ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

DƯƠNG XUÂN LỢI

TIẾP CẬN SƠ CẤP GIẢI PHƯƠNG TRÌNH NGHIỆM NGUYÊN VÀ MỘT SỐ BÀI TOÁN VỀ ƯỚC SỐ

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

DƯƠNG XUÂN LỢI

TIẾP CẬN SƠ CẤP GIẢI PHƯƠNG TRÌNH NGHIỆM NGUYÊN VÀ MỘT SỐ BÀI TOÁN VỀ ƯỚC SỐ

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số: 8 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS. NGUYỄN VĂN HOÀNG

THÁI NGUYÊN - 2019

Mục lục

Mở đầu

Trong các kỳ thi HSG thường xuất hiện các bài toán tìm nghiệm nguyên. Loại toán này còn xuất hiện trong các kỳ thi quốc tế. Đó là loại toán đòi hỏi một phản xạ nhanh và chính xác, một lý luận chặt chẽ và logic. Chính vì vậy giải phương trình nghiệm nguyên là phát triển tốt cho trí tưởng tượng và sự thông minh.

Vấn đề thừa nhận rằng: Nếu như người học nắm chắc các cách tiếp cận để giải bài toán của phương trình nghiệm nguyên thì việc giải dạng toán này sẽ dễ dàng hơn và ngày càng hăng say học tập hơn.

Qua nghiên cứu đề tài luận văn "**Tiếp cận sơ cấp giải phương trình nghiệm nguyên và một số bài toán về ước số**" để bản thân tôi và đồng nghiệp có thêm tư liệu về dạy toán nói chung và dạy dạng toán nghiệm nguyên nói riêng.

Mục đích chính của luận văn là nêu ra được một số cách tiếp cận sơ cấp giải phương trình nghiệm nguyên và tìm ước của một vài lớp số đặc biệt. Có ví dụ và lời giải chi tiết cho từng cách tiếp cận, từng lớp số đặc biệt. Đưa ra được hệ thống các bài tập tham khảo cho từng cách.

Nội dung của luận văn gồm hai chương:

Chương 1: Kiến thức chuẩn bị:

Chương này nhắc lại một số kiến thức cơ bản cần thiết dùng cho các kết quả ở chương sau, chẳng hạn về số nguyên tố, đồng dư thức, phương trình đồng dư, phần tử bất khả quy và ký hiệu Legendre...

Chương 2: Các phương pháp sơ cấp giải phương trình nghiệm nguyên.

Phần thứ nhất của chương này dự kiến giới thiệu một số phương pháp sơ cấp giải nghiệm nguyên. Mỗi phương pháp có trình bày định lý, bổ đề, nguyên tắc, phương pháp, ví dụ minh họa liên quan đến phương pháp. Phần thứ hai trình bày một số phương trình nghiệm nguyên cổ điển. Phần cuối giới thiệu sơ lược cách tiếp cận cao cấp liên quan đến ký hiệu Legendre và

phương trình nghiệm nguyên để tìm ước của một vài lớp số đặc biệt.

Luận văn này được hoàn thành tại trường Đại học Khoa học, Đại học Thái Nguyên dưới sự hướng dẫn tận tình của Phó giáo sư-Tiến sĩ Nguyễn Văn Hoàng. Tôi xin bày tỏ lòng biết ơn chân thành và sâu sắc về sự tận tâm và nhiệt tình của thầy trong suốt quá trình tác giả thực hiện luận văn.

Trong quá trình học tập và làm luận văn, từ bài giảng của các giáo sư, tiến sĩ đang công tác tại Trường Đại học Khoa Học - Đại học Thái Nguyên, tôi đã trau dồi thêm rất nhiều kiến thức để nâng cao trình độ của mình. Từ đáy lòng mình, tôi xin bày tỏ lòng cảm ơn sâu sắc tới tất cả các thầy, cô.

