BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

TRẦN THẾ HÙNG

ỨNG DỤNG CỦA MỘT SỐ LỚP VÀNH SỐ VÀO GIẢI TOÁN SƠ CẤP

ĐỒ ÁN THẠC SĨ TOÁN HỌC

Nghệ An - 2024

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

TRẦN THẾ HÙNG

ỨNG DỤNG CỦA MỘT SỐ LỚP VÀNH SỐ VÀO GIẢI TOÁN SƠ CẤP

Chuyên ngành: **ĐẠI SỐ VÀ LÝ THUYẾT SỐ**
Mã số: 8460104

ĐỒ ÁN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học
TS. THIỀU ĐÌNH PHONG

Nghệ An - 2024

MỤC LỤC

MỞ ĐẦU

Trong đại số, lý thuyết vành là lĩnh vực nghiên cứu về các cấu trúc đại số với phép cộng và phép nhân được định nghĩa và có các thuộc tính tương tự như các phép toán được định nghĩa cho số nguyên. Lý thuyết vành nghiên cứu cấu trúc của các vành, các biểu diễn của chúng và các lớp vành đặc biệt. Trong đó, các lớp vành số như vành đa thức, vành chuỗi lũy thừa hình thức hay các tính chất chia hết trên vành số nguyên đã được nghiên cứu trên nhiều đối tượng sơ cấp và đã có nhiều kết quả phố dụng.

Tuy vậy, việc tiếp cận giải quyết các bài toán sơ cấp thông qua xây dựng các đồng cấu vành trên các lớp vành số cũng như vận dụng các tính chất số học, đại số đặc trưng của các lớp vành số này vẫn còn nhiều khía cạnh chưa được khai thác và trình bày một cách có hệ thống.

Trên cơ sở quá trình nghiên cứu và thực tiễn giảng dạy ở bậc phổ thông, chúng tôi xây dựng các nhóm bài toán liên quan có thể giải được bằng các kiến thức về lớp các vành số và ngược lại, từ các nhóm bài toán cụ thể, xây dựng, tìm kiếm những lý thuyết, công cụ phù hợp để giải quyết chúng một cách hiệu quả. Với mong muốn tìm hiểu, cũng như hệ thống hóa lại một cách cơ bản những ứng dụng của một số lớp vành số trong việc tiếp cận, giải quyết một số đối tượng bài toán sơ cấp, chúng tôi chọn đề tài: **"Ứng dụng của một số lớp vành số vào giải toán sơ cấp"** làm nội dung nghiên cứu trong đồ án tốt nghiệp của mình.

Ngoài phần mở đầu, kết luận và tài liệu tham khảo, nội dung của đồ án được chia thành hai chương.

Chương 1. Kiến thức chuẩn bị, Chương này trình bày các kiến thức cơ sở, các ví dụ cũng như tập trung hoàn thiện một số vấn đề lý thuyết theo góc nhìn sơ cấp để thuận tiện sử dụng ở chương 2. Do khuôn khổ của đồ án, các chứng minh cơ bản và kinh điển sẽ không được nhắc lại .

Chương 2. Ứng dụng của một số lớp vành số vào giải toán sơ cấp, Chương này là nội dung chính của đồ án, trọng tâm là việc xây dựng và trình bày các tính chất liên quan của các lớp vành số và sử dụng chúng trong giải quyết bài toán sơ cấp.

Đồ án được thực hiện tại Trường Đại học Vinh dưới sự hướng dẫn khoa học của TS. Thiều Đình Phong và được thực nghiệm tại Trường THPT Chuyên Hà Tĩnh - nơi tác giả công tác. Tác giả xin được bày tỏ lời cảm ơn sâu sắc tới quý Trường, quý thầy cô, bạn bè, gia đình và đồng nghiệp đã quan tâm tạo điều kiện giúp đỡ tác giả trong quá tình học tập và hoàn thành đồ án.

Trân trọng.

Nghệ An, tháng 11 năm 2024

Tác giả

CHƯƠNG 1

KIẾN THỨC CHUẨN BỊ

1.1 Vành, vành con, miền nguyên, iđêan

Định nghĩa 1.1.1. Tập hợp R khác rỗng cùng với các phép toán hai ngôi $(+), (.)$ trên R được gọi là một *vành* nếu thỏa mãn các điều kiện sau:

(i) $(R, +)$ là một nhóm Abel có phần tử đơn vị là 0.

(ii) $(R, .)$ là một nửa nhóm.

(iii) Phép nhân $(.)$ phân phối về hai phía đối với phép cộng.

Vành R được gọi là *vành giao hoán* nếu phép nhân trong R có tính chất giao hoán, vành R được gọi là *có đơn vị* nếu phép nhân có đơn vị.

Vành R giao hoán, có đơn vị, thỏa mãn thêm điều kiện đơn vị 1 khác 0 và mọi phần tử khác 0 của R đều khả nghịch đối với phép nhân thì khi đó R được gọi là một *trường*.

Ví dụ 1.1.2. (i) Với phép cộng và phép nhân thông thường, $\mathbb{Z}$ là vành giao hoán có đơn vị là 1; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ là trường.

(ii) Cho n là số nguyên dương lớn hơn 1, $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n}\}$ cùng với phép cộng và phép nhân các lớp thặng dư là một vành giao hoán có đơn vị và được gọi là *vành các lớp thặng dư môđun n*. Nếu n là số nguyên tố p thì $\mathbb{Z}_p$ là một trường.

(iii) Cho i là đơn vị ảo trong trường các số phức $\mathbb{C}$, tức là $i^2 = -1$. Khi đó $\mathbb{Z}[i] = \{m + ni | m, n \in \mathbb{Z}\}$ với các phép cộng và phép nhân số phức là một vành giao hoán, có đơn vị.

Định nghĩa 1.1.3. Tập con khác rỗng A của một vành R là một *vành con* của R nếu và chỉ nếu hai điều kiện sau được thỏa mãn:

(i) $x - y \in A$ với mọi $x, y \in A$;

(ii) $xy \in A$ với mọi $x, y \in A$.

Ví dụ 1.1.4. (i) Cho m là số nguyên dương. Khi đó $m\mathbb{Z} = \{0, \pm m, \pm 2m, ...\}$ là vành con của $\mathbb{Z}$.

(ii) Cho R là một vành có đơn vị, khi đó tập U các phần tử khả nghịch trong R lập thành một vành con của R.

Định nghĩa 1.1.5. Cho R là một vành giao hoán có đơn vị và có nhiều hơn một phần tử.

(i) Một phần tử $a \in R$ được gọi là một *ước của không*, nếu tồn tại phần tử $b \in R, b \neq 0$ để $ab = 0$.

(ii) R được gọi là *miền nguyên* nếu trong R không có ước của không nào ngoài phần tử 0.

Ví dụ 1.1.6. (i) Trong vành $\mathbb{Z}_6$, các lớp $\overline{2}, \overline{3}$ là các ước của không. Vành $\mathbb{Z}_p$ với p là số nguyên tố, không có ước của không nên là một miền nguyên.

(ii) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[i]$ là các miền nguyên.

(iii) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ là miền nguyên.

(iv) $\mathbb{Z}_2[i] = \{a + bi | a, b \in \mathbb{Z}_2\}$ không là một miền nguyên do có các ước của không, chẳng hạn như là $(\overline{1} + i)$ vì $(\overline{1} + i)(\overline{1} - i) = \overline{1} + \overline{1} = \overline{0}$.

Định nghĩa 1.1.7. Một tập con khác rỗng I của vành R là một *iđêan* của R nếu và chỉ nếu các tính chất sau được thỏa mãn.

(i) $a - b \in I$ với mọi $a, b \in I$;

(ii) $ax \in I$ và $xa \in I$, với mọi $a \in I$ và $x \in R$.

Ví dụ 1.1.8. (i) $\{0\}$ và R là các iđêan con của vành R.

(ii) $\mathbb{Z}$ là một vành con của $\mathbb{Q}$ tuy nhiên $\mathbb{Z}$ không là iđêan của $\mathbb{Q}$.

Định nghĩa 1.1.9. (i) Cho I là một iđêan của vành R và S là một tập con của I. Tập S được gọi là *hệ sinh* của iđêan I nếu mọi phần tử của I đều biểu diễn được dưới dạng

$$t_1x_1r_1 + t_2x_2r_2 + ... + t_nx_nr_n \text{ với } n \in \mathbb{N}^*, x_i \in S, r_i, t_i \in R, i = \overline{1,n}.$$

Khi đó, ta ký hiệu $I = \langle S \rangle$.

(ii) Cho R là một vành giao hoán, một iđêan P của R được gọi là *iđêan nguyên tố* nếu thỏa mãn các điều kiện:

(a) $P \neq R$

(b) Với $a, b \in R$, nếu $ab \in P$ thì $a \in P$ hoặc $b \in P$.

(iii) Cho R là một vành giao hoán, một iđêan M của R được gọi là *iđêan tối đại* nếu thỏa mãn các điều kiện:

(a) $M \neq R$

(b) Với bất kỳ iđêan A của R thỏa mãn $M \subseteq A \subseteq R$ thì $A = M$ hoặc $A = R$.

Ví dụ 1.1.10. (i) Iđêan $\langle 4 \rangle = \{4n | n \in \mathbb{Z}\}$ không là một iđêan nguyên tố của $\mathbb{Z}$ do $2.6 = 12 \in \langle 4 \rangle$ nhưng $2 \notin \langle 4 \rangle$ và $6 \notin \langle 4 \rangle$.

(ii) $\langle \overline{2} \rangle = \{\overline{0}; \overline{2}; \overline{4}\}$ và $\langle \overline{3} \rangle = \{\overline{0}; \overline{3}\}$ là các iđêan tối đại của $\mathbb{Z}_6$.

(iii) Iđêan $\langle 4 \rangle$ không là iđêan tối đại của $\mathbb{Z}$ nhưng là iđêan tối đại của $2\mathbb{Z}$.

1.2 Đồng cấu vành

Định nghĩa 1.2.1. Một ánh xạ f từ vành X đến vành Y được gọi là một *đồng cấu vành* nếu $f(a + b) = f(a) + f(b)$ và $f(ab) = f(a).f(b)$ với mọi $a, b \in X$.

Ví dụ 1.2.2. Với số nguyên dương $d > 1$ là số không chính phương (không tồn tại số nguyên tố p sao cho $p^2|d$). Ta có

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$$

và

$$\mathbb{Z}[\sqrt{-d}] = \mathbb{Z}[i\sqrt{d}] = \{a + ib\sqrt{d} | a, b \in \mathbb{Z}, i^2 = -1\}$$

với phép cộng và phép nhân thông thường lập thành một vành giao hoán có đơn vị, Khi đó các ánh xạ:

(i) $f : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$
$a + b\sqrt{d} \mapsto a - b\sqrt{d}$

(ii) $f : \mathbb{Z}[\sqrt{-d}] \to \mathbb{Z}[\sqrt{-d}]$
$a + ib\sqrt{d} \mapsto a - ib\sqrt{d}$
đều là các tự đẳng cấu.

Định lí 1.2.3. *Giả sử $f : X \to Y$ là một đồng cấu vành, khi đó:*

(i) $f(0) = 0$.

(ii) $f(-x) = -f(x), \forall x \in X$.

(iii) Ảnh $\operatorname{Im} f = f(X)$ *của f là một vành con của Y.*

(iv) Hạch $\operatorname{Ker} f = f^{-1}(0) = \{x \in X | f(x) = 0\}$ *là một iđêan của X.*

1.3 Quan hệ chia hết trên miền nguyên

Định nghĩa 1.3.1. Cho R là một miền nguyên với đơn vị 1. Trên R ta có các khái niệm như sau:

(i) Phần tử a được gọi là một *ước* của phần tử b nếu tồn tại phần tử c để $b = ac$.

(ii) Mọi phần tử khả nghịch của R đều là ước của đơn vị.

(iii) Hai phần tử a, b được gọi là *liên kết* nếu a là ước của b và b là ước của a.

(iv) a được gọi là một *ước thực sự* của b nếu a là một ước của b, đồng thời a không khả nghịch và cũng không liên kết với b.

(v) Phần tử khác 0 và không khả nghịch p được gọi là một *phần tử bất khả quy* nếu p không có ước thực sự nào.

(vi) Phần tử khác 0 và không khả nghịch p được gọi là *phần tử nguyên tố* nếu p chia hết xy thì p chia hết x hoặc p chia hết y.

Ví dụ 1.3.2. (i) Trong $\mathbb{Z}_7$, ta có $\overline{3}.\overline{4} = \overline{12} = \overline{5}$ và $\overline{5}.\overline{2} = \overline{10} = \overline{3}$ hay $\overline{3}$ và $\overline{5}$ là hai phần tử liên kết với nhau trong $\mathbb{Z}_7$.

(ii) Các phần tử $1-i, 1+i$ là các phần tử bất khả quy trong $\mathbb{Z}[i]$.

(iii) Phần tử $\overline{2}$ là phần tử nguyên tố nhưng không là phần tử bất khả quy trong vành $\mathbb{Z}_6$.

(iv) Phần tử $1+\sqrt{3}$ là phần tử bất khả quy nhưng không là phần tử nguyên tố trong $\mathbb{Z}[\sqrt{3}]$.

(v) Trong vành $\mathbb{Z}$, các số $\pm 2, \pm 3, \pm 4, \pm 6$ là các ước thực sự của 12 còn $\pm 1, \pm 12$ là các ước không thực sự của 12.

1.4 Vành chính, vành Gauss, vành Euclide

Định nghĩa 1.4.1. Giả sử R là một miền nguyên. Khi đó R được gọi là *vành chính* nếu mọi iđêan của R đều là iđêan chính (iđêan sinh bởi một phần tử).

Định nghĩa 1.4.2. Cho R là một vành và $a, b \in R$.

(i) Phần tử $d \in R$ được gọi là *ước chung* của a và b nếu $d|a$ và $d|b$.

(ii) Phần tử $d \in R$ được gọi là *ước chung lớn nhất* của a và b, ký hiệu $d = \gcd(a, b)$ nếu thỏa mãn hai điều kiện sau:

(a) d là một ước chung của a và b.

(b) Nếu c là một ước chung của a và b thì $c|d$.

Nhận xét 1.4.3. Trong một vành chính, ước chung lớn nhất của hai phần tử luôn tồn tại.

Định nghĩa 1.4.4. Một phần tử $x \neq 0$ trong miền nguyên R được gọi là có sự phân tích duy nhất thành tích các phần tử bất khả quy nếu thoản mãn các điều kiện sau:

(i) x phân tích được thành tích các phần tử trong R dạng

$$x = u.p_1.p_2...p_n,$$

trong đó u khả nghịch, p_i là các phần tử bất khả quy.

(ii) Nếu x có một sự phân tích tương tự khác dạng

$$x = v.q_1.q_2...q_m,$$

trong đó v khả nghịch, q_i là các phần tử bất khả quy thì $m = n$ và p_i và q_i là liên kết (sau một phép hoán vị các chỉ số nếu cần thiết).

Định nghĩa 1.4.5. Một miền nguyên R thoả mãn điều kiện mọi phần tử khác 0 đều có phân tích duy nhất thành tích các phần tử bất khả quy, được gọi là một *vành nhân tử hóa* (hay còn gọi là *vành Gauss*).

Nhận xét 1.4.6. Mỗi vành chính là một vành nhân tử hóa.

