số hữu tỉ, chẳng hạn xấp xỉ bởi số hữu tỉ (xấp xỉ Diophantine).

2 Buổi đầu của lý thuyết số

Chỉ dẫn lịch sử đầu tiên tìm thấy của một vật thể tự nhiên số học là một mảnh vỡ của một bảng: một bảng đất sét vỡ Plimton 322 (Larsa, Mesopotamia, ca. 1800 BCE) chứa một danh sách các 'bộ ba Pythagorean', tức là các số

nguyên (a, b, c) sao cho $a^2 + b^2 = c^2$. Các bộ ba quá nhiều và quá lớn để thu được bằng cách chia trường hợp. Đầu đề trên cột đầu tiên đọc: "Takiltum của đường chéo được trừ sao cho độ rộng..."



Hình 2: Bảng Plimpton 322.

Bố trí của bảng gợi ý rằng nó được xây dựng, theo ngôn ngữ hiện đại bởi đồng nhất thức

$$\left(\frac{1}{2}\left(x - \frac{1}{x}\right)\right)^2 + 1 = \left(\frac{1}{2}\left(x + \frac{1}{x}\right)\right)^2$$

ẩn trong các bài tập Babylon cổ hằng ngày. Nếu phương pháp khác nào đó được sử dụng, các bộ ba trước hết được xây dựng và rồi được sắp lại bởi $\frac{c}{a}$, có lẽ thực sự sử dụng như một 'bảng', tức là mục đích ứng dụng.

Không rõ về các ứng dụng này; thiên văn Babylon, chẳng hạn, thực sự nở rộ chỉ sau này. Gợi ý thay rằng bảng là một dữ liệu số cho các bài toán trường học.

Trong khi lý thuyết số Babylon chứa những mảnh đơn lẻ, điểm xuyết này, đại số Babylon đặc biệt được phát triển tốt. Dữ liệu Late Neoplatonic nói rằng Pythagoras đã học toán học từ những người Babylon. Các dữ liệu sớm hơn nói rằng Thales và Pythagoras đã di chuyển và nghiên cứu ở Ai Cập.

Sách Cơ sở của Euclid, quyển IX, trang 21-34 rất có khả năng là thuộc về người Pythagorean. Đó là một dữ kiện đơn giản ('lẻ nhân chẵn là chẵn', 'nếu một số lẻ chia hết một số chẵn thì nó cũng chia hết một nửa của số đó') nhưng nó là tất cả những gì cần thiết để chứng minh rằng $\sqrt{2}$ là vô tỉ. Thần học Pythagorean cho điều tuyệt quan trọng về số lẻ và số chẵn. Khám phá rằng $\sqrt{2}$ là vô tỉ được ghi công cho những người Pythagorean (Theodorus trước đó). Bằng việc chỉ ra các số có thể là vô tỉ, khám phá này có vẻ như kích thích khủng hoảng nền tảng đầu tiên trong lịch sử toán học. Chứng minh của nó hay tiết lộ của nó được ghi công cho Hippasus, người bị trục xuất hay tách khỏi môn phái Pythagorean. Điều này tạo một sự khác biệt giữa các số (các số nguyên và các số hữu tỉ-các chủ đề của lý thuyết số), theo một cách, và độ dài và tỉ lệ (mà ta

sẽ đồng nhất với các số thực, dù có hữu tỉ hay không), theo cách khác.

Truyền miệng Pythagorean nói về cái được gọi là các số đa giác hay hình học. Trong khi các số bình phương, lập phương,..., giờ được thấy tự nhiên hơn các số tam giác, các số ngũ giác,..., nghiên cứu của tổng các số tam giác và ngũ giác được chứng minh thành công trong thời kì tiền hiện đại (thế kỉ 17 tới đầu thế kỉ 19).

Chúng ta biết không có tài liệu số học rõ ràng trong các dữ kiện Ai Cập cổ đại hay Vệ Đà, mặc dù có một ít đại số trong cả hai. Định lý phần dư Trung Hoa xuất hiện như một bài tập trong Suan Ching của Sun Zi, cũng được biết đến như Kinh Điển Toán Học của Sun Zi (thế kỉ thứ 3, 4 hoặc 5 sau công nguyên.) (có một bước quan trọng được che đậy trong lời giải của Sun Zi: vấn đề được giải sau này bởi kuttaka của Aryabhata.)

Cũng có một ít thần học số học trong toán học Trung Hoa, nhưng, không giống như Pythagorean, nó dường như không dẫn tới đâu. Giống các số hoàn hảo của Pythagorean, các bình phương kì diệu chuyển từ mê tín vào giải trí.

3 Hy Lạp cổ điển và thời kì tiền Hellenistic

Bên cạnh một vài mảnh vỡ, toán học của Hy Lạp cổ điển được biết tới chúng ta thông qua các báo cáo của các công trình không phải toán học đương thời hoặc các công trình toán học từ thời kì tiền Hellenistic. Trong trường hợp của lý thuyết số, bởi và phần lớn, lần lượt, Plato và Euclid.

