ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐÀO THỊ THƯƠNG HOÀI

MỘT VÀI VẤN ĐỀ VỀ PHƯƠNG TRÌNH DIOPHANTE

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP

Mã số: 60.46.36

LUẬN VĂN THẠC SỸ TOÁN HỌC

Người hướng dẫn khoa học: PGS.TS. NÔNG QUỐC CHINH

THÁI NGUYÊN - 2010

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐÀO THỊ THƯƠNG HOÀI

MỘT VÀI VẤN ĐỀ VỀ PHƯƠNG TRÌNH DIOPHANTE

LUẬN VĂN THẠC SỸ TOÁN HỌC

THÁI NGUYÊN - 2010

Mục lục

PHẦN MỞ ĐẦU

Phương trình nói chung và phương trình Diophante nói riêng là một trong những vấn đề thu hút sự quan tâm không chỉ đối với giáo viên và học sinh các trường trung học phổ thông mà còn đối với tất cả những người yêu thích Toán.

Trong hầu hết các kì thi quan trọng như thi học sinh giỏi toán các cấp, thi Olympic toán, các bài toán liên quan đến phương trình Diophate cũng hay được đề cập đến và thường là rất khó.

Trong luận văn này chúng tôi xin trình bày một số vấn đề về phương trình Diophante.

Mục đích của luận văn là trình bày tổng quan về phương trình Diophante; khái quát lịch sử phát triển của nó; trình bày Định lí lớn Fermat và một số dạng cụ thể của phương trình Diophante; trình bày một vài vấn đề mở rộng, trong đó có kết quả mới tìm được về phương trình Diophante.

Nội dung chính của luận văn chia làm 3 chương.

Chương 1. Chúng tôi trình bày tổng quan về phương trình Diophante, khái niệm về phương trình Diophante và khái quát lịch sử phát triển của nó.

Chương 2. Định lí lớn Fermat và các phương trình Diophante dạng:
$x^2 + y^2 = z^2; x^4 + y^4 = z^2; x^3 + y^3 = z^3; x^3 + y^3 = 3z^3; x^3 + y^3 + z^3 = t^3$.
Để giải quyết được những phương trình Diophante trên chúng tôi đã đưa vào một số khái niệm và tính chất trong trường $\mathbb{Q}(\rho)$ - là mở rộng đại số của trường số hữu tỉ.

Ngoài những phương trình đã nêu trên còn rất nhiều dạng phương trình Diophante khác, trong Chương 3 chúng tôi sẽ trình bày thêm một kết quả mới về phương trình Diophate và vài phương trình Diophante bậc cao khác.

Mặc dù đã rất cố gắng học tập và nghiên cứu một cách nghiêm túc, song chắc chắn luận văn này không tránh khỏi những thiếu sót. Rất mong nhận được

những ý kiến quý báu chỉ bảo của các thầy cô, sự góp ý chân thành của các bạn học viên.

Để hoàn thành được luận văn tôi đã nhận được sự giúp đỡ ủng hộ rất lớn của các thầy cô và bạn bè. Tôi xin chân thành cảm ơn PGS.TS Nông Quốc Chinh, thầy đã tận tình giảng dạy, chỉ bảo và ủng hộ trong suốt quá trình học tập và nghiên cứu của tôi. Cảm ơn Ban giám hiệu trường Đại học Khoa học cùng toàn thể các thầy cô đã tạo điều kiện giúp đỡ tôi hoàn thành luận văn. Cảm ơn các bạn học viên lớp cao học Toán khóa 2 của trường đã quan tâm giúp đỡ và ủng hộ tôi trong suốt thời gian học tập. Cảm ơn tập thể cán bộ giáo viên trường THPT Nguyễn Huệ nơi tôi đang công tác đã tạo điều kiện giúp đỡ tôi trong suốt quá trình học tập và hoàn thành luận văn này.

Thái Nguyên, ngày 20 tháng 8 năm 2010.

Học viên

Đào Thị Thương Hoài

Chương 1

Tổng quan về phương trình Diophante. Khái quát lịch sử phát triển của nó

Trong kho tàng văn hoá dân gian Việt Nam có bài toán "trăm trâu trăm cỏ" như sau:

" Trăm trâu trăm cỏ,

Trâu đứng ăn năm,

Trâu nằm ăn ba,

Lụ khụ trâu già,

Ba con một bó"

Hỏi có bao nhiêu trâu đứng, bao nhiêu trâu nằm, bao nhiêu trâu già.

Hoặc bài toán sau:

" Mai em đi chợ phiên,

Anh gửi một tiền,

Mua cam cùng quýt,

Không nhiều thì ít,

Mua lấy một trăm.

Cam ba đồng một,

Quýt một đồng năm,

Thanh yên tươi tốt,

Năm đồng một trái."

Hỏi mua mỗi thứ mấy trái? (biết rằng một tiền bằng 60 đồng). Để giải bài toán "trăm trâu trăm cỏ" ta làm như sau

Gọi số trâu đứng là x,

Số trâu nằm là y,

Số trâu già là $100-(x+y)$,

Ta có phương trình: $5x+3y+\dfrac{100-(x+y)}{3}=100$

hay $7x+4y=100$.

Vì x,y là số trâu nên điều kiện là:

$$\begin{cases} x,y \quad \text{là số nguyên dương} \\ x+y<100 \\ 7x<100 \\ 4y<100 \end{cases}$$

điều này tương đương với

$$\begin{cases} x,y\in\mathbb{N} \\ x+y<100 \\ x<14 \\ y<25 \end{cases}$$

Trên đây là một ví dụ về phương trình Diophante.

1.1. Định nghĩa phương trình Diophante

1.1.1. Định nghĩa. *Phương trình Diophante* là phương trình có nhiều ẩn số, với tất cả các hệ số đều là số nguyên và ta phải tìm nghiệm nguyên của nó.

1.1.2. Ví dụ. .

(i) Phương trình $ax+by=1$ với $a,b\in\mathbb{Z},(a,b)=1$ là *phương trình Diophante tuyến tính* có vô số nghiệm nguyên $x=x_0+bt$; $y=y_0-at$ với $(x_0;y_0)$ là một nghiệm nào đó của phương trình và $t\in\mathbb{Z}$.

(ii) Phương trình Diophante nổi tiếng nhất là *phương trình Fermat*.

$$x^n+y^n=z^n$$

+, Với $n=2$ ta được *phương trình Pitago* $x^2+y^2=z^2$ có vô số các bộ nghiệm $(x;y;z)$ được gọi là *bộ ba Pitago*. Ta có thể liệt kê một số bộ ba Pitago như sau : $(3;4;5),(5;12;13),(8;15;17),(7;24;25),(20;21;29)$.

+, Với $n>2$ Fermat khẳng định rằng không tồn tại bộ các số nguyên dương $(x;y;z)$ thỏa mãn phương trình.

(iii) $x^2-ny^2=\pm1$, trong đó n là số không chính phương(*phương trình Pell* - tên nhà toán học người Anh John Pell, phương trình này cũng được nghiên cứu bởi Brahmagrupta vào thế kỷ thứ VII và được giải quyết trọn vẹn bởi Fermat vào thế kỷ thứ XVII).

(iv) $\dfrac{4}{n}=\dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z}\Leftrightarrow 4xyz=nyz+nxz+nxy.$

1.2. Khái quát lịch sử phát triển

Diophante là một nhà toán học cổ Hilạp (thế kỷ thứ 3), và thường được nhắc đến như "ông tổ của ngành đại số". Ông là tác giả của cuốn sách nổi tiếng "số học" đã có nhiều đóng góp lớn đối với sự phát triển của Toán học, ông đã có nhiều kết quả trong việc giải phương trình đại số và lí thuyết số.

Phương trình Diophante là một lĩnh vực lý thú của toán học, trong đó chúng ta tìm thấy sự đóng góp của nhiều nhà toán học nổi tiếng: Euclide, Archimede, Fermat, Euler, Lagrange, Gauss, Dirichlet, Riemann, Hilbert,...

Một số nhà toán học Trung cổ Ân Độ như Sulba Stras; Baud hayana; Apastamba; Aryabhata (đã nghiên cứu và có nhiều kết quả về phương trình Dio-

phante tuyến tính); Kuttaka; Brahamagupta; Bhaskara.

