ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

——————o0o——————

PHẠM THỊ ĐỊNH

ỨNG DỤNG CỦA CẤP VÀ CHỈ SỐ CHO SỐ NGUYÊN THEO MODULO

THÁI NGUYÊN, 5/2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

——————o0o——————

PHẠM THỊ ĐỊNH

ỨNG DỤNG CỦA CẤP VÀ CHỈ SỐ CHO SỐ NGUYÊN THEO MODULO

Chuyên ngành: **Phương pháp Toán sơ cấp**
Mã số: **8460113**

LUẬN VĂN THẠC SĨ TOÁN HỌC

GIÁO VIÊN HƯỚNG DẪN

TS. NGÔ THỊ NGOAN

THÁI NGUYÊN, 5/2019

Mục lục

Lời cảm ơn

Trước tiên tôi xin gửi lời cảm ơn chân thành và sâu sắc nhất tới TS. Ngô Thị Ngoan với lòng nhiệt huyết đã luôn chỉ bảo tận tình cho tôi từ những ngày đầu tiên, đồng thời đưa ra những lời khuyên bổ ích giúp tôi hoàn thiện luận văn này.

Tôi cũng xin gửi lời cảm ơn tới các thầy cô, tập thể cán bộ khoa Toán - Tin, Trường Đại học Khoa học - Đại học Thái Nguyên, Ban lãnh đạo và các đồng nghiệp trường Trung học phổ thông Hoành Bồ - tỉnh Quảng Ninh, cùng các bạn học viên lớp cao học toán K11D, đã không chỉ trang bị cho tôi những kiến thức bổ ích mà còn luôn giúp đỡ, tạo điều kiện thuận lợi trong quá trình tôi học tập tại trường.

Cuối cùng tôi xin cảm ơn gia đình, bạn bè người thân là những người luôn ủng hộ, động viên tôi vượt qua những khó khăn để em hoàn thành tốt luận văn.

Thái Nguyên, ngày 25 tháng 5 năm 2019

Mở đầu

Nội dung luận văn nghiên cứu về khái niệm và tính chất của cấp và chỉ số cho số nguyên theo modulo m, đồng thời xét một số ứng dụng điển hình của chúng trong các bài toán số học có liên quan. Luận văn bao gồm hai chương.

Chương 1 của luận văn trình bày các kiến thức chuẩn bị về lý thuyết chia hết trong tập số nguyên, đồng dư thức, các lớp thặng dư đầy đủ, hệ thặng dư đầy đủ, hệ thặng dư thu gọn .... Các kiến thức này được tham khảo chủ yếu từ tài liệu [1].

Nội dung của Chương 2 gồm 6 mục, từ Mục 2.1 đến Mục 2.6, đề cập đến các khái niệm và ứng dụng của cấp cho số nguyên theo modulo, căn nguyên thủy modulo, chỉ số cho số nguyên theo modulo. Trước tiên luận văn trình bày về khái niệm cấp cho số nguyên a theo modulo m (với điều kiện a nguyên tố với modulo m), đó là số mũ nguyên dương nhỏ nhất e sao cho $a^e \equiv 1 \pmod{m}$, kí hiệu $e = \operatorname{ord}_m a$. Sau đó luận văn giới thiệu khái niệm và tính chất của căn nguyên thủy cho số nguyên theo modulo m, đó là thặng dư không âm nhỏ nhất α modulo m thỏa mãn $\operatorname{ord}_m \alpha = \varphi(m)$. Khái niệm căn nguyên thủy modulo m có nhiều ứng dụng trong số học, chẳng hạn nó sẽ sinh ra đủ $\varphi(m)$ thặng dư nguyên tố với modulo m,... Tiếp đến luận văn khảo sát tiêu chuẩn để kiểm tra tính nguyên tố của một số số nguyên dương bằng cách ứng dụng các tính chất của cấp cho số nguyên theo modulo và căn nguyên thủy modulo (Định lý 2.3.1). Vì vai trò quan trọng của căn nguyên thủy trong số học và những bài toán liên quan nên, luận văn khảo sát kĩ hơn về bài toán nhận diện các căn nguyên thủy modulo số nguyên tố (Định lý 2.4.7), đó cũng là áp dụng hiệu quả của cấp cho số nguyên theo modulo. Lưu ý rằng có những số nguyên dương không có căn nguyên thủy, chẳng hạn: số 8, số 12 đều không có căn nguyên thủy,... Do đó, tiếp đến luận văn trình bày ứng dụng của cấp cho