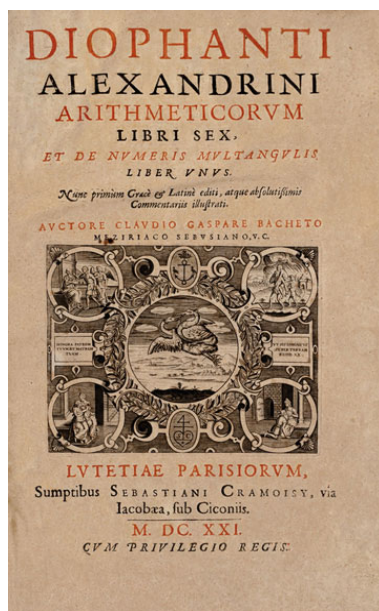
Plato có một quan tâm mãnh liệt trong toán học, và phân biệt rõ ràng giữa số học và tính toán. Thông qua một trong số các đối thoại của Plato-ấy là, Theaetetus-ta biết rằng Theodorus đã chứng minh rằng $\sqrt{3}, \sqrt{5}, \dots, \sqrt{17}$ là vô tỉ. Theaetetus là, giống Plato, một tín đồ của Theodorus. Ông đã làm công việc phân loại các kiểu khác nhau của tỉ số vô tỉ, và do đó được cho là một người tiên phong trong nghiên cứu các hệ thống số. (quyển X của sách Cơ Bản của Euclid được mô tả bởi Pappus là được dựa trên phần lớn công trình của Theodorus)

Euclid góp phần trong sách Cơ Bản của mình về các số nguyên tố và tính chia hết, các chủ đề rõ ràng về lý thuyết số và là cơ bản về nó (quyển VII tới quyển IX của Cơ Bản của Euclid). Nói riêng, ông cho một thuật toán cho việc tính ước chung lớn nhất của hai số (thuật toán Euclid, Cơ Bản, Mệnh đề VII.2) và chứng minh được biết đến đầu tiên của tính vô hạn của các số nguyên tố (Cơ Bản, mệnh đề IX.20).

Năm 1773, Lessing đã công bố một bài thơ ông tìm thấy trong một bản viết tay trong thời gian ông làm quản thư. Nó được xác nhận là một bức thư được gửi bởi Archimedes tới Eratosthenes. Bài thơ đề ra một bài toán trở nên được biết đến là bài toán đàn gia súc của Archimedes; lời giải của nó (thiếu vắng trong bản viết tay) yêu cầu giải một phương trình bậc hai vô định (mà giảm về cái sau này sẽ được đặt sai tên phương trình Pell). Trong chừng mực ta biết, những phương trình như vậy được tiếp cận thành công đầu tiên bởi trường học Ấn Độ. Không rõ Archimedes có tự tìm được một phương pháp giải.

4 Diophantus

Ta biết rất ít về Diophantus của Alexandria; có khả năng ông sống vào thế kỉ thứ ba sau công nguyên, tức là, khoảng năm trăm năm sau Euclid. Sáu trong số mười ba quyển của Arithmetica của Diophantus vẫn tồn tại theo tiếng Hy Lạp gốc. Hơn bốn quyển tồn tại dưới dạng bản dịch tiếng Ả Rập. Arithmetica là một tập hợp các vấn đề giải chi tiết ở đó nhiệm vụ luôn là tìm các lời giải hữu tỉ cho một hệ các phương trình đa thức, thường có dạng $f(x, y) = z^2$ hoặc $f(x, y, z) = w^2$. Do đó, ngày nay ta nói có dạng các phương trình Diophantine khi ta nói có dạng các phương trình đa thức cho phương trình mà nghiệm cần tìm là hữu tỉ hoặc nguyên.



Hình 3: Tiêu đề của phiên bản năm 1621 của Arithmetica của Diophantus, được dịch sang tiếng Latin bởi Claude Gaspard Bachet de Méziriac.

Người ta có thể nói rằng Diophantus lúc đó đang nghiên cứu các điểm hữu tỉ-tức là, các điểm có tọa độ là hữu tỉ- trên các đường cong và đa tạp đại số; tuy nhiên, không giống những người Hy Lạp của thời kì cổ điển, người đã làm cái mà giờ ta gọi là hình học đại số cơ bản theo ngôn ngữ đại số thuần túy. Theo ngôn ngữ hiện đại, cái Diophantus đã làm là tìm các tham số hóa hữu tỉ của các đa tạp; tức là, cho một phương trình có dạng $f(x_1, x_2, x_3) = 0$, mục đích của ông là tìm (về bản chất) ba hàm hữu tỉ g_1, g_2, g_3 sao cho với tất cả các giá trị của r và s , hệ $x_i = g_i(r, s)$ với $i = 1, 2, 3$ cho một lời giải tới $f(x_1, x_2, x_3) = 0$

Diophantus cũng đã nghiên cứu các phương trình của một vài đường cong

không-hữu tỉ, với chúng không tham số hóa hữu tỉ nào có thể. Ông đã thành công trong việc tìm một số điểm hữu tỉ trên các đường cong này (các đường cong elliptic, như nó xảy ra, trong cái dường như là sự kiện được biết đến đầu tiên của chúng) bằng cái mà chúng quy là phép dựng một tiếp tuyến: Chuyển sang hình học tọa độ (không tồn tại trong thời của Diophantus), phương pháp của ông được hình dung là vẽ một tiếp tuyến tới một đường cong tại một điểm hữu tỉ đã biết, và rồi tìm điểm khác là giao của tiếp tuyến với đường cong; điểm khác đó là một điểm hữu tỉ mới. (Diophantus cũng đã dùng tới cái được gọi là một trường hợp đặc biệt của một phép dựng cát tuyến.)