Năm 1673, Fermat đã viết bên lề một cuốn sách rằng: "không thể phân tích một lập phương thành tổng của hai lập phương; cũng như một lũy thừa bậc 4 thành tổng của hai lũy thừa bậc 4. Và một cách tổng quát không thể phân tích hai lũy thừa với số mũ lớn hơn 2 thành tổng của hai lũy thừa với cùng số mũ đó". Phát biểu này theo ngôn ngữ hiện đại tức là "phương trình $x^n + y^n = z^n$ không có nghiệm nguyên dương nào với bất kì n lớn hơn 2". Sau đó ông viết một cách thách thức rằng: "Tôi đã phát minh ta chân lý này bằng một chứng minh tuyệt diệu, nhưng lề sách quá chật nên không thể ghi lại được ".

Định lý Fermat sau cùng còn được gọi là Định lí lớn Fermat được đưa ra: "với mọi số tự nhiên $n > 2$, phương trình $x^n + y^n = z^n$ không có nghiệm nguyên dương". Fermat không để lại chứng minh của định lí. Người ta chỉ tìm thấy giấy tờ của Fermat chứng minh với $n = 4$, Bài toán Fermat là một trong những sự kiện lí thú nhất trong lịch sử toán học. Nó vẫn không được giải quyết triệt để trong nhiều thế kỉ sau đó. Bao nhiêu nhà toán học nổi tiếng đã đầu tư thời gian và công sức vào vấn đề này nhưng chỉ đạt được kết quả trong một số trường hợp riêng lẻ:

+) Euler đã chứng minh cho $n = 3$ (năm 1770).

+) A.Legendre (nhà toán học người Pháp, 1752-1833) đã chứng minh cho $n = 5$ (năm 1825).

+) Trường hợp $n = 6$ quy về $n = 3$ và tổng quát chỉ cần chứng minh định lí cho số mũ n nguyên tố.

+) Năm 1839, nhà toán học Pháp G.Lamé (1795-1870) đã chứng minh cho $n = 7$.

Kết quả đáng kể là của nhà toán học Đức E.Kummer (1810-1893) đã chứng minh được rằng định lí đúng với mọi $n \leq 100$. Sau đó nhờ máy tính điện tử, người ta đã kiểm tra được định lí với mọi số nguyên tố nhỏ hơn 100000 ...,

Nhà toán học trẻ Hà Lan G.Faltings (sinh năm 1954) đã có đóng góp mới cho định lí Fermat với việc chứng minh (năm 1983) rằng phương trình $x^n+y^n=z^n$ với $n>3$, nếu có nghiệm nguyên thì chỉ có hữu hạn nghiệm mà thôi.

Năm 1657, Fermat đã thử với phương trình Diophante $61x^2+1=y^2$ (Brahumagupta đã giải quyết được 1000 năm trước đó). Phương trình đã được giải quyết triệt để bởi Euler vào đầu thế kỉ 18 - người có công giải quyết một số phương trình Diophante khác.

Vào năm 1900, nhận ra tầm quan trọng của chúng, David Hilbert đã phát biểu các vấn đề Diophante như là vấn đề nổi tiếng thứ 10 của ông.

Điều có ý nghĩa đối với sự phát triển của toán học là trong khi đi tìm chứng minh của định lí Fermat, các nhà toán học đã sáng tạo ra những lí thuyết toán học mới, những phương pháp mới mà thời Fermat chưa biết tới. Đáng lưu ý là đã có nhiều "chứng minh" được công bố và sau đó được phát hiện là sai lầm (gần đây nhất là "chứng minh " năm 1988 của Miyaoka ở CHLB Đức).

Vì vậy, người ta không khỏi dè dặt đón nhận tin A.Wiles ở trường Đại học Cambridge (Anh) công bố vào ngày 23-6-1993. Bản chứng minh của định lí Fermat (dài khoảng 200 trang). Quả thật, chỉ một thời gian ngắn sau đó, nhiều nhà Toán học và cả Wiles đã phát hiện một thiếu sót trong chứng minh này. Và A.Wiles đã cùng học trò của mình là R.Taylor nhanh chóng sửa chữa được thiếu sót đó, qua bài báo được công bố ngày 7-10-1994. Như vậy, A.Wiles (cùng với R.Taylor) đã có vinh dự kết thúc một cuộc hành trình dài 3 thế kỉ đi tìm lời giải của một trong những bài toán khó nhất và hấp dẫn nhất từ xưa đến nay.

Các phương trình Diophante, ngoài những liên hệ về lí thuyết với những vấn đề khác, còn có những ứng dụng trong kĩ thuật; chẳng hạn phương trình Pell đã được ứng dụng rất nhiều trong thiên văn học.

Nói chung, giải phương trình Diophante, đặc biệt là phương trình Diophante

bậc cao là một bài toán rất khó. Nhiều khi ta gặp hai phương trình Diophante tương tự nhau, chỉ khác nhau về hệ số, mà phương trình này có vô số nghiệm, phương trình kia lại vô nghiệm; phương trình này rất dễ giải, trong khi phương trình kia lại rất khó giải, thậm chí chưa ai giải được. Nhiều phương trình mang tên người đã giải được nó. Rất nhiều phương trình Diophante giải bằng các phương pháp của toán học cao cấp; việc nghiên cứu về phương trình Diophante đã trở thành một lĩnh vực riêng được gọi là giải tích Diophante.

Chương 2

Định lí lớn Fermat

Trong chương này chúng ta sẽ xét Định lí lớn Fermat và một số phương trình Diophante cụ thể.

2.1. Định lí lớn Fermat

Với mọi số tự nhiên $n > 2$, phương trình $x^n + y^n = z^n$ (2.1)
không có nghiệm nguyên dương.

Lưu ý: Phương trình Diophante (2.1) có nghiệm tầm thường trong trường hợp một trong các biến x, y, z bằng 0.

2.2. Phương trình $x^2 + y^2 = z^2$

Không mất tính chất tổng quát, giả sử $x > 0; y > 0$. Nếu $d \mid x$ và $d \mid y$ thì $d \mid z$. Suy ra, nếu (x, y, z) là một nghiệm với $(x; y) = d$ thì $(x'; y'; z')$ cũng là một nghiệm với $x = dx'; y = dy'; z = dz'$, trong đó $(x'; y') = 1$.

Từ đó, ta giả thiết rằng $(x, y) = 1$. Nghiệm tổng quát là bội của nghiệm thỏa mãn điều kiện này.

Ta nhận thấy rằng, nếu: $\begin{cases} x \equiv 1(\mod 2) \\ y \equiv 1(\mod 2) \end{cases}$

Thế thì $z^2 \equiv 2(\mod 4)$, điều này vô lý. Suy ra x, y không cùng tính chẵn lẻ.

Từ đó ta có các giải thiết cho định lí sau:

Nghiệm tổng quát của phương trình
$x^2 + y^2 = z^2$ (2.2.1)
thỏa mãn các điều kiện $x > 0; y > 0; z > 0; (x; y) = 1; 2 \mid x$ (2.2.2) là
$x = 2ab; y = a^2 - b^2; z = a^2 + b^2$ (2.2.3).
trong đó a, b là các số nguyên dương không cùng tính chẵn lẻ $a > b > 0$ và
$(a; b) = 1$ (2.2.4).

Đây là tương ứng 1-1 giữa các giá trị của a, b với các giá trị của x, y, z.

Chứng minh. par Trước tiên ta giả thiết như (2.2.1) và (2.2.3), từ $2 \mid x$ và $(x; y) = 1$; y và z là lẻ và $(y; z) = 1$.
Suy ra $\frac{1}{2}(z - y)$ và $\frac{1}{2}(z + y)$ là các số nguyên và $(\frac{z-y}{2}; \frac{z+y}{2}) = 1$.
Từ phương trình (2.2.1) suy ra

$$x^2 = z^2 - y^2 \Leftrightarrow \frac{x^2}{4} = (\frac{z-y}{2})(\frac{z+y}{2}) \Leftrightarrow (\frac{x}{2})^2 = (\frac{z+y}{2})(\frac{z-y}{2})$$

Vế phải gồm hai hạng tử nguyên tố cùng nhau nên cùng là các số chính phương.
Suy ra $\frac{z-y}{2} = a^2; \quad \frac{z+y}{2} = b^2$. Trong đó $a > 0, b > 0, a > b, (a; b) = 1$.
Cũng có, $a + b \equiv a^2 + b^2 = z \equiv 1(\mod 2)$, a và b không cùng tính chẵn lẻ.

Vậy nghiệm bất kì của phương trình (2.2.1) phải thỏa mãn điều kiện (2.2.2) và có dạng (2.2.3) với a và b là các số thỏa mãn (2.2.4).

Tiếp theo, ta giả sử a, b là các số không cùng tính chẵn lẻ và thỏa mãn (2.2.4) thế thì

$$x^2 + y^2 = 4a^2b^2 + (a^2 - b^2)^2 = z^2, x > 0, y > 0, z > 0, 2 \mid z.$$

Nếu $(x; y) = d$ thì $d \mid z$ và ta có $d \mid y = a^2 - b^2; d \mid z = a^2 + b^2$. Suy ra $d = 1$ hoặc $d = 2$.
Lại do y là lẻ nên $d = 1$.

