Vành các số nguyên Gauss và ứng dụng Diophante

NCG. Vượng-Viện Toán học Hà Nội

12/2010

Nội dung chủ yếu của bài giảng này là việc nghiên cứu các tính chất số học của vành $\mathbb{Z}[i]$ áp dụng điều này vào việc giải một số phương trình Diophante.

1 Vành các số nguyên Gauss

Định nghĩa. Ta nhắc lại định nghĩa vành các số nguyên Gauss

$$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

(với $i^2 = -1$.) Chú ý rằng ta có thể coi $\mathbb{Z}[i]$ là một vành con chứa $\mathbb{Z}$ của $\mathbb{C}$. Nói một cách khác, với $\alpha, \beta \in \mathbb{Z}[i]$ ta có $\alpha + \beta, \alpha\beta \in \mathbb{Z}[i]$. Với $\alpha = a + bi$, ta định nghĩa **liên hợp** $\bar{\alpha} = a - bi$ và **chuẩn**

$$\mathrm{N}(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$$

Ta cũng nhắc lại rằng $\mathrm{N}(\alpha) = 0 \Leftrightarrow \alpha = 0$ và $\mathrm{N} : \mathbb{Z}[i] \to \mathbb{N}$ có tính chất nhân:

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$$

Quan hệ chia hết, phần tử khả nghịch và phần tử bất khả qui. Với hai số nguyên Gauss α và β, ta nói rằng α là một **ước** của β hay β là **bội** của α, kí hiệu là $\alpha \mid \beta$, nếu tồn tại γ sao cho $\alpha\gamma = \beta$. Khái niệm này mở rộng khái niệm chia hết quen thuộc trên $\mathbb{Z}$ theo nghĩa sau: nếu $a, b \in \mathbb{Z}$ thì $a \mid b$ trong $\mathbb{Z}$ khi và chỉ khi $a \mid b$ trong $\mathbb{Z}[i]$.

Một số nguyên Gauss được gọi là **khả nghịch** nếu là ước của 1, nói một cách khác, nếu $\neq 0$ và sao cho nghịch đảo trong $\mathbb{C}$ cũng là một số nguyên của Gauss. Một phần tử là khả nghịch nếu và chỉ nếu là ước của mọi số nguyên Gauss.

Ta nói hai số nguyên Gauss α, β là **liên kết** với nhau, kí hiệu là $\alpha \sim \beta$, nếu $\alpha \mid \beta$ và $\beta \mid \alpha$. Hai số nguyên của Gauss là liên kết với nhau khi và chỉ khi sai khác với nhau bằng phép nhân với một phần tử khả nghịch.

Cuối cùng, có lẽ khái niệm quan trọng nhất trong quan hệ chia hết là về các phần tử bất khả qui. Ta nói $\alpha \in \mathbb{Z}[i]$ là **bất khả qui** nếu $\alpha \neq 0, \alpha$ không khả nghịch và nếu $\alpha = \beta\gamma$ thì hoặc β khả nghịch (khi đó $\gamma \sim \alpha$) hoặc γ khả nghịch (khi đó $\beta \sim \alpha$). Nói một cách khác, một số nguyên của Gauss là bất khả qui nếu $\neq 0$ và không có các ước thực sự nào. Khái niệm này mở rộng khái niệm các số nguyên tố. Lưu ý rằng nếu $a \in \mathbb{Z}$ là bất khả qui trong $\mathbb{Z}[i]$ thì $\pm a$ là một số nguyên tố thông thường. Tuy nhiên, điều ngược lại là không đúng, chẳng hạn 2 không phải là một phần tử bất khả qui của $\mathbb{Z}[i]$ bởi vì $2 = i(1 + i)^2$. Ta sẽ nghiên cứu các phần tử bất khả qui một cách chi tiết hơn

Các phần tử khả nghịch của $\mathbb{Z}[i]$ được miêu tả như sau.

Mệnh đề 1.1. *Tập các phần tử khả nghịch của $\mathbb{Z}[i]$ là*

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{\alpha \in \mathbb{Z}[i]; \mathrm{N}(\alpha) = 1\}$$

Chứng minh. Thật vậy, giả sử α khả nghịch và $\alpha^{-1} \in \mathbb{Z}[i]$ là nghịch đảo của nó. Ta có $\mathrm{N}(\alpha)\mathrm{N}(\alpha^{-1}) = \mathrm{N}(1) = 1$. Do $\mathrm{N}(\alpha), \mathrm{N}(\alpha^{-1}) \in \mathbb{Z}_{>0}$ nên ta phải có $\mathrm{N}(\alpha) = \mathrm{N}(\alpha^{-1}) = 1$. Ngược lại, nếu $\mathrm{N}(\alpha) = 1$ thì $\alpha\bar{\alpha} = 1$ nên hoặc $\bar{\alpha}$ là nghịch đảo của α. Cuối cùng, nhận xét rằng $\mathrm{N}(a+bi) = a^2 + b^2 = 1$ kéo theo $(a,b) = (\pm 1, 0)$ hoặc , $(a,b) = (0, \pm 1)$, nói cách khác $a + bi = \pm 1$ hoặc $\pm i$. □

Tính Euclid của vành Gauss. Ta có kết quả bản lề sau.

