Lý thuyết số: từ cổ điển đến hiện đại

Ngô Bảo Châu

Viasm
07/09/2015-11/09/2015

Trong bài giảng này, chúng ta sẽ đề cập đến các chủ đề sau:

- Một số nội dung trong các quyển $7-9$ sách "Cơ sở" của Euclid;
- Một số công trình của Fermat-Euler-Gauss về dạng toàn phương;
- Lý thuyết số đại số của Kummer và Dedekind;
- Công trình của Riemann, Dirichlet và Tate về ζ-hàm và L-hàm;
- Dạng modular và L-hàm của Hecke.

Đối với những người muốn làm quen với lý thuyết số, những tài liệu sau có thể sẽ rất bổ ích.

- Serre: A course in arithmetics;
- Cox: Primes of the form x^2+ny^2;
- Ireland-Rosen: Modern introduction to classical number theory;
- Miyake: Modular forms.

1 Một số định lý cổ điển: Euclid

1.1 Phép chia Euclid và định lý cơ bản của số học

Euclid, quyển $7-9$.

Định lí 1.1.1. *Mọi số tự nhiên đều có thể phân tích được một cách duy nhất thành tích của các số nguyên tố.*

Chứng minh về sự tồn tại dựa trên nguyên lý *lùi vô hạn* $\Leftrightarrow$ nguyên lý quy nạp $\Leftrightarrow$ xây dựng số tự nhiên.

Chứng minh. **Sự duy nhất.** Tồn tại ước chung lớn nhất.

1. $\forall a, b \in \mathbb{N}, \exists \gcd(a, b)$: ước số chung lớn nhất.
2. p nguyên tố, $p \mid ab$ thì $p \mid a$ hoặc $p \mid b$.

$$(a, b) = ma + nb.$$

Từ tính chất số 2 ta suy ra nếu $p_1 \cdots p_n = q_1 \cdots q_m$ là hai phân tích thành tích của các số nguyên tố của một số nguyên dương cho trước thì $p_1 \mid q_1 \cdots q_m$ nên $p_1 = q_1$ hoặc $p_1 \mid q_2 \cdots q_m$. Từ đây, ta dễ dàng suy ra $p_1 = q_i$ với i nào đó.

Tính chất 1 dẫn đến tính chất 2: Giả sử $p \nmid a$. Thế thì $(p, a) = 1$. Suy ra tồn tại các số nguyên m, n để $mp + na = 1$. Do $p \mid ab$ nên $p \mid b$.

□

Tính chất 1^***.** Cho $a, b \in \mathbb{N}$, tồn tại ước chung lớn nhất của a, b và nó có dạng $ma + nb$ với $m, n \in \mathbb{Z}$ nào đó.

Chứng minh. Ta dựa vào phép chia Euclid

$$a = qb + r$$

$q \in \mathbb{Z}, 0 \leq r < b$.

Lưu ý rằng tính chất 1^* có thể được phát biểu lại một cách tương đương như sau.

Tính chất 1. Trường $\mathbb{Q}$ các số hữu tỷ có chuẩn Euclid:

$$\begin{array}{rcl} |\cdot| : \mathbb{Q} & \to & \mathbb{R}_+ \\ \alpha & \mapsto & |\alpha| \end{array}$$

Hơn nữa, với mọi $\alpha \in \mathbb{Q}$, tồn tại $n \in \mathbb{Z}$ sao cho $|\alpha - n| < 1$: $\alpha = \frac{a}{b}, q = n$,

$$\left| \frac{a}{b} - q \right| < 1$$

Như vậy ta viết vế trái thành $|r/b|$ thì $|r| < |b|$.

□

Nhận xét 1.1.2. *Về định lý cơ bản của số học*

1. *Mở rộng: thay thế các số nguyên tố bằng các ideal*
2. *Phương pháp xuống thang.*

1.2 Sự tồn tại vô hạn của các số nguyên tố

Định lí 1.2.1. *Tồn tại vô hạn số nguyên tố.*

Chứng minh của Euclid. Chứng minh bằng phản chứng. Lưu ý rằng đây là chứng minh nguyên thuỷ của Euclid. Nằm trong quyển số ?? của Euclid. Đây là một phương pháp chứng minh kỳ diệu.

Ta suy luận như sau. Giả sử tồn tại hữu hạn số nguyên tố. Hãy liệt kê chúng, chẳng hạn $p_1, \ldots, p_n$. Xét số $p_1 \cdots p_n + 1$. Theo Định lý 1, tồn tại một số nguyên tố $p \mid p_1 \cdots p_n + 1$. Thế thì $p \notin \{p_1, \ldots, p_n\}$. Ta có điều mâu thuẫn. □

Ta cũng có chứng minh khác, của Euler, như sau. Và chứng này có thể coi như là một tư tưởng của lý thuyết số giải tích phát triển về sau.

Chứng minh của Euler. Xét hàm số

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \cdots = \sum_{n=1}^{+\infty} n^{-s}.$$

Cho dù tôi (NBC) tin rằng Euler có mường tượng rất rõ ràng về các số phức. Tuy nhiên, ở thời điểm đó, các số phức vẫn chưa được đưa vào. Như vậy, hàm ζ ở đây được coi như là một hàm biến thực.

Định lý cơ bản của số học (Định lý 1) có thể được phát biểu một cách tương đương dưới ngôn ngữ của hàm zeta như sau. Ký hiệu $\mathbb{P}$ tập hợp các số nguyên tố, thế thì

$$\zeta(s) = \prod_{p \in \mathbb{P}} (1 + p^{-s} + p^{-2s} + \cdots).$$

Đẳng thức đúng với mọi $s > 1$: vế phải hội tụ tuyệt đối với mọi $s > 1$. Thật vậy, ta chỉ cần viết $n^{-s} = p_1^{-m_1 s} \cdots p_k^{-m_k s}$, trong đó p_i là các số nguyên tố với các số mũ tương ứng m_i trong phân tích của n. Cho đến hiện giờ, ta mới chỉ sử dụng các biến đổi đại số thuần túy.

Bây giờ là bước phản chứng. Giả sử $\mathbb{P}$ hữu hạn. Thế thì, $\prod_{p\in\mathbb{P}}(1-p^{-s})^{-1}$ hội tụ cả tại $s=1$! Nhưng điều này lại dẫn đến việc chuỗi $\sum_n n^{-s}$ hội tụ tại $s=1$. Đây là điều vô lý. □

Chứng minh thứ của Euler, ngoài việc thiết lập tính vô hạn của các số nguyên tố còn cho phép *đo đạc* sự vô hạn của các số nguyên tố. Thật vậy, ta có thể nhận thấy rằng sự vô hạn của các số nguyên tố có liên quan đến sự phân kỳ của chuỗi $\sum_n n^{-s}$.

Từ chứng minh thứ của Euler, Riemann đã nhìn nhận và nghiên cứu hàm ζ, về sau được biết đến dưới tên gọi hàm zeta của Riemann.

Riemann coi ζ là một hàm biến phức $s\in\mathbb{C}$. Chú ý rằng, khi đó ζ vẫn còn là một chuỗi hội tụ tuyệt đối với $\Re s>1$. Từ đây, ζ định nghĩa một hàm chỉnh hình trên miền $\Re s>1$. Ngoài ra, hàm zeta còn có thể được thác triển một cách duy nhất thành một hàm phân hình trên toàn bộ mặt phẳng phức, với cực điểm đơn duy nhất tại $s=1$, và thoả mãn một phương trình hàm liên kết các giá trị $\zeta(s)\leftrightarrow\zeta(1-s)$.

Từ đây, Riemann đã phác thảo một chứng minh về sự phân bố của các số nguyên tố (Prime number theorem). Đây là một kết quả đã biết bởi Gauss. Kết quả này được viết trong bài báo duy nhất của Riemann về Lý thuyết số (Về độ lớn của số các số số nguyên tố nhỏ hơn một số cho trước).

Định lí 1.2.2 (Định lý về số nguyên tố)**.** *Đặt* $\pi(x)=\sharp\{p\in\mathbb{P};p<x\}$. *Thế thì*

$$\pi(x)\sim\frac{x}{\log x}\quad khi\ x\to+\infty.$$

Riemann đã phác thảo một chứng minh của PNT (Prime number theorem) dựa vào các tính chất của hàm ζ.

Nếu mọi không điểm của ζ ($\Re s>0$) đều nằm trên trục $\Re s=1/2$.

Thế thì Riemann chứng minh khẳng định mạnh hơn PNT.

Dựa vào lược đồ của Riemann, Hadamard (và de la Vallée-Poussin) đã chứng minh PNT.

Chứng minh:

1. $\zeta(s)$ không có không điểm trên miền mở chứa $\Re(s)\geq 1$
2. ???

1.3 Fermat-Euler-Gauss

Sau Euclid, toán học phải chờ đến thời ký phục hưng mới có các bước phát triển rực rỡ tiếp theo (với một số ngoại lệ của các nhà toán học Ba tư, v.v)

Khẳng định: với mọi $n\in\mathbb{N}$ thì n đều có thể biểu diễn được dưới dạng $n=x^2+y^2$.

Định lí 1.3.1. *Cho n là một số nguyên tố lẻ. Khi đó tồn tại $x, y \in \mathbb{Q}$ sao cho $p = x^2 + y^2$ khi và chỉ khi tồn tại $x, y \in \mathbb{Z}$ sao cho $p = x^2 + y^2$ và điều này khi và chỉ khi $p \equiv 1 \pmod 4$.*

Hệ quả 1.3.2. *Với mọi số tự nhiên n, viết $n = 2^m p_1^{m_1} \cdots p_r^{m_r}$ với p_i là các số nguyên tố lẻ đôi một khác nhau. Thế thì $n = x^2 + y^2$ với $x, y \in \mathbb{Q}$ khi và chỉ khi $n = x^2 + y^2$ với $x, y \in \mathbb{Z}$ và điều này khi và chỉ khi nếu m_i lẻ thì $p_i \equiv 1 \pmod 4$ với mọi i.*

Định lý dẫn đến Hệ quả. Nếu $a_1 = x_1^2 + y_1^2, a_2 = x_2^2 + y_2^2$ thì $a_1 a_2 = x^2 + y^2$. Đây là một mẹo rất quen thuộc. Tuy nhiên, phải chờ đến Gauss, với sự đưa vào **vành** các số nguyên của Gauss thì mẹo này mới được hiểu một cách sâu sắc.

Xét trường các số hữu tỷ Gauss

$$\mathbb{Q}[i] = \{x + yi \mid x, y \in \mathbb{Q}\}$$

với phép $+$ và $\times$ quen thuộc. Đây là một không gian vector trên $\mathbb{Q}$ với số chiều bằng 2.

Cho dù lý thuyết trường, và đặc biệt là lý thuyết vành chỉ được khái niệm hoá về sau bởi Noether, tuy nhiên Gauss hiểu rất rõ các cấu trúc đại số này. Chẳng hạn, chương đầu tiên của cuốn Disquisitiones đã trình bày rất cận thận chứng minh vì sao tập các lớp đồng dư modulo n tạo thành một vành.

$\mathbb{Q}[i]$ là một vành giao hoán. Thậm chí, đây là một trường. Với $z = x + iy$, xét phép *liên hợp* $\bar{z} = x + iy$. Ta có khái niệm hàm **chuẩn**:

$$\mathrm{Nm} : \mathbb{Q}[i] \to \mathbb{Q}$$

gửi z lên $\mathrm{Nm}(z) = z\bar{z}$. Nói một cách khác

$$x + iy \mapsto (x + iy)(x - iy) = x^2 + y^2.$$

Tính chất quan trọng của Nm là tính nhân của nó:

$$\mathrm{Nm}(z_1 z_2) = \mathrm{Nm}(z_1)\,\mathrm{Nm}(z_2).$$

Công thức này giải thích "mẹo" mà ta đã đề cập tới ở phần đầu chứng minh.

Dưới ngôn ngữ hiện đại, Nm là một đồng cấu nhóm từ $\mathbb{Q}[i]^\times \to \mathbb{Q}^\times$.