Cuối cùng, nếu y và z cho trước, ta sẽ tìm được a^2 và b^2, từ đó sẽ suy ra a, b. Như vậy các giá trị x, y, z khác nhau sẽ có các giá trị a, b khác nhau.
Lưu ý: Trong công thức tính nghiệm, x và y có thể đổi chỗ cho nhau.

□

2.3. Phương trình $x^4 + y^4 = z^2$

2.3.1. Định lý. *Phương trình*

$$x^4 + y^4 = z^2 \qquad (2.3.1)$$

không có nghiệm nguyên dương.

Chứng minh. Giả sử rằng u là số bé nhất sao cho phương trình

$$x^4 + y^4 = u^2, \quad x > 0, y > 0, u > 0 \qquad (2.4.2)$$

có nghiệm, thế thì $(x; y) = 1$. Vì nếu Giả sử x, y không nguyên tố cùng nhau, $(x; y) = d$, chúng ta chia hai vế phương trình cho $d^4 = (x; y)^4$ và thay u bởi $\frac{u}{d^2}$ thỏa mãn phương trình (2.4.2).

Suy ra ít nhất một trong hai số x, y là lẻ và
$u^2 = x^4 + y^4 \equiv 1(\mod 4)$
hoặc $u^2 = x^4 + y^4 \equiv 2(\mod 4)$.
Ta có $u^2 = x^4 + y^4 \equiv 2(\mod 4)$ là không thể.

Vậy u là lẻ và chỉ một trong hai số x và y là chẵn.
Nếu x là chẵn, từ Định lí 2.2.1 ta có

$$x^2 = 2ab; y^2 = a^2 - b^2; u = a^2 + b^2$$

$a > 0, b > 0, (a; b) = 1$, a và b không cùng tính chẵn lẻ.
Nếu a chẵn và b lẻ thì $y^2 = -1(\mod 4) \equiv 3(\mod 4)$, điều này là là vô lí.

Vậy a lẻ và b chẵn. Đặt $b = 2c$ ta có:

$$\left(\frac{x}{2}\right)^2 = ac, \qquad \text{với} (a; c) = 1$$

và ta đặt được $a = d^2; c = f^2; d > 0; f > 0; (d; f) = 1$ và d lẻ.

Như vậy $y^2 = a^2 - b^2 = d^4 - 4z^4 \Leftrightarrow y^2 + b^2 = a^2 \Leftrightarrow (2f^2)^2 + y^2 = (d^2)^2$.
Ap dụng Định lí 2.2.1 ta thu được:

$$2f^2 = 2lm, d^2 = l^2 + m^2, l > 0, m > 0, (l; m)$$

Suy ra $f^2 = lm; (l; m) = 1$.
Ta lại có $l = r^2; m = s^2; (r > 0; s > 0)$
suy ra $r^4 + s^4 = d^2$. Nhưng $d \leq d^2 = a \leq a^2 < a^2 + b^2 = u$.
Điều này mâu thuẫn với giả thiết u là số bé nhất thỏa mãn phương trình (2.3.1).

Vậy phương trình (2.3.1) không có nghiệm nguyên dương.

□

2.4. Phương trình $x^4 + y^4 = z^4$

Bằng cách đặt $Z = z^2$ ta được phương trình
$x^4 + y^4 = z^4$ (2.4.1) sẽ trở thành phương trình (2.3.1). Ta sẽ áp dụng Định lí 2.3.1 cho chứng minh Định lí Fermat với $n = 4$.

2.5. Một số khái niệm và tính chất trong trường $\mathbb{Q}(\rho)$

+, Số $\xi \in \mathbb{C}$ được gọi là số đại số nếu nó là nghiệm của đa thức $f(x) \in \mathbb{Z}[x]$.
+, Số $\xi \in \mathbb{C}$ được gọi là số nguyên đại số nếu nó là nghiệm của đa thức $f(x) \in \mathbb{Z}[x]$, có hệ tử cao nhất bằng 1.
+, Nếu ξ là nghiệm của đa thức $f(x) \in \mathbb{Z}[x]$ có bậc n và không là nghiệm của mọi đa thức khác trong $\mathbb{Z}[x]$ có bậc thấp hơn n thì ta nói ξ có bậc n.
+, Ta kí hiệu $\mathbb{Q}(\xi)$ là một mở rộng đại số của $\mathbb{Q}$.

Khi $n = 1$ thì $\xi \in \mathbb{Q}$, ta có $\mathbb{Q}(\xi) = Q$. Kí hiệu $\rho = \frac{1}{2}(-1 + i\sqrt{3}) \in \mathbb{C}$. Ta có $\rho^2 + \rho + 1 = 0$ nên ρ là nghiệm của phương trình $x^2 + x + 1 = 0$.

Vậy ρ là số nguyên đại số.
Ta có $\rho^2 = \frac{1}{2}(-1 - i\sqrt{3}); \rho^3 = 1; \rho^2 + \rho = -1$.

Xét $\xi = a + b\rho$ (với $a, b \in \mathbb{Z}$), khi đó

$$(\xi - a - b\rho)(\xi - a - b\rho^2) = 0$$

nên $\xi^2 - (2a - b)\xi + a^2 - ab + b^2 = 0$. Vì vậy ξ là số đại số bậc hai trên $\mathbb{Q}$. Ta sẽ nói ξ có dạng như trên là số nguyên trong $\mathbb{Q}(\rho)$.

Xét trên $\mathbb{Q}(\rho)$ ta sẽ có khái niệm sau

2.5.1. Định nghĩa. .
a) Số nguyên ξ trong $\mathbb{Q}(\rho)$ là chia hết cho số nguyên η khác 0 trong $\mathbb{Q}(\rho)$ nếu tồn tại số nguyên ζ trong $\mathbb{Q}(\rho)$ sao cho $\xi = \eta\zeta$. Khi đó ta cũng nói η là ước của ξ và kí hiệu $\eta \mid \xi$.
b) Số nguyên ϵ trong $\mathbb{Q}(\rho)$ được gọi là phần tử khả nghịch của $\mathbb{Q}(\rho)$ nếu $\epsilon \mid 1$.
c) Hai số nguyên ξ_1 và ξ_2 trong $\mathbb{Q}(\rho)$ thỏa mãn $\xi_1 \mid \xi_2$ và $\xi_2 \mid \xi_1$ được gọi là liên kết với nhau.
d) Số nguyên ξ trong $\mathbb{Q}(\rho)$ là số khác 0, không khả nghịch, chỉ có ước là các phần tử khả nghịch và liên kết với nó được gọi là phần tử nguyên tố trong $\mathbb{Q}(\rho)$.
e) Với mỗi số nguyên $\xi = a + b\rho$ trong $\mathbb{Q}(\rho)$ ta kí hiệu

$$N\xi = (a + b\rho)(a + b\rho^2) = a^2 - ab + b^2$$

và gọi $N\xi$ là chuẩn của ξ.

Ta có nhận xét sau:
Vì $\rho^2 = -1 - \rho$ nên $\eta = c + d\rho^2 = c + d(-1 - \rho) = (c - d) - d\rho$. Do đó η cũng là số nguyên trong $\mathbb{Q}(\rho)$.
$N\xi$ luôn là số dương nếu $\xi \neq 0$, vì

$$a^2 - ab + b^2 = (a - \frac{1}{2}b)^2 + \frac{3}{4}b^2 \geq 0$$

Với hai số nguyên ξ và β trong $\mathbb{Q}(\rho)$ ta luôn có

$$N(\xi\beta) = N(\xi)N(\beta).$$

2.5.2. Bổ đề. *Ta có khẳng định sau:*
a) Chuẩn của mọi phần tử khả nghịch bằng 1.
b) Mọi số nguyên trong $\mathbb{Q}(\rho)$ có chuẩn bằng 1 đều là phần tử khả nghịch.

Chứng minh. a) Giả sử ϵ là phần tử khả nghịch, như vậy tồn tại η để $\epsilon\eta = 1$ suy ra

$$N(\epsilon\eta) = N(\epsilon)N(\eta) = N(1) = 1 \Rightarrow N(\epsilon) \mid 1 \Rightarrow N(\epsilon) = 1$$

b) Giả sử $\xi = a + b\rho$ thỏa mãn $N\xi = N(a + b\rho) = 1$, do đó $a^2 - ab + b^2 = 1$.
Xét $\eta = a + b\rho^2$. Ta có $\xi\eta = (a + b\rho)(a + b\rho^2) = a^2 + ab\rho^2 + ab\rho + b^2\rho^3$
$= a^2 + ab(\rho^2 + \rho) + b^2 = a^2 - ab + b^2 = 1$, (Vì $\rho^2 + \rho = -1$).
Suy ra $\xi \mid 1$. Vậy ξ là phần tử khả nghịch.

