ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ YẾN

SỐ NGUYÊN TỐ VÀ SỰ PHÂN BỐ SỐ NGUYÊN TỐ

LUẬN VĂN THẠC SỸ TOÁN HỌC

THÁI NGUYÊN - NĂM 2010

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

NGUYỄN THỊ YẾN

SỐ NGUYÊN TỐ VÀ SỰ PHÂN BỐ SỐ NGUYÊN TỐ

Chuyên nghành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số: 60.46.40

LUẬN VĂN THẠC SỸ TOÁN HỌC

Người hướng dẫn khoa học:
PGS. TS. NÔNG QUỐC CHINH

THÁI NGUYÊN - NĂM 2010

Mục lục

Mở đầu

Vành số nguyên Z là một vành chính mà $+1$ và -1 là các phần tử khả nghịch duy nhất. Ta đã biết mọi số nguyên khác 0 và khác ± 1 đều phân tích được một cách duy nhất thành một tích các phần tử bất khả quy trong Z. Một số nguyên dương bất khả quy được gọi là một số nguyên tố. Vì vậy mọi số tự nhiên lớn hơn 1 đều phân tích được một cách duy nhất thành tích các thừa số nguyên tố. Vấn đề số nguyên tố là một trong những vấn đề trọng tâm của lý thuyết số. Một câu hỏi đương nhiên được đặt ra là "có bao nhiêu số nguyên tố trong tập hợp số tự nhiên?". Nếu chỉ có một số hữu hạn các số nguyên tố thì vấn đề số nguyên tố sẽ trở nên rất đơn giản, và các vấn đề khác trong số học cũng trở thành đơn giản. Song, ngay từ thời Euclid người ta đã biết rằng tập các số nguyên tố là vô hạn. Từ đó một loạt các câu hỏi được đặt ra. Bài toán về mật độ các số nguyên tố trong dãy số tự nhiên, bài toán tìm một biểu thức lấy giá trị là các số nguyên tố với mọi giá trị tự nhiên của biến, bài toán tìm số nguyên tố thứ n,.... Một vấn đề lớn của lý thuyết số nguyên tố là nghiên cứu hàm $\pi(x)$, biểu thị số các số nguyên tố không vượt quá x, với x là một số thực dương.

Người ta không hi vọng xác định được dễ dàng $\pi(x)$ theo x. Đầu tiên A. M. Legendre đã chứng minh được rằng $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x} = 0$, nghĩa là hầu khắp các số tự nhiên là hợp số. Tiếp theo, người ta tìm một hàm số sơ cấp $f(x)$ tương đương với $\pi(x)$. P. L. Chebyshev đã chứng minh được rằng nếu giới hạn $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{x/lnx}$ tồn tại thì giới hạn đó chỉ có thể bằng 1, tuy nhiên ông không chứng minh được sự tồn tại giới hạn trên. Sau đó ông

đã định nghĩa hai hàm $\vartheta(x)$, $\psi(x)$ và chứng minh định lý "$\pi(x) \sim \frac{x}{lnx}$ nếu và chỉ nếu $\psi(x) \sim x$"Năm 1896, định lý số nguyên tố đã được chứng minh bởi Hadamard và Dela Vallee Poussin bằng cách sử dụng phương pháp giải tích phức. Năm 1949, Selberg đã chứng minh được định lý số nguyên tố bằng phương pháp sơ cấp, không sử dụng giải tích phức. Với mục đích nghiên cứu sự phân bố các số nguyên tố trong tập các số tự nhiên chúng tôi đã chọn đề tài này.

Nội dung của luận văn gồm 2 chương:

Chương 1: *Số nguyên tố.* Trình bày định nghĩa số nguyên tố, những tính chất cơ bản của số nguyên tố và một số định lý quan trọng của số học.

Chương 2: *Sự phân bố các số nguyên tố.* Nêu khái niệm hàm $\pi(x)$, trình bày ước giá đơn giản nhất của hàm $\pi(x)$ và chứng minh định lý số nguyên tố.