Trong khi Diophantus quan tâm phần lớn với các lời giải hữu tỉ, ông đã giả sử một số kết quả trên các số nguyên, nói riêng rằng mọi số nguyên là tổng của bốn bình phương (mặc dù ông đã không bao giờ phát biểu rõ ràng).

5 Aryabhata, Brahmagupta, Bhaskara

Trong khi thiên văn Hi Lạp chắc chắn đã ảnh hưởng tới học thuật Ấn Độ, ở điểm giới thiệu lượng giác, mặt khác dường như toán học Ấn Độ là một truyền thống mang bản sắc riêng; nói riêng, không có bằng chứng rằng Cơ Bản của Euclid tới Ấn Độ trước thế kỉ 18.

Aryabhata (476-550 sau công nguyên) chứng tỏ rằng các cặp đồng dư đồng thời

$$n \equiv a_1 \pmod{m_1}, n \equiv a_2 \pmod{m_2}$$

có thể được giải bằng một phương pháp được gọi là kuttaka, hay phân hủy, đây là một thủ tục gần với (một dạng tổng quát của) thuật toán Euclid, mà rõ ràng được khám phá độc lập ở Ấn Độ. Aryabhata dường như có ý tưởng áp dụng vào các tính toán thiên văn.

Brahmagupta (628 sau công nguyên) bắt đầu nghiên cứu có hệ thống của các phương trình bậc hai-nói riêng, cái tên bị đặt sai phương trình Pell, trong đó Archimedes quan tâm đầu tiên, và nó đã không được bắt tay vào giải ở phương Tây cho tới tận thời của Fermat và Euler. Sau đó các tác giả Sanskrit tiếp nối, sử dụng thuật ngữ kỹ thuật của Brahmagupta. Một thủ tục tổng quát (chakravala, hay 'phương pháp xích') cho giải phương trình Pell cuối cùng được tìm ra bởi Jayadeva (được trích dẫn vào thế kỉ mười một; công trình của ông mặt khác đã bị mất); trình bày tồn tại sớm nhất xuất hiện trong Bija-ganita của Bhaskara II (thế kỉ 12).

Không may, các nhà toán học Ấn Độ phần lớn vẫn không được biết đến ở Châu Âu cho tới cuối thế kỉ 18. Công trình của Brahmagupta và Bhaskara được dịch sang tiếng Anh năm 1817 bởi Henry Colebrooke.

6 Số học trong thời kì vàng Islamic

Vào đầu thế kỉ thứ chín, vua Al-Ma'mun ra lệnh dịch nhiều công trình toán học Hi Lạp và ít nhất một công trình Sanskrit (Sindhind, có thể hoặc không phải là Brahmasphutasiddhanta của Brahmagupta). Công trình chính của Diophantus, Arithmetica, đã được dịch sang tiếng Ả Rập bởi Qusta ibn Luqa (820-912). Một phần trong luận án al-Fakhri (bởi al-Karaji, 953-ca. 1029) xây dựng trên nó. Theo Rashed Roshdi, bạn cùng thời của Al-Karaji Ibn al-Haytham đã biết cái sau này được gọi là định lý Wilson.

7 Tây Âu trong Thời Trung Cổ

Ngoài một luận án về các bình phương trong cấp số cộng bởi Fibonacci người đã sống và nghiên cứu ở bắc Phi và Constantinople trong suốt thời gian sống, 1175-1200 sau công nguyên-không có gì đáng nói về lý thuyết số ở Tây Âu trong suốt thời Trung Cổ. Chuyện bắt đầu thay đổi ở Châu Âu vào cuối thời Phục Hưng, nhờ vào một nghiên cứu được làm mới của các công trình thời cổ Hi Lạp. Một chất xúc tác là việc sửa lỗi và dịch sang tiếng Latin Arithmetica của Diophantus (Bachet, 1621, tiếp nối một cố gắng đầu tiên bởi Xylander, 1575).

8 Lý thuyết số tiền hiện đại

8.1 Fermat

Pierre de Fermat (1601-1665) không bao giờ công bố các ghi chép của ông; nói riêng, công trình của ông về lý thuyết số hầu như được chứa hoàn toàn trong các bức thư tới các nhà toán học và trong lề các ghi chép cá nhân. Ông gần như không ghi chứng minh nào trong lý thuyết số; ông không có mô hình nào trong chứng minh. Ông đã lập lại quy nạp toán học, giới thiệu phương pháp lùi vô hạn.



