ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

LƯƠNG THỊ BĂNG

MỘT SỐ VẤN ĐỀ VỀ LÝ THUYẾT SỐ NGUYÊN TỐ

CHUYÊN NGÀNH: PHƯƠNG PHÁP TOÁN SƠ CẤP
MÃ SỐ: 60.46.40

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học: GS.TSKH. HÀ HUY KHOÁI

THÁI NGUYÊN - 2010

Công trình được hoàn thành tại
TRƯỜNG ĐẠI HỌC KHOA HỌC - ĐẠI HỌC THÁI NGUYÊN

Người hướng dẫn khoa học:GS.TSKH. HÀ HUY KHOÁI

Phản biện 1:.....

.....

Phản biện 2:.....

.....

Luận văn sẽ được bảo vệ trước hội đồng chấm luận văn họp tại:
TRƯỜNG ĐẠI HỌC KHOA HỌC - ĐẠI HỌC THÁI NGUYÊN
Ngày .... tháng .... năm 2010

Có thể tìm hiểu tại
THƯ VIỆN ĐẠI HỌC THÁI NGUYÊN

Lời cảm ơn

Luận văn này được hoàn thành dưới sự hướng dẫn tận tình và nghiêm khắc của GS.TSKH. Hà Huy Khoái. Tôi xin bày tỏ lòng kính trọng và biết ơn sâu sắc tới Thầy và gia đình.

Tôi xin chân thành cảm ơn Ban giám hiệu trường Đại học Khoa học, Phòng đào tạo và nghiên cứu khoa học đã quan tâm giúp đỡ, tạo mọi điều kiện thuận lợi cho tôi được học tập tốt.

Tôi xin chân thành cảm ơn Sở Giáo dục và Đào tạo Tỉnh Bắc Kạn, Trường Trung học phổ thông Ngân Sơn, đặc biệt là tổ Toán Tin đã giúp đỡ tôi về tinh thần và vật chất trong suốt quá trình học tập.

Thái Nguyên, ngày 19 tháng 9 năm 2010

Tác giả

Mở đầu

Trong số học số nguyên tố đóng vai trò rất quan trọng. Từ xưa các nhà toán học đã mất rất nhiều thời gian để nghiên cứu số nguyên tố nhưng cho đến nay, còn nhiều điều bí ẩn về số nguyên tố vẫn chưa được biết. Ngày nay nhờ vào sự tiến bộ của KHKT, nhờ vào máy tính điện tử, người ta đã tìm ra được rất nhiều số nguyên tố lớn (có hàng chục triệu chữ số). Bên cạnh đó những định lí về số nguyên tố luôn lôi cuốn sự chú ý của các nhà toán học, vì thế người ta luôn cố gắng tìm những chứng minh mới. Chứng minh tính vô hạn của các số nguyên tố có thể sử dụng các lí thuyết khác nhau của số học, lí thuyết chuỗi, tô pô, và nhiều công cụ khác.

Luận văn gồm hai chương. Chương 1, chúng tôi trình bày những chứng minh khác nhau của định lí Euclid. Cũng trong chương này, chúng tôi sẽ trình bày một số bài toán tồn tại nổi tiếng trong lí thuyết số nguyên tố. Chương 2, chúng tôi sẽ trình bày lịch sử tìm ra một số số nguyên tố lớn và ứng dụng, mà trọng tâm của chương là nghiên cứu lịch sử tìm ra số nguyên tố Mersenne vì từ trước cho đến nay những số nguyên tố lớn tìm được thường là số nguyên tố Mersenne.

Nhận thức được lí thuyết số nguyên tố là nền tảng của số học, chúng ta đã được học về số nguyên tố từ rất sớm, ngay từ bậc học phổ thông cơ sở, nhưng rất ít tài liệu viết về số nguyên tố. Bản luận văn này sẽ cung cấp thêm một tài liệu về lịch sử nghiên cứu lí thuyết số nguyên tố và quá trình tìm ra các số nguyên tố lớn. Chúng tôi hy vọng luận văn này sẽ đáp ứng được phần nào lòng yêu thích nghiên cứu số nguyên tố của các bạn đồng nghiệp, của các em học sinh.

Sau một thời gian nghiên cứu luận văn được hoàn thành. Tuy nhiên sẽ

không tránh khỏi nhiều sai sót. Kính mong sự góp ý của quý thầy cô, các bạn đồng nghiệp. Chúng tôi xin chân thành cảm ơn!

Thái Nguyên, ngày 19 tháng 9 năm 2010

Tác giả

Mục lục

Chương 1
Định lí Euclid về số nguyên tố

Những định lí tồn tại luôn luôn lôi cuốn sự chú ý của các nhà toán học, vì thế người ta luôn luôn cố gắng tìm những chứng minh mới của các định lý toán học cổ điển. Chẳng hạn cho đến nay người ta đã biết 350 chứng minh khác nhau của định lí Pytago. Những chứng minh như vậy không chỉ thú vị về mặt khoa học mà còn có ý nghĩa về mặt lịch sử. Hơn nữa nhiều chứng minh cho thấy mối liên quan giữa những lĩnh vực và sự kiện khác nhau ở trong toán học. Ở đây chúng tôi sẽ trình bày 19 chứng minh khác nhau của một trong những định lí nổi tiếng nhất của toán học, đó là định lí Euclid:

1.1. Định lí: Tập hợp số nguyên tố là vô hạn

1.2. Những chứng minh khác nhau của định lí Euclid

1.2.1. Chứng minh 1 (Euclid, thế kỉ III trước công nguyên)

Giả sử tập hợp số nguyên tố là hữu hạn. Gọi p là số nguyên tố lớn nhất.

Xét k là tích của tất cả các số nguyên tố cộng thêm 1:

$$k = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p + 1.$$

Số k không có ước nguyên tố bởi vì khi chia cho số nguyên tố tùy ý ta được phần dư bằng 1. Trong khi đó dễ thấy rằng ước số bé nhất $m > 1$ của số tự nhiên k là số nguyên tố, mâu thuẫn này chứng minh định lí.

1.2.2. Chứng minh 2 (Kummer)

Thực chất của chứng minh Eculid là ở chỗ, với giả thiết về tính hữu hạn của tập hợp số nguyên tố, người ta xây dựng số nguyên k nào đó không chia hết cho một số nguyên tố nào.
Nhà toán học Đức Kummer đã thay trong lập luận của Euclid chỉ một dấu trong định nghĩa của k:

$$k = 2 \cdot 3 \cdot 5 \cdots p - 1.$$

Trước khi đi đến các chứng minh khác ta có bổ đề sau:

Bổ đề 1.2.1. *Nếu tồn tại dãy vô hạn các số nguyên, nguyên tố cùng nhau từng cặp thì tập hợp số nguyên tố là vô hạn.*

Chứng minh. Thật vậy, các số nguyên tố cùng nhau từng cặp không có ước nguyên tố chung. Vì thế nếu lấy mỗi một ước nguyên tố của mỗi một số trong dãy ta sẽ nhận được một tập hợp vô hạn mà các phần tử của chúng đều là số nguyên tố.

Bây giờ để chứng minh có vô hạn số nguyên tố ta chỉ cần đi tìm những dãy số nguyên tố cùng nhau từng cặp.

1.2.3. Chứng minh 3 (Silvestre)

Xét dãy a_n xác định bởi quan hệ sau:

$a_1 = 2$

$a_{k+1} = (a_k)^2 - a_k + 1, k \in N.$

Chẳng hạn một số số hạng đầu tiên của dãy là như sau: $2, 3, 7, 43$.
Ta sẽ chứng minh bằng quy nạp rằng với mọi $n \in N$ ta có đẳng thức sau:

$$a_{n+1} = a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1} \cdot a_n + 1.$$

Với n = 1 hiển nhiên.

Bây giờ giả sử quan hệ đúng với n tức là

$$a_{n+1} = a_1 \cdot a_2 \cdots a_{n-1} \cdot a_n + 1.$$

Khi đó:

$a_{n+2} = (a_{n+1})^2 - a_{n+1} + 1,$

$a_1 \cdot a_2 \cdots \cdot a_{n+1} + 1 = a_1 \cdot a_2 \cdots a_n[(a_1 \cdot a_2 \cdots a_{n-1} \cdot a_n) + 1] + 1$

$=[(a_1 \cdot a_2 \cdots \cdot a_n)^2 + a_1 \cdot a_2 \cdot a_n] + 1$

$=[(a_{n+1})^2 - 2a_{n+1} + 1 + a_{n+1} - 1 + 1$

$=(a_{n+1})^2 - a_{n+1} + 1.$

Vậy (1) đã được chứng minh.

Từ (1) suy ra rằng mỗi phần tử với dãy Silvestre nguyên tố cùng nhau với tất cả các phần tử đứng trước đó. Như vậy ta được một dãy vô hạn các số nguyên tố cùng nhau từng cặp.

1.2.4. Chứng minh 4 (Goldbach)

Giả sử $a_n = 2^{2^n} + 1$

Ta sẽ chứng minh rằng hai số tùy ý trong dãy $3, 5, 17, ..., 2^{2^n} + 1, ...$ là nguyên tố cùng nhau từng cặp.

Giả sử ngược lại a_n và a_k trong đó $n > k$ không nguyên tố cùng nhau tức là có ước chung nào đó $d > 1$.

Ta nhận thấy rằng dãy đang xét gồm toàn số lẻ, do đó $d > 2$.

Xét đồng nhất thức sau đây:

$(1 + 2) \cdot (1 + 2^2) \cdot (1 + 2^{2^2})...(1 + 2^{2^{n-1}}) = 2^{2^n} - 1$

Đồng nhất thức trên chứng tỏ rằng số $a_n - 2 = 2^{2^n} - 1$ chia hết cho a_k, và do đó chia hết cho d. Nhưng khi đó $2 = a_n - (a_n - 2)$ cũng chia hết cho d (mâu thuẫn).

