ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ GIANG

VỀ TỔNG GAUSS VÀ MỘT SỐ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ GIANG

VỀ TỔNG GAUSS VÀ MỘT SỐ ỨNG DỤNG

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 8 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. Nguyễn Duy Tân

THÁI NGUYÊN - 2019

Mục lục

Mở đầu **1**

Chương 1. Một số kiến thức chuẩn bị **2**

1.1 Ký hiệu Legendre 2

1.2 Một số kiến thức chuẩn bị khác 8

Chương 2. Tổng Gauss bậc hai **10**

2.1 Giá trị tuyệt đối của tổng Gauss bậc hai 10

2.2 Dấu của tổng Gauss bậc hai 13

2.3 Mở rộng lên modulo hợp số lẻ 21

Chương 3. Một vài ứng dụng của tổng Gauss **26**

3.1 Luật thuận nghịch bậc hai 26

3.2 Một số bài toán lượng giác liên quan 29

Kết luận **34**

Tài liệu tham khảo **35**

Mở đầu

Tổng Gauss là một loại tổng gồm hữu hạn căn của đơn vị. Gauss nghiên cứu tổng Gauss bậc hai, và ứng dụng chúng trong nghiên cứu về luật thuận nghịch bậc hai.

Mục tiêu của luận văn là tìm hiểu tổng Gauss bậc hai và một số ứng dụng liên quan.

Ngoài phần Mở đầu, Kết luận và Tài liệu tham khảo, bố cục của luận văn được chia làm ba chương.

Chương 1. Một số kiến thức chuẩn bị.

Chương 2. Tổng Gauss bậc hai.

Chương 3. Một vài ứng dụng của tổng Gauss.

Thái Nguyên, tháng 5 năm 2019

Người viết luận văn

Nguyễn Thị Giang

Chương 1

Một số kiến thức chuẩn bị

Trong chương này, chúng tôi trình bày một số kiến thức cần thiết trong quá trình xây dựng định nghĩa tổng Gauss như khái niệm ký hiệu Legendre, định lý Euler, định lý Fermat, căn nguyên thủy, thặng dư bậc hai, ... Các kiến thức trong phần này được tham khảo chủ yếu từ tài liệu [3].

1.1 Ký hiệu Legendre

Định nghĩa 1.1.1 ([3])**.** Nếu $a, b, m \in \mathbb{Z}$ và $m \neq 0$, ta nói rằng a đồng dư với b modulo m nếu m là ước của $b - a$. Mối quan hệ này được ký hiệu bởi $a \equiv b \pmod{m}$. Kí hiệu $a \not\equiv b \pmod{m}$ có nghĩa là a không đồng dư với b modulo m.

Ví dụ, vì $4 \mid 25 - 1$, ta có $25 \equiv 1 \pmod{4}$. Vì $6 \mid 4 - 10$, ta có $4 \equiv 10 \pmod{6}$. Vì $7 \mid 10 - (-4)$, ta có $10 \equiv -4 \pmod{7}$. Vì $5 \nmid -7 - 2$, ta có $-7 \not\equiv 2 \pmod{5}$.

Định nghĩa 1.1.2 ([3])**.** Ta nói rằng hai số nguyên a và b là nguyên tố cùng nhau nếu ước chung duy nhất của chúng là ± 1.

Định nghĩa 1.1.3 ([3])**.** Cho $n \in \mathbb{Z}^+$, hàm ϕ Euler được định nghĩa là $\phi(n)$ bằng số số nguyên dương nhỏ hơn hoặc bằng n mà là nguyên tố cùng nhau với n, tức là

$$\phi(n) = |\{x \in \mathbb{Z} : 1 \leq x \leq n, (x, n) = 1\}|.$$

Ví dụ, $\phi(1) = 1, \phi(5) = |\{1, 2, 3, 4\}| = 4, \phi(6) = |\{1, 5\}| = 2$, và $\phi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6$. Nếu p là số nguyên tố thì rõ ràng tất cả các số $1, 2, \ldots, p-1$ đều nguyên tố cùng nhau với p nên $\phi(p) = p - 1$.