Trong quá trình thực hiện luận văn của mình em đã nhận được sự hướng dẫn, giúp đỡ tận tình của PGS. TS. Nông Quốc Chinh, nhận được những ý kiến quý báu của các thầy cô khoa Toán - tin cùng tập thể các bạn học viên lớp cao học K2 trường Đại học Khoa Học. Em xin bày tỏ lòng cảm ơn sâu sắc tới thầy giáo Nông Quốc Chinh, em xin chân thành cảm ơn các thầy cô và các bạn. Em xin chân thành cảm ơn trường THPT Lê Hồng Phong và gia đình đã giúp đỡ, động viên em hoàn thành khoá học. Đến nay luận văn đã được hoàn thành. Tuy nhiên với khoảng thời gian không nhiều, và năng lực của bản thân có hạn nên luận văn không tránh khỏi những thiếu sót. Em rất mong nhận được những ý kiến đóng góp của các thầy cô cùng toàn thể bạn đọc.

Thái Nguyên, ngày 20 tháng 08 năm 2010.

Nguyễn Thị Yến.

Chương 1

Số nguyên tố

1.1 Định nghĩa và các tính chất

Định nghĩa 1.1. *Số nguyên p được gọi là số nguyên tố nếu $p > 1$ và p chỉ có ước là 1 và chính nó. Số nguyên $p > 1$ không là số nguyên tố thì là hợp số.*

Tập các số nguyên tố thường được kí hiệu là P.

Tính chất 1.1. *Ước tự nhiên khác 1 nhỏ nhất của một số tự nhiên là một số nguyên tố.*

Chứng minh.

Cho số $a \in N$, cho d là ước nhỏ nhất của a, $d \neq 1$. Nếu d không nguyên tố thì $d = d_1.d_2$, trong đó $1 < d_1, d_2 < d$. Suy ra d_1 là ước thực sự của d. Vì vậy d_1 là ước của a, $d_1 < d$. Điều này mâu thuẫn với sự nhỏ nhất của d. □

Tính chất 1.2. *Cho p nguyên tố, $a \in N$, $a \neq 0$. Khi đó:*

$$(a, p) = p \Leftrightarrow p|a.$$

$$(a, p) = 1 \Leftrightarrow p \nmid a.$$

Tính chất 1.3. *Nếu tích của nhiều số chia hết cho số nguyên tố p thì có ít nhất một thừa số chia hết cho p.*

Tính chất 1.4. *2 là số nguyên tố nhỏ nhất và là số nguyên tố chẵn duy nhất.*

Tính chất 1.5. *Nếu n là hợp số thì n có ít nhất một ước nguyên tố không vượt quá $\sqrt{n}$.*

Chứng minh.

Giả sử n là hợp số, $n = a.b$, trong đó $a, b \in Z$, $1 < a \leq b < n$. Ta có hoặc $a \leq \sqrt{n}$ hoặc $b \leq \sqrt{n}$. Giả sử $a \leq \sqrt{n}$, vì a có ước nguyên tố, giả sử đó là p, nên p cũng là ước của n, $p \leq \sqrt{n}$.

Vậy n có ước nguyên tố không vượt quá $\sqrt{n}$. □

Hệ quả 1.1. *Nếu số tự nhiên $a > 1$ không có ước nguyên tố nào trong nửa khoảng $(1,\sqrt{a}]$ thì a là số nguyên tố.*

1.2 Một số định lý quan trọng của số học

Định lí 1.1. *Mọi số nguyên dương $a > 1$ đều phân tích được thành tích các thừa số nguyên tố, sự phân tích đó là duy nhất nếu không kể đến thứ tự các thừa số.*

Chứng minh.

** Tính phân tích được:* Giả sử a là số nguyên bất kì thoả mãn $a > 1$, thế thì a phải có một ước nguyên tố, chẳng hạn là p_1. Vậy ta có $a = p_1.a_1$, trong đó $1 \leq a_1 < a$.

Nếu $a_1 = 1$ thì ta có $a = p_1$ và đó là sự phân tích a thành thừa số nguyên tố.

Nếu $a_1 > 1$ thì a_1 phải có một ước nguyên tố p_2, và ta có $a_1 = p_2.a_2$, do đó $a = p_1.p_2.a_2$, với $1 \leq a_2 < a_1$. Nếu $a_2 = 1$ thì $a = p_1.p_2$ là dạng phân tích của a thành thừa số nguyên tố, còn nếu $a_2 > 1$ thì ta lập lại lý luận ở trên được số nguyên tố p_3,.... Quá trình này phải kết thúc sau một số hữu hạn lần vì ta có $a > a_1 > a_2 > ....$, nên tồn tại $n \in N$ thoả mãn $a_n = 1$, và ta được $a = p_1.p_2.....p_n$.