Bài toán xác định tập các số hữu tỷ $a \in \mathbb{Q}^\times$ sao cho a biểu diễn được dưới dạng $a = x^2 + y^2$ qui về việc xác định **ảnh** của $\mathrm{Nm} : \mathbb{Q}[i]^\times \to \mathbb{Q}^\times$! Ảnh là một nhóm con của $\mathbb{Q}^\times$.

Trước khi xác định ảnh, ta hãy quan tâm đến việc xác định **hạch** của nó. Cụ thể, ta hãy xác định

$$\ker \mathrm{Nm} = \{z = x + iy; x^2 + y^2 = 1\}.$$

Đây chính là phương trình Pitago quen thuộc!

Quay trở lại bài toán gốc của chúng ta. Viết $n = 2^m p_1^{m_1} \cdots p_r^{m_r}$. Ta có $2 \in \mathfrak{J}(\mathrm{Nm}), p^2 \in \mathfrak{J}(\mathrm{Nm})$. Từ đó, $n = x^2 + y^2$ với $x, y \in \mathbb{Q}$ khi và chỉ khi với mọi m_i lẻ $p_i = x_i^2 + y_i^2$ với $x_i, y_i \in \mathbb{Q}$ và điều này khi và chỉ khi (theo Định lý) với mọi m_i lẻ thì $p_i \equiv 1 \pmod 4$.

□

Chứng minh Định lý. Việc chứng minh được chia thành hai bước cơ bản.

Bước 1. Đây là bước **đồng dư**. Xét bài toán đồng dư: với p lẻ nào thì tồn tại $x, y \in \mathbb{Z}$ không đồng dư (chia hết cho p) sao cho

$$p \mid x^2 + y^2.$$

Câu trả lời là $p \mid x^2 + y^2 \Leftrightarrow p \equiv 1 \pmod 4$.

Cách tiếp cận như sau. Nhận xét rằng $\mathbb{Z}/p\mathbb{Z}$ là một trường, $y \not\equiv 0 \pmod p$ nên tồn tại $z \in \mathbb{Z}$ sao cho $yz \equiv 1 \pmod p$. Như vậy $x^2 + y^2 \equiv 0 \pmod p \Leftrightarrow (xz)^2 + (yz)^2 \equiv 0 \pmod p$. Bài toán qui về việc xác định các p lẻ sao cho tồn tại $x \in \mathbb{Z}$ để $x^2 + 1 \equiv 0 \pmod p$.

Xét ánh xạ

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ x & \mapsto & x^2 \end{array}$$

Với p nào thì -1 là một số chính phương modulo p.

Ta sử dụng định lý Fermat nhỏ: với mọi $x \equiv 0 \pmod p$ thì

$$x^{p-1} \equiv 1 \pmod p.$$

Cho dù kết quả được cho là của Fermat tuy nhiên Fermat chỉ phát biểu kết quả này mà không đưa ra chứng minh. Euler rất ấn tượng với kết quả này và vì thế trình bày 3 chứng minh khác nhau. Chứng minh đầu tiên dựa vào việc sử dụng hệ số nhị thức và qui nạp. Chứng minh thứ 2 là một chứng minh hiện đại hơn và đây là chứng minh vẫn được coi là chứng minh kinh điển của kết quả này. Đặc biệt, chứng minh thứ 2 về mặt bản chất sử dụng sự kiện $(\mathbb{Z}/p\mathbb{Z})^\times$ là một nhóm với phép nhân và có lực lượng bằng $p - 1$. Lưu ý rằng, lý thuyết nhóm mãi về sau mới được đưa vào và phổ thông hoá với các đóng góp quan trọng của Galois. Ta cũng lưu ý rằng, thật ra chứng minh của Euler sử dụng tác động của nhóm! Điều này cũng cho thấy "tác động nhóm" là một khái niệm tự nhiên hơn khái niệm "nhóm".

Quay trở lại bài toán xác định khi nào -1 là một chính phương modulo p. Tính chất mà ta sử dụng ở đây là

Tính chất. Nhóm $(\mathbb{Z}/p\mathbb{Z})^\times$ là một nhóm cyclic, đẳng cấu với $\mathbb{Z}/(p-1)\mathbb{Z}$.

Từ tính chất này, ta có dãy khớp sau đây

$$0 \to \{\pm 1\} \to (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\} \to 0,$$

trong đó các cấu xạ được cho bởi $x \mapsto x^2$ rồi $y \mapsto y^{\frac{p-1}{2}}$.

Từ dãy khớp trên đây, ta suy ra -1 là chính phương modulo p khi và chỉ khi $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$ và điều này hiển nhiên xảy ra khi và chỉ khi $p \equiv 1 \pmod 4$.

Bước 2. Bước lùi vô hạn. Như vậy, theo bước 1 trên đây, nếu $p \equiv -1 \pmod 4$ thì p không biểu diễn được dưới dạng tổng của hai bình phương của các số hữu tỷ. Ta còn phải chỉ ra rằng với mọi $p \equiv 1 \pmod 4$ ta có thể biểu diễn p được thành tổng của hai số chính phương.

Khẳng định. Trường $\mathbb{Q}[i]$ có chuẩn Euclid.

Phái biểu tương đương: vành $\mathbb{Z}[i] = \{x + iy; x, y \in \mathbb{Z}\}$ có phép chia Euclid.

Từ đó, tồn tại gcd theo nghĩa sau đây: với mọi $a, b \in \mathbb{Z}[i]^\times$, xét ideal

$$(a, b) = \{ax + by; x, y \in \mathbb{Z}[i]\} = \{cz; z \in \mathbb{Z}[i]\},$$

trong đó $c \in \mathbb{Z}[i]^\times$ được xác định duy nhất chính xác tới đơn vị của $\mathbb{Z}[i]^\times$.

Theo định nghĩa,

$$\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i]; \exists \beta \in \mathbb{Z}[i], \alpha\beta = 1\}.$$

Ta dễ dàng chỉ ra rằng

$$\mathbb{Z}[i]^\times = \{\alpha = x + iy \in \mathbb{Z}[i]; x^2 + y^2 = 1\} = \{\pm 1, \pm i\}.$$

Bây giờ, để kết thúc bước 2, ta lập luận như sau. Ta có, theo bước 1, tồn tại các số nguyên x, y không chia hết cho p sao cho $p \mid x^2 + y^2$. Giả sử $p^2 \nmid x^2 + y^2$. Đặt

$$\gcd(p, x + iy) = m + in,$$

$m, n \in \mathbb{Z}$. Khi đó, ta có $\mathrm{Nm}(m+in) \mid \mathrm{Nm}(p)$ và như vậy $m^2+n^2 \mid p^2$. Tương tự $\mathrm{Nm}(m+in) \mid \mathrm{Nm}(x+iy)$

nên $m^2+n^2 \mid x^2+y^2$. Thế nhưng, theo giả thiết $p^2 \nmid x^2+y^2$, nên ta phải có $m^2+n^2=p$. Như vậy, trong trường hợp này ta đã biểu diễn được số nguyên tố p thành tổng của hai chính phương.

Xét trường hợp cuối cùng $p^2 \mid x^2+y^2$? [1]

□

Ngày 9/9/2015.

2 Luật thuận nghịch toàn phương

Nhắc lại kết quả cơ bản sau đây,

Định lí 2.0.3. *Với mọi p nguyên tố, nhóm nhân của $\mathbb{F}_p$ là cyclic. Nói cách khác, ta có đẳng cấu*

$$\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Như vậy, $\alpha \in \mathbb{F}_p^\times$ là bình phương của một phần tử khác khi và chỉ khi ảnh của α trong $\mathbb{Z}/(p-1)\mathbb{Z}$ là một số chẵn. Từ đó suy ra ta có dãy khớp sau đây

$$0 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times \longrightarrow \{\pm 1\} \longrightarrow 0\,,$$

trong đó ánh xạ $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ gửi x lên x^2, còn ánh xạ $\mathbb{F}_p^\times \to \{\pm 1\}$ gửi y lên $y^{\frac{p-1}{2}}$.

Nói một cách khác, nếu ta sử dụng **biểu tượng Legendre** $\left(\frac{y}{p}\right)$ định nghĩa bởi

$$\left(\frac{y}{p}\right) = \begin{cases} 1 & \text{nếu tồn tại } x \in \mathbb{F}_p \text{ sao cho } y = x^2 \\ -1 & \text{nếu không} \end{cases}$$

thế thì đồng cấu $\mathbb{F}_p^\times \to \{\pm 1\}$ thực ra có thể được viết lại thành

$$y \mapsto y^{\frac{p-1}{2}} = \left(\frac{y}{p}\right).$$

Nhận xét rằng, nói riêng $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{\pm 1\}$ là một đồng cấu nhóm.

[1] Nếu cần, xuất phát từ $p \mid x^2+y^2$: ta có thể thay thế x bởi phần dư của x cho p và x bởi $-x$ nên ta có thể giả sử $|x| < p/2$. Tương tự, ta cũng có thể giả sử $|y| < p/2$. Dưới lập luận này, trường hợp cuối cùng được giải quyết dễ dàng dựa vào đánh giá: $x^2+y^2 < p^2$!

Ta có

Định lí 2.0.4 (Luật thuận nghịch toàn phương)**.** *Ta có, với mọi số nguyên tố p lẻ thì*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{nếu } p \equiv 3 \pmod 4 \end{cases}$.
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{nếu } p \equiv 1 \text{ hoặc } 7 \pmod 8 \\ -1 & \text{nếu } p \equiv 3 \text{ hoặc } 5 \pmod 8 \end{cases}$.
3. *Nếu l là một số nguyên tố lẻ* $\neq p$ *thì*

$$\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}} \left(\frac{p}{l}\right).$$

Kết quả kinh điển trên đây cho phép tính ký hiệu Legendre.

Ta đã chứng minh khẳng định đầu tiên của Định lý 2.0.4. Ta sẽ phác thảo chứng minh của Gauss cho các khẳng định còn lại dựa vào khái niệm các tổng Gauss.

Trước hết, ta sẽ trình bày tư tưởng chứng minh của khẳng định thứ 2. Kí hiệu $\bar{\mathbb{F}}_p$ một bao đóng đại số của $\mathbb{F}_p$. Kí hiệu $\alpha \in \bar{F}_p$ một căn nguyên thuỷ thứ 8 của đơn vị, như vậy $\alpha^8 = 1$ nhưng $\alpha^4 = -1$. Chú ý rằng vì $\alpha^4 = -1$ nên $(\alpha^2 + \alpha^{-2})^2 = 0$ và như vậy $\alpha^2 + \alpha^{-2} = 0$. Từ đây, $(\alpha + \alpha^{-1})^2 = 2$. Như vậy,

$$\alpha + \alpha^{-1} = \sqrt{2},$$

trong đó $\sqrt{2}$ được hiểu như là một căn bậc 2 của 2 trong $\bar{\mathbb{F}}_p$. Công thức trên đây là một ví dụ về việc biểu diễn căn bậc hai của một phần tử nào đó của trường cơ sở thành tổ hợp tuyến tính của các căn nguyên thuỷ đơn vị.

Đặt $\beta = \alpha + \alpha^{-1}$ với α là một phần tử nào đó của $\bar{\mathbb{F}}_p$. Thế thì do $\bar{\mathbb{F}}_p$ có đặc số p nên $\beta^p = \alpha^p + \alpha^{-p}$ và $\beta \in \mathbb{F}_p$ khi và chỉ khi $\beta^p = \beta$ (hay $\alpha^p + \alpha^{-p} = \alpha + \alpha^{-1}$).

Kí hiệu Legendre, tổng Gauss và nhúng một trường số bậc hai vào một trường cyclotomic. Trong phần này, ta sẽ sử dụng kí hiệu Legendre $\left(\frac{q}{p}\right)$ để biểu diễn $\sqrt{l}$ như tổ hợp tuyến tính của các căn nguyên thuỷ bậc p của đơn vị. Điều này cho phép ta nhúng trường $\mathbb{Q}(\sqrt{l})$ vào trong một mở rộng cyclotomic. Luật thuận nghịch toàn phương (khẳng định thứ 3) sẽ được thiết lập khi ta thiết lập luật thuận nghịch cho trường cyclotomic và sử dụng phép nhúng trên đây.