Ví dụ 1.4.7. (i) Vành các số nguyên $\mathbb{Z}$ là vành chính vì mọi iđêan của $\mathbb{Z}$ là iđêan chính dạng $m\mathbb{Z}$ với $m \in \mathbb{Z}$.

(ii) Vành $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}$ là một miền nguyên nhưng không phải là vành Gauss vì có phân tích không duy nhất, chẳng hạn như

$$4 = 2.2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

(iii) Vành $\mathbb{Z}[i]$ là một vành chính.

Định nghĩa 1.4.8. Một miền nguyên R được gọi là *vành Euclide* nên trên R có một ánh xạ $J : R\backslash\{0\} \to \mathbb{N}$ thỏa mãn các điều kiện sau:

(i) $J(ab) \geq J(a)$ với mọi a, b khác 0 trong R.

(ii) Với $\forall a, b \in R, b \neq 0$, tồn tại $q, r \in R$ sao cho $a = bq + r$, trong đó $r = 0$ hoặc nếu $r \neq 0$ thì $J(r) < J(b)$.

Ánh xạ J được gọi là *ánh xạ Euclide* trên R.

Nhận xét 1.4.9. Mọi vành Euclide đều là vành chính.

Ví dụ 1.4.10. (i) Vành các số nguyên $\mathbb{Z}$ là vành Euclide vì có ánh xạ Euclide $J : \mathbb{Z}\backslash\{0\} \to \mathbb{N}$, xác định bởi $J(n) = |n|$

(ii) Vành các số nguyên Gauss $\mathbb{Z}[i]$ là vành Euclide với ánh xạ Euclide $J : \mathbb{Z}[i]\backslash\{0\} \to \mathbb{N}$, xác định bởi $J(n) = |n|^2$

1.5 Vành đa thức một ẩn

Định nghĩa 1.5.1. Cho R là một vành và S là một vành chứa R với $x \in S$. Khi đó ta nói x là một *phần tử siêu việt* trên R nếu với mọi $a_0, a_1, ..., a_n \in R$, $(n \geq 0)$ mà $a_0 + a_1x + ... + a_nx^n = 0$ trong S thì $a_i = 0, \forall 0 \geq i \geq n$.

Nếu x không phải là phần tử siêu việt trên R thì x được gọi là *phần tử đại số* trên R.

Định lí 1.5.2. *Cho R là một vành giao hoán có đơn vị 1. Khi đó tồn tại cặp (S, x) thỏa mãn các điều kiện sau.*

(i) S là một vành giao hoán chứa R như là một vành con của S.

(ii) $x \in S$ và x siêu việt trên R.

(iii) Mỗi phần tử $0 \neq f \in S$ đều biểu diễn được một cách duy nhất dưới dạng $f = a_0 + a_1x + ... + a_nx^n$ trong đó $a_0, a_1, ..., a_n \in R(n \geq 0)$ và $a_n \neq 0$.

Định nghĩa 1.5.3. Vành S xác định duy nhất như trong Định lý 1.5.2 được gọi là *vành đa thức một ẩn* x trên vành R và ký hiệu $S := R[x]$

Nhận xét 1.5.4. Nếu R là một miền nguyên thì vành đa thức $R[x]$ cũng là miền nguyên.

Mệnh đề 1.5.5. *(i) Cho R là một miền nguyên, khi đó phần tử khả nghịch của R và $R[x]$ là như nhau.*

(ii) Nếu I là một iđêan của vành R, thì $I[x]$ là một iđêan của $R[x]$.

Định nghĩa 1.5.6. R là một miền nguyên, đa thức $f(x)$ thuộc $R[x]$ được gọi là *bất khả quy* trên R nếu:

(i) $f(x)$ khác không và không khả nghịch.

(ii) Nếu $f(x) = g(x).h(x)$ với $g(x), h(x) \in R[x]$ thì $f(x)$ hoặc $g(x)$ là khả nghịch

Ví dụ 1.5.7. (i) $f(x) = x^2 - 2$ là bất khả quy trên $\mathbb{Q}$ nhưng khả quy trên $\mathbb{R}$.

(ii) $g(x) = 2x^2 + 4$ là bất khả quy trên $\mathbb{Q}$ nhưng khả quy trên $\mathbb{Z}$.

(iii) $h(x) = 2x^2 + 4$ là bất khả quy trên $\mathbb{R}$ nhưng khả quy trên $\mathbb{C}$.

Định lí 1.5.8. *Ta có các khẳng định sau đây:*

(i) Cho F là một trường. Với $f(x) \in F[x]$ mà $\deg f(x) = 2$ hoặc 3. Khi đó $f(x)$ khả quy trên F khi và chỉ khi $f(x)$ có nghiệm thuộc F.

(ii) Cho $f(x)$ là một đa thức thuộc $\mathbb{Z}[x]$. Nếu $f(x)$ khả quy trên $\mathbb{Q}$ thì $f(x)$ khả quy trên $\mathbb{Z}$.

Mệnh đề 1.5.9. *Cho F là một trường và a là phần tử khác 0 của F. Khi đó, nếu $af(x), f(ax)$ hay $f(x+a)$ là bất khả quy trên F thì $f(x)$ cũng bất khả quy trên F.*

Ví dụ 1.5.10. (i) $f(x) = x^2 + 1$ bất khả quy trên $\mathbb{Z}_3$ nhưng khả quy trên $\mathbb{Z}_5$.

(ii) $g(x) = x^2 + x + 1$ bất khả quy trên $\mathbb{Z}_2$ nhưng khả quy trên $\mathbb{Z}_3$.

Mệnh đề 1.5.11. *Với mỗi số nguyên a, $\overline{a}$ là lớp đồng dư của a theo* $\bmod p$ *(p là số nguyên tố). Khi đó ánh xạ $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ được cho bởi*

$$\varphi(a_0 + a_1x + ... + a_nx^n) = \overline{a_0} + \overline{a_1}x + ... + \overline{a_n}x^n$$

là một đồng cấu vành.

CHƯƠNG 2

ỨNG DỤNG CỦA MỘT SỐ LỚP VÀNH SỐ VÀO GIẢI TOÁN SƠ CẤP

2.1 Ứng dụng vành các lớp thặng dư vào giải toán

Việc phân hoạch thành các lớp thặng dư giúp ta thay vì làm việc trên tập $\mathbb{Z}$ - tập vô hạn thì ta sẽ làm việc trên tập $\mathbb{Z}_n$ - tập hữu hạn. Ngoài ra có một điều đặc biệt mà ở tập $\mathbb{Z}$ không thực hiện được là phép chia giữa các số nguyên a, b (kết quả có thể là số hữu tỷ). Tuy nhiên khi n là số nguyên tố thì $\mathbb{Z}_n$ khắc phục được điều này. Chúng ta cùng tìm hiểu cụ thể điều đó qua các ứng dụng trực tiếp sau.

2.1.1 Giải phương trình nghiệm nguyên

Xét phương trình $f(x, y, ...) = 0$ trên tập $\mathbb{Z}$. Nếu phương trình có nghiệm trong $\mathbb{Z}_n$. Như vậy chúng ta sẽ có sự thuận lợi trong tình huống chứng minh phương trình vô nghiệm hoặc hạn chế được số trường hợp phải xét.

Chúng ta cùng tìm hiểu thông qua các ví dụ sau.

Ví dụ 2.1.1. Tìm tất cả các nghiệm nguyên của phương trình

(i) $x^2 = y^3 + 7$

(ii) $x^2 + 1 = 3y$

(iii) $x^3 + y^3 = z^6 + 3$.

Lời giải.

(i) Nếu phương trình có nghiệm trong $\mathbb{Z}$ thì nó cũng có nghiệm trong $\mathbb{Z}_4$. Khi đó có $\overline{x}, \overline{y} \in \mathbb{Z}_4$ để $\overline{x}^2 = \overline{y}^3 + \overline{3}$ trong $\mathbb{Z}_4$ có $\overline{x}^2 \in \{0; 1\}$ từ đó suy ra

$y = 2k + 1, x = 2m$. Như vậy,

$$4m^2 + 1 = (2k + 1)^3 + 2^3 = (2k + 3)(4k^2 + 3).$$

Vậy $4m^2 + 1$ phải chia hết cho một số có dạng $4h + 3$, điều này không xảy ra được. Hay phương trình vô nghiệm.

(ii) Tương tự xét trên $\mathbb{Z}_3$.

(iii) Tương tự xét trên $\mathbb{Z}_7$:

Trong Z_7 có $\overline{0}^3 = \overline{0}$, $\overline{1}^3 = \overline{1}$, $\overline{2}^3 = \overline{1}$, $\overline{3}^3 = \overline{6}$, $\overline{4}^3 = \overline{1}$, $\overline{5}^3 = \overline{6}$, $\overline{6}^3 = \overline{6}$.

Vậy $\overline{x}^3, \overline{y}^3$ chỉ có thể là $\overline{0}, \overline{1}, \overline{6}$. Từ đó, $\overline{x}^3 + \overline{y}^3$ chỉ có thể là $\overline{0}, \overline{1}, \overline{2}, \overline{5}, \overline{6}$ nhưng $\overline{z}^6 + 3$ chỉ có thể là $\overline{3}, \overline{4}$. Điều này chứng tỏ phương trình vô nghiệm.

Ví dụ 2.1.2. Tìm tất cả các nghiệm nguyên của phương trình

(i) $x^2 + 4y^4 = z^6 + 6$

(ii) $x^2 + 1 = 3y + 2016z^4$

(iii) $x^2 + 2015y^3 + 2 = 5z^{10}$.

Lời giải.

Hoàn toàn tương tự ví dụ trên, ta kiểm tra được.

(i) Phương trình vô nghiệm trên $\mathbb{Z}_8$.

(ii) Phương trìnhvô nghiệm trên $\mathbb{Z}_3$.

(iii) Phương trình vô nghiệm trên $\mathbb{Z}_5$.

Một số ví dụ khác cho chúng ta thấy lợi ích khi hạn chế được số trường hợp trên $\mathbb{Z}_n$

Ví dụ 2.1.3. Xác định số nguyên x, số nguyên dương y thỏa mãn phương trình

$$x^2 - y! = 2015$$

Lời giải. Do $(-x)^2 = x^2$ nên ta chỉ cần xét $x \in \mathbb{Z}^+$.

Nếu phương trình đã cho có nghiệm trong $\mathbb{Z}^+$ thì nó cũng có nghiệm trên $\mathbb{Z}_7$ Xét trường hợp $y \geq 7$. Khi đó $y! \equiv 0 \pmod 7$ nên $x^2 \equiv 2015$ hay $x^2 \equiv 6 \pmod 7$. Điều này không xảy ra. Kiểm tra lần lượt ta chỉ nhận được $x = 45, y = 4$ thỏa mãn.

Do vậy nghiệm của phương trình là $x = \pm 45, y = 4$.

Sau đây là một số bài toán tương tự để chúng ta có thể tự rèn luyện.

Bài toán 2.1.4. Tìm các số nguyên x, y, z thỏa mãn

(i) $x^4 + 7y^3 + 2 = 2016z^5$

(ii) $x^{2016} + 2^{2016} + 3 = 2017y$

(iii) $(x+1)^2 + (x+2)^2 + ...(x+2019)^2 = y^2$

(iv) $x^5 - y^2 = 4$

Bài toán 2.1.5. Xác định tất cả các cặp số nguyên tố (p, q) thỏa mãn phương trình $p^3 - q^5 = (p+q)^2$

2.1.2 Bài toán chứng minh sự tồn tại

Bài toán chứng minh tồn tại trong số học có nhiều hướng tiếp cận từ việc sử dụng hệ thặng dư, định lý CRT, định giá p - adic,... cho đến các yếu tố giải tích. Ở đây chúng ta sử dụng tính chất nghịch đảo theo môđun p, một số kiến thức sẽ được nhắc lại để sử dụng trong mục này.

Mệnh đề 2.1.6. Lớp $\overline{a} \in \mathbb{Z}_n$ được gọi là *lớp khả nghịch* nếu có $\overline{b} \in \mathbb{Z}_n$ để $\overline{a}.\overline{b} = \overline{1}$

Khi $n = p$ là số nguyên tố, mọi phần tử khác 0 đều khả nghịch.

Định lí 2.1.7. *Lớp $\overline{a} \in \mathbb{Z}_n$ là khả nghịch nếu và chỉ nếu $(a, n) = 1$*

Như vậy với hai số nguyên dương a, n thỏa mãn $(a, n) = 1$ thì a luôn có nghịch đảo theo môđun n hay phương trình $ax \equiv b \pmod{n}$ luôn có nghiệm $x \equiv a^{-1}b \pmod{n}$

Kết quả trên khá hữu ích trong một số bài toán chỉ ra sự tồn tại theo quan hệ đồng dư.

Ví dụ 2.1.8. Giả sử a và b là hai số nguyên dương thỏa mãn $(a, b) = 1$. Xét cấp số cộng (a_n) với $a_0 = a, a_n = a_0 + nb$ với n là số tự nhiên. Chứng minh rằng tồn tại vô hạn số hạng trong cấp số cộng có cùng ước nguyên tố.

Lời giải

Vì $(a, b) = 1$ nên a có nghịch đảo môđun b.

Giả sử số nguyên m thỏa mãn $am \equiv 1 \pmod{b}$. Với mọi số tự nhiên r ta xét $s_r = (a+b)(am)^r$.

Ta có $s_r \equiv a \pmod b$. Do vậy s_r là một số hạng thuộc cấp số cộng (a_n).

Các số hạng s_r này có cùng ước nguyên tố, chẳng hạn ước nguyên tố của $a, m, a+b$.

Ví dụ 2.1.9. Tồn tại hay không $f(x) \in \mathbb{Z}[x]$ sao cho: với mọi số nguyên tố p và cặp số nguyên a, b thỏa mãn $p|ab-1$ thì $p|f(a)f(b)-1$.

Lời giải. Dựa vào định nghĩa của nghịch đảo theo môđun p thì với a không chia hết cho p thì luôn tìm được số nguyên b thỏa mãn $ab \equiv 1 \pmod p$. Giả sử

$$f(x) = \sum_{i=0}^{d} c_i x^i$$

theo giả thiết ta có

$$f(a)f(b) \equiv 1 \pmod p \Rightarrow a^d f(a)f(b) \equiv a^d \pmod p.$$

Tuy nhiên

$$\begin{aligned} a^d f(b) &\equiv c_d(ab)^d + c_{d-1}(ab)^{d-1}a + ... + c_1(ab)a^{d-1} + c_0 a^d \pmod p \\ &\equiv c_d + c_{d-1}a + ... + c_1 a^{d-1} + c_0 a^d \pmod p. \end{aligned}$$

Vì thế nếu gọi $g(x) = \sum_{i=0}^{d}$ thì $f(a)g(a) \equiv a^d \pmod p$ với mọi a nguyên tố với p.

Điều này dẫn đến với mỗi số nguyên a thì $f(a)g(a) - a^d$ chia hết cho vô hạn số nguyên tố $p > a$, kéo theo $f(a)g(a) - a^d = 0$.

Vì thế $f(x)g(x) = n^d$, từ đây đồng nhất hệ số hai bên, ta có: $f(x) = \pm x^d$.

