ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI ANH DŨNG

MỘT SỐ PHƯƠNG TRÌNH DIOPHANT ĐẶC BIỆT

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI ANH DŨNG

MỘT SỐ PHƯƠNG TRÌNH DIOPHANT ĐẶC BIỆT

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 60 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC

GS.TSKH. HÀ HUY KHOÁI

Thái Nguyên - 2015

Mục lục

Lời cảm ơn

Luận văn này được thực hiện và hoàn thành tại Trường Đại học Khoa học - Đại học Thái Nguyên.

Đầu tiên, em xin bày tỏ lòng biết ơn sâu sắc nhất tới người thầy đáng kính GS.TSKH Hà Huy Khoái - ĐH Thăng Long Hà Nội. Thầy đã dành nhiều thời gian hướng dẫn và giải đáp các thắc mắc trong suốt quá trình xây dựng đề cương, làm và hoàn thiện luận văn.

Em xin gửi lời cảm ơn chân thành nhất đến các Thầy cô khoa Toán, phòng Đào tạo sau Đại học, trường Đại học Khoa học - Đại học Thái Nguyên, cùng các Thầy cô giáo tham gia trực tiếp giảng dạy lớp cao học khóa 1/2014 - 1/2016. Đồng thời tôi xin gửi lời cảm ơn tới tập thể lớp K7C Cao học Toán - Đại học Khoa học đã động viên giúp đỡ tôi trong quá trình học tập và làm luận văn này.

Em xin chân thành cảm ơn!

Thái Nguyên, 2015 **Bùi Anh Dũng**

Học viên Cao học Toán lớp C, khóa 01/2014-01/2016

Chuyên ngành phương pháp Toán sơ cấp

Trường Đại học Khoa học - Đại học Thái Nguyên

Email: buianhdung@gmail.com

Mở đầu

Phương trình Diophant là một trong những dạng toán lâu đời nhất của Toán học và đã trải qua một lịch sử phát triển lâu dài.

Thông qua việc giải các phương trình Diophant, các nhà Toán học đã tìm ra được những tính chất sâu sắc của số nguyên, số hữu tỷ, số đại số.

Trong các kỳ thi học sinh giỏi quốc gia, quốc tế, phương trình Diophant vẫn thường xuyên xuất hiện dưới các hình thức khác nhau và luôn được đánh giá là khó do tính phi tiêu chuẩn của nó.

Luận văn này có mục đích trình bày một số kết quả nghiên cứu gần đây về một số phương trình Diophant đặc biệt, liên quan đến hàm số học (Hàm tổng các ước và hàm tích các ước nguyên tố) và biểu diễn số nguyên trong cơ số tùy ý.

Luận văn gồm phần mở đầu, hai chương, phần kết luận và danh mục tài liệu tham khảo.

Chương 1. Phương trình dạng $\sigma(n) = \gamma(n)^2$.

Trong chương này trình bày một số hàm số học, cấu trúc nghiệm của phương trình và nghiệm trong một số trường hợp đặc biệt.

Chương 2. Phương trình dạng $a^x \equiv x(mod b^n)$.

Chương này trình bày Bài toán về dãy chữ số cuối của một số và cơ sở đúng đắn, sự tồn tại nghiệm của phương trình.

Chương 1

Phương trình dạng $\sigma(n) = \gamma(n)^2$.

1.1 Một số hàm số học

1.1.1 Phi - hàm Ơle

Định nghĩa 1.1. Giả sử n là một số nguyên dương. Giá trị của phi - hàm Ơ - le tại n là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n. Kí hiệu Phi - hàm Ơ - le là $\varphi(n)$.

Ví dụ 1.1. $\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2,\ \varphi(5) = 4$

Định nghĩa 1.2. Cho n là số nguyên dương. Nếu a là số nguyên với $(a, n) = 1$ thì luôn tồn tại số nguyên dương k để $a^k \equiv 1\ (mod\, n)$. Số nguyên dương k bé nhất thỏa mãn $a^k \equiv 1\ (mod\, n)$ được gọi là cấp của số nguyên $a\ (mod\, n)$.