Tôi xin chân thành cám ơn Ban Giám hiệu, phòng Đào tạo Khoa học, Khoa Toán - Tin trường Đại học Khoa học, Đại học Thái Nguyên đã quan tâm và giúp đỡ tôi trong suốt thời gian học tập tại trường.

Nhân dịp này tôi xin chân thành cảm ơn đồng nghiệp, bạn bè và gia đình đã tạo mọi điều kiện giúp đỡ, động viên để tôi hoàn thành luận văn này.

Thái Nguyên, tháng 11 năm 2019

Tác giả

Dương Xuân Lợi

Chương 1

Kiến thức chuẩn bị

Trong chương này, ta quy ước rằng tất cả các chữ $a, b, c, x, y, z, \ldots$ biểu thị các số nguyên và tất cả các mô-đun $m, n, \ldots$ là các số nguyên dương. Nội dung của chương được tổng hợp từ các tài liệu [1], [2] và [6].

1.1 Số nguyên tố

Định nghĩa 1.1.1. (xem [1]) (i) Cho các số nguyên a, b, với $a \neq 0$. Ta nói rằng a *chia hết* b hoặc a là một *ước* số của b nếu $b = ac$ với một số nguyên c nào đó, ký hiệu $a \mid b$. Ta cũng nói rằng b chia hết cho a hoặc b là một bội số của a, ký hiệu $b \vdots a$.

(ii) Cho a, b các số nguyên không đồng thời bằng 0. *Ước chung lớn nhất* của a, b là số nguyên dương d thỏa mãn các điều kiện (1) $d|a$ và $d|b$; (2) nếu có số nguyên e sao cho $e|a$ và $e|b$, thì $e|d$. Kí hiệu ước chung lớn nhất của a và b là $\gcd(a, b)$ hoặc (a, b).

(iii) Hai số nguyên a và b được gọi là *nguyên tố cùng nhau* nếu $\gcd(a, b) = 1$.

Định nghĩa 1.1.2. (xem [1]) Số 1 chỉ có đúng một ước dương. Mỗi số nguyên lớn hơn 1 đều có ít nhất hai ước dương (chẳng hạn 1 và chính nó). Các số nguyên dương lớn hơn 1 mà chỉ có đúng hai ước dương được gọi là *số nguyên tố*. Bất kỳ số nguyên lớn hơn 1 không phải là số nguyên tố được gọi là *hợp số*.

Mệnh đề 1.1.3. (xem [1]) (i) Cho $a, b, c \in \mathbb{Z}$. Nếu $a|bc$ và $(a, b) = 1$ thì $a|c$.

(ii) Cho $a_1, a_2, \ldots, a_n$ và $b_1, b_2, \ldots, b_m$ là hai dãy các số nguyên thỏa mãn điều kiện $\gcd(a_i, b_j) = 1$ với mọi i mọi j. Khi đó $\gcd(a_1a_2 \ldots a_n, b_1b_2 \ldots b_m) = 1$.

Đặc biệt, nếu $\gcd(p, q) = 1$ thì $\gcd(p^n, q^m) = 1$ với mọi m, n là các số nguyên dương.

Định lý 1.1.4 (Định lý cơ bản về số nguyên tố)**.** (xem [1]) Cho n là số nguyên lớn hơn 1. Khi đó n luôn có thể biểu diễn được một cách duy nhất dưới dạng

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots . p_k^{\alpha_k}$$

trong đó $k > 0$, α_i $(i = 1, 2, \ldots, k)$ là các số tự nhiên và p_i là các số nguyên tố thỏa mãn $p_1 < p_2 < \cdots < p_k$.

1.2 Đồng dư thức

Định nghĩa 1.2.1 (Đồng dư thức)**.** (xem [1]) Cho m là số nguyên dương. Ta nói số nguyên a đồng dư với số nguyên b theo mô-đun m nếu $m \mid (a - b)$, kí hiệu $a \equiv b \pmod{m}$. Trường hợp ngược lại ta kí hiệu $a \not\equiv b \pmod{m}$.

Sau đây là một số tính chất cơ bản của đồng dư thức.