Tổng Gauss. Cố định một số nguyên tố lẻ l và α là một căn nguyên thuỷ thứ l của đơn vị trong $\bar{\mathbb{F}}_p$. Đặt

$$y = \sum_{n \in \mathbb{F}_l} \left(\frac{n}{l}\right) \alpha^n.$$

Đây được gọi là một tổng Gauss. Ta chỉ ra được rằng

$$y^2 = (-1)^{\frac{l-1}{2}} l.$$

Đẳng thức này cho thấy

$$\mathbb{Q}\left(\sqrt{(-1)^{\frac{l-1}{2}} l}\right) \hookrightarrow \mathbb{Q}(\sqrt[l]{1}).$$

2.1 Bước lùi trong bài toán biểu diễn $p = x^2 + ny^2$

Ta đã thấy rằng lời giải của bài toán biểu diễn $p = x^2 + y^2$ (khi $p \equiv 1 \pmod 4$) được chia thành hai bước: bước đồng dư và bước lùi. Nhắc lại rằng bước đồng dư thiết lập sự tồn tại của các số nguyên x, y không chia hết cho p sao cho $p \mid x^2 + y^2$. Xuất phát từ điều này, bước lùi cho phép tìm được các số nguyên a, b để $p = a^2 + b^2$. Ta hãy quan tâm đến bài toán tương tự: biểu diễn một số nguyên tố lẻ p dưới dạng

$$p = x^2 + 2y^2.$$

Bước đồng dư được giải quyết rất đơn giản bởi luật thuận nghịch toàn phương. Bằng cách thay thế x, y tương ứng bởi xy', yy' trong đó $yy' \equiv 1 \pmod p$ ta nhận thấy rằng tồn tại các số nguyên x, y không chia hết cho p sao cho $p \mid x^2 + 2y^2$ khi và chỉ khi tồn tại số nguyên z sao cho $p \mid z^2 + 2$ và điều này xảy ra khi và chỉ khi -2 là một số chính phương modulo p. Bằng cách sử dụng luật thuận nghịch toàn phương

$$\left(\frac{-2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}} = (-1)^{\frac{(p-1)(p+5)}{8}}.$$

và do đó điều này xảy ra khi và chỉ khi $p \equiv 1$ hoặc $3 \pmod 8$.

Giả sử số nguyên tố p thoả mãn điều kiện này. Như vậy, tồn tại các số nguyên x, y không chia hết cho p để $p \mid x^2 + 2y^2$. Ý tưởng kỹ thuật của bước xuống thang, với mục đích xác định các số nguyên a, b sao cho $p = a^2 + 2b^2$, là việc sử dụng trường số bậc 2 $K = \mathbb{Q}(\sqrt{-2}) = \{z = x + y\sqrt{-2}; x, y \in \mathbb{Q}\}$.

Tương tự như đối với trường Gauss $\mathbb{Q}(i)$, trường $K = \mathbb{Q}(\sqrt{-2})$ có **vành các số nguyên**

$$R = \mathcal{O}_K = \{x + y\sqrt{-2}; x, y \in \mathbb{Z}\}.$$

và cũng như đối với vành các số nguyên của Gauss, vành R được trang bị ánh xạ chuẩn:

$$\begin{array}{rcl} \mathrm{Nm} : K & \to & \mathbb{R}_+ \\ x + y\sqrt{-2} & \mapsto & x^2 + 2y^2. \end{array}$$

Chú ý rằng ánh xạ chuẩn gửi R lên $\mathbb{N}$. Hơn thế nữa, ánh xạ chuẩn có tính chất sau: với mọi $\alpha \in K$, tồn tại $a \in R$ để

$$\mathrm{Nm}(\alpha - a) < 1.$$

Sự tồn tại của ánh xạ chuẩn với tính chất trên dẫn đến việc R là một miền Euclid, nói riêng là một miền chính.

Quay trở lại với bước lùi của chúng ta. Giả sử x, y là các số nguyên không chia hết cho p sao cho $p \mid x^2+2y^2$. Kí hiệu $a+b\sqrt{-2}$ $(a, b \in \mathbb{Z})$ là một phần tử sinh của ideal $\langle p, x+y\sqrt{-2}\rangle$ (của vành chính R).

Giả sử $p \mid x^2+2y^2$ nhưng $p^2 \nmid x^2+2y^2$. Thế thì do $a+b\sqrt{-2} \mid p$ ta suy ra $\mathrm{Nm}(a+b\sqrt{-2}) \mid \mathrm{Nm}(p)$, có nghĩa là $a^2+2b^2 \mid p^2$. Nhưng $a+b\sqrt{-2} \mid x+y\sqrt{-2}$ nên $\mathrm{Nm}(a+b\sqrt{-2}) \mid \mathrm{Nm}(x+y\sqrt{-2})$, hay $a^2+2b^2 \mid x^2+2y^2$ và do đó $p^2 \nmid a^2+2b^2$. Từ đó suy ra $a^2+2b^2 = 1$ hoặc p. Nhưng ta dễ dàng kiểm tra được rằng trường hợp đầu tiên không thể xảy ra. Từ đó suy ra $a^2+2b^2 = p$. Bước lùi kết thúc. [2]

Bây giờ, ta quan tâm đến bài toán biểu diễn số nguyên tố lẻ p dưới dạng

$$p = x^2 + 3y^2.$$

Cách tiếp cận giống hệt với các bài toán biểu diễn $p = x^2 + y^2$ và $p = x^2 + 2y^2$. Bước đồng dư được thiết lập dựa vào luật thuận nghịch toàn phương và bước lùi vô hạn sử dụng trường số bậc 2 $K = \mathbb{Q}(\sqrt{-3})$. Tuy nhiên, ta sẽ lưu ý rằng trái với các trường hợp trước, vành các số nguyên của K là vành

$$R = \left\{ x + y\frac{\sqrt{-3}+1}{2}; x, y \in \mathbb{Z} \right\}$$

chứ không phải là $R' = \{x + y\sqrt{-3}; x, y \in \mathbb{Z}\}$ như một số bạn đọc có thể chờ đợi tới. Ta vẫn có tính chất cơ bản rằng R là một miền Euclid (dựa vào ánh xạ chuẩn) và do đó là một miền chính. Tính chất này cho phép chúng ta suy luận cho bước lùi giống hệt với các trường hợp trước.

Một cách tổng quát, nếu $K = \mathbb{Q}(\sqrt{d})$ với d là một số nguyên (không chính phương) thì vành các số nguyên của K được mô tả bởi

[2] Một lần nữa, trường hợp $p^2 \mid x^2+2y^2$ có thể được giải quyết bằng cách giả thiết ngay từ đầu $|x| < p/2, |y| < p/2$.

$$\mathcal{O}_K = \left\{ z = x + y\sqrt{d} \in K; \mathrm{Tr}(z) = z + \bar{z} = 2x \in \mathbb{Z}, \mathrm{Nm}(z) = z\bar{z} = x^2 + dy^2 \in \mathbb{Z} \right\}.$$

Cụ thể hơn, ta có

$$\mathcal{O}_K = \begin{cases} \{x + y\sqrt{d}; x, y \in \mathbb{Z}\} & \text{nếu } d \equiv 2,3 \pmod 4 \\ \{x + y\frac{1+\sqrt{d}}{2}; x, y \in \mathbb{Z}\} & \text{nếu } d \equiv 1 \pmod 4 \end{cases}.$$

2.2 Vành Dedekind

Đối với bài toán biểu diễn $p = x^2 + ny^2$ với $n = 5$, phương pháp trên đây của chúng ta không còn áp dụng được nữa. Nếu như bước đồng dư vẫn còn hoạt động thì bước lùi vô hạn gặp trở ngại. Cụ thể là, vành các số nguyên của nó $R = \mathcal{O}_K = \{x + y\sqrt{-5}; x, y \in \mathbb{Z}\}$ của trường số $K = \mathbb{Q}(\sqrt{-5})$ không còn là một miền chính. Đây thậm chí không còn là một vành nhân tử hoá:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}(1 - \sqrt{-5})$$

là hai phân tích khác nhau của 6 thành tích các phần tử nguyên tố trong vành $\mathbb{Z}[\sqrt{-5}]$. Nói riêng, $\mathbb{Z}[\sqrt{-5}]$ không phải là một miền chính nữa. Chính vì vậy, trở ngại chính trong bước lùi vô hạn là việc ideal $(p, x + y\sqrt{-5}\rangle)$ có thể không là một ideal chính.

Để giải quyết trường hợp này, trước tiên, ta cần phải thay thế định lý cơ bản của số học (cho $\mathbb{Z}$) bởi một phiên bản phù hợp. Ta sẽ thấy rằng tương tự của định lý cơ bản của số học trong trường hợp các vành các số nguyên của các trường số là tính phân tích duy nhất của các ideal thành tích các ideal nguyên tố.

Trước tiên, ta đưa vào một số khái niệm và ký hiệu sau. Giả sử R là một miền nguyên với trường các thương K. Nhắc lại rằng các iđêan của R là các R-mô đun con của R. Ta định nghĩa **iđêan phân thức** của R như là các R-mô đun con hữu hạn sinh của K. Ta kí hiệu $Fr(R)$ tập hợp các iđêan phân thức của R. Ta có thể trang bị cho $Fr(R)$ **phép nhân**: với mọi $I_1, I_2 \in Fr(R)$, đặt

$$I_1 I_2 = \langle x_1 x_2; x_1 \in I_1, x_2 \in I_2 \rangle.$$

$Fr(R)$. Ta muốn

- $Fr(R)$ có cấu trúc nhóm;
- có tính chất phân tích duy nhất của các phần tử của $Fr(R)$ thành tích của các iđêan nguyên tố.
- mọi iđêan nguyên tố $\neq 0$ của R đều là cực đại.

Ví dụ cơ bản: các trường số. Giả sử K là một trường số, nói cách khác, một mở rộng hữu hạn của $\mathbb{Q}$. Vành $R = \mathcal{O}_K \subset K$ các số nguyên của K có các tính chất mong muốn đã nêu:

- mọi iđêan nguyên tố $\neq 0$ của $\mathcal{O}_K$ là cực đại;
- $Fr(R)$ là nhóm Abel tự do sinh bởi các iđêan nguyên cực đại: mọi $I = Fr(R)$ đều có thể được viết một cách duy nhất (chính xác tới thứ tự) dưới dạng

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

các $\mathfrak{p}_i$ là các iđêan nguyên tố của R.

Một cách tổng quát,

Định lí 2.2.1 (Dedekind)**.** *Với một miền nguyên R, các khẳng định sau là tương đương:*

1. *$Fr(R)$ là một nhóm Abel tự do sinh bởi các i đêan nguyên tố của R;*
2. *Mọi phần tử của $Fr(R)$ là khả nghịch;*
3. *R là một vành Noether, đóng nguyên, có độ cao bằng 1 (nói cách khác, mọi iđêan nguyên tố $\neq 0$ là cực đại)*

Nhắc lại rằng nói rằng R là một vành đóng nguyên nghĩa là yêu cầu rằng với mọi $x \in K$, nếu x là một phần tử nguyên trên R, có nghĩa là x thoả mãn một phương trình nguyên

$$x^n + a_1 x^{n-1} + \cdots + a_0; a_i \in R$$

thế thì x nằm trong R.

Các vành thoả mãn các tính chất của định lý 2.2.1 trên đây được gọi là các vành Dedekind.