Hình 4: Pierre de Fermat.

Một trong các quan tâm đầu tiên của Fermat là các số hoàn hảo (xuất hiện trong quyển IX, sách Cơ Bản của Euclid) và các số uyên ương; điều đã dẫn ông tới các ước số nguyên, là điểm bắt đầu giữa những trao đổi (1636 trở về trước) đưa ông tiếp xúc với cộng đồng toán học ngày đó. Ông đã nghiên cứu xong phiên bản Diophantus của Bachet một cách cẩn trọng; năm 1643, phần lớn mối quan tâm của ông chuyển sang các bài toán Diophantine và các tổng của các bình phương (cũng đã được tiếp cận bởi Diophantus).

Thành tựu của Fermat trong số học bao gồm:

1. Định lý nhỏ Fermat (1640), phát biểu rằng, nếu a không chia hết bởi một số nguyên tố p , thì $a^{p-1} \equiv 1 \pmod{p}$.

2. Nếu a và b là nguyên tố cùng nhau, thì $a^2 + b^2$ không chia hết bởi bất kì số nguyên tố nào đồng dư -1 modulo 4; và mọi số nguyên tố đồng dư 1 modulo 4 có thể được viết dưới dạng $a^2 + b^2$. Hai phát biểu này cũng đề từ 1640; năm 1659, Fermat nói với Huygens rằng ông đã chứng minh được phát biểu sau bằng phương pháp lùi vô hạn. Fermat và Frenicle cũng làm một số công trình (một phần sai sót) về các dạng bậc hai.

3. Fermat đề ra bài toán giải phương trình $x^2 - Ny^2 = 1$ như một thách thức tới các nhà toán học Anh (1657). Bài toán đã được giải trong một vài tháng bởi Wallis và Brouncker. Fermat quan tâm lời giải hợp lệ của chúng, nhưng đã chỉ ra họ đã dùng một thuật toán mà không chứng minh (Jayadeva và Bhaskara đã làm rồi, dù vậy Fermat đã không bao giờ biết điều này.) Ông nói rằng một chứng minh có thể được tìm thấy bằng phương pháp lùi.

4. Fermat đã phát triển các phương pháp cho (làm cái mà theo ngôn ngữ của chúng ta chung quy là) việc tìm các điểm trên các đường cong có giống 0 và 1. Như Diophantus, có rất nhiều thủ tục đặc biệt và chung quy là một phép dựng tiếp tuyến, nhưng không dùng một phép dựng cát tuyến.

5. Fermat phát biểu và chứng minh (bằng phương pháp lùi) trong phụ lục cho Nhận Xét về Diophantus rằng $x^4 + y^4 = z^4$ không có lời giải không tầm thường trong các số nguyên. Fermat cũng đề cập với bạn thư của ông rằng $x^3 + y^3 = z^3$ không có lời giải tầm thường, và rằng điều này có thể được chứng minh bằng phương pháp lùi. Chứng minh được biết đầu tiên là bởi Euler (1753; đúng là bằng phương pháp lùi).

Xác nhận của Fermat (định lý cuối cùng Fermat) rằng đã chứng tỏ không có lời giải cho $x^n + y^n = z^n$ với mọi $n \geq 3$ (chứng minh duy nhất được biết tới vượt quá xa phương pháp của ông) xuất hiện duy nhất trong các chú thích của ông bên lề một phiên bản của Diophantus; ông đã không bao giờ xác nhận điều này với người khác và do đó không cần rút lại nó nếu ông tìm thấy bất kì lỗi sai trong chứng minh giả định của ông.

8.2 Euler

Mối quan tâm của Leonhard Euler (1707-1783) trong lý thuyết số lần đầu tiên được thúc đẩy vào năm 1729, khi một người bạn của ông, Goldbach, chỉ ông một phần công trình của Fermat về lý thuyết số. Đây được gọi là sự tái sinh của lý thuyết số hiện đại, sau sự thiếu tương đối của Fermat của sự thành công trong việc có được sự chú ý của những người cùng thời cho lý thuyết số. Công trình của Euler cho lý thuyết số gồm:

1. Các chứng minh cho các phát biểu của Fermat. Bao gồm định lý nhỏ Fermat (tổng quát hóa bởi Euler cho modulo không-nguyên tố); sự kiện $p = x^2 + y^2$ nếu và chỉ nếu $p \equiv 1 \pmod{4}$; công trình ban đầu về chứng minh rằng mọi



Hình 5: Leonhard Euler.

số nguyên là tổng của bốn bình phương (chứng minh đầy đủ đầu tiên là bởi Joseph-Louis Lagrange (1770), sau một thời gian ngắn Euler tự hoàn thiện); không có lời giải nguyên khác không cho $x^4 + y^4 = z^2$ (dẫn tới trường hợp $n = 4$ của định lý cuối cùng của Fermat, trường hợp $n = 3$ của nó Euler cũng đã chứng minh bằng một phương pháp liên quan).

