ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VŨ PHÚ BÌNH

PHƯƠNG TRÌNH DIOPHANTINE DẠNG $x^2 - Dy^2 = \pm 4$

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2018

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VŨ PHÚ BÌNH

PHƯƠNG TRÌNH DIOPHANTINE DẠNG
$x^2 - Dy^2 = \pm 4$

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 8460113

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS. Nông Quốc Chinh

THÁI NGUYÊN - 2018

Mục lục

Lời nói đầu

Xét phương trình có dạng

$$f(x_1, x_2, ..., x_n) = 0 \tag{1}$$

với $n \geq 2$ và $f(x_1, x_2, ..., x_n)$ là một đa thức nguyên một hoặc nhiều biến được gọi là phương trình nghiệm nguyên hay phương trình Diophantine, nó được gọi theo tên nhà toán học Hy Lạp ở thế kỉ thứ 3 sau công nguyên. Phương trình Diophantine là một trong những dạng toán lâu đời nhất của Toán học và nhận được nhiều sự quan tâm nghiên cứu của nhiều nhà toán học. Từ Euclid, Diophantus, qua Fibonacci, Pell rồi đến Fermat, Euler, Lebesgue... và thời hiện đại là Gelfold, Matiasevic, Shenzel, Serpinsky... Phương trình Diophantine đã trải qua một lịch sử phát triển lâu dài.

Thông qua việc giải các phương trình Diophantine, các nhà toán học đã tìm ra được những tính chất thú vị của số nguyên, số hữu tỷ, số đại số. Giải phương trình Diophantine đã đưa đến sự ra đời của Liên phân số, Lý thuyết đường cong elliptic, Lý thuyết xấp xỉ Diophantine, Thặng dư bình phương, Số học modular...

Các bài toán về phương trình Diophantine không có quy tắc giải tổng quát, hoặc nếu có cũng chỉ là đối với các dạng đơn giản. Mỗi phương trình với dạng riêng của nó đòi hỏi một cách giải đặc trưng phù hợp. Chính vì vậy, phương trình Diophantine vẫn thường xuyên xuất hiện dưới các hình thức khác nhau và luôn được đánh giá là khó do tính không mẫu mực của nó. Một dạng đặc biệt của phương trình Diophante là $x^2 - Dy^2 = N$ rất được quan tâm và có rất nhiều kết quả xung quanh dạng phương trình này. Gần đây một kết quả thú vị của A. Tekcan về phương trình $x^2 - Dy^2 = \pm 1$ và $x^2 - Dy^2 = \pm 4$ đã được công bố. Mục đích của luận văn là trình bày lại các kết quả về cấu trúc

nghiệm của các phương trình $x^2 - Dy^2 = \pm 1$ và $x^2 - Dy^2 = \pm 4$.
Luận văn gồm 2 chương:
Chương 1: Chúng tôi giới thiệu các kết quả về liên phân số, giản phân và cấu trúc nghiệm của phương trình Diophantine $x^2 - Dy^2 = \pm 1$.
Chương 2: Chúng tôi trình bày lại cấu trúc nghiệm của phương trình Diophantine $x^2 - Dy^2 = \pm 4$ và một số ứng dụng trong toán phổ thông.

Luận văn này được thực hiện và hoàn thành vào tháng 5 năm 2018 tại trường Đại học Khoa học - Đại học Thái Nguyên. Qua đây, tác giả xin bày tỏ lòng biết ơn sâu sắc tới PGS.TS. Nông Quốc Chinh, người đã tận tình hướng dẫn tác giả trong suốt quá trình làm việc để hoàn thành luận văn này. Tác giả xin gửi lời cảm ơn chân thành đến Khoa Toán - Tin, Trường Đại học Khoa học - Đại học Thái Nguyên, đã tạo mọi điều kiện để giúp tác giả học tập và hoàn thành luận văn cũng như chương trình thạc sĩ. Tác giả cũng xin gửi lời cảm ơn tới tập thể lớp cao học, khóa 05/2016 - 05/2018 đã động viên giúp đỡ tác giả trong quá trình học tập và hoàn thành luận văn này. Đồng thời tác giả xin gửi lời cảm ơn tới Ban giám hiệu, các đồng nghiệp tại trường THPT Nguyễn Khuyến, huyện Vĩnh Bảo, Hải Phòng và gia đình bạn bè đã tạo điều kiện tốt nhất cho tác giả trong suốt quá trình học tập và hoàn thành luận văn.

