ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ HẰNG

VỀ TÍNH CHẤT ĐÔI MỘT NGUYÊN TỐ CÙNG NHAU

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2018

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ HẰNG

VỀ TÍNH CHẤT ĐÔI MỘT NGUYÊN TỐ CÙNG NHAU

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số: 8460113

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. TRẦN ĐỖ MINH CHÂU

THÁI NGUYÊN - 2018

Mục lục

Mở đầu

Cho A là tập con của tập tích Đề Các $\{1,\ldots,k\}^2$. Bộ $(a_1,\ldots,a_k)\in\mathbb{Z}^k$ được gọi là *nguyên tố cùng nhau từng đôi một trên* A nếu $\gcd(a_i,a_j)=1$ với mọi $(i,j)\in A$. Trong trường hợp $\gcd(a_i,a_j)=1$ với mọi $1\leq i<j\leq k$, bộ $(a_1,\ldots,a_k)\in\mathbb{Z}^k$ được gọi là *nguyên tố cùng nhau từng đôi một*. Nếu $\gcd(a_i,a_j)\neq 1$ với mọi $1\leq i<j\leq k$ thì ta nói $(a_1,\ldots,a_k)$ *không nguyên tố cùng nhau từng đôi một*. Tính chất nguyên tố cùng nhau từng đôi một có vai trò quan trọng trong lý thuyết số. Nó là giả thiết không thể thiếu trong Định lý phần dư Trung Hoa nổi tiếng được chứng minh cách đây 750 năm (xem [11]). Cho đến nay, Định lý này vẫn được áp dụng rất nhiều trong các lĩnh vực khác nhau của toán học hiện đại như nhân đồng dư; tính toán bắc cầu; lý thuyết mã hóa và mật mã ... (xem [6]). Ngày nay, việc tính toán các bộ nguyên tố cùng nhau từng đôi một là rất cần thiết để xác định được số các bộ không nguyên tố cùng nhau từng đôi một (xem [8], [14]). Chính vì các lý do này, tôi đã chọn đề tài "**Về tính chất đôi một nguyên tố cùng nhau**".

Mục đích thứ nhất của luận văn là trình bày lại một số kết quả về giả thuyết của Erdös cho trường hợp $k=1,2,3,4$, dựa theo các bài báo [3] và [4]. Giả thuyết phát biểu rằng, số lớn nhất các số nguyên dương không vượt quá số nguyên dương n, sao cho từ các số này không thể trích ra $k+1$ số nguyên nguyên tố cùng nhau từng đôi một đúng bằng số các số nguyên dương không vượt quá n và là bội của ít nhất một trong k số nguyên tố đầu tiên.

Mục đích thứ hai của luận văn là trình bày lại kết quả của Randell

Heyman trong bài báo [9] về xây dựng các công thức gần đúng với sai số thích hợp để tính số bộ gồm ba số nguyên dương nhỏ hơn số H cho trước, không nguyên tố cùng nhau từng đôi một và số bộ gồm v số nguyên dương nhỏ hơn số H cho trước, nguyên tố cùng nhau từng đôi một trên một tập A xác định.

Ngoài phần mở đầu và kết luận, luận văn gồm 2 chương. Chương 1 trình bày một số bài toán liên quan đến các số nguyên tố cùng nhau từng đôi một và chứng minh khẳng định cho giả thuyết của Erdös trong các trường hợp $k \leq 4$. Chương 2 trình bày kết quả và chứng minh chi tiết các công thức tính gần đúng các bộ số nguyên dương nhỏ hơn số H và không nguyên tố cùng nhau từng đôi một hoặc nguyên tố cùng nhau từng đôi một trên một tập A dựa trên lý thuyết đồ thị và một số công cụ giải tích.

Luận văn được hoàn thành tại trường Đại học Khoa học, Đại học Thái Nguyên, dưới sự hướng dẫn tận tình của cô giáo TS. Trần Đỗ Minh Châu. Cô đã dành nhiều thời gian hướng dẫn cũng như giải đáp các thắc mắc của tôi trong suốt quá trình làm luận văn. Tôi xin bày tỏ lòng biết ơn sâu sắc tới cô.