Mệnh đề 1.2 (Phép chia Euclid trên vành các số nguyên Gauss)**.** *Cho $\alpha, \beta \in \mathbb{Z}[i]$ với $\beta \neq 0$. Tồn tại các số nguyên Gauss μ, ρ sao cho $\alpha = \beta\mu + \rho$ và $\mathrm{N}(\rho) < \mathrm{N}(\beta)$.*

Chứng minh. Đặt $\frac{\alpha}{\beta} = x + yi$ với $x, y \in \mathbb{R}$. Trong mặt phẳng phức $\mathbb{C}$ với trục tung $\mathbb{R}i$ và trục hoành $\mathbb{R}$, các số nguyên Gauss là các điểm có tọa độ nguyên. Ta chọn $\mu \in \mathbb{Z}[i]$ là một điểm tọa độ nguyên gần $x + yi$ nhất. Dễ thấy khi đó khoảng cách giữa μ và $x + iy$ không vượt quá một nửa của độ dài đường chéo một hình vuông đơn vị, nghĩa là $\leq \frac{\sqrt{2}}{2}$, nói riêng luôn nhỏ hơn 1. Điều này lại có nghĩa là $\mathrm{N}(\frac{\alpha}{\beta} - \mu) < 1$. Do đó $\mathrm{N}(\alpha - \beta\mu) = \mathrm{N}\left(\beta\left(\frac{\alpha}{\beta} - \mu\right)\right) = \mathrm{N}(\beta)\mathrm{N}(\frac{\alpha}{\beta} - \mu) < \mathrm{N}(\beta)$. □

Kết quả trên cho thấy sự tồn tại của thuật toán Euclid (phép chia Euclid) trên vành Gauss. Nhắc lại rằng thuật toán này áp dụng cho một cặp $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$ cho ta tìm được **ước chung lớn nhất** δ của α, β theo nghĩa sau

1. $\delta \mid \alpha, \delta \mid \beta$;
2. Với mọi δ' sao cho $\delta' \mid \alpha, \delta' \mid \beta$ thì hoặc δ' liên kết với δ hoặc $\mathrm{N}(\delta') < \mathrm{N}(\delta)$.

Ước chung lớn nhất của hai số nguyên Gauss (mà sự tồn tại được nêu ra ở trên) là không duy nhất. Nếu δ là một ước chung lớn nhất của α, β thì mọi $\delta' \sim \delta$ cũng là một ước chung lớn nhất và tập $\{\delta'; \delta' \sim \delta\}$ là tập các ước chung lớn nhất của α, β. Hơn thế nữa, thuật toán Euclid cũng đem lại hai phần tử $\mu, \nu \in \mathbb{Z}[i]$ sao cho

$$\mu\alpha + \nu\beta = \delta$$

Ta nói rằng hai số nguyên Gauss $\neq 0$ là **nguyên tố cùng nhau** nếu 1 là một ước chung lớn nhất của chúng.

Tính Euclid của vành $\mathbb{Z}[i]$ cho ta một trường hợp đặc biệt của bổ đề Gauss.

Bổ đề 1.3. *Cho α, β, γ là các số nguyên Gauss với α bất khả qui. Nếu $\alpha \mid \beta\gamma$ thì $\alpha \mid \beta$ hoặc $\alpha \mid \gamma$.*

Chứng minh. Giả sử $\alpha \nmid \beta$. Ta biết rằng thuật toán Euclid cho bộ β, α (điều kiện α bất khả qui đảm bảo $\alpha \neq 0$) cho ta ước chung lớn nhất δ của β, α cùng với các số nguyên Gauss μ, ν sao cho $\delta = \beta\mu + \alpha\nu$. Do $\delta \mid \alpha$ và α bất khả qui theo giả thiết, δ hoặc là một phần tử khả nghịch hoặc là một liên kết với a. Nhưng δ không thể là một liên kết của α vì khi đó ta có $\alpha \mid \delta \mid \beta$. Như vậy δ là một phần tử đơn vị. Ta suy ra $\gamma = \delta^{-1}\gamma\beta\mu + \delta^{-1}\gamma\alpha\nu$. Vì $\alpha \mid \beta\gamma$ đẳng thức này kéo theo $\alpha \mid \gamma$.

□

Định lý cơ bản của số học cho vành Gauss. Sự tồn tại của phép chia Euclid đảm bảo rằng Định lý cơ bản của số học đúng cho vành $\mathbb{Z}[i]$.

Định lý 1.4 (Định lý cơ bản của số học cho vành Gauss)**.** *Mọi số nguyên Gauss $\alpha \neq 0$ đều có thể được viết dưới dạng*

$$\alpha = \epsilon\gamma_1 \cdots \gamma_n$$

trong đó ϵ là một phần tử khả nghịch, $\gamma_1, \ldots, \gamma_n$ là các phần tử bất khả qui (không nhất thiết phân biệt, thậm chí không nhất thiết đôi một không liên kết). Cách phân tích này là duy nhất theo nghĩa sau: nếu $\alpha = \epsilon'\delta_1 \cdots \delta_m$ là một phân tích tương tự của α thì $m = n$ và tồn tại một hoán vị σ trên tập $\{1, 2, \ldots, n\}$ sao cho với mọi i, ta có $\delta_i \sim \gamma_{\sigma(i)}$.

Chứng minh. Sự tồn tại. Ta tiến hành qui nạp theo $\mathrm{N}(\alpha)$. Trường hợp $\mathrm{N}(\alpha) = 1$ là tầm thường vì khi đó α là một phần tử khả nghịch. Giả sử phân tích như vậy tồn tại với mọi $\alpha \in \mathbb{Z}[i]$ sao cho $\mathrm{N}(\alpha) < k$ với k nguyên dương nào đó và α là một số nguyên Gauss với $\mathrm{N}(\alpha) = k$. Nếu α là một phần tử bất khả qui thì bài toán không có gì phải chứng minh. Giả sử α là khả qui, viết $\alpha = \mu\nu$ với μ, ν là các phần tử không khả nghịch. Do $\mathrm{N}(\alpha) = \mathrm{N}(\mu)\mathrm{N}(\nu)$ nên $1 < \mathrm{N}(\mu), \mathrm{N}(\nu) < k$. Áp dụng giả thiết qui nạp cho μ và ν ta nhận được một phân tích thỏa mãn các yêu cầu của định lý.