Tác giả

Vũ Phú Bình

Chương 1

Phương trình Diophantine $x^2 - Dy^2 = \pm 1$

Trong chương này, chúng tôi trình bày một số kết quả về liên phân số, một số cách giải phương trình Diophantine dạng $x^2 - Dy^2 = \pm 1$ và ứng dụng của nó. Các kết quả trong chương này được viết theo các tài liệu [1] và [2].

1.1 Liên phân số và giản phân

1.1.1 Liên phân số hữu hạn và giản phân

Định nghĩa 1.1.1. Cho $\{a_i\}_{i=0}^{\infty}$ và $\{b_i\}_{i=0}^{\infty}$ là dãy các số thực.

(i) Biểu thức có dạng

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \ldots}} \tag{1.1}$$

được gọi là *một liên phân số* của hai dãy số $\{a_i\}_{i=0}^{\infty}$ và $\{b_i\}_{i=0}^{\infty}$.

(ii) Dãy các biểu thức $u_0 = a_0, u_1 = a_0 + \dfrac{b_0}{a_1}, u_2 = a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2}}, \ldots,$ được gọi là *các giản phân* của hai dãy số $\{a_i\}_{i=0}^{\infty}$ và $\{b_i\}_{i=0}^{\infty}$.

(iii) Phần tử u_n xác định như trên được gọi là *giản phân thứ n* của hai dãy số $\{a_i\}_{i=0}^{\infty}$ và $\{b_i\}_{i=0}^{\infty}$.

Chú ý 1.1.2. (i) Nếu n là hữu hạn và $b_0 = b_1 = \ldots = b_n = 1$ ta kí hiệu liên phân số của hai dãy số $\{a_i\}_{i=0}^{n}$ và $\{b_i\}_{i=0}^{n}$ là $[a_0; a_1, \ldots, a_n]$.
(ii) Nếu $a_0 \in \mathbb{Z}$ và $a_1, ..., a_n$ là các số nguyên dương thì ta nói $[a_0; a_1, ..., a_n]$ là

một *liên phân số hữu hạn* có độ dài n.

(iii) Một liên phân số hữu hạn là một số hữu tỷ.

Với hai dãy số thực $\{a_i\}_{i=0}^{\infty}$ và $\{b_i\}_{i=0}^{\infty}$ ta xét hai dãy số $\{p_n\}_{n=-1}^{\infty}$ và $\{q_n\}_{n=-1}^{\infty}$ như sau:

$$p_{-1} = 1, p_0 = a_0, \dots, p_{n+1} = a_{n+1}p_n + b_n p_{n-1}.$$

$$q_{-1} = 0, q_0 = 1, \dots, q_{n+1} = a_{n+1}q_n + b_n q_{n-1}.$$

Khi đó mối quan hệ giữa giản phân thứ n của hai dãy số $\{a_i\}_{i=0}^{\infty}$ và $\{b_i\}_{i=0}^{\infty}$ với thương thứ n của hai dãy số $\{p_n\}_{n=-1}^{\infty}$ và $\{q_n\}_{n=-1}^{\infty}$ được thể hiện trong bổ đề sau.

Bổ đề 1.1.3. *Với các kí hiệu và giả thiết như trên ta có giản phân* $u_n = \dfrac{p_n}{q_n}$ *với mọi* $n \geq 0$.