Ví dụ 2.1.10. Giả sử hai số nguyên dương m, n có tính chất

$$(2017k - 1, m) = (2017k - 1, n)$$

với mọi số nguyên dương k. Chứng minh rằng tồn tại số nguyên r để

$$m = 2017^r.n.$$

Lời giải. Trước hết, ta chỉ ra rằng, với mọi số nguyên tố $p \neq 2017$ ta luôn có $v_p(m) = v_p(n)$. Thật vậy, giả sử rằng $v_p(m) > v_p(n)$. Ta biểu diễn $m = p^\alpha b$ và $n = p^\gamma c$ với $\alpha > \gamma$ và $(b, p) = (c, p) = 1$. Khi đó tồn tại k để $2017k \equiv 1 \pmod{p^\alpha}$.

Như vậy $p^\alpha | (2017k - 1, m) = (2017k - 1, n)$ và suy ra $p^\alpha | n$. Mâu thuẫn do $\alpha > \gamma$. Từ đó suy ra tồn tại số nguyên r để $2017^n = m$.

Ví dụ 2.1.11. Xác định một cấp số cộng gồm vô hạn các số nguyên dương khác nhau sao cho mỗi số hạng không thể biểu diễn thành hai số lập phương.

Lời giải. Giả sử cấp số cộng (a_n) với $a_0 = a$ và $a_{n+1} = a_n + d$ với mọi số nguyên $n \geq 0$. Ta xét giới hạn số lớp thặng dư là những lập phương theo môđun d.

Trước tiên, xét $a^3 \equiv 1 \pmod{d}$ cho tất cả các số nguyên a.

Với số nguyên tố p và $(a, p) = 1$ ta có $a^{p-1} \equiv 1 \pmod{p}$.

Nếu $p - 1 = 3 \Rightarrow p = 4$. Mâu thuẫn.

Nếu $p - 1 = 6 \Rightarrow p = 7$.

Ta kiểm tra được

$$A = \{\overline{a}^3 | \overline{a} \in \mathbb{Z}_7\} = \{\overline{0}, \overline{1}, \overline{6}\}.$$

Từ đây suy ra $A + A = \{\overline{0}, \overline{1}, \overline{2}, \overline{5}, \overline{6}\}$. Vậy ta chọn a sao cho $\overline{a}$ theo môđun 7 không phụ thuộc vào $A + A$. Ta có thể chọn hai cấp số cộng (a_n) với $a_0 = 3$ hoặc $a_0 = 4$ và $d = 7$.

2.1.3 Tính khả quy, bất khả quy của đa thức trên trường $\mathbb{Z}_p$

Trong suốt mục này, ta luôn giả thiết p là số nguyên tố, khi đó $\mathbb{Z}_p$ là một trường.

Với mỗi đa thức $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ và mỗi số nguyên tố p, ta đặt $\overline{f(x)} = \overline{a}_n x^n + ... + \overline{a}_1 x + \overline{a}_0 \in \mathbb{Z}_p[x]$

Định lý sau đây cho ta một công cụ rất mạnh để xét tính bất khả quy trên $\mathbb{Q}$ của các đa thức với hệ số nguyên.

Định lí 2.1.12. *Nếu tồn tại số nguyên tố p sao cho* $\deg f(x) = \deg \overline{f(x)}$ *và* $\overline{f(x)}$ *bất khả quy trên* $\mathbb{Z}_p$ *thì* $f(x)$ *bất khả quy trên* $\mathbb{Q}$.

Chứng minh. Vì $\overline{f(x)}$ bất khả quy trên $\mathbb{Z}_p$ nên $\deg \overline{f(x)} > 0$ suy ra $\deg f(x) > 0$.

Giả sử $f(x)$ bất khả quy trên $\mathbb{Q}$. Theo Bổ đề Gauss, $f(x)$ có phân tích $f(x) = g(x)h(x)$ trong đó $g(x), h(x) \in \mathbb{Z}[x]$ và $g(x)$,$h(x)$ có bậc nhỏ hơn bậc của $f(x)$. Chú ý rằng $\overline{f(x)} = \overline{g(x)}.\overline{h(x)}$, do đó $\deg \overline{f(x)} = \deg \overline{g(x)} + \deg \overline{h(x)}$.

Mặt khác $\deg g(x) \geq \deg \overline{g(x)}$ và $\deg h(x) \geq \deg \overline{h(x)}$, tuy nhiên $\deg f(x) = \deg \overline{f(x)}$ nên $\deg g(x) = \deg \overline{g(x)}$ và $\deg h(x) = \deg \overline{h(x)}$.

Do đó $\overline{f(x)}$ phân tích được thành tích của hai đa thức $\overline{g(x)}$ và $\overline{h(x)}$ có bậc thấp hơn. Điều này mâu thuẫn với tính bất khả quy của $\overline{f(x)}$ trên $\mathbb{Z}_p$ □

Như vậy, để chứng minh đa thức là bất khả quy trên $\mathbb{Q}$, ta sẽ cố gắng tìm một số nguyên tố p sao cho $f(x)$ có bậc không giảm khi chuyển vào $\mathbb{Z}_p[x]$ và $\overline{f(x)}$ bất khả quy trên $\mathbb{Z}_p$.

Tuy nhiên, phương pháp này đôi khi không áp dụng được vì chiều ngược lại của định lý không được đảm bảo, có những đa thức bất khả quy trên $\mathbb{Q}$ nhưng khả quy trên $\mathbb{Z}_p$ với mọi số nguyên tố p, chẳng hạn

$$f(x) = x^4 - 10x^2 + 1, g(x) = x^4 + 1.$$

Ví dụ 2.1.13. Chứng minh các đa thức sau là bất khả quy trên $\mathbb{Q}$

(i) $f(x) = 5x^2 + 10x + 4$

(ii) $g(x) = 3x^3 + 7x^2 + 10x - 5$

(iii) $h(x) = 11x^4 - 5x^3 + 21x^2 - 9x + 6.$

Lời giải.

(i) $\overline{f(x)} = 2x^2 + x + 1 \in \mathbb{Z}_3[x]$ không có nghiệm trong $\mathbb{Z}_3$ và $\deg \overline{f(x)} = 2$ nên $\overline{f(x)}$ bất khả quy trên $\mathbb{Z}_3$. Rõ ràng $\deg f(x) = \deg \overline{f(x)}$ nên $f(x)$ bất khả quy trên $\mathbb{Q}$.

(ii) Tương tự, ta xét $\overline{g(x)} = x^3 + x^2 - 1 \in \mathbb{Z}_2[x]$.

(iii) Vì $\overline{h(x)} = x^4 + x^2 + x + 1 \in \mathbb{Z}_5[x]$ không có nghiệm trong $\mathbb{Z}_5$ nên nó không có nhân tử bậc nhất. Giả sử $\overline{h(x)}$ khả quy trên $\mathbb{Z}_5$. Khi đó

$$\overline{h(x)} = (x^2 + ax + b)(x^2 + cx + d) \text{ với } a, b, c, d \in \mathbb{Z}_5.$$

Đồng nhất hệ số ta được hệ

$$\begin{cases} a + c = 0 \\ b + ac + d = 1 \\ ad + bc = 1 \\ bd = 1. \end{cases}$$

Dễ kiểm tra được hệ này vô nghiệm. Vì $\deg h(x) = \deg \overline{h(x)}$ nên $h(x)$ bất khả quy trên $\mathbb{Q}$.

Ta có bài toán tự luyện sau đây.

Bài toán 2.1.14. Các đa thức sau là bất khả quy trên $\mathbb{Q}$

(i) $f(x) = 21x^3 - 3x^2 + 2x + 9$

(ii) $g(x) = \frac{3}{7}x^4 - \frac{2}{7}x^2 + \frac{9}{35} + \frac{3}{5}$

(iii) $h(x) = x^5 + 2x + 4$

(iv) $u(x) = x^4 + x + 1$.

Nhận xét 2.1.15. Cho $f(x)$ là đa thức dạng chuẩn với hệ số nguyên. Giả sử tìm được số nguyên tố p sao cho $\deg(f(x)) = \deg \overline{f(x)}$ và trong vành $\mathbb{Z}_p[x]$ ta phân tích được $\overline{f(x)}$ thành tích của các phần tử bất khả quy dạng chuẩn $\overline{f(x)} = f_1^{\#}(x)...f_k^{\#}(x)$. Chúng ta cần tìm phân tích bất khả quy của $f(x)$ trên $\mathbb{Q}$ thông qua phân tích bất khả quy của f(x) trên Z_p. Ta minh họa bằng ví dụ dưới đây.

Ví dụ 2.1.16. Chứng minh $f(x) = x^5 + 5x^4 + 4x^3 + 16x^2 + 8x + 1$ là đa thức khả quy trên $\mathbb{Q}$. Hãy tìm phân tích bất khả quy của $f(x)$.

Lời giải.

Ta có $\overline{f(x)} = x^5 + 2x^4 + x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$

Vì -1 là nghiệm của $\overline{f(x)}$ nên ta phân tích $\overline{f(x)} = (x+1)f_1^{\#}(x)$ với $f_1^{\#}(x) = x^4 + x^3 + x + 1 \in \mathbb{Z}_3[x]$.

Do -1 là nghiệm của $f_1^{\#}(x)$ nên $f_1^{\#}(x) = (x+1)(x^3+1) = (x+1)^2(x^2-x+1)$.

Vì $-1 \equiv 2 \pmod 3$ suy ra $\overline{f(x)} = (x+1)^3(x^2-x+1) = (x+1)^5$

Dễ kiểm tra được $f(x)$ không có nghiệm hữu tỷ. Giả sử $f(x) = g(x).h(x) \in \mathbb{Z}[x]$ và $\deg g(x) = 2, \deg h(x) = 3$. Với $g(x), h(x)$ là bất khả quy

Giả sử $g(x) = x^2 + ax + b$, $h(x) = x^3 + cx^2 + dx + e$.

Đồng nhất hệ số ta thu được

$$a + c = 5, b + ac + d = 4, cb + ad + e = 16, db + ea = 8, be = 1.$$

Mặt khác

$$\overline{g(x)} = (x+1)^2 = x^2 + 2x + 1 \in \mathbb{Z}_3[x], h(x) = (x+1)^3 = x^3 + 1 \in Z_3[x].$$

Suy ra $b \equiv 1, a \equiv 2, e \equiv 1, d \equiv 0, c \equiv 0 \pmod 3$

Từ đây dễ dàng suy ra được $g(x) = x^2 + 5x + 1$ và $h(x) = x^3 + 3x + 1$.

Chúng ta có một số bài toán tương tự để rèn luyện

Bài toán 2.1.17. Chứng minh rằng đa thức $f(x) = x^6 - 8x^4 - 19x^2 + 2$ khả quy trên $\mathbb{Q}$. Hãy tìm phân tích bất khả quy của $f(x)$.

Bài toán 2.1.18. Với các số nguyên a và b, đa thức $f(x) = x^4 + ax^2 + b^2$ là khả quy trên $\mathbb{Z}_p$ với mọi số nguyên tố p.

Bài toán 2.1.19. Với mọi số nguyên dương không chính phương d, đa thức $x^4 + 2(1-d)x^2 + (1+d)^2$ bất khả quy trên $\mathbb{Z}$ nhưng khả quy trên $\mathbb{Z}_p$

Ta tiếp tục xét một số ví dụ khác.

Ví dụ 2.1.20. Chứng minh rằng không tồn tại hai đa thức $p(x)$ và $q(x)$ thuộc $\mathbb{Z}[x]$ với bậc lớn hơn 0 thỏa mãn điều kiện $31x^4 - 25x^3 + 41x^2 - 14x + 11 = p^2(x).q(x)$.

Lời giải.

Đặt $f(x) = 31x^4 - 25x^3 + 41x^2 - 14x + 11$

$\overline{f(x)} = x^4 + x^2 + x + 1 \in \mathbb{Z}_5[x]$. Vì đa thức này không có nghiệm trên $\mathbb{Z}_5$ nên nó không có nhân tử bậc nhất. Giả sử $\overline{f(x)} = (x^2 + ax + b)(x^2 + cx + d)$ với $a, b, c, d \in \mathbb{Z}_5$. Khi đó $\begin{cases} a + c = 0, bd = 1 \\ b + ac + d = 1 \\ ad + bc = 1. \end{cases}$

Từ $bd = 1$ và do vai trò bình đẳng nên ta chỉ cần xét $(b, d) = (1; 1); (2; 3); (4; 4)$.

Ta dễ dàng kiểm tra được hệ trên vô nghiệm hay $f(x)$ bất khả quy trên $\mathbb{Q}$, từ đó dẫn đến không tồn tại $p(x)$ và $q(x)$.

Ví dụ 2.1.21. Với số nguyên $n \geq 0$, đa thức $f(x) = (x^2 + x)^{2^n} + 1$ bất khả quy trên $\mathbb{Z}$.

Lời giải.

$n = 0$ là hiển nhiên. $n \neq 1, \overline{f(x)} \in \mathbb{Z}_2[x]$ ta có

$$(x^2 + x + 1)^{2^n} = ((x^2 + 1)^2 + 1)^{2^{n-1}} = ((x^2 + 1)^{2^2} + 1)^{2^{n-2}} = ...$$

Như vậy, $(x^2 + x + 1)^{2^n} = (x^2 + x)^{2^n} + 1 = \overline{f(x)}$.

Giả sử ta có phân tích $f(x) = g(x).h(x)$ với $g(x), h(x) \in \mathbb{Z}[x]$ và $0 < \deg g(x), \deg h(x) < n$.

Vậy $\overline{f(x)} = \overline{g(x)}.\overline{h(x)}$ trong $\mathbb{Z}_2[x]$. Suy ra

$$\overline{g(x)} = (x^2 + x + 1)^s, \overline{h(x)} = (x^2 + x + 1)^{2^n - s}.$$

Biểu diễn trong $\mathbb{Z}[x]$ ta có $g(x) = (x^2+x+1)^s + 2v(x)$ và $h(x) = (x^2+x+1)^{2^n-s} + 2t(x)$ với $v(x), t(x) \in \mathbb{Z}[x]$.

Với nghiệm phức u của x^2+x+1 từ $(x^2+x)^{2^n}+1 = f(x) = g(x).h(x)$ ta có $(x^2+x)^{2^n}+1 = g(x).h(x)$.

Suy ra $2 = f(u) = g(u).h(u) = 4v(u).t(u)$.

Vì $u^2 = -u-1$ nên $v(u).t(u) = a+bu$ với $a, b \in \mathbb{Z}$

Vậy $a+bu = \frac{1}{2}$, vô lý. Điều giả sử là sai hay $f(x)$ là đa thức bất khả quy.

Tương tự ta có bài toán sau:

Bài toán 2.1.22. Với số nguyên $n \geq 1$ và số nguyên tố p dạng $4m+3$, đa thức $f(x) = (x^2+1)^n + p$ là đa thức bất khả quy trong $\mathbb{Z}[x]$.

2.2 Ứng dụng các vành $\mathbb{Z}[\sqrt{d}], \mathbb{Z}[\sqrt{p}, \sqrt{q}]$ vào giải toán

Khi tìm hiểu, nghiên cứu giải quyết các phương trình dạng Pell: $x^2 - dy^2 = n$ đã giúp chúng tôi để ý đến các mô hình biểu diễn nghiệm của chúng và phát hiện nhiều tính chất thú vị và các ứng dụng của vành $\mathbb{Z}[\sqrt{d}]$ vào giải toán và tương tự với vành $\mathbb{Z}[\sqrt{p}, \sqrt{q}]$.

