ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**NGUYỄN THỊ MÁT**

# PHƯƠNG TRÌNH DIOPHANT TRONG LỚP ĐỒNG DƯ BẬC HAI VÀ ÁP DỤNG

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

**THÁI NGUYÊN - 2016**

ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**NGUYỄN THỊ MÁT**

# PHƯƠNG TRÌNH DIOPHANT TRONG LỚP ĐỒNG DƯ BẬC HAI VÀ ÁP DỤNG

## LUẬN VĂN THẠC SĨ TOÁN HỌC

**Chuyên ngành : Phương pháp toán sơ cấp**
**Mã số : 60. 46. 01. 13**

NGƯỜI HƯỚNG DẪN KHOA HỌC:
**GS.TSKH. Nguyễn Văn Mậu**

**THÁI NGUYÊN - 2016**

# Mục lục

# MỞ ĐẦU

Chuyên đề "Phương trình Diophant trong lớp đồng dư bậc hai" là một nội dung quan trọng của số học. Các dạng toán liên quan đến đồng dư thường khó và phức tạp. Trong chương trình trung học phổ thông, những bài toán giải phương trình trong đồng dư thường rất khó và trừu tượng đối với hầu hết học sinh.

Trong các kỳ thi học sinh giỏi quốc gia, thi Olympic toán khu vực và quốc tế, các bài toán liên quan đến đồng dư cũng hay được đề cập và thường thuộc loại khó song chưa được dạy nhiều ở phổ thông, ít có trong các tài liệu tham khảo. Các bài toán về đồng dư trong chương trình phổ thông nhiều kiến thức chưa được đề cập đến.

Với mong muốn nâng cao trình độ nghiệp vụ chuyên môn, đáp ứng việc bồi dưỡng học sinh giỏi cùng với những lí do trên, tôi chọn đề tài: "Phương trình diophant trong lớp đồng dư bậc hai và áp dụng" để làm đề tài luận văn thạc sĩ của mình.

Chuyên đề "Phương trình Diophant trong lớp đồng dư bậc hai và áp dụng" gồm ba chương: Đồng dư và đồng dư bậc hai; Một số lớp phương trình Diophant trong lớp đồng dư bậc hai; các dạng toán liên quan đến đồng dư bậc hai. Các kết quả của luận văn được tham khảo từ [1] đến [7] và các bài toán chọn lọc từ các kì thi học sinh giỏi quốc gia, Olympic quốc tế.

Luận văn được hoàn thành dưới sự hướng dẫn khoa học đầy nhiệt tình, nghiêm túc và trách nhiệm của GS. TSKH Nguyễn Văn Mậu. Nhân dịp này, tác giả xin được bày tỏ lòng biết ơn chân thành và kính trọng sâu sắc đối với giáo sư - Người Thầy đã truyền đạt nhiều kiến thức quý báu cùng với kinh nghiệm nghiên cứu khoa học trong suốt thời gian tác giả theo học và nghiên cứu đề

tài. Đồng thời tác giả cũng xin bày tỏ lòng biết ơn sâu sắc đến Ban giám hiệu trường Đại học Khoa học - Đại học Thái Nguyên; Phòng Đào tạo, Khoa Toán - Tin, các anh em, bạn bè lớp K8B - Đại học Khoa học - Đại học Thái Nguyên; Ban giám hiệu trường THCS Thành Nhân - Ninh Giang, Hải Dương và gia đình đã tạo mọi điều kiện thuận lợi, động viên tác giả trong suốt quá trình học tập, công tác và thực hiện đề tài luận văn.

*Thái Nguyên, ngày 15 tháng 5 năm 2016*

**Tác giả luận văn**

**Nguyễn Thị Mát**

# Chương 1

# ĐỒNG DƯ VÀ ĐỒNG DƯ BẬC HAI

Trong chương này ta xét các tính chất cơ bản của đồng dư và đồng dư bậc hai và các dạng toán về phép chia hết và phép chia có dư (xem [2]-[5]).

## 1.1 Đồng dư và các lớp đồng dư

Trong phần này ta xét các lớp đồng dư bậc một và bậc hai theo modulo $m$, trong đó $m$ là số nguyên dương cho trước.

**Định nghĩa 1.1.1** (xem [2]-[5])**.** Cho $m$ là một số nguyên dương. Ta nói hai số nguyên $a, b$ là đồng dư với nhau theo modulo $m$ nếu trong phép chia $a$ và $b$ cho $m$ ta được cùng một số dư.
Ký hiệu

$$a \equiv b \pmod{m}. \tag{1.1}$$

Hệ thức (1.1) gọi là đồng dư thức.