Áp dụng vào các mở rộng hữu hạn của $\mathbb{Q}$. Giả sử K là một mở rộng như vậy, thế thì $K \simeq \mathbb{Q}[X]/(f(X))$, trong đó $f(X) \in \mathbb{Q}[X]$ là một đa thức bất khả qui. Ta định nghĩa

$$\begin{aligned} R &= \text{bao đóng nguyên của } \mathbb{Z} \text{ trong } K \\ &= \left\{x \in K; \exists a_i \in \mathbb{Z} \text{ để } x^n + a_{n-1} + \cdots + a_0 = 0\right\} \\ &= \left\{x \in K; \exists \mathbb{Z} - \text{mô đun con hữu hạn sinh M của } K \text{ sao cho}, xM \subset M\right\} \end{aligned}$$

Thế thì, R là một miền Dedekind. Nói riêng $Fr(R)$ là một nhóm Abel tự do sinh bởi các iđêan cực đại của R.

Ta tiếp tục với ví dụ trên: $K/\mathbb{Q}$ là một mở rộng hữu hạn, $R = \mathcal{O}_K$ là vành các số nguyên của nó, $Fr(R)$ là nhóm Abel tự do sinh bởi các i đêan cực đại. Xét dãy khơp sau đây

$$\ker \to K^\times \to Fr(R) \to Coker = Cl(K)$$

cảm sinh từ đồng cấu tự nhiên $K^\times \to Fr(R)$ gửi mỗi $\alpha \in K$ lên αR. Ta có kết quả cơ bản sau đây

Định lí 2.2.2 (Định lý cơ bản của Lý thuyết số đại số)**.** *Ta có*

1. $Coker = Cl(K)$ *là nhóm Abel hữu hạn.*
2. *(***Định lý Dirichlet về đơn vị, có thể được coi như một mở rộng của lý thuyết các phương trình Pell.***)* $ker = \{\alpha \in K^\times, \alpha R = R\} = R^\times$. *Hơn nữa,* $R^\times$ *là một nhóm Abel hữu hạn sinh. Cụ thể hơn,*

$$R^\times \simeq \mathbb{Z}^r \oplus Q,$$

trong đó Q *là một nhóm hữu hạn (tạo thành từ các căn của đơn vị nằm trong* K*) và* r *được xác định bởi* K *như sau: nếu* $n_1, 2n_2$ *tương ứng là số các nhúng thực, nhúng phức của* K *thì* $r = n_1 + n_2 - 1$ *(*$K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$*).*

Ta hãy lấy ví dụ về các mở rộng bậc 2. Như vậy,

$$K = \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d}; x, y \in \mathbb{Q}\}$$

với d là một số nguyên không chính phương nào đó.

Giả sử $d < 0$. Khi đó $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}(\sqrt{d}) = \mathbb{C}$ và như vậy $n_1 = 0, n_2 = 1$ và như vậy $r = n_1 + n_2 - 1 = 0$ và vì vậy $R^\times$ là một nhóm hữu hạn. Ta cũng dễ dàng kiểm tra được sự kiện này một cách trực tiếp như sau. Giả sử $d \not\equiv 1 \pmod 4$ (vẫn dưới giả thiết $d < 0$). Thế thì $R = \{x + y\sqrt{d}; x, y \in \mathbb{Z}\}$ và

$$R^\times = \{x + y\sqrt{d}; \mathrm{Nm}(x + y\sqrt{d}) = x^2 - dy^2 = \pm 1\}.$$

Từ đây, do $d < 0$, rõ ràng tập các bộ số nguyên x, y thoả mãn điều kiện trên phải là hữu hạn. Trường hợp $d \equiv 2, 3 \pmod 4$ được chứng minh hoàn toàn tương tự.

Trường hợp $d > 0$ thú vị hơn. Như vậy, ta có $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R} \oplus \mathbb{R}$ và như vậy $n_1 = 2, n_2 = 0$. Điều này chứng tỏ $R^\times \simeq \mathbb{Z} \oplus Q$, với Q là nhóm hữu hạn, gồm các căn đơn vị chứa trong K. Giả sử $d \neq 1 \pmod 4$ sao cho $R = \{x + y\sqrt{d}; x, y \in \mathbb{Z}\}$ và

$$R^\times = \{x + y\sqrt{d}; \mathrm{Nm}(x + y\sqrt{d}) = x^2 - dy^2 = \pm 1\}.$$

Như vậy, việc xác định tập $R^\times$ tương đương với việc giải phương trình Pell

$$x^2 - dy^2 = \pm 1.$$

Ngoài ra, trong đẳng cấu $R^\times \simeq \mathbb{Z} \oplus Q$, một phần tử sinh của $\mathbb{Z}$ tương ứng với một nghiệm cơ bản của phương trình Pell đã nêu.

2.3 Số các lớp của một trường số bậc 2

Với K là một trường số, ta nhắc lại rằng $Cl(K)$ kí hiệu nhóm hữu hạn $Fr(R)/K^\times$. Ta quan tâm đến các trường số bậc 2 $K = \mathbb{Q}(\sqrt{d})$ với $d < 0$ (các trường bậc 2 ảo). Gauss đã tính $Cl(K)$ với $-100 < d < 0$.

Tiếp cận của Gauss là như sau. Việc tính toán $Cl(K)$ tương đương với việc xác định số các lớp tương đương của các dạng toàn phương nguyên, nguyên thuỷ với biệt thức bằng d.

Ta nhắc lại rằng một dạng toàn phương hai biến với hệ số nguyên

$$f(x, y) = ax^2 + bxy + cy^2$$

được gọi là **nguyên thuỷ** nếu $\gcd(a, b, c) = 1$.

Các lớp tương đương mà ta nói tới tương ứng với tác động sau đây của nhóm $\mathrm{SL}_2(\mathbb{Z})$ lên tập các dạng toàn phương hai biến, nguyên, nguyên thuỷ: nếu $\gamma = \begin{pmatrix} m & n \\ p & q \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ và f là một dạng toàn phương hai biến,

$$f_{|\gamma}(x, y) = f(mx + ny, px + qy).$$

Chú ý rằng các dạng toàn phương trong một lớp tương đương có cùng định thức:

$$\mathrm{disc}\left(f_{|\gamma}\right) = \mathrm{disc}(f).$$

Định lí 2.3.1. *Giả sử d là một số nguyên âm và $K = \mathbb{Q}(\sqrt{d})$. Tồn tại một song ánh giữa $Cl(K)$, nhóm các lớp các iđêan phân thức của K, và tập các lớp tương đương các dạng toàn phương hai biến, hệ số nguyên, với biệt thức bằng d, xác định dương.*

Chứng minh chi tiết có thể được tìm thấy trong các tài liệu tham khảo sau:

- W. Stein Elementary number theory, chap. 9.
- H. Cohn Advanced number theory.

Ý tưởng chứng minh có thể được tóm lược như sau. Giả sử $I \subset R$ là một iđêan $\neq 0$. Thế thì ta có thể chọn được $a, b \in I$ sao cho

$$I = \{ax + by; x, y \in \mathbb{Z}\}.$$

Hơn nữa, ta có thể chọn a, b sao cho (a, b) là một $\mathbb{Z}$-cơ sở của I. Ta xét dạng toàn phương

$$q(x, y) = \frac{\mathrm{Nm}(ax + by)}{\mathrm{Nm}(I)}.$$

Với x, y chọn cố định thì q xác định dương, nguyên sơ và có biệt thức bằng d. Trong công thức trên đây, $\mathrm{Nm}(ax + by)$ kí hiệu chuẩn của phần tử $ax + by$ trong mở rộng $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ và $\mathrm{Nm}(I)$ kí hiệu chuẩn của iđêan I (mà ta có thể định nghĩa bởi công thức $\mathrm{Nm}(I) =$ lực lượng của nhóm thương R/I.)

Theo Gauss, ta đưa vào khái niệm **dạng rút gọn** như sau. Dạng toàn phương $ax^2 + bxy + cy^2$ được hợi là rút gọn nếu thoả mãn hai tính chất sau:

- $|b| \leq a \leq |c|$;
- Nếu một trong hai bất đẳng thức trên là đẳng thức thì $b \geq 0$.

Định lí 2.3.2 (Gauss)**.** *Mọi lớp tương đương các dạng toàn phương 2 biến chứa duy nhất một dạng rút gọn.*

Bài toán đếm số các lớp của chúng ta qui về việc đếm số các dạng toàn phương rút gọn, nguyên sơ với biệt thức bằng d.

Cụ thể hơn, nếu ta kí hiệu h_d cho số các lớp của $K = \mathbb{Q}(\sqrt{d})$ thì các tính toán của Gauss đem lại:

- $h_d = 1$ với $d = -3, -4, -7, \ldots, -163, \ldots$;
- $h_d = 2$ với $d = -15. - 20, \ldots$.

Ngày 9/9/2015.

3 Các số nguyên tố dạng $x^2 + ny^2$

Ta quan tâm đến bài toán sau đây:

Bài toán: Với p là một số nguyên tố lẻ. Khi nào tồn tại $x, y \in \mathbb{Z}$ để $p = x^2 + ny^2$.

Ta xét các trường hợp $n = 1, 2, 3$. Trong cả ba trường hợp, các lời giải là tương tự nhau và có thể được chia thành hai bước: bước đồng dư và bước lùi vô hạn.

Bước đồng dư. Cụ thể, ta xét phương trình $x^2 + ny^2 \equiv 0 \pmod{p}$ với $x, y \not\equiv 0 \pmod{p}$. Một cách tổng quát, ta có thể sử dụng luật thuận nghịch toàn phương: phương trình có nghiệm khi và chỉ khi $\left(\frac{-n}{p}\right) = 1$.

Bước lùi vô hạn. Đối với các trường hợp $n = 1, 2, 3$, nhận xét cơ bản là trường $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$ là các trường với các vành các số nguyên của chúng là các vành Euclid.

Tuy nhiên, trường hợp $n = 5$ đặt ra vấn đề. Thật vậy, đặt $K = \mathbb{Q}(\sqrt{-5})$ và $\mathcal{O}_K$ vành các số nguyên của nó. Thế thì, ta biết rằng $\mathcal{O}_K$ không là vành nhân tử hoá (do đó không là vành chính và như vậy không Euclid).

Nhận xét rằng điều kiện $p \mid \mathrm{Nm}(x + y\sqrt{-n})$ nhưng $p^2 \nmid \mathrm{Nm}(x + y\sqrt{-n}) \implies$ ideal sinh vởi $(x + y\sqrt{-n}, p)$.

Phương trình $p = a^2 + nb^2$ có lời giải nguyên khi và chỉ khi $(x + y\sqrt{-n}, p)$ là ideal chính với phần tử sinh $a + b\sqrt{-n}$.

Bài toán qui về việc tìm tiêu chuẩn đối với p để:

- $\left(\frac{-n}{p}\right) = 1$;
- $(x + y\sqrt{-n}, p)$ là ideal chính.

Định lí 3.0.3. *Với mọi $n \in \mathbb{N}$, n không có ước chính phương và $n \equiv 3 \pmod 4$, tồn tại đa thức $f_n \in \mathbb{Z}[X]$ với bậc h_{-4n} (ở đây h_{-4h} kí hiệu cấp của nhóm các lớp ideal của $K = \mathbb{Q}(\sqrt{-n})$) sao cho phương trình $p = x^2 + ny^2$ có nghiệm nguyên khi và chỉ khi*

- $\left(\frac{-n}{p}\right) = 1$*, nói cách khác phương trình $x^2 + n \equiv 0 \pmod{p}$ có nghiệm;*
- *phương trình $f_n(x) \equiv 0 \pmod{p}$ có nghiệm.*

[3]

Nhận xét 3.0.4. *Ta cần luật thuận nghịch cho cả hai điều kiện đã nêu trong định lý trên.*

Lời giải tổng quát cần sử dụng việc tìm hiểu cấu trúc của vành các số nguyên đại số của K.

[3]Hơn nữa, ta có thể chọn $f_n(x)$ là đa thức cực tiểu của bất kì một phần tử nguyên $\alpha \in L$ thoả mãn $L = K(\alpha)$ sao cho L là trường các lớp Hilbert của $K = \mathbb{Q}(\alpha)$.

