ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN LÊ MINH

MỘT SỐ BÀI TOÁN VỀ QUAN HỆ CHIA HẾT, SỐ NGUYÊN TỐ VÀ ĐỊNH GIÁ $P-$ADIC

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2016

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN LÊ MINH

MỘT SỐ BÀI TOÁN VỀ QUAN HỆ CHIA HẾT, SỐ NGUYÊN TỐ VÀ ĐỊNH GIÁ $P-$ADIC

LUẬN VĂN THẠC SĨ TOÁN HỌC

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

NGƯỜI HƯỚNG DẪN KHOA HỌC:
PGS. TS. ĐÀM VĂN NHỈ

Thái Nguyên - 2016

Mục lục

Mở đầu 1

Chương 1. Quan hệ chia hết, số nguyên tố **3**
1.1 Quan hệ chia hết 3
1.1.1 Quan hệ chia hết 3
1.1.2 Ước chung lớn nhất và thuật toán Euclid 4
1.2 Số nguyên tố và hợp số 10
1.3 Định lý cơ bản của số học 12
1.4 Biểu diễn số và hàm tổng các chữ số 14
1.4.1 Biểu diễn số tự nhiên theo một cơ số 14
1.4.2 Hàm tổng các chữ số của số tự nhiên 16

Chương 2. Số mũ, định giá $p-$adic và vận dụng **19**
2.1 Định lý Euler và số mũ 19
2.1.1 Định lý Euler và Định lý Fermat nhỏ 19
2.1.2 Số mũ theo modulo 20
2.2 Định giá p-adic $v_p(n)$ 21
2.2.1 Khái niệm định giá p-adic 21
2.2.2 Định giá $2-$adic 25
2.3 Kết quả của Wolstenholme, Thue, Schur 26
2.4 Vận dụng giải một số bài thi học sinh giỏi 30
2.4.1 Vận dụng số mũ 30
2.4.2 Vận dụng định giá $p-$adic 35
2.4.3 Vận dụng kết quả Thue, Schur 37
2.4.4 Vận dụng Định lý cơ bản của số học 38
Kết luận 40
Tài liệu tham khảo 41

Mở đầu

Số học luôn được coi là nữ hoàng của Toán học bởi trong nó chứa đựng nhiều vẻ đẹp của tư duy logic. Không như nhiều ngành toán học khác, trong Số học tồn tại rất nhiều giả thuyết chưa có câu trả lời mà học sinh có thể hiểu được với các kiến thức trung học cơ sở. Quá trình tìm kiếm lời giải cho các giả thuyết đó đã làm nhiều tư tưởng lớn, nhiều lý thuyết lớn của toán học được nảy sinh. Nếu như trước đây, Số học vẫn được xem như là lĩnh vực toán học lý thuyết thuần túy, xa rời thực tiễn thì ngày nay, nhờ có sự phát triển mạnh mẽ của công nghệ máy tính mà nhiều thành tựu mới nhất của Số học có ứng dụng trực tiếp vào các lĩnh vực như bảo mật thông tin, mật mã, số hóa. Do Số học được mệnh danh là nữ hoàng của tư duy nên các bài toán về Số học luôn luôn xuất hiện và giữ một vị trí quan trọng trong các kì thi học sinh giỏi quốc gia, quốc tế. Số học như cầu nối tự nhiên đưa học sinh tiếp cận với khoa học hiện đại. Vì thế việc trang bị những kiến thức cơ bản của Số học cho học sinh phổ thông là hết sức cần thiết.

Bản thân tôi là một giáo viên giảng dạy môn Toán ở cấp THCS. Trong quá trình giảng dạy và ôn thi học sinh giỏi, tôi thường xuyên gặp các bài toán số học đặc biệt là các bài toán về quan hệ chia hết và số nguyên tố. Vì vậy, tôi đã chọn đề tài: "Một số bài toán về quan hệ chia hết, số nguyên tố và định giá p-adic" nhằm tìm hiểu sâu hơn về quan hệ chia hết, số nguyên tố và cách vận dụng để giải các bài toán trong các đề thi học sinh giỏi, đặc biệt là việc tìm hiểu bổ đề nâng, định giá p-adic và cách vận dụng chúng.