1.2.5. Chứng minh 5

Chúng ta sẽ chỉ ra một cách xây dựng tổng quát mà hai chứng minh liền trên đây chỉ đều là trường hợp riêng.

Giả sử a và b là những số nguyên tố cùng nhau. Xét dãy a_n thiết lập như sau:

$a_1 = a,$

$a_{k+1} = a_1 \cdot a_2 \cdot ... \cdot a_k + b.$

Ta nhận thấy rằng các dãy trong hai chứng minh trước đây nhận được khi lấy $a = 2$, $b = 1$, và $a = 1$, $b = 2$ tương ứng.

Ta sẽ chứng minh rằng hai số tùy ý của dãy a_n nguyên tố cùng nhau. Trước tiên ta nhận xét rằng khi $n > k$ số

$a_n - b = a_1 \cdot a_2 \cdot ... \cdot a_{n-1}$ chia hết cho a_k.

Giả sử d là ước chung của a_n và a_k. Do a_n chia hết cho d và $a_n - b$ chia hết cho a_k mà a_k chia hết cho d, suy ra b chia hết cho d. Ta lại dùng quy nạp.

Hiển nhiên a_1, a_2 nguyên tố cùng nhau.

Giả sử a_1, a_2, ..., a_k nguyên tố cùng nhau từng cặp. Giả sử $d > 1$ là một ước số tùy ý của của số a_{k+1}. Ta sẽ chứng minh rằng d không là ước của các số a_1, a_2, ..., a_k. Giả sử ngược lại kí hiệu a_i là số bé nhất sao cho a_i chia hết cho d. Nếu $i > 1$ thì số $a_i = a_1 \cdot a_2 \cdot ... \cdot a_{i-1} + b$ chia hết cho d mà vì b chia hết cho d nên tích $a_1 \cdot a_2 \cdot ... \cdot a_{i-1}$ cũng chia hết cho d. Điều này mâu thuẫn với giả thiết a_i nguyên tố cùng nhau với các số đứng trước nó. Còn với $i = 1$ thì $a_1 = a$ chia hết cho d, mâu thuẫn với giả thiết a và b nguyên tố cùng nhau.

1.2.6. Chứng minh 6

Cấu trúc tổng quát của Silvestre có thể xây dựng theo cách khác. Giả sử

$$a_1 = a \geq 2, a_{k+1} = 1 + a_k(a_k - 1)b_k,$$

trong đó b_k là dãy tùy ý các số tự nhiên. Ta nhận thấy rằng dãy Silvestre sẽ nhận được nếu lấy $a = 2$, $b_k = 1$.

Trước hết, là nhắc lại một trong những bài toán của kỳ thi Ôlympic Liên Xô năm 1978:

"Giả sử $f_(x) = x^3 - x + 1$, và $a > 1$ là một số tự nhiên. Chứng minh rằng các số của dãy vô hạn: a, $f(a)$, $f(f(a))$, ... nguyên tố cùng nhau từng cặp". Dễ thấy rằng nếu trong cách xây dựng của chúng ta lấy $b_k = a_k + 1$, thì xuất hiện dãy đã xét.
Ta sẽ chứng minh rằng dãy a_n lập nên từ các số nguyên tố cùng nhau từng cặp.

Thật vậy nếu $m > k$ thì

$a_m - 1$ chia hết cho $a_{m-1} - 1$, chia hết cho $a_{m-2} - 1$, ... chia hết cho $a_{k+1} - 1$, chia hết cho a_k.
Từ đó $a_m \equiv 1 \pmod{a_k}$, tức là a_m và a_k nguyên tố cùng nhau.
Tiếp theo chứng minh ta cần kết quả sau đây:

Bổ đề 1.2.2. *Giả sử $k > 1$,a, b là các số tự nhiên. Khi đó*

$$(k^a - 1, k^b - 1) = k^{(a,b)} - 1,$$

trong đó (x, y) là ước chung lớn của hai số x và y.

Chứng minh. Trước hết ta xét trường hợp khi a là bội của b. Khi đó với số q nào đó ta có $a = b \cdot q$ và $(a, b) = b$. Đẳng thức cần chứng minh có dạng:

$(k^a - 1, k^b - 1) = k^b - 1$ và tương đương với $k^a - 1$ là bội của $k^b - 1$. Điều này là rõ ràng bởi vì

$k^a - 1 = k^{bq} - 1 = (k^b)^q - 1$ chia hết cho $k^b - 1$.

Bây giờ giả sử a không chia hết cho b, tức là:

$a = bq + r, 0 < r < b$.

Ta có

$k^a - 1 = k^{bq+r} - 1 + k^r(k^{bq} - 1) + k^r - 1.$

Như đã thấy trên đây:

$k^{bq} - 1$ chia hết cho $k^b - 1$ hơn nữa $0 < k^r - 1 < k^b - 1$.

Như vậy phần dư của phép chia $k^a - 1$ cho $k^b - 1$ là $k^r - 1$.

Do đó UCLN của $(k^a - 1, k^b - 1) = (k^b - 1, k^r - 1)$.

Sử dụng thuật chia Euclid ta có.

$a = bq^0 + r_1,$

$b = r_1q_1 + r_2,$

$r_1 = r_2q_2 + r_3,$

. . . . .

$r_{n-2} = r_{n-1}q_{n-1} + r_n,$

$r_{n-1} = r_nq_n.$

Ta nhận được các đẳng thức:

$(k^a-1, k^b-1) = (k^b-1, k_1^r-1) = (k_1^r-1, k_2^r-1) = \cdots = (k_{n-1}^r-1, k_n^r-1) = k_n^r - 1 = k^{(a,b)} - 1.$

Đó chính là điều phải chứng minh.

Hệ quả: Nếu n và m nguyên tố cùng nhau thì $2^m - 1$ và $2^n - 1$ cũng nguyên tố cùng nhau.

Thật vậy$(n, m) = 1$ cho nên $(2^{m-1}, 2^{n-1})$=$2^{(m,n)} - 1$=$2^1 - 1$=1.

1.2.7. Chứng minh 7 (Kholsinskii 1994)

Giả sử rằng $F = \{n_1, n_2, n_3, \cdots, n_k\}$ là tập hợp tất cả các số nguyên tố $n_1 = 2, n_2 = 3, n_3 = 5, \cdots$.

Rõ ràng rằng các số thuộc F nguyên tố cùng nhau từng cặp. Do hệ quả của bổ đề 2, các số $2^{n_i} - 1$ và $2^{n_j} - 1$ cũng nguyên tố cùng nhau. Bây giờ với

mỗi $i = 1, 2, \cdots, k$ ta lấy một ước nguyên tố p_i nào đó của số $2^{m_i} - 1$. Khi đó các số $p_1, p_2, \cdots, p_k$ sẽ khác nhau từng cặp. Như vậy ta được tập hợp.

$$G = \{p_1, p_2, \cdots, p_k\}$$

là các số nguyên tố .
Các phần tử của G đều là các số lẻ, mà vì các tập hợp F và G đều có cùng số phần tử, cho nên G phải chứa phần tử không thuộc F, ta có mâu thuẫn.

Những chứng minh của định lý Euclid có thể nhận được bằng cách xây dựng dãy (a_n) mà số các ước nguyên tố của số hạng thứ n tăng một cách không giới nội.

1.2.8. Chứng minh 8

Ta sẽ chứng minh rằng số $a_n = 2^{2^n} + 2^{2^{n-1}} + 1$ có không dưới n ước nguyên tố khác nhau.
Trong đồng nhất thức

$x^4 + x^2 + 1 = (x^2 + 1 - x)(x^2 + 1 + x)$

ta đặt

$x = 2^{2^{n-1}}$.

Ta nhận được

$$\begin{aligned} a_{n+1} &= 2^{2^{n+1}} + 2^{2^n} + 1 \\ &= \left(2^{2^n} + 1 - 2^{2^{n-1}}\right)\left(2^{2^n} + 1 + 2^{2^{n-1}}\right) \\ &= \left(2^{2^n} + 1 - 2^{2^{n-1}}\right) a_n. \end{aligned}$$

Như vậy a_{n+1} chia hết cho a_n.

Các số $2^{2^n} - 2^{2^{n-1}} + 1$ và $a_n = 2^{2^n} + 2^{2^{n-1}} + 1$ nguyên tố cùng nhau, bởi vì nếu chúng có ước chung q thì ước chung q đó lẻ, đồng thời hiệu của hai số bằng $2^{2^{n-1}+1}$ chia hết cho q (vô lí).
Như vậy khi chuyển từ a_n sang a_{n+1}, số các ước nguyên tố tăng lên. Do đó số hạng thứ n của dãy đang xét có ít nhất là n ước nguyên tố khác nhau.