Mệnh đề 1.2.2. (xem [1]) (i) $a \equiv b \pmod{m} \Leftrightarrow$ tồn tại $k \in \mathbb{Z}$ để $a = b + km$.

(ii) $a \equiv b \pmod{m} \Leftrightarrow a$ và b chia cho m có cùng một số dư.

(iii) $a \equiv a \pmod{m}$.

(iv) Nếu $a \equiv b \pmod{m}$, thì $b \equiv a \pmod{m}$.

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

Mệnh đề 1.2.3. (xem [1]) Nếu $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$ thì

$$a + c \equiv b + d \pmod{m} \text{ và } ac \equiv bd \pmod{m}.$$

Mệnh đề 1.2.4. (xem [1]) (i) Nếu $ac \equiv bc \pmod{m}$, $(c, m) = 1$, thì $a \equiv b \pmod{m}$.

(ii) Nếu $ac \equiv bc \pmod{m}$ và $(c, m) = d$, thì $a \equiv b \pmod{\frac{m}{d}}$.

Định lý 1.2.5 (Định lý Fermat nhỏ)**.** (xem [1]) Cho p là một số nguyên tố và a là số nguyên. Khi đó $a^p \equiv a \pmod{p}$. Đặc biệt, nếu $(a, p) = 1$, thì $a^{p-1} \equiv 1 \pmod{p}$.

Định lý 1.2.6 (Định lý Euler)**.** (xem [1]) Nếu m là số nguyên dương và $\gcd(a, m) = 1$, thì $a^{\varphi(m)} \equiv 1 \pmod{m}$ trong đó $\varphi(m)$ là hàm số Euler của m.

1.3 Thặng dư bậc hai và ký hiệu Legendre

Định nghĩa 1.3.1. (xem [2]) Cho số nguyên dương n. Số nguyên a được gọi là *thặng dư bậc hai* theo $\mod n$, hay, gọi là *số chính phương theo* $\mod n$, nếu tồn tại số nguyên x sao cho $x^2 \equiv a \pmod{n}$.

Ví dụ 1.3.2. $1^2 \equiv 1 \pmod 6$, $3^2 \equiv 3 \pmod 6$, $4^2 \equiv 4 \pmod 6$. *Suy ra các số* $1, 3, 4$ *là các thặng dư bậc hai theo* $\mod 6$.

Số 2 *là một thặng dư bậc hai theo* $\mod 7$, *vì* $3^2 \equiv 2 \pmod 7$. *Trong khi đó* 3 *không là thặng dư bậc hai theo* $\mod 7$.

Định nghĩa 1.3.3. (xem [2]) Giả sử p là một số nguyên tố lẻ, a là một số nguyên tùy ý. *Ký hiệu Legendre* $\left(\frac{a}{p}\right)$ được xác định như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{nếu } \gcd(a,p) = 1 \text{ và } a \text{ là số chính phương mod } p; \\ -1 & \text{nếu } \gcd(a,p) = 1 \text{ và } a \text{ không là số chính phương mod } p; \\ 0 & \text{nếu } a \vdots p. \end{cases}$$

Tiếp theo ta nhắc lại một số tính chất của ký hiệu Legendre

Mệnh đề 1.3.4. (xem [2]) *Cho* p *là số nguyên tố lẻ. Khi đó*

(0) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(2) Nếu $a \equiv b \pmod p$ *thì* $\left(\frac{\alpha}{p}\right) = \left(\frac{b}{p}\right)$.