2. Phương trình Pell, bị đặt sai tên đầu tiên bởi Euler. Ông đã viết về liên kết giữa các phân số liên tục và phương trình Pell.

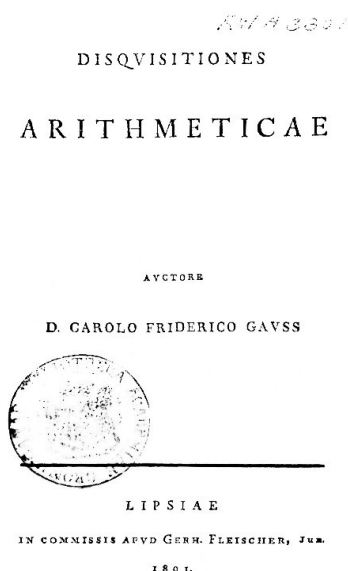
3. Bước đầu về lý thuyết số giải tích. Trong công trình của ông về các tổng của bốn bình phương, phân hoạch, các số ngũ giác, và phân bố của các số nguyên tố, Euler tiên phong sử dụng cái có thể xem như giải tích (nói riêng, chuỗi vô hạn) trong lý thuyết số. Vì ông sống trước khi sự phát triển của giải tích phức, phần lớn công trình của ông được hạn chế về các thao tác hình thức của chuỗi lũy thừa. Ông đã, tuy nhiên, làm một số công trình rất đáng kể ban đầu (mặc dù không hoàn toàn chặt chẽ) về cái sau này được gọi là hàm zeta Riemann.

4. Các dạng bậc hai. Tiếp nối tìm tòi của Fermat, Euler đã làm thêm nghiên cứu về câu hỏi các số nguyên tố có thể được biểu dưới dạng $x^2 + Ny^2$, một phần của nó mô tả trước luật thuận nghịch bậc hai.

5. Các phương trình Diophantine. Euler đã dành thời gian cho các phương trình Diophantine có giống 0 và 1. Nói riêng, ông đã nghiên cứu công trình của

Diophantus; ông đã cố gắng hệ thống hóa nó nhưng thời điểm ấy chưa chín muồi cho một nỗ lực như vậy-hình học đại số vẫn còn nằm trong trứng nước. Ông đã chú ý rằng có một kết nối giữa các bài toán Diophantine và các tích phân elliptic, công trình mà ông đã tự khởi đầu.

9 Lagrange, Legendre và Gauss



Hình 6: Disquisitiones Arithmeticae của Carl Friedrich Gauss, phiên bản đầu tiên.

Joseph-Louis Lagrange (1736-1813) là người đầu tiên cho các chứng minh đầy đủ của một phần công trình của Fermat và Euler và các nhận xét - ví dụ, định lý bốn-bình phương và lý thuyết cơ bản của 'phương trình Pell' (một lời giải thuật toán cho nó được tìm ra bởi Fermat và những người cùng thời của ông, và cũng bởi Jayadeva và Bhaskara II trước đó.) Ông cũng nghiên cứu các dạng bậc hai dưới dạng tổng quát nhất - định nghĩa quan hệ tương đương của chúng, chỉ ra cách trình diễn chúng dưới dạng rút gọn, vân vân.

Adrien-Marie Legendre (1752-1833) là người đầu tiên phát biểu luật thuận nghịch bậc hai. Ông cũng đã phỏng đoán cái chung quy là định lý số nguyên tố và định lý Dirichlet về cấp số cộng. Ông đã cho một tiếp cận đầy đủ của phương trình $ax^2 + by^2 + cz^2 = 0$ và làm về các dạng bậc hai dọc theo các đường mà sau này được phát triển đầy đủ bởi Gauss. Cuối đời, ông đã là người đầu tiên

chứng minh 'định lý cuối cùng của Fermat' cho $n = 5$ (công trình hoàn thiện bởi Peter Gustav Lejeune Dirichlet, và ghi nhận cả ông và Sophi Germain)



Hình 7: Carl Friedrich Gauss

Trong *Disquisitiones Arithmeticae* của mình (1798), Carl Friedrich Gauss (1777-1855) đã chứng minh luật thuận nghịch bậc hai và phát triển lý thuyết của các dạng bậc hai (nói riêng, định nghĩa hợp của chúng). Ông cũng đã giới thiệu một vài khái niệm cơ bản (đồng dư) và dành một chương về các vấn đề tính toán, bao gồm các kiểm tra số nguyên tố. Chương cuối của *Disquisitiones* thiết lập một liên kết giữa các nghiệm của đơn vị và lý thuyết số:

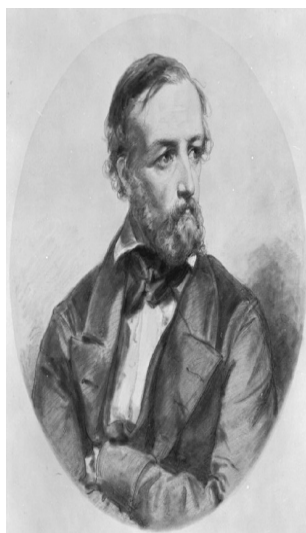
"Lý thuyết của phép chia đường tròn...được tiếp cận trong chương 7 tự nó không thuộc về lý thuyết số, nhưng các nguyên lý của nó chỉ có thể được mô tả từ số học cao cấp"

Theo cách này, Gauss được cho đã làm một công phá đầu tiên vào cả công trình của Esvariste Galois và lý thuyết số đại số.