1.2.9. Chứng minh 9

Các chứng minh sau đây xuất hiện khi xét biểu diễn số $n!$ dưới dạng tích của lũy thừa các số nguyên tố.

$$n! = \prod_{p \le n} p^{fp}.$$

Như ta đã biết bội fp của số nguyên tố p trong khai triển chính tắc của số $n!$ được xác định như sau:

$$fp = \sum_{k \ge 1} \left[\frac{n}{p^k} \right].$$

Như vậy, với fp ta có ước lượng

$$fp \le \sum_{k \ge 1} \frac{n}{p^k} = \frac{n}{p-1}.$$

Từ đó, suy ra rằng

$$\sqrt[n]{n!} \le \prod_{p \backslash n} p^{\frac{1}{p-1}}. \qquad (2)$$

(tích lấy theo mọi ước của n).
Bây giờ ta sẽ chứng minh bất đẳng thức sau:

$$\sqrt[n]{n!} \ge \frac{n}{e}. \qquad (3)$$

Bất đẳng thức này tương đương với bất đẳng thức sau

$$\frac{1}{n}(ln2 + ln3 + \cdots + lnn) \ge lnn - 1.$$

Bất đẳng thức này được chứng minh bằng cách lấy tổng các bất đẳng thức dạng

$$lnk \ge \int_{k-1}^{k} lnx dx, \;\; k = 1, 2, \ldots, n.$$

$$\frac{1}{n}(ln2 + ln3 + \cdots + lnn) \geq \frac{1}{n}\int_1^n lnxdx = \frac{1}{n}(xlnx - x)\Big|_1^n$$
$$= \frac{1}{n}(nlnn - n + 1)$$
$$= lnn - 1 + \frac{1}{n} > lnn - 1.$$

Kết hợp bất đẳng thức (2) và (3), ta nhận được

$$\prod p^{\frac{1}{p-1}} \geq \frac{n}{e}. \qquad (4)$$

Như vậy, vế trái của bất đẳng thức là đại lượng không giới nội, suy ra phải tồn tại vô hạn số nguyên tố.

1.2.10. Chứng minh 10

Giả sử $P(x)$ là đa thức có hệ số nguyên, ta gọi một số k là ước của đa thức $P(x)$ nếu với số tự nhiên n nào đó $P(n)$ chia hết cho k. Ta sẽ chứng minh rằng trong các ước của đa thức $P(x)$ bậc lớn hơn hoặc bằng 1 có vô hạn số nguyên tố.

Giả sử rằng $P(x)$ chỉ có hữu hạn ước nguyên tố $p_1, p_2, p_3, \cdots, p_k$.

Giả sử $P(a) = b \neq 0$. Xét đa thức

$Q(x) = P(a + bp_1p_2 \cdot \cdot p_kx)/b.$

$Q(x) - 1 = \dfrac{P(a + bp_1p_2 \cdots p_kx) - P(a)}{b}$ chia hết cho $bp_1p_2 \cdots p_k$. Điều đó có nghĩa là các số $p_1, p_2, \cdots, p_k$ không phải là ước của $Q(x)$.

Mặt khác đa thức $Q(x)$ khác hằng số sẽ nhận mỗi giá trị một số hữu hạn lần. Do đó trong số các giá trị của nó có những số không bằng 0,1 và -1. Như vậy nó phải có các ước nguyên tố. Mặt khác mọi ước của Q đều là ước của P bởi vì khi

$t = a + bp_1 \cdot p_2 \cdots p_kx$ thì ta có đẳng thức

$P(t) = bQ(x).$

Như vậy đa thức $P(x)$ có ước nguyên tố khác với $p_1, p - 2, \cdots, p_k \Longrightarrow$mâu

thuẫn.

Ta biết rằng, đối với cấp số cộng $a_n = a_1 + (n-1)d$, trong đó $d \neq 0$, $a_1 \in Z$, tập hợp các ước nguyên tố của các số hạng của dãy là một tập hợp vô hạn. Định lí nổi tiếng của Dirichlet khẳng định rằng nếu a_1 và d nguyên tố cùng nhau thì trong số các số hạng của cấp số cộng với số hạng đầu a_1 và công sai d có vô hạn số nguyên tố.

Ở phần tiếp theo chúng ta sẽ xét một số trường hợp riêng của định lí Dirichlet.

1.2.11. Chứng minh 11

Tồn tại vô hạn số nguyên tố có dạng $3n + 2$.

Chứng minh: Giả sử ngược lại $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, ..., p_s là tất cả các số nguyên tố có dạng đã nói.

Ta xét số

$$k = 3p_1 \cdot p_2 \cdot ... \cdot p_s - 1$$

Rõ ràng rằng k không chia hết cho 3 và không chia hết cho các số p_1, p_2, ..., p_s. Nếu mọi ước nguyên tố của k khi chia cho 3 dư 1 thì k cũng có tính chất đó.

Nhưng vì $k \equiv 2 \pmod 3)$ nên k phải có ước nguyên tố q.

Đặt $q = 3n + 2$. Số q khác với các số p_1, p_2, ..., p_s, mâu thuẫn.

Rõ ràng nếu $3n + 2$ là số nguyên tố thì n lẻ, điều đó có nghĩa là khẳng định vừa chứng minh tương đương với việc nói rằng tồn tại vô hạn số nguyên tố dạng $6n + 5$. Hơn nữa có thể chứng minh sự kiện phức tạp hơn sau đây.

1.2.12. Chứng minh 12

Tồn tại vô hạn số nguyên tố dạng $6n + 1$.

Trước hết ta cần bổ đề sau đây:

Bổ đề 1.2.3. *Ước nguyên tố tùy ý* $p > 3$ *của đa thức* $x^2 + x + 1$ *có dạng* $p = 6n + 1$.

Chứng minh. Thật vậy nếu $p = 3k + 2$ và $x^2 + x + 1$ chia hết cho p thì $x^3 \equiv 1 \pmod{p}$ và x không chia hết cho p. Nâng hai vế lên lũy thừa k ta có:

$x^{p-2} \equiv 1 \pmod{p}$.

Từ đó suy ra

$x^{p-1} \equiv x \pmod{p}$.

Mặt khác theo định lí Fermat nhỏ thì $x^{p-1} \equiv 1 \pmod{p}$

Như vậy: $x \equiv 1 \pmod{p}$, $x^2 + x + 1 \equiv 3 \pmod{p}$ và p chia hết cho 3.

Điều này mâu thuẫn với việc số nguyên tố p chia 3 dư 1 (đpcm).

Bây giờ ta giả thiết rằng $p_1 = 7, p_2 = 13, \cdots p_s$ là tất cả các số nguyên tố dạng $6n + 1$. Giả sử $m = p_1 \cdot p_2 \cdots p_s$ và $k = m^2 + m + 1$. Khi đó số m có dạng

$m = 6r + 1$ và $k = 36r^2 + 18r + 3 \equiv 3 \pmod{9}$).

Số k lẻ và không là lũy thừa của 3 cho nên nó có ước nguyên tố $q > 3$. Theo bổ đề 3, đối với số n nào đó ta có $q = 6n + 1$. Đồng thời số $q \neq p_1, p_2, \cdots, p_s$ vì khi chia k cho số p_i tùy ý thì phần dư là $1 \Longrightarrow$ mâu thuẫn.

Lập luận trên đây có thể mở rộng như sau:

Bổ đề 1.2.4. *Giả sử m và p là các số nguyên tố khác nhau. Nếu p là ước của số $x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1$, trong đó $x \in N$ thì*

$p \equiv 1 \pmod{m}$.

Chứng minh. Giả sử $p = mk + r, r = 1, 2, \cdots, m - 1$. Cần chứng minh rằng $r = 1$.

Từ giả thiết suy ra $x^m \equiv 1 \pmod{p}$, (5)

tức là số x không chia hết cho p. Trước tiên ta chứng tỏ rằng

$x^{r-1} \equiv 1 \pmod{p}$. (6)

Nếu $p < m$ thì $p = r$, và (6) đúng do định lí Fermat.

Nếu $p > m$ thì ta nâng hai vế của (5) lên lũy thừa

$k = \frac{p-r}{m}$. Ta nhận được

$x^{p-r} \equiv 1 \pmod{p}$ (7)

Mặt khác theo định lí Fermat bé $x^{p-1} \equiv 1 \pmod{p}$. (8)

Bây giờ trừ (8) cho (7) ta được:

$x^{p-r}(x^{r-1} - 1) \equiv 0 \pmod{p}$.

Do x không chia hết cho p nên từ đó suy ra (6).

Bây giờ để chứng minh bổ đề bằng phản chứng ta giả thiết rằng $r > 1$. Khi đó m và $r - 1$ là các số nguyên tố cùng nhau bởi vì m là số nguyên tố và $m \neq r - 1$.

Áp dụng bổ đề 2 ta có

$(x^m - 1, x^{r-1} - 1) = x^{(m,r-1)} - 1 = x - 1.$

Từ (5) và (6) suy ra rằng, số p là ước chung của các số $x^m - 1$ và $x^{r-1} - 1$, nghĩa là UCLN của chúng là $x - 1$. Như vậy $x \equiv 1(modp)$. Từ đó $p(x) \equiv m \pmod{p}$ và do giả thiết $p(x) \equiv 0 \pmod{p}$ ta đi đến kết luận rằng m chia hết cho p, mâu thuẫn. Vậy $r = 1$.

1.2.13. Chứng minh 13

Tồn tại vô hạn số nguyên tố dạng $m \cdot n + 1$, trong đó m là số nguyên tố.

Xét đa thức

$P(x) = x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1.$

Giả sử $p_1, p_2, ..., p_s$ là tất cả các số nguyên tố dạng $m \cdot n + 1$. Xác định số k bởi đẳng thức

$$k = p(p_1 \cdot p_2 \cdots p_k).$$

Theo bổ đề 4 mọi ước nguyên tố q của số k có dạng $q = m \cdot n + 1$. Trong khi đó q khác với $p_1, p_2, \cdots, p_s$. Bởi vì khi chia k cho số p_i tùy ý ta có phần dư 1, mâu thuẫn.

1.2.14. Chứng minh 14

Giả sử $2^n > (1 + n)^m$. Ta sẽ chứng minh rằng trong các số $1, 2, 3, \cdots, 2^n$ tồn tại ít nhất $m + 1$ số nguyên tố.