Định lý 1.1.4 (Định lý Euler, [3]). *Cho $a, m \in \mathbb{Z}$ với $m > 0$. Nếu $(a, m) = 1$ thì $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Chứng minh. Gọi $r_1, r_2, \ldots, r_{\phi(m)}$ là $\phi(m)$ số nguyên dương khác nhau không lớn hơn m sao cho $(r_i, m) = 1, i = 1, 2, \ldots, \phi(m)$. Xét $\phi(m)$ số nguyên $r_1a, r_2a, \ldots, r_{\phi(m)}a$. Chú ý rằng $(r_ia, m) = 1, i = 1, 2, \ldots, \phi(m)$. (Nếu $(r_ia, m) > 1$ với i nào đó thì tồn tại ước nguyên tố p của (r_ia, m) và $p \mid r_ia$ và $p \mid m$. Bây giờ $p \mid r_ia$ kéo theo $p \mid r_i$ hoặc $p \mid a$ nên hoặc ta có $p \mid r_i$ và $p \mid m$ hoặc ta có $p \mid a$ và $p \mid m$, các điều này là không thể vì $(r_i, m) = 1$ và $(a, m) = 1$.) Ngoài ra, chú ý rằng không có hai số nào trong dãy số $r_1a, r_2a, \ldots, r_{\phi(m)}a$ đồng dư với nhau. (Vì $(a, m) = 1$, tồn tại nghịch đảo của a modulo m, ký hiệu là a'. Do đó, nếu $r_ia \equiv r_ja \pmod{m}$ với $i \neq j$ thì $r_iaa' \equiv r_jaa' \pmod{m}$, điều này là không thể). Nên các thặng dư không âm nhỏ nhất modulo m của các số nguyên $r_1a, r_2a, \ldots, r_{\phi(m)a}$ sắp theo thứ tự tăng dần là $r_1, r_2, \ldots, \phi(m)$. Khi đó, ta có

$$(r_1a)(r_2a)\cdots(r_{\phi(m)}a) \equiv r_1r_2\cdots r_{\phi(m)} \pmod{m}.$$

Hay

$$m \mid (a^{\phi(m)}r_1r_2\cdots r_{\phi(m)}) - r_1r_2\cdots r_{\phi(m)}.$$

Kéo theo

$$m \mid r_1r_2\cdots r_{\phi(m)} \times (a^{\phi(m)} - 1).$$

Vì $(r_1r_2\cdots r_{\phi(m)}, m) = 1$, ta có

$$m \mid (a^{\phi(m)} - 1)$$

và $a^{\phi(m)} \equiv 1 \pmod{m}$, điều phải chứng minh. □

Định lý 1.1.5 (Định lý Fermat nhỏ, [3]). *Cho p là một số nguyên tố và cho $a \in \mathbb{Z}$. Nếu $p \nmid a$ thì $a^{p-1} \equiv 1 \pmod{p}$.*

Chứng minh. Xét $p - 1$ số nguyên xác định bởi $a, 2a, 3a, \ldots, (p-1)a$. Ta có $p \nmid ia, i = 1, 2, \ldots, p-1$. Chú ý rằng không có 2 số nào trong $p-1$ số nguyên bên trên đồng dư modulo p. (Vì $p \nmid a$, tồn tại nghịch đảo của a modulo p, ký hiệu là a'. Nếu $ia \equiv ja \pmod{p}$ với $i \neq j$ thì $iaa' = jaa' \pmod{p}$, từ đó $i \equiv j \pmod{p}$, vô lý). Nên các thặng dư không âm bé nhất modulo p của các số nguyên $a, 2a, 3a, \ldots, (p-1)a$ theo tứ tự tăng dần là $1, 2, 3, \ldots, p-1$. Khi đó,

$$(a)(2a)(3a)\cdots((p-1)a) \equiv (1)(2)(3)\cdots(p-1) \pmod{p},$$

hay tương đương

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Theo định lý Wilson, ta có $(p-1)! \equiv -1 \pmod{p}$ nên đồng dư thức bên trên trở thành

$$-a^{p-1} \equiv -1 \pmod{p},$$

hay tương đương với $a^{p-1} \equiv 1 \pmod{p}$, điều phải chứng minh. □

Định nghĩa 1.1.6 ([3])**.** Cho $a, n \in \mathbb{Z}$. Số a được gọi là *căn nguyên thủy modulo* n nếu a và n nguyên tố cùng nhau và $\phi(n)$ là số nguyên dương bé nhất sao cho $a^{\phi(n)} \equiv 1 \pmod{n}$.