2.2.1 Cơ sở lý thuyết

Chúng ta đã biết đến $\mathbb{Z}[\sqrt{d}]$ và tự đẳng cấu của nó ở mục 1.2.2, ta bổ sung khái niệm chuẩn qua mệnh đề sau.

Mệnh đề 2.2.1. *Cho $\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} | a, b \in \mathbb{Z}\}, d \neq 1$ và không tồn tại p nguyên tố sao cho $p^2|d$. Khi đó hàm $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}^+$ với $N(a+b\sqrt{d}) = |a-db^2|$ được gọi là chuẩn và thỏa mãn các tính chất sau:*

(i) $N(x) = 0 \Leftrightarrow x = 0$

(ii) $N(xy) = N(x).N(y), \forall x, y \in \mathbb{Z}[\sqrt{d}]$

(iii) x *là khả nghịch* $\Leftrightarrow N(x) = 1$

(iv) Nếu $N(x)$ là số nguyên tố thì x là bất khả quy trong $\mathbb{Z}[\sqrt{d}]$.

Ví dụ 2.2.2. (i) 7 là phần tử bất khả quy trong $\mathbb{Z}[\sqrt{6}]$ mặc dù $N(7)$ không là nguyên tố.

(ii) 2 là bất khả quy nhưng không nguyên tố trong $\mathbb{Z}[\sqrt{5}]$.

Mệnh đề 2.2.3. *Giả thiết p, q là hai số nguyên dương không có nhân tử là số chính phương với $(p, q) = 1$. Khi đó tập*

$$\mathbb{Z}[\sqrt{p}, \sqrt{q}] = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} | a, b, c, d \in \mathbb{Z}\}$$

cùng với phép cộng và phép nhân lập thành một vành giao hoán với đơn vị và các ánh xạ dưới đây

$$\varphi_i : \mathbb{Z}[\sqrt{p}, \sqrt{q}] \to \mathbb{Z}[\sqrt{p}, \sqrt{q}]$$

$$z = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \longmapsto \begin{cases} \varphi_1 = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \\ \varphi_2 = a - b\sqrt{p} + c\sqrt{q} - d\sqrt{pq} \\ \varphi_3 = a + b\sqrt{p} - c\sqrt{q} - d\sqrt{pq} \\ \varphi_4 = a - b\sqrt{p} - c\sqrt{q} + d\sqrt{pq} \end{cases}$$

là những tự đẳng cấu.

Với $z \in \mathbb{Z}[\sqrt{p}, \sqrt{q}]$ thì $N(z) = \varphi_1(z).\varphi_2(z).\varphi_3(z).\varphi_4(z)$ và ta cũng có tính chất:

$$N(z_1 z_2) = N(z_1).N(z_2), \forall z_1, z_2 \in \mathbb{Z}[\sqrt{p}, \sqrt{q}].$$

2.2.2 Ứng dụng trong giải toán

Với các bài toán số học, đặc biệt là các phương trình nghiệm nguyên có cấu trúc tương tự như phương trình Pell, chúng ta có thể sử dụng các nhóm vành đã nêu cùng với chuẩn và tự đẳng cấu của chúng để tìm ra lời giải hiệu quả cho một số bài toán tồn tại hay bài toán chứng minh, tính toán.

Ta sẽ tìm hiểu cụ thể thông qua một số ví dụ sau.

Ví dụ 2.2.4. Với số nguyên dương n, giả sử các số $a_1, b_1, ..., a_n, b_n, a, b \in \mathbb{Z}$ thỏa mãn quan hệ $\prod_{i=1}^{n}(a_i + b_i\sqrt{5}) = a + b\sqrt{5}$

Chứng minh rằng

(i) $\prod_{i=1}^{n}(a_i^2 - 5b_i^2) = a^2 - 5b^2$

(ii) Giả sử $(9 + 4\sqrt{5})^n = a_n + b_n\sqrt{5}$. Chứng minh $a_n^2 - 5b_n^2 = 1$. Từ đó suy ra phương trình $x^2 - 5y^2 = 4$ có vô hạn nghiệm nguyên dương x, y.

Lời giải.

(i) Xét vành giao hoán $\mathbb{Z}[5] = \{r + s\sqrt{5}, |r, s \in \mathbb{Z}\}$.

Đồng cấu $f : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]; r + s\sqrt{5} \mapsto r - s\sqrt{5}$ là một đẳng cấu.

Tác động f lên hai vế

$$f\Big(\prod_{n=1}^{n}(a_i + b_i\sqrt{5}\Big) = f(a + b\sqrt{5})$$

hay

$$\prod_{i=1}^{n}(a_i - b_i\sqrt{5}) = a - b\sqrt{5}.$$

Nhân vế theo vế với giả thiết ta được

$$\prod_{i=1}^{n}(a_i^2 - b_i^2) = a^2 - 5b^2$$

(ii) Ta có $a_n^2 - 5b_n^2 = (9 + 4\sqrt{5})^n(9 - 4\sqrt{5})^n = 1$ (theo (i)). Đặt

$$x_n + y_n\sqrt{5} = (a_n + b_n\sqrt{5})(3 + \sqrt{5}) = 3a_n + 5b_n + (a_n + 3b_n)\sqrt{5}.$$

Khi đó $x_n^2 - 5y_n^2 = (a_n^2 - 5b_n^2)(3^2 - 5.1^2) = 4, \forall n$. Như vậy phương trình $x^2 - 5y^2 = 4$ có vô hạn nghiệm nguyên x, y. Mặt khác, khi x, y là nghiệm thì $\pm x, \pm y$ cũng là nghiệm.

Do vậy phương trình $x^2 - 5y^2 = 4$ có vô hạn nghiệm nguyên dương x, y.

Chúng ta tiếp tục nghiên cứu thêm một ví dụ nữa để hiểu rõ hơn phương pháp này.

Ví dụ 2.2.5. Chứng minh rằng luôn luôn tồn tại hai số nguyên x và y để

$$19^n = x^2 - 6y^2 \text{với} \begin{cases} x \text{ lẻ và } y \text{ lẻ khi } n \text{ lẻ} \\ x \text{ lẻ và } y \text{ chẵn khi } n \text{ chẵn.} \end{cases}$$

Lời giải.

Xét vành giao hoán $\mathbb{Z}[\sqrt{6}] = \{r + s\sqrt{6}|r, s \in \mathbb{Z}\}$.

Đồng cấu $f : \mathbb{Z}[\sqrt{6}] \to \mathbb{Z}[\sqrt{6}]; r + s\sqrt{6} \mapsto r - s\sqrt{6}$ là một đẳng cấu.

Do vậy mà khi $(a + b\sqrt{6})(c + d\sqrt{6}) = u + v\sqrt{6}$ thì tác động f lên hai vế ta được

$$(a - b\sqrt{6})(c - d\sqrt{6}) = u - v\sqrt{6}.$$

Sử dụng kết quả này với $z = a + b\sqrt{6}$ và đặt $N(z) = a^2 - 6b^2$ ta có ngay $N(z_1z_2) = N(z_1).N(z_2)$.

Với $n = 1$ ta có $19 = 5^2 - 6.1^2$ và $19^2 = 31^2 - 6.10^2$.

Giả sử số nguyên $n \geq 1$ và hai số nguyên a, b để $19^n = a^2 - 6b^2$ trong đó a, b đều lẻ khi n lẻ, còn a lẻ và b chẵn khi n chẵn với $n + 1$, ta xét

(1) Nếu n lẻ thì có a lẻ và b lẻ để $a^2 - 6b^2 = 19^n$. Khi đó $n + 1$ là số chẵn và $19^{n+1} = (5a + 6b)^2 - 6(a + 5b)^2$ với $5a + 6b$ lẻ và $a + 5b$ chẵn.

(2) Nếu n chẵn thì có a lẻ và b chẵn để $a^2 - 6b^2 = 19^n$. Khi đó $n + 1$ là số lẻ và $19^{n+1} = (5a + 6b)^2 - 6(a + 5b)^2$ với $5a + 6b$ lẻ và $a + 5b$ lẻ.

Vậy ta có điều phải chứng minh.

Bài toán 2.2.6. Chứng minh rằng phương trình $x^3 = y^2 - 6$ không có nghiệm nguyên.

Bài toán 2.2.7. Có hay không một số nguyên dương n thỏa mãn hệ thức

$$(\sqrt{2023} - \sqrt{2022})^{2024} = \sqrt{n} - \sqrt{n-1}.$$

Bài toán 2.2.8. Tìm các số $x, y, z, t \in \mathbb{Z}$ thỏa mãn phương trình

$$(x + y\sqrt{3})^4 + (z + t\sqrt{3})^4 = 20 + 12\sqrt{3}.$$

Bài toán 2.2.9. Cho hai số nguyên dương a và b thỏa mãn $(a, b) = 1$. Hai dãy số nguyên (a_n) và (b_n) được xác định qua $a_n + b_n\sqrt{2} = (a + b\sqrt{2})^2 n$ với mỗi số nguyên $n \geq 0$. Xác định tất cả những số nguyên tố p để có số nguyên dương $n \neq p$ sao cho $b_n \equiv 0 \pmod{p}$.

Bài toán 2.2.10. Giải phương trình nghiệm nguyên $x^2 - 5y^2 = 1$.

Bài toán 2.2.11. Chứng minh rằng số $A = \dfrac{(17 + 12\sqrt{2})^n - (17 - 12\sqrt{2})^n}{4\sqrt{2}}$ là một số nguyên, nhưng không là số chính phương.

Các bài toán tiếp theo sử dụng vành $\mathbb{Z}[\sqrt{p}, \sqrt{q}]$ và các tự đẳng cấu của nó để giải quyết.

Ví dụ 2.2.12. Giả sử các dãy số $(a_n), (b_n), (c_n), (d_n)$ xác định như sau

$$\begin{cases} a_1 = 1, b_1 = 1, c_1 = 1, d_1 = 0 \\ a_{n+1} = a_n + 2b_n + 5c_n \\ b_{n+1} = a_n + b_n + 5d_n \\ c_{n+1} = a_n + c_n + 2d_n \\ d_{n+1} = b_n + c_n + d_n. \end{cases}$$

Khi đó với mỗi số nguyên dương n ta có:

$$(1+\sqrt{2}+\sqrt{5})^n = a_n + b_n\sqrt{2} + c_n\sqrt{5} + d_n\sqrt{10}$$

và $a_n^2 - 10d_n^2$ chia hết cho 2^{n-1}. Tìm $\lim\limits_{n\to+\infty} \dfrac{a_n}{d_n}$.

Lời giải.

Với mỗi số nguyên dương n ta biểu diễn

$$(1+\sqrt{2}+\sqrt{5})^n = A_n + B_n\sqrt{2} + C_n\sqrt{5} + D_n\sqrt{10},$$

trong đó $A_n, B_n, C_n, D_n \in \mathbb{N}$.

Hiển nhiên

$$A_1 = 1 = a_1, B_1 = 1 = b_1, C_1 = 1 = c_1, D_1 = 0 = d_1,$$

từ

$$(1+\sqrt{2}+\sqrt{5})^{n+1} = A_{n+1} + B_{n+1}\sqrt{2} + C_{n+1}\sqrt{5} + D_{n+1}\sqrt{10}$$

ta suy ra

$$A_{n+1} = a_{n+1}, B_{n+1} = b_{n+1}, C_{n+1} = c_{n+1}, D_{n+1} = d_{n+1}.$$

Sử dụng các tự đẳng cấu của vành $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$ cho đồng nhất thức

$$(1+\sqrt{2}+\sqrt{5})^n = a_n + b_n\sqrt{2} + c_n\sqrt{5} + d_n\sqrt{10}$$

ta nhận được

$$\begin{aligned}
(1-\sqrt{2}+\sqrt{5})^n &= a_n - b_n\sqrt{2} + c_n\sqrt{5} - d_n\sqrt{10} \\
(1+\sqrt{2}-\sqrt{5})^n &= a_n + b_n\sqrt{2} - c_n\sqrt{5} - d_n\sqrt{10} \\
(1-\sqrt{2}-\sqrt{5})^n &= a_n - b_n\sqrt{2} - c_n\sqrt{5} + d_n\sqrt{10}.
\end{aligned}$$

Từ đó suy ra được

$$4a_n^2 - 40d_n^2 = 2^n[(2+\sqrt{5})^n + (2-\sqrt{5})^n + (-1+\sqrt{2})^n + (-1-\sqrt{2})^n]$$

hay

$$a_n^2 - 10d_n^2 = 2^{n-1}[(2^n + (-1)^n)C_n^0 + ... + (2^{n-2k}.5^k + (-1)^n.2^k).C_n^{2k} + ...]$$

chia hết cho 2^{n-1} và $\lim\limits_{n\to+\infty} \dfrac{a_n}{d_n} = \sqrt{10}$.

Ví dụ 2.2.13. Chứng minh rằng với mọi số nguyên dương n luôn có các số nguyên dương x, y, z, t thỏa mãn các điều kiện sau.

(i) x, y, z là những số lẻ, còn t là số chẵn và

$$x^2 + 9y^2 - 6z^2 - 12t^2 = 3748.$$

(ii) x, y, z, t là những số chẵn và

$$3748^n = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 4 & 8 & 1 & 3 \\ 9 & 12 & 1 & 2 \\ 24 & 9 & 4 & 1 \end{vmatrix}^n = x^2 + 9y^2 - 6z^2 - 12t^2.$$

Lời giải.

$x_1 = 1, y_1 = 2, z_1 = 3, t_1 = 4$ thỏa mãn điều kiện

$$\begin{cases} N(x_1, y_1\sqrt{2}, z_1\sqrt{3}, t_1\sqrt{6}) = 3748 \\ x = |x_1^2 - 2y_1^2|, y = |z_1^2 - 2t_1^2| \\ z = |x_1z_1 - 2y_1t_1|, t = |x_1t_1 - y_1z_1| \\ x, y, z, t \text{ là những số tự nhiên} \\ x^2 + 9y^2 - 6z^2 - 12t^2 = 3748. \end{cases}$$

Bốn dãy số $(x_n), (y_n), (z_n)$ và (t_n) được xác định bởi công thức:

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \\ t_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \text{ và } \begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 4 & 9 & 24 \\ 2 & 1 & 12 & 9 \\ 3 & 8 & 1 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \\ t_n \end{pmatrix}.$$

Chú ý rằng với $u_{n+1} = x_{n+1} + y_{n+1}\sqrt{2} + z_{n+1}\sqrt{3} + t_{n+1}\sqrt{6}$ và $u_n = x_n + y_n\sqrt{2} + z_n\sqrt{3} + t_n\sqrt{6}$, ta có $N(u_{n+1}) = 3748N(u_n)$.

Các số tự nhiên $x = |x_n^2 - 2y_n^2|, y = |z_n^2 - 2t_n^2|, z = |x_nz_n - 2y_nt_n|$ và $t = |x_nt_n - y_nz_n|$ thỏa mãn $x^2 + 9y^2 - 6z^2 - 12t^2 = 3748^n$.

Như vậy khi $x_1 = 1, y_1 = 2, z_1 = 3.t_1 = 4$ ta có x, y, z là những số nguyên dương lẻ, còn t là số nguyên dương chẵn thỏa mãn $x^2 + 9y^2 - 6z^2 - 12t^2 = 3748$ thỏa mãn điều phải chứng minh ở (i).