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

(4) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 \text{ khi } p \equiv 1 \pmod 4 \\ -1 \text{ khi } p \equiv 3 \pmod 4. \end{cases}$

(5) $\left(\dfrac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 \text{ } khi\ p \equiv 1 \text{ } hoặc\ 7 \pmod 8 \\ -1 \text{ } khi\ p \equiv 3 \text{ } hoặc\ 5 \pmod 8. \end{cases}$

(6) $\left(\dfrac{3}{p}\right) = (-1)^{\left[\frac{p+1}{6}\right]} = \begin{cases} 1 \text{ } khi\ p \equiv 1 \text{ } hoặc\ 11 \pmod{12} \\ -1 \text{ } khi\ p \equiv 5 \text{ } hoặc\ 7 \pmod{12}. \end{cases}$

(7) Với mỗi số nguyên tố lẻ p bất kỳ,

$$\left(\frac{5}{p}\right) = (-1)^{\left[\frac{p-2}{5}\right]} = \begin{cases} 1 \text{ } khi\ p \equiv 1 \text{ } hoặc\ 4 \pmod 5 \\ -1 \text{ } khi\ p \equiv 2 \text{ } hoặc\ 3 \pmod 5. \end{cases}$$

(8) Với mỗi số nguyên tố lẻ p bất kỳ,

$$\left(\frac{7}{p}\right) = (-1)^{\left[\frac{p+1}{6}\right]} = \begin{cases} 1 \text{ } khi\ p \equiv 1, 3, 9, 19, 25 \text{ } hoặc\ 27 \pmod{28} \\ -1 \text{ } khi\ p \equiv 5, 11, 13, 15, 17 \text{ } hoặc\ 23 \pmod{28}. \end{cases}$$

(9) Nếu p và q là các sốp nguyên tố lẻ thì

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

1.4 Sơ lược về đa thức bất khả quy

Định nghĩa 1.4.1 (Đa thức bất khả quy)**.** (xem [6]) Cho A là một miền nguyên. Một đa thức $f(x) \in A[x]$ được gọi là bất khả quy trên A nếu $f(x) \neq 0$, $f(x)$ không khả nghịch và $f(x)$ không có ước thực sự. Một đa thức khác 0, không khả nghịch, mà không bất khả quy thì được gọi là đa thức khả quy.

Định nghĩa 1.4.2 (Vành Gauss)**.** (xem [6]) Một vành giao hoán D được là một vành Gauss (hay vành nhân tử hóa, hay vành phân tích duy nhất), viết tắt UFD, nếu D là một miền nguyên thỏa mãn các điều kiện:

(1) Mọi phần tử a khác không, khác đơn vị của D đều được phân tích được thành một tích của các phần tử bất khả quy của D.

(2) Sự phân tích của một phần tử a như ở điều kiện (1) là duy nhất với sai khác là hoán vị các thừa số bất khả quy.

Định lý 1.4.3. (xem [6]) Nếu D là một UFD thì $D[x]$ cũng là một UFD.

Chương 2

Cách tiếp cận sơ cấp giải phương trình nghiệm nguyên

Nội dung của chương được tổng hợp từ các tài liệu [3], [4] và [5]. Chủ yếu sử dụng tài liệu [4].

2.1 Cách tiếp cận sơ cấp giải phương trình nghiệm nguyên

2.1.1 Cách phân tích

Trước hết ta xét sự phân tích của đa thức ra các đa thức bất khả quy. Ta biết rằng trong vành đa thức $\mathbb{Z}[x_1, x_2, \ldots, x_n]$, mọi đa thức khác 0 và khác ± 1 của nó đều phân tích được thành tích các đa thức bất khả quy trong $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ (vì nó là vành Gauss).

Xét phương trình

$$f(x_1, x_2, \ldots, x_n) = 0. \tag{2.1}$$

Ta có thể viết (2.1) ở dạng tương đương

$$f_1(x_1, x_2, \ldots, x_n) f_2(x_1, x_2, \ldots, x_n) \cdots f_k(x_1, x_2, \ldots, x_n) = a$$

với $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ và $a \in \mathbb{Z}$. Lại vì a có thể phân tích được thành các thừa số nguyên tố, nên ta luôn có thể viết được a là tích của k số nguyên $a_1, a_2, \ldots, a_k$ (khi cần thiết ta có thể thêm các thừa số đơn vị, hoặc nhóm các thừa số dư thừa lại với nhau). Ứng với mỗi phân tích như vậy ta