10 Phát triển và chia thành các lĩnh vực con

Bắt đầu sớm vào thế kỉ mười chín, các sự phát triển sau đã dần dần xảy ra:

1. Sự gia tăng tự ý thức của lý thuyết số như một lĩnh vực nghiên cứu.
2. Sự phát triển của nhiều phần của toán học hiện đại cần thiết cho lý thuyết số hiện đại cơ bản: giải tích phức, lý thuyết nhóm, lý thuyết Galois - được đi kèm sự chính xác lớn hơn trong giải tích và trừu tượng trong đại số.
3. Phân chia thô của lý thuyết số thành các lĩnh vực con hiện đại của nó - nói riêng, lý thuyết số giải tích và lý thuyết số đại số.



Hình 8: Peter Gustav Lejeune Dirichlet.

Có thể nói lý thuyết số đại số khởi đầu với nghiên cứu của luật thuận nghịch và cyclotomy, nhưng thực sự đã đi vào con đường riêng với sự phát triển của đại số trừu tượng và lý thuyết ideal lúc đầu và lý thuyết định giá. Một điểm bắt đầu quy ước cho lý thuyết số giải tích là định lý Dirichlet về cấp số cộng (1837), chứng minh đã giới thiệu các L-hàm và chứa một phần giải tích tiệm cận và một quá trình giới hạn trên một biến thực. Việc dùng lần đầu các ý tưởng giải tích trong lý thuyết số thực sự đến từ Euler (những năm 1730), người đã dùng chuỗi lũy thừa hình thức và các lập luận giới hạn không chặt chẽ (hoặc ẩn). Sử dụng giải tích phức trong lý thuyết số đến sau này: công trình của Bernhard Riemann (1859) về hàm zeta Riemann là điểm bắt đầu chính thức; định lý bốn-bình phương của Jacobi (1839), lùi về trước, thuộc về một phần khác lúc ban đầu mà ngày nay chiếm một vai trò chủ đạo trong lý thuyết số giải tích (các



Hình 9: Ernst Kummer.

dạng modular).

11 Lý thuyết số giải tích

Lý thuyết số giải tích có thể được định nghĩa

1. theo công cụ của nó, như là nghiên cứu các số nguyên bằng các công cụ từ giải tích thực và giải tích phức; hoặc
2. theo các vấn đề của nó, như là nghiên cứu nằm trong lý thuyết số của kích thước và mật độ, đối lập với các đồng nhất.

Một vài lĩnh vực nói chung được xem như một phần của lý thuyết số giải tích; ví dụ, lý thuyết sàng, nên được xem xét theo định nghĩa thứ hai thay vì định nghĩa thứ nhất: một số phần của lý thuyết sàng, chẳng hạn, sử dụng rất ít giải tích, dù vậy nó vẫn thuộc về lý thuyết số giải tích.

Sau đây là các ví dụ của các bài toán trong lý thuyết số giải tích: định lý số nguyên tố, giả thuyết Goldbach (hay giả thuyết số nguyên tố sinh đôi, hay các giả thuyết Hardy-Littlewood), bài toán Waring và Giả Thuyết Riemann. Một số các công cụ quan trọng nhất của lý thuyết số giải tích là phương pháp đường tròn, các phương pháp sàng và các L-hàm (hoặc nghiên cứu các tính chất của chúng). Lý thuyết của các dạng modular (và, tổng quát hơn, các dạng tự đẳng cấu) cũng chiếm một vị trí trung tâm ngày càng tăng trong chiếc hộp công cụ

của lý thuyết số giải tích.

Người ta có thể đặt các câu hỏi giải tích về các số đại số, và sử dụng các phương tiện giải tích để trả lời những câu hỏi đó; như vậy lý thuyết số giải tích và lý thuyết số đại số giao nhau. Chẳng hạn, ta có thể định nghĩa các ideal nguyên tố (các tổng quát của các số nguyên tố trong trường các số đại số) và đặt câu hỏi có bao nhiêu ideal nguyên tố lên tới một kích thước xác định. Câu hỏi này có thể được trả lời bằng một khảo sát của các hàm zeta Dedekind, tổng quát của hàm zeta Riemann, một đối tượng giải tích chìa khóa của lý thuyết. Đây là một ví dụ của một cách làm chung trong lý thuyết số giải tích: thu nhận các thông tin về phân bố của một dãy (ở đây, các ideal nguyên tố hoặc các số nguyên tố) từ tiếp cận giải tích của một hàm giá trị phức được xây dựng phù hợp.