□

2.5.3. Bổ đề. *Nếu số nguyên ξ trong $\mathbb{Q}(\rho)$ có chuẩn là một số nguyên tố thì ξ là phần tử nguyên tố trong $\mathbb{Q}(\rho)$*

Chứng minh. Giả sử ξ không là phần tử nguyên tố trong $\mathbb{Q}(\rho)$. Khi đó tồn tại các số nguyên $\beta = c + d\rho; \eta = u + v\rho$ trong $\mathbb{Q}(\rho)$ thỏa mãn
$\xi = \beta\eta$ (β và η không khả nghịch).
Ta có

$$N(\beta\eta) = N\beta N\eta = N\xi = p$$

(p là số nguyên tố). Vì $N\beta$ và $N\eta$ là các số nguyên, lại là ước của p nên hoặc $N\beta = \pm 1$ hoặc $N\eta = \pm 1$. Điều này mâu thuẫn, vì β và η đều không khả nghịch.
Vậy ξ là phần tử nguyên tố trong $\mathbb{Q}(\rho)$. □

Nhận xét:

+,Điều ngược lại không đúng, tồn tại những phần tử nguyên tố nhưng chuẩn của nó không là số nguyên tố, chẳng hạn 2 là phần tử nguyên tố trong $\mathbb{Q}(\rho)$ nhưng $N2 = 4$ không là số nguyên tố.

Thật vậy, ta đi chứng minh 2 là phần tử nguyên tố trong $\mathbb{Q}(\rho)$.
Giả sử

$$2 = (a + b\rho)(c + d\rho)$$

suy ra $N2 = 4 = (a^2 - ab + b^2)(c^2 - cd + d^2)$.
Nếu xảy ra

$$(a^2 - ab + b^2)(c^2 - cd + d^2) = 2$$

suy ra a và b đều là số chẵn (vì nếu ít nhất một trong hai số là số lẻ thì tổng $a^2 - ab + b^2$ là số lẻ)
Khi a, b đều chẵn suy ra $(a^2 - ab + b^2)$ chia hết cho 4 (vì mọi số hạng đều chia hết cho 4). Nhưng 2 lại không chia hết cho 4. Vậy điều này không xảy ra.
Từ đó ta có hoặc $(a^2 - ab + b^2) = 1$ hoặc $(c^2 - cd + d^2) = 1$. Nghĩa là phần tử 2 không có ước thực sự trong $\mathbb{Q}(\rho)$.

+ , Không phải mọi số nguyên tố trong $\mathbb{Z}$ đều là phần tử nguyên tố trong $\mathbb{Q}(\rho)$, chẳng hạn $3 = (1 - \rho)(1 - \rho^2)$, $N(1 - \rho) = 3$ và $N(1 - \rho^2) = 3$. Nên 3 không là phần tử nguyên tố trong $\mathbb{Q}(\rho)$.

2.5.4. Bổ đề. *Mọi số nguyên trong $\mathbb{Q}(\rho)$ khác 0, không khả nghịch đều là tích của các số nguyên tố trong $\mathbb{Q}(\rho)$.*

Chứng minh. Ta sẽ chứng minh bổ đề này theo hai bước
Bước 1: một số nguyên trong $\mathbb{Q}(\rho)$, khác 0, không khả nghịch luôn có ít nhất một ước nguyên tố trong $\mathbb{Q}(\rho)$.

Giả sử y là số nguyên trong $\mathbb{Q}(\rho)$, không là phần tử nguyên tố trong $\mathbb{Q}(\rho)$, khi đó tồn tại các số nguyên γ_1, β_1 trong $\mathbb{Q}(\rho)$ sao cho

$$y = \gamma_1\beta_1; \quad N\gamma_1 > 1; \quad N\beta_1 > 1$$

do $Ny = N\gamma_1 N\beta_2 \Rightarrow 1 < N\gamma_1 < Ny$.
Nếu γ_1 không là số nguyên tố thì

$$\gamma_1 = \gamma_2\beta_2; \quad N\gamma_2 > 1; \quad N\beta_2 > 1$$

và ta có $1 < N\gamma_2 < N\gamma_1$.
Thực hiện liên tiếp quá trình như trên ta nhận được $y = \gamma_k\beta_1\beta_2 \dots \beta_k$ thỏa mãn $Ny > N\gamma_1 > N\gamma_2 > \dots > 1$. Dãy $Ny, N\gamma_1, N\gamma_2, \dots, N\gamma_k$ là một dãy số nguyên dương giảm dần, vì vậy quá trình này phải chấm dứt sau một số hữu hạn bước.

Nghĩa là tồn tại r để $y = \gamma_r\beta_1 \dots \beta_r$ mà γ_r là phần tử nguyên tố trong $\mathbb{Q}(\rho)$. Như vậy tồn tại số nguyên γ_r trong $\mathbb{Q}(\rho)$ thỏa mãn $\gamma_r \mid y$.
Bước 2: Giả sử y là số nguyên khác 0, không khả nghịch trong $\mathbb{Q}(\rho)$. Theo chứng minh trên ta có $y = \pi_1\gamma_1$, với π_1 là số nguyên tố trong $\mathbb{Q}(\rho)$.
Xét γ_1 ta thấy có hai khả năng: hoặc γ_1 là phần tử khả nghịch hoặc $\gamma_1 = \pi_2\gamma_2$, trong đó π_2 là phần tử nguyên tố trong $\mathbb{Q}(\rho)$, thỏa mãn

$$N\gamma_2 < N\gamma_1.$$

Cứ tiếp tục quá trình như vậy, ta sẽ được dãy các số nguyên dương giảm dần $N\gamma_1 > N\gamma_2 > N\gamma_3 > \dots$ nên tồn tại số r để $N\gamma_r = 1$; khi đó γ_r là phần tử khả nghịch $\gamma_r = \epsilon$. Chọn $\pi'_r = \pi_r\epsilon$ ta có π'_r là phần tử nguyên tố.

Khi đó ta có $y = \pi_1\pi_2 \dots \pi_{r-1}\pi'_r$.

Bổ đề được chứng minh.

□

Tương tự như trong tập hợp các số nguyên, đối với tập các số nguyên trong $\mathbb{Q}(\rho)$ chúng ta cũng đưa ra khái niệm phép chia với dư, khái niệm đồng dư theo modulo một số nguyên tô nào đó.

2.5.5. Bổ đề. *Cho hai số nguyên tố bất kỳ* $w, \quad \gamma_1$ *với* $(\gamma_1 \neq 0)$ *trong* $\mathbb{Q}(\rho)$,

khi đó luôn tồn tại số nguyên k trong $\mathbb{Q}(\rho)$ sao cho

$$w = k\gamma_1 + \gamma_2$$

trong đó $N\gamma_2 < N\gamma_1$

Chứng minh. Giả sử

$$\begin{cases} w = a + b\rho \\ \gamma_1 = c + d\rho \end{cases}$$

thỏa mãn $a, b, c, d \in \mathbb{Z}, \quad c^2 + d^2 \neq 0.$

Ta có

$$\frac{w}{\gamma_1} = \frac{a + b\rho}{c + d\rho} = \frac{(a + b\rho)(c + d\rho^2)}{(c + d\rho)(c + d\rho^2)} = \frac{(ac + bd - ad) + (bc - ad)\rho}{c^2 - cd + d^2}$$

$$= \frac{ac + bd - ad}{c^2 - cd + d^2} + \frac{bc - ad}{c^2 - cd + d^2}\rho = R + S\rho$$

với $R, S \in \mathbb{Q}$.

Do R, S là các số hữu tỉ nên tồn tại các số nguyên x và y thỏa mãn

$$| R - x | \leq \frac{1}{2}; | S - y | \leq \frac{1}{2}$$

Khi đó ta có $\frac{w}{\gamma_1} - (x + y\rho) = (R - x) + (S - y)\rho$ thỏa mãn

$$(R - x)^2 - (R - x)(S - y) + (S - y)^2 \leq \frac{3}{4}.$$

Vì vậy, nếu đặt $k = x + y\rho$; $\gamma_2 = w - k\gamma_1$ ta có

$$N\gamma_2 = N(w - k\gamma_1) \leq \frac{3}{4}N\gamma_1 < N\gamma_1.$$

Bổ đề được chứng minh.