Ví dụ, 3 là căn nguyên thủy modulo 7 vì $\phi(7) = 6$ là số nguyên dương x bé nhất để $3^x \equiv 1 \pmod{7}$. Thật vậy, $3^1 \equiv 3 \pmod{7}, 3^2 \equiv 2 \pmod{7}, 3^3 \equiv 6 \pmod{7}, 3^4 \equiv 4 \pmod{7}, 3^5 \equiv 5 \pmod{7}, 3^6 \equiv 1 \pmod{7}$. Tương tự, ta có 2 là căn nguyên thủy modulo 13 nhưng 2 không là căn nguyên thủy modulo 7 và $2^3 \equiv 1 \pmod{7}$ nhưng $\phi(7) = 6 > 3$.

Mệnh đề 1.1.7 ([3])**.** *Nếu $m \in \mathbb{Z}^+$ có các căn nguyên thủy và $(a, m) = 1$ thì a là thặng dư lũy thừa n modulo m khi và chỉ khi $a^{\phi(m)/d} \equiv 1 \pmod{m}$, trong đó $d = (n, \phi(m))$.*

Chứng minh. Gọi g là căn nguyên thủy modulo m và $a = g^b$, $x = g^y$. Khi đó phương trình đồng dư $x^n \equiv a \pmod{m}$ tương đương với $g^{ny} \equiv g^b \pmod{m}$, nên tương đương với $ny \equiv b \pmod{\phi(m)}$. Phương trình này có nghiệm khi và chỉ khi $d \mid b$. Ngoài ra, chú ý rằng nếu phương trình đồng dư có nghiệm thì nó có đúng d nghiệm.

Nếu $d \mid b$ thì $a^{\phi(m)/d} \equiv g^{b\phi(m)/d} \equiv 1 \pmod{m}$. Ngược lại, nếu $a^{\phi(m)/d} \equiv 1 \pmod{m}$ thì $g^{b\phi(m)/d} \equiv 1 \pmod{m}$, điều này kéo theo $\phi(m)$ là ước của $b\phi(m)/d$ hay $d \mid b$. Điều phải chứng minh. □

Nhận xét 1.1.8. Chứng minh của mệnh đề trên còn kéo theo thông tin bổ sung. Nếu $x^n \equiv a \pmod{m}$ có nghiệm thì có đúng $(n, \phi(m))$ nghiệm.

Mệnh đề 1.1.9 ([3])**.** *Nếu p là số nguyên tố lẻ, $p \nmid a$ và $p \nmid n$, khi đó nếu phương trình $x^n \equiv a \pmod{p}$ có nghiệm thì phương trình $x^n \equiv a \pmod{p^e}$ cũng có nghiệm với mọi $e \geq 1$. Tất cả các phương trình đồng dư này có cùng số nghiệm.*

Chứng minh. Nếu $n = 1$, kết luận là tầm thường, nên ta có thể giả sử $n \geq 2$. Giả sử $x^n \equiv a \pmod{p^e}$ giải phương trình. Gọi x_0 là một nghiệm và đặt $x_1 = x_0 + bp^e$. Tính toán ta được

$$x_1^n \equiv x_0^n + nbp^e x_0^{n-1} \pmod{p^{e+1}}.$$

Ta cần giải phương trình

$$x_1^n \equiv a \pmod{p^{e+1}}.$$

Việc này tương đương với tìm số nguyên b sao cho

$$nx_0^{n-1}b \equiv ((a - x_0^b)/p^2) \pmod{p}.$$

Chú ý rằng $(a - x_0^n)/p^e$ là số nguyên và $p \nmid nx_0^{n-1}$. Do đó phương trình này có nghiệm duy nhất theo b, và với giá trị này của b, $x_1^n n \equiv a \pmod{p^{e+1}}$.

