ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐẶNG TUẤN LONG

BIỂU DIỄN SỐ NGUYÊN THÀNH TỔNG HAI BÌNH PHƯƠNG CỦA SỐ NGUYÊN

LUẬN VĂN THẠC SỸ TOÁN HỌC

THÁI NGUYÊN - 2016

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐẶNG TUẤN LONG

BIỂU DIỄN SỐ NGUYÊN THÀNH TỔNG HAI BÌNH PHƯƠNG CỦA SỐ NGUYÊN

LUẬN VĂN THẠC SỸ TOÁN HỌC

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

NGƯỜI HƯỚNG DẪN KHOA HỌC
GS.TS. TRẦN VŨ THIỆU

Thái Nguyên - 2016

Mục lục

Mở đầu

Lý thuyết số nghiên cứu tập hợp số tự nhiên (các số nguyên dương) 1, 2, 3, 4, 5, 6, 7, ... và các mối quan hệ giữa các loại số khác nhau.

Người ta chia ra nhiều loại số nguyên:

- số chẵn: 2, 4, 6, 8, 10, ...
- số lẻ: 1, 3, 5, 7, 9, 11, ...
- số chính phương: 1, 4, 9, 16, 25, 36, ...
- số lập phương: 1, 8, 27, 64, 125, ...
- số nguyên tố: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...
- hợp số: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, ...
- 1 (modulo 4): 1, 5, 9, 13, 17, 21, 25, ...
- 3 (modulo 4): 3, 7, 11, 15, 19, 23, 27, ...
- số tam giác: 1, 3, 6, 10, 15, 21, 28, ...
- số hoàn hảo: 6, 28, 496, ...
- số Fibonacci: 1, 1, 2, 3, 5, 8, 13, 21, 34, ...

Một trong những mục tiêu chính của lý thuyết số là khám phá ra những quan hệ thú vị bất ngờ giữa các loại số khác nhau và chứng minh những quan hệ này là đúng.

Có nhiều bài toán tiêu biểu về lý thuyết số, trong số đó một số đã có lời giải, một số cho tới nay vẫn chưa giải được.

Một số bài toán đã có lời giải: những số nào bằng tổng bình phương của hai số tự nhiên? Ví dụ, $5 = 1^2 + 2^2, 13 = 2^2 + 3^2, \ldots$

Chúng có những đặc tính chung gì? Có bao nhiêu cách biểu diễn như thế? Bài toán tương tự: số nào bằng tổng lập phương của hai số nguyên dương? Ví dụ, $9 = 1^3 + 2^3, 28 = 1^3 + 3^3, 35 = 2^3 + 3^3, \ldots$

Đặc điểm của những số này là gì?

Đề tài luận văn *Biểu diễn số nguyên thành tổng hai bình phương của số nguyên* có mục đích tìm hiểu và trình bày các kết quả của lý thuyết số về các tính chất đặc trưng của những số nguyên dương (nói riêng là các số nguyên tố) biểu diễn được dưới dạng tổng bình phương của hai số nguyên, số cách biểu diễn thành tổng hai bình phương, một số bài toán và định lý có liên quan tới bài toán tổng của hai số bình phương: bộ số Pythagoras, nghiệm nguyên của phương trình bậc hai với hệ số nguyên, định lý cơ bản của số học, định lý Fermat bé, định lý Wilson, định lý Thue, định lý hai số bình phương, ...

Luận văn được viết dựa chủ yếu trên các tài liệu tham khảo [1] - [6] lấy từ nguồn Internet và được chia thành ba chương.

Chương 1 *Kiến thức chuẩn bị* trình bày lại các khái niệm về các số tự nhiên, số nguyên tố, hợp số, về phép chia hết, phép phân tích số nguyên ra thừa số nguyên tố, về phép tính đồng dư modulo.

Chương 2 *Tổng bình phương của hai số nguyên* đề cập tới bài toán cổ điển trong lý thuyết số: biểu diễn một số nguyên dương (nói riêng, số nguyên tố) dưới dạng tổng hai bình phương của số nguyên. Trình bày các định lý về tính chất đặc trưng của các số nguyên tố, các số nguyên dương biểu diễn được dưới dạng tổng hai bình phương của số nguyên.

