ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI THỊ THỦY

MỘT SỐ TÍNH CHẤT SỐ HỌC CỦA HỆ SỐ NHỊ THỨC

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2016

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

BÙI THỊ THỦY

MỘT SỐ TÍNH CHẤT SỐ HỌC CỦA HỆ SỐ NHỊ THỨC

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: **Phương pháp Toán sơ cấp**

Mã số: **60 46 01 13**

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. NGUYỄN DUY TÂN

Thái Nguyên - 2016

Mục lục

Lời nói đầu

Đồng dư số học là một chủ đề cổ điển nhưng vẫn luôn ẩn chứa nhiều kết quả đẹp đẽ và sâu sắc, thu hút nghiên cứu của các nhà toán học. Tính chất đồng dư của hệ số nhị thức là một trong số đó. Khởi đầu từ phát biểu của nhà toán học người Đức Ernst Kummer trong bài báo *"Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen"* công bố năm 1852, người ta bắt đầu quan tâm đến đồng dư theo modulo nguyên tố của hệ số nhị thức, và ý nghĩa của nó theo biểu diễn trong cơ số nguyên tố đó. Nếu như phát biểu của Kummer nghe còn tương đối mơ hồ thì đến năm 1878, nhà toán học Pháp Édouard Lucas trong serie bài báo đăng trên American Journal of Mathematics, *Théorie des Fonctions Numériques Simplement Périodiques*, đã phát biểu một cách tường minh cho mối liên hệ đồng dư theo modulo nguyên tố của hệ số nhị thức với tích các hệ số nhị thức tạo thành từ các chữ số trong biểu diễn của các thành phần trong hệ số nhị thức theo cơ số của chính số nguyên tố ấy.

Không chỉ dừng lại ở việc là một phát biểu tường minh, kết quả của Lucas còn làm tiền đề và tạo cảm hứng cho những mở rộng đầu tiên của Anton (1969), Stickelberger (1890) và Hensel (1902). Vẫn dựa trên biểu diễn của các thành phần trong hệ số nhị thức theo cơ số nguyên tố, họ xem xét tính chất đồng dư theo cơ số nguyên tố của hệ số nhị thức sau khi chia cho lũy thừa bậc cao nhất của số nguyên tố chia hết nó. Đây là một kết quả đặc sắc, nhưng trong suốt hơn 112 năm từ sau Định lý Lucas, không có thêm một mở rộng nào nữa, cho tới khi Granville nâng modulo từ số nguyên tố thành lũy thừa của nó.

Một hướng mở rộng khác của Định lý Lucas đó là loại bỏ biểu diễn theo cơ số nguyên tố mà liên kết trực tiếp số nguyên tố, các số thành phần trong hệ số nhị thức và bậc lũy thừa cao nhất chia hết hệ số nhị thức của

số nguyên tố đó. Bắt đầu từ kết quả của Charles Babbage (1819) - một mở rộng lên lũy thừa bậc hai cho một hệ quả đặc biệt của Định lý Lucas - sau đó Joseph Wolstenholme đã mở rộng chính kết quả này lên bậc ba. Được gợi ý từ những kết quả này, Ljunggren (1949) đã chứng minh một kết quả kiểu Lucas, rằng hệ số nhị thức của hai bội của một số nguyên tố sẽ đồng dư với chính hệ số nhị thức gồm hai thành phần thu được sau khi chia các bội cho số nguyên tố kia, theo modulo lũy thừa bậc ba của số nguyên tố đó. Kết quả cuối cùng của E. Jacobsthal mở rộng chính kết quả của Ljunggren lên lũy thừa bậc cao hơn.

Luận văn có cấu trúc như sau: Mở đầu, ba chương, Kết luận và Tài liệu tham khảo

Chương 1: *Định lý Kummer và Định lý Lucas*

Chương này phát biểu và chứng minh hai định lý trên, kèm theo các hệ quả, chứng minh của chúng và một số bài tập ứng dụng.

Chương 2: *Hệ số nhị thức modulo lũy thừa nguyên tố*

Chương này trình bày hai mở rộng của Định lý Wilson, một mở rộng của Định lý Lucas và cuối cùng là kết quả của Granville về hệ số nhị thức modulo lũy thừa nguyên tố.