số nguyên theo modulo vào bài toán nhận diện lớp các số nguyên dương có các căn nguyên thủy đó là các số nguyên $1, 2, 4, p^k, 2p^k$ với p là số nguyên tố lẻ (Định lý 2.5.19). Phần cuối của luận văn giới thiệu khái niệm chỉ số cho số nguyên theo modulo đối với một cơ số, và xét một số ứng dụng vào phương trình đồng dư. Ngoài ra luận văn cũng trình bày nhiều ví dụ minh họa giúp cho người đọc dễ theo dõi, và đó cũng là những bài tập thích hợp cho phổ thông. Dưới đây là tóm lược nội dung các mục của Chương 2.

- Mục 2.1 sẽ đề cập đến các khái niệm và tính chất cơ bản về cấp cho số nguyên theo modulo và các ví dụ minh họa.
- Mục 2.2 trình bày về khái niệm và tính chất của căn nguyên thủy modulo.
- Mục 2.3 trình bày ứng dụng của cấp cho số nguyên theo modulo vào bài toán kiểm tra tính nguyên tố dựa trên định lý Lucas và các hệ quả của nó.
- Mục 2.4 trình bày ứng dụng của cấp cho số nguyên theo modulo vào nhận diện các căn nguyên thuỷ của số nguyên tố.
- Mục 2.5 khảo sát ứng dụng của cấp cho số nguyên theo modulo vào bài toán nhận diện các số nguyên có căn nguyên thủy.
- Mục 2.6 dành để trình bày về một khái niệm tương tự khái niệm lôgarit, đó là khái niệm chỉ số cho số nguyên theo modulo đối với một cơ sở, và xét một vài ứng dụng của nó vào phương trình đồng dư.

Thái Nguyên, ngày 25 tháng 5 năm 2019

Tác giả luận văn

Phạm Thị Định

Chương 1

Kiến thức chuẩn bị

Nội dung Chương 1 được tham khảo chủ yếu từ tài liệu [1] và một phần nhỏ trong tài liệu [3]. Các kiến thức ở chương này nhằm chuẩn bị những kiến thức cơ bản giúp cho việc trình bày chương sau được hệ thống và dễ theo dõi hơn.

Mục 1.1 sẽ nhắc lại về lý thuyết chia hết trong tập số nguyên; đồng thời mục này cũng nhắc lại khái niệm hệ số nhị thức và định lý nhị thức.

Mục 1.2 nhắc lại các khái niệm cơ bản về đồng dư thức thức, hệ thặng dư đầy đủ, định lý Euler, định lý Fermat nhỏ, phương trình đồng dư.

1.1 Lý thuyết chia hết trong tập số nguyên

Trong tập hợp số nguyên $\mathbb{Z}$, các phép toán cộng, trừ và nhân luôn thực hiện được, tuy nhiên phép chia cho một số nguyên khác 0 không phải bao giờ cũng thực hiện được, nghĩa là phương trình $ax = b$, trong đó $a, b \in \mathbb{Z}; a \neq 0$ không phải lúc nào cũng có nghiệm trong $\mathbb{Z}$. Trong trường hợp $ax = b$ có nghiệm trong $\mathbb{Z}$, chúng ta đi đến khái niệm chia hết.

Định nghĩa 1.1.1. Giả sử a, b là hai số nguyên, $b \neq 0$. Ta nói b *chia hết* a hay b là một *ước* của a và kí hiệu $b \mid a$ nếu như có một số nguyên q sao cho $a = bq$. Khi đó ta cũng nói a *chia hết cho* b hay a là bội của b và viết $a \vdots b$.