Ngoài phần mở đầu, kết luận và tài liệu tham khảo, luận văn gồm hai chương:

Chương 1. Trong chương này luận văn tập trung trình bày một số kiến thức cơ bản về lý thuyết chia hết: quan hệ chia hết, số nguyên tố và hợp số, ước chung lớn nhất và thuật toán Euclid, trình bày định lý cơ bản của số học, biểu diễn số tự nhiên theo một cơ số và hàm tổng các chữ số.

Chương 2. Trong chương này luận văn tập trung trình bày về số mũ, định giá p-adic, và vận dụng kết quả đạt được vào việc giải một số bài toán số học trong các đề thi học sinh giỏi.

Luận văn này được hoàn thành dưới sự hướng dẫn và chỉ bảo tận tình của thầy giáo PGS. TS. Đàm Văn Nhỉ - Trường Đại học Sư phạm Hà Nội. Tôi xin bày tỏ lòng kính trọng và biết ơn sâu sắc đến Thầy về sự hướng dẫn hiệu quả cùng những kinh nghiệm trong suốt quá trình học tập, nghiên cứu và hoàn thành luận văn.

Tôi xin gửi tới các thầy, cô giáo khoa Toán - Tin, phòng Sau Đại học, Trường Đại học Khoa Học - Đại học Thái Nguyên cũng như các thầy giáo, cô giáo tham gia giảng dạy lớp Cao học Toán K8B khóa 2014 - 2016 lời cảm ơn sâu sắc về công lao dạy dỗ trong suốt quá trình giáo dục, đào tạo của nhà trường. Tôi cũng xin gửi lời cảm ơn đến Ban giám hiệu trường THCS Đằng Hải - Hải An - Hải Phòng, các bạn bè đồng nghiệp và các bạn học viên đã động viên và giúp đỡ tôi trong quá trình hoàn thành luận văn này.

Hải Phòng, tháng 08 năm 2016.

Học viên

Nguyễn Lê Minh

Chương 1

Quan hệ chia hết, số nguyên tố

1.1 Quan hệ chia hết

1.1.1 Quan hệ chia hết

Định nghĩa 1.1.1. Cho hai số nguyên $a, b \in \mathbb{Z}, b \neq 0$. Số nguyên a được gọi là *chia hết cho* số nguyên b hay b *chia hết* a nếu tồn tại $c \in \mathbb{Z}$ thỏa mãn $a = bc$. Nếu số nguyên a chia hết cho 2 thì a được gọi là số *chẵn*; Còn nếu số nguyên a không chia hết cho 2 thì a được gọi là số *lẻ*.

Trong nhiều trường hợp, thay cho việc nói a chia hết cho b ta viết $a \vdots b$ hoặc nói b chia hết a và viết $b \mid a$.[1] Khi $a = bc$ thì b được gọi là *một ước* của a. Sau đây ta có các tính chất cơ bản về quan hệ chia hết.

(1) $1 \mid a$ với mọi $a \in \mathbb{Z}$.

(2) $a \mid a$ với mọi $a \in \mathbb{Z}, a \neq 0$.

(3) Nếu $a \mid b$ và $b \mid c$ thì $a \mid c$ với mọi $a, b, c \in \mathbb{Z}$ và $b \neq 0$.

(4) Nếu $a \mid b$ thì $|a| \leqslant |b|$ với mọi $a, b \in \mathbb{Z}$ và $b \neq 0$.

(5) Nếu $a \mid b_i$ với $a, b_i \in \mathbb{Z}, i = 1, \ldots, n$, thì $a \mid \sum\limits_{i=1}^{n} b_i x_i$ với $x_i \in \mathbb{Z}$.

(6) Nếu $a \mid b$ và $b \mid a$ thì $a = b$ hoặc $a = -b$ với $a, b \in \mathbb{Z}$ và $a, b \neq 0$.

Định lý 1.1.2. [Phép chia có dư] *Với mỗi cặp số nguyên $a, b \in \mathbb{Z}, b \neq 0$, tồn tại duy nhất một cặp số nguyên $q, r \in \mathbb{Z}$ sao cho $a = qb + r$, với $0 \leqslant r < |b|$.*

---

[1] Theo thông lệ quốc tế, người ta hay dùng ký hiệu $b \mid a$ thay cho $a \vdots b$.