Tính duy nhất. Đây là một hệ quả quen thuộc của tính Euclid. Nếu α là một phần tử khả nghịch thì bài toán là tầm thường. Giả sử α không khả nghịch. Không mất tổng quát, ta có thể viết một phân tích ra tích các phần tử bất khả qui dưới dạng

$$\alpha = \gamma_1\gamma_2 \cdots \gamma_n$$

với a_i là các phần tử bất khả qui, không nhất thiết đôi một không liên kết. Chú ý rằng phần tử đơn vị của phân tích nguyên gốc được hấp thụ vào một trong các phần tử bất khả qui.

Giả sử ta có một phân tích khác $\alpha = \delta_1 \cdots \delta_m$. Áp dụng Bổ đề 1.3 ở trên, từ đẳng thức

$$\gamma_1 \cdots \gamma_n = \delta_1 \cdots \delta_m$$

ta suy ra γ_1 liên kết với một trong các phần tử γ_i nào đó. Thật vậy, do $\gamma_1 \mid \delta_1 \cdots \delta_m$, tồn tại i sao cho $\gamma_1 \mid \delta_i$. Thế nhưng δ_i cũng là một phần tử bất khả qui, ta phải có γ_1 liên kết với δ_i. Bây giờ, chia cả hai vế của đẳng thức $\gamma_1 \cdots \gamma_n = \delta_1 \cdots \delta_m$ cho γ_1 ta nhận được một đẳng thức tương tự với độ dài của phân tích ở mỗi vế giảm đi 1. Tiến hành liên tiếp như vậy ta dễ dàng nhận được điều cần chứng minh. □

Các phần tử bất khả qui của vành Gauss. Định lý cơ bản của số học cho vành $\mathbb{Z}[i]$ mà ta đã thiết lập ở trên cho thấy sự cần thiết của việc nghiên cứu các phần tử khả nghịch và các phần tử bất khả qui của vành này. Nhắc lại rằng các phần tử khả nghịch đã được miêu tả tại Mệnh đề 1.1. Về phía các phần tử bất khả qui, trước hết ta có kết quả sau.

Mệnh đề 1.5. *Cho $\gamma \in \mathbb{Z}[i]$ là một phần tử bất khả qui của $\mathbb{Z}[i]$. Tồn tại duy nhất một số nguyên tố $p \in \mathbb{Z}$ sao cho $\gamma \mid p$.*

Chứng minh. Ta có $\gamma \mid \gamma\bar{\gamma} = \mathrm{N}(\gamma)$. Như vậy, theo Bổ đề 1.3 γ là ước của một ước nguyên tố p nào đó của $\mathrm{N}(x)$. Số nguyên tố p như vậy là duy nhất. Thật vậy, nếu tồn tại một số nguyên tố $q \neq p$ sao cho $\gamma \mid q$. Theo Định lý Bezout cho các số nguyên, ta biết rằng tồn tại các số nguyên a, b sao cho $ap + bq = 1$. Do đó $\gamma \mid 1$, mâu thuẫn với giả thiết γ bất khả qui.

□

Nhận xét 1.6. *Mệnh đề trên, đơn giản nhưng rất sâu sắc, nói rằng mọi phần tử bất khả qui của* $\mathbb{Z}[i]$ *đều nằm trên một số nguyên tố nào đó. Nói một cách khác, ta đã có một miêu tả ban đầu các phần tử bất khả qui của* $\mathbb{Z}[i]$.

Theo Mệnh đề 1.5 và Định lý 1.4, việc miêu tả các phần tử bất khả qui của $\mathbb{Z}[i]$ tương đương với việc miêu tả các nhân tử bất khả qui của các số nguyên tố thông thường p trong vành $\mathbb{Z}[i]$. Ta bắt đầu với $p = 2$.

Mệnh đề 1.7. *Các ước bất khả qui của* 2 *trong* $\mathbb{Z}[i]$ *là* $1+i$ *và các phần tử liên kết với nó, nghĩa là* $\{\pm 1 \pm i\}$.

Chứng minh. Ta có $2 = (1+i)(1-i)$ nên $1+i \mid 2$ cũng như các phần tử liên kết với $1+i$, nghĩa là $\pm 1 \pm i$.. Mặt khác $1+i$ là bất khả qui vì $\mathrm{N}(1+i) = 2$ là nguyên tố. Điều này được suy ra từ nhận xét đơn giản nhưng hữu hiệu sau: một phần tử có chuẩn là một số nguyên tố là bất khả qui. □

Bổ đề 1.8. *Cho* $\alpha \in \mathbb{Z}[i]$ *sao cho* $\mathrm{N}(\alpha)$ *là một số nguyên tố. Thế thì* α *là một phần tử bất khả qui.*

Chứng minh. Thật vậy, nếu $\alpha = \beta\gamma$ thì $\mathrm{N}(\beta)\mathrm{N}(\gamma) = \mathrm{N}(\alpha)$ là một số nguyên tố, ta suy ra $\mathrm{N}(\beta) = 1$ hoặc $\mathrm{N}(\gamma) = 1$, nghĩa là một trong hai phần tử β, γ là khả nghịch. □

Với các số nguyên tố p lẻ, ta chia ra làm hai trường hợp $p \equiv 1 \pmod 4$ và $\equiv 3 \pmod 4$.

Mệnh đề 1.9. *Giả sử* p *là một số nguyên tố* $\equiv 3 \pmod 4$. *Khi đó* p *là một phần tử bất khả qui của* $\mathbb{Z}[i]$.