Giả thiết rằng trong các số $1, 2, 3, \cdots, 2^n$ chứa $s \leq m$ số nguyên tố $p_1, p_2, \cdots, p_s$. Khi đó mỗi số không vượt quá 2^n đều biểu diễn được dưới dạng $p_1^{k_1}, p_2^{k_2}, \cdots, p_s^{k_s}$. Trong đó rõ ràng mỗi số mũ k_i đều không vượt quá n. Tuy nhiên các số dạng $(1+n)^r$ thì ít hơn là 2^n, điều này mâu thuẫn.

Bởi vì như ta đã biết hàm mũ tăng nhanh hơn hàm lũy thừa cho nên với $\forall m$ khi n đủ lớn ta có $2^n > (1+n)^m$, và như vậy ta nhận được chứng minh về tập hợp vô hạn số nguyên tố.

1.2.15. Chứng minh 15

Trước tiên ta chứng minh rằng trong các số $1, 2, 3, \cdots, n$ không có quá $1/4$ số không có ước là một số chính phương khác 1.

Trong các số $1, 2, 3, \cdots, n$ có không quá $\frac{n}{p^2}$ số chia hết cho p^2. Do đó số các số chia hết cho bình phương của một số nguyên tố không vượt quá

$$\begin{aligned}\sum_{p\leq\sqrt{n}} \frac{n}{p^2} <& \frac{n}{4} + \sum_{k=2} \frac{n}{k(k+1)} \\ &= \frac{n}{4} + n(\sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) = \frac{3n}{4}.\end{aligned}$$

Bây giờ giả sử p_k là số nguyên tố thứ k, $k-1$ số nguyên tố đầu tiên sinh ra 2^{k-1} số không có ước chính phương. Do đó trong các số từ 1 đến $4 \cdot 2^{k-1} = 2^{k+1}$ có ít nhất là k số nguyên tố (nếu ngược lại thì số các số mà không có ước chính phương phải nhỏ hơn $1/4$), tức là $p_k < 2^{k+1}$.

Điều đó không chỉ chứng minh định lí Euclid mà còn cho một ước lượng trên của số nguyên tố thứ k.

1.2.16. Chứng minh 16 (Euler)

Với mỗi số nguyên tố p thì chuỗi

$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ...$ (9) là chuỗi hội tụ (vì nó là chuỗi hình học).

Nếu các số nguyên tố là hữu hạn $p_1, p_2, p_3, ..., p_s$ thì khi nhân các chuỗi hội

tụ (9) tương ứng với chúng ta lại nhận được một chuỗi hội tụ. Trong khi đó, số hạng tổng quát của chuỗi có dạng $\frac{1}{p_1^{k_1}p_2^{k_2}.....p_s^{k_s}}$ trong đó k_i là các số nguyên tố không âm. Do định lí cơ bản của số học và giả thiết trên, chuỗi đang xét chính là chuỗi có các số dạng $\frac{1}{n}$, mà chuỗi này phân kỳ, có mâu thuẫn.
Như vậy tính hội tụ của chuỗi hình học chứng minh được tính vô hạn của tập hợp số nguyên tố.

1.2.17. Chứng minh 17

Đối với số nguyên tố p ta có

$$1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + ... = \frac{p^2}{p^2 - 1}. \qquad (10)$$

Nếu tập hợp các số nguyên tố là tập hợp hữu hạn $p_1, p_2, ..., p_s$ thì khi nhân các chuỗi (10) tương ứng ta lại nhận được một chuỗi hội tụ với tổng

$S = \frac{p_1^2}{p_1^2-1}.\frac{p_2^2}{p_2^2-1}...\frac{p_s^2}{p_s^2-1}$.
Rõ ràng rằng S là số hữu tỷ, số hạng tổng quát của chuỗi có dạng $\frac{1}{p_1^{2k_1}.p_2^{2k_2}...p_s^{2k_s}}$, trong đó k_i là các số nguyên không âm. Do định lí cơ bản của số học và giả thiết trên đây chuỗi đang xét là chuỗi gồm tất cả các số hạng dạng $\frac{1}{n^2}$. Nhưng ta đã biết tổng của chuỗi này là $\frac{\pi^2}{6}$ mà $\frac{\pi^2}{6}$ lại là một số vô tỷ nên ta có mâu thuẫn.

Để đi đến những chứng minh tiếp theo ta nhắc lại hàm Euler.
Phi hàm Euler, kí hiệu $\phi(n)$, là hàm có giá trị tại n bằng số các số nhỏ hơn hoặc bằng n và nguyên tố cùng nhau với n. Nếu m nguyên dương, $(a, m) = 1$ thì $a^{\phi(n)} \equiv 1 \pmod{m}$.

1.2.18. Chứng minh 18

Giả thiết rằng tập hợp các số nguyên tố là hữu hạn, gồm các số $p_1, p_2, ...p_s$. Ta xét tích

$P = p_1.p_2....p_s$. Rõ ràng không có số nào ngoài số 1 có thể nguyên tố cùng nhau với P. Do đó $\varphi(p) \leq 1$.

Mặt khác $\varphi(p) = \varphi(p_1.p_2....p_s) = (p_1 - 1)(p_2 - 1)....(p_s - 1) > 1$, mâu thuẫn.

1.2.19. Chứng minh 19 (chứng minh sử dụng tô pô, Furstenberg,1955)

Ta đưa vào tập hợp các số nguyên một tô pô sau đây: Một tập hợp được gọi là *mở* nếu nó biểu diễn được dưới dạng hợp của một số cấp số cộng vô hạn.

Dễ thử lại rằng định nghĩa trên thỏa mãn các tiên đề của không gian tô pô. Xét tập hợp $A_p = \{tp \mid t \in Z\}$. Nó không chỉ là mở (bởi vì nó là cấp số cộng với công sai p) mà còn là tập đóng bởi vì phần bù của nó là hợp của những tập mở

$$A_{p_i} = \{tp + i \mid t \in Z\}, i = 1, 2, 3, ..., p - 1.$$

Nếu tập hợp các số nguyên tố là hữu hạn thì hợp của hữu hạn tập đóng

$B = \cup A_p$ sẽ là tập đóng.

Một số tùy ý khác 1 và -1 đều là bội của số nguyên tố nào đó, nghĩa là phải thuộc tập hợp B. Như vậy $B = Z \setminus \{1, -1\}$. Do đó tập hợp $\{1, -1\}$ là tập mở vì nó là phần bù của tập đóng B. Nhưng điều này mâu thuẫn với định nghĩa của tập mở, đpcm.

Chương 2
Số nguyên tố lớn và ứng dụng

Số nguyên tố từ lâu đã hấp dẫn các nhà toán học. Trong lịch sử, có rất nhiều nhà toán học đã bỏ ra rất nhiều công sức để nghiên cứu và tìm ra những số nguyên tố. Người Hy Lạp cổ đại (khoảng 300 năm TCN) đã chứng minh rằng có vô số số nguyên tố, nhưng khoảng cách giữa chúng không đều nhau. Từ thế kỷ 19 và những năm đầu của thế kỷ 20, cùng với sự phát triển của KHKT, cùng với sự trợ giúp của máy tính điện tử càng ngày người ta càng tìm ra được những số nguyên tố lớn. Tại sao ngày càng có nhiều chương trình, dự án để tìm ra những số nguyên tố lớn như GIMPS, Seventeen, Bust,.....với số tiền thưởng rất cao? Đó là vì số nguyên tố ngày nay có nhiều ứng dụng quan trọng, chẳng hạn trong việc lập mật mã, nhằm tạo ra những mã không tài nào bẻ gãy được. Việc tìm những số nguyên tố lớn dựa rất nhiều vào một số định lí về dạng của ước nguyên tố của những số thuộc những họ nào đó. Cho đến nay, nhiều số nguyên tố lớn nhất được biết đến là số nguyên tố Mersenne. Vì thế, trong chương này, chúng ta sẽ dành một phần thích hợp để giới thiệu về số Mersenne và các ước của nó.

2.1. Tại sao cần phải tìm số nguyên tố lớn?

Cho đến khoảng cuối những năm 70, người ta vẫn xem việc nghiên cứu số nguyên tố là một trong những ngành lí thuyết thuần túy của toán học, vì hầu như không có ứng dụng trong thực tiễn. Quan niệm đó thay đổi hẳn sau khi số nguyên tố được áp dụng để xây dựng hệ mật mã khóa công khai. Để minh họa điều này, ta sẽ tìm hiểu một vài hệ mật mã xây dựng trên cơ sở sử dụng những số nguyên tố lớn.

2.1.1. Hệ mã mũ

Hệ mã mũ (chưa phải là mã khóa công khai) được Pohig và Hellman đưa ra năm 1978. Mục tiêu của hệ này là khắc phục một nhược điểm rất lớn của những hệ mã có trước đó: khi lộ một số văn bản thì sẽ bị lộ khóa. Đối với hệ mã mũ, việc lộ bí mật một số (có thể rất nhiều) văn bản vẫn không làm ảnh hưởng đến tính bảo mật của toàn hệ thống. Sau đây là những nguyên lý chung khi xây dựng hệ mã mũ.

Giả sử p là một số nguyên tố lẻ, giả sử e là một số nguyên dương sao cho $(e, p-1) = 1$. Khi đó cặp e, p sẽ được dùng làm khóa lập mã. Để nhằm mục đích này, số nguyên tố p được chọn phải là số nguyên tố đủ lớn (khoảng 200 chữ số).

Khi mã hóa một khối P trong văn bản, ta lập khối C tương ứng trong văn bản mật theo công thức sau

$$C \equiv P^e \pmod{p}, 0 \leq P < p.$$

Số p được chọn đủ lớn sao cho văn bản mật sẽ chứa những khối chữ số là các số nguyên nhỏ hơn p.