3.1 Vành các số nguyên của một trường số

Ta xét tình huống tổng quát sau đây. Giả sử K là một trường số. Kí hiệu $R = \mathcal{O}_K$, vành các số nguyên của K, $Fr(R)$ kí hiệu tập các ideal phân thức của R. Thế thì $Fr(R)$ là một nhóm Abel tự do sinh bởi các ideal cực đại của R. Nói một cách khác, với mọi $\mathfrak{a} \in Fr(R)$ thì ta có phân tích duy nhất sau đây

$$\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r},$$

trong đó $\mathfrak{p}_1, \cdots, p_r$ là các ideal cực đại của R và $m_1, \ldots, m_r$ là các số nguyên.

Ta quan tâm đến tình huống tương đối: $K/\mathbb{Q}, R/\mathbb{Z}$. Câu hỏi đặt ra là: với số nguyên tố p, thế thì $p\mathbb{R}$ (ideal chính sinh bởi p trong R) được phân tích ra sao? Nói một cách khác, công thức

$$p\mathbb{R} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$$

phụ thuộc như thế nào vào p ?

Ta biết rằng mở rộng K có thể được hiểu dưới dạng $K \simeq \mathbb{Q}[X]/(P)$, trong đó $P(X) \in \mathbb{Q}[X]$ là một đa thức bất khả qui.

Đặt

$$S = \{p \in \mathbb{P}; p \mid \text{ chia hết các mẫu số của } P\}.$$

Thế thì với mọi $p \notin S$, đa thức $P \mod p \in \mathbb{F}_p[X]$ là rút gọn modulo p của P (có nghĩa). Đặt

$$T = \{p \in \mathbb{P}; p \mid \text{disc}(P)\}.$$

Có các khả năng sau đây:

- P có nghiệm bội trong $\bar{\mathbb{F}}_p$, nghĩa là $p \mid \text{disc}(P)$.
- P không có nghiệm bội trong $\bar{\mathbb{F}}_p$.

Bây giờ, ta xét trường hợp $p \notin S \sqcup T$. Thế thì, $P \mod p$ không có nghiệm bội.

Câu hỏi: phân tích $P \mod p$ thành tích các đa thức bất khả qui.

Định lí 3.1.1. *Ta có $P \mod p = Q_1 \cdots Q_m$, với $\mathbb{Q}_i \in \mathbb{F}_p[X$ là các đa thức bất khả qui khi và chỉ khi $(p) = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ là phân tích của $(p) = pR$ trong $Fr(R)$.*

Chứng minh. Chứng minh dựa vào Bổ đề Hensel quen thuộc. □

Để có một hình dung về kết quả trên đây, ta đưa ra một vài ví dụ về các mở rộng bậc 2.

Xét đa thức $P = X^2 - d$ với d không chính phương (sao cho P bất khả qui) và $K = \mathbb{Q}[X]/(P)$. Chú ý rằng khi đó $\text{disc}(P) = 4d$.

Xét các số nguyên tố $p \nmid \text{disc}(P) = 4d$. Xét đa thức $X^2 - d \mod p$:

- Nếu $\left(\frac{d}{p}\right) = 1$ thì $X^2 - d$ có nghiệm $\alpha, \beta \in \mathbb{F}_p$ và $X^2 - d = (X - \alpha)(X - \beta)$. Trong trường hợp này thì

$$(p) = \mathfrak{q}_1\mathfrak{q}_2$$

  với $\mathfrak{q}_1 \neq \mathfrak{q}_2$ là các ideal nguyên tố trong R. Trong trường hợp này, ta nói p **chẻ ra** trong R.
- Nếu $\left(\frac{d}{p}\right) = -1$ thì $X^2 - d \mod p$ bất khả qui. Như vậy, trong trường hợp này (p) vẫn còn là một ideal nguyên tố trong R. Trong trường hợp này, ta nói p là **trơ** trong R.
- Nếu $p \mid d$ (nhưng $p \nmid 4d$) thế thì $(p) = \mathfrak{q}^2$. Trong trường hợp này, ta nói p **rẽ nhánh** trong R.

Chú ý rằng p rẽ nhánh thì $p \mid \text{disc}(P)$ nhưng $p \mid \text{disc}(P)$ không dẫn đến p rẽ nhánh!

Trong trường hợp tổng quát $K = \mathbb{Q}[X]/(P)$. $p \mid \text{disc}(P)$, $n = \deg P = [K : \mathbb{Q}]$.

Thế thì $(p) = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ và $P \mod p = Q_1 \cdots Q_r$ với $\deg Q_i = n_i$. Ta luôn có

$$n = n_1 + \cdots n_r.$$

Nói cách khác, môdulo việc sắp thứ tự, $(n_1 \geq n_2 \geq \cdots \geq n_r)$ là một phân hoạch của n.

Mục tiêu của chúng ta là phát biểu lại dưới ngôn ngữ của lý thuyết Galois. Nhắc lại rằng ta có $K = \mathbb{Q}[X/(P)$ là một mở rộng bậc n của $\mathbb{Q}$. Kí hiệu $\alpha_1, \ldots, \alpha_n$ là các nghiệm của P trong $\bar{Q}$. Nhóm Galois tuyệt đối

$$\Gamma = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

tác động một cách tự nhiên lên tập các nghiệm $\{\alpha_1, \ldots, \alpha_n\}$.

Nói rằng P là một đa thức bất khả qui nghĩa là nói Γ tác động một cách bắc cầu lên tập các nghiệm của nó.

Tương tự, ta có khái niệm các trường $\mathbb{F}_p, \mathbb{Q}_p$, vân vân. Giả sử $p \notin S$, khi đó $P \in \mathbb{Z}_p[X]$ và $\text{disc}(P) \in \mathbb{Z}_p^\times$ nếu $p \notin T$.

Ta viết $P(X) = (X - \alpha_1)\cdots(X - \alpha_n)$ với α_i là các nghiệm trong $\bar{\mathbb{Q}}_p$ của P.

Xét trường hợp $p \nmid \text{disc}(P)$, ta có phần tử $\sigma_p \in \mathfrak{S}_n$ xác định duy nhất sai khác liên hợp (tương ứng phân hoạch $n = n_1 + \cdots n_r$).

Bài toán của chúng ta có thể được phát biểu lại dưới ngôn ngữ của lý thuyết Galois như sau: với một mở rộng hữu hạn $K/\mathbb{Q}$ và $p \nmid \text{disc}(K) = \text{disc}(P)$, kí hiệu $[\sigma_p]$ lớp liên hợp trong $\mathfrak{S}_n$ (đã đưa vào ở trên), hãy tìm hiểu "qui luật" của ánh xạ

$$p \mapsto [\sigma_p]$$

Ánh xạ này được biết đến dưới tên gọi: "ánh xạ thuận nghịch". Tìm hiểu "qui luật" của ánh xạ này nghĩa là hiểu "luật thuận nghịch".

Dưới ngôn ngữ của lý thuyết Galois, trường hợp các mở rộng cyclotomic lại đơn giản hơn các mở rộng bậc hai. Nhắc lại rằng, K là một mở rộng cyclotimic của $\mathbb{Q}$ có nghĩa là $K = \mathbb{Q}(\zeta_l)$ với ζ là một căn nguyên thuỷ bậc l của đơn vị nào đó. Ta xét trường hợp l là một số nguyên tố. Khi đó, ζ là nghiệm của đa thức $P = \Phi_l = X^{l-1} + \cdots + 1$.

Câu hỏi: $P \mod p = \Phi_l \mod p$ phân tích như thế nào trong $\mathbb{F}_p[X]$ và σ_p tác động như thế nào lên các nghiệm của $\Phi_l \mod p$ trong $\bar{\mathbb{F}}_p$. Kí hiệu $\zeta \in \bar{\mathbb{F}}_p$ là nghiệm của $\Phi_l \mod p$: $\zeta^l = 1, \zeta \neq 1$. Thế thì

$$\sigma_p(\zeta) = \zeta^p.$$

Câu hỏi là: σ_p phân tích như thế nào trong $\mathfrak{S}_{l-1}$? Câu trả lời là

$$\sigma_p = (q, q, \cdots, q)$$

với q là số tự nhiên nhỏ nhất sao cho $l \mid p^q - 1$.

Để chứng minh luật thuận nghịch toàn phương, ta có thể nhúng vào các mở rộng cyclotomic. Lưu ý rằng, việc nhúng các mở rộng bậc 2 vào các mở rộng cylcotomic có thể được thực hiện thông qua việc sử dụng các tổng Gauss.

Nhận xét rằng $\text{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ là một nhóm Abel. Trong trường hợp K là một mở rộng Abel của $\mathbb{Q}$, nói cách khác khi $\text{Gal}(K/\mathbb{Q})$ thế thì ta có thể nhúng K vào trong một mở rộng cyclotomic nào đó của $\mathbb{Q}$.

Luật thuận nghịch Artin: xét mở rộng Abel $K/\mathbb{Q}$ với $\text{Gal}(K/\mathbb{Q}) = A$. Ta có một **ánh xạ thuận nghịch Artin**

$$p \mapsto \sigma_p \in A.$$

Luật thuận nghịch Hilbert. Xét mở rộng L/K trong trường hợp

- Abel;
- không rẽ nhánh:
  - $\text{disc}(\mathcal{O}_L : \mathcal{O}_K) = 1$
  - không rẽ nhánh ở vô cùng: $L \otimes \mathbb{R} = \mathbb{R}^{nn_1} \times \mathbb{C}^{nn_2}$ thì $K \otimes \mathbb{R} = \mathbb{R}^{n_1} \otimes \mathbb{C}^n$ (đây là một điều kiện kĩ thuật).
- cực đại.

Thế thì ta có

$$\text{Gal}(L/K) \simeq Cl(K) = Fr(K)/K^\times$$

Ánh xạ $\mathfrak{p} \in Fr(K)/K^\times \mapsto \text{Gal}(L/K)$ được gọi là ánh xạ thuận nghịch Artin.

Xét một trường số bậc 2, $K = \mathbb{Q}(\sqrt{-n})$, h_K có thể lớn. GọiL là trường các lớp của Hilbert của K: như vậy, L là mở rộng Abel, không rẽ nhánh, cực đại của K và ta có

$$\text{Gal}(L/K) \simeq Cl(K).$$

Ta có sơ đồ sau đây:

trong đó các mở rộng L/K và $K/\mathbb{Q}$ là Abel.

Với một số nguyên tố p, phương trình $x^2 + ny^2 = p$ có nghiệm nguyên khi và chỉ khi

trong đó p chẻ và mỗi $\mathfrak{q}_1, \mathfrak{q}_2$ là chẻ và điều này xảy ra khi và chỉ khi

- $\left(\frac{-n}{p}\right) = 1$;
- Đặt $p\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ thì ảnh của $\mathfrak{q}_1$ trong $\text{Gal}(L/K)$ bằng $Cl(K)$.

Điều kiện cuối phiên dịch lại điều kiện $f(X) \equiv 0 \pmod{p}$ có nghiệm với $L = \mathbb{Q}[X]/(f))$. Như vậy, ta cần một luật thuận nghịch cho mở rộng không Abel (mở rộng $L/\mathbb{Q}$ không nhất thiết Abel.)

10/9/2015.

Chủ đề của 3 buổi trước: tính hữu hạn của nhóm các lớp, tính hữu hạn sinh của nhóm các phần tử khả nghịch của vành các số nguyên của một trường số và cuối cùng là lý thuyết trường các lớp.

Chủ đề của bài giảng hôm nay là về Lý thuyết số giải tích. Một số cuốn sách tham khảo:

- Apostol.
- Chandrashekarar.
- Kowalski's blog: smoothing sum.
- Mellin transform (xem Zagier: Appendix to some article: The Mellin transform and related techniques).

Bài toán cơ bản nhất của lý thuyết số là bài toán sau

Bài toán: Sự phân bố của các số nguyên tố ?