Chứng minh. Giả sử p là khả qui. Viết $p = \alpha\beta$ với α, β là các phần tử không khả nghịch, như vậy $\mathrm{N}(\alpha), \mathrm{N}(\beta) > 1$. Từ tính nhân của chuẩn $\mathrm{N}(\alpha)\mathrm{N}(\beta) = \mathrm{N}(p) = p^2$ và do $\mathrm{N}(\alpha), \mathrm{N}(\beta) > 1$ ta suy ra $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$. Viết $\alpha = a + bi, a, b \in \mathbb{Z}$ thế thì $a^2 + b^2 = p \equiv 3 \pmod 4$ nhưng đồng dư này rõ ràng không thể xảy ra. Như vậy p là một phần tử bất khả qui của $\mathbb{Z}[i]$. □

Mệnh đề 1.10. *Giả sử* p *là một số nguyên tố* $\equiv 1 \pmod 4$.

1. *Tồn tại duy nhất một bộ nguyên dương* (a, b), *chính xác tới thứ tự, sao cho* $a^2 + b^2 = p$;
2. *Các ước bất khả qui của* p *trong* $\mathbb{Z}[i]$ *gồm* $a + bi, a - bi$ *(với* a, b *như trên) và các phần tử liên kết với chúng.*

Để minh họa, số nguyên tố $p = 5$ có thể viết duy nhất dưới dạng tổng của hai số chính phương $5 = 1^2 + 2^2$. Số nguyên tố 5 không là bất khả qui trong $\mathbb{Z}[i]$ mà có hai ước bất khả qui $1+2i, 1-2i$. Có nghĩa là 5 có 8 ước bất khả qui gồm các phần tử liên kết với $1+2i$, nghĩa là $\{1+2i, -1-2i, -2+i, 2-i\}$ và các phần tử liên kết với $1-2i$, nghĩa là $\{1-2i, -1+2i, 2+i, -2-i\}$.

Ta nhắc lại Bổ đề Lagrange.

Bổ đề 1.11 (Lagrange)**.** *Cho* p *là một số nguyên tố* $\equiv 1 \pmod 4$. *Tồn tại một số nguyên* n *sao cho* $p \mid n^2 + 1$.

Chứng minh. Thật vậy, đặt $p = 4k+1$. Theo Định lý Wilson ta có $(4k)! \equiv -1 \pmod p$. Mặt khác ta có $(4k!) = (1 \cdot 2 \cdots 2k)((2k+1) \cdot (2k+2) \cdots (4k)) \equiv (1 \cdot 2 \cdots 2k)((-2k)(-2k+1) \cdots (-1)) \equiv (-1)^{2k}(1 \cdot 2 \cdots 2k)^2 \equiv (2k!)^2 \pmod p$. □

Nhận xét 1.12. *Tất nhiên, ta cũng có thể sử dụng các công thức thặng dư toàn phương để chứng minh kết quả trên.*

Chứng minh. Theo Bổ đề Lagrange, tồn tại một số nguyên n sao cho $p \mid n^2+1$. Như vậy, nếu xét trong vành Gauss, $p \mid (n+i)(n-i)$. Tuy nhiên $p \nmid n+i, p \nmid n-i$ (vì $\frac{n}{p} \pm \frac{1}{p}i \notin \mathbb{Z}[i]$). Từ đó suy ra p không phải là một phần tử bất khả qui. Gọi $a+bi \in \mathbb{Z}[i]$ là một ước bất khả qui của p. Rõ ràng liên hợp $a-bi$ cũng là một ước của p (chỉ cần lấy liên hợp hai vế của một phân tích của p ra tích các phần tử bất khả qui trong $\mathbb{Z}[i]$).

Ta sẽ chỉ ra $a+bi, a-bi$ là các ước bất khả qui duy nhất (sai khác phép liên kết) của p. Thật vậy giả sử $c+di$ (và do đó $c-di$) là một ước bất khả qui của p. Theo sự tồn tại của phép phân tích ra tích các phần tử bất khả qui ta suy ra $(c+di)(c-di)(c+di)(c-di) \mid p$ (trong $\mathbb{Z}[i]$). Điều này có nghĩa là $(a^2+b^2)(c^2+d^2) \mid p$ (trong $\mathbb{Z}[i]$) hay $\frac{p}{(a^2+b^2)(c^2+d^2)} \in \mathbb{Z}[i]$, vô lý.

□

Kết hợp các Mệnh đề 1.7, 1.9 và 1.10 ta thu được kết quả sau.

Định lý 1.13. *Các phần tử bất khả qui của $\mathbb{Z}[i]$ gồm*

1. *$1+i$ và các phần tử liên kết của nó, nghĩa là $\{\pm 1 \pm i\}$;*
2. *Các số nguyên tố $p \equiv 3 \pmod 4$ và các phần tử liên kết của nó, nghĩa là $\{\pm p, \pm pi\}$;*
3. *Hai nhân tử bất khả qui $a+bi, a-bi$ trong phân tích ra tích các nhân tử bất khả qui của một số nguyên tố $p \equiv 1 \pmod 4$ và các phần tử liên kết của nó. Các số (a,b) có thể được đặc trưng như là bộ số nguyên duy nhất, chính xác tới dấu và tới thứ tự thỏa mãn $a^2+b^2=p$.*

2 Sử dụng $\mathbb{Z}[i]$ trong một số phương trình Diophante

Phương trình bậc hai $x^2+y^2=n$. Ta bắt đầu với n nguyên tố.