Để giải mã một khối C trong văn bản mật, ta cần biết khóa giải mã d. Đó là số d thỏa mãn $de \equiv 1 \pmod{p} - 1$, có nghĩa d là một nghịch đảo của e modulo $p-1$. Nghịch đảo đó tồn tại do giả thiết $(e, p-1 = 1)$. Để tìm lại được khối C trong văn bản, ta chỉ việc nâng khối C lên lũy thừa d modulo p.

Thật vậy,

$$C^d \equiv (P^e)^d \equiv P^{de} \equiv P^{k(p-1)+1} \equiv P \pmod{p},$$

trong đó $de = k(p-1) + 1$ đối với số nguyên k nào đó, bởi vì

$$de \equiv 1 \pmod{p-1}.$$

Ta sẽ xem xét về độ phức tạp của hệ mã mũ. Với một khối P trong văn bản, khi mã hóa bằng cách tính $P^e \pmod{p}$, số các phép tính bít cần thiết là

$O(log_2 p)^3$. Để giải mã trước hết ta cần phải tìm nghịch đảo d của e modulo $p-1$, điều này thực hiện được với $O(log^3 p)$ phép tính bít, và chỉ cần làm một lần. Tiếp theo đó, để tìm lại được khối P của văn bản từ khối C của văn bản mật, ta chỉ cần tính thặng dư nguyên dương bé nhất của $C^d modulo p$: số các phép tính bít đòi hỏi là $O(log_2 p)^3$. Như vậy, thuật toán lập mã và giải mã được thực hiện tương đối nhanh bằng máy tính.

Tuy nhiên ta sẽ chứng tỏ rằng, việc giải mã một văn bản mật được mã hóa bằng mã mũ nói chung không thể làm được nếu như không biết khóa e. Thật vậy, giả sử ta đã biết số nguyên tố p dùng làm khóa khi lập mã, và hơn nữa, giả sử đã biết một số khối C nào đó trong văn bản mật tương ứng với một số khối P trong văn bản, tức là ta đã biết một số đồng dư thức $C \equiv P^e \pmod{p}$.

Vấn đề còn lại là xác định e từ công thức trên. Số e thỏa mãn điều kiện đó được được gọi là logarit cơ số P của C modulo p. Có nhiều thuật toán khác nhau để tìm logarit cơ số đã cho modulo một số nguyên tố. Thuật toán nhanh nhất được biết hiện nay đòi hỏi khoảng $exp(\sqrt{logploglogp})$ phép tính bít. Để tìm logarit modulo một số nguyên tố có n chữ số thập phân, các thuật toán nhanh nhất cũng đòi hỏi số phép tính bít xấp xỉ số phép tính bít cần dùng khi phân tích một số nguyên n chữ số thành thừa số. Như vậy, nếu làm việc với các máy tính có tốc độ 1 triệu phép tính trong một giây, khi p có khoảng 100 chữ số thập phân, việc tìm logarit modulo p cần khoảng 74 năm, còn trong trường hợp p có khoảng 200 chữ số, thời gian cần thiết là 3,8 tỷ năm!

Cần phải lưu ý rằng, có những trường hợp việc tìm ra logarit modulo p được thực hiện bằng những thuật toán nhanh hơn rất nhiều. Chẳng hạn khi $p-1$ chỉ có những ước nguyên tố nhỏ, tồn tại những thuật toán đặc biệt cho phép tính logarit modulo p với $O(log_2 p)$ phép tính bít. Rõ ràng những số nguyên tố như vậy không thể dùng để lập mã. Trong trường hợp đó, ta có thể lấy q với $p = 2q + 1$, nếu số q cũng là số nguyên tố (khi đó $q-1$ không

thể chỉ có các ước nguyên tố nhỏ).

2.1.2. Các hệ mật mã khóa công khai

a. Nguyên lý chung.

Trong hệ mật mã trình bày trên đây, các khóa lập mã đều phải được giữ bí mật, vì nếu khóa lập mã bị lộ thì người ta có thể tìm ra khóa giải mã trong một thời gian tương đối ngắn. Như vậy nếu trong một hệ thống có nhiều cặp cá thể hoặc nhiều nhóm cá thể cần trao đổi thông tin mật với nhau, số khóa mật mã chung cần giữ bí mật là rất lớn, và như vậy, khó có thể đảm bảo được. Hệ mã mà chúng ta nghiên cứu dưới đây được lập theo một nguyên tắc hoàn toàn mới, trong đó việc biết khóa lập mã không cho phép tìm ra khóa giải mã trong một thời gian chấp nhận được. Vì thế, mỗi cá thể chỉ cần giữ bí mật khóa giải mã riêng của mình, trong khi khóa lập mã được thông báo công khai. Trong trường hợp một trong các cá thể bị lộ khóa giải mã của mình, bí mật của các cá thể còn lại không hề bị ảnh hưởng. Lý do của việc có thể xây dựng những hệ mã như vậy chính là điều ta đã nói đến khi xét hệ mã mũ: độ phức tạp của thuật toán tìm logarit modulo p là quá lớn.

Trước hết, ta nói sơ qua về nguyên tắc của các hệ mã khóa công khai. Giả sử trong hệ thống đang xét có n cá thể cùng trao đổi các thông tin mật. Mỗi các thể chọn cho mình một khóa lập mã k và một công thức mã hóa $E(k)$, được thông báo công khai. Như vậy có n khóa lập mã công khai $E(k_1), E(k_2), ..., E(k_n)$. Khi cá thể thứ i muốn gửi thông báo cho cá thể thứ j, mỗi chữ trong thông báo được chuyển thành số, nhóm thành từng khối với độ dài nào đó. Sau đó, mỗi khối P trong văn bản được mã hóa bằng khóa lập mã $E(k_j)$ của cá thể thứ j (đã thông báo công khai), và gửi đi dưới dạng $C = E(k_j)(P)$. Để giải mã thông báo này, cá thể thứ j chỉ cần dùng khóa giải mã (bí mật riêng cho mình) D_{k_j}

$$D_{k_j}(C) = D_{k_j}, E_{k_j}(P) = P,$$

bởi vì D_{k_j} và E_{k_j} là các khóa giải mã và lập mã của cùng cá thể thứ j.

Các cá thể trong hệ thống, nếu nhận được văn bản mật, cũng không thể nào giải mã, vì việc biết khóa lập mã E_{k_j} không cho phép tìm ra khóa giải mã D_{k_j}.

Để cụ thể hóa nguyên tắc vừa trình bày, ta xét ví dụ trên hệ mã khóa công khai được xây dựng đầu tiên năm 1978 bởi Rivest, Shamir và Adleman (xem[RSA]) (thường được gọi là hệ mã RSA).

b. Hệ mã RSA

Hệ RSA được xây dựng trên cơ sở mã mũ, trong đó khóa lập mã là cặp (e, n) gồm số mũ e và modun n. Số n được dùng ở đây là tích của hai số nguyên tố rất lớn nào đó, $n = pq$, và e được chọn sao cho $(e, \phi(n)) = 1$, trong đó $\phi(n)$ là hàm Euler (trong trường hợp này $\phi(n) = (p-1)(q-1)$). Để mã hóa một thông báo, trước tiên ta chuyển các chữ cái thành các số tương ứng và nhóm thành các khối với độ dài đủ lớn (tùy thuộc khả năng tính toán và không vượt quá số n) với một số chẵn chữ số. Để mã hóa một khối P trong văn bản, ta lập khối C trong văn bản mật bằng công thức:

$$E(P) \equiv C \equiv P^e \pmod{n}, 0 < C < n.$$

Quá trình giải mã đòi hỏi phải biết được một nghịch đảo d của e modulo $\phi(n)$. Nghịch đảo này tồn tại theo điều kiện $(e, \phi(n)) = 1$. Muốn giải mã một khối C trong văn bản mật, ta tính

$$D(C) \equiv C^d \equiv P^{ed} \equiv P^{k\phi(n)+1} \equiv (P^{\phi(n)})^k P \equiv P \pmod{n},$$

trong đó $ed = k\phi(n) + 1$ đối với số nguyên k nào đó, vì $ed \equiv 1 (\pmod{\phi(n)})$, và do định lí Euler ta có: $P^{\phi(n)} \equiv 1 \pmod{p}$, khi $(P, n) = 1$ (chú ý rằng, xác suất để P và n không nguyên tố cùng nhau là hết sức nhỏ, vì điều đó chỉ xảy ra khi P có ước là p hoặc q). Cặp (d, n) được gọi là khóa giải mã.

Bây giờ ta chỉ ra rằng , hệ mã RSA thỏa mãn các nguyên tắc của hệ mã khóa công khai nói ở trên. Trước tiên, ta chú ý rằng, mỗi cá thể phải chọn

hai số nguyên tố lớn p và q, cỡ chừng 100 chữ số thập phân. Điều này có thể thực hiện trong ít giây nhờ một máy tính. Khi các số nguyên tố p và q đã được chọn, số mũ dùng để mã hóa e sẽ được lấy sao cho $(e, \phi(qp)) = 1$. Nói chung nên chọn e là số nguyên tố tùy ý lớn hơn p và q. Số e được chọn nhất thiết phải thỏa mãn $2^e > n = pq$. Nếu điều kiện này không được thỏa mãn, ta có $C = P^e < n$, và như vậy để tìm ra P, ta chỉ việc tính căn bậc e của C. Khi điều kiện $2^e > n$ được thỏa mãn, mọi khối P khác 0 và 1 đều được mã hóa bằng cách nâng lên lũy thừa và lấy đồng dư theo modulo n.

Ta cần phải chứng tỏ rằng, việc biết khóa lập mã (công khai) (e, n) không dẫn đến việc tìm được khóa giải mã (d, n).