□

2.5.6. Định nghĩa. Nếu w, k, γ_1, γ_2 là các số nguyên trong $\mathbb{Q}(\rho)$ thỏa mãn $w = k\gamma_1 + \gamma_2$, ta nói w đồng dư với γ_2 theo modulo γ_1 và kí hiệu
$w \equiv \gamma_2(\mod \gamma_1)$.

2.5.7. Bổ đề. *Mọi số nguyên trong $\mathbb{Q}(\rho)$ đều thuộc về một trong ba lớp theo modulo $\lambda = 1 - \rho$, tương ứng có phần tử đại diện là $-1; 0; 1$. Nghĩa là nếu w là một số nguyên bất kì trong $\mathbb{Q}(\rho)$ với $\lambda = 1 - \rho$, ta luôn có*

$$w \equiv 1(\mod \lambda)$$

$$w \equiv 0(\mod \lambda)$$

$$w \equiv -1(\mod \lambda)$$

Chứng minh. Giả sử w là số nguyên bất kì trong $\mathbb{Q}(\rho)$ và $\lambda = 1 - \rho$.
Ta có

$$\begin{aligned} w &= a + b\rho = a + b(1 - \lambda) \\ &= a + b - b\lambda \equiv (a + b)(\mod \lambda). \end{aligned}$$

Do $3 = (1 - \rho)(1 - \rho^2) = \lambda(1 - \rho^2)$ nên $\lambda \mid 3$. Mặt khác $a + b$ là số nguyên nên ta có

$$\begin{array}{c} a + b \equiv 0(\mod 3) \\ a + b \equiv 1(\mod 3) \\ a + b \equiv 2(\mod 3) \equiv -1(\mod 3) \end{array}$$

suy ra

$$w \equiv 1(\mod \lambda)$$

$$w \equiv 0(\mod \lambda)$$

$$w \equiv -1(\mod \lambda).$$

Bổ đề được chứng minh.

□

Ta có một số ví dụ sau:

i) Số 3 là phần tử liên kết với λ^2 trong $\mathbb{Q}(\rho)$. Vì $\lambda^2 = (1-\rho^2) = 1-2\rho+\rho^2 = -3\rho$, trong đó $(-\rho)$ là phần tử khả nghịch.
ii) Tất cả các số $(1 - \rho); \pm(1 - \rho^2); \rho(1 - \rho)$ đều liên kết với λ trong $\mathbb{Q}(\rho)$.

2.6. Phương trình $x^3 + y^3 = z^3$

Ta có thể viết phương trình Fermat lớn dưới dạng

$$(x + y)(x + \rho y)(x + \rho^2 y) = z^3$$

và nghiên cứu các phương trình đó trong trường $\mathbb{Q}(\rho)$.

2.6.1. Định lý. *Phương trình* $\xi^3 + \eta^3 + \zeta^3 = 0 \quad (\xi \neq 0; \eta \neq 0; \zeta \neq 0)$ *không có nghiệm nguyên trong* $\mathbb{Q}(\rho)$. *Đặc biệt, phương trình* $x^3 + y^3 = z^3$ *không có nghiệm trong tập các số nguyên, trừ trường hợp tầm thường là một trong các ẩn* x, y, z *bằng* 0.

Trong các phần sau ta kí hiệu $\lambda = 1 - \rho$ là số nguyên tố. Ta giả thiết rằng $(\xi; \eta) = (\eta; \zeta) = (\zeta; \xi) = 1$, trong đó ξ, ζ, η là các số nguyên trong $\mathbb{Q}(\rho)$. Chúng ta sẽ chứng minh định lí trên thông qua việc chứng minh bốn bổ đề sau.

2.6.2. Bổ đề. *Nếu* λ *không là ước của số nguyên* ω *trong* $\mathbb{Q}(\rho)$, *thế thì* $\omega^3 \equiv \pm 1 (\mod \lambda^4)$.

Chứng minh. Theo bổ đề đã chứng minh, ta có $\omega \equiv 0 (\mod \lambda)$ hoặc $\omega \equiv 1 (\mod \lambda)$ hoặc $\omega \equiv -1 (\mod \lambda)$ và theo giả thiết $\lambda \not| \omega$ ta có
$\omega \equiv \pm 1 (\mod \lambda)$.
Ta có thể chọn $\alpha = \pm\omega$ thỏa mãn $\alpha \equiv 1 (\mod \lambda)$ và $\alpha = 1 + \beta\lambda$. Thế thì

$$\begin{aligned}
\pm(\omega^3 \mp 1) &= \alpha^3 - 1 \\
&= (\alpha - 1)(\alpha^2 + \alpha + 1) \\
&= (\alpha - 1)(\alpha^2 - \rho^2 + \alpha - \rho) \\
&= (\alpha - 1)(\alpha - \rho)(\alpha + \rho + 1) \\
&= (\alpha - 1)(\alpha - \rho)(\alpha - \rho^2) \\
&= \beta\lambda(\beta\lambda + 1 - \rho)(\beta\lambda + 1 - \rho^2)
\end{aligned}$$

$$=\beta\lambda(\beta\lambda+1)[\beta\lambda+(1-\rho)(1+\rho)]$$
$$=\beta\lambda^3(\beta+1)(\beta-\rho^2)$$

(theo cách đặt $1-\rho=\lambda$ và $1+\rho+\rho^2=0\Rightarrow\rho^2=-1-\rho$).
Từ $1-\rho^2=\lambda(1+\rho)=\lambda(-\rho^2)=-\lambda\rho^2$ suy ra $\rho^2\equiv 1(\mod\lambda)$. Nên

$$\beta(\beta+1)(\beta-\rho^2)\equiv\beta(\beta+1)(\beta-1)$$

Nhưng theo kết quả của Bổ đề 2.5.5, ta có: hoặc $\beta\equiv 0(\mod\lambda)$ hoặc $\beta\equiv\pm 1(\mod\lambda)$.
Tức là hoặc $\beta\equiv 0(\mod\lambda)$ hoặc $\beta\mp 1\equiv 0(\mod\lambda)$.
Suy ra $\beta(\beta+1)(\beta-1)\equiv 0(\mod\lambda)$ hay $\beta(\beta+1)(\beta-\rho^2)\equiv 0(\mod\lambda)$.
Do đó $\pm(\omega^3\mp 1)=\beta\lambda^3(\beta+1)(\beta-\rho^2)\equiv 0(\mod\lambda^4)$.

Vậy $\omega^3\equiv\pm 1(\mod\lambda^4)$. Định lý được chứng minh.

□

2.6.3. Bổ đề. *Nếu $\xi^3+\eta^3+\zeta^3=0$, thì một trong các số $\xi,\quad\eta,\quad\zeta$ chia hết cho λ trong $\mathbb{Q}(\rho)$.*

Chứng minh. Ta giả sử ngược lại, tức là $\xi^3+\eta^3+\zeta^3=0$ và $\lambda\not|\xi;\lambda\not|\eta;\lambda\not|\zeta$.
Theo Bổ đề 2.6.2

$$\lambda\not|\xi\Rightarrow\xi\equiv\pm 1(\mod\lambda^4)$$
$$\lambda\not|\eta\Rightarrow\eta\equiv\pm 1(\mod\lambda^4)$$
$$\lambda\not|\zeta\Rightarrow\zeta\equiv\pm 1(\mod\lambda^4)$$

khi đó $0=\xi^3+\eta^3+\zeta^3\equiv\pm 1\pm 1\pm 1(\mod\lambda^4)$. Từ đó suy ra hoặc
$\pm 1\equiv 0(\mod\lambda^4)$ hoặc $\pm 3\equiv 0(\mod\lambda^4)$.
Tức là hoặc$\lambda^4\mid 1$ hoặc $\lambda^4\mid 3$.
Vì λ không là phần tử khả nghịch nên ta thấy không xảy ra trường hợp $\lambda^4\mid 1$.
Tương tự theo nhận xét trên ta thấy 3 và λ^2 là hai phần tử liên kết nên 3 không

thể chia hết cho λ^4.
Điều đó cho thấy điều giả sử ở trên là sai. Bổ đề được chứng minh.