Định lý 2.1 (Fermat)**.** *Một số nguyên tố p biểu diễn được dưới dạng tổng của hai số chính phương khi và chỉ khi $p=2$ hoặc $p \equiv 1 \pmod 4$. Hơn nữa biểu diễn như vậy là duy nhất chính xác tới thứ tự.*

Chứng minh. Với $p=2$ khẳng định là hiển nhiên, với p lẻ, kết quả này nằm trong chứng minh của các Mệnh đề 1.9 và 1.10. □

Định lý trên, ngoài phương pháp sử dụng các số nguyên Gauss, còn có nhiều chứng minh khác nhau. Nhân cơ hội này, tôi trình bày chứng minh một dòng của Zagier về sự tồn tại của biểu diễn khi $p=4k+1$. Đặt $S=\{(x,y,z) \in \mathbb{N}^3; x^2+4yz=p\}$. Tập hợp S có hai phép hoán vị cấp 2: $f(x,y,z)=(x,z,y)$ và g định nghĩa bởi

$$g(x,y,z)=\begin{cases} (x+2z,z,y-x-z) & \text{nếu} \quad x<y-z \\ (2y-x,y,x-y+z) & \text{nếu} \quad y-z<x<2y \\ (x-2y,x-y+z,y) & \text{nếu} \quad x>2y \end{cases}$$

Chú ý rằng lực lượng của tập con các điểm bất động của một hoán vị cấp 2 của S có cùng tính chẵn lẻ với S. Mặt khác S^f chính là tập các biểu diễn của p thành tổng của hai số chính phương. $S^g=\{(1,k,k)\}$. Ta suy ra $|S| \equiv |S^f| \equiv |S^g| \equiv 1 \pmod 2$. Như vậy số các biểu diễn của p là tổng các số chính phương là lẻ và do đó ≥ 1.

Với n tổng quát, Định lý 2.1 có thể được mở rộng dưới dạng sau.

Định lý 2.2. *Cho một số nguyên dương n. Số nghiệm nguyên của phương trình $x^2 + y^2 = n$ bằng 4 lần hiệu của số các ước $\equiv 1 \pmod 4$ của n trừ cho số các ước $\equiv 3 \pmod 4$ của n.*

Nhận xét 2.3. *Tất nhiên ta có thể phát biểu một cách hình học kết quả trên bằng cách thể hiện các nghiệm của phương trình trên bằng các điểm nguyên trên đường tròn $x^2 + y^2 = n$.*

Chứng minh. Theo Định lý về phân tích ra tích các nhân tử bất khả qui, ta có thể viết

$$\begin{aligned} n &= 2^m p_1^{r_1} \cdots p_k^{r_k} \gamma_1^{s_1} \bar{\gamma}_1^{s_1} \cdots \gamma_h^{s_h} \bar{\gamma}_h^{s_h} \\ &= (-i)^m (1+i)^{2m} p_1^{r_1} \cdots p_k^{r_k} \gamma_1^{s_1} \bar{\gamma}_1^{s_1} \cdots \gamma_h^{s_1} \bar{\gamma}_h^{s_h} \end{aligned}$$

trong đó p_i, γ_j là các phần tử bất khả qui của $\mathbb{Z}[i]$ với $p_i = \bar{p}_i$ (như vậy p_i là các số nguyên tố $\equiv 3$ thông thường và γ_j có dạng $a + bi$ với $a^2 + b^2 =$ một số nguyên tố $\equiv 1 \pmod 4$).

Giả sử $n = x^2 + y^2 = (x + yi)(x - yi)$. Theo tính duy nhất của phân tích ra tích các phần tử bất khả qui trong $\mathbb{Z}[i]$ ta suy ra

$$x + yi \text{ là một phần tử liên kết của } (1+i)^m p_1^{\frac{r_1}{2}} \cdots p_k^{\frac{r_k}{2}} \gamma_1^{t_1} \bar{\gamma}_1^{s_1 - t_1} \cdots \bar{\gamma}_h^{s_h - t_h} \tag{1}$$

với $0 \le t_j \le s_j$. Như vậy số nghiệm nguyên của $x^2 + y^2$ bằng

- 0 nếu một trong các r_i là lẻ;
- $4(s_1 + 1) \cdots (s_h + 1)$ nếu tất cả các r_i là chẵn.

Chú ý rằng thừa số 4 xuất hiện ở công thức trên đến từ việc biểu diễn 1 ở trên sai khác $x + yi$ bởi một trong 4 phần tử khả nghịch $\{\pm 1, \pm i\}$.

Mặt khác mọi ước lẻ của n đều có thể viết dưới dạng tích các phần tử bất khả qui trong $\mathbb{Z}[i]$

$$d = p_1^{u_1} \cdots p_k^{u_k} \gamma_1^{v_1} \bar{\gamma}_1^{v_1} \cdots \gamma_h^{v_h} \bar{\gamma}_h^{v_h}$$

với $0 \le u_i \le r_i, 0 \le v_j \le s_j$. Nhưng $p_i \equiv 3 \pmod 4$ với mọi i và $\gamma_j \bar{\gamma}_j \equiv 1 \pmod 4$ với mọi j nên

$$d \equiv 1 \pmod 4 \Leftrightarrow u_1 + \cdots + u_k \equiv 1 \pmod 2$$

Tương đương này dễ dàng dẫn đến hiệu của số các ước $\equiv 1 \pmod 4$ và số các ước $\equiv 3 \pmod 4$ của n bằng

- 0 nếu một trong các r_i là lẻ;
- $(s_1 + 1) \cdots (s_h + 1)$ nếu tất cả các r_i là chẵn.

Và ta có điều phải chứng minh. □

Kết quả trên đem đến cho ta một hệ quả quen biết sau.

Hệ quả 2.4. *Một số nguyên dương n biểu diễn được dưới dạng tổng của hai số chính phương khi và chỉ khi trong phân tích ra thừa số nguyên tố của n các số nguyên tố $\equiv 3 \pmod 4$ có lũy thừa chẵn.*

Chứng minh. Đây là hệ quả trực tiếp của công thức cho bởi Định lý 2.2. Ngoài ra, kết quả này cũng có thể được suy ra từ Định lý 2.1. □

Phương trình Catalan $x^n - y^2 = 1, n \geq 3$**.** .

Một trong số các bài toán nổi tiếng nhất về phương trình Diophante là giả thuyết Catalan mà ta nhắc lại sau đây.