Chú ý rằng, để tìm nghịch đảo d của e modulo $\phi(n)$, trước tiên phải tìm được $\phi(n)$. Việc tìm $\phi(n)$ không dễ hơn so với phân tích n, bởi vì, một khi biết $\phi(n)$ và n, ta sẽ phân tích được $n = pq$. Thật vậy, ta có:

$$p + q = n - \phi(n) + 1,$$

$$p - q = \sqrt{(p+q)^2 - 4pq} = \sqrt{(p+q)^2 - 4n}.$$

Từ các công thức đó ta tìm được p và q.

Nếu ta chọn các số p và q khoảng 100 chữ số thập phân, thì n sẽ có khoảng 200 chữ số thập phân. Để phân tích một số nguyên cỡ lớn như thế, với các thuật toán nhanh nhất hiện nay và với những máy tính hiện đại nhất, ta mất hàng tỷ năm!

Có một điều cần lưu ý khi chọn các số p và q để tránh rơi vào trường hợp tích pq bị phân tích nhanh nhờ những thuật toán đặc biệt: p và q cần chọn sao cho $p-1$ và $q-1$ phải có các thừa số nguyên tố lớn, ước chung lớn nhất $(p-1, q-1)$ phải nhỏ, q và p phải có số chữ số trong khai triển thập phân khác nhau không nhiều.

Thực tế triển khai cho đến nay đã chứng tỏ rằng hệ mã RSA là rất an toàn, nhưng có một nhược điểm là tốc độ mã hóa chậm (bằng một phần ngàn các hệ đối xứng có cùng cấp độ bảo mật hiện nay), cho nên nó thường được

dùng để mã hóa các bản tin ngắn, trong giao thức trao đổi chìa khóa của các hệ mã đối xứng.

Trên đây là hệ mật mã công khai xuất hiện đầu tiên. Từ đó đến nay, có nhiều hệ mật mã khóa công khai ra đời. Tuy vậy, nguyên tắc chung của các hệ mã đó là sử dụng những "thuật toán một chiều", tức là những thuật toán cho phép tìm ra một đại lượng nào đó tương đối nhanh, nhưng việc tìm "nghịch đảo" (theo một nghĩa nào đó) của nó đòi hỏi thời gian quá lớn. Độc giả nào quan tâm đến vấn đề này có thể tìm đọc trong những tài liệu chuyên về lý thuyết mật mã.
Vì số nguyên tố lớn có nhiều ứng dụng quan trọng, nên đã thu hút được nhiều sự quan tâm của các nhà toán học. Nhưng tại sao các số nguyên tố lớn tìm được thường là số nguyên tố Mersenne, ở phần tiếp theo chúng ta sẽ biết được câu trả lời.

2.2. Số nguyên tố Mersenne

2.2.1. Số hoàn hảo và số nguyên tố Mersenne

Phần này dành để mô tả một dạng đặc biệt của số nguyên tố, có vai trò quan trọng trong lý thuyết và ứng dụng. Ta bắt đầu bằng một số hàm số học quan trọng.

Định nghĩa 2.2.1. Hàm $\tau(n)$, số các ước, có giá trị tại n bằng số các ước dương của n. Hàm $\sigma(n)$, tổng các ước, có giá trị tại n bằng tổng các ước dương của n. Nói cách khác, ta có:

$$\tau(n) = \sum_{d\backslash n} 1, \sigma(n) = \sum_{d\backslash n} d.$$

Ví dụ. Nếu p là số nguyên tố thì $\tau(p) = 2, \sigma(p) = p + 1$.

Định lý 2.2.1. *$\tau(n)$ và $\sigma(n)$ là các hàm nhân tính.*

Dễ thấy rằng, định lý trên suy ra từ bổ đề sau.

Bổ đề 2.2.1. *Nếu f là hàm nhân tính, thì*

$$F(n) = \sum_{d\backslash n} f(d)$$

cũng là hàm nhân tính.

Thật vậy, giả sử m, n là các số dương nguyên tố cùng nhau. Ta có

$$F(mn) = \sum_{d\backslash mn} f(d).$$

Vì $(m, n) = 1$, mỗi ước d của mn có thể viết duy nhất dưới dạng $d = d_1 d_2$ trong đó d_1, d_2 tương ứng là ước của m, n và d_1, d_2 nguyên tố cùng nhau. Do đó ta có

$$F(mn) = \sum_{d_1\backslash m, d_2\backslash n} f(d_1 d_2).$$

Vì f là hàm nhân tính và $(d_1, d_2) = 1$ nên

$$F(mn) = \sum f(d_1) f(d_2) = \sum_{d_1\backslash m} f(d_1) \sum_{d_2\backslash m} f(d_2) = F(m)F(n).$$

Định lý được chứng minh.

Sử dụng định lý trên, ta có công thức sau đây cho các hàm $\tau(n)$ và $\sigma(n)$.

Định lý 2.2.2. *Giả sử n có phân tích sau đây ra thừa số nguyên tố $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$. Khi đó ta có*

$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{a_{j+1}} - 1}{p_j - 1},$$

$$\tau(n) = (a_1 + 1)(a_2 + 1)...(a_k + 1) = \prod_{j=1}^{k} (a_j + 1).$$

Do các quan niệm thần bí, người Hy Lạp quan tâm đến các số nguyên bằng tổng tất cả các ước dương thật sự của nó. Họ gọi các số đó là các số hoàn hảo.

Định nghĩa 2.2.2. Số nguyên dương n được gọi là số hoàn hảo nếu $\tau(n) = 2n$.

Ví dụ. Các số 6, 28 là các số hoàn hảo: $\tau(6) = 1 + 2 + 3 + 6 + 12, \tau(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$.

Định lý sau đây được biết từ thời Hy Lạp.

Định lý 2.2.3. *Số nguyên dương chẵn n là số hoàn hảo khi và chỉ khi $n = 2^{m-1}(2^m - 1)$, trong đó m là một số nguyên sao cho $m \geq 2$ và $2^m - 1$ là số nguyên tố.*

Chứng minh. Trước tiên, giả sử rằng, m có dạng như trên. Vì σ là hàm nhân tính, ta có $\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1)$. Từ công thức của hàm σ và giả thiết $2^m - 1$ là nguyên tố, dễ thấy rằng $\sigma(2^{m-1}) = 2^m - 1, \sigma(2^m - 1) = 2^m$, và do đó $\sigma(n = 2n)$.

Ngược lại, giả sử n là số hoàn hảo chẵn. Viết $n = 2^s t$, trong đó s, t là các số nguyên dương, t lẻ, ta được:

$$\sigma(n) = \sigma(2^s t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t).$$

Vì n là số hoàn hảo nên $\sigma(n) = 2n = 2^{s+1}t$. Như vậy, $2^{s+1} \mid \sigma(t)$, giả sử $\sigma(t) = 2^{s+1}q$. Ta có đẳng thức

$$(2^{s+1} - 1)2^{s+1}q = 2^{s+1}t,$$

tức là $q \backslash t$ và $q \neq t$. Mặt khác ta có

$$t + q = (2^{s+1} - 1)q + q = 2^{s+1}q = \sigma(t).$$

Ta chứng tỏ rằng, $q = 1$. Thật vậy, nếu ngược lại, t có ít nhất 3 ước khác nhau là $1, t, q$, mâu thuẫn đẳng thức vừa chứng minh. Vậy $\sigma(t) = t + 1$, có nghĩa t là số nguyên tố. Định lý được chứng minh. Như vậy để tìm các số hoàn hảo, ta cần tìm các số nguyên tố có dạng $2^m - 1$.

Định nghĩa 2.2.3. Giả sử m là một số nguyên dương, khi đó $M_m = 2^m - 1$ được gọi là số Mersenne thứ m. Nếu p là số nguyên tố, và M_p cũng nguyên tố, thì M_p được gọi là số nguyên tố Mersenne.

Ví dụ .M_2, M_3, M_5, M_7 là các số nguyên tố Mersenne, trong khi M_11 là hợp số. Có nhiều định lý khác nhau dùng để xác định số nguyên tố Mersenne. Chẳng hạn nhờ định lý sau đây, ta só thể kiểm tra nhanh chóng dựa vào dạng của các ước nguyên tố của số Mersenne.

Định lý 2.2.4. *Nếu p là một số nguyên tố lẻ, thì mọi ước nguyên tố của số Mersenne M_p đều có dạng $2kp + 1$, trong đó k là số nguyên dương.*

Chứng minh. Giả sử q là một ước nguyên tố của M_q. Theo định lý Fermat bé, $q \mid (2^{q-1})$. Theo hệ quả (Nếu a và b là các số nguyên dương, thì ước chug lớn nhất của $2^a - 1$ và $2^b - 1$ là $2^(a, b) - 1$), $(2^p - 1, 2^q - 1) = 2^{(p,q-1)} - 1$. Ước chung này lớn hơn 1, vì nó là bội của q. Do đó, $(p, q - 1) = p$, vì p là một số nguyên tố. Ta có $q = mp + 1$, và vì q lẻ nên $m = 2k$, định lý được chứng minh.
Sau đây là vài ví dụ cho thấy ứng dụng của định lý trên.

Ví dụ 1. Để xét xem $M_{13} = 2^{13} - 1 = 8191$ có phải là số nguyên tố hay không, ta cần xem các phép chia cho những số nguyên tố không vượt quá $\sqrt{8191} \approx 90$. Mặt khác, theo định lý trên, mọi ước nguyên tố đều phải có dạng $26k + 1$. Như vậy chỉ cần thử với hai số 53 và 79: ta thấy M_{13} là số nguyên tố.

Ví dụ 2. Xét $M_{23} = 8388607$. Ta cần xét các phép chia của nó cho các số nguyên tố dạng $46k + 1$. Số đầu tiên 47 là ước của nó: M_{23} là hợp số.