Chương 3: *Định lý Wolstenholme*

Trình bày các kết quả về đồng dư của hệ số nhị thức với thành phần nguyên tố modulo lũy thừa nguyên tố, từ kết quả của Charles Babbage, tới Định lý Wolstenholme và mở rộng của nó là Định lý Ljunggren.

Luận văn này được thực hiện và hoàn thành vào tháng 6 năm 2016 tại trường Đại học Khoa học- Đại học Thái Nguyên. Qua đây, tác giả xin bày tỏ lòng biết ơn sâu sắc tới TS Nguyễn Duy Tân, người đã tận tình hướng dẫn trong suốt quá trình làm việc để hoàn thành luận văn này. Tác giả xin gửi lời cảm ơn chân thành đến Khoa Toán, Trường Đại học Khoa học- Đại học Thái Nguyên, đã tạo mọi điều kiện để giúp tác giả học tập và hoàn thành luận văn cũng như chương trình thạc sĩ.Tác giả cũng xin gửi lời cảm ơn tới tập thể lớp cao học YB, khóa 06/2014 - 06/2016 đã động viên giúp đỡ tác giả trong quá trình học tập và hoàn thành luận văn này.Đồng thời tác giả

xin gửi lời cảm ơn tới Sở GD-ĐT tỉnh Yên Bái, Ban giám hiệu và các đồng nghiệp tại trường THPT Sơn Thịnh đã tạo điều kiện cho tác giả trong suốt quá trình học tập và hoàn thành luận văn.

Tác giả

Bùi Thị Thủy

Chương 1

Định lý Kummer và Định lý Lucas

Trong chương này chúng ta sẽ giới thiệu Định lý Kummer và Định lý Lucas, các phép chứng minh cùng với các ví dụ minh họa và một số bài tập ứng dụng của hai định lý.

1.1 Định lý Kummer

Năm 1852, nhà toán học Đức Ernst Kummer trong bài báo *"Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen"* đã chỉ ra rằng

Định lý 1.1.1 (Kummer)**.** *Cho p là một số nguyên tố, $m \leq n$ là hai số tự nhiên. Khi đó, số tự nhiên k lớn nhất sao cho p^k là ước của hệ số nhị thức $\binom{n}{m}$ là số các lần nhớ khi cộng m và $n-m$ theo cơ số p.*

Gọi $\lfloor x \rfloor$ là phần nguyên của số thực x.

Cho p là số nguyên tố. Ta ký hiệu $v_p(n)$ cho số mũ của lũy thừa cao nhất của p chia hết n, $\sigma_p(n)$ là tổng các chữ số của n khi viết theo cơ số p.

Bổ đề 1.1.2 (Legendre)**.** *Cho $n \geq 1$ là số tự nhiên và p là số nguyên tố. Khi đó*

$$v_p(n!) = \sum_{i \geq 1} \lfloor \frac{n}{p^i} \rfloor = \frac{n - \sigma_p(n)}{p-1}.$$

Chứng minh. Vì $n!$ là tích tất cả các số tự nhiên từ 1 đến n nên với mỗi bội của p trong các số từ 1 đến n ta được một thừa số p và do vậy có đúng $\lfloor \frac{n}{p} \rfloor$. Tương tự, từ mỗi bội của p^2, ta có thêm $\lfloor \frac{n}{p^2} \rfloor$ thừa số p... Do đó lũy thừa cao nhất của p chia hết $n!$ sẽ bằng $\sum_{i \geq 1} \lfloor \frac{n}{p^i} \rfloor$.