12 Lý thuyết số đại số

Một số đại số là số phức bất kì là lời giải của phương trình đa thức $f(x) = 0$ nào đó với các hệ số hữu tỉ; ví dụ, mọi lời giải x của $x^5 + \frac{11}{2}x^3 - 7x^2 + 9 = 0$ là một số đại số. Các trường của các số đại số cũng được gọi là các trường số đại số, hay đơn giản các trường số. Lý thuyết số đại số nghiên cứu các trường số đại số. Do đó lý thuyết số đại số và lý thuyết số giải tích chồng lấn nhau: Lý thuyết số đại số được định nghĩa theo phương pháp của nó, lý thuyết số giải tích được định nghĩa theo đối tượng nghiên cứu của nó.

Có thể lý lẽ rằng kiểu đơn giản nhất của các trường (các trường bậc hai) đã được nghiên cứu bởi Gauss, vì thảo luận về các dạng bậc hai trong *Disquisitiones arithmeticae* có thể được phát biểu lại dưới ngôn ngữ của các ideal và chuẩn trong các trường bậc hai. (Một trường bậc hai chứa tất cả các số có dạng $a + b\sqrt{d}$, ở đó a và b là các số hữu tỉ và d là một số hữu tỉ cố định có căn bậc hai không hữu tỉ.) Vấn đề đó, vào thế kỉ 11 phương pháp chakravala chung quy-theo ngôn ngữ hiện đại-là một thuật toán tìm các đơn vị của một trường số bậc hai thực. Tuy nhiên Bhaskara và Gauss đều không biết về các trường số.

Các mảnh đất của lý thuyết số đại số như ta biết được thiết lập vào cuối thế kỉ mười chín, khi các số ideal, lý thuyết của các ideal và lý thuyết định giá được phát triển; đây là ba con đường bổ sung giải quyết việc không có phân tích nhân tử duy nhất trong các trường số đại số (ví dụ, trong trường được sinh bởi các số hữu tỉ và $\sqrt{-5}$, số 6 có thể được phân tích cả như $6=2.3$ và $6=(1+\sqrt{-5})(1-\sqrt{-5})$); tất cả $2, 3, 1+\sqrt{-5}$ và $1-\sqrt{-5}$ là bất khả quy.) Động lực ban đầu cho sự phát triển của các số ideal (bởi Kummer) dường như đến từ nghiên cứu các luật thuận nghịch bậc hai nâng cao, tức là các dạng tổng quát của luật thuận nghịch.

Các trường số thường được nghiên cứu như các mở rộng của các trường số nhỏ hơn: một trường L được gọi là một mở rộng của trường K nếu L chứa K (ví dụ, các số phức $\mathbb{C}$ là một mở rộng của các số thực $\mathbb{R}$, và các số thực $\mathbb{R}$ là một

mở rộng của các số hữu tỉ $\mathbb{Q}$.) Phân loại các mở rộng có thể của một trường số cho trước là một bài toán mở không hoàn chỉnh và khó. Các mở rộng abel-tức là, các mở rộng L của K sao cho nhóm Galois $\text{Gal}(L/K)$ của L trên K là một nhóm abel-được hiểu rõ tương đối. Phân loại của chúng là đối tượng của chương trình lý thuyết trường lớp, được khởi xướng vào cuối thế kỷ 19 (góp phần bởi Kronecker và Eisenstein) và được mở mang phần lớn vào 1900-1950.

Một ví dụ của một lĩnh vực tích cực nghiên cứu in trong lý thuyết số đại số là lý thuyết Iwasawa. Chương trình Langlands, một trong các kế hoạch nghiên cứu quy mô lớn trong toán học, đôi khi được miêu tả như một thử nghiệm để tổng quát hóa lý thuyết trường lớp cho các mở rộng không-abel của các trường số.

13 Hình học Diophantine

Bài toán trung tâm của hình học Diophantine là xác định khi nào một phương trình Diophantine có lời giải, và nếu có, thì bao nhiêu. Cách tiếp cận là nghĩ các lời giải của một phương trình như một đối tượng hình học.

Ví dụ, một phương trình hai biến định nghĩa một đường cong trong mặt phẳng. Tổng quát hơn, một phương trình, hay hệ các phương trình, theo hai biến hoặc nhiều hơn định nghĩa một đường cong, một mặt phẳng hay đối tượng nào đó khác như vậy trong không gian n -chiều. Trong hình học Diophantine, người ta đặt câu hỏi có điểm hữu tỉ nào (các điểm mà tất cả tọa độ của nó hữu tỉ) hoặc các điểm nguyên nào (các điểm mà tất cả tọa độ nguyên) trên một đường cong hoặc mặt phẳng. Nếu có một điểm như vậy bất kì, bước tiếp theo là đặt câu hỏi có bao nhiêu và chúng phân bố thế nào. Một câu hỏi cơ bản theo hướng này là: có nhiều hữu hạn hay vô hạn các điểm hữu tỉ trên một đường cong cho trước (hay mặt phẳng)? Tương tự về các điểm hữu tỉ?