Khi b không chia hết a ta kí hiệu là $b \nmid a$.

Ví dụ 1.1.2. Trong tập số nguyên $\mathbb{Z}$, ta có

(i) -5 chia hết 10 hay 10 chia hết cho -5, vì $10 = (-2).(-5)$.

(ii) 1 và -1 là ước của mọi số nguyên a vì $a = 1.a = (-1).(-a)$.

(iii) 0 là bội của mọi số nguyên $b \neq 0$ vì $0 = b.0$.

Chú ý 1.1.3. Nếu $b \mid a$ và $a \neq 0$ thì từ $a = bq$ ta có $q \neq 0$ do đó $|q| \geq 1$ cho nên $|a| = |b|.|q| \geq |b|$.

Các tính chất chia hết sẽ được trình bày vắn tắt dưới đây.

(i) Số nguyên a là ước của 1 khi và chỉ khi $a = \pm 1$.

(ii) Nếu $b \mid a$ thì $\pm b \mid \pm a$.

(iii) Nếu $a \mid b$ và $b \mid a$ thì $a = \pm b$.

(iv) Nếu $b \mid a_1,\ b \mid a_2, \ldots, b \mid a_n$, với $b, a_1, a_2, \ldots, a_n \in \mathbb{Z}$ thì $b \mid (a_1x_1 + a_2x_2 + \cdots + a_nx_n),\ \forall x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

Định lý 1.1.4. *Với mỗi cặp số nguyên a, b cho trước ($b \neq 0$), tồn tại duy nhất cặp số nguyên q, r thỏa mãn hệ thức*

$$a = bq + r,\ \ 0 \leq r < |b|.$$

Chứng minh. Sự tồn tại cặp số nguyên q, r: Xét tập hợp M gồm các bội của b không vượt quá a

$$M = \{bx : x \in \mathbb{Z}, bx \leq a\}.$$

Ta thấy $-|b|.|a|$ là một bội của b không vượt quá a nên $M \neq \emptyset$. Hơn nữa, M là một bộ phận của $\mathbb{Z}$ và bị chặn trên bởi a do đó trong M có số lớn nhất, chẳng hạn là $bq, q \in \mathbb{Z}$. Vì $|b| \geq 1$ nên $ba + |b| > bq$, do đó $bq + |b| \notin M$ cũng là bội của b cho nên ta có

$$bq \leq a < bq + |b| \ \text{ hay } \ 0 \leq a - bq < |b|.$$

Đặt $r = a - bq$ ta được $r \in \mathbb{Z},\ a = bq + r$ và $0 \leq r < |b|$.

Để chứng minh tính duy nhất của cặp q, r ta giả sử có cặp số nguyên q_1, r_1 cùng thỏa mãn hệ thức

$$a = bq + r,\ 0 \leq r < |b|;$$
$$a = bq_1 + r_1,\ 0 \leq r_1 < |b|.$$

Từ đây ta có

$$b(q - q_1) = -(r - r_1) \text{ và } |r - r_1| < |b|.$$

Khi đó do $|b| > 0$ và $|b||q - q_1| = |r - r_1| < |b|$ ta được $|q - q_1| < 1$. Do đó $|q - q_1| = 0$ hay $q = q_1$ kéo theo $r = r_1$. □

Định nghĩa 1.1.5. Cho a, b là các số nguyên cho trước, $b \neq 0$. Khi có đẳng thức $a = bq + r$, trong đó q là một số nguyên, $0 \leq r < |b|$, thì ta nói *a chia cho b được thương là q và số dư r*. Kí hiệu $a \equiv r \pmod{b}$.

Chú ý 1.1.6. Trong trường hợp số dư $r = 0$, ta có $a = bq$, nghĩa là a chia hết cho b. Như vậy, phép chia hết là một trường hợp riêng của phép chia có dư.

Số nguyên d được gọi là một *ước chung* của các số nguyên $a_1, a_2, \ldots, a_n$ nếu d là ước đồng thời của mỗi số nguyên đó.