Khi $n > 1$ ta thấy x_n, y_n, z_n, t_n là những số nguyên dương chẵn thỏa mãn

$$3748^n = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 4 & 8 & 1 & 3 \\ 9 & 12 & 1 & 2 \\ 24 & 9 & 4 & 1 \end{vmatrix}^n = x^2 + 9y^2 - 6z^2 - 12t^2,$$

ta có điều phải chứng minh ở (ii).

Tương tự như vậy, chúng ta có thể giải quyết các bài toán sau.

Bài toán 2.2.14. Với mọi số nguyên dương n ta biểu diễn

$$(1+\sqrt{2}+\sqrt{3})^n = a_n + b_n\sqrt{2} + c_n\sqrt{3} + d_n\sqrt{6} \text{ với } a_n, b_n, c_n, d_n \in \mathbb{N}.$$

Tìm $\lim\limits_{n\to\infty} \dfrac{b_n}{a_n}$; $\lim\limits_{n\to\infty} \dfrac{d_n}{a_n}$.

Bài toán 2.2.15. Với số nguyên dương n, chứng minh tổng sau chia hết cho 4

$$S = (1+\sqrt{2}+\sqrt{3})^n + (1-\sqrt{2}+\sqrt{3})^n + (1+\sqrt{2}-\sqrt{3})^n + (1-\sqrt{2}-\sqrt{3})^n.$$

2.3 Ứng dụng vành số nguyên Gauss, vành $\mathbb{Z}[\sqrt{-d}]$ vào giải toán

2.3.1 Ứng dụng vành số nguyên Gauss vào giải toán.

Ở các mục 1.1.2, 1.3.2, 1.4.7, 1.4.10 chúng ta đã được giới thiệu sơ lược về vành số nguyên Gauss $\mathbb{Z}[i]$ cùng một số tính chất, với $z = a+bi \in \mathbb{Z}[i]$ và chuẩn $N(z) = a^2 + b^2$, ta bổ sung một số tính chất sau.

Mệnh đề 2.3.1. *Cho $x, y \in \mathbb{Z}[i]$. Khi đó:*

(i) $N(x) = 0 \Leftrightarrow x = 0$

(ii) $N(x) = 1 \Leftrightarrow x \in \{\pm 1; \pm i\}$ *là các phần tử khả nghịch*

(iii) $N(xy) = N(x).N(y)$

(iv) $N(x)$ *là số chẵn* $\Leftrightarrow x$ *là bội của* $1+i$.

Mệnh đề 2.3.2. *Cho $x, y \in \mathbb{Z}[i]$ với $y \neq 0$, tồn tại các số nguyên Gauss z, t sao cho $x = yz + t$ và $N(t) < N(y)$.*

Định lí 2.3.3. *(Định lý cơ bản của số học cho vành Gauss).*

Mọi số nguyên Gauss $\alpha \neq 0$ đều có thể được viết dưới dạng

$$\alpha = \epsilon.\gamma_1.\gamma_2.\ldots.\gamma_n$$

trong đó ϵ là một phần tử khả nghịch và $\alpha_1, ..., \alpha_n$ là các phần tử bất khả quy. Biểu diễn này là duy nhất theo cách hiểu ở mục 1.4.4.

Mệnh đề 2.3.4. *Cho $\alpha \in \mathbb{Z}[i]$ sao cho $N(\alpha)$ là một số nguyên tố. Thế thì α là một phần tử bất khả quy.*

Định lí 2.3.5. *Các phần tử bất khả quy của $\mathbb{Z}[i]$ gồm*

(i) $1+i$ *và các phần tử liên kết của nó, nghĩa là* $\{1-i, -1+i, -1-1\}$.

(ii) Các số nguyên tố $p \equiv 3 \pmod 4$ *và các phần tử liên kết của nó, nghĩa là* $\{\pm p; \pm pi\}$.

(iii) Hai phần tử bất khả quy $a+bi, a-bi$ *trong phân tích ra tích các nhân tử bất khả quy 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* $a^2 + b^2 = p$.

Định nghĩa 2.3.6. Số nguyên Gauss γ được gọi là ước chung của α và β nếu γ đều là ước của α và β. Nếu $N(\gamma)$ lớn nhất thì γ được gọi là ước chung lớn nhất của α và β.

Cho $\gamma = (a, b)$. Nếu $\gamma \in \{\pm 1; \pm i\}$ thì α nguyên tố cùng nhau với β.

Định lí 2.3.7. *Cho $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ và số nguyên dương $k \geq 2$. Nếu α, β nguyên tố với nhau và $\alpha\beta = \gamma^k$ thì tồn tại $\epsilon_1, \epsilon_2, \gamma_1, \gamma_2 \in \mathbb{Z}[i]$ sao cho ϵ_1, ϵ_2 khả nghịch và $\alpha = \epsilon_1.\gamma_1^k, \beta = \epsilon_2.\alpha_2^k$.*

Chúng ta cùng tìm hiểu ứng dụng của vành Gauss qua một số ví dụ sau.

Trước hết, định lý Fermat về tổng hai số chính phương có thể được mở rộng như sau.

Ví dụ 2.3.8. Cho một số nguyên dương n. Số nghiệm nguyên của phương trình $x^2 + y^2 = n$ bằng 4 lần hiệu số các ước $\equiv 1 \pmod 4$ của n trừ cho số các ước $\equiv 3 \pmod 4$ của n

Lời giải.

Theo định lý cơ bản của số học cho vành Gauss, ta có thể viết:

$$\begin{aligned} n &= 2^m.p_1^{r_1}.\ldots.p_k^{r_k}.\gamma_1^{s_1}.\overline{\gamma_1}^{s_1}.\ldots.\gamma_h^{s_h}.\overline{\gamma_h}^{s_h} \\ &= (-i)^m.(1+i)^{2m}.p_1^{r_1}.\ldots.p_k^{r_k}.\gamma_1^{s_1}.\overline{\gamma_1}^{s_1}.\ldots.\gamma_h^{s_h}.\overline{\gamma_h}^{s_h} \end{aligned}$$

trong đó p_i, γ_i là các phần tử bất khả quy của $\mathbb{Z}[i]$ với $p_i = \overline{p_i}$ (như vậy p_i là các số nguyên tố $\equiv 3 \pmod 4$ và γ_i có dạng $a + b_i$ 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 quy trong $\mathbb{Z}[i]$ ta suy ra $x + yi$ là một phần tử liên kết của

$$(1+i)^m = p_1^{\frac{r_1}{2}} \ldots . p_k^{\frac{r_k}{2}} . \gamma_1^{t_1} . \overline{\gamma_1}^{s_1 - t_1} \ldots . \overline{\gamma_h}^{s_h - t_h}$$

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

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

Chú ý rằng nhân tử 4 xuất hiện ở công thức trên là do việc biểu diễn 1 ở trên sai khác $x + yi$ bởi 1 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 quy trong $\mathbb{Z}[i]$

$$d = p_1^{u_1} \ldots . p_k^{u_k} . \gamma_1^{u_1} . \overline{\gamma_1}^{v_1} \ldots . \gamma_h^{u_h} . \overline{\gamma_h}^{v_h}$$

với $0 \leq u_i \leq r_i, 0 \leq v_j \leq s_j$. Nhưng $p_i \equiv 3 \pmod 4$ với mọi i và $\gamma_i . \overline{\gamma_i} \equiv 1 \pmod 4$ với mọi j nên $d \equiv 1 \pmod 4 \Leftrightarrow u_1 + u_2 + ... + u_k \equiv 1 \pmod 2$

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

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

Vậy ta có điều phải chứng minh.

Chúng ta cùng tìm hiệu sự phân tích tổng hai bình phương qua các ví dụ cụ thể với công cụ chuẩn như sau: một số nguyên dương $m = x^2 + y^2$ là tổng của hai bình phương chính là chuẩn của một số nguyên Gauss, khi đó $m = N(x + iy)$.

Ví dụ 2.3.9. Phân tích các số nguyên dương sau thành tổng hai bình phương

(i) 65 (ii) 100 (iii) 19890

Lời giải.

Các ví dụ (i),(ii) với trường hợp số nhỏ, ta hoàn toàn có thể giải quyết như một bài toán số học thông thường, tuy nhiên với (iii) thì khác, chúng ta cùng theo dõi cách giải quyết sau đây.

(i) Ta có $65 = 5.13 = x^2 + y^2 = N(\alpha)$ với $\alpha = x + i.y$;

$5 = N(2 \pm i)$ và $13 = N(3 \pm 2i)$, $\alpha = \mu(2 \pm i)(3 \pm 2i)$

Với 4 tổ hợp dấu cộng trừ μ là khả nghịch nên có tổng cộng 16 trường hợp xảy ra.

Chúng ta sẽ xét 2 trường hợp đại diện sau đó đổi dấu và hoán vị.

$$\alpha_1 = (2+i)(3+2i) = 4 + 7i$$
$$\alpha_2 = (2+i)(3-2i) = 8 - i$$
$$\text{hay } 65 = 7^2 + 4^2 = 8^2 + 1^2.$$

(ii) Tương tự ta có

$$100 = 2^2.5^2 = N(\alpha) \Rightarrow \alpha = \mu.(1+i)^2(2 \pm i).(2 \pm i)$$

Chúng ta có 2 sự lựa chọn

$$\begin{aligned} 100 &= N((1+i)^2(2+i)^2) = N(-8+6i) = 8^2 + 6^2 \\ &= N((1+i)^2(2+i)(2-i)) = N(10i) = 10^2 + 0^2. \end{aligned}$$

Đổi dấu và hoán vị chúng ta có 12 trường hợp có thể xảy ra.

(iii) Ta có $19890 = 2.3^2.5.13.17 = N(3(1+i)(2 \pm i)(3 \pm 2i)(4 \pm i))$.

Chúng ta có 4 sự lựa chọn

$$\begin{aligned} 19890 &= N(3(1+i)(2+i)(3+2i)(4+i)) = N(-69+123i) = 123^2 + 69^2 \\ &= N(3(1+i)(2+i)(3+2i)(4-i)) = N(-3+141i) = 141^2 + 3^2 \\ &= N(3(1+i)(2+i)(3-2i)(4+i)) = N(87+111i) = 111^2 + 87^2 \\ &= N(3(1+i)(2+i)(3-2i)(4-i)) = N(129-57i) = 129^2 + 57^2. \end{aligned}$$

Đổi dấu và hoán vị chúng ta có 32 trường hợp tất cả.

Ví dụ 2.3.10. Giải phương trình nghiệm nguyên $x^2 + y^2 = z^2$.

Lời giải. Hiển nhiên ở đây ta chỉ xét bộ ba Pitago nguyên thủy, tức là hai số bất kỳ nguyên tố cùng nhau và z là số lẻ. Khi đó:

$$(x+yi)(x-yi) = z^2.$$

Ta sẽ chứng minh $(x+yi, x-yi) = 1$. Thật vậy:

Gọi α là một ước nguyên tố chung của $x+yi$ và $x-yi$

$$\Rightarrow \begin{cases} \alpha | 2x \\ \alpha | 2yi \end{cases} \quad \text{vì } i \text{ khả nghịch nên } \alpha | 2y.$$

Nếu $\alpha | x$ thì suy ra $\alpha | y$ mà $(x,y) = 1$ nên tồn tại u, v sao cho $ux + vy = 1$. Kéo theo $\alpha | 1$ (vô lý). Vậy $x \not\vdots \alpha \Rightarrow \alpha | 2 = -i(i+1)^2$ và $1+i$ là số nguyên tố Gauss nên $\alpha = 1+i$.

Vì $\alpha^2 | x^2 + y^2 = z^2$ nên $4 | N(\alpha^2) | N(z^2) = z^4 \Rightarrow z$ chẵn, điều này mâu thuẫn với giả thiết.

Lúc này $x+yi, x-yi$ sẽ liên kết với một bình phương của số nguyên Gauss theo Định lý 2.3.3.

Chú ý rằng trong 4 phần tử khả nghịch $\pm 1, \pm i$ thì $-1 = i^2$ cũng là một bình phương. Xét số nguyên Gauss $m+ni$ sao cho

$$\begin{aligned} x + yi &= (m+ni)^2 \\ \text{hoặc } x + yi &= i(m+ni)^2 \\ \text{tương đương với } x + yi &= m^2 - n^2 + 2mni \\ \text{hoặc } x + yi &= -2mn + (m^2 - n^2)i \end{aligned}$$

Như vậy ta có bộ nghiệm

$$\begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases} \quad \text{hoặc} \quad \begin{cases} x = -2mn \\ y = m^2 - n^2 \\ z = m^2 + n^2. \end{cases}$$

Ở đây m, n khác tính chẵn lẻ và nguyên tố cùng nhau.

Kỹ thuật tương tự cũng giúp chúng ta giải quyết một kết quả đáng chú ý sau đây.

Ví dụ 2.3.11. Chứng minh rằng số nguyên tố lẻ p có thể biểu diễn được dưới dạng

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

với $x, y \in \mathbb{Z}$ khi và chỉ khi p đồng dư với 1 modulo 4.

Lời giải. Giả sử tồn tại $x, y \in \mathbb{Z}$ sao cho $x^2 + y^2 = p$. Khi đó, ta thấy ngay rằng $0 < |x|, |y| < p$ cho nên cả x và y đều là các số nguyên nguyên tố cùng nhau với p. Khi đó, tồn tại $z \in \mathbb{Z}$ sao cho $yz \equiv 1 \pmod{p}$. Ta có $(xz)^2 + 1 \equiv 0 \pmod{p}$ vì thế -1 là lớp thặng dư chính phương modulo p. Mà theo tính toán thặng dư chính phương thì ta có

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

cho nên -1 là thặng dư chính phương modulo p khi và chỉ khi $p \equiv 1 \pmod{4}$. Vì vậy, nếu $x, y \in \mathbb{Z}$ sao cho $x^2 + y^2 = p$ thì -1 là thặng dư chính phương modulo p và vì thế ta có $p \equiv 1 \pmod{4}$.

Ngược lại, giả sử $p \equiv 1 \pmod{4}$ ta sẽ chứng minh tồn tại $x, y \in \mathbb{Z}$ sao cho $x^2 + y^2 = p$. Vì -1 là thặng dư chính phương modulo p, tồn tại $x \in \mathbb{Z}$ sao cho $x^2 + 1$ là bội của p. Nếu cần thiết ta có thể thay x bằng $x + p$ cho nên ta có thể giả thiết rằng x là số chẵn.

Ý chính của phần còn lại của chứng minh là xét phân tích

$$x^2 + 1 = (x + i)(x - i)$$

trong các vành số nguyên Gauss.

Ta nhận xét rằng nếu x là số chẵn thì $x + i$ và $x - i$ là nguyên tố cùng nhau. Thật vậy, $2i = (x + i) - (x - i)$ cho nên 2 thuộc về iđêan sinh bởi $x + i$ và $x - i$. Do x là số chẵn cho nên i cũng thuộc về iđêan sinh bởi $x + i$ và $x - i$ vì thể iđêan này là toàn bộ vành $\mathbb{Z}[i]$ các số nguyên Gauss.