Có nhiều thuật toán đặc biệt để kiểm tra nguyên tố các số Mersenne. Nhờ đó, người ta phát hiện được những số nguyên tố rất lớn. Mỗi lần có một số nguyên tố Mersenne, ta lại được một số hoàn hảo. Số nguyên tố Mersenne tìm được gần đây nhất là số $M_{43.112.609}$, gồm 12.978.189 chữ số.

Giả thuyết sau đây vẫn còn chưa được chứng minh.

GIẢ THUYẾT. Tồn tại vô hạn số nguyên tố Mersenne.

Người ta biết được rằng, trong khoảng từ 1 đến 10^{200} không có số hoàn hảo lẻ. Tuy nhiên câu hỏi sau đây vẫn chưa được trả lời.

Câu hỏi.Tồn tại hay không các số hoàn hảo lẻ?

2.2.2. Lịch sử tìm số nguyên tố Mersenne

Như đã biết, các số nguyên tố Mersenne có quan hệ chặt chẽ với các số hoàn hảo. Trong lịch sử, việc nghiên cứu các số số nguyên tố Mersenne đã từng bị thay đổi do các liên quan này: vào thế kỷ $4TCN$, Euclid phát biểu rằng, nếu M là số nguyên tố Mersenne thì $M \cdot (M+1)/2$ là số hoàn hảo. Vào thế kỷ 18, Leonhard Euler chứng minh rằng tất cả các số hoàn hảo chẵn đều có dạng này. Không một số hoàn hảo lẻ nào được biết và người ta nghi ngờ rằng chúng không tồn tại.

Bốn số nguyên tố Mersenne đàu tiên $M_2 = 3, M_3 = 7, M_5 = 31$ và $M_7 = 127$ đã được biết từ cổ xưa. Số thứ năm $M_{13} = 8191$ được tìm thấy vào trước năm 1461; hai số tiếp theo M_{17} và M_{19} được tìm thấy bởi Cataldi vào năm 1588. Sau hơn một thế kỷ M_{31} được kiểm tra bởi Euler vào năm 1750. Số tiếp theo là M_{127}, do Lucas tìm thấy vào năm 1876 , sau đó M_{61} do Pervushin tìm thấy vào năm 1883. Hai số nữa M_{89} và M_{207} được tìm thấy vào thế kỷ 20, bởi Powers vào năm 1911 và 1914.

Từ thế kỷ 17 các số này được mang tên nhà toán học Pháp Marin Mersenne, người đã chứng minh một loạt các số nguyên tố Mersenne với số mũ lên đến 257. Danh sách của ông đã mắc một số sai lầm, như bao gồm cả M_{67}, M_{257}, và bỏ quên M_{61}, M_{89} và M_{107} .

Phương pháp tốt nhất để kiểm tra tính nguyên tố của các số Mersenne dựa vào sự tính toán một dãy tuần hoàn, được phát biểu đầu tiên bởi Lucas năm 1878 và chứng minh bởi Lehmer vào những năm 1930. Hiện nay nó được gọi là kiểm tra Lucas-Lehmer với số nguyên tố Mersenne. Đặc biệt, ta có thể chứng minh rằng (với $n > 2$) $M_n = 2^n - 1$ là số nguyên tố nếu và chỉ nếu M_n chia hết cho $S_n - 2$ trong đó $S_0 = 4$ với $k > 0$, $S_k = S_{k-1}^2 - 2$.

Việc tìm các số nguyên tố Mersenne thực sự được cách mạng bởi các máy tính điện tử số. Thành công đầu tiên của tư tưởng này thuộc về số nguyên tố

Mersenne M_{52}, nhờ nỗ lực khéo léo vào lúc $10^h.00.P.M$ ngày 30.1.1952 khi sử dụng máy tính tự động Western U.S. National Bureau of Standards (SWAC) tại Institute for Numerical Analysis thuộc Đại học California tại LosAngeles, dưới sự điều khiển trực tiếp của Lehmer, sử dụng chương trình viết và chạy bởi GS. RM. Robinson. Nó là số nguyên tố Mersenne tìm thấy sau 38 năm; số tiếp theo M_{607}đã được tìm thấy bởi máy tính này sau gần hai giờ chạy máy. Ba số tiếp theo M_{1279}, M_{2203}, M_{2281} đã được tìm thấy với cùng chương trình trên sau nhiều tháng nữa. M_{4253} là số nguyên tố Mersenne đầu tiên siêu lớn, trên 1000 chữ số thập phân (titanic), và M_{44497} là số nguyên tố đầu tiên có trên 10.000 chữ số thập phân (gigantic).

Đến tháng 9 năm 2008, chỉ mới biết 46 số nguyên tố Mersenne; số lớn nhất đã biết là số có dạng $2^{43112609} - 1$. Cũng như nhiều số nguyên tố Mersenne trước đó, nó được tìm ra nhờ dự án máy tính phân tán trên Internet, được biết với tên gọi: Tìm kiếm số nguyên tố Mersenne khổng lồ trên Internet(Great Internet Mersenne Prime Search GIMPS).

2.2.3. Danh sách các số nguyên tố Mersenne đã biết

STT	Số nguyên tố	Chữ số	Ai	Khi nào	Bình luận
1	$2^{6972593} - 1$	2098960	G4	1999	Mersenne 38
2	$2^{13466917} - 1$	4053946	G5	2001	Mersenne 39
3	$2^{20996011} - 1$	6320430	G6	2003	Mersenne 40?
4	$2^{24036583} - 1$	7235733	G7	2004	Mersenne 41?
5	$2^{25964951} - 1$	7816230	G8	2005	Mersenne 42?
6	$2^{30402457} - 1$	9152052	G9	2005	Mersenne 43??
7	$2^{32582657} - 1$	9808358	G9	2006	Mersenne 44??
8	$2^{37156667} - 1$	11185272	G12	2008	Mersenne 45??
9	$2^{42643801} - 1$	12837064	G12	2009	Mersenne 46??
10	$2^{43112609} - 1$	12978189	G10	2008	Mersenne 47??

2.3. Một số số nguyên tố lớn được biết đến

2.3.1. Các số nguyên tố sinh đôi

Số nguyên tố sinh đôi là số nguyên tố có dạng p và $p+2$ chúng khác nhau 2 đơn vị.

Ngày 28.9.2002 Daniel Papp phát hiện ra một số nguyên tố sinh đôi có 51090 chữ số ($33218925.2^{169690} \pm 1$,) Danh sách một số số nguyên tố sinh đôi đã biết:

STT	Số nguyên tố	Chữ số	Ai	Khi nào	Bình luận
1	$16869987339975.2^{171960} - 1$	51779	x24	2005	Twin(p)
2	$16869987339975.2^{171960} + 1$	51779	x24	2005	Twin(p+2)
3	$100314512544015.2^{171960} - 1$	51780	x24	2006	Twin(p)
4	$100314512544015.2^{171960} + 1$	51780	x24	2006	Twin(p+2)
5	$194772106074315.2^{1719601} - 1$	51780	x24	2007	Twin(p)
6	$194772106074315.2^{1719601} + 1$	51780	x24	2007	Twin(p+2)
7	$2003663613.2^{195000} - 1$	58711	L202	2007	Twin(p)
8	$2003663613.2^{195000} + 1$	58711	L202	2007	Twin(p+2)
9	$65516468355.2^{333333} - 1$	100355	L923	2009	Twin(p)
10	$65516468355.2^{333333} + 1$	100355	L923	2009	Twin(p+2)

2.3.2. Các số nguyên tố Sophie Germain

Một số nguyên tố Sophie Germain là một nguyên tố lẻ p mà $2p+1$ cũng là một số nguyên tố.

Ngày 18.1.2003, David Underbakko đã phát hiện ra một nguyên tố Sophie Germain có 34547 chữ số $(2540041185.2^{114729} - 1)$. Danh sách các số nguyên tố Sophie Germain đã được tìm thấy

STT	Số nguyên tố	Chữ số	Ai	Khi nào	Bình luận
1	$18912879.2^{98395}-1$	29628	p94	2002	SophieGermain(p)
2	$112886032245.2^{108000}-1$	32523	L99	2006	SophieGermain(p)
3	$1124044292325.2^{107999}-1$	32523	L99	2006	SophieGermain(p)
4	$2540041185.2^{114729}-1$	34547	g294	2003	SophieGermain(p)
5	$7068555.2^{121301}-1$	36523	L100	2005	SophieGermain(p)
6	$33759183.2^{123458}-1$	37173	L527	2009	SophieGermain(p)
7	$137211941292195.2^{171960}-1$	51780	x24	2006	SophieGermain(p)
8	$48047305725.2^{171960}-1$	51910	L99	2007	SophieGermain(p)
9	$607095.2^{176311}-1$	53081	L983	2009	SophieGermain(p)
10	$620366307356565.2^{253824}-1$	76424	x24	2009	SophieGermain(p)

2.3.3. Các số giai thừa nguyên tố, nguyên tố giai thừa

Số có dạng $n! \pm 1$ được gọi là những giai thừa nguyên tố.

Danh sách các số giai thừa nguyên tố đã biết

STT	Số nguyên tố	Chữ số	Ai	Khi nào	Bình luận
1	$974!-1$	2490	CD	1992	Factorial
2	$1477!+1$	4042	D	1984	Factorial
3	$1963!-1$	5614	CD	1992	Factorial
4	$3507!-1$	10912	C	1992	Factorial
5	$3610!-1$	11277	C	1993	Factorial
6	$6380!+1$	21507	gl	1998	Factorial
7	$6917!-1$	23560	gl	1998	Factorial
8	$21480!-1$	83727	p65	2001	Factorial
9	$26951!+1$	107707	p65	2002	Factorial
10	$34790!-1$	142891	p85	2002	Factorial

Số nguyên tố giai thừa là các số nguyên tố có dạng $2.3.5.p+1$.