Ta có thể liệt kê một số kết quả kinh điển sau:

Định lý về số nguyên tố $\pi(x) = \sharp\{p \in \mathbb{P}; p < x\}$ thì

$$\pi(x) \sim \frac{x}{\log x}, \text{khi } x \to \infty.$$

Định lý Dirichlet về

1. sự tồn tại vô hạn số nguyên tố trong cấp số cộng $\{an + b; n \in \mathbb{N}\}$ với $(a, b) = 1$.
2. Hơn nữa, $\pi_{a,b}(x) = \{p \in \mathbb{P}; p < x, p \equiv b \pmod{a}\}$ thì

$$\pi_{a,b}(x) \sim \frac{x}{\log x \phi(a)}, \text{khi } x \to \infty.$$

Chẳng hạn, ta sẽ chỉ ra sự tồn tại vô hạn số nguyên tố có dạng $4k + 3$. Ý tưởng chứng minh giống hệt với chứng minh của Euclid về sự tồn tại vô hạn số nguyên tố. Ta tiến hành như sau: giả sử tồn tại hữu hạn các số nguyên tố dạng $4k + 3$ là $p_1, \ldots, p_n$. Thế thì tồn tại một ước nguyên tố q của $4p_1^2 \cdots p_n^2 + 3$ có dạng $4k + 3$. Số nguyên tố này hiển nhiên không nằm trong tập $\{p_1, \ldots, p_n\}$ đã liệt kê.

Lập luận trên đây không thể được áp dụng để chứng minh sự tồn tại vô hạn số nguyên tố trong một cấp số cộng.

Ý tưởng của Dirichlet là như sau: sự phân bố các số nguyên tố $\Leftrightarrow$ cực của ζ tại 1. Nhắc lại rằng

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s}, \quad \Re(s) > 1.$$

Hàm ζ có các tính chất cơ bản sau đây:

- chỉnh hình trên miền $\Re(s) > 1$;
- thác triển được thành một hàm phân hình trên toàn bộ $\mathbb{C}$;
- có cực đơn tại $s = 1$ và nếu ta viết

  $$\zeta = \frac{1}{1-s} + \Psi(s)$$

  thì Ψ chỉnh hình trên miền $\Re(s) > 0$.
- Tích Euler:

  $$\zeta(s) = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1}, \quad \Re(s) > 1.$$

  Hay một cách tương đương

  $$\log \zeta(s) = \sum_{p \in \mathbb{P}} -\log(1 - p^{-s}).$$

  Như vậy,

  $$\log \zeta(s) \sim \sum_{p \in \mathbb{P}} p^{-s}.$$

Từ đó suy ra, khi $s \to 1^+$ thì

$$\sum_{p \in \mathbb{P}} p^{-s} \sim \log\left(\frac{1}{s-1}\right).$$

Mật độ. Với $M \subset \mathbb{P}$, ta định nghĩa mật độ Dirichlet của M như sau:

$$\delta_D(M) := \lim_{s \to 1^+} \frac{\sum_{p \in M} p^{-s}}{\log\left(\frac{1}{1-s}\right)}.$$

Nhận xét rằng khi $M = \mathbb{P}$ thì $\delta_D(M) = 1$ còn nếu $M_+ = \{p \in \mathbb{P}; p \equiv 1 \pmod 4\}$ và $M_- = \{p \in \mathbb{P}; p \equiv 3 \pmod 4\}$ thì $\delta_D(M_+) = \delta_D(M_-) = 1/2$ (Dirichlet). Một cách tổng quát, nếu $M = \{p; p \equiv b \pmod a\}$ thì $\delta_D(M) = \frac{1}{\phi(a)}$.

Ta viết lại dưới ngôn ngữ L-hàm như sau. Xét đặc trưng $\chi : \mathbb{N} \to \mathbb{C}^\times$ gửi n lên

- 0 nếu $2 \mid n$;
- -1 nếu $n \equiv 3 \pmod 4$;
- 1 nếu $n \equiv 1 \pmod 4$.

Thế thì χ là một hàm số học theo nghĩa $\chi(mn) = \chi(m)\chi(n)$ với mọi $(m,n) = 1$. Đặt

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}.$$

Tính nhân của χ cho phép biểu diễn lại hàm số trên đây dưới dạng tích Eucler:

$$L(\chi, s) = \prod_{p \in \mathbb{P}} (1 - \chi(p)p^{-s})^{-1}.$$

Do đó ta có định lý Dirichlet do $L(\chi, s)$ có thác triển chỉnh hình (không có cực tại $s = 1$).

Đối với trường hợp sự phân bố các số nguyên tố modulo 4 ta quan sát sự phân tích của các số nguyên tố p trong $K = \mathbb{Q}(\sqrt{-1})$. Từ luật thuận nghich toàn phương ta có

- $p \equiv 1 \pmod 4$ thì p chẻ trong K;
- $p \equiv 1 \pmod 4$ thì p trơ trong K.

—

Qui trình để chứng minh định lý về số nguyên tố là như sau: hàm số học $n \mapsto a_n$ (đến từ việc ước lượng $\sum_{n \le X} a_n$) $\implies$ chuỗi Dirichlet $D_{(a_n)}(s) = \sum_n a_n n^{-s}$ $\implies$ thác triển phân hình trên $\mathbb{C}$ $\implies$ cực của D tại 1 $\implies$ ước lượng $\sum_{n \le X} a_n$.

Các từ khóa cho qui trình này gồm: biến đổi Mellin, chuỗi Dirichlet, tổng trơn.

3.2 Biến đổi Mellin

Giả sử có

$$\phi : \mathbb{R}_+ \to \mathbb{C}$$

là một hàm liên tục theo từng đoạn.

Ta giả thiết ϕ có giá compact: $\phi = 0$ ngoài một khoảng $[a, b]$ với $0 < a < b < \infty$ nào đó. Thế thì ta đặt

$$\tilde{\phi}(s) = \int_0^\infty \phi(t) t^{s-1} dt.$$

Chú ý rằng nếu ϕ có giá compact thì tích phân trên hội tụ tuyệt đối và hội tụ là đều trên các tập compact. Hơn nữa, $\tilde{\phi}(s)$ là chỉnh hình trên $\mathbb{C}$.

Ta có biến đổi Mellin ngược:

$$\phi(t) = \frac{1}{2\pi i} \int_{C-i\infty}^{C+i\infty} \tilde{\phi}(s) t^{-s} dt.$$

Một số nhận xét về biến đổi Mellin:

- $\bar{\phi}(s)$, $s \to +\infty$.
- Modulo việc đồng nhất $\mathbb{R}$ với $\mathbb{R}_+$ bằng biến đổi mũ (nhận xét rằng dt/t là độ đo bất biến của $\mathbb{R}_+$) thì biến đổi Mellin thực ra là biến đổi Fourier: $\bar{\phi}(s)_{|\Im(s)=0}$ là biến đổi Fourier của ϕ
- Trái với biến đổi Fourier, ta chỉ có 1 trục, biến đổi Mellin ngược có thể được hiểu như biến đổi Fourier trên $\mathbb{C}$, hay biến đổi Fourier theo nhiều trục khác nhau.
- Chú ý rằng để có công thức biến đổi Fourier ngược, ta cần phải thêm một số giả thiết về hàm số, chẳng hạn, các hàm là trơn. Khi ϕ là trơn thì $\bar{\phi}$ là một hàm giảm nhanh khi $\Im(s) \to \infty$.

Ta hãy tìm hiểu biến đổi Mellin của một hàm $\phi : \mathbb{R}_+ \to \mathbb{C}$ trơn, giảm nhanh (tại 0 và ∞). Điều kiện giảm nhanh nói rằng với mọi $n \in \mathbb{N}$ thì

$$|\phi(t)| < t^{-n}, \text{khi } t \to +\infty, \quad \text{và } |\phi(t)| < t^n, \text{khi } t \to 0.$$

Khi đó $\tilde{\phi}(s)$ là một hàm chỉnh hình trên toàn bộ $\mathbb{C}$.

Ta viết lại biến đổi Mellin dưới dạng

$$\tilde{\phi}(s) = \int_0^\infty \phi(t) t^{s-1} dt = \int_0^1 \phi(t) t^{s-1} dt + \int_1^\infty \phi(t) t^{s-1} dt.$$

Bây giờ, ta giả thiết ϕ giảm nhanh tại ∞ và giả thiết tại 0 ϕ có khai triển Taylor tiệm cận

$$\phi(t) = a_0 + a_1 t + \cdots$$

Với mọi n,

$$\phi(t) = \sum_{i=0}^{n} a_i t^i + o(t^n).$$

Dưới giả thiết này về hàm ϕ thì

- tích phân $\int_1^\infty \phi(t)t^{s-1}dt$ hội tụ tuyệt đối với mọi s.
- tích phân $\int_0^1 \phi(t)t^{s-1}dt$ hội tụ tuyệt đối với $\Re(s) > 0$.

Như vậy $\tilde{\phi}$ định nghĩa một hàm chỉnh hình trên $\Re(s) > 0$. Để thác triên $\tilde{\phi}(s)$ lên toàn bộ $\mathbb{C}$ ta viết

$$\begin{aligned} \tilde{\phi}(s) &= \int_0^1 \phi(t)t^{s-1}dt + \int_1^\infty \phi(t)t^{s-1}dt \\ &= \int_0^1 \left(\phi(t) - \sum_{i=0}^n a_i t^i\right) t^{s-1}dt + \int_1^\infty \left(\sum_{i=0}^n a_i t^i\right) t^{s-1}dt + \int_1^\infty \phi(t)t^{s-1}dt \end{aligned}$$

Tích phân thứ nhất hội tụ tuyệt đối với mọi $\Re(s) > -n$, tích phân thứ hai có thể ước lượng được $\sum_0^n \frac{a_i}{i+s}$.

—

Chú ý rằng, với $\phi(t) = e^{-t}$ thì biến đổi Mellin nhận được chính là hàm $\Gamma(s)$. Ta nhắc lại rằng $\Gamma(s)$ có thác triển phân hình lên toàn bộ $\mathbb{C}$ với các cực đơn tại $0, -1, -2, \ldots$. Chứng minh trên đây hoàn toàn dựa vào ý tưởng các lập luận quen thuộc để thiết lập các tính chất đã nêu của Γ: ϕ là hàm trơn $\implies$ công thức nghịch đảo Mellin bởi vì $\tilde{\phi}(\sigma + it)$ là một hàm giảm nhanh khi $t \to \pm\infty$. Điều này dẫn đến $\tilde{\phi}$ là hàm chỉnh hình trên $\Re(s) > -1$ và ta có công thức

$$\phi(t) = \frac{1}{2\pi i} \int_{-i\infty}^{+i\infty} \tilde{\phi}(s)t^{-s}dt.$$

Điều này cho thấy nếu ta biết $\tilde{\phi}$ thác triển phân hình trên $\mathbb{C}$ với các cực tại $0, -1, \ldots$ thì do tính trơn của ϕ và sử dụng công thức tích phân Cauchy cho $\tilde{\phi}$ ta có thể đưa ra dáng điệu tiệm cận của $\phi(t)$ khi $t \to 0$.

Ứng dụng. Ta hãy áp dụng qui trình trên đây cho các hàm số học $a : n \mapsto a_n$ với:

- $a_n = 1$;
- $a_n = \mu(n) = 0$ nếu n có ước chính phương và $(-1)^r$ nếu n là tích của đúng r số nguyên số phân biệt.
- $a_n = 1$ nếu n nguyên tố và 0 nếu không.
- $a_n = \Lambda(n) = \begin{cases} \log p & \text{nếu } n = p^r \\ 0 & \text{nếu không.} \end{cases}$.

Các chuỗi Dirichlet nhận được tương ứng là

- $\zeta(s) = \sum_n n^{-s} = \prod_p (1 - p^{-s})^{-1}$;
- $\zeta(s)^{-1} = \sum_n \mu(n) n^{-s} \prod_p (1 - p^{-s})^{-1}$
- $D_{\mathbb{P}}(s)$;
- $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}$ (đạo hàm log của ζ).

Chẳng hạn để chứng minh rằng $\pi(x) \sim \frac{x}{\log(x)}$. Khẳng định này tương đương với

$$\sum_{n \leq X} \Lambda(n) \sim X.$$

Kỹ thuật ở đây là việc làm trơn tổng trên bằng cách viết lại

$$\sum_{n \leq X} \Lambda(n) = sum_{n \leq X} \Lambda(n) \phi(\frac{n}{X}),$$

trong đó ϕ là một hàm trơn, xấp xỉ hàm $\mathbf{1}_{[0,1]}$.