Nếu $x^n \equiv a \pmod{p}$ không có nghiệm, thì $x^n \equiv a \pmod{p^e}$ không có nghiệm. Mặt khác, nếu $x^n \equiv a \pmod{p}$ có một nghiệm thì tất cả các phương trình $x^n \equiv a \pmod{p^e}$ cũng có nghiệm. Dựa theo nhận xét sau Mệnh đề 1.1.7 số nghiệm của $x^n \equiv a \pmod{p^e}$ là $(n, \phi(p^e))$ miễn là phương trình có nghiệm. Nếu $p \nmid n$, dễ thấy $(n, \phi(p)) = (n, \phi(p^e))$ với mọi $e \geq 1$. Điều phải chứng minh. □

Mệnh đề 1.1.10 ([3])**.** *Cho 2^l là lũy thừa cao nhất của 2 là ước của n. Giả sử a lẻ và phương trình $x^n \equiv a \pmod{2^{2l+1}}$ có nghiệm. Khi đó, phương trình $x^n \equiv a \pmod{2^e}$ có nghiệm với mọi $e \geq 2l + 1$ (và do đó với mọi $e \geq 1$). Ngoài ra, tất cả phương trình đồng dư này có cùng số nghiệm.*

Định nghĩa 1.1.11 ([3])**.** Giả sử $a, m \in \mathbb{Z}$, $m \neq 0$ và $(a, m) = 1$. Số a được gọi là thặng dư bậc hai modulo m nếu phương trình đồng dư $x^2 \equiv a \pmod{m}$ có một nghiệm. Nếu ngược lại, a được gọi là phi thặng dư bậc hai modulo m.

Ví dụ 1.1.12. Ta có 2 là thặng dư bậc hai modulo 7 nhưng 3 thì không. Thật ra, $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ lần lượt đồng dư với $1, 4, 2, 2, 4, 1$ modulo 7. Do đó, $1, 2$ và 4 là thặng dư bậc hai modulo 7 và 3, 5, và 6 là phi thặng dư bậc hai modulo 7.

Mục tiêu của chúng ta trong phần này là trả lời câu hỏi khi nào phương trình đồng dư bậc hai $x^2 \equiv a \pmod{m}$ có nghiệm. Mệnh đề sau cho cách xác định khi nào một số nguyên cho trước là thặng dư bậc hai modulo m.

Mệnh đề 1.1.13 ([3])**.** *Cho $m = 2^e p_1^{e_1} \cdots p_l^{e_l}$ là phân tích thừa số nguyên tố của m và giả sử $(a, m) = 1$. Khi đó $x^2 \equiv a \pmod{m}$ có nghiệm khi và chỉ khi các điều kiện sau được thỏa mãn:*

(a) *Nếu* $e = 2$ *thì* $a \equiv 1 \pmod 4$. *Nếu* $e \geq 3$ *thì* $a \equiv 1 \pmod 8$.

(b) *Với mỗi* i *ta có* $a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$.

Chứng minh. Theo định lý thặng dư Trung Hoa phương trình đồng dư $x^2 \equiv a \pmod p$ tương đương với hệ phương trình $x^2 \equiv a \pmod{2^e}, x^2 \equiv a \pmod{p_1^{e_1}}, \ldots, x^l \equiv a \pmod{p_l^{e_l}}$.

Xét đồng dư thức $x^2 \equiv a \pmod{2^e}$. Số 1 là thặng dư bậc hai duy nhất modulo 4 và 1 là thặng dư bậc hai duy nhất modulo 8. Do đó ta có tính giải được khi và chỉ khi $a \equiv 1 \pmod 4$ nếu $e = 2$ và $a \equiv 1 \pmod 8$ nếu $e = 3$. Áp dụng [3, Mệnh đề 4.2.4] ta có $x^2 \equiv a \pmod 8$ là có nghiệm khi và chỉ khi $x^2 \equiv a \pmod{2^e}$ có nghiệm với mọi $e \geq 3$.