Chương 3 *Một số bài toán có liên quan* đề cập tới bài toán mở rộng về biểu diễn số nguyên thành tổng của nhiều số bình phương (bài toán Waring), bộ số Pythagoras ($x^2 + y^2 = z^2$) và Định lý lớn Fermat về sự không tồn tại nghiệm nguyên khác không của phương trình $x^n + y^n = z^n$, với mọi $n > 2$. Cuối chương giới thiệu một số bài toán của lý thuyết số chưa có lời giải.

Nhân dịp này, tác giả xin bày tỏ lòng biết ơn sâu sắc tới thầy hướng dẫn

GS.TS. Trần Vũ Thiệu đã tận tình giúp đỡ trong suốt quá trình làm luận văn. Tác giả cũng xin chân thành cảm ơn các thầy cô giáo của khoa Toán-Tin, Trường Đại học Khoa học Thái Nguyên và của Viện Toán học, Viện Công nghệ thông tin thuộc Viện Hàn lâm Khoa học và Công nghệ Việt Nam đã giảng dạy và tạo điều kiện thuận lợi trong quá trình tác giả học tập và nghiên cứu.

Thái Nguyên, tháng 5 năm 2016

Tác giả luận văn

Đặng Tuấn Long

Chương 1

Kiến thức chuẩn bị

Chương này nhắc lại một số khái niệm cơ bản của lý thuyết số: phần dư của phép chia nguyên, ước chung lớn nhất của các số nguyên, số nguyên tố và hợp số, khái niệm đồng dư và tính chất. Số nguyên Gauss và vành các số nguyên Gauss.

Nội dung của chương được tham khảo từ các tài liệu [1], [2], [3] và [5].

1.1 Ước chung lớn nhất

1.1.1 Ước số và phần dư

Xét tập số nguyên $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$. Từ lý thuyết số, ta biết kết quả sau.

Định lý 1.1 (Định lý chia)**.** *Với mọi $a, b \in \mathbb{Z}, b \neq 0$, tồn tại duy nhất $q, r \in \mathbb{Z}, 0 \leq r < |b|$, sao cho $a = bq + r$. (Chia a cho b được q là thương số, r là phần dư).*

Ví dụ 1.2. a) Với $a = 13, b = 3$ ta có $q = 4, r = 1$, vì $13 = 3 \times 4 + 1$.

b) Với $a = 17, b = -5$ ta có $q = -3, r = 2$, vì $17 = (-5) \times (-3) + 2$.

c) Với $a = -5, b = 4$ ta có $q = -2, r = 3$, vì $-5 = 4 \times (-2) + 3$.

d) Với $a = -11, b = -5$ ta có $q = 3, r = 4$, vì $-11 = (-5) \times 3 + 4$.

Định nghĩa 1.3. Với $a, b \in \mathbb{Z}$, ta nói a là *ước* (divisor) của b nếu tồn tại số nguyên x sao cho $a.x = b$. Trong trường hợp này ta nói rằng b *chia hết* (divisible) cho a hay b là *bội* (multiple) của a và viết $a \mid b$ (đọc là a là ước của b). Trái lại, ta nói a không là ước của b và viết $a \nmid b$.

Ví dụ 1.4. Các ước của 6 là $-6, -3, -2, -1, 1, 2, 3$ và 6. Ta chỉ ra điều này bằng cách viết $-3 \mid 6, 2 \mid 6, 3 \mid 6, \ldots$ Nhưng 4 không là ước của 6 nên ta viết $4 \nmid 6$.

Định nghĩa 1.5. Với bất kỳ $a \in \mathbb{Z}$, các điều sau đây luôn đúng: $1 \mid a$, $-1 \mid a$, $a \mid a$, $-a \mid a$. Ta nói $1, -1, a$ và $-a$ là các *ước tầm thường* (trivial divisors) của a; 1 và -1 gọi là đơn vị (units), mọi ước bất kỳ khác của a gọi là ước *thực sự* (proper divisors).

Ví dụ 1.6. -3, -2, 2, 3 là các ước thực sự của 6.