Giả sử $n = n_0 + n_1 p + ... + n_t p^t$ là biểu diễn của n theo cơ số p. Khi đó ta có

$$\begin{aligned} v_p(n!) &= \sum_{i\geq 1}\left(\lfloor \frac{n}{p^i} \rfloor\right) = \sum_{i=1}^{t}(n_t p^{t-i} + \cdots + n_{i+1}p + n_i) \\ &= \sum_{i=1}^{t}\sum_{j=i}^{t} n_j p^{j-i} = \sum_{j=1}^{t}\sum_{i=1}^{j} n_j p^{j-i} \\ &= \sum_{j=1}^{t} n_j \frac{p^j - 1}{p-1} = \sum_{j=0}^{t} n_j \frac{p^j - 1}{p-1} \\ &= \frac{1}{p-1}\sum_{j=0}^{t}(n_j p^j - n_j) = \frac{n - \sigma_p(n)}{p-1}. \end{aligned}$$

□

Chứng minh Định lý Kummer. Giả sử rằng $n = m + r$. Ta viết ba số này theo cơ số p: $n = n_0 + n_1 p + \cdots + n_t p^t$, tương tự cho m và r . Đặt $\varepsilon_j = 1$ nếu khi cộng m và r theo cơ số p có nhớ ở chữ số thứ j, và $\varepsilon_j = 0$ nếu không có nhớ. Dễ thấy rằng $n_0 = m_0 + r_0 - p\varepsilon_0$ và $n_j = m_j + r_j + \varepsilon_{j-1} - p\varepsilon_j$ với mỗi $j \geq 1$.

Khi đó, theo công thức trên ta có

$$\begin{aligned} v_p\left(\binom{n}{m}\right) &= v_p(n!) - v_p(m!) - v_p(r!) \\ &= \frac{n - \sigma_p(n)}{p-1} - \frac{m - \sigma_p(m)}{p-1} - \frac{r - \sigma_p(r)}{p-1} \\ &= \frac{\sigma_p(m) + \sigma_p(r) - \sigma_p(n)}{p-1} = \sum_{j=0}^{t}\frac{m_j + r_j - n_j}{p-1} \\ &= \frac{p\varepsilon_0 + \sum_{j=1}^{t} p\varepsilon_j - \varepsilon_{j-1}}{p-1} = \sum_{j=0}^{t}\varepsilon_j. \end{aligned}$$

chính là số các phép nhớ khi cộng m và $n-m$ theo cơ số p. Chứng minh hoàn tất. □

Ví dụ 1.1.3. Lấy $n = 32$, $m = 18$. Biểu diễn theo cơ số $p = 5$ ta có

$$32 = \overline{112}_5,\ 18 = \overline{33}_5,\ 14 = \overline{24}_5$$

Dễ thấy rằng phép cộng $\overline{33}_5 + \overline{24}_5$ có hai lần nhớ.

Mặt khác $\binom{32}{18} = 471435600 = 5^2.18877424$, do vậy $v_p\left(\binom{32}{18}\right) = 2$, cũng chính bằng số lần nhớ ở trên.

1.1.1 Hệ quả

Dưới đây là một số hệ quả của Định lý Kummer.

Hệ quả 1.1.4. *Với n là một số nguyên dương, khi đó $\binom{n}{k} \equiv 0 \pmod{n}$ nếu và chỉ với mọi ước nguyên tố p là một ước nguyên tố của n mà $v_p(n) = a$, thì phép trừ $n-k$ theo cơ số p cần ít nhất a phép mượn.*

Chứng minh. Chú ý rằng $\binom{n}{k} \equiv 0 \pmod{n}$ khi và chỉ khi $\binom{n}{k} \equiv 0 \pmod{p^a}$, với mọi ước nguyên tố p của n với $v_p(n) = a$. Theo Định lý Kummer, $\binom{n}{k} \equiv 0 \pmod{p^a}$ khi và chỉ khi phép trừ n cho k trong cơ số p cần ít nhất a phép mượn. □

Hệ quả 1.1.5. *Nếu m,n,k là các số nguyên dương thỏa mãn $gcd(n,k) = 1$ thì $\binom{mn}{k} \equiv 0 \pmod{n}$.*