Ta có

$$(\Lambda * \phi)(t) = \sum_n \Lambda(n) \phi(nt)$$

Dáng điệu tiệm cận của $\Lambda * \phi(t)$ khi $t \to 0$ được cho bởi $t^{-1} + o(t^{-1})$ theo Riemann:

$$-\frac{\zeta'(s)}{\zeta(s)} \cdot \tilde{\phi}$$

Biến đổi Mellin:

- thác triển phân hình;
- cực;
- tích phân Cauchy.

3.3 Hàm zeta của Riemann

Nhắc lại rằng

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

là hội tụ tuyệt đối với $\Re(s) > 1$, thác triển phân hình trên $\mathbb{C}$.

Ta đã nói rằng thay vì làm việc trực tiếp với ζ, sẽ dễ dàng hơn nếu làm việc với $\zeta \cdot \phi$, với $\phi : \mathbb{R}_+ \to \mathbb{C}$ thích hợp. Ta sẽ chọn ϕ sao cho

- là một hàm giảm nhanh;
- có khai triển Taylor tại 0: $\phi(t) = \sum_{n=0}^{\infty} a_n t^n$ (xung quanh 0).

Ta biết rằng khi đó $\tilde{\phi}$ là một hàm phân hình trên $\mathbb{C}$ với các cực tại $0, -1, -2, \ldots$ với các thặng dư tương ứng là $a_0, a_1, a_2, \ldots$.

Đặt

$$\phi_+(t) = \sum_{n=0}^{\infty} \phi(nt).$$

Giả sử đây là một hàm:

- trơn,
- giảm nhanh tại ∞;
- (Điều kiện khó): biết dáng điệu tiệm cận khi $t \to 0$.

Khi đó ta có biến đổi Mellin $\tilde{\phi_+}$:

$$\tilde{\phi_+}(s) = \int_0^{\infty} \phi_+(t) t^{s-1} dt = \zeta(s)\tilde{\phi}(s).$$

Ta hãy trình bày qui trình trên cho trường hợp $\phi(t) = e^{-t}$. Khi đó ta có $\tilde{\phi}(s) = \Gamma(s)$,

$$\phi_+(t) = \sum_{n=1}^{\infty} e^{-nt} = \frac{1}{e^t - 1} = t^{-1} + \cdots .$$

Hơn nữa, ta có thác triển Taylor khi $t \to 0$:

$$\phi_+(t) = \sum_{0}^{\infty} \frac{B_n}{n!} t^n$$

trong đó B_n là số Bernoulli thứ n: $B_0 = 1, B_1 = -1/2, B_2 = 1/6, \ldots$.

Ta suy ra $\tilde{\phi_+}$ thác triển phân hình trên $\mathbb{C}$ với các cực tại $1, 0, -1, \ldots$ với các thặng dư là các số Bernoulli tương ứng. Bây giờ, công thức

$$\tilde{\phi_+}(s) = \zeta(1)\tilde{\phi}(s)$$

dẫn đến

$$\zeta(s) = \frac{\tilde{\phi_+}(s)}{\Gamma(s)}$$

là một hàm phân hình, có cực tại $s = 1$ và với thặng dư tại $s = 1$ bằng 1!

Ví trên đây với $\phi(t) = e^{-t}$ dựa vào một công thức may mắn của $\tilde{\phi}$. Trong trường hợp tổng quát thì sao ? Ý tưởng tổng quát là sử dụng công thức tổng Poisson.

Giả sử $\phi : \mathbb{R}_+ \to \mathbb{C}$ là một hàm trơn, giảm nhanh tại ∞ và

$$\psi(t) = \sum_{n \in \mathbb{N}} \phi(nt)$$

Ta giả sử rằng ϕ đến từ một hàm $\mathbb{R} \to \mathbb{C}$ với các tính chất: trơn, chẵn,giảm nhanh khi $|t| \to \infty$, Thế thì biến đổi Fourier của nó $\hat{\phi} : \mathbb{R} \to \mathbb{C}$ cũng là một màm giảm nhanh khi $|t| \to \infty$. Ta có công thức tổng Poisson sau đây

$$\sum_{n \in \mathbb{Z}} \phi(n) = \sum_{n \in \mathbb{Z}} \hat{\phi}(n).$$

Từ công thức tổng Poisson ta suy ra

$$\sum_{n\in\mathbb{Z}}\phi(nt)=t^{-1}\sum_{n\in\mathbb{Z}}\hat{\phi}(nt^{-1})$$

Khi $t^{-1}\to 0$, ta có ước lượng

$$\sum_{n\in\mathbb{Z}}\hat{\phi}(nt^{-1})=\hat{\phi}(0)+o(t^{-n}).$$

Từ đó suy ra

$$\phi(0)+2\phi_+(t)=t^{-1}\hat{\phi}(0)+o(t^{-n})$$

Và do vậy,

$$\phi_+(t)=\frac{1}{2}\left(t^{-1}\phi\hat{(}0)+o(t^{-n})\right)$$

Kết hợp phương trình hàm của ζ ta có

$$\tilde{\phi}(s)=\ \tilde{\hat{\phi}}_+(1-s)$$

Với $\phi=e^{-\pi t^2}$ thì $\phi=\hat{\phi}$.

11/9/2015.

4 Một số mở rộng

Mục tiêu của bài giải là trình bày một số mở rộng một số vấn đề về lý thuyết số, cả trong lý thuyết số đại số lẫn lý thuyết số giải tích đã được trình bày tại các bài giảng trước.

Nhắc lại rằng, bài toán biểu diễn $p=x^2+ny^2$ đã dẫn đến một số trở ngại và đòi hỏi một luật thuận nghịch không Abel. Ta cũng lưu ý rằng, thông qua các ví dụ đã trình bày, ta có thể nhận thấy rằng luật thuận nghịch trong trường hợp Abel rất hữu hiệu, kể về khía cạnh thực hành lẫn khía cạnh lý thuyết.

4.1 Luật thuận nghịch Abel

Ta nhắc lại luật thuận nghịch toàn phương

$$\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}} \left(\frac{p}{l}\right).$$

Công thức này cho thấy khi ta cố định l thì ký hiệu $\left(\frac{l}{p}\right)$ chỉ phụ thuộc vào lớp đồng dư $p \pmod{4l}$. Một cách cụ thể hơn, ta nhận được một **đặc trưng Dirichlet**

$$\left(\frac{l}{\cdot}\right) : (\mathbb{Z}/4l\mathbb{Z})^\times \to \{\pm 1\}.$$

Hơn nữa, giá trị này phụ thuộc vào tính chất phân tích (chẻ ra, trơ) của số nguyên tố p trong mở rộng bậc hai $\mathbb{Q}(\sqrt{l})$.

Ta cũng đã đề cập đến luật thuận nghịch Hilbert. Cố định một trường số K. Khi đó, tồn tại duy nhất một trường L (trường các lớp của Hilbert) với các tính chất sau: L/K hoàn toàn không rẽ nhánh (kể cả tại ∞), Abel, cực đại (với các tính chất đó.)

Khi đó, ta có

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\quad = \quad} & Cl(\mathcal{O}_K) \\ & \nwarrow^{Art} \quad \nearrow & \\ & \mathrm{Specm}(\mathcal{O}_K) & \end{array}$$

Một cách tổng quát, ta có luật thuận nghịcg Abel (lý thuyết trường các lớp). Một trong các mục tiêu chính của lý thuyết trường các lớp là việc mô tả các mở rộng Abel L của một trường số K cho trước và mô tả ánh xạ thuận nghịch Artin $\mathrm{Specm}(\mathcal{O}_K) \to \mathrm{Gal}(L/K)$.

Nhóm các lớp idele. Một trong các điểm chung của luật thuận nghịch bậc hai và luật thuận nghịch Artin là "các lớp" (các lớp modulo $4l$ với luật thuận nghịch toàn phương và các lớp iđêan trong luật thuận nghịch Hilbert).

Ta sẽ chỉ trình bày các lớp idele của trường các số hữu tỷ. Với $K = \mathbb{Q}$, ta xét cảc **định giá** của nó, nói cách khác, các ánh xạ $|\cdot| : \mathbb{Q}^\times \to \mathbb{R}_+$ với các tính chất

$$|xy| = |x||y|, \quad |x+y| \le |x| + |y|, \forall x, y \in \mathbb{Q}.$$

Ta có thể mô tả một các chi tiết tất cả các định giá có thể của $\mathbb{Q}$ (Định lý Ostrowski). Cụ thể, sai khác tương đương, các định giá của $\mathbb{Q}$ được liệt kê như sau

- định giá Euclid: $|\cdot|_\infty$ gửi mỗi x lên giá trị tuyệt đối quen thuộc
- các định giá p-adic: với mỗi số nguyên tố p, $|\cdot|_p$ gửi mỗi số hữu tỷ $p^r \frac{m}{n}, (p, mn) = 1$ lên p^{-r}.

Đối với các định giá trên đây của $\mathbb{Q}$, ta có thể đầy đủ $\mathbb{Q}$ (tương ứng với các định giá đó). Kết quả là, ta nhận được các trường đầy đủ hóa của $\mathbb{Q}$, cụ thể là $\mathbb{R}$ (đối với định giá Ac-si-mét) và $\mathbb{Q}_p$, và mỗi định giá ban đầu có thể được mở rộng thành một định giá trên các đầy đủ hoá đó.

Ta định nghĩa các **adele** như sau:

$$\mathbb{A} = \{(x_p, x_\infty); x_p \in \mathbb{Q}_p, x_\infty \in \mathbb{R}, x_p \in \mathbb{Z}_p \quad \text{với hầu hết các } \ p\}.$$

Tập hợp $\mathbb{A}$ cùng các phép toán $+, \times$ tự nhiên hiển nhiên là một vành. Ta có

$$\mathbb{Q} \hookrightarrow \mathbb{A}$$

bởi phép nhúng đường chéo. Hơn nữa, ta có thể trang bị cho $\mathbb{A}$ một tô pô tự nhiên. Ta có một số tính chất quan trọng:

- $\mathbb{A}$ là một vành compact địa phương.
- $\mathbb{Q}\backslash\mathbb{Q}$ là compact.

Ta có $\mathbb{A}/\mathbb{Q} \to \mathbb{R}/\mathbb{Z}$ và $\mathbb{A}/\mathbb{Q}$ là một phủ hầu hữu hạn.

Ta định nghĩa $\mathbb{A}^\times$ là nhóm các phần tử khả nghịch của $\mathbb{A}$. Thế thì

$$\mathbb{A}^\times = \{(x_p, x_\infty); x_p \in \mathbb{Q}_p^\times, x_\infty \in \mathbb{R}^\times, x_p \in \mathbb{Z}_p^\times \quad \text{với hầu hết các } \ p\}.$$

Ta có

$$\begin{array}{ccc} \mathbb{Q}^\times & \longrightarrow & \mathbb{A}^\times \\ \downarrow & & \downarrow \\ \{1\} & \longrightarrow & \mathbb{R}_+ \end{array}$$

trong đó ánh xạ $\mathbb{A}^\times \to \mathbb{R}_+$ gửi mỗi x lên $|x| = |x|_\infty \prod_p |x|_p$ và việc $\mathbb{Q}^\times \to \{1\}$ chính là công thức tích: với mọi $x \in \mathbb{Q}^\times$

$$\prod_p |x|_p = 1.$$

Ta biết rằng $\mathbb{A}^\times$ là compact địa phương. Sơ đồ trên cho một ánh xạ

$$\mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{R}_+$$

Câu hỏi: $\mathbb{Q}^\times \ \mathbb{A}^\times$ là compact ?