Xét $x^2 \equiv a \pmod{p_i^{e_i}}$. Vì $(2, p_i) = 1$ từ [3, Mệnh đề 4.2.3] suy ra phương trình đồng dư này có nghiệm khi và chỉ khi phương trình $x^2 \equiv a \pmod{p_i}$ có nghiệm. Áp dụng Mệnh đề 1.1.7 với $n = 2, m = p$ và $d = (n, \phi(m)) = (2, p-1) = 2$, ta thu được phương trình $x^2 \equiv a \pmod{p_i}$ có nghiệm khi và chỉ khi $a^{(p_i-1)/2} \equiv 1 \pmod{p_i}$. □

Kết quả trên rút gọn phương trình thặng dư bậc hai về câu hỏi tương ứng modulo số nguyên tố. Trong phần sau đây, ký hiệu p là số nguyên tố.

Định nghĩa 1.1.14 ([3])**.** Cho p là một số nguyên tố lẻ và cho $a \in \mathbb{Z}$ với $p \nmid a$. *Ký hiệu Legendre*, viết là (a/p), được xác định bởi

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{nếu } a \text{ là một thặng dư bậc hai modulo } p \\ -1, & \text{nếu } a \text{ là một phi thặng dư bậc hai modulo } p. \end{cases}$$

Ta quy ước thêm rằng nếu $p \mid a$ thì $\left(\frac{a}{p}\right) = 0$.

Ví dụ 1.1.15. Theo Ví dụ 1.1.12, ta có $1, 2, 4$ là thặng dư bậc hai modulo 7 nên $(2/7) = 1 = (1/7) = (4/7)$, 3, 5 và 6 là phi thặng dư bậc hai modulo 7 nên $(3/7) = -1 = (5/7) = (6/7)$.

Theo định nghĩa, ký hiệu Legendre (a/p) chỉ ra a có là thặng dư bậc hai modulo p hay không. Nói cách khác, ký hiệu Legendre (a/p) ghi lại phương trình đồng dư bậc hai $x^2 \equiv a \pmod p$ có giải được hay không. Ký hiệu Legendre là công cụ cực kỳ thuận tiện để thảo luận về thặng dư bậc hai.

Mệnh đề 1.1.16 ([3])**.**

(a) $a^{(p-1)/2} \equiv (a/p) \pmod{p}$.

(b) $(ab/p) = (a/p)(b/p)$.

(c) *Nếu* $a \equiv b \pmod{p}$ *thì* $(a/p) = (b/p)$.

Chứng minh. Nếu p là ước của a hoặc của b, tất cả các 3 kết luận trên đều tầm thường. Giả sử $p \nmid a$ và $p \nmid b$.

Ta biết rằng $a^{p-1} \equiv 1 \pmod{p}$, do đó

$$(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Suy ra $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Theo Mệnh đề 1.1.13, ta có $a^{(p-1)/2} \equiv 1 \pmod{p}$ khi và chỉ khi a là thặng dư bậc hai modulo p. Điều này chứng minh (a).

Để chứng minh (b) ta áp dụng phần (a). Ta có

$$(ab)^{(p-1)/2} \equiv (ab/p) \pmod{p}$$

và

$$(ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p)(b/p).$$

Do đó

$$(ab/p) = (a/p)(b/p).$$

Phần (c) được suy ra trực tiếp từ định nghĩa. □

Hệ quả 1.1.17. *Số thặng dư bậc hai modulo p bằng số phi thặng dư bậc hai modulo p.*

Hệ quả 1.1.18. *Tích của hai thặng dư bậc hai là một thặng dư bậc hai, tích của hai phi thặng dư bậc hai là một thặng dư bậc hai, tích của một thặng dư bậc hai với một phi thặng dư bậc hai là phi thặng dư bậc hai.*

Hệ quả 1.1.19. $(-1)^{(p-1)/2} = (-1/p)$.

Hệ quả trên đặc biệt thú vị. Mọi số nguyên lẻ có dạng $4k+1$ hoặc $4k+3$. Sử dụng kết quả này ta có thể phát biểu là Hệ quả 1.1.19 như sau: $x^2 \equiv -1 \pmod{p}$ có nghiệm khi và chỉ khi p có dạng $4k+1$. Do đó -1 là thặng dư bậc hai của các số nguyên tố $5, 13, 17, 29, \ldots$ và là phi thặng dư bậc hai của các số nguyên tố $3, 7, 11, 19, \ldots$.