Trong sự phân tích trên thì có thể xảy ra trường hợp trong tích có nhiều thừa số nguyên tố lặp lại, gọi $p_1, p_2, ..., p_k$ là các thừa số nguyên tố đôi một khác nhau của a, với các bội tương ứng là $\alpha_1, \alpha_2, ...\alpha_k$,

$(\alpha_i > 0, i = 1, ..., k)$, thì ta được $a = p_1^{\alpha_1}.p_2^{\alpha_2}....p_k^{\alpha_k}$, gọi là dạng phân tích tiêu chuẩn của a.

* *Tính duy nhất:* Ta giả sử a có hai dạng phân tích tiêu chuẩn:

$$a = p_1^{\alpha_1}.p_2^{\alpha_2}....p_k^{\alpha_k} = q_1^{\beta_1}.q_2^{\beta_2}....q_l^{\beta_l}.$$

Khi đó: $p_i | \quad q_1^{\beta_1}.q_2^{\beta_2}....q_l^{\beta_l}, \forall i = 1, ..., k$. Vì các $q_j (j = 1, ..., l)$ là đôi một khác nhau nên mỗi p_i trùng với một q_j nào đó và tương tự mỗi q_j trùng với một p_i nào đó. Vì vậy $k = l$ và nếu trong hai dạng phân tích tiêu chuẩn trên đều sắp xếp các thừa số nguyên tố theo thứ tự tăng dần thì $p_i = q_i, \forall i$.

Nếu $\alpha_i > \beta_i$ thì ta chia cả hai phân tích trên cho $p_i^{\beta_i}$, ta được:

$$p_1^{\alpha_1}.p_2^{\alpha_2}...p_i^{\alpha_i - \beta_i}....p_k^{\alpha_k} = p_1^{\beta_1}.p_2^{\beta_2}....p_{i-1}^{\beta_{i-1}}.p_{i+1}^{\beta_{i+1}.}....p_k^{\beta_k}.$$

Khi đó vế trái của đẳng thức trên chia hết cho p_i nhưng vế phải thì không chia hết cho p_i. Điều này là mâu thuẫn.

Tương tự, nếu $\beta_i > \alpha_i$ ta dễ dàng suy ra mâu thuẫn.

Vì vậy $\alpha_i = \beta_i, \forall i$. □

Định lí 1.2. (Định lý thứ nhất của Euclid)
Nếu p nguyên tố, $p|ab$ thì $p|a$ hoặc $p|b$.

Chứng minh.

Giả sử p là số nguyên tố và $p|ab$. Nếu $p \nmid a$ thì $(a, p) = 1$, do đó $\exists x, y : xa + yp = 1$ hay $xab + ypb = b$. Mà $p|ab$ và $p|pb$ nên suy ra $p|b$. □

Hệ quả 1.2. *Nếu $p|abc....l$ thì $p|a$ hoặc $p|b$ .....hoặc $p|l$.*

Định lí 1.3. (Định lý thứ hai của Euclid)
Số các số nguyên tố là vô hạn.

Chứng minh.

*** Cách 1 (Chứng minh của Euclid):** Giả sử $2, 3, 5, ..., p$ là dãy các số nguyên tố không vượt quá p. Đặt $q = 2.3.5....p+1$, khi đó q không

chia hết cho số nào của dãy $2, 3, 5, ..., p$. Từ đó suy ra q nguyên tố hoặc q phân tích được thành tích các thừa số nguyên tố, trong đó không có thừa số nào là $2, 3, 5, ..., p$ nên phải có một ước nguyên tố nằm trong khoảng(p, q) hay q chia hết cho một số nguyên tố nằm trong khoảng (p, q). Từ đó suy ra luôn tồn tại số nguyên tố lớn hơn p. Định lý được chứng minh.

*** Cách 2:** Xét số $Q_n = n! + 1, n \geq 1$. Khi đó Q_n có ít nhất một ước nguyên tố, kí hiệu là q_n. Nếu $q_n \leq n$ thì $q_n | n!$ và do đó $q_n | (Q_n - n!) = 1$. Mâu thuẫn. Vậy $q_n > n$, tức là với mọi số nguyên dương n thì đều tồn tại số nguyên tố lớn hơn n nên tập các số nguyên tố là vô hạn. Định lý được chứng minh.