Ta chọn một ước chung lớn nhất của p và $x + i$ và ký hiệu là $m + in$. Khi đó $m - in$ là một ước chung lơn nhất của p và $x - i$. Ta biết rằng $p|(x + i)(x - i)$ và $x + i$ và $x - i$ là hai số nguyên Gauss nguyên tố cùng nhau cho nên

$$p = (m + in)(m - in)\alpha \text{ với } \alpha \in \mathbb{Z}[i]^\times$$

là một số nguyên Gauss khả nghịch.

Vì $Z[i]^\times = \{\pm 1, \pm i\}$ và cả p và $(m + in)(m - in) = m^2 + n^2$ là số nguyên dương cho nên ta có kết luận $p = m^2 + n^2$ như mong muốn.

Ví dụ 2.3.12. Giải phương trình nghiệm nguyên $y^2 = x^3 - 1$.

Lời giải.

Giả sử (x, y) là nghiệm nguyên của phương trình đã nêu, dễ dàng suy ra được x lẻ và y chẵn. Viết lại phương trình dưới dạng:

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

Theo chứng minh ở Ví dụ 2.3.10 thì $y+i$ và $y-i$ nguyên tố cùng nhau. Như vậy $y + i, y - i$ là lập phương của các phần tử của $\mathbb{Z}[i]$. Do đó tồn tại các số nguyên a, b sao cho $y + i = (a + bi)^3$.

So sánh phần thực và áo ta được: $1 = b(3a^2 - b^2)$.

Giải ra ta được $(a, b) = (0; -1)$. Từ đây suy ra $y = 0$ và $x = 1$.

Nhận xét 2.3.13. Có sự tương tự về mặt phương pháp trong việc giải quyết hai ví dụ 2.3.35 và 2.3.12.

Ta xét bài toán tương tự sau.

Bài toán 2.3.14. Tìm tất cả các nghiệm nguyên của phương trình:

$$y^2 = x^3 - 4.$$

Ví dụ 2.3.15. Với mọi $n \geq 2$, chứng minh rằng:

Phương trình $x^n - y^2 = 1$ chỉ có nghiệm $(x, y) = (1; 0)$.

Lời giải.

Chỉ cần xét $n = p$ là số nguyên tố. Hơn nữa, $p = 2$ bài toán là tầm thường nên ta sẽ giả sử p lẻ. Bằng cách xét theo môđun 4, dễ thấy nếu (x, y) là một nghiệm thì x lẻ và y chẵn. Viết phương trình dưới dạng $x^p = (y - i)(y + i)$ ta suy ra $y + i = (a + bi)^p$ với a, b là các số nguyên nào đó. Từ đẳng thức này ta dễ dàng chứng minh được $b = \pm 1$ và

$$\sum_{k=0}^{\frac{p-1}{2}} C_p^{2k}(-a^2)^k = \pm 1.$$

Lại chú ý rằng vì $b = \pm 1$ nên $x = a^2 + 1$ và do đó a chẵn. Nếu $a = 0$ thì $(x, y) = (1, 0)$.

Ta giả sử $a \neq 0$. Khi đó vế trái của đẳng thức trên $\equiv 1 \pmod 4$ nên vế phải của đẳng thức trên bằng 1 và có thể viết lại một cách tương đương dưới dạng

$$T = \sum_{k=1}^{\frac{p-1}{2}} (-1)^k . \frac{C_p^{2k}}{C_p^2} . a^{2k-2} = 1.$$

Theo công thức Kummer ta có $v_2(T) > 0$ mâu thuẫn với $v_2(1) = 0$.

Ta kết thúc mục này bằng một số bài tập tự luyện sau đây.

Bài toán 2.3.16. Cho p là một số nguyên tố. Hãy xác định phần dư của $\prod_{n=1}^{p-1}(n^2+1)$ khi chia cho p.

Bài toán 2.3.17. Cho một số nguyên dương n. Chứng minh rằng n có thể biểu diễn được dưới dạng của hai số chính phương khi và chỉ khi trong phân tích ra thừa số nguyên tố của n, các ước nguyên tố $\equiv 3$ đều có lũy thừa chẵn.

Bài toán 2.3.18. Cho a, b là hai số nguyên tố cùng nhau. Chứng minh rằng mọi ước (nguyên dương) của a^2+b^2 đều có dạng c^2+d^2 với c, d là các số nguyên tố cùng nhau.

Bài toán 2.3.19. Chứng minh rằng phương trình $x^5 - y^2 = 1$ chỉ có nghiệm nguyên duy nhất $(x, y) = (1, 0)$.

Bài toán 2.3.20. Chứng minh rằng phương trình $x^4 - y^4 = z^2$ không có nghiệm nguyên khác 0.

Bài toán 2.3.21. Chứng minh rằng tất cả các nghiệm nguyên của phương trình $a^2 + b^2 = c^3$ với $(a, b) = 1$ là $a = m^3 - 3mn^2, b = 3m^2n - n^3, c = m^2 + n^2$ với $(m, n) = 1$ và m, n khác tính chẵn lẻ.

Bài toán 2.3.22. Với p là số nguyên tố lẻ, khi đó tồn tại số nguyên x, y sao cho $x^2 + y^2 = p$ khi và chỉ khi $p \equiv 1 \pmod 4$.

Bài toán 2.3.23. Phân tích số nguyên dương $n = p_1^{m_1}.p_2^{m_2}.\ldots.p_k^{m_k}$ với $p_1, p_2, ..., p_k$ là các số nguyên tố phân biệt. Tồn tại $a, b \in \mathbb{N}$ sao cho $n = a^2 + b^2$ khi và chỉ khi $p_i \equiv 3 \pmod 4$. Chứng minh rằng khi đó n chẵn.

Bài toán 2.3.24. Giả sử x, y, z là các số tự nhiên thỏa mãn $xy = z^2+1$. Chứng minh rằng tồn tại các số nguyên a, b, c, d sao cho $x = a^2 + b^2, y = c^2 + d^2$ và $z = ac + bd$.

Bài toán 2.3.25. n là số tự nhiên > 1. Tìm (x, y, z) nguyên thỏa mãn $(x, y) = 1$ và $x^2 + y^2 = z^n$.

2.3.2 Ứng dụng vành $\mathbb{Z}[\sqrt{-d}]$ vào giải toán

Ở mục 1.2.2 chúng ta đã biết đến $\mathbb{Z}[\sqrt{-d}]$ và các tự đẳng cấu của nó, ta bổ sung khái niệm chuẩn bằng một mệnh đề sau.

Mệnh đề 2.3.26. *Cho $\mathbb{Z}[\sqrt{-d}] = \{a + ib\sqrt{d} | a, b \in \mathbb{Z}\} d \neq 1$ và không tồn tại p nguyên tố sao cho $p^2|d$. Khi đó hàm $N : \mathbb{Z}[\sqrt{-d}] \to \mathbb{Z}^+$ với $N(a + bi\sqrt{d}) = a^2 + db^2$ được gọi là chuẩn và thỏa mãn các tính chất sau.*

(i) $N(x) = 0 \Leftrightarrow x = 0$.

(ii) $N(xy) = N(x)N(y), \forall x, y \in \mathbb{Z}[\sqrt{-d}]$.

(iii) x *là khả nghịch* $\Leftrightarrow N(x) = 1$.

(iv) Có duy nhất hai phần tử khả nghịch là 1 và -1.

Ví dụ 2.3.27. (i) Phần tử $1 + 3\sqrt{5}$ là bất khả quy nhưng không là nguyên tố trong $\mathbb{Z}[\sqrt{-5}]$.

(ii) Chỉ có $\mathbb{Z}[\sqrt{-1}]$ và $\mathbb{Z}[\sqrt{-2}]$ là miền phân tích nhân tử duy nhất.

Cũng như quá trình tìm hiểu phương trình Pell, việc nghiên cứu và vận dụng lớp vành số này xuất phát từ quá trình tìm hiểu phương trình Mordell $y^2 = x^3 + k$, ta nhận thấy rằng với $-k$ là số có ước chính phương hoặc cả k và $-k$ là số không chính phương đều là những thử thách khó khăn.

Ví dụ mở đầu sau đây sẽ cho thấy sự cần thiết của việc xây dựng vành $\mathbb{Z}[\sqrt{-d}]$, ý tưởng giải quyết cũng tương tự như Ví dụ 2.2.5.

Ví dụ 2.3.28. Chứng minh rằng với bất kỳ số nguyên $n \geq 3$ đều tồn tại hai số nguyên lẻ x và y để $2^n = 7x^2 + y^2$.

Lời giải.

Xét vành giao hoán $\mathbb{Z}[\sqrt{-7}] = \{r + is\sqrt{7} | r, s \in \mathbb{Z}\}$.

Chuẩn của $z = r + is\sqrt{7}$ là $N(z) = r^2 + 7s^2 = (r + is\sqrt{7})(r - is\sqrt{7})$.

Ta sẽ quy nạp để chỉ ra x, y.

Với $n = 3$ ta có $2^3 = 1^2 + 7.1^2$.

Giả sử đã có hai số nguyên lẻ x, y để $y^2 + 7x^2 = 2^n$ với số nguyên $n \geq 3$. Với số nguyên $n+1$ ta xét

$$z_1 = (y + ix\sqrt{7})(1 + i\sqrt{7}) = (y - 7x) + i(x + y)\sqrt{7}$$
$$z_2 = (y + ix\sqrt{7})(1 - i\sqrt{7}) = (y + 7x) + i(x - y)\sqrt{7}.$$

Vì x, y lẻ nên $x = 2k + 1, y = 2h + 1$. Khi đó trong hai số $x + y$ và $y - x$ chỉ có đúng một số chia hết cho 4.

Nếu $x + y$ chia hết cho 4 thì $\dfrac{y - x}{2}$ là số nguyên lẻ.

Khi đó $z_3 = (\dfrac{y - x}{2} + 4x) + i.\dfrac{x - y}{2}.\sqrt{7}$ với

$$N(z_3) = \frac{N(y + ix\sqrt{7}).N(1 - i\sqrt{7})}{4} = 2^n.2 = 2^{n+1}.$$

Nếu $y - x$ chia hết cho 4 thì $\dfrac{y + x}{2}$ là số lẻ. Khi đó

$$z_4 = (\frac{x + y}{2} + 4x) + i.\frac{x + y}{2}.\sqrt{7} \text{ với } N(z_4) = 2^{n+1}.$$

Với kỹ thuật tương tự, ta hoàn toàn có thể giải quyết các bài toán sau.

Bài toán 2.3.29. Chứng minh rằng với mọi n nguyên dương, phương trình $x^2 + 15y^2 = 4^n$ có đúng n nghiệm nguyên không âm.

Bài toán 2.3.30. Với bất kỳ số nguyên $n \geq 1$ đều có hai số nguyên lẻ x và y để $4.3^n = 11x^2 + y^2$.

Bài toán 2.3.31. Chứng minh rằng luôn tồn tại hai số nguyên x và y để $31^n = x^2 + 6y^2$ với $\begin{cases} x \text{ lẻ và } y \text{ lẻ khi } n \text{ lẻ} \\ x \text{ lẻ và } y \text{ chẵn khi } n \text{ chẵn} \end{cases}$

Bài toán 2.3.32. Với mọi số tự nhiên n, luôn tồn tại hai số nguyên lẻ x và y để $507^{2n+1} = 4x^2 + 503y^2$.

Bài toán 2.3.33. Với mọi số tự nhiên n, luôn tồn tại hai số nguyên lẻ x và y để $2013^{2n+1} = 4x^2 + 249y^2$.

Ví dụ 2.3.34. Chứng minh rằng số nguyên tố lẻ p có thể biểu diễn được dưới dạng

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

với $x, y \in \mathbb{Z}$ khi và chỉ khi p đồng dư với 1 hoặc 3 modulo 8.

Lời giải. Nếu $p = x^2 + 2y^2$ với $x, y \in \mathbb{Z}$ thì cả $|x|$ và $|y|$ là các số nguyên dương nhỏ hơn p. Điều này kéo theo lớp đồng dư modulo p của y là khả nghịch và ta suy ra rằng -2 là một thặng dư chính phương modulo p nghĩa là

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

Mặt khác, ta biết rằng

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

Ta suy rằng với p là một số nguyên tố lẻ, -2 là thặng dư chính phương modulo p khi và chỉ khi p đồng dư với 1 hoặc 3 modulo 8.

Giả sử p đồng dư với 1 hoặc 3 modulo 8. Khi đó tồn tại $x \in \mathbb{Z}$ sao cho $x^2 + 2 \equiv 0 \pmod 8$. Trong vành $R = \mathbb{Z}[\sqrt{-2}]$, ta có phân tích

$$x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$$

với $x + i\sqrt{2}$ và $x - \sqrt{2}$ là phần tử có ước chung lớn nhất là ước của $2\sqrt{2}$. Vì p là ước của $x^2 + 2$ và p nguyên tố cùng nhau với 2 cho nên ta có thể phân tích thành

$$p = \alpha q \overline{q}$$

với α là phần tử khả nghịch của $\mathbb{Z}[\sqrt{-2}]$, $q = m + in\sqrt{2}$ là một phần tử sinh của iđêan sinh bởi p và $x + i\sqrt{2}$, $\overline{q} = m - in\sqrt{2}$ là một phần tử sinh của iđêan sinh bởi p và $x - i\sqrt{2}$. Vì $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$, ta có $p = \pm(m^2 + 2n^2)$. Vì p là số nguyên dương, ta có $p = m^2 + 2n^2$ như mong muốn.

Ta tiếp tục xem xét một số ví dụ liên quan đến phương trình nghiệm nguyên.

Ví dụ 2.3.35. Giải phương trình nghiệm nguyên

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

Lời giải. Ta có $x^3 = (y+\sqrt{-2})(y-\sqrt{-2})$. Chú ý rằng nếu $y = 2k$ thì $y^2+2 \equiv 2 \pmod 4$, không có số nguyên x thỏa mãn $x^3 \equiv 2 \pmod 4$.

Do vậy, y lẻ $\Rightarrow x$ lẻ.

Đặt $\gcd(y+\sqrt{-2}, y-\sqrt{-2}) = u$. Khi đó $u|2\sqrt{-2} = -(\sqrt{-2})^3$ trong $\mathbb{Z}[\sqrt{-2}]$ và suy ra u là một lũy thừa của $\sqrt{-2}$.

Nếu $\sqrt{-2}|(y \pm \sqrt{-2})$ thì $N(y \pm \sqrt{-2})$ là một số chẵn và

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}) = y^2 + 2$$

chia hết cho 2 nên x là một số chẵn (vô lý).

Từ đây suy ra $u \not| \sqrt{-2}$. Như vậy $y + \sqrt{-2}$ và $y - \sqrt{-2}$ là số nguyên tố cùng nhau. Do $\mathbb{Z}[\sqrt{-2}]$ là một vành Euclide nên nó là vành chính, vậy có một số $a + b\sqrt{-2}$ để $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3 = (a + b\sqrt{-2})^3$.

Vì $y + \sqrt{-2}$ và $y - \sqrt{-2}$ là số nguyên tố cùng nhau nên dễ dàng suy ra $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ và $y - \sqrt{-2} = \pm 1$ chẳng hạn.

Từ đây suy ra $y = a^3 - 6ab^2$ và $3a^2b - 2b^3 = 1$.

Ta giải được $b = \pm 1$ và $a = \pm 1$.

Từ đó ta có nghiệm $x = 3$ và $y = \pm 5$.