**Định lý 1.1.2.** Định lý Thue *Cho $p$ là một số nguyên tố. Khi đó với mọi số nguyên $a$ thỏa mãn $p \nmid a$ luôn tồn tại $x, y \in \{1, 2, \ldots, [\sqrt{p}]\}$ sao cho $ax \equiv y \pmod{p}$ hoặc $ax \equiv -y \pmod{p}$.*

***Chứng minh.*** Ta định nghĩa

$$S = \{1, 2, \ldots, [\sqrt{p}]\} \times \{1, 2, \ldots, [\sqrt{p}]\},$$

$S$ chứa $([\sqrt{p}]+1)^2$ cặp có thứ tự. Bình phương hai vế của $\sqrt{p} < [\sqrt{p}]+1$ ta nhận được $p < ([\sqrt{p}]+1)^2$, vì thế $S$ có nhiều hơn $p$ phần tử. Giả sử cho trước $a \in \mathbb{Z}$ sao cho $p \nmid a$. Do $(x, y)$ biến thiên trên $S$, cho nên có nhiều hơn $p$ biểu thức dạng $ax-y$. Lưu ý rằng $ax-y$ là một số nguyên và mọi số nguyên là đồng dư modulo $p$ với duy nhất một phần tử trong $F_p^X = \{0, 1, \ldots, p-1\}$. Có $p$ phần tử thuộc $F_p^X$ và nhiều hơn $p$ biểu thức $ax-y$. Do đó theo nguyên lý chuồng chim bồ câu, phải có ít nhất hai biểu thức $ax-yy$ cùng đồng dư modulo $p$. Lấy cặp $(x_1, y_1) \neq (x_2, y_2)$ mà $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$. Ta rút gọn để được $a(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}$. Đặt $x = |x_1 - x_2|, y = |y_1 - y_2|$ thì $(x, y) \in S$. Ta muốn loại trừ khả năng $x = 0$ hoặc $y = 0$ để $x, y \in \{1, 2, \ldots, [\sqrt{p}]\}$.

Đầu tiên giả sử $x = |x_1 - x_2| = 0$, tức là $x_1 = x_2$. Khi đó $a(x_1 - x_2) = 0 \equiv y_1 - y_2 \pmod{p}$. Vì $y_1, y_2 \in \{1, 2, \ldots, [\sqrt{p}]\}$ nên $y_1 < p, y_2 < p$. Khi đó, ta phải có $y_1 = y_2$, mâu thuẫn với $(x_1, y_1) \neq (x_2, y_2)$.

Bây giờ giả sử $y = |y_1 - y_2| = 0$, do đó $y_1 = y_2$. Khi đó $a(x_1 - x_2) \equiv 0 \pmod{p}$. Vì $p \nmid a$ nên từ tính chất của các phép toán đồng dư đã nêu trước đây thì $x_1 - x_2 \equiv 0 \pmod{p}$. Lập luận tương tự như trên ta kết luận rằng $x_1 = x_2$ , mâu thuẫn với $(x_1, y_1) \neq (x_2, y_2)$.

Như vậy ta có $ax \equiv \pm y \pmod{p}$ và đó là điều cần chứng minh. □

**Tính chất 1.1.3** (xem [2]-[5])**.**
a. Với mọi số nguyên $a$ ta có $a \equiv a \pmod{m}$.

b. Nếu $a \equiv b \pmod{m}$ thì $b \equiv a \pmod{m}$.

c. Nếu $a \equiv b \pmod{m}$ và $b \equiv c \pmod{m}$ thì $a \equiv c \pmod{m}$.

**Tính chất 1.1.4** (xem [2]-[5])**.** Nếu $a \equiv b \pmod{m}$ và $c$ là một số nguyên tùy ý thì

$$a \pm c \equiv b \pm c \pmod{m}.$$

**Tính chất 1.1.5** (xem [2]-[5])**.**
a. Nếu $a_1 \equiv a_2 \pmod{m}$; $b_1 \equiv b_2 \pmod{m}$ thì

$$(a_1 \pm b_1) \equiv (a_2 \pm b_2) \pmod{m}.$$

b. Nếu $a_1 \equiv a_2 \pmod{m}$; $b_1 \equiv b_2 \pmod{m}$ thì

$$(a_1 \times b_1) \equiv (a_2 \times b_2 \pmod{m}.$$

**Tính chất 1.1.6** (xem [3]-[5])**.**
a. Nếu $a + c \equiv b \pmod{m}$ thì $a \equiv b - c \pmod{m}$.

b. Nếu $a \equiv b \pmod{m}$ thì $a + km \equiv a \pmod{m}$.

c. Nếu $a \equiv b \pmod{m}$ thì $a^k \equiv b^k \pmod{m}$.

d. Giả sử $f(x) = a_n x^{n-1} + \cdots + a_1 x + a_0$ là một đa thức với hệ số nguyên. Nếu ta có $\alpha \equiv \beta \pmod{m}$ thì ta cũng có $f(\alpha) \equiv f(\beta) \pmod{m}$.