Chứng minh. Ta chứng minh đẳng thức trên là đúng bằng quy nạp theo n. Thật vậy, với $n = 0$ và $n = 1$ thì hiển nhiên kết quả là đúng. Giả sử quy nạp đúng cho n, nghĩa là ta có $u_n = \dfrac{p_n}{q_n}$. Thay a_n trong biểu thức u_n bởi $a_n + \dfrac{b_n}{a_{n+1}}$ ta thu được u_{n+1}. Theo định nghĩa ta có p_n, q_n không phụ thuộc vào b_n và a_{n+1} nên từ công thức truy hồi

$$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + b_{n-1}p_{n-2}}{a_n q_{n-1} + b_{n-1}q_{n-2}}$$

ta có

$$\begin{aligned}
u_{n+1} &= \frac{(a_n + \dfrac{b_n}{a_{n+1}})p_{n-1} + b_{n-1}p_{n-2}}{(a_n + \dfrac{b_n}{a_{n+1}})q_{n-1} + b_{n-1}q_{n-2}} \\
&= \frac{(a_n a_{n+1} + b_n)p_{n-1} + a_{n+1}b_{n-1}p_{n-2}}{(a_n a_{n+1} + b_n)q_{n-1} + a_{n+1}b_{n-1}q_{n-2}} \\
&= \frac{a_{n+1}(a_n p_{n-1} + b_{n-1}p_{n-2}) + b_n p_{n-1}}{a_{n+1}(a_n q_{n-1} + b_{n-1}q_{n-2}) + b_n q_{n-1}} \\
&= \frac{a_{n+1}p_n + b_n p_{n-1}}{a_{n+1}q_n + b_n q_{n-1}} \\
&= \frac{p_{n+1}}{q_{n+1}}.
\end{aligned}$$

Bổ đề được chứng minh. □

Bổ đề 1.1.3 cho ta một công thức tính các giản phân qua thương của các dãy số. Mệnh đề tiếp theo chỉ ra rằng mọi số hữu tỷ đều biểu diễn được dưới dạng một liên phân số hữu hạn và biểu diễn đó là duy nhất. Trước tiên ta nhắc lại thuật toán Euclid tìm ước chung lớn nhất của hai số nguyên.

Chú ý 1.1.4. (i) Cho các số nguyên $a, b \in \mathbb{Z}, b > 0$. Khi đó như đã biết chúng ta có thể tìm được ước chung lớn nhất của a và b bằng cách thức hiện thuật toán Euclid như sau:

$$\begin{aligned}
&a = a_0 b + r_1, 0 < r_1 < b\\
&b = a_1 r_1 + r_2, 0 < r_2 < r_1,\\
&r_1 = a_2 r_2 + r_3, 0 < r_3 < r_1,\\
&\ldots,\\
&r_{n-2} = a_{n-1} r_{n-1} + r_n, 0 < r_n < r_{n-1},\\
&r_{n-1} = a_n r_n,
\end{aligned}$$

quá trình này phải dừng và sau hữu hạn bước ta có $\gcd(a, b) = r_n$.

(ii) Từ thuật toán trên ta thu được hai dãy số nguyên hữu hạn là $\{a_i\}_{i=0}^n$ và

$$b_0 = b_1 = \ldots = b_n = 1.$$

Khi đó các giản phân của $\{a_i\}_{i=0}^n$ và $\{b_i\}_{i=0}^n$ là

$$u_0 = a_0 = [a_0], u_1 = a_0 + \frac{1}{a_1} = [a_0; a_1], \ldots, u_n = ... = [a_0; a_1, a_2, \ldots, a_n].$$

(iii) Từ thuật toán trên ta cũng thu được các dãy truy hồi là

$$p_0 = a_0, p_1 = a_1 p_0 + 1, \ldots, p_n = a_n p_{n-1} + p_{n-2}$$

và

$$q_0 = 1, q_1 = a_1, \ldots, q_n = a_n q_{n-1} + q_{n-2}.$$

Ta có tính chất quan trọng của số hữu tỷ thể hiện trong mệnh đề sau:

Mệnh đề 1.1.5. *Mỗi số hữu tỷ đều được biểu diễn dưới dạng một liên phân số hữu hạn.*

Chứng minh. Cho a/b là một số hữu tỷ với $b > 0$. Theo thuật toán tìm ước chung lớn nhất và công thức giản phân ta có

$$
\begin{aligned}
\frac{a}{b} &= a_0 + \cfrac{1}{\cfrac{b}{r_1}} \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cfrac{r_1}{r_2}}} \\
&\dots \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_{n-2} + \cfrac{\dots}{a_{n-1} + \cfrac{1}{a_n}}}}}}.
\end{aligned}
$$

Vậy mọi số hữu tỷ a/b đều viết được thành một liên phân số hữu hạn là

$$a/b = [a_0; a_1, \dots, a_n].$$

Mệnh đề được chứng minh. □

Như chúng ta đã biết biểu diễn của một số hữu tỷ dưới dạng phân số không là duy nhất. Tuy nhiên mệnh đề tiếp theo chỉ ra rằng biểu diễn của một số hữu tỷ thành liên phân số là duy nhất.

Mệnh đề 1.1.6. *Biểu diễn số hữu tỷ thành một liên phân số hữu hạn dạng $[a_0; a_1, \dots, a_n]$ là duy nhất.*

Chứng minh. Cho a/b là một số hữu tỷ và giả sử

$$[a_0; a_1, \dots, a_n] = \frac{a}{b} = [b_0; b_1, \dots, b_m].$$

Ta cần chứng minh $m = n$ và $a_i = b_i$, với mọi $i = 0, 1, \dots, n$. Thật vậy, với $n = 0$ ta có $a_0 = [b_0; b_1, \dots, b_m]$. Vì b_0 là phần nguyên của a_0 và a_0 là số nguyên nên $m = 0$ và $a_0 = b_0$. Giả sử quy nạp đúng cho $n - 1$, nghĩa là kết luận trên là đúng cho mọi liên phân số hữu hạn có độ dài nhỏ hơn n. Từ biểu thức

$$[a_0; a_1, \dots, a_n] = \frac{a}{b} = [b_0; b_1, \dots, b_m]$$

ta suy ra $a_0 = b_0$, vì đều là phần nguyên của cùng một số hữu tỷ. Khi đó ta có

$$[0; a_1, \ldots, a_n] = \frac{a}{b} - a_0 = [0; b_1, \ldots, b_n].$$

Do đó $[a_1; a_2, \ldots, a_n] = [b_1; b_2, \ldots, b_m]$. Theo giả thiết quy nạp ta có $n-1 = m-1$ và $a_i = b_i$, với mọi $i = 1, \ldots, n$. $\square$

Ví dụ 1.1.7. Xét số hữu tỷ 187/4, ta có

$$\begin{aligned} 187 &= 46.4 + 3, \\ 4 &= 1.3 + 1, \\ 3 &= 3.1. \end{aligned}$$

Do đó $\dfrac{187}{4} = [46; 1, 3]$.

1.1.2 Liên phân số vô hạn

Trong mục này chúng tôi tập trung trình bày các kiến thức về liên phân số vô hạn. Trong đó chúng tôi trình bày lại một tính chất tốt của liên phân số vô hạn đó là mọi số vô tỷ đều viết được dưới dạng một liên phân số vô hạn. Các kết quả trong mục này được viết theo các tài liệu [1].

Định nghĩa 1.1.8. (i) Liên phân số vô hạn là một biểu thức có dạng

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_s} \ddots}} \tag{1.2}$$

trong đó, q_0 là một số nguyên, q_s với $s = 1, 2, ...$ là các số nguyên dương và được kí hiệu là $[q_0; q_1, \ldots, q_s, \ldots]$.

(ii) Phần tử q_s được gọi là số thương hụt hay số hạng thứ s của liên phân số.