Bài toán 2.3.36. Giải phương trình nghiệm nguyên

(i) $x^3 = y^2 + 5$

(ii) $x^2 + 11 = y^3$

(iii) $x^2 + 19 = y^3$

(iv) $x^2 + 61 = y^3$

(v) $x^2 + 19 = y^5$.

Bài toán 2.3.37. Cho p là số nguyên tố. Chứng minh rằng

(i) $p \equiv 1, 3 \pmod 8 \Leftrightarrow p = x^2 + 2y^2$ với $x, y \in \mathbb{Z}$.

(ii) $p \equiv 1 \pmod 3 \Leftrightarrow p = x^2 + 3y^2$ với $x, y \in \mathbb{Z}$.

Bài toán 2.3.38. Cho tập hợp $S = \{x^2 + 3y^2 | x, y \in \mathbb{Z}\}$. Chứng minh rằng nếu a là một số nguyên mà $3a$ thuộc S thì a thuộc S.

2.4 Ứng dụng vành $\mathbb{Z}_p[\sqrt{d}]$, vành $\mathbb{Z}_p[i]$ vào giải toán

Trong mục này, chúng ta tìm hiểu một số vành số được xây dựng dựa trên các vành đã để xuất ở các mục 2.1, 2.2, 2.3.

2.4.1 Ứng dụng vành $\mathbb{Z}_p[\sqrt{d}]$ vào giải toán

Định nghĩa 2.4.1. Cho p là số nguyên tố lẻ và số nguyên d không là thặng dư chính phương môđun p. Đặt

$$\mathbb{Z}_p[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}_p\}.$$

Rõ ràng $\mathbb{Z}_p[\sqrt{d}]$ có đúng p^2 phần tử. Chúng ta định nghĩa các phép toán trên $\mathbb{Z}_p[\sqrt{d}]$ như sau:

Với $x = a + b\sqrt{d}, y = m + n\sqrt{d}; x, y \in \mathbb{Z}_p[\sqrt{d}]$

(i) $x = y \Leftrightarrow a = m; b = n$

(ii) $x \pm y = a \pm m + (b \pm n)\sqrt{d} \in \mathbb{Z}_p[\sqrt{d}]$

(iii) $xy = am + bnd + (an + bm)\sqrt{d} \in \mathbb{Z}_p[\sqrt{d}]$.

Khi đó $\mathbb{Z}_p[\sqrt{d}]$ là một vành giao hoán có đơn vị.

Mệnh đề 2.4.2. *Cho $x = a + b\sqrt{d} \in \mathbb{Z}_p^*[\sqrt{d}], (a^2 + b^2 \neq 0)$. Khi đó*

$$y = (a^2 - db^2)^{-1}.(a - b\sqrt{d}) \in \mathbb{Z}_p^*[\sqrt{d}]$$

là nghịch đảo của x trong $\mathbb{Z}_p^*[\sqrt{d}]$.

Ta có tính chất sau đây trình bày về cấp của phần tử trong $\mathbb{Z}_p$ và $\mathbb{Z}_p[\sqrt{d}]$.

Mệnh đề 2.4.3. *(i) Trong $\mathbb{Z}_p$, mọi phần tử khác 0 đều có cấp và cấp của nó là ước của $p - 1$.*

(ii) Trong $\mathbb{Z}_p[\sqrt{d}]$, mọi phần tử khác 0 đều có cấp và cấp của nó đều là ước của $p^2 - 1$ và $x^{p^2-1} = 1$ với mọi $x \in \mathbb{Z}_p^*[\sqrt{d}]$.

Định lí 2.4.4. *Cho $x \in \mathbb{Z}_p[\sqrt{d}]$ và $k > 1$ là số nguyên dương. Khi đó*

$$\text{ord}(x^k) = \frac{\text{ord}(x)}{\gcd(\text{ord}(x), k)}.$$

Định lí 2.4.5. *Cho $x \in \mathbb{Z}_p[\sqrt{d}]$ có cấp là l, khi đó x^k có cấp là l khi và chỉ khi* $\gcd(l, k) = 1$.

Khi d không là số chính phương ta có định nghĩa $\mathbb{Z}_p[\sqrt{d}]$ như ở Mệnh đề 2.4.1, còn khi d là thặng dư chính phương ta hoàn toàn có thể đồng nhất $\mathbb{Z}_p[\sqrt{d}]$ và $\mathbb{Z}_p$. Việc phân chia như vậy giúp ta giải quyết 1 số bài toán.

Ví dụ 2.4.6. Cho dãy số $a_0, a_1, a_2, ...$ được định nghĩa như sau:

$$a_0 = 2, a_{k+1} = 2a_k^2 - 1 \text{ với mọi } k \geq 0.$$

Chứng minh rằng nếu p là ước nguyên tố lẻ của a_n thì 2^{n+3} là ước của $p^2 - 1$.

Lời giải.

Ta tìm được công thức tổng quát của a_n như sau:

$$a_n = \frac{(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}}{2}, \forall n \geq 0.$$

Bây giờ xét ước nguyên tố lẻ p của x_n. Vì $p|a_p = 2a_{p-1}^2 - 1$ nên $2a_{p-1}^2 \equiv 1 \pmod{p}$, kéo theo 2 là thặng dư chính phương môđun p, từ đó suy ra $8|p^2 - 1$.

Nếu 3 là thặng dư chính phương môđun p thì ta xét dãy $\{a_n\}$ trên $\mathbb{Z}_p$.

Mặt khác, tồn tại $x \in \mathbb{Z}_p$ sao cho $x^2 = 3$. Khi đó

$$a_n = \frac{(2+x)^{2^n} + (2-x)^{2^n}}{2} = 0.$$

Vì $2 - x = \dfrac{1}{2-x}$ nên suy ra $(2+x)^{2^{n+1}} = -1$. Do 2 là thặng dư chính phương nên tồn tại $y \in \mathbb{Z}_p$ sao cho $y^2 = 2$. Suy ra

$$2 + x = \frac{4+2x}{2} = \frac{(x+1)^2}{2} = \left(\frac{1+x}{y}\right)^2.$$

Đặt $z = \dfrac{1+x}{y}$, ta có $z^{2^{n+2}} = -1$ và $z^{2^{n+3}} = 1$. Lúc này $\text{ord}(z) = 2^i$ với $i \leq n+3$.

Nếu $i \leq n+2$ ta bình phương hai vế $z^i = 1$ cho đến khi bằng $n+2$ ta sẽ gặp ngay mâu thuẫn. Vì thế $\text{ord}(2) = 2^{n+3}$.

Vậy $2^{n+3}|p-1$, suy ra điều phải chứng minh.

Nếu 3 không là thặng dư chính phương thì ta sẽ xét dãy $\{a_n\}$ trên $\mathbb{Z}_p[\sqrt{3}] = \{u + v\sqrt{3} | u, v \in \mathbb{Z}_p\}$.

Vì $a_n = 0$ nên $(2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n} = 0$ mà $2 - \sqrt{3} \neq 0$ trên $\mathbb{Z}_p[\sqrt{d}]$ nên $(2+\sqrt{3})^{2^{n+1}} = -1$.

Mặt khác $2 = y^2 = (y + 0\sqrt{3})^2$ nên 2 cũng là số chính phương trên $\mathbb{Z}_p[\sqrt{d}]$.

Đặt $z = \dfrac{1+\sqrt{3}}{y}$, khi đó $z^{2^{n+2}} = -1$. Lập luận tương tự như trên ta cũng có $\text{ord}(z) = 2^{n+3}$. Vì thế $2^{n+3}|p^2 - 1$.

Ví dụ 2.4.7. Dãy số $\{x_n\}$ được định nghĩa $x_1 = 2, x_2 = 12$ và $x_{n+2} = 6x_{n+1} - x_n$ với mọi $n \geq 1$. Gọi p là số nguyên tố lẻ, q là ước nguyên tố của x_p. Chứng minh rằng nếu $q \neq 2, 3$ thì $q \geq 2p - 1$.

Lời giải.

Ta có công thức tổng quát cho dãy số

$$x_n = \frac{(\sqrt{2}+1)^{2n} - (\sqrt{2}-1)^{2n}}{2\sqrt{2}}, \forall n \geq 1.$$

Gọi p là số nguyên tố lẻ và q là ước nguyên tố của x_p.

Tiếp theo, chúng ta có thể thực hiện giống như ví dụ trên là xét trên $\mathbb{Z}_q$ hoặc $\mathbb{Z}_q[\sqrt{d}]$ để chứng minh $p|q^2 - 1$.

Khi đó, $p|q-1$ hoặc $p|q+1$ mà p là số nguyên tố lẻ nên $p|\dfrac{q-1}{2}$ hoặc $p|\dfrac{q+1}{2}$ suy ra $p \leq \dfrac{q-1}{2}$ hoặc $p \leq \dfrac{q+1}{2}$.

Vậy từ cả hai ta đều có $q \geq 2p - 1$.

Bài toán 2.4.8. Cho a là một số nguyên dương và p là ước nguyên tố của $a^3 - 3a + 1$ với $p > 3$. Chứng minh rằng p có dạng $9k + 1$ hoặc $9k - 1$ với k là số nguyên.

Bài toán 2.4.9. Gọi S là tập tất cả các số có dạng $a + b\sqrt{2}$, trong đó a và b là các số nguyên không âm nhỏ hơn 83 và không đồng thời bằng 0. Giả sử tích tất cả các phần tử của S được viết dưới dạng $m + n\sqrt{2}$, trong đó m và n là các số nguyên. Tìm số dư của m và n khi đem chia cho 83.

2.4.2 Ứng dụng vành $\mathbb{Z}_p[i]$ vào giải toán

Định nghĩa 2.4.10. Tập $\mathbb{Z}_p[i] = \{a + bi | a, b \in \mathbb{Z}_p, i^2 = -1\}$ cùng với các phép toán được xác định như sau với $x = a + bi, y = m + ni \in \mathbb{Z}_p[i]$

(i) $x = y \Leftrightarrow a = m, b = n$

(ii) $x \pm y = a \pm m + (b \pm n)i \in \mathbb{Z}_p[i]$

(iii) $xy = am - bn + (an + bm)i \in \mathbb{Z}_p[i]$

là một vành.

Chúng ta sẽ sử dụng vành $\mathbb{Z}_p[i]$ để giải quyết một số bài toán liên quan.

Ví dụ 2.4.11. Với số nguyên tố p có dạng $4n + 1$, hãy xét số dư của số $\prod_{k=1}^{p}(k^2 + 1)$ khi chia cho p.

Lời giải.

Xét số này trong vành $\mathbb{Z}_p[i]$ và đồng nhất k với ảnh của nó, ta có biểu diễn thành tích

$$\prod_{k=1}^{p}(k^2 + 1) = \prod_{k=1}^{p}(k + i)(k - i) = \prod_{k=1}^{p}(k + i)\prod_{k=1}^{p}(k - i) = f(i).f(-i)$$

ở đó $f(x) = \prod_{k=1}^{p}(x + k)$.

Vì $f(x) = x^p - x$ trên $\mathbb{Z}_p[i]$ nên ta có được

$$\prod_{k=1}^{p}(k^2+1) = f(i).f(-i) = (i^p - i)((-i)^p + i) = i.(-i).(i^{p-1} - 1).((-i)^{p-1} - 1).$$

Do đó $\prod_{k=1}^{p}(k^2 + 1) = 0$ nên $\prod_{k=1}^{p}(k^2 + 1) \equiv 0 \pmod{p}$.

Ví dụ 2.4.12. Cho p là số nguyên tố dạng $7k - 1$. Chứng minh rằng tồn tại số nguyên dương m sao cho $m^3 + m^2 - 2m - 1$ là bội của p.

Lời giải.

Ý tưởng là tìm a sao cho $a + \dfrac{1}{a}$ là số nguyên và $a^7 = 1$.

Ta xét vành $\mathbb{Z}_p[\sqrt{-7}] = \{x + y\sqrt{-7} | x, y \in \mathbb{Z}_p\}$. Vì $7|p^2 - 1$ nên tồn tại $a = x + y\sqrt{-7} \in \mathbb{Z}_p[\sqrt{-7}]$ sao cho $\text{ord}(a) = 7$, suy ra $\text{ord}(\overline{a}) = -7$. Từ đây ta có $(x^2 + 7y^2)^7 = (a.\overline{a})^7 = 1$.

Mặt khác, vì $x^2 + 7y^2$ nguyên tố với p nên theo định lý Fermat nhỏ, ta có:

$$(x^2 + 7y^2)^{p-1} \equiv 1 \pmod{p}.$$

Mà $(7, p-1) = 1$ nên $x^2 + 7y^2 \equiv 1 \pmod{p}$. Do đó ta có

$$a + \frac{1}{a} = x + y\sqrt{7} + \frac{x}{x^2+7y^2} - \frac{y\sqrt{7}}{x^2+7y^2} = 2x.$$

Vậy số cần tìm là $n = 2x$.

Ví dụ 2.4.13. Cho k là một số nguyên và $p \equiv 3 \pmod{4}$ là một số nguyên tố, chúng ta định nghĩa dãy $\{a_n\}$ như sau

$$a_0 = 0, a_1 = 1, a_n = 2k.a_{n-1} - (k^2+1)a_{n-2}, (n \geq 2).$$

Chứng minh rằng $a_{n+p^2-1} \equiv a_n \pmod{p}$.

Lời giải.

Xét phương trình đặc trưng

$$X^2 - 2kX + k^2 + 1 = 0.$$

từ đó ta có công thức tổng quát

$$a_n = \frac{i(k-i)^n - i(k+i)^n}{2}, \forall n \geq 0.$$

Vì $p \equiv 3 \pmod{4}$ nên -1 không là thặng dư chính phương môđun p. Lúc này

$$\mathbb{Z}_p[i] = \{a + bi | a, b \in \mathbb{Z}_p\}.$$

Chú ý rằng với mọi $x \in \mathbb{Z}_p^*[i]$ thì $x^{p^2-1} = 1$, suy ra

$$a_{n+p^2-1} = \frac{i(k-i)^{n+p^2-1} - i(k+i)^{n+p^2-1}}{2} = \frac{i(k-i)^n - i(k+i)^n}{2} = a_n.$$

Vì thế $a_{n+p^2-1} \equiv a_n \pmod{p}$.

2.5 Ứng dụng vành các số nguyên Eisenstein vào giải toán

2.5.1 Cơ sở lý thuyết

Định nghĩa 2.5.1.

(i) $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ là một nghiệm nguyên thủy của phương trình $x^3 = 1$.

(ii) $\omega^2 + \omega + 1 = 0$.

Ta làm việc trên vành các số nguyên Eisenstein $\mathbb{Z}[\omega]$ được xây dựng như sau

Định nghĩa 2.5.2. Tập $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$ có các phép toán được định nghĩa như sau: $x = a + b\omega, y = m + n\omega; x, y \in \mathbb{Z}[\omega]$

(i) $x = y \Leftrightarrow a = m, b = n$

(ii) $x \pm y = (a \pm m) + (b \pm n)\omega \in \mathbb{Z}[\omega]$

(iii) $xy = (am - bn) + (mb + an - bn)\omega \in \mathbb{Z}[\omega]$

lập thành một vành.

Nhận xét 2.5.3. Khi đó, chuẩn $N(a + b\omega) = a^2 - ab + b^2$ và các phần tử khả nghịch là $\pm 1, \pm\omega$ và $\pm(1 + \omega) = \mp\omega^2$.