Đặc biệt nếu ta có $f(\alpha) \equiv 0 \pmod{m}$ thì ta cũng có $f(\alpha+km) \equiv 0 \pmod{m}$ $(k \in \mathbb{Z})$.

**Tính chất 1.1.7** (xem [2]-[5])**.** Nếu $ac \equiv bc \pmod{m}$ $(c, m) = 1$ thì $a \equiv b \pmod{m}$.

**Tính chất 1.1.8** (xem [2]-[5])**.** Nếu $a \equiv b \pmod{m}$ thì $ac \equiv bc \pmod{m}$.

**Tính chất 1.1.9** (xem [2]-[5])**.** Nếu $a \equiv b \pmod{m}$ và $d \mid (a, b, m)$ $(d > 0)$ thì ta có

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

**Tính chất 1.1.10** (xem [2]-[5])**.** Nếu $a \equiv b \pmod{m_i},\ i = 1, 2, 3, \ldots k$ thì

$$a \equiv b \pmod{m}; m = m_1 m_2 \ldots m_k.$$

Cho tập $A = \{a_1, a_2, \ldots, a_n\}$. Giả sử $0 \leq r_i \leq n - 1$ là số dư khi chia $a_i$ cho $n$. Nếu tập các số dư $\{r_1, r_2, \ldots, r_n\}$ trùng với tập $\{0, 1, \ldots, n-1\}$ thì ta nói $A$ là một hệ thặng dư đầy đủ (modulo $n$). Dễ thấy: Tập $A$ lập thành một hệ đầy đủ (modulo $m$) nếu và chỉ nếu $i \neq j \Rightarrow a_i \neq a_j \pmod{n}$.

Nếu $A = \{a_1, a_2, \ldots, a_n\}$ là hệ đầy đủ mod $n$ thì từ định nghĩa dễ suy ra

- Với mọi $m \in \mathbb{Z}$ tồn tại và duy nhất $a_i \in a$ sao cho $a_i \equiv m \pmod{n}$.
- Với mọi $a \in \mathbb{Z}$ tập $A + a = \{a_1 + a, a_2 + a, \ldots, a_n + a\}$, cũng lập thành hệ đầy đủ mod $n$.

- Nếu $c \in \mathbb{Z}$, $(c, n) = 1$ thì tập $cA = \{ca_1, ca_2, \ldots, ca_n\}$ cũng lập thành hệ đầy đủ mod $n$.

**Ví dụ 1.1.11.** Cho hai hệ đầy đủ mod $n$: $A = \{a_1, a_2, \ldots, a_n\}$ và $B = \{b_1, b_2, \ldots, b_n\}$. Chứng minh rằng nếu $n$ là số chẵn thì tập $A + B = \{a_1 + b_1, \ldots, a_n + b_n\}$ không lập thành một hệ đầy đủ mod $n$. Có thể nói gì nếu $n$ là số lẻ?

***Lời giải.*** Ta nhận xét rằng nếu $C = \{c_1, \ldots, c_n\}$ là hệ đầy đủ mod $n$, thì ta có

$$\sum_{i=1}^{n} c_1 \equiv \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \equiv 0$$

(do $n$ chẵn). Ta có

$$\begin{aligned}\sum_{i=1}^{n}(a_i + b_i) &\equiv \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \equiv \frac{n(n+1)}{2} + \frac{n(n+1)}{2} \\ &= n(n_1) \equiv 0 \pmod{n}.\end{aligned}$$

Vậy nên $A + B = \{a_1 + b_1, \ldots, a_n + b_n\}$ không lập thành một hệ đầy đủ.

Nếu $n$ lẻ thì chưa kết luận được. Nghĩa là $A + B$ có thể là hệ đầy đủ, có thể không là hệ đầy đủ. Chẳng hạn, xét $n = 3$. Nếu $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ thì $A + B = \{5, 7, 9\}$ là hệ đầy đủ mod 3. Tuy nhiên với $B' = \{5, 4, 6\}$ thì $A + B' = \{6, 6, 9\}$ lại không là hệ đầy đủ mod 3.

**Ví dụ 1.1.12.** Cho hai số nguyên dương $m, n$ và hai tập $A = \{a_1, \ldots, a_n\}$ và $B = \{b_1, \ldots, b_n\}$ trong đó $A$ là hệ đầy đủ mod $n$ và $B$ là hệ đầy đủ mod $m$. Chứng minh rằng nếu $(m, n) > 1$ thì tập $AB = \{a_i b_j\}$ $i = 1, 2, \ldots, n, j = 1, 2, \ldots, m$ không lập thành một hệ đầy đủ mod $mn$. Có thể nói gì nếu $(m, n) = 1$.