Một ước chung d của các số nguyên $a_1, a_2, \ldots, a_n$ sao cho mọi ước chung của $a_1, a_2, \ldots, a_n$ đều là ước của d được gọi là *ước chung lớn nhất* (viết tắt là ƯCLN) của các số đó.

Các số nguyên $a_1, a_2, \ldots, a_n$ được gọi là *nguyên tố cùng nhau* nếu như ƯCLN của các số đó là 1.

Số tự nhiên lớn hơn 1 không có ước nào khác ngoài 1 và chính nó được gọi là *số nguyên tố*.

Chúng ta sẽ nhắc lại định lý cơ bản nhưng không đề cập đến chứng minh của nó.

Định lý 1.1.7 (Định lý cơ bản)**.** *Mỗi số tự nhiên lớn hơn 1 đều phân tích được thành tích những thừa số nguyên tố và sự phân tích đó là duy nhất nếu không kể đến thứ tự của các thừa số.*

Nội dung định lý cơ bản đã nói lên vai trò quan trọng của số nguyên tố trong tập các số tự nhiên: mỗi số tự nhiên lớn hơn 1 đều được "cấu tạo" từ những số nguyên tố bởi phép nhân, mà chúng ta biết số nguyên tố là những số có ít ước nhất. Từ định lý cơ bản, các nhà toán học đã đi đến các ứng dụng của nó như: tiêu chuẩn chia hết, ước chung lớn nhất - bội chung nhỏ nhất. Các ứng dụng của định lý cơ bản đã được đề cập trong chương trình học đại học, trong luận văn này ta bỏ qua không nhắc lại.

Phần cuối của mục này ta nhắc lại khái niệm và tính chất của hệ số nhị thức.

Định nghĩa 1.1.8. Cho n, r là các số nguyên không âm, *hệ số nhị thức* được kí hiệu là $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ nếu $r \leq n$ và bằng 0 nếu ngược lại; ta cũng thường kí hiệu hệ số nhị thức bởi C_n^r.

Từ định nghĩa, ta có $\binom{n}{0} = 1 = \binom{n}{n}$ và $\binom{n}{r} = \binom{n}{n-r}$.

Định lý 1.1.9 (Đồng nhất thức Pascal)**.** *Cho n và r là hai số nguyên dương, trong đó $r \leq n$. Khi đó $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$.*

Chứng minh. Ta sẽ biến đổi vế phải và đưa dần dần về vế trái:

$$\begin{aligned}
\binom{n-1}{r-1} + \binom{n-1}{r} &= \frac{(n-1)!}{(r-1)!(n-r)!} + \frac{(n-1)!}{r!(n-r-1)!} \\
&= \frac{r(n-1)!}{r(r-1)!(n-r)!} + \frac{(n-r)(n-1)!}{r!(n-r)(n-r-1)!} \\
&= \frac{r(n-1)!}{r!(n-r)!} + \frac{(n-r)(n-1)!}{r!(n-r)!} \\
&= \frac{(n-1)![r+(n-r)]}{r!(n-r)!} = \frac{(n-1)!n}{r!(n-r)!} \\
&= \frac{n!}{r!(n-r)!} = \binom{n}{r}.
\end{aligned}$$

□

Định lý sau đây chỉ ra rằng ta có thể sử dụng các hệ số nhị thức để tìm khai triển của $(x+y)^n$.

Định lý 1.1.10 (Định lý nhị thức)**.** *Cho x, y là hai số thực bất kỳ và n là số nguyên không âm. Khi đó $(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$.*

Chứng minh. Chứng minh bằng phương pháp quy nạp. Với $n = 0$, ta có $(x+y)^0 = 1$ và $\sum_{r=0}^{0} \binom{r}{0} x^{0-r} y^r = x^0 y^0 = 1$. Do đó giả thiết đúng với $n = 0$. Giả sử định lý đúng với số $k \geq 0$ nào đó, tức là

$$(x+y)^k = \sum_{r=0}^{k} \binom{k}{r} x^{k-r} y^r. \tag{1.1}$$