□

Theo Bổ đề 2.6.3 ta có thể giả sử $\lambda \mid \zeta$ và có $\zeta = \lambda^n\gamma$. Trong đó $\lambda \not\mid \gamma$. Thế thì $\lambda \not\mid \xi; \lambda \not\mid \eta$, vì theo Định lí 2.6.1 $(\eta;\zeta) = (\xi;\zeta) = (\xi;\eta) = 1$.
Chúng ta phải chứng minh không thể có

$$\xi^3 + \eta^3 + \lambda^{3n}\gamma^3 = 0 \qquad (2.6.1)$$

trong đó $(\xi;\eta) = 1; n \geq 1; \quad \lambda \not\mid \xi; \quad \lambda \not\mid \eta; \quad \lambda \not\mid \gamma \quad (2.6.2).$
Điều đó tương đương với việc chứng minh $\xi^3 + \eta^3 + \epsilon\lambda^{3n}\gamma^3 = 0 \quad (2.6.3)$ không thể xảy ra với ξ, η, γ thỏa mãn điều kiện (2.6.2) và một phần tử khả nghịch ϵ bất kì.

2.6.4. Bổ đề. *Nếu ξ, η, γ là các số nguyên trong $\mathbb{Q}(\rho)$ thỏa mãn (2.6.2) và (2.6.3) thì $n \geq 2$.*

Chứng minh. Từ Bổ đề 2.6.2 ta có:

$$-\epsilon\lambda^{3n}\gamma^3 = \xi^3 + \eta^3 \equiv \pm 1 \pm 1 (\mod \lambda^4)$$

Nếu ξ và η cùng dấu, thì $-\epsilon\lambda^{3n}\gamma^3 \equiv \pm 2 (\mod \lambda^4)$. Điều này vô lí vì $\lambda \not\mid 2$. Suy ra ξ và η trái dấu và do đó

$$-\epsilon\lambda^{3n}\gamma^3 \equiv 0 (\mod \lambda^4),$$

từ điều kiện $\lambda \not\mid \gamma$ suy ra $n \geq 2$.

2.6.5. Bổ đề. *Nếu biểu thức (2.6.3) thỏa mãn với $n = m > 1$ thì nó sẽ phải thỏa mãn với $n = m - 1$.*

Chứng minh. Giả thiết (2.6.3):

$$\xi^3 + \eta^3 + \epsilon\lambda^{3n}\gamma^3 = 0, \qquad (n = m)$$
$$\Leftrightarrow -\epsilon\lambda^{3m}\gamma^3 = \xi^3 + \eta^3 = (\xi + \eta)(\xi^2 - \xi\eta + \eta^2)$$
$$\Leftrightarrow -\epsilon\lambda^{3m}\gamma^3 = (\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta)(2.6.4)$$

Do $m \geq 2; 3m > 3$ nên vế trái của (2.6.4) chia hết cho λ^4, suy ra vế phải cũng chia hết cho λ^4.

Nên ít nhất một trong ba nhân tử của vế phải phải chia hết cho λ^2. Giả sử nhân tử đó là $\xi + \eta$ nghĩa là $\xi + \eta \equiv 0(\mod \lambda^2)$.

Ta thấy $\eta, \quad \rho\eta, \quad \rho^2\eta\lambda$ là ba phần tử liên kết với nhau vì ρ là phần tử khả nghịch. Nên nếu $(\xi + \eta)$ chia hết cho λ thì cả hai phần tử $(\xi + \rho\eta)$ và $(\xi + \rho^\eta)$ cũng chia hết cho λ. Tuy nhiên khi đó nhân tử $(\xi + \rho\eta)$ không chia hết cho λ^2. Thật vậy, giả sử ngược lại ta có

$$(\xi + \rho\eta) \equiv 0(\mod \lambda^2)$$

suy ra $\eta - \rho\eta = \eta(1 - \rho) = \eta\lambda \equiv 0(\mod \lambda^2) \Rightarrow \eta \equiv 0(\mod \lambda)$.

Vô lí vì $\lambda \not| \eta$.

Tương tự ta cũng chứng minh được $(\xi + \rho^2\eta)$ không chia hết cho λ^2.

Như vậy hai nhân tử còn lại là $(\xi + \rho\eta)$ và $(\xi + \rho^2\eta)$ cần phải đồng thời chia hết cho λ và cùng chia hết cho λ^2.

Vậy thì

$$\begin{cases} \xi + \eta = \lambda^{3m-2}k_1 & (1) \\ \xi + \rho\eta = \lambda k_2 & (2) \\ \xi + \rho^2\eta = \lambda k_3 & (3) \end{cases} \qquad (2.6.5)$$

trong đó λ không là ước của k_1, k_2, k_3.

Lấy phương trình (2) trừ phương trình (3) ta có: $\rho\eta(1 - \rho) = \lambda(k_2 - k_3)$, nên $\rho\eta = k_2 - k_3$.

Nhân phương trình (3) với ρ, phương trình (2) với ρ^2 rồi trừ hai phương trình cho nhau ta có

$$\rho\xi - \rho^2\xi = \lambda(k_3\rho - k_2\rho^2) \Leftrightarrow \rho\xi(1 - \rho = \rho\xi\lambda)$$

suy ra $k_3\rho - k_2\rho^2 = \rho\xi$.

Nếu $\delta \mid k_2$ và $\delta \mid k_3$ thì $\delta \mid (k_2 - k_3) = \rho\eta$ và $\delta \mid \rho k_3 - \rho^2 k_2 = \rho\xi$, suy ra $\delta \mid \xi$ và $\delta \mid \eta$. Thế thì ρ khả nghịch và $(k_2, k_3) = 1$. Tương tự ta cũng có $(k_1, k_2) = 1$ và $(k_1, k_3) = 1$.

Thay (2.6.5) vào (2.6.4), ta thu được $-\epsilon\gamma^3 = k_1k_2k_3$;do k_1, k_2, k_3 là nguyên tố cùng nhau từng đôi một nên mỗi phần tử k_1, k_2, k_3 là liên kết với luỹ thừa bậc 3 của một phần tử nào đó.

Khi đó

$$\begin{cases} \xi + \eta = \lambda^{3m-2}k_1 = \epsilon_1\lambda^{3m-2}\theta^3, \\ \xi + \rho\eta = \epsilon_2\lambda\phi^3, \\ \xi + \rho^2\eta = \epsilon_3\lambda\psi^3, \end{cases}$$

trong đó θ, ϕ, ψ không có ước chung và không chia hết cho λ, và $\epsilon_1, \epsilon_2, \epsilon_3$ là các phần tử khả nghịch. Điều này dẫn đến:

$$0 = (1 + \rho + \rho^2)(\xi + \eta)$$

$$=\xi + \eta + \rho(\xi + \rho\eta) + \rho^2(\xi + \rho^2\eta)$$

$$=\epsilon_1\lambda^{3m-2}\theta^3 + \epsilon_2\rho\lambda\phi^3 + \epsilon_3\rho\lambda^2\psi^3$$

suy ra $\phi^3 + \epsilon_4\psi^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0 \qquad (2.6.6)$.

Trong đó $\epsilon_4 = \dfrac{\epsilon_3}{\epsilon_2}\rho; \quad \epsilon_5 = \dfrac{\epsilon_1}{\epsilon_2\rho}$ và ϵ_4, ϵ_5 là các phần tử khả nghịch.

Từ đó suy ra với $m \geq 2$, $\phi^3 + \epsilon_4\psi^3 \equiv 0(\mod \lambda^2)$

(Thực ra là $\phi^3 + \epsilon_4\psi^3 \equiv 0(\mod \lambda^3)$), nhưng $\lambda \not| \phi$ và $\lambda \not| \psi$ nên theo Bổ đề 2.6.2 ta có

$$\phi^3 \equiv \pm 1(\mod \lambda^2); \varphi^3 \equiv \pm 1(\mod \lambda^2).$$

Nên $\pm 1 \pm \epsilon^4 \equiv 0 \pm 1(\mod \lambda^2)$, trong đó ϵ^4 là ± 1 hoặc $\pm\rho$ hoặc $\pm\rho^2$.

Như vậy ta thấy $\pm 1 \pm \rho, \pm 1 \pm \rho^2$ không thể chia hết cho λ^2 vì chúng là những phần tử liên kết với 1 hoặc λ. Từ đó suy ta $_4 = \pm 1$

Nhưng $\pm 1 \pm \rho$ và $\pm 1 \pm \rho^2$ đều không chia hết cho λ^2. Vì chúng là các phần tử liên kết của 1 hoặc của λ. Vậy $\epsilon_4 = \pm 1$.

Nếu $\epsilon_4 = 1$ thì (2.6.6) là một phương trình cần tìm.

Nếu$\epsilon_4 = -1$ ta sẽ thay ψ bởi $-\psi$.

Nghĩa là cả hai trường hợp đều cho ta lũy thừa của λ là $3(m-1)$. Bổ đề được chứng minh.

□

Từ Bổ đề 2.6.5 ta suy ra kết quả của Định lý 2.6.1.