Giả thuyết Catalan (1844)**.** *Cho m, m là hai số nguyên dương > 1. Phương trình*

$$x^n - y^m = 1$$

không có nghiệm nguyên với $x \neq 0, y \neq 0$ trừ khi $(n, m) = (2, 3)$, khi đó nó các nghiệm $x \neq 0, y \neq 0$ duy nhất $(x, y) = (\pm 3, 2)$.

Giả thuyết Catalan được chứng minh vào năm 2002 bởi Mihailescu. Trong bài giảng này, ta sẽ không đi vào trình bày chứng minh của giả thuyết này mà sẽ nghiên cứu trường hợp đặc biệt $m = 2$ nhằm minh họa cho việc sử dụng vành $\mathbb{Z}[i]$ trong việc giải các phương trình Diophante.

Trường hợp $n = 2$ được giải quyết một cách dễ dàng thông qua phân tích $x^2 - y^2 = (x-y)(x+y)$. Ngoài ra, không mất tổng quát, ta có thể giả sử n là một số nguyên tố, trường hợp tổng quát dễ dàng được suy ra từ trường hợp này.

Mệnh đề 2.5. *Phương trình*

$$y^2 = x^3 - 1$$

chỉ có nghiệm nguyên duy nhất $(x, y) = (1, 0)$.

Chứng minh. Giả sử (x, y) là nghiệm nguyên của phương trình đã nêu. Nếu x chẵn thì $y^2 \equiv -1 \pmod 8$ nhưng -1 không phải chính phương modulo 8. Vậy x lẻ và y chẵn. Viết lại phương trình dưới dạng

$$x^3 = (y + i)(y - i)$$

Trước hết ta có nhận xét đơn giản sau.

Bổ đề 2.6. *Với mọi $a \in 2\mathbb{Z}$, các phần tử $a + i$ và $a - i$ là nguyên tố cùng nhau trong $\mathbb{Z}[i]$.*

Chứng minh. Thật vậy, giả sử $\gamma \in \mathbb{Z}$ sao cho $\gamma \mid a + i, \gamma \mid a - i$ như vậy $\gamma \mid 2i$. Nói riêng ta có $\mathrm{N}(\gamma) \mid \mathrm{N}(2i) = 4$. Mặt khác, $\gamma \mid a + i \Rightarrow \mathrm{N}(\gamma) \mid \mathrm{N}(a + i) = a^2 + 1$. Như vậy số nguyên dương $\mathrm{N}(\gamma)$ vừa là ước của 4 vừa là ước của số nguyên lẻ $a^2 + 1$, do đó $\mathrm{N}(\gamma) = 1$. Điều này chứng tỏ γ là một phần tử đơn vị.

□

Ta biết rằng Định lý cơ bản của số học còn đúng cho $\mathbb{Z}[i]$ và tập các phần tử khả nghịch của $\mathbb{Z}[i]$ là $\{\pm 1, \pm i\}$. Mặt khác, theo Bổ đề trên, $y + i, y - i$ là nguyên tố cùng nhau. Như vậy $y + i, y - i$ là lập phương của các phần tử của $\mathbb{Z}[i]$ (do mọi phần tử khả nghịch đều là lập phương của một phần tử khả nghịch nào đó). Do đó tồn tại các số nguyên a, b sao cho $y + i = (a + bi)^3$ (khi đó, bằng cách lấy liên hợp, ta có $y - i = (a - bi)^3$). So sánh các phần ảo của hai vế của đẳng thức $y + i = (a + bi)^3$ ta được $1 = b(3a^2 - b^2)$. Giải phương trình nghiệm nguyên đơn giản này ta được $(a, b) = (0, -1)$. Từ đây, ta suy ra $y = 0$ và như vậy $x = 1$. □

Mệnh đề 2.7. *Phương trình $x^5 - y^2 = 1$ chỉ có nghiệm nguyên duy nhất $(x, y) = (1, 0)$.*

Chứng minh. Bài tập. □

Với cùng ý tưởng trên, nhưng với các lập luận kỹ thuật hơn, ta có kết quả sau.

Định lý 2.8 (Lebesgue 1850)**.** *Với mọi $p \geq 2$ phương trình*

$$x^p - y^2 = 1$$

không có nghiệm nguyên (x, y) với $y \neq 0$.

Chứng minh. Bài tập. Gợi ý: sử dụng định giá 2-adic để suy luận. □

Phương trình Mordell. Phương trình Mordell (hay còn gọi là phương trình Bachet) là phương trình Diophante

$$y^2 = x^3 + k \tag{2}$$

với k là một số nguyên $\neq 0$ cho trước.

Tính hữu hạn của các nghiệm nguyên của một phương trình Mordell được chứng minh bởi Siegel.

Định lý 2.9 (Siegel)**.** *Với mọi $k \neq 0$, phương trình $y^3 = x^3 + k$ chỉ có một số hữu hạn các nghiệm nguyên.*

Ngược lại với tính hữu hạn của các nghiệm nguyên, các phương trình Mordell, hay tổng quát hơn là các phương trình elliptic, có thể có vô hạn nghiệm hữu tỷ. Đây chính là nội dung của Định lý Mordell (mà sau này được mở rộng bởi Weil).

Lẽ dĩ nhiên, ta sẽ không đi vào chứng minh chi tiết các kết quả của Siegel hay Mordell-Weil mà chỉ dùng chúng như một kim chỉ nam cho các dự đoán của chúng ta trong các tình huống cụ thể.

Trước hết, một số phương trình Mordell có thể được giải quyết bằng phương pháp đồng dư.