Tôi xin chân thành cảm ơn toàn thể các thầy, cô giáo trong Khoa Toán - Tin, trường Đại học Khoa học - Đại học Thái Nguyên đã tận tình hướng dẫn, truyền đạt kiến thức trong suốt thời gian theo học, thực hiện và hoàn thành luận văn. Tôi xin cảm ơn bạn bè, người thân và các đồng nghiệp đã giúp đỡ, động viên tôi để tôi hoàn thành luận văn này.

Thái Nguyên, tháng 5 năm 2018

Người viết luận văn

Nguyễn Thị Hằng

Chương 1

Giả thuyết Erdös về k số nguyên tố cùng nhau từng đôi một

Mục tiêu của chương 1 là trình bày câu trả lời khẳng định cho giả thuyết của P. Erdös về k số nguyên tố cùng nhau từng đôi một khi $k \leq 4$. Hai tiết đầu dành để nhắc lại khái niệm và một số tính chất cơ bản của ước, bội, ước chung lớn nhất, bội chung nhỏ nhất và một số bài toán về các số nguyên tố cùng nhau từng đôi một. Trong hai tiết tiếp theo, chúng tôi trình bày chi tiết chứng minh cho giả thuyết của Erdös khi $k = 1, 2, 3$.

1.1 Chuẩn bị

Trong tiết này, chúng tôi nhắc lại một số khái niệm và tính chất cơ bản về ước, bội, ước chung lớn nhất, bội chung nhỏ nhất của các số nguyên, khái niệm các số nguyên tố cùng nhau từng đôi một để tiện cho việc theo dõi các nội dung phía sau.

Định nghĩa 1.1.1. Giả sử a và b là hai số nguyên, $b \neq 0$. Ta nói b *chia hết* a hay a *chia hết cho* b nếu tồn tại số nguyên q sao cho $a = bq$. Khi ấy ta còn nói b là *ước* của a hay a là *bội* của b và viết $b \mid a$ hay $a \vdots b$. Khi b không chia hết a ta viết $b \nmid a$.

Ví dụ 1.1.2. $-1, 1$ là hai ước của mọi số nguyên a và 0 là bội của mọi số nguyên $b \neq 0$.

Trong trường hợp không xảy ra quan hệ chia hết, ta có định lý về phép chia có dư phát biểu như sau.

Định lý 1.1.3. *Với mọi cặp số nguyên $a, b, b \neq 0$ tồn tại duy nhất cặp số nguyên q, r thỏa mãn các hệ thức*

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

Hệ quả của Định lý 1.1.3 là vành các số nguyên $\mathbb{Z}$ là vành chính. Vì thế trong vành $\mathbb{Z}$ có các khái niệm ước chung lớn nhất, bội chung nhỏ nhất...Chúng ta sẽ lần lượt nhắc lại các kết quả về các khái niệm này ở trong $\mathbb{Z}$, bỏ qua chứng minh.

Định nghĩa 1.1.4. (i) Một số nguyên d được gọi là *ước chung* của các số nguyên $a_1, a_2, \ldots, a_n$ nếu d là ước đồng thời của mỗi số nguyên đó.

(ii) Với mỗi số nguyên a_i $(i = 1, 2, \ldots, n)$ ta kí hiệu $\mathbf{U}(a_i)$ là tập hợp các ước của a_i. Hiển nhiên $\mathbf{U}(a_i) \neq \emptyset$ và có hữu hạn phần tử.

Rõ ràng $\bigcap_{i=1}^{n} \mathbf{U}(a_i) \neq \emptyset$ và bị chặn trên bởi số lớn nhất trong các số $|a_1|, |a_2|, \ldots, |a_n|$, do đó nó có số lớn nhất d. Hiển nhiên d là một chung của $a_1, a_2, \ldots, a_n$ và có thể thấy rằng mọi ước chung của $a_1, a_2, \ldots, a_n$ đều là ước của d.

Định nghĩa 1.1.5. 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* của các số đó.

Ví dụ 1.1.6. Các số $1, -1, 2, -2$ là các ước chung của 4 và -6. Các ước chung lớn nhất của 4 và -6 là 2 và -2.

Nhận xét 1.1.7. (i) Tập hợp các ước chung của nhiều số cho trước trùng với tập hợp các ước của ước chung lớn nhất của các số đó.