2.7. Phương trình $x^3 + y^3 = 3z^3$

2.7.1. Định lý. *Phương trình $x^3 + y^3 = 3z^3$ không có nghiệm nguyên, trừ nghiệm tầm thường khi $z = 0$.*

Chứng minh. Ta sẽ chứng minh định lí này tương tự như Định lí 2.6.1. Vì 3 là một liên kết với λ^2. Ta sẽ chứng minh phương trình

$$\xi^3 + \eta^3 + \epsilon\lambda^{3n+2}\gamma^3 = 0 \qquad (2.7.1)$$

không có nghiệm nguyên trong $\mathbb{Q}(\rho)$, với $(\xi;\eta) = 1, \lambda \nmid \gamma$ thông qua việc chứng minh hai mệnh đề

a) Nếu (2.7.1) có nghiệm thì $n > 0$;

b) Nếu (2.7.1) có nghiệm với $n = m \geq 1$, thì nó phải có nghiệm với $n = m-1$ và từ đó ta sẽ chỉ ra mâu thuẫn nếu (2.7.1) có lời giải với n bất kỳ.

Thật vậy, với $n = m$, ứng dụng quá trình chứng minh của Bổ đề 2.6.5 ta có

$$(\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta) = -\epsilon\lambda^{3m+2}\gamma^3$$

suy ra một trong các nhân tử ở vế trái chia hết cho λ và do đó lập luận tương tự như trong Bổ đề 2.6.5 ta có mọi nhân tử đều chia hết cho λ. Vậy $m > 0$. Từ đó suy ra $3m + 2 > 3$ và một trọng các nhân tử phải chia hết cho λ^2. Theo lập luận trong 2.6 thì chỉ có một nhân tử chia hết cho λ^2. Chúng ta có thể biểu diễn

$$\begin{cases} \xi + \eta = \lambda^{3m} k_1, \\ \xi + \rho\eta = \lambda k_2, \\ \xi + \rho^2\eta = \lambda k_3. \end{cases}$$

trong đó k_1, k_2, k_3 đôi một nguyên tố cùng nhau và không chia hết cho λ.

Tương tự như mục 2.5 ta có $-\epsilon\gamma^3 = k_1k_2k_3$ và k_1, k_2, k_3 là liên kết với luỹ thừa bậc ba của một phần tử nào đó. Vậy:

$$\begin{cases} \xi + \eta = \epsilon_1\lambda^{3m}\theta^3, \\ \xi + \rho\eta = \epsilon_2\lambda\phi^3, \\ \xi + \rho^2\eta = \epsilon_3\lambda\psi^3. \end{cases}$$

Theo đó ta có

$$0 = \xi + \eta + \rho(\xi + \rho\eta) + \rho^2(\xi + \rho^2\eta)$$

$$=\epsilon_1\lambda^{3m}\theta^3 + \epsilon_2\rho\lambda\phi^3 + \epsilon_3\rho^2\lambda\psi^3$$

và $\phi^3 + \epsilon_4\psi^3 + \epsilon_5\lambda^{3m-1}\theta^3 = 0$. Với $\epsilon_4 = \dfrac{\epsilon_3\rho}{\epsilon_2}; \epsilon_5 = \dfrac{\epsilon_1}{\epsilon_2\rho}$ là các phần tử khả nghịch.

Các phần còn lại trong chứng minh được thực hiện tương tự như trong quá trình chứng minh Định lí 2.6.1.

□

2.8. Phương trình $x^3 + y^3 + z^3 = t^3$

2.8.1. Phương trình $x^3 + y^3 + z^3 = t^3$

.

Xét phương trình $x^3 + y^3 + z^3 = t^3$. (2.8.1)

Đặt $z = -u; t = v$ ta được

$$x^3 + y^3 + z^3 = t^3 \Leftrightarrow x^3 + y^3 = u^3 + v^3 \qquad (2.8.2).$$

Đặt $x = X - Y; y = X + Y; u = U - V; v = U + V$. Khi đó (2.8.2) có dạng

$$(X-Y)^3+(X+Y)^3=(U-V)^3+(U+V^3)$$
$$\Leftrightarrow X^3+3XY^2=U^3+3UV^2$$
$$\Leftrightarrow X(X^2+3Y^2)=U(U^2+3V^2) \qquad (2.8.3).$$

Giả sử X, Y không đồng thời bằng 0, ta viết

$$\frac{U+V\sqrt{(-3)}}{X+Y\sqrt{(-3)}}=a+b\sqrt{(-3)} \qquad (*)$$
$$\frac{U-V\sqrt{(-3)}}{X-Y\sqrt{(-3)}}=a-b\sqrt{(-3)} \qquad (**)$$

trong đó a, b là các số hữu tỉ. Từ (*) và (**) suy ra

$$\begin{cases} U=aX-3bY \\ V=bX+aY \end{cases} \qquad (2.8.4)$$

thay vào (2.8.3) ta được

$$X=U(a^2+3b^2)$$

Từ (*) và (**) và (2.8.4) ta được

$$cX=dY.$$

Trong đó $c=a(a^2+3b^2)-1, \quad d=3b(a^2+3b^2)$.

Nếu $c=d=0$ thì $b=0, a=1, X=U, Y=V$. Mặt khác

$$\begin{cases} X=\lambda d=3\lambda b(a^2+3b^2) \\ Y=\lambda c=\lambda\{a(a^2+3b^2)-1\} \end{cases} \qquad (2.8.5)$$

trong đó $\lambda \neq 0$.

Kết hợp với (2.8.4) ta thấy

$$\begin{cases} U=3\lambda b \\ V=\lambda\{a(a^2+3b^2)^2-a\} \end{cases} \qquad (2.8.6)$$

Như vậy trừ hai nghiệm tầm thường

$$X = Y = U = 0, \quad X = U; Y = V$$

thì mọi nghiệm hữu tỉ của (2.8.3) đều có dạng như (2.8.5) và (2.8.6) với các số hữu tỉ thích hợp λ, a, b.

Ngược lại, nếu λ, a, b là các số hữu tỉ bất kì và X, Y, U, V được xác định bởi các biểu thức (2.8.5) và (2.8.6) thì từ (2.8.4) ta có

$$U(U^2 + 3V^2) = 3\lambda b\{(aX - 3bY)^2 + 3(bX + aY)^2\}$$

$$=3\lambda b(a^2 + 3b^2)(X^2 + 3Y^2)$$

$$=\mathrm{X}(\mathrm{X}^2 + 3Y^2).$$

Như vậy ta đã chứng minh được định lí sau đây.

2.8.2. Định lý

.

Trừ các nghiệm tầm thường

$$x = y = 0, \quad u = -v; \text{ hoặc} x = u, \quad y = v \qquad (2.8.7)$$

các nghiệm hữu tỉ tổng quát của (2.8.2) có dạng sau:

$$\begin{cases} x = \lambda\{1 - (a - 3b)(a^2 + 3b^2)\} \\ y = \lambda\{(a + 3b)(a^2 + 3b^2) - 1\} \\ u = \lambda\{(a + 3b) - (a^2 + 3b^2)^2\} \\ v = \lambda\{(a^2 + 3b^2)^2 - (a - 3b)\} \end{cases} \qquad (2.8.8)$$

Trong đó λ, a, b là các số hữu tỉ bất kì, $\lambda \neq 0$.

Việc tìm thấy mọi nghiệm nguyên của (2.8.2) là rất khó. Các giá trị nguyên của a, b, λ trong (2.8.8) cho ta nghiệm nguyên, tuy nhiên có thể có các nghiệm nguyên của (2.8.2) là x, y, u, v nhưng $a, \quad b, \quad \lambda$ không là các số nguyên.

Ví dụ: Ta có $x = 1, y = 12, u = 9, v = 10.$ là nghiệm của (2.8.2) và các giá trị tương ứng $a = \frac{10}{19}, b = -\frac{7}{19}, \lambda = -\frac{361}{42}$.

Hoặc với $a = b = 1, \lambda = \frac{1}{3}$, ta có:

$$x = 3, y = 5, u = -4, v = 6$$

là nghiệm của (2.8.2).

Ta có thể chia ra một số nghiệm khác đơn giản của (2.8.1) hoặc (2.8.2) là

$$1^3 + 6^3 + 8^3 = 9^3$$

$$2^3 + 34^3 = 15^3 + 33^3$$

$$9^3 + 15^3 = 2^3 + 16^3.$$

Chương 3

Một số vấn đề mở rộng

Trong chương này ta sẽ nghiên cứu một kết quả mới tìm được và một vài bài tập về phương trình Diophante

3.1. Phương trình Diophante $2^x + 5^y = z^2$

3.1.1. Định lý. *Phương trình Diophante*

$$2^x + 5^y = z^2 \qquad (3.1.1)$$

có đúng hai nghiệm nguyên không âm là $(3; 0; 3)$ *và* $(2; 1; 3)$.