***Lời giải.*** Ta có nhận xét sau: Nếu $A = \{a_1, \ldots, a_n\}$ là hệ đầy đủ mod $n$ và $p$ là ước nguyên tố của $n$ thì trong $A$ có đúng $n - \dfrac{n}{p}$ số không chia hết cho $p$. Thật vậy, giả sử $a_i = q_i n + r_i, 1 \leq r_i \leq n$. Do $A$ là hệ đầy đủ nên các $r_i$ phân biệt. Ta có $a_i$ chia hết cho $p$ khi và chỉ khi $r_i$ chia hết cho $p$. Số phần tử của $A$ chia hết cho $p$ bằng số các số nguyên dương $k, k \leq n$ là bội của $n$, Dễ thấy số đó là $\dfrac{n}{p}$. Do đó số các số không chia hết cho $p$ trong $A$ là $n - \dfrac{n}{p}$.

Một phần tử $a_ib_j \in AB$ không chia hết cho $p$ khi và chỉ khi cả $a_i$ và $b_j$ đều không chia hết cho $p$. Nếu $AB$ là một hệ đầy đủ mod $mn$ thì từ nhận xét trên ta suy ra đẳng thức

$$mn - \frac{mn}{p} = (n - \frac{n}{p})(m - \frac{m}{p}) \Leftrightarrow \frac{mn}{p} = \frac{mn}{p^2}.$$

Đây là điều vô lý vì $p > 1$. Nếu $(m, n) = 1$ thì chưa kết luận được. Nghĩa là $A + B$ có thể là hệ đầy đủ, có thể không là hệ đầy đủ. Ví dụ $n = 2, m = 3$. Nếu $A = \{1, 2\},\ B = \{5, 7, 9\}$ thì $AB = \{5, 7, 9, 10, 14, 18\}$ là hệ đầy đủ mod 6. Nếu $A = \{1, 2\}, B = \{5, 6, 7\}$ thì $AB = \{5, 6, 7, 10, 12, 14\}$ không là hệ đầy đủ mod 6.

**Ví dụ 1.1.13.** Một số nguyên dương $T$ gọi là số tam giác nếu nó có dạng $T = \frac{k(k+1)}{2}$. Tìm tất cả các số nguyên dương $n$ có tính chất: Tồn tại một hệ đầy đủ mod $n$ gồm $n$ số tam giác.

***Lời giải.*** Ta chứng minh số $n$ có dạng $n = 2^s$.

i) Nếu $n = 2^s$. Ta xét tập $A = \{T_{2i-1}\}_{i=1}^{n}$ ở đó $T_k = \frac{k(k+1)}{2}$. Ta có $A$ là hệ đầy đủ mod $n$ vì nếu $T_{2i-1} \equiv T_{2j-1} \Rightarrow (i - j)(2i + 2j - 1)$ chia hết cho $n$. Vì $n$ không có ước lẻ nên $i - j$ chia hết cho $n$. Mâu thuẫn. Đảo lại giả sử tồn tại một hệ đầy đủ $A$ mod $n$ gồm $n$ số tam giác với $n = 2^s m$ ở đó $m > 1$ là số lẻ. Xét tập $B = \{T_i\}_{i=1}^{m}$. Ta chứng minh $B$ là hệ đầy đủ mod $m$. Thật vậy, lấy $x \in \{1, 2, \ldots, m\}$. Vì $A$ là hệ đầy đủ mod $n$ nên tồn tại số tam giác $T_k \in A$ sao cho $T_k \equiv x \pmod{n} \Rightarrow T_k \equiv \pmod{m}$. Giả sử $k \equiv i \pmod{m}, i \in \{1, 2, \ldots, m\}$. Khi đó $k(k + 1) \equiv i(i + 1) \pmod{m}$. Vì $m$ lẻ nên từ đó suy ra $T_i \equiv T_k \equiv x \pmod{m}$. Vậy $B$ là hệ đầy đủ mod $m$. Nhưng điều này là mâu thuẫn, vì $T_m = \frac{m(m+1)}{2} \equiv 0 \pmod{m}$, $T_{m-1} = \frac{m(m-1)}{2} \equiv 0 \pmod{m}$.

**Nhận xét 1.1.14.** Ví dụ trên có thể phát biểu dưới dạng một bài toán vui như sau: Một lớp gồm $n$ học sinh đứng thành vòng tròn để chuyền bóng ngược chiều kim đồng hồ theo quy tắc sau: Lớp trưởng (coi là học sinh mang số một) bỏ qua học sinh bên cạnh (học sinh mang số hai) chuyền bóng cho học sinh mang số ba. Học sinh mang số ba có bóng, bỏ qua hai học sinh kế tiếp (mang số bốn và số năm) chuyền bóng cho học sinh mang số sáu. Học sinh mang số sáu có bóng, bỏ qua ba học sinh kế tiếp (mang số 7,8,9) chuyền bóng cho học sinh mang số