Định nghĩa 1.3. Một hệ thặng dư thu gọn môđulô n là một tập hợp gồm $\varphi(n)$ số nguyên sao cho mỗi phần tử của tập hợp đều nguyên tố cùng nhau với n và không có hai phần tử khác nhau nào đồng dư môđulô n.

Ví dụ 1.2. Các số $1, 2, 3, 4, 5, 6$ lập thành một hệ thặng dư thu gọn môđulô 7. Các số $1, 3, 5, 7$ lập thành một hệ thặng dư thu gọn môđulô 8.

Định nghĩa 1.4. Một tập A nào đó được gọi là một hệ thặng dư đầy đủ theo môđulô n nếu với bất kỳ số $x \in Z$ tồn tại một $a \in A$ để $x \equiv a\ (mod\, n)$.

Ví dụ 1.3. Các số $0, 1, 2, ..., n-1$ lập thành một hệ thặng dư đầy đủ theo môđulô n.

Tính chất 1.1. Giả sử $\left\{r_1, r_2, ..., r_{\varphi(n)}\right\}$ là một hệ thặng dư thu gọn môđulô n, a là số nguyên dương và $(a, n) = 1$. Khi đó, tập hợp $\left\{ar_1, ar_2, ..., ar_{\varphi(n)}\right\}$ cũng là hệ thặng dư thu gọn môđulô n.

Chứng minh. Trước tiên ta chứng tỏ rằng, mỗi số nguyên ar_j là nguyên tố cùng nhau với n. Giả sử ngược lại, $(ar_j, n) > 1$ với j nào đó. Khi đó tồn tại ước nguyên tố p của (ar_j, n). Do đó, hoặc $p\,|a$, hoặc $p\,|r_j$, tức là hoặc $p\,|a$ và $p\,|n$, hoặc $p\,|r_j$ và $p\,|n$. Tuy nhiên, không thể có $p\,|r_j$ và $p\,|n$ vì r_j và n là nguyên tố cùng nhau. Tương tự, không thể có $p\,|a$ và $p\,|n$. Vậy, ar_j và n nguyên tố cùng nhau với mọi $j = 1,\ 2, ..., \varphi(n)$.

Còn phải chứng tỏ hai số $ar_j,\ ar_k\ (j \neq k)$ tùy ý không đồng dư môđulô n. Giả sử $ar_j \equiv ar_k\,(mod\,n)$, $j \neq k$ và $1 \leq j \leq \varphi(n)$, $1 \leq k \leq \varphi(n)$. Vì $(a, n) = 1$ nên ta suy ra $r_j \equiv r_k\,(mod\,n)$. Điều này mâu thuẫn vì $r_j,\ r_k$ cùng thuộc một hệ thặng dư thu gọn ban đầu môđulô n.

Ví dụ 1.4. Tập hợp $\{1,\ 3,\ 5,\ 7\}$ là một hệ thặng dư thu gọn theo môđulô 8. Do $(5, 8) = 1$ nên $\{5,\ 15,\ 25,\ 35\}$ cũng là một hệ thặng dư môđulô 8.

Tính chất 1.2. *(Định lí Euler)* Giả sử m là số nguyên dương và a là số nguyên với $(a, m) = 1$. Khi đó $a^{\varphi(m)} \equiv 1\,(mod\,m)$

Chứng minh. Giả sử $\left\{r_1,\ r_2, ..., r_{\varphi(n)}\right\}$ là một hệ thặng dư thu gọn gồm các số nguyên dương không vượt quá m và nguyên tố cùng nhau với m. Do Tính chất 1 và do $(a, m) = 1$, tập hợp $\left\{ar_1,\ ar_2, ..., ar_{\varphi(n)}\right\}$ cũng là một hệ thặng dư thu gọn môđulô m. Như vậy, các thặng dư dương bé nhất của $ar_1,\ ar_2, ..., ar_{\varphi(m)}$ phải là các số nguyên $r_1,\ r_2, ..., r_{\varphi(m)}$ xếp theo thứ tự nào đó. Vì thế, nếu ta nhân các vế từ trong hệ thặng dư thu gọn trên đây, ta được: $ar_1.a\,r_2...ar_{\varphi(m)} \equiv r_1.\,r_2...r_{\varphi(m)}\,(mod\,m)$.