Ngoài ra

$$\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\} = \left\{ \frac{c + d\sqrt{-3}}{2} | c, d \in \mathbb{Z}, 2|c - d \right\}.$$

Định lí 2.5.4. *Định lý cơ bản của số học vẫn đúng trên vành* $\mathbb{Z}[\omega]$.

Định lí 2.5.5. *Phần tử* $x \in \mathbb{Z}[\omega]$ *là nguyên tố khi và chỉ khi* $N(x)$ *là nguyên tố hoặc* $|x|$ *là số nguyên tố có dạng* $3k + 2$.

2.5.2 Ứng dụng vành $\mathbb{Z}[\omega]$ vào giải toán

Ví dụ 2.5.6. Chứng minh rằng số nguyên tố p có dạng

$$p = m^2 + 3n^2$$

với $m, n \in \mathbb{Z}$ khi và chỉ khi $p = 3$ hoặc $p \equiv 1 \pmod 3$.

Lời giải. Dễ dàng kiểm tra được số nguyên tố 2 không có dạng $m^2 + 3n^2$ còn 3 thì có dạng $m^2 + 3n^2$, cho nên ta có thể giả sử $p > 3$. Tính ký hiệu Legendre bằng luật thuận nghịch ta có:

$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right). \end{aligned}$$

Ta thấy rằng -3 là bình phương modulo p khi và chỉ khi p là bình phương modulo 3 có nghĩa là $p \equiv 1 \pmod 3$.

Nếu $p = x^2 + 3y^2$ với x, y là các số tự nhiên thì ta có $0 < y < p$ cho nên y nguyên tố cùng nhau với p. Chọn $a \in \mathbb{N}$ sao cho $ay \equiv 1 \pmod p$. Nhân cả hai vế của phương trình $p = x^2 + 3y^2$ với a^2, ta có $(ax)^2 + 3 \equiv 0 \pmod p$. Như tính toán ký hiệu Legendre phía trên chỉ ra, điều này chỉ xảy ra nếu $p \equiv 1 \pmod 3$.

Vì vành các nguyên tố Eisenstein $\mathbb{Z}[\omega]$ là vành Euclide như trong trường hợp $\mathbb{Z}[i]$ và $Z[i\sqrt{2}]$ cho nên tồn tại $x \in \mathbb{Z}$ sao cho $x^2 + 3 \equiv 0 \pmod p$ kéo theo sự tồn tại của số nguyên Eisenstein $z = m + \omega n$ là phần tử sinh của iđêan sinh bởi p và $x + i\sqrt{3}$. Lập luận như trong trường hợp $\mathbb{Z}[i\sqrt{2}]$ ta có

$$p = z\overline{z} = (m + \omega n)(m + \omega^2 n) = m^2 - mn + n^2$$

với

$$m^2 - mn + n^2 = \left(m - \frac{n}{2}\right)^2 + \frac{3n^2}{4} = \left(n - \frac{m}{2}\right)^2 + \frac{3m^2}{4}.$$

Như vậy p có dạng $p = a^2 + 3b^2$ với $a, b \in \mathbb{Z}$ nếu hoặc m hoặc n là số chẵn. Trong trường hợp cả m và n là số lẻ thì ta có thể thay $z = m + \omega n$ bằng

$$\omega z = -n + (m - n)\omega$$

với $m - n$ là số nguyên chẵn. Vì ω là phần tử khả nghịch của $\mathbb{Z}[\omega]$ cho nên ωz cũng là một phần tử sinh của iđêan sinh bởi p và $x + i\sqrt{3}$ và ta có thể kết thúc chứng minh như ở trên.

Ví dụ 2.5.7. Chứng minh rằng mọi số nguyên tố có dạng $6k + 1$ luôn có thể tìm được các số nguyên a, b thỏa mãn $p = a^2 - ab + b^2$.

Lời giải.

Ta chỉ cần chứng minh p là hợp số trong $\mathbb{Z}[\omega]$. Thật vậy nếu tồn tại phần tử $z = a + b\omega \in \mathbb{Z}[\omega](a, b \in \mathbb{Z})$ nguyên tố chia hết p, suy ra $\overline{z}|\overline{p} = p$. Để ý rằng, z và $\overline{z}$ nguyên tố cùng nhau; nếu không thì $z|\overline{z}$, suy ra tồn tại phần tử đơn vị ϵ sao cho $\overline{z} = \epsilon.z$ và do đó $z \sim (1 - \omega)|3$, vô lý. Vì vậy, $a^2 - ab + b^2 = z\overline{z}|p$, suy ra $a^2 - ab + b^2 = p$.

Do đó, ta sẽ chứng minh p là hợp số trong $\mathbb{Z}[\omega]$. Điều này suy ra từ điều kiện trên p rằng -3 là thặng dư bình phương môđun p, suy ra tồn tại $m, n \in \mathbb{Z}$ không chia hết cho p sao cho

$$p|(2m - n)^2 + 3n^2 = 4(m^2 - mn + n^2),$$

suy ra $p|(m-n\omega)\overline{m-n\omega}$. Tuy nhiên, p không chia hết $(m-n\omega), \overline{m-n\omega}$, vì vậy p là hợp số.

Ví dụ 2.5.8. Chứng minh rằng phương trình sau đây không có nghiệm nguyên khác 0.

$$x^3 + y^3 = z^3 \qquad (*)$$

Lời giải.

Gọi x, y, z là các phần tử khác 0 thuộc $\mathbb{Z}[\omega]$ thỏa mãn phương trình (*). Không mất tính tổng quát, giả sử x, y, z đôi một nguyên tố cùng nhau.

Xét $\rho = 1-\omega$. Số ρ là số nguyên tố vì chuẩn của nó bằng $(1-\omega)(1-\omega^2) = 3$. Ta thấy rằng

$$\overline{\rho} = 1 - \omega^2 = (1-\omega)(1+\omega) \sim \rho,$$

từ đây $\alpha \in \mathbb{Z}[\omega]$ chia hết cho ρ khi và chỉ khi $\alpha = \overline{\alpha}$. Mỗi phần tử thuộc $\mathbb{Z}[\omega]$ đồng dư với -1, 0 hoặc 1 $\pmod{\rho}$: thật vậy

$$a + b\omega \equiv a + b = 3q + r \equiv r \pmod{\rho} \text{ với } q \in \mathbb{Z} \text{ và } r \in \{-1, 0, 1\}.$$

Số ρ có tính chất quan trọng sau:

$$\alpha \equiv \pm 1 \pmod{\rho}\ (\alpha \in \mathbb{Z}[\omega]) \text{ suy ra } \alpha^3 \equiv \pm 1 \pmod{\rho^4}. \qquad (2)$$

Thật vậy, nếu $\alpha = \pm 1 + \beta\rho$, ta có

$$a^3 \mp 1 = (a \mp 1)(a \mp \omega)(a \mp \omega^2) = \rho^3\beta(\beta \pm 1)(\beta \pm (1+\omega)),$$

trong đó các phần tử $b, b \pm 1, b \pm (1+\omega)$ có 3 số dư phân biệt khi chia cho ρ, tức là có 1 số chia hết cho ρ, từ đó tính chất (2) là đúng.

Trong các số x, y, z, có đúng 1 số chia hết cho ρ; nếu không thì $x^3, y^3, z^3 \equiv \pm 1 \pmod{4}$, dẫn đến $x^3 + y^3 \not\equiv z^3 \pmod{4}$, vô lý. Không mất tính tổng quát, giả sử $\rho|z$. Hơn nữa, từ (2) suy ra $p^2|z$.

Gọi $k \geq 2$ là số tự nhiên nhỏ nhất thỏa mãn phương trình $(*)$ với $(x, y, z) = 1$ và $p^k|z, p^{k+1} \nmid z$

Ta có $x+y, \omega x+\omega^2 y, \omega^2 x+\omega y$ đồng dư theo môđun ρ và có tổng là 0. Điều này được suy ra từ $p|z$ rằng mỗi số đều chia hết cho ρ và ρ là ước chung lớn nhất của chúng. Đặt

$$x + y = A\rho, \quad \omega x + \omega^2 y = B\rho, \quad \omega^2 x + \omega y = C\rho,$$

với $A, B, C \in \mathbb{Z}[\omega]$ nguyên tố cùng nhau và $A + B + C = 0$. Tích ABC là lập phương và bằng $(z/\rho)^3$ và do đó A, B, C được viết như sau:

$$A = \alpha\zeta^3, \quad B = \beta\eta^3, \quad C = \gamma\xi^3$$

với các số nguyên tố cùng nhau $\zeta, \eta, \xi \in \mathbb{Z}[\omega]$ và các đơn vị α, β, γ. Vì vậy,

$$\alpha\zeta^3 + \beta\eta^3 + \gamma\xi^3 = 0. \qquad (3)$$

Vì $\alpha\beta\gamma$ là đơn vị và là lập phương nên ta có $\alpha\beta\gamma = \pm 1$. Hơn nữa, $ABC = (z/\rho)^3$ chia hết cho ρ, (vì $\rho^2 \mid z$), vì vậy có đúng 1 trong 3 số ζ, η, ξ, giả sử là ξ chia hết cho ρ. Thực tế, ξ^3 chia hết ABC, mà ABC chia hết cho ρ^{3k-3} mà không chia hết cho ρ^{3k-2}, vì vậy ρ^{k-1} là lũy thừa lớn nhất của ρ chia hết ξ. Số ζ và η không chia hết cho ρ, suy ra $\zeta^3, \eta^3 \equiv \pm 1 \pmod 4$. Như vậy, $A+B+C = 0$ cho ta $\alpha \pm \beta \equiv 0 \pmod{p^4}$, vì vậy, $\beta = \pm\alpha$, từ đây $\alpha\beta\gamma = \pm 1$ suy ra $\gamma = \pm\alpha$.

Bỏ α trong phương trình (3), ta có $\zeta^3 \pm \eta^3 \pm \xi^3 = 0$ với $(\zeta, \eta, \xi) = 1$. Tuy nhiên, ta có $\rho^{k-1} \mid \xi$ và $\rho^k \nmid \xi$, điều này mâu thuẫn với sự lựa chọn k.

Ví dụ 2.5.9. Cho p là số nguyên tố dạng $3k+1$. Chứng minh rằng tồn tại cặp số nguyên (a, b) sao cho $p^5 | (a+b)^p - a^p - b^p$.

Lời giải.

Chúng ta sẽ chứng minh rằng $f(x, y) = (x+y)^p - x^p - y^p$ chia hết cho $(x^2 + xy + y^2)^2$ với mọi số nguyên khác 0. Thật vậy, gọi $\omega \neq 1$ là nghiệm của $z^3 = 1$. Khi đó ta xem $f(x, y)$ là một đa thức theo biến x và y là tham số. Lúc này $\omega^2 + \omega + 1 = 0$, phương trình $x^2 + xy + y^2 = 0 \Leftrightarrow x = \omega y$.

Chúng ta sẽ chứng minh $y\omega$ là nghiệm của $f(a)$ và $f'(a)$. Ta có

$$\begin{aligned} f(y\omega) &= (y\omega + y)^p - (y\omega)^p - y^p \\ &= y^p[(\omega+1)^p - \omega^p - 1] \\ &= y^p(\omega + 1 - \omega - 1) = 0 \end{aligned}$$

và $f'(x) = p(x+y)^{p-1} - px^{p-1}$ vì thế

$$\begin{aligned} f'(y\omega) &= p(y\omega + y)^{p-1} - p(y\omega)^{p-1} \\ &= py^{p-1}[(\omega+1)^{p-1} - \omega^{p-1}] \\ &= py^{p-1}[(-1)^{\frac{p-1}{3}} - 1] = 0. \end{aligned}$$

Vậy $(x^2+xy+y^2)^2|f(x,y)$.

Xét đa thức $f(x)=x^2+x+1$, vì $p\equiv 1 \pmod 3$ nên phương trình $x^2+x+1\equiv 0 \pmod p$ có nghiệm. Khi đó $(2x+1)^3+3\equiv 0 \pmod p$ nên $f'(x)=2x+1$ không thể chia hết cho p. Vì thế theo bổ đề Hensel thì tồn tại nghiệm x để $x^2+x+1\equiv 0 \pmod{p^2}$ tức là tồn tại cặp số nguyên (a,b) sao cho $0<a,b<p$ và $p^2|a^2+ab+b^2$. Kết hợp cả hai kết quả ta có điều phải chứng minh.

KẾT LUẬN

Nội dung chính của đồ án là tìm hiểu và trình bày các đặc trưng của các lớp vành số được xây dựng trên vành số nguyên $\mathbb{Z}$. Từ đó hệ thống hóa và đưa ra các ứng dụng trong việc giải quyết các bài toán sơ cấp lĩnh vực đại số, số học.

Cụ thể chúng tôi đã trình bày các nội dung sau:

(i) Các khái niệm và tính chất cơ bản của lý thuyết vành.

(ii) Khái niệm, tính chất các lớp vành số: $\mathbb{Z}_n, \mathbb{Z}_p, \mathbb{Z}[\sqrt{d}], \mathbb{Z}[\sqrt{-d}]$, $\mathbb{Z}[\sqrt{p}, \sqrt{q}]$, $\mathbb{Z}[i], \mathbb{Z}_p[\sqrt{d}]$, $\mathbb{Z}_p[i], \mathbb{Z}[\omega]$.

(iii) Ứng dụng các lớp vành số ở trên vào giải toán sơ cấp.

TÀI LIỆU THAM KHẢO

[1] Trần Tuấn Nam (Chủ biên) (2015), *Một số ứng dụng của đại số hiện đại vào giải toán sơ cấp*, Nhà xuất bản Đại học Sư phạm thành phố Hồ Chí Minh.

[2] Đàm Văn Nhỉ (Chủ biên) (2017), *Lý thuyết số và chuyên đề nâng cao*, Nhà xuất bản Thông tin và truyền thông.

[3] Dương Thái Bảo (2023), *Bài giảng số học*, Nhà xuất bản Đại học Quốc gia Hà Nội.

[4] Lê Thị Thanh Nhàn (2015), *Giáo trình Lý thuyết Đa thức*, Nhà xuất bản Đại học Quốc gia Hà Nội.

[5] Nguyễn Thị Hồng Loan, Phạm Hùng Quý, Nguyễn Thành Quang (2022), *Giáo trình đại số đại cương*, Nhà xuất bản Đại học Vinh.

[6] Ngô Bảo Châu, Đỗ Việt Cường (2024), *Lý thuyết số sơ cấp*, Nhà xuất bản Đại học Quốc gia Hà Nội .

[7] Nguyễn Chu Gia Vượng (2011), *Các số nguyên Gauss*, Tạp chí thông tin Toán học tập 15 số 1+2, Hội Toán học Việt Nam

[8] Dinesh Khattar and Neha Agrawal (2023), *Ring Theory*, Springer.

[9] P.Stevenhagen (2019), *Number Rings*, Univesiteit Leiden.

[10] Beverly Molelekeng (2022), *Arithmetic in the ring of Gauss integer*, University of the Witwatersrand Johannesburg.

[11] Alexandria, Kaeli, William (2020), T*he Arithmetic of the Gauss integers*, Math 444, Assignment 8

[12] Dusan Djukic, *Arimethic in Extention of Q*, imomath.com.