Định lý 2.10 (Lebesgue)**.** *Phương trình $y^2 = x^3 + 7$ không có nghiệm nguyên.*

Chứng minh. Giả sử (x, y) là một nghiệm nguyên của phương trình đã nêu. Suy luận đơn giản theo modulo 4 cho thấy x không thể chẵn. Vậy x lẻ và do đó y chẵn. Ta viết lại phương trình đã cho dưới dạng

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$$

Vì x lẻ nên $x^2 - 2x + 4 = (x - 1)^2 + 3 \equiv 3 \pmod 4$ do đó $x^2 - 2x + 4$ có một ước nguyên tố lẻ $p \equiv 3 \pmod 4$. Nhưng ta lại có $y^2 + 1 \equiv 0 \pmod p$. Điều này chứng tỏ -1 là chính phương modulo p và như vậy $p \equiv 1 \pmod 4$, mâu thuẫn.

□

Trong cùng mạch ý tưởng này ta nhận được khá nhiều kết quả tương tự.

Mệnh đề 2.11. *Các phương trình*

1. $y^2 = x^3 - 5$;

2. $y^2 = x^3 - 6$;

3. $y^2 = x^3 + 46$;

4. $y^2 = x^3 + 45$

không có nghiệm nguyên.

Chứng minh. Bài tập. □

Ta đưa ra một ví dụ về phương trình có nghiệm nguyên, cũng dựa vào suy luận đồng dư.

Mệnh đề 2.12. *Phương trình $y^2 = x^3 + 16$ chỉ có các nghiệm nguyên $(x, y) = (0, \pm 4)$.*

Chứng minh. Viết lại phương trình dưới dạng $y^2 - 16 = (y-4)(y+4) = x^3$. Nếu y lẻ thì $(y - 4, y + 4) = 1$ nên $y - 4$ và $y + 4$ là hai lũy thừa bậc 3 của các số nguyên sai khác 8. Nhưng các lập luận đơn giản cho thấy không có hai số lập phương với hiệu bằng 8. Vậy y, x là các số chẵn. Do $y^2 = x^3 + 16 \equiv 0 \pmod 8$ nên $y \equiv 0 \pmod 4$. Viết $y = 4y'$ ta được $16y'^2 = x^3 + 16$. Từ đây ta cũng suy ra $x \equiv 0 \pmod 4$ và do đó $x = 4x'$ và như vậy phương trình đã cho có thể viết lại thành $y'^2 = 4x'^3 + 1$. Như vậy y' lẻ, đặt $y' = 2n + 1$ ta được $n(n+1) = x'^3$. Ta suy ra $n, n+1$ là các số lập phương. Điều này dĩ nhiên chỉ xảy ra khi $n = -1$ hoặc $n = 0$. Với cả hai trường hợp ta thu được $x' = 0$ và do đó $x = 0$ và $y = \pm 4$. □

Tuy nhiên, một số phương trình Mordell phải cần đến các công cụ phức tạp hơn. Chẳng hạn như phương trình

$$y^2 = x^3 - 1$$

mà ta đã giải quyết ở Mệnh đề 2.5 đã cần đến vành Gauss. Tương tự như vậy.

Mệnh đề 2.13. *Phương trình $y^2 = x^3 - 4$ chỉ có các nghiệm nguyên $(x, y) = (2, \pm 2), (5 \pm 11)$.*

Chứng minh. Giả sử (x, y) là một nghiệm nguyên. Trước hết ta thấy rằng $x \equiv y \pmod 2$.

$x \equiv y \equiv 1 \pmod 2$. Ta viết lại đẳng thức $y^2 = x^3 - 4$ dưới dạng

$$(y + 2i)(y - 2i) = x^3$$

Trước hết ta có

Bổ đề 2.14. *Nếu y lẻ thì $y - 2i, y + 2i$ nguyên tố cùng nhau trong $\mathbb{Z}[i]$.*

Chứng minh. Thật vậy, giả sử $\alpha \mid y - 2i, \alpha \mid y + 2i$ với $\alpha \in \mathbb{Z}[i]$. Như vậy $\alpha \mid 4i$ và do đó $\alpha \mid 4$. Ta suy ra $N(\alpha) \mid N(4) = 16$. Mặt khác $N(\alpha) \mid N(y - 2i) = y^2 + 2 = x^3$. Như vậy, $N(\alpha)$, một số nguyên dương, vừa là ước của $16 = 2^4$ vừa là ước của x^3, một số nguyên lẻ. Ta suy ra $N(\alpha) = 1$ và do đó α là một phần tử đơn vị và $y - 2i, y + 2i$ là các phần tử nguyên tố cùng nhau. □

Đẳng thức $(y-2i)(y+2i)=x^3$ kết hợp với Bổ đề trên (và nhận xét đơn giản rằng mọi phần tử đơn vị đều là lập phương của một phần tử đơn vị nào đó) chứng tỏ mỗi nhân tử $y-2i, y+2i$ là lập phương của một số nguyên Gauss. Ta viết $y+2i=(a+bi)^3, a,b\in\mathbb{Z}$ (khi đó $y-2i=(a-bi)^3$). Khai triển vế phải của đẳng thức này rồi so sánh phần ảo của hai vế ta được $2=b(3a^2-b^2)$. Do $a,b\in\mathbb{Z}$ giải phương trình đơn giản này ta thu được các giá trị $(a,b)=(\pm1,1),(-2,\pm2)$. Các giá trị này cho ta các nghiệm $(x,y)=(2,\pm2)$ và $(x,y)=(5,\pm11)$. Tuy nhiên chỉ có các nghiệm $(x,y)=(5,\pm11)$ được chấp nhận vì ta đã giả sử x,y lẻ.