Chứng minh: Sự tồn tại: Đặt $T = \{n|b|$ sao cho $n|b| \leqslant a, n \in \mathbb{Z}\}$. Vì $|b| \geqslant 1$ nên $-|a||b| \leqslant -|a| \leqslant a$. Do đó $-|a||b| \in T$, vậy $T \neq \emptyset$. Vì T là tập bị chặn trên nên T có một số lớn nhất $m|b|$. Từ $m|b| \leqslant a$ ta suy ra $r = a - m|b| \geqslant 0$ và $r \in \mathbb{Z}$. Ta lại có $(m+1)|b| = m|b| + |b| > m|b|$. Do tính lớn nhất của $m|b|$ trong T nên $(m+1)|b| > a$. Như vậy $|b| > a - m|b| = r$ và ta có $a = qb + r$ với $0 \leqslant r < |b|$.
Tính duy nhất: Giả sử có hai sự biểu diễn $a = qb + r$ với $0 \leqslant r < |b|$ và $a = q_1 b + r_1$ với $0 \leqslant r_1 < |b|$. Trừ vế cho vế, ta được $r - r_1 = b(q_1 - q)$. Nhưng $|r - r_1| < |b|$ do đó $|q_1 - q||b| < |b|$. Vậy $q = q_1$ và hiển nhiên $r = r_1$. □

Trong biểu diễn $a = qb + r, 0 \leqslant r < |b|$, ở định lý trên, q được gọi là *thương* và r gọi là *số dư* trong phép chia a cho b. Rõ ràng $r = 0$ nếu và chỉ nếu $b \mid a$.

Ví dụ 1.1.3. *Ta có các ví dụ sau:*

(1) *Với* $a = 57, b = 14$ *thì* $q = 4$ *và* $r = 1$.

(2) *Với* $a = -82, b = -17$ *thì* $q = 5$ *và* $r = 3$.

(3) *Với* $a = -51, b = 10$ *thì* $q = -6$ *và* $r = 9$.

1.1.2 Ước chung lớn nhất và thuật toán Euclid

Ước chung lớn nhất

Cho a, b là các số nguyên không đồng thời bằng 0, khi đó tập hợp các ước chung của a và b là hữu hạn.

Định nghĩa 1.1.4. Ước chung lớn nhất của hai số a và b không đồng thời bằng 0 là số nguyên lớn nhất là ước của cả a và b. Ta kí hiệu ước chung lớn nhất bởi $\gcd(a, b)$ hoặc (a, b).

Định nghĩa 1.1.5. Các số nguyên a, b được gọi là *nguyên tố cùng nhau* nếu $(a, b) = 1$.

Định lý 1.1.6. *Cho a và b là hai số nguyên không đồng thời bằng 0, khi đó tồn tại số nguyên x_0, y_0 sao cho $ax_0 + by_0 = (a, b)$. Hơn nữa*

$$\{ax + by; x, y \in \mathbb{Z}\} = \{k(a, b); k \in \mathbb{Z}\}.$$

Chứng minh: Đặt $S = \{ax + by; x, y \in \mathbb{Z}\}$ và gọi d là số nguyên dương nhỏ nhất thuộc S. Giả sử x_0, y_0 là hai số nguyên sao cho $ax_0 + by_0 = d$. Ta chứng minh $\{kd; k \in \mathbb{Z}\} = S$. Thật vậy, hiển nhiên rằng $\{kd; k \in \mathbb{Z}\} \subset S$. Xét phần tử tùy ý $u = ax_1 + by_1 \in S$. Bởi Định lý **??**, tồn tại hai số nguyên q, r với $u = dq + r$ và $0 \leqslant r < d$. Mặt khác

$$r = u - dq = a(x_1 - x_0 q) + b(y_1 - y_0 q) \in S.$$

Suy ra $r = 0$ và $u = dq$. Hơn nữa, từ $a, b \in S$ nên theo trên $d \mid a$ và $d \mid b$, dẫn đến d là một ước chung của a, b, vậy $d \leqslant (a, b)$. Lại có $d = ax_0 + by_0$ nên $(a, b)|d$, do đó $(a, b) \leqslant d$. Tóm lại $d = (a, b)$. □

Từ chứng minh trên ta nhận được hệ quả sau:

Hệ quả 1.1.7. (1) *Ước chung lớn nhất của a, b chính là số nguyên dương nhỏ nhất biểu diễn được dưới dạng $ax + by$ với $x, y \in \mathbb{Z}$.*

(2) *Mọi ước chung của a, b đều là ước của (a, b).*

(3) *Nếu $a, b, c, d \in \mathbb{Z} \setminus \{0\}, a = bc + d$ thì $(a, b) = (b, d)$.*

(4) $(0, a) = |a|$ *với mọi* $a \in \mathbb{Z}, a \neq 0$.