(ii) Nếu tất cả các số $a_1, a_2, \ldots, a_n$ đều bằng 0 thì tập hợp các ước chung của chúng là $\mathbb{Z} \setminus \{0\}$. Khi ấy khái niệm ước chung lớn nhất không có nghĩa nữa. Do đó giả thiết các số $a_1, a_2, \ldots, a_n$ đang xét không phải bằng 0 tất cả. Hơn nữa tập hợp các ước chung của các số đang xét sẽ không thay đổi nếu

ta thêm hay bớt một số bằng 0. Vì thế ta có thể giả thiết thêm $a_i \neq 0$ với mọi $i = 1, 2, \ldots, n$.

(iii) Nếu d là một ước chung lớn nhất của $(a_1, a_2, \ldots, a_n)$ thì $-d$ cũng một ước chung lớn nhất của $(a_1, a_2, \ldots, a_n)$. Hơn nữa nếu d và d' cùng là ước chung lớn nhất của $a_1, a_2, \ldots, a_n$ thì $d' = \pm d$. Do đó từ đây về sau, nếu không có nói gì thêm ta sẽ lấy số dương d trong các ước chung lớn nhất của $a_1, a_2, \ldots, a_n$ làm ước chung lớn nhất của $a_1, a_2, \ldots, a_n$ và kí hiệu $d = \gcd(a_1, a_2, \ldots, a_n)$. Như vậy, ta có thể định nghĩa: ước chung lớn nhất của các số nguyên $a_1, a_2, \ldots, a_n$ là các số lớn nhất trong tập hợp các ước chung của chúng.

Với khái niệm ước chung lớn nhất, ta có thể định nghĩa các số nguyên tố cùng nhau và nguyên tố cùng nhau từng đôi một như sau.

Định nghĩa 1.1.8. (i) Các số nguyên $a_1, \ldots, a_n$ được gọi là *nguyên tố cùng nhau* nếu ước chung lớn nhất của chúng bằng 1.

(ii) Các số nguyên $a_1, \ldots, a_n$ được gọi là *nguyên tố cùng nhau từng đôi một* nếu hai số bất kì trong chúng nguyên tố cùng nhau.

Ví dụ 1.1.9. $6, 10, 15$ là nguyên tố cùng nhau vì $\gcd(6, 10, 15) = 1$. Các số $6, 7, 13$ là nguyên tố cùng nhau từng đôi một vì

$$\gcd(6, 7) = \gcd(7, 13) = \gcd(6, 13) = 1.$$

Định lý sau đây khẳng định ước chung lớn nhất của các số nguyên khác không cho trước luôn tồn tại.

Định lý 1.1.10. *Tồn tại ước chung lớn nhất của các số nguyên khác không $a_1, a_2, \ldots, a_n$ cho trước.*

Hệ quả 1.1.11. *Các khẳng định sau là đúng.*

(i) Nếu $d = \gcd(a_1, a_2, \ldots, a_n)$ thì tồn tại các số nguyên $u_1, u_2, \ldots, u_n$ sao cho

$$d = a_1u_1 + a_2u_2 + \ldots + a_nu_n.$$

(ii) Điều kiện cần và đủ để $a_1, a_2, \ldots, a_n$ nguyên tố cùng nhau là tồn tại các

số nguyên $u_1, u_2, \ldots, u_n$ *sao cho*

$$1 = a_1u_1 + a_2u_2 + \ldots + a_nu_n.$$

Ta luôn tìm được ước chung lớn nhất của các số khác không cho trước nhờ vào thuật toán Ơclit. Tiếp theo, chúng ta nhắc lại các tính chất của ước chung lớn nhất.

Mệnh đề 1.1.12. *Các khẳng định sau là đúng.*

(i) Với $k \in \mathbb{Z}$, $k > 0$ *ta có* $\gcd(ka_1, ka_2, \ldots, ka_n) = k \cdot \gcd(a_1, a_2, \ldots, a_n)$.

(ii) Với $\delta \in \mathbb{Z}$, $\delta > 0$, $\delta \mid a_i$ $(i = 1, 2, \ldots, n)$ *ta có*

$$\gcd\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \ldots, \frac{a_n}{\delta}\right) = \frac{\gcd(a_1, a_2, \ldots, a_n)}{\delta}.$$

(iii) Một ước chung dương d *của các số* $a_1, a_2, \ldots, a_n$ *là ước chung lớn nhất của chúng khi và chỉ khi* $\gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}) = 1$.