$x\equiv y\equiv 0 \pmod 2$. Chú ý rằng trong trường hợp này $y-2i, y+2i$ không còn nguyên tố cùng nhau nữa nên ta tiến hành hơi khác như sau. Đặt $x=2x', y=2y'$, ta nhận được phương trình theo các biến mới

$$y'^2=2x'^3-1\Leftrightarrow 2x'^3=(y'+i)(y'-i)$$

Ta suy ra y' lẻ. Do đó $y'^2\equiv 1 \pmod 8$ và $x'^3\equiv 1 \pmod 4$. Vậy x' cũng lẻ. Dễ thấy do $N(y'+i)=N(y'-i)$ là chẵn nên $1+i\mid y+i, 1+i\mid y-i$. Quan hệ của x', y' có thể được viết lại thành

$$-ix'^3=\frac{y'+i}{1+i}\frac{y'-i}{1+i}$$

Bổ đề 2.15. *Với mọi $a\in 1+2\mathbb{Z}$ ta có $1+i$ là một ước chung lớn nhất của $a+i$ và $a-i$.*

Chứng minh. Thật vậy dễ thấy $1+i\mid a+i, 1+i\mid a-i$ (tổng quát hơn, $1+i\mid\alpha\Leftrightarrow 2\mid \mathrm{N}(\alpha)$). Giả sử $\gamma\in\mathbb{Z}[i]$ sao cho $\gamma\mid a+i, \gamma a-i$, như vậy $\gamma\mid 2i$. Thế thì, một mặt $\gamma\mid a+i\Rightarrow \mathrm{N}(\gamma)\mid a^2+1$, mặt khác $\gamma\mid 2i\Rightarrow \mathrm{N}(\gamma)\mid 4$. Như vậy $\mathrm{N}(\gamma)\mid (4,a^2+1)$, nhưng do a lẻ nên $(a^2+1,4)=2$. Ta suy ra $\mathrm{N}(\gamma)\mid 2$ và như vậy $\mathrm{N}(\gamma)=1$ hoặc $=2$. Nếu $\mathrm{N}(\gamma)=1$ thì γ là một phần tử đơn vị. Nếu $\mathrm{N}(\gamma)=2$ thì $\gamma=\pm1\pm i$, có nghĩa là một phần tử liên kết của $1+i$. Các lập luận trên chứng tỏ $1+i$ là một ước chung lớn nhất của $a+i$ và $a-i$ trong $\mathbb{Z}[i]$.

□

Theo Bổ đề 2.15 ta có $\frac{y'+i}{1+i}, \frac{y'-i}{1+i}\in\mathbb{Z}[i]$ và nguyên tố cùng nhau. Một lần nữa, bởi vì trong $\mathbb{Z}[i]$ mọi phần tử đơn vị đều là lập phương của một phần tử đơn vị nên đẳng thức $-ix^3=\frac{y'+i}{1+i}\frac{y'-i}{1+i}$ kết hợp với tính nguyên tố cùng nhau của các nhân tử ở vế phải dẫn đến $\frac{y'+i}{1+i}, \frac{y'-i}{1+i}$ là các lập phương của các số nguyên Gauss nào đó. Mặt khác, do

$$y+2i=2(y'+i)=-i(1+i)^2(y'+i)=-i(1+i)^3\frac{y'+i}{1+i}=i^3(1+i)\frac{y+i}{1+i}=(-1+i)^3\frac{y+i}{1+i}$$

nên $y+2i$ cũng là lập phương của một số nguyên Gauss. Nhưng điều này, với các lập luận ở phần trước, dẫn đến $(x,y)=(2,\pm2)$ hoặc $=(5,\pm11)$. Tất nhiên, do điều kiện y chẵn, chỉ có nghiệm $(x,y)=(2,\pm2)$ là được chấp nhận ở trường hợp này.

Kết hợp hai trường hợp ở trên ta nhận được các nghiệm $(x,y)=(2,\pm2),(5,\pm11)$ của phương trình ban đầu. □

3 Đôi điều về vành $\mathbb{Z}[\sqrt{-2}]$

Ta định nghĩa

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{2}i; a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

Ta kiểm tra dễ dàng rằng $\mathbb{Z}[\sqrt{-2}]$ là một vành con chứa $\mathbb{Z}$ của $\mathbb{C}$ Tương tự như với vành $\mathbb{Z}[i]$ và bằng việc sử dụng hàm chuẩn tương ứng:

$$\mathrm{N} : \mathbb{Z}[\sqrt{-2}] \to \mathbb{N}, \mathrm{N}(a + b\sqrt{-2}) = a + 2b^2$$

ta suy ra

Mệnh đề 3.1. *Tồn tại phép chia Euclid trên* $\mathbb{Z}[\sqrt{-2}]$.

Chứng minh. Tương tự như với vành Gauss. Chi tiết được để lại như bài tập.

□

Cũng như với vành Gauss, kết quả trên dẫn đến

Định lý 3.2. *Định lý cơ bản của số học còn đúng cho các vành* $\mathbb{Z}[\sqrt{-2}]$.

Chứng minh. Bài tập.

□

Việc miêu tả các phần tử bất khả qui của $\mathbb{Z}[\sqrt{-2}]$ dẫn đến

Định lý 3.3. *Cho p là một số nguyên tố lẻ. Phương trình*

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

có nghiệm nguyên khi và chỉ khi $p \equiv 1$ *hoặc* $\equiv 3 \pmod 8$.

Chứng minh. Bài tập. □

Hệ quả 3.4. *Một số nguyên n có thể được viết dưới dạng* $n = a^2 + 2b^2$*, với a, b nguyên, khi và chỉ khi trong phân tích của n ra thừa số nguyên tố, các số nguyên tố* 2 *và các số nguyên tố* $p \equiv 5 \pmod 8$ *và* $p \equiv 7 \pmod 8$ *xuất hiện với lũy thừa chẵn.*

Giống như với $\mathbb{Z}[i]$, ta có thể sử dụng vành $\mathbb{Z}[\sqrt{-2}]$ trên để giải quyết một số phương trình Diophante bậc cao hơn, chẳng hạn như phương trình Mordell sau đây.

Định lý 3.5 (Fermat)**.** *Phương trình* $y^2 = x^3 - 2$ *chỉ có các nghiệm nguyên duy nhất* $(x, y) = (3, \pm 5)$.

Chứng minh. Bài tập. □