Chứng minh. Giả sử p là một ước nguyên tố bất kỳ của n với $v_p(n) = a$. Ta viết $k = k_0 + k_1 p + ... + k_t p^t$ trong cơ số p. Vì $\gcd(n,k) = 1$ nên $k_0 \neq 0$. Chú ý rằng $mn = mn' p^a$ với số nguyên n' nào đó. Do đó phép trừ mn cho k theo cơ số p phải có ít nhất là a phép nhớ. Theo Định lý Kummer ta có $\binom{mn}{k} \equiv 0 \pmod{p^a}$. Vì p là ước nguyên tố bất kỳ của n nên $\binom{mn}{k} \equiv 0 \pmod{n}$. □

1.2 Định lý Lucas

Năm 1878, Lucas đã đưa ra một phương pháp để tính $\binom{n}{m} \pmod{p}$. Định lý Lucas phát biểu như sau

Định lý 1.2.1. *Cho m,n là hai số tự nhiên, p là một số nguyên tố. Giả sử m,n có biểu diễn theo cơ số p dưới dạng*

$$m = m_0 + m_1 p + \cdots + m_s p^s, \;\; n = n_0 + n_1 p + \cdots + n_s p^s$$

với $0 \leq m_i, n_i \leq p-1$, khi đó

$$\binom{n}{m} \equiv \prod_{i=0}^{s} \binom{n_i}{m_i} \pmod{p}$$

Ta sẽ chứng minh định lý này. Trước tiên ta có định nghĩa sau.

Định nghĩa 1.2.2. Cho đa thức $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$. Ta viết $f(X) \equiv 0 (\bmod p)$ nếu $a_i \equiv 0 (\bmod p)$ với mọi $i = 1, \ldots, n$. Với hai đa thức $f(X)$ và $g(X)$ trong $\mathbb{Z}[X]$, ta viết $f(X) \equiv g(X) (\bmod p)$ nếu $f(X) - g(X) \equiv 0 (\bmod p)$.

Bổ đề 1.2.3. *Với $i \geq 0$, ta có $(1+X)^{p^i} \equiv 1 + X^{p^i} (\bmod p)$.*

Chứng minh. Ta chứng minh bằng quy nạp theo i. Với $i = 0$ thì khẳng định là hiển nhiên. Giả sử khẳng định đã đúng với $i \geq 0$. Ta có

$$\begin{aligned}(1+X)^{p^{i+1}} &\equiv \left(1 + X^{p^i}\right)^p (\bmod p) \\ &\equiv 1 + \sum_{k=1}^{p-1} \binom{p}{k} X^{p^i k} + X^{p^{i+1}} (\bmod p) \\ &\equiv 1 + X^{p^{i+1}} (\bmod p),\end{aligned}$$

vì ta có $p \mid \binom{p}{k}$ với mọi $k = 1, \ldots, p-1$. □

Chứng minh Định lý Lucas. Ta có

$$\begin{aligned}\sum_{m=0}^{n} \binom{n}{m} X^m = (1+X)^n &= \prod_{i=0}^{s} \left((1+X)^{p^i}\right)^{n_i} \\ &\equiv \prod_{i=0}^{s} (1+X^{p^i})^{n_i} = \prod_{i=0}^{s} \left(\sum_{m_i=0}^{n_i} \binom{n_i}{m_i} X^{m_i p^i} \right) (\bmod p) \\ &= \prod_{i=0}^{s} \left(\sum_{m_i=0}^{p-1} \binom{n_i}{m_i} X^{m_i p^i} \right) \\ &= \sum_{m=0}^{n} \left(\prod_{i=0}^{s} \binom{n_i}{m_i} \right) X^m (\bmod p)\end{aligned}$$

Đồng nhất hệ số ở hai vế ta được $\binom{n}{m} \equiv \prod_{i=0}^{s} \binom{n_i}{m_i} (\bmod p)$. □

Ví dụ 1.2.4. Với $n = 57, m = 32, p = 5$, ta có $n = 57 = \overline{212}_5$, $m = 32 = \overline{112}_5$.

Dễ thấy $\binom{57}{32} = 9929472283517787 \equiv 2 (\bmod 5)$, còn $\binom{2}{1}\binom{1}{1}\binom{2}{2} = 2 \equiv 2 (\bmod 5)$, do đó $\binom{57}{32} \equiv \binom{2}{1}\binom{1}{1}\binom{2}{2} (\bmod 5)$.