1.1.2 Số nguyên tố và hợp số

Định nghĩa 1.7. Số nguyên dương $a > 1$ được gọi là một số *nguyên tố* (prime) nếu a không có ước thực sự. Số nguyên dương a gọi là một *hợp số* (composite) nếu a có ước thực sự. Nếu a là số nguyên dương và các số nguyên tố $p_1, p_2, p_3..., p_k$ thỏa mãn $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_k^{\alpha_k}$ thì tích $p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times ... \times p_k^{\alpha_k}$ gọi là *phân tích thừa số nguyên tố* (prime factorization) của a.

Ví dụ 1.8. Các số nguyên tố nhỏ hơn 40 là 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.

Định lý 1.9 (Định lý cơ bản của số học)**.** *Mọi số $a, a > 1$, có phân tích thừa số nguyên tố duy nhất (không kể sự sai khác về thứ tự các thừa số).*

Ví dụ 1.10. $12 = 2^2 \times 3; 18 = 2 \times 3^2; 231 = 3 \times 7 \times 11$.

Định nghĩa 1.11. Cho $a, b \in \mathbb{Z}$. Ta định nghĩa *ước chung lớn nhất* (greatest common divisor) của a và b là số nguyên lớn nhất d mà cả a và b đều chia hết cho $d : d \mid a$ và $d \mid b$. Ước chung lớn nhất được ký hiệu là $(a, b) = d$ hoặc $\gcd(a, b) = d$. Trong luận văn này ta sẽ sử dụng $\gcd(a, b)$ để chỉ ước chung lớn nhất của a và b.

Ví dụ 1.12. Hãy tìm ước chung lớn nhất của 8 và 12. Ta thấy các ước của 8 là ± 1, ± 2, ± 4, ± 8 và các ước của 12 là ± 1, ± 2, ± 3, ± 4, ± 6, ± 12. Từ đó, ước

chung của 8 và 12 là ± 1, ± 2, ± 4. Vì thế, ước chung lớn nhất của 8 và 12 là 4 và ta viết $\gcd(8, 12) = 4$.

Có thể thấy $\gcd(6, -9) = 3, \gcd(-15, 25) = 5$ và $\gcd(-3, -7) = 1$.

Định nghĩa 1.13. Nếu ước chung lớn nhất $\gcd(a, b) = 1$ thì ta nói hai số nguyên a và b là *nguyên tố cùng nhau* (relatively prime).

Định lý 1.14. Nếu $a, b \in \mathbb{Z}$ và $\gcd(a, b) = d$ thì $\gcd(a/d, b/d) = 1$.

Chứng minh. Giả sử $\gcd(a/d, b/d) = k$. Từ đó $a/d = mk, b/d = nk$ với m, n nguyên và ta có $a = mkd, b = nkd$. Điều này cho thấy a và b chia hết cho kd, tức là $kd \mid a$ và $kd \mid b$. Do d là ước chung lớn nhất của a và b nên $kd \leq d$. Suy ra $k \leq 1$. Do k nguyên dương nên phải có $k = 1$. Vậy $\gcd(a/d, b/d) = k = 1$. □

Ví dụ 1.15. Hãy tìm ước chung lớn nhất của 15 và 40. Bằng cách phân tích ra thừa số nguyên tố ta có $15 = 3 \times 5$ và $40 = 2^3 \times 5$. Từ đó, ta tìm được ước chung lớn nhất của 15 và 40 bằng 5, tức là $\gcd(15, 40) = 5$. Ta thấy $\gcd(15/5, 40/5) = \gcd(3, 8) = 1$.

Định lý 1.16. Cho $a, b, c \in \mathbb{Z}$. Khi đó $\gcd(a + cb, b) = \gcd(a, b)$.

Chứng minh. Giả sử $\gcd(a, b) = d, \gcd(a + cb, b) = k$. Ta cần chứng minh rằng $d = k$. Do $\gcd(a, b) = d$ nên $a = pd$ và $b = qd$ với p, q nguyên tố cùng nhau (Định lý 1.14). Trong $\gcd(a + cb, b) = k$ thay $a = pd, b = qd$ và $cb = cqd$, ta được

$$k = \gcd(a + cb, b) = \gcd(pd + cqd, qd) = \gcd((p + cq)d, qd).$$

Đẳng thức này cho thấy ước chung lớn nhất của $(p + cq)d$ và qd bằng d, bởi vì $(p + cq)$ có trong $(p + cq)d$ đúng d lần và q có trong qd cũng d lần.