Danh sách các số nguyên tố giai thừa đã biết:

STT	Số nguyên tố	Chữ số	Ai	Khi nào	Bình luận
1	$13033\sharp - 1$	5610	CD	1992	Primorial
2	$13649\sharp + 1$	5862	D	1987	Primorial
3	$15877\sharp - 1$	6845	CD	1992	Primorial
4	$18523\sharp + 1$	8002	D	1989	Primorial
5	$23801\sharp + 1$	10273	C	1993	Primorial
6	$24029\sharp + 1$	10387	C	1993	Primorial
7	$42209\sharp + 1$	18241	p8	1999	Primorial
8	$15877\sharp + 1$	63142	p21	2000	Primorial
9	$366439\sharp + 1$	158936	p16	2001	Primorial
10	$392113\sharp + 1$	169966	p16	2001	Primorial

2.4. Lịch sử nghiên cứu số nguyên tố

2.4.1. Các chủ đề lịch sử lí thuyết số nguyên tố

Số nguyên tố và các tính chất của nó lần đầu tiên được nghiên cứu rộng rãi bởi các nhà toán học Hy Lạp cổ đại.
Các nhà toán học của trường học của Pythagoras ($500TCN$ đến $300TCN$) đã quan tâm đến các tính chất của số nguyên tố. Họ đã quan tâm đến con số hoàn hảo.

Cho đến thời gian xuất hiện cuốn "Nguyên lý" của Euclid (khoảng $300TCN$), một số kết quả quan trọng về số nguyên tố đã được chứng minh. Trong sách Nguyên lý IX đã chứng minh rằng có vô hạn số nguyên tố. Đây là một trong những bằng chứng được biết từ rất sớm trong đó sử dụng phương pháp phản chứng. Euclid cũng cung cấp một chứng minh định lí cơ bản của số học: tất cả các số nguyên có thể được viết như tích những số nguyên tố. Euclid cũng cho thấy nếu $2^n - 1$ là số nguyên tố thì $2^{n-1}.(2^n - 1)$ là một số hoàn hảo. Euler (năm 1747) đã chỉ ra rằng tất cả các số hoàn hảo đều có dạng trên.

Trong khoảng $200TCN$, Eratosthenes (Hy Lạp) nghĩ ra một thuật toán để tính số nguyên tố, được gọi là sàng Eratosthenes .

Sau đó có một thời gian dài trong lịch sử không có tiến triển gì thêm về số nguyên tố.

Những phát minh quan trọng tiếp theo được thực hiện bởi Fermat vào đầu thế kỷ 17. Ông chứng minh một sự suy đoán của Albert Giard rằng mỗi số nguyên tố có dạng $4n - 1$ có thể được viết theo một cách duy nhất dưới dạng tổng bình phương.
Ông nghĩ ra một phương pháp mới để tìm thừa số của những số lớn, và khai triển số $2027651281 = 44021 \cdot 44061$.
Ông đã chứng minh điều mà ngày nay được biết đến như là định lí Fermat *bé* (để phân biệt với *định lí cuối cùng* của ông).

Định lí Fermat bé là một cơ sở cho nhiều kết quả khác trong lí thuyết số và là cơ sở cho phương pháp kiểm tra cho dù con số chính mà vẫn còn được sử dụng trên các máy tính điện tử ngày nay.

Fermat thường trao đổi với các nhà toán học đương thời khác, đặc biệt là Marin Mersenne. Trong một lá thư gửi Mersenne, ông phỏng đoán rằng những số $2^n + 1$ luôn nguyên tố nếu n là một lũy thừa của 2. Ông đã xác minh điều này với $n = 1, 2, 4, 8$ và 16, và ông biết rằng nếu n không chia hết cho 2, kết quả không đúng. Số dạng nói trên được gọi là số Fermat và đã không được nhắc đến cho đến khi hơn 100 năm sau đó, Euler chỉ ra trường hợp $2^{32} + 1 = 4294967297$ là chia hết cho 641, và như vậy không phải là số nguyên tố:
Các số có dạng $2^n - 1$ cũng thu hút sự chú ý vì dễ thấy rằng nếu n không là số nguyên tố, số này phải là hợp số. Những số như thế được gọi là số Mersenne M_n vì Mersenne nghiên cứu chúng.

Euler là người có ảnh hưởng lớn đến lí thuyết số nói chung và các số nguyên tố nói riêng. Ông mở rộng định lí Fermat bé và đưa ra phi hàm Euler $\Phi(n)$. Như đã đề cập ở trên ông phân tích số Fermat thứ năm $2^{32} + 1$, và ông phát

biểu (nhưng đã không thể chứng minh) điều mà ngày nay gọi là luật thuận nghịch bình phương

Ông là người đầu tiên nhận ra rằng lí thuyết số có thể được nghiên cứu bằng cách sử dụng các công cụ giải tích, và xây dựng nên lí thuyết số giải tích.

Thoạt nhìn, các số nguyên tố dường như được phân phối giữa các số nguyên một cách khá lộn xộn. Ví dụ trong số 100 số đứng liền trước 10000000 có chín số nguyên tố, trong khi 100 số sau chỉ có hai số nguyên tố. Legendre và Gauss đã tính toán đến mật độ của các số nguyên tố. Gauss nói với một người bạn rằng, bất cứ khi nào ông có 15 phút rảnh rỗi ông sẽ dành nó trong tính số nguyên tố. Đến cuối đời, ông ước tính rằng ông đã tính tất cả các số nguyên tố lên đến khoảng 3000000. Cả Legendre và Gauss kết luận rằng, đối với n đủ lớn, mật độ các số nguyên tố nhỏ hơn n là $1/log(n)$. Legendre đã cho một ước tính cho $\sqcap(n)$ số nguyên tố $\leq n$ của $\sqcap(n) = n/(log(n) - 1,08366)$.

Mệnh đề nói rằng mật độ của các số nguyên tố là $1/log(n)$ được gọi là định lí số nguyên tố. Người ta đã cố gắng để chứng minh điều này trong suốt thế kỉ 19, và đạt tiến bộ đáng chú ý bởi Chebyshev và Riemann. Kết quả cuối cùng đã được chứng minh (sử dụng phương pháp mạnh mẽ của giải tích phức) bởi Hadamard và Dela Vallee Poussin vào năm 1896.
Vẫn còn nhiều câu hỏi mở (một số trong số đó có niên đại hàng trăm năm) liên quan đến số nguyên tố.

2.4.2. Một số vấn đề chưa được giải quyết

1. Có vô hạn số nguyên tố sinh đôi?
2. Phỏng đoán của Goldbach (phát biểu trong một bức thư của Goldbach gửi Euler vào năm 1742) rằng mỗi số nguyên lớn hơn 2 có thể được viết như là tổng của hai số nguyên tố?
3. Có vô hạn số nguyên tố dạng $n^2 + 1$?

4. Luôn luôn có một số nguyên tố giữa n^2 và $(n+1)^2$?

5. Có vô hạn số nguyên tố Fermat?

6. Có nhiều vô hạn bộ ba số nguyên tố liên tiếp trong cấp số cộng?

8. $n^2 - n + 41$ là số nguyên tố với $0 \leq n \leq 40$. Có vô hạn số nguyên tố có dạng này? 9. Có vô hạn số nguyên tố có dạng $n\sharp + 1$? (ở đây $n\sharp$ là tích của tất cả các số nguyên tố $\leq n$).

10. Có vô hạn số nguyên tố có dạng $n\sharp - 1$?

11. Có vô hạn số nguyên tố có dạng $n! + 1$?

12. Có vô hạn số nguyên tố có dạng $n! - 1$?

13. Nếu p là một số nguyên tố thì $2^p - 1$ luôn luôn không có ước chính phương khác 1 (squarefree?).

14. Các dãy Fibonacci chứa một số lượng vô hạn các số nguyên tố?.

Kết luận

Luận văn nhằm trình bày một số điều thú vị về số nguyên tố:

1/ 19 chứng minh khác nhau của Định lý Euclid về sự vô hạn của tập hợp các số nguyên tố. Những chứng minh này sử dụng nhiều công cụ khác nhau, kể cả tô pô để xét tập hợp các số nguyên tố.

2/ Một số ứng dụng của số nguyên tố trong việc xây dựng các hệ mật mã hiện đại.

3/ Sơ lược lịch sử nghiên cứu số nguyên tố, đặc biệt lịch sử tìm các số nguyên tố lớn.

Tài liệu tham khảo

[1] Hà Huy Khoái - Phạm Huy Điển - *Số học thuật toán* - Nxb Khoa học , Hà Nội, năm 1996.

[2] Nguyễn Văn Mậu - *Một số vấn đề toán học chọn lọc*, NXB Giáo dục, tháng 10, 2008.

[3] Nguyễn Thành Quang - *Luận án tiến sĩ toán học* - Trường Đại học sư phạm vinh 1998.

[4] Andrew Granville anh Thomas J. Tucker, *It's As Easy As abc*, Vol. 49 Number 10, Notices of the AMS, November 2002.

[5] Alin Bostan and Philippe Dumas, *Bodu09 Wronskians and Linear indenpendence, Algorithms Project*, Inria Rocquencourt, France.

[6] Frits Beukers, *The genneralized Fermat equation*, January 20, 2006.

[7] Henri Cohen, *Number Theory, Vol. 2, Analytic and mondern tool*, Springer, 2007.

[8] Mason, *Equations over function fields*, Oxford Unierssity Press, 1990.