Đặt

$$A^1 = \{x \in \mathbb{A}^\times; |x| = 1\}.$$

Định lí 4.1.1. *$\mathbb{Q}^\times \ \mathbb{A}^1$ là một nhóm compact. Khẳng định đúng khi ta thay $\mathbb{Q}$ bởi mọi trường số (với các định nghĩa tương tự).*

Bạn đọc quan tâm có thể xem hai chứng minh thú vị của kết quả trên trong Weil (Basic number theory). Đây là một kết quả không tầm thường, ta có thể chỉ ra rằng hai kết quả cơ bản của lý thuyết số đại số là tính hữu hạn của nhóm các lớp và tính hữu hạn sinh của nhóm các phần tử đơn vị của vành các số nguyên đại số của một trường số.

Dựa vào các khái niệm trên đây, ta có thể phát biểu kết quả chính của luật thuận nghịch Artin (lý thuyết trường các lớp như sau).

Với K là một trường số, kí hiệu $\bar{K}$ bao đóng đại số của nó. Với mỗi mở rộng Abel L (nằm trong $\bar{K}$), mỗi đặc trưng $\sigma : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ cảm sinh một đặc trưng $\sigma : \mathrm{Gal}(\bar{K}/K) \to \mathbb{C}$ (hữu hạn).

Luật thuận nghịch Artin khẳng định rằng với mỗi đặc trưng hữu hạn $\sigma : \mathrm{Gal}(\bar{K}/K) \to \mathbb{C}^\times$ tương ứng với một đặc trưng

$$\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{C}^\times$$

Luật thuận nghịch Langlands. Phát biểu trên đây của lý thuyết trường các lớp rất thuận tiện cho việc mở rộng thành một phát biểu của luật thuận nghịch không Abel. Một cách nôm na, luật thuận nghich Langlands khẳng định rằng với mỗi biểu diễn $\sigma : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_n(\mathbb{C})$ tương ứng $(1-1)$ với một biểu diễn (bất khả qui) của $\mathrm{GL}_n(\mathbb{A}_n)$ "tham gia vào" trong $\mathscr{A}(\mathrm{GL}_n(K)\backslash \mathrm{GL}(\mathbb{A}))$.

Như là một ví dụ, nhắc lại bài toán ban đầu về các số nguyên tố p có dạng $x^2 + ny^2$. Ta biết rằng tính biểu diễn của p với dạng như trên được chi phối bởi trường các lớp của Hilbert L của $K = \mathbb{Q}(\sqrt{-n})$ và ta cần xác định xem các số nguyên tố p nào hoàn toàn chẻ ra trong L. Ta có $G = \mathrm{Gal}(L/\mathbb{Q})$ không nhất thiết Abel và ta có

$$0 \to H = Cl(K) \to G \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Lấy $\chi : H \to \mathbb{C}^\times$. Biểu diễn cảm sinh $Ind_H^G(\chi) : G \to \mathrm{GL}_2(\mathbb{C})$, theo luật thuận nghịch Langlands, tương ứng với một dạng tự đẳng cấu của GL_2 (dạng modula với trọng bằng 1.)

4.2 Dạng modula

Nửa mặt phẳng trên của Poincaré được định nghĩa như sau

$$\mathscr{H} = \mathscr{H}^+ = \{z \in \mathbb{C}; \Im(z) > 0\}.$$

Ta có định nghĩa tương tự với $\mathscr{H}^-$. Ta cũng xét $\mathbb{P}^1_{\mathbb{C}}$, mặt cầu Riemann $= \mathbb{C} \cup \{\infty\} = \mathbb{P}^1_{\mathbb{R}} \sqcup \mathscr{H}^+ \sqcup \mathscr{H}^-$.

Nhóm $\mathrm{SL}_2(\mathbb{C})$ tác động một cách tự nhiên lên mặt cầu $\mathbb{P}^1_{\mathbb{C}}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}, \quad (ab - cd = 1.)$$

Tác động trên đây cảm sinh một tác động của nhóm con liên thông $\mathrm{SL}_2(\mathbb{R}) \subset \mathrm{SL}_2(\mathbb{C})$ lên $\mathbb{P}^1_{\mathbb{C}}$. Hơn nữa, tác động hạn chế này bảo toàn $\mathbb{P}^1_{\mathbb{R}}, \mathscr{H}^+, \mathscr{H}^-$.

Xét một nhóm con $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ với chỉ số hữu hạn (nhóm con đồng dư). Các ví dụ cơ bản:

- $\Gamma = \mathrm{SL}_2(\mathbb{Z})$;
- $\Gamma = \{\gamma; \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N\}$.

Xét tác động của nhóm đồng dư $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ lên $\mathscr{H}^+$.

Nhắc lại rằng $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ được sinh bởi hai phần tử $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (tác động của phần tử này gửi z lên $z+1$) và $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (tác động gửi z lên z^{-1}).

Dạng modula cổ điển có trọng k Theo định nghĩa, một dạng modula (tương ứng với nhóm $\mathrm{SL}_2(Z)$) với trọng k là một hàm chỉnh hình

$$f : \mathscr{H}^+ \to \mathbb{C}$$

thoả mãn các tính chất sau:

1. $f\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^k} f(z)$;
2. f chỉnh hình tại điểm nhọn (cusp.)

Chú ý rằng, điều kiện 1, áp dụng cho phần tử $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ cho thấy $f(z+1) = f(z)$. Hệ quả là f có khai triển Fourier

$$f(z) = \sum_{n=-\infty}^{+\infty} a_n q^n, \quad q = e^{2\pi z}.$$

Nói rằng f chỉnh hình tại điểm nhọn nghĩa là yêu cầu $a_{-n} = 0$ với mọi $n > 0$.

Ngoài ra, ta nói rằng f là một **dạng nhọn** (dạng cusp) nếu hơn nữa

$$a_0 = 0.$$

Đối với một nhóm ddoofng dư $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ tổng quát, ta có định nghĩa tương tự. Ta lưu ý rằng trong trường hợp tổng quát, số các điểm nhọn có thể > 1 và ta sẽ yêu cầu các dạng modula chỉnh hình tại mọi điểm nhọn.

Ta kí hiệu, với một nhóm đồng dư Γ:

$$M_k = \{\text{các dạng modula có trọng } k \text{ cho nhóm } \Gamma\}.$$

$$S_k = \{\text{các dạng nhọn có trọng } k \text{ cho nhóm } \Gamma\}.$$

Ta dễ dàng kiểm tra được rằng đây là các không gian vector phức.

Định lí 4.2.1. *Ta có, với mọi k, Γ,*

$$\dim M_k(\Gamma) < +\infty, \dim S_k(\Gamma) < +\infty.$$

Phiên dịch các dạng modula dưới dạng nhát cắt toàn cục của phân thớ trên X_Γ. Từ các miền cơ bản của $\mathscr{H}$ dưới tác động của Γ cùng với các điểm cusp của nó, với một cấu trúc phức hợp lý, ta xây dựng được một diện Riemann compact X_Γ. Ta có thể mô tả lại các dạng cusp dưới ngôn ngữ của X_Γ, chẳng hạn

$$S_2(\Gamma) = H^0(X_\Gamma, \omega),$$

Nói cách khác, các dạng cusp trọng bằng 2 đồng nhất với không gian các dạng vi phân chỉnh hình trên X_Γ. Ta có các mô tả tương tự cho các dạng khác. Dựa vào lý thuyết các dạng Riemann, từ đây, ta chỉ ra được tính hữu hạn của chiều các không gian $M_k(\Gamma), S_k(\Gamma)$. Hơn thế nữa, ta có công thức tường minh cho các số chiều này.

Như là một ví dụ tầm thường, với $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ thì $X_\Gamma = \mathbb{P}^1$ và do vậy, trong trường hợp này

$$\dim S_2(\mathrm{SL}_2(Z)) = \dim H^0(\mathbb{P}^1, \omega_{\mathbb{P}^1}) = 0.$$

Khi nào một chuỗi Dirichlet là một dạng modula. Nhắc lại rằng, theo định nghĩa, một dạng modula cổ điển f luôn có một thác triển Fourier

$$f(z) = \sum_{n\geq 0} a_n q^n, q = e^{2\pi z}.$$

Ta có câu hỏi tự nhiên: khi nào một chuỗi như trên định nghĩa một dạng modula ?

Hecke đã đưa ra lời giải cho câu hỏi trên như sau. Xét hàm L liên kết với một dạng modula f:

$$L(f,s) := \sum_{n=0}^{+\infty} a_n n^{-s}$$

Hecke chỉ ra rằng $L(f,s)$ có các tính chất quen thuộc sau đây:

- Hội tụ tuyệt đối với $\Re(s) >> 0$;
- có thác triển phân hình trên toàn bộ $\mathbb{C}$;
- thoả mãn phương trình hàm $L(f,2-s) = * \cdot L(f,s)$, trong đó $*$ liên quan đến Γ-factor.

Ý tưởng của Hecke là như sau: xét hạn chế của f xuống đường thẳng thuần ảo: $t \mapsto f(it)$. Sau đó, áp dụng biến đổi Mellin, ta nhận đươc hàm số

$$L(f,s) = \sum_n a_n n^{-s}.$$

trong đó, nếu f là một dạng modula thì a_n chính là các hệ số của khai triển Fourier của nó.

$t \mapsto f(it)$ là hàm giảm nhanh tại $t \mapsto \infty$, cùng với $f(it) = (-1)f(it^{-1})$ giảm nhanh tại 0.

Phương trình hàm $f(it) = *f(it^{-1})$ $(\rightarrow)$ $L(f,s) = *L(f,2-s)$.

Ngược lại, nếu $L(f,s)$ thác triển phân hình trên $\mathbb{C}$ và thoả mãn một phương trình hàm quen thuộc thì f là một dạng modula (Định lý đảo của Weil).

Tính chất tích Euler của L-hàm của dạng modula. Nhắc lại rằng hàm zeta của Riemann có tích Euler.

Câu hỏi đặt ra là xác định các dạng modula f sao cho $L(f,s)$ có tích Euler ?

Hecke đã đưa ra một câu trả lời đẹp đẽ cho câu hỏi trên. Một cách cụ thể, Hecke định nghĩa một họ giao hoán các toán tử (Hecke) trên các không gian $M_k(\Gamma), S_k(\Gamma)$.

Định lí 4.2.2 (Hecke)**.** *Cho f là một dạng modula trọng k đối với Γ. Thế thì $L(f,s)$ có khai triển thành tích Euler khi và chỉ khi f là vector riêng đối với toàn bộ các toán tử Hecke.*

(Xét trường hợp các dạng modula với trọng bằng 2!) Cụ thể hơn, Hecke các toán tử $T(n)$ được sinh ra bởi các toán tử $T(p)$ với p nguyên tố. Giả sử $f = \sum_n a_n q^n$ là một vector riêng với các toán tử Hecke, thế thì

$$T(p)f = a_p f.$$

Từ đó suy ra khai triển tích Euler

$$L(f,s) = \prod_p (1 - a_p p^{-s} + p^{-2s})^{-1}$$

Ta giả sử f là các dạng nhọn và đồng thời là dạng riêng (eigenform) , nói cách khác, là các vector riêng đối với tác động của các toán tử Hecke. Thế thì

$$a_n \in \bar{\mathbb{Q}}.$$

Hơn nữa, tồn tại một mở rộng hữu hạn $K/\mathbb{Q}$ chứa các hệ số $a_1, a_2, \ldots$. Các hệ số a_i, như vậy, là các đại lượng số học. Ta chỉ ra rằng chúng tương ứng với các biểu diễn Galois

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C}).$$

Đối với trường hợp trọng $k = 2, K = \mathbb{Q}$, Shimura-Taniyama-Weil xây dựng một đường cong elliptic $E/\mathbb{Q}$ sao cho

$$\sharp E(\mathbb{F}_p) = p - a_p$$

Giả thuyết Shimura-Taniyama-Weil: Mọi đuowfng cong elliptic trên $\mathbb{Q}$ đều có dạng như trên.

Định lí 4.2.3 (Wiles)**.** *Giả thuyết Shimura-Taniyama-Weil là đúng.*

Cho dù không phải là ... Đây là một bước quan trọng trong chứng minh định lý Fermat.