Một ví dụ ở đây có thể giúp ích. Xét phương trình Pythagorean $x^2 + y^2 = 1$; ta muốn nghiên cứu các lời giải hữu tỉ của nó. Điều này cũng là hỏi tất cả các lời giải nguyên cho $a^2 + b^2 = c^2$; lời giải bất kì lời giải của phương trình sau cho ta một lời giải $x = \frac{a}{c}, y = \frac{b}{c}$ của phương trình trước. Đó cũng là đặt câu hỏi tất cả các điểm với tọa độ hữu tỉ trên đường cong được mô tả bởi $x^2 + y^2 = 1$ (Đường cong là xuất hiện là một đường tròn bán kính 1 xung quanh gốc tọa độ)

Đặt lại câu hỏi về phương trình theo ngôn ngữ của các điểm trên các đường cong hóa ra là phù hợp. Tính hữu hạn hay không của số các điểm hữu tỉ và nguyên trên một đường cong đại số - tức là, các lời giải hữu tỉ hoặc nguyên cho một phương trình $f(x, y) = 0$, ở đó f là một đa thức hai biến-hóa ra phụ thuộc chủ yếu vào giống của đường cong. Giống có thể được định nghĩa như sau. Cho các biến trong $f(x, y) = 0$ là các số phức; thì $f(x, y) = 0$ định nghĩa một mặt 2-chiều trong (chiều) không gian 4-chiều (vì hai biến phức có thể được phân tích

thành bốn biến thực, tức là, bốn chiều). Đếm số (vòng) hồ trong mặt phẳng; gọi số này là giống của $f(x, y) = 0$.

Cũng có phần liên kết gần với các xấp xỉ Diophantine: cho trước một số x , nó có thể được xấp xỉ bởi số hữu tỉ tốt thế nào? (Gọi $\frac{a}{q}$ (với $\gcd(a, q)=1$) là một xấp xỉ tốt với x nếu $|x - \frac{a}{q}| < \frac{1}{q^c}$, ở đó c đủ lớn). Câu hỏi này trở nên đặc biệt nếu x là một số đại số. Nếu x không thể được xấp xỉ tốt, thì một vài phương trình không có nghiệm nguyên hoặc hữu tỉ. Câu hỏi này cũng trở nên đặc biệt trong lý thuyết số siêu việt: nếu một số có thể được xấp xỉ tốt hơn bởi số đại số bất kì, thì nó là một số siêu việt. Theo lập luận này, π và e được chứng minh là siêu việt.

Hình học Diophantine không nên bị nhầm lẫn với hình học của các số, một tập hợp các phương pháp hình nhằm trả lời các câu hỏi xác định trong lý thuyết số đại số. Hình học số học, mặt khác, là một khái niệm hiện đại cho miền giống khá nhiều với miền được giới hạn bởi thuật ngữ hình học Diophantine. Thuật ngữ hình học số học được sử dụng thường xuyên nhất khi ta muốn nhấn mạnh các kết nối với hình học đại số (ví dụ, định lý Faltings) hơn là các công cụ trong xấp xỉ Diophantine.

14 Tài liệu

Hai trong số các nhập môn phổ biến nhất cho lý thuyết số là:

1. G.H.Hardy; E.M.Wright (2008) [1938]. An introduction to the theory of numbers (sửa lại bởi D.R.Heath-Brown và J.H.Silverman, phiên bản thứ 6). Oxford University Press. ISBN 978-0-19-921986-5.

2. Vinogradov, I.M. (2003) [1954]. Elements of Number Theory (tái bản của phiên bản 1954). Mineola, NY: Dover Publications.

Sách của Hardy và Wright là một kinh điển toàn diện, mặc dù tính trong sáng của nó đôi khi do các ý định của các tác giả nhấn mạnh các phương pháp cơ bản. Tâm điểm chính của Vinogradov nằm trong tập hợp các bài toán của nó, nhanh chóng dẫn tới các quan tâm nghiên cứu riêng của Vinogradov; cuốn sách tự nó là rất cơ bản và gần như tối giản. Các nhập môn đầu tiên phổ biến khác là:

3. Ivan M. Niven; Herbert S. Zuckerman; Hugh L. Montgomery (2008) [1960]. An introduction to the theory of numbers (tái bản phiên bản lần thứ 5 phiên bản 1991). John Wiley and Sons. ISBN 978-8-12-651811-1.

4. Kenneth H.Rosen (2010). Elementary Number Theory (phiên bản thứ 6). Pearson Education. ISBN 978-0-32-171775-7.

Các lựa chọn phổ biến cho một cuốn sách thứ hai gồm:

1. Borevich, A. I.; Shafarevich, Igor R. (1966). Pure and Applied Mathematics 20. Boston, MA: Academic Press. ISBN 978-0-12-117850-5. MR 0195803.

2. Serre, Jean-Pierre (1996) [1973]. A course in arithmetic. Graduate texts in mathematics 7. Springer. ISBN 978-0-387-90040-7.

15 Giải thưởng

Hội toán học Mỹ trao tặng Giải Cole trong Lý Thuyết Số. Lý thuyết số là một trong ba lĩnh vực toán học được trao bởi Giải Fermat.