Chứng minh. Trường hợp $x = 0$, ta có phương trình $5^y = z^2 - 1$ hay

$$(z - 1)(z + 1) = 5^y$$

trong đó $z - 1 = 5^u$ và $z + 1 = 5^{y-u}; y > 2u$ và $u \in \mathbb{N}$.
Ta có phương trình

$$5^{y-u} - 5^u = 2 \Leftrightarrow 5^u(5^{y-2u} - 1) = 2$$

suy ra $5^u = 1$ và $(5^{y-2u} - 1) = 2$ hay $u = 0$ và $5^{y-2u} = 3$. Tức là $u = 0$ và $5^y = 3$, điều này không thể xảy ra.

Trường hợp $y = 0$, ta có phương trình $z^2 - 1 = 2^x$ hay

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

trong đó $z-1=2^v$ và $z+1=2^{x-v}; x>2v; v\in\mathbb{N}$.
Ta có phương trình

$$2^{x-v}-2^v=2$$

hay $2^v(2^{x-2v}-1)=2$, suy ra $2^v=2$ và

$$2^{x-v}-1=1,$$

vậy $2^v=2$ và $2^{x-v}=2$, thế thì $v=1$ và $x=3$.

Do đó $x=3; y=0; z=3$ hay $(3;0;3)$ là một nghiệm của phương trình Diophante $2^x+5^y=z^2$.

Trường hợp $x\geq 1, y\geq 1$, từ 3.1.1 ta thấy z lẻ và không chia hết cho 5.
Nếu $z\equiv\pm 1(\mod 5)$ thì ta có $z^2\equiv\pm 1(\mod 5)$;
Nếu $z\equiv\pm 2(\mod 5)$ thì ta có $z^2\equiv\pm 4(\mod 5)\equiv -1(\mod 5)$.

Như vậy $2^x=z^2-5^y(\pm 1)(\mod 5)$.
Nếu x là số lẻ $x=2k+1, k\in\mathbb{N}$, suy ra
$2^{2k+1}=2.4^k\equiv 2(-1)^k(\mod 5), \quad k\in\mathbb{N}$, loại trừ.
Nếu x là số chẵn ta có $x=2k, k\in\mathbb{N}$, khi đó
$2^{2k}=4^k=(5-1)^k\equiv(-1)^k(\mod 5)$. Điều này thỏa mãn. từ đó suy ra x là số chẵn.

Bây giờ ta xét $x=2k, k\in\mathbb{N}$. Từ phương trình (3.1.1) chúng ta có:
$z^2-2^{2k}=5^y$ hay

$$(z-2^k)(z+2^{2k})=5^y$$

trong đó $z-2^k=5^w$ và $z+2^k=5^{y-w}; y>2w$ và $w\in\mathbb{N}$.
Từ đó ta thu được $5^{y-w}-5^w=2.2^k\Leftrightarrow 5^w(5^{y-2w}-1)=2^{k+1}$
kéo theo $w=0$ và $5^{y-2w}-1=2^{k+1}$ (3.1.2).

Phương trình Diophante (3.1.2) là một phương trình Diophante cho bởi Catalan có dạng

$$a^b-c^d=1.$$

Năm 1952, Leveque đã chứng minh định lí chỉ ra rằng phương trình chỉ có nghiệm nguyên dương lớn hơn 1 là $a = 3, b = 2, c = 2$ và $d = 3$.
Điều này dẫn đến phương trình (3.1.2) chỉ có nghiệm khi $y = 1$. Suy ra ta có $2^{k+1} = 2^2$, trong đó $k = 1$ và như vậy $x = 2, y = 1, z = 3$.

Vậy phương trình (3.1.1) có đúng hai nghiệm $(3; 0; 3)$ và $(2; 1; 3)$. □

3.2. Một số bài tập giải phương trình Diophante

3.2.1. Bài tập. *Giải phương trình Diophante sau*

$$x^3 - 2y^3 - 4z^3 = 0 \qquad (3.2.1)$$

Giải. $x^3 - 2y^3 - 4z^3 = 0 \Leftrightarrow x^3 = 2y^3 + 4z^3 \Leftrightarrow x^3 = 2(y^3 + 2z^3)$
suy ra x^3 là số chẵn, thế thì x cũng là số chẵn.

Đặt $x = 2x'$. Khi đó
$x^3 = 2(y^3 + 4z^3) \Leftrightarrow 8x'^3 = 2(y^3 + 2z^3) \Leftrightarrow 4x'^3 = y^3 + 2z^3 \Leftrightarrow y^3 = 4x'^3 - 2z^3 \Leftrightarrow y^3 = 2(2x'^3 - z^3)$
suy ra y^3 là số chẵn và như vậy y là số chẵn.

Đặt $y = 2y'$ là tương tự như trên ta được z là số chẵn và $z = 2z'$. Suy ra phương trình (3.2.1) có dạng

$$(2x')^3 = 2[(2y')^3 + 2(2z')^3] \Leftrightarrow x'^3 = 2(y'^3 + 2z'^3).$$

Như vậy, nếu $(x; y; z)$ là một nghiệm của phương trình (3.2.1) thì $(x'; y'; z')$ hay $(\frac{x}{2}; \frac{y}{2}; \frac{z}{2})$ cũng là một nghiệm của phương trình (3.2.1).

Quá trình này tiếp diễn mãi được $(\frac{x}{2n}; \frac{y}{2n}; \frac{z}{2n})$ với $n \in \mathbb{N}$ cũng là nghiệm. Do đó $(x; y; z)$ chỉ có thể là $(0; 0; 0)$.

Vậy phương trình Diophante (3.2.1) có nghiệm duy nhất $(0; 0; 0)$.

3.2.2. Bài tập. *Tìm nghiệm nguyên của phương trình*

$$1! + 2! + 3! + ... + x! = y^2$$

Giải.

Thử $x = 1$ có $1! = y^2 \Leftrightarrow y^2 = 1 \Leftrightarrow y = \pm 1$, vậy phương trình có nghiệm $(1; 1), (1; -1)$.

Thử $x = 2$ có $1! + 2! = y^2 \Leftrightarrow y^2 = 5$, phương trình vô nghiệm.

Thử $x = 3$ có $1! + 2! + 3! = y^2 \Leftrightarrow y^2 = 9 \Leftrightarrow y = \pm 3$, suy ra phương trình có nghiệm $(3; 3), (3; -3)$.

Thử $x = 4$ có $1! + 2! + 3! + 4! = y^2 \Leftrightarrow y^2 = 33$, suy ra phương trình vô nghiệm.

Với $x \geq 5$ ta có $1! + 2! + 3! + 4! = 33$ còn $5!, 6!, 7!, ...$ đều tận cùng là 0, vì vậy $1! + 2! + 3! + 4! + ... + x!$ tận cùng bằng 3 với $x \geq 5$, mà y^2 không thể tận cùng là 3. Do đó với $x \geq 5$ phương trình vô nghiệm.

Vậy phương trình Diophante đã cho có nghiệm:

$$(1; 1), (1; -1), (3; 3), (3; -3).$$

KẾT LUẬN

Trong luận văn này chúng tôi đã hoàn thành được những việc sau.

Trình bày khái niệm phương trình Diophante và khái quát lịch sử phát triển của nó. Trình bày Định lý Fermat sau cùng với một số phương trình Diophante dạng $x^2 + y^2 = z^2; x^4 + y^4 = z^4; x^3 + y^3 = 3z^3; x^3 + y^3 + z^3 = t^3$. Để hỗ trợ cho việc giải quyết một số phương trình trên chúng tôi phải dùng tới một số khái niệm và tính chất trong trường $\mathbb{Q}(\rho)$ - một mở rộng đại số của trường số hữu tỉ.

Những năm gần đây vẫn có nhiều kết quả mới đạt được trong quá trình nghiên cứu các phương trình Diophante khác nhau. Hướng phát triển tiếp theo của đề tài là nghiên cứu một số dạng cụ thể phương trình Diophante mà hiện nay vẫn chưa có lời giải.

Tài liệu tham khảo

[1] Hoàng Chúng (1993), *Số học bà chúa của Toán học*, Nhà xuất bản Đại học Quốc gia Hà Nội.

[2] Dumitru Acu (25 December, 2007), "On a diophantine equation", General Mathematics Vol. 15,No, (2007), pp.145-148.

[3] G. H. Hardy, E. M. Wright (1975), *An introduction to the theory of numbers*, Oxford at the clarendon press.

[4] M. B. Nathanson (1999), *Elementary methods in number theory*, Springer.