*** Cách 3 (Chứng minh của Goldbach):**

Số $F_n = 2^{2^n} + 1$ được gọi là số Fermat thứ n. Cho trước hai số Fermat F_n và $F_{n+k}(k > 0)$, giả sử $m | F_n, m | F_{n+k}$.
Đặt $x = 2^{2^n}$, ta có:

$$\begin{aligned}
\frac{F_{n+k} - 2}{F_n} &= \frac{(2^{2^{n+k}} + 1) - 2}{2^{2^n} + 1} \\
&= \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} \\
&= \frac{x^{2^k} - 1}{x + 1} \\
&= x^{2^k - 1} - x^{2^k - 2} + ... - 1
\end{aligned}$$

Vì vậy $F_n | (F_{n+k} - 2)$. Mặt khác $m | F_n$ nên $m | (F_{n+k} - 2)$. Từ đó suy ra $m | 2$. Do F_n là số lẻ nên $m = 1$. Như vậy ta chứng minh được hai số Fermat bất kỳ không có ước chung lớn hơn 1.

Từ đó suy ra rằng mỗi một trong các số $F_1, F_2, ..., F_n$ đều chia hết cho một số nguyên tố lẻ p mà p không là ước của bất kỳ số nào khác trong dãy trên. Vậy có ít nhất n số nguyên tố không vượt quá F_n. Do dãy số Fermat là vô hạn nên có vô hạn số nguyên tố. □

Định lí 1.4. *Tồn tại những dãy số liên tục là các hợp số mà độ dài của nó lớn hơn một số n bất kỳ cho trước.*

Chứng minh.

Cho trước số n bất kỳ. Theo định lý Euclid ở trên ta thấy luôn tồn tại số nguyên tố $p > n$. Xét dãy $2, 3, 5, ..., p$ các số nguyên tố không vượt quá p. Đặt $q = 2.3.5....p$ thì $q+2, q+3, q+4, ..., q+p$ là các hợp số. Rõ ràng đó là p-1 số hợp số liền nhau thoả mãn $p - 1 > n$. □

Định lí 1.5. *Không tồn tại đa thức $f(x) \in Z[x]$ mà tất cả các giá trị của nó tại các điểm $x \in Z$ đều là nguyên tố.*

Chứng minh.

Giả sử $f(x) \in Z[x]$, $degf(x) \geq 1$. Khi đó $\lim\limits_{x \to +\infty} f(x) = \pm\infty$. Suy ra $\exists n_0 \in Z$ sao cho $|f(n_0)| > 1$. Giả sử p là một ước nguyên tố của $f(n_0)$, xét khai triển

$$f(n_0 + pt) = f(n_0) + p.f_1(n_0, p, t).$$

Suy ra $p|f(n_0+pt)$ với t tuỳ ý. Ta chọn được t đủ lớn để $|f(n_0+pt)| > p$. Suy ra $f(n_0 + pt)$ là một hợp số. □

Định lí 1.6. *Cho a là một số nguyên với dạng phân tích tiêu chuẩn $a = p_1^{\alpha_1}.p_2^{\alpha_2}....p_k^{\alpha_k}$. Khi đó số nguyên d là ước của a khi và chỉ khi nó có dạng $d = p_1^{\beta_1}.p_2^{\beta_2}....p_k^{\beta_k}$ với $0 \leq \beta_i \leq \alpha_i, i = 1, ..., k$.*

Chứng minh.

Giả sử d là ước của a, khi đó tồn tại số nguyên q sao cho $a = dq$. Đẳng thức này chứng tỏ rằng nếu $d > 1$ thì mọi ước nguyên tố của d là ước nguyên tố của a và số mũ của ước nguyên tố ấy trong dạng phân tích tiêu chuẩn của d không lớn hơn số mũ của nó trong dạng phân tích tiêu chuẩn của a. Bởi vậy:

$$d = p_1^{\beta_1}.p_2^{\beta_2}....p_k^{\beta_k}, 0 \leq \beta_i \leq \alpha_i, i = 1, ..., k.$$

Nếu $d = 1$ thì ta viết $d = p_1^{\beta_1}.p_2^{\beta_2}....p_k^{\beta_k}, \beta_i = 0, \forall i$.

Ngược lại, giả sử a và d là hai số nguyên thoả mãn điều kiện của định lý, khi đó $\alpha_i - \beta_i \geq 0$, $i = 1, ..., k$ nên $q = p_1^{\alpha_1-\beta_1}.p_2^{\alpha_2-\beta_2}....p_k^{\alpha_k-\beta_k}$ là một số nguyên và $a = dq$, nghĩa là d là ước của a. □