Do đó, $a^{\varphi(m)} r_1\, r_2 ... r_{\varphi(m)} \equiv r_1 .\, r_2 ... r_{\varphi(m)} \,(mod\, m)$. Vì $\left(r_1 .\, r_2 ... r_{\varphi(m)}, m\right) = 1$ nên $a^{\varphi(m)} \equiv 1 \,(mod\, m)$.

Ví dụ 1.5. Ta có: $2^{\varphi(5)} = 2^4 = 16 \equiv 1 \,(\, mod\, 5)$

Nhận xét 1.1. Ta có thể tìm nghịch đảo môdulô n bằng cách sử dụng định lí Euler. Giả sử a, m là các số nguyên tố cùng nhau, khi đó:

$$a.a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1 \,(mod\, m)$$

Vậy $a^{\varphi(m)-1}$ là nghịch đảo của a môdulô m.

Ví dụ 1.6. Ta có: $2^{\varphi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \,(mod\, 9)$ là một nghịch đảo của 2 môdulô 9.

Hệ quả 1.1. Nếu $(a, b) = 1$ thì $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \,(mod\, ab)$.

Hệ quả 1.2. Với $(a, b) = 1$ và n, v là hai số nguyên dương nào đó thì

$$a^{n\varphi(b)} + b^{v\varphi(a)} \equiv 1 \,(mod\, ab)$$

Hệ quả 1.3. Giả sử có k $(k \geq 2)$ số nguyên dương $m_1,\ m_2,\ ..., m_k$ và chúng nguyên tố với nhau từng đôi một.
Đặt $M = m_1 .\, m_2 ... m_k = m_i.t_i$ với $i = 1, 2, ..., k$ ta có

$$t_1^n + t_2^n + ... + t_k^n \equiv (t_1 + t_2 + t_3)^n \,(\mathrm{mod} M)$$

với n nguyên dương.

Tính chất 1.3. Với số nguyên tố p ta có $\varphi\,(p) = p - 1$. Ngược lại, nếu p là số nguyên dương sao cho $\varphi\,(p) = p - 1$ thì p là số nguyên tố.
Chứng minh. Nếu p nguyên tố thì với mọi số nguyên dương nhỏ hơn p đều nguyên tố cùng nhau với p. Do có $p - 1$ số nguyên dương như vậy nên $\varphi\,(p) = p - 1$.

Ngược lại, nếu p là hợp số thì p có các ước d, $1 < d < p$, p và d không nguyên tố cùng nhau. Như vậy, trong các số $1, 2, ..., p-1$ phải có những số không nguyên tố cùng nhau với p, nên $\varphi(p) \leq p-2$. Theo giả thiết $\varphi(p) = p-1$. Vậy p là số nguyên tố.

Ví dụ 1.7. $\varphi(3) = 3-1 = 2, \quad \varphi(31) = 31-1 = 30$

Tính chất 1.4. Giả sử p là số nguyên tố và a là số nguyên dương. Khi đó

$$\varphi(p^a) = p^a - p^{a-1}$$

Chứng minh. Các số nguyên dương nhỏ hơn p^a không nguyên tố cùng nhau với p là các số không vượt quá p^{a-1} và chia hết cho p. Có đúng p^{a-1} số như vậy. Do đó tồn tại $p^a - p^{a-1}$ số nguyên nhỏ hơn p^a và nguyên tố cùng nhau với p^a . Vậy $\varphi(p^a) = p^a - p^{a-1}$.

Ví dụ 1.8. $\varphi(125) = \varphi\left(5^3\right) = 5^3 - 5^2 = 100, \ \ \varphi\left(2^{10}\right) = 2^{10} - 2^9 = 525$

Tính chất 1.5. Nếu m, n là các số nguyên dương, nguyên tố cùng nhau thì

$$\varphi(m.n) = \varphi(m).\varphi(n)$$

Chứng minh. Ta viết các số nguyên dương không vượt quá mn thành bảng sau:

$$\begin{array}{lllll}
1 & m+1 & 2m+1 & ... & (n-1)m+1 \\
2 & m+2 & 2m+2 & ... & (n-1)m+2 \\
3 & m+3 & 2m+3 & ... & (n-1)m+1 \\
... & ... & .... & ... & ..... \\
r & m+r & 2m+r & ... & (n-1)m+r
\end{array}$$