(iv) Nếu $\gcd(a, b) = 1$ *và* $b \mid ac$ *thì* $b \mid c$.

(v) Nếu $\gcd(a, b) = 1$ *thì* $\gcd(ac, b) = \gcd(c, b)$ *với mọi* $c \in \mathbb{Z}$.

(vi) Nếu $\gcd(a, b) = \gcd(a, c) = 1$ *thì* $\gcd(a, bc) = 1$.

1.2 Về các số nguyên tố cùng nhau từng đôi một

Mục tiêu của tiết này là nhắc lại khái niệm, tính chất và một số bài toán liên quan đến các số nguyên tố cùng nhau từng đôi một.

Định nghĩa 1.2.1. Một tập con A của tập các số tự nhiên được gọi là *nguyên tố cùng nhau từng đôi một* nếu $\gcd(a, b) = 1$ với mọi $a, b \in A, a \neq b$.

Nhận xét 1.2.2. (i) Nếu các số tự nhiên $a_1, \ldots, a_t$ nguyên tố cùng nhau từng đôi một, thì chúng nguyên tố cùng nhau, tức là $\gcd(a_1, \ldots, a_t) = 1$. Tuy nhiên, điều ngược lại không đúng. Chẳng hạn, các số $3, 5, 6$ là nguyên tố cùng nhau, nhưng không nguyên tố cùng nhau từng đôi một.
(ii) Tồn tại những tập hợp gồm vô hạn số nguyên tố cùng nhau từng đôi một. Chẳng hạn như tập tất cả các số nguyên tố. Trong Bài tập 1.2.5, chúng ta thấy rằng tập hợp $\{6^{2^n} + 1 \mid n \in \mathbb{N}\}$ là tập vô hạn số tự nhiên nguyên tố cùng nhau từng đôi một.

Giả thiết nguyên tố cùng nhau từng đôi một đã được sử dụng trong rất nhiều kết quả quan trọng của số học. Một trong những kết quả như thế là Định lí phần dư Trung Hoa. Định lí phần dư Trung Hoa là một kết quả của lí thuyết số, phát biểu rằng nếu chúng ta biết được các phần dư khi chia một số n cho những số $m_1, \ldots, m_t$ nguyên tố cùng nhau từng đôi một, thì ta xác định được phần dư của phép chia số n cho tích $m_1 \ldots m_t$.

Định lí phần dư Trung Hoa được nhà toán học Trung Quốc Sunzi ghi chép vào thế kỉ thứ 3 sau công nguyên. Người Trung Quốc gọi nó là Bài toán Hàn Tín điểm binh. Tục truyền rằng khi Hàn Tín (229-196 trước công nguyên) điểm quân số, ông cho quân lính xếp hàng 3, hàng 5, hàng 7 rồi báo số dư. Từ đó ông tính chính xác quân số đến từng người. Ngày nay, Định lí phần dư Trung Hoa được sử dụng rộng rãi trong Lí thuyết mật mã, đặc biệt là trong việc tính toán các số nguyên tố lớn.

Định lý 1.2.3. *Cho $m_1, \ldots, m_t$ là các số nguyên dương nguyên tố cùng nhau từng đôi một. Khi đó với t số nguyên $a_1, \ldots, a_t$ bất kì cho trước, hệ phương trình đồng dư*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots\cdots\cdots \\ x &\equiv a_t \pmod{m_t} \end{aligned}$$

có duy nhất một nghiệm modulo M, trong đó $M = m_1 \ldots m_t$.

Chứng minh. Trước hết ta chứng minh sự tồn tại nghiệm. Với mỗi $i = 1, \ldots, t$, đặt

$$n_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_t.$$

Do $m_1, \ldots, m_t$ là các số nguyên dương nguyên tố cùng nhau từng đôi một nên $\gcd(n_i, m_i) = 1$, với mọi $i = 1, \ldots, t$. Suy ra tồn tại các số nguyên k_i sao cho $n_i k_i \equiv 1 \pmod{m_i}$. Đặt $b_i = n_i k_i$. Khi đó $b_i \equiv 1 \pmod{m_i}$ và $b_i \equiv 0 \pmod{m_j}$ với mọi $j \neq i$. Suy ra $x = b_1 a_1 + \ldots + b_t a_t$ là nghiệm của hệ phương trình đồng dư đã cho.