Thuật toán Euclid

Để tìm ước chung lớn nhất của hai số, chúng ta thường phân tích số đó thành nhân tử. Ví dụ $(55, 85) = (5 \cdot 11, 5 \cdot 17) = 5; (225, 180) = (3^2 \cdot 5^2, 3^2 \cdot 5 \cdot 2^2) = 3^2 \cdot 5 = 45$. Tuy nhiên việc tìm ước chung lớn nhất theo cách này thực sự khó nếu hai số đã cho khá lớn. Hãy thử tìm $(1324567908, 25367892)$? Bằng cách sử đụng phép chia với dư, Định lý **??**, người ta đã chỉ ra một thuật toán cho phép tìm ước chung lớn nhất của hai số một cách nhanh chóng, đó là thuật toán Euclid.

Định lý 1.1.8. [Thuật toán Euclid] *Cho $a, b \in \mathbb{Z}, b > 0$. Thực hiện liên tiếp các phép chia có dư, ta có*

$$\begin{aligned}
a &= q_0 b + r_1 \ \text{ với } \ 0 < r_1 < b, \\
b &= q_1 r_1 + r_2 \ \text{ với } \ 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \ \text{ với } \ 0 < r_3 < r_2 \\
&\dots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \ \text{ với } \ 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n, q_n > 1.
\end{aligned}$$

Khi đó $(a, b) = r_n$.

Chứng minh: Đặt $d = (a, b)$, khi đó $d \mid r_i$ với $0 \leqslant i \leqslant r_n$. Suy ra $d \leqslant r_n$ từ $r_n > 0$. Bằng quy nạp ta suy ra $r_n \mid r_{n-j}$ với $1 \leqslant j \leqslant n$. Do đó $r_n \mid a$ và $r_n \mid b$. Bởi định nghĩa của (a, b) ta suy ra $r_n = (a, b)$. □

Chú ý rằng, do $(a, b) = (b, r)$ nên ta có thể giả thiết hai số nguyên a và b không âm và $a \geqslant b$.

Như đã nhận xét ở trên, (a, b) chính là số nguyên dương nhỏ nhất biểu diễn được dưới dạng $ax + by$ với $x, y \in \mathbb{Z}$. Vấn đề đặt ra là tìm x, y như thế nào? Thuật toán Euclid sẽ cho ta cách tìm ra chúng qua kết quả dưới đây:

Định lý 1.1.9. *Nếu $d = (a, b)$ thì có $x, y \in \mathbb{Z}$ thỏa mãn $d = ax + by$.*

Chứng minh: Xây dựng hai dãy số nguyên $(a_i), (b_i)$ theo công thức truy hồi sao cho

$$r_i = a_i a + b_i b, i = 0, 1, 2, \ldots \text{với } r_0 = r.$$

Vì $r = a - q_0 b$, nên ta chọn $a_0 = 1, b_0 = -q_0$ và có được $r_0 = r = a_0 a + b_0 b$. Từ $a_1 a + b_1 b = r_1 = b - q_1 r_0 = b - q_1(a_0 a + b_0 b)$ nên ta có thể chọn $a_1 = -q_1 a_0 = -q_1, b_1 = 1 - q_1 b_0 = 1 + q_0 q_1$. Tổng quát, bởi

$$a_{i+1} a + b_{i+1} b = r_{i+1} = r_{i-1} - q_{i+1} r_i = a_{i-1} a + b_{i-1} b - q_{i+1}(a_i a + b_i b)$$

ta chọn công thức truy hồi

$$\begin{cases} a_0 = 1 \\ b_0 = -q_0 \end{cases} \quad \begin{cases} a_1 = -q_1 \\ b_1 = 1 + q_0 q_1 \end{cases} \quad \begin{cases} a_{i+1} = a_{i-1} - q_{i+1} a_i \\ b_{i+1} = b_{i-1} - q_{i+1} b_i, i \geqslant 1. \end{cases}$$

Vì $q_m = 0$ nên $x = a_{m-1}, y = b_{m-1}$ thỏa mãn $xa + yb = (a, b)$. □

Ví dụ 1.1.10. *Với $a = 1832, b = 234$, ta có $(a, b) = 2$ và $a \cdot (-41) + b \cdot 321 = 2$.*