Vì thế, $\gcd(a + cb, b) = d$, nghĩa là $d = k$. Định lý được chứng minh. □

Ví dụ 1.17. Xét ba số: $a = 110, b = 44, c = 22$. Theo Định lý 1.16, ta có

$$\gcd(110 + 22 \times 44, 44) = \gcd(110, 44)$$

hay

$$\gcd(1078, 44) = \gcd(110, 44).$$

Để kiểm tra đẳng thức này, ta tính $\gcd(1078, 44)$ và $\gcd(110, 44)$. Ta thấy

$$44 = 2^2 \times 11, 110 = 2 \times 5 \times 11 \text{ và } 1078 = 2 \times 7^2 \times 11.$$

Từ đó suy ra $\gcd(1078, 44) = \gcd(110, 44) = 22$. Kết quả kiểm tra đúng.

Định nghĩa 1.18. Cho $a, b \in \mathbb{Z}$. *Tổ hợp tuyến tính* (linear combination) của a và b là tổng có dạng $ax + by$, trong đó $x, y \in \mathbb{Z}$.

Định lý 1.19. *Nếu $a, b, m, n \in \mathbb{Z}$ và c là ước số chung của a và b thì c cũng là ước số của $ma + nb$, nghĩa là $c \mid a$ và $c \mid b$ thì $c \mid (ma + nb)$.*

Chứng minh. Nếu $c \mid a$ và $c \mid b$ thì theo định nghĩa của ước sẽ tìm được $u, v \in \mathbb{Z}$ sao cho $a = cu, b = cv$. Khi đó $ma + nb = mcu + ncv = c(mu + nv)$. Do đó $(ma + nb)$ là bội của c. Vì thế $c \mid (ma + nb)$. □

Ví dụ 1.20. Giả sử $a = 21, b = 39$, và $c = 3$. Ta có $21 = 3 \times 7$ và $39 = 3 \times 13$. Vì thế, 21 và 39 chia hết cho 3. Giả sử $m = 7, n = -3$. Khi đó

$$7 \times 21 - 3 \times 39 = 147 - 117 = 30.$$

Rõ ràng 3 là ước của 30, vì $30 = 3 \times 10$.

Định lý 1.21. *Cho hai số $a, b \in \mathbb{Z}$. Khi đó $d = \gcd(a, b)$ là số nguyên dương nhỏ nhất biểu diễn được dưới dạng $d = ax + by$ với $x, y \in \mathbb{Z}$.*

Chứng minh. Giả sử k là số nguyên dương nhỏ nhất có dạng $k = ax + by$ với $x, y \in \mathbb{Z}$. Ta chứng minh $d = k$. Thật vậy, do d là ước chung của a và b nên theo Định lý 1.19, d cũng là ước của $ax + by$, tức là $d \mid (ax + by) = k$, do đó $d \leq k$.a phải chia hết cho k, vì nếu trái lại thì $a = ku + v$ với $0 < v < k$, trong đó $u, v \in \mathbb{Z}$. Từ đó $v = a - ku = a - u(ax + by) = a(1 - ux) + b(-uy)$. Như vậy, v cũng là một tổ hợp tuyến tính của a và b. Thế nhưng $v < k$, điều này trái với giả thiết: k là số nguyên dương nhỏ nhất có dạng $ax + by$. Chứng minh tương tự cho thấy b cũng chia hết cho k. Vậy phải có $k \leq \gcd(a, b) = d$. Ở trên ta đã thấy $d \leq k$. Vì thế, $k = d$. □

Ví dụ 1.22. Giả sử $a = 51$ và $b = 187$. Ta thấy $51 = 3 \times 17$ và $187 = 11 \times 17$. Từ đó $\gcd(51, 187) = 17$. Nếu chọn $x = 4, y = -1$, ta có $51 \times 4 - 187 \times 1 = 204 - 187 = 17 = \gcd(51, 187)$.