Hệ quả 1.1.11. *Cho $a, b \in \mathbb{Z}$ không đồng thời bằng không. Khi đó $(a, b) = 1$ khi và chỉ khi tồn tại $x, y \in \mathbb{Z}$ để $ax + by = 1$.*

Tổng quát hơn nữa ta có hệ quả sau:

Hệ quả 1.1.12. *Cho $a, b \in \mathbb{Z}$ không đồng thời bằng không. Khi đó $(a, b) = d$ khi và chỉ khi tồn tại $x, y \in \mathbb{Z}$ để $ax + by = d$ và d là ước chung của a và b.*

Chứng minh: Ta có $(a, b) = d$ khi và chỉ khi $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Theo Hệ quả **??** tồn tại $x, y \in \mathbb{Z}$ để $\frac{a}{d}x + \frac{b}{d}y = 1$. Nhân hai vế với d ta có $ax + by = d$. □

Hệ quả 1.1.13. *Cho $a, b, c \in \mathbb{Z}$ không đồng thời bằng không. Nếu $(a, c) = 1$, $(b, c) = 1$ thì $(ab, c) = 1$.*

Chứng minh: Theo Hệ quả **??** tồn tại $x, y, z, t \in \mathbb{Z}$ để $ax + cy = 1, bz + ct = 1$. Nhân vế với vế ta có

$$1 = (ax + cy)(bz + ct) = abxy + c(axt + byz + cyt).$$

Vẫn theo Hệ quả **??** ta có $(ab, c) = 1$. □

Hệ quả 1.1.14. *Cho số nguyên tố p và số nguyên tuỳ ý m. Khi đó*

(1) $$(m, p) = \begin{cases} p & \text{nếu } p \mid m \\ 1 & \text{nếu } p \nmid m. \end{cases}$$

(2) *Nếu $p \mid ab$ thì $p \mid a$ hoặc $p \mid b$.*

Định nghĩa 1.1.15. Cho các số nguyên $a_1, \ldots, a_n \in \mathbb{Z}$ không đồng thời bằng 0. Số nguyên d được gọi là *ước chung* của các a_i nếu $d \mid a_i$ với mọi $i = 1, \ldots, n$.

Hiển nhiên $+1, -1$ là ước chung của mọi tập hữu hạn các số nguyên. Ký hiệu tập tất cả các ước chung của $a_1, \ldots, a_n \in \mathbb{Z}$ là $\mathrm{uc}(a_1, \ldots, a_n)$ và ta thấy ngay tập này khác rỗng. Ví dụ $\mathrm{uc}(18, -15, 21) = \{1, -1, 3, -3\}$.

Định nghĩa 1.1.16. Cho các số nguyên $a_1, \ldots, a_n \in \mathbb{Z}$ không đồng thời bằng 0. Số nguyên d được gọi là *ước chung lớn nhất* của các a_i nếu d là số nguyên lớn nhất trong các ước chung của các a_i. Ta kí hiệu ước chung lớn nhất là $(a_1, a_2, \ldots, a_n)$.

Như vậy, số nguyên d là ước chung lớn nhất của $a_1, \ldots, a_n \in \mathbb{Z}$ khi và chỉ khi $d \mid a_i, i = 1, \ldots, n$, và nếu $c \mid a_i, i = 1, \ldots, n$, thì $c \mid d$. Khi số nguyên d là ước chung lớn nhất của $a_1, \ldots, a_n$ thì $-d$ cũng là ước chung lớn nhất của $a_1, \ldots, a_n$. Người ta ký hiệu ước chung lớn nhất của $a_1, \ldots, a_n$ qua $(a_1, \ldots, a_n)$ và chọn nó là $|d|$. Dễ thấy rằng, $(a_1, \ldots, a_n)$ là số nguyên dương lớn nhất nằm trong tập $\mathrm{uc}(a_1, \ldots, a_n)$.

Chú ý. Mọi số nguyên đều là ước của 0. Vậy $\mathrm{uc}(0, \ldots, 0) = \mathbb{Z}$ và không có $(0, \ldots, 0)$. Vì thế ta không xét trường hợp này.

Từ việc chứng minh ước chung lớn nhất cho hai số, chúng ta có thể tổng quát lên các tính chất sau cho nhiều số: