NHỮNG CHỨNG MINH KHÁC NHAU CỦA ĐỊNH LÝ EUCLID VỀ SỰ VÔ HẠN CỦA TẬP HỢP SỐ NGUYÊN TỐ

Hà Huy Khoái (Viện Toán học)

Định lý Euclid về sự vô hạn của tập hợp số nguyên tố là một trong những định lý nổi tiếng nhất của toán học. Thật khó hình dung sự phát triển của toán học nếu không có định lý đó! Vì thế, không có gì đáng ngạc nhiên khi người ta thích tìm kiếm những chứng minh khác nhau cho định lý Euclid. Nhưng trước khi trình bày một số chứng minh khác nhau, ta cũng cần tự hỏi: tại sao trong toán học, người ta thường "chứng minh" lại những định lý đã biết?

I. Những chứng minh khác nhau: tại sao và để làm gì?

Thường thì sau khi có chứng minh cho một định lý quan trọng nào đó, người ta cố gắng tìm những chứng minh đơn giản hơn. Việc làm này có hai mục đích: làm rõ hơn bản chất của định lý và làm dễ dàng hơn cho những người muốn tìm hiểu và sử dụng nó. *Làm rõ hơn*, vì người đầu tiên chứng minh định lý đó có thể đã phải lần mò qua những con đường quanh co để đi đến đích, trong khi thực ra có những con đường bằng phẳng hơn nhiều mà cũng dẫn đến đó, và bản chất vấn đề đơn giản hơn nhiều so với cái mà ta hình dung ban đầu.

Trong nhiều trường hợp, người ta lại cố gắng tìm những chứng minh khác không phải vì đơn giản hơn, mà vì muốn hiểu rõ hơn bản chất vấn đề. Điều này đặc biệt hay xẩy ra với những định lý mà cách chứng minh có vẻ không dễ hình dung từ trước. Một trong những ví dụ nổi tiếng là Định lý Dirichlet về số nguyên tố: *Trong cấp số cộng mà công sai và số hạng đầu tiên nguyên tố cùng nhau, có vô hạn số hạng là số nguyên tố*. Định lý này được Dirichlet chứng minh năm 1837, mà công cụ chủ yếu trong chứng minh là hàm zeta Riemann và lý thuyết hàm biến phức. Rõ ràng với phát biểu như trên, khó có thể hình dung là chứng minh Định lý Dirichlet lại phải dùng đến giải tích phức, và người ta hy vọng có cách chứng minh không cần đến công cụ đó. Sau nỗ lực bất thành của nhiều nhà toán học, phải đến hơn 100 năm sau (1949), Alte Selberg mới đưa ra một chứng minh "sơ cấp" (không dùng hàm biến phức) của định lý này. Năm 1950, Selberg được tặng Giải thưởng Fields.

Ngược với ví dụ nêu trên, có rất nhiều định lý mà ngay sau khi được chứng minh, người ta tìm thấy rất nhiều chứng minh khác đơn giản hơn nhiều. Tại sao sau hàng chục, thậm chí hàng trăm năm không có được một cách chứng minh nào, mà sau khi có chứng minh đầu tiên, người ta tìm ngay được những chứng minh đơn giản hơn? Và người tìm được chứng minh đơn giản có "giỏi" hơn người đã đưa ra chứng minh phức tạp trước đó không?

Câu hỏi trên khá dễ trả lời. Khi bạn đang muốn trèo lên một đỉnh núi nào đó mà chưa thấy đường, việc tìm đường là không dễ. Nhưng khi theo chân ai đó (người đầu tiên tìm ra con đường) để lên đến đỉnh cao và nhìn về chỗ xuất phát, bạn có thể sẽ phát hiện ra rất nhiều con đường khác đơn giản hơn, "tự nhiên" hơn để leo đến đỉnh. Cũng có thể ví mỗi "định lý" (đúng hơn là *giả thuyết*) chưa được chứng minh giống như một bức tường sừng sững chặn lối tiến lên của toán học. Bạn cần đục một lỗ để thông sang phía bên kia. Có thể mất nhiều ngày, nhiều tháng, nhiều năm mới có ai đó đục xuyên được bức tường để bạn đi qua. Nhưng khi đã sang được phía bên kia, bạn có thể phát hiện ra rằng, hóa ra bức tường sừng sững đó không phải là quá chắn chắn, mà phía sau nó có nhiều chỗ rất yếu, thậm chí có chỗ gần thủng! Quay lại phía ban đầu và đục vào chỗ đó, bạn phá được bức tường khá dễ dàng! Cũng như vậy, chứng minh đầu tiên cho ta thấy rõ hơn bản chất vấn đề, và vì thế có thể dễ dàng chứng minh được giả thuyết bằng những cách khác.

Trong trường hợp Định lý Euclid mà ta sẽ nhắc đến trong bài này, không có chứng minh nào đơn

giản hơn chứng minh của Euclid! Vậy ta còn cần tìm những chứng minh khác (thường là phức tạp hơn) để làm gì? Vấn đề ở đây là: leo lên đỉnh núi không phải là mục tiêu duy nhất của chúng ta (vì đến đó có thể chỉ còn việc...quay về!), mà chúng ta còn muốn tìm kiếm những điều thú vị trên con đường đi đến đó, còn muốn ngắm nhìn chung quanh, để hiểu rõ hơn vị trí mà ta đang hướng đến trong khung cảnh chung của cả khu rừng. Những chứng minh khác nhau của định lý Euclid giúp ta hiểu rõ hơn mối liên hệ của định lý này với nhiều vấn đề khác nhau của toán học.

II. Những chứng minh khác nhau của Định lý Euclid.

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

Những chứng minh trình bày trong bài này được sưu tầm từ tạp chí Kvant.

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.

Chứng minh 2 (Kummer, 1810-1893)

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:

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

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

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

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

Chứng minh 3 (Silvestre, 1814-1897)

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: $2, 3, 7, 43$.

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 đúng.

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 ta có:

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

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

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

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

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

Suy ra rằng mỗi phần tử của 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.

Chứng minh 4 (Goldbach, 1690-1764).

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:

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

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.

Chứng minh 5

Ta sẽ chỉ ra một cách xây dựng tổng quát mà hai chứng minh trên đây chỉ 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 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, nên 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 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.

Chứng minh 6.

Có thể tổng quát hóa cấu trúc của Silvestre 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 (dãy Silvestre ứng với $a = 2$, $b_k = 1$).

Ta sẽ chỉ ra 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.

Nhận xét. Năm 1978 trong kỳ thi Olympic toán của Liên Xô có bài toán sau đây: *Giả sử* $f_(x) = x^3 - x + 1$, $a > 1$ *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.*

Tiếp theo, ta cần kết quả sau đây (chứng minh có thể tìm thấy trong nhiều sách giáo khoa về số học):

Bổ đề *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 nhất của hai số* x *và* y.

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.

Chứng minh 7 (Kholsinskii, 1994)

Giả sử $F = \{n_1, n_2, n_3, \cdots, n_k\}$ 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 trên đây, 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 $2^{n_i} - 1$. Khi đó các số $p_1, p_2, \cdots, p_k$ sẽ khác nhau từng cặp. Như vậy ta được tập hợp

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

gồm các số nguyên tố. Các phần tử của G đều là các số lẻ, và do các tập hợp F và G có cùng số phần tử, nên G phải chứa phần tử không thuộc F, 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.

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:

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

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.

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

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

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

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

Như vậy, với f_p ta có ước lượng

$$f_p \leq \sum_{k\geq 1} \frac{n}{p^k} = \frac{n}{p-1}.$$

Từ đó, suy ra rằng

$$\sqrt[n]{n!} \leq \prod_{p|n} p^{\frac{1}{p-1}}, \quad (1)$$

(tích lấy theo mọi ước của n).

Bây giờ ta sẽ chứng minh bất đẳng thức sau:

$$\sqrt[n]{n!} \geq \frac{n}{e}. \quad (2)$$

Bất đẳng thức trên đây tương đương với bất đẳng thức sau

$$\frac{1}{n}(\ln 2 + \ln 3 + \ldots + \ln n) \geq \ln n - 1.$$

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

$$\ln k \geq \int_{k-1}^{k} \ln x dx,$$

trong đó $k = 1, 2, \ldots, n$:

$$\frac{1}{n}(\ln 2+\ln 3+\cdots+\ln n) \geq \frac{1}{n}\int_1^n \ln x dx = \frac{1}{n}(xlnx - x)\Big|_1^n = \frac{1}{n}(n\ln n - n + 1) = \ln n - 1 + \frac{1}{n} > \ln n - 1.$$

Kết hợp bất đẳng thức (1) và (2), ta nhận được

$$\prod p^{\frac{1}{p-1}} \geq \frac{n}{e}.$$

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

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

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

Do đa thức

$$Q(x) - 1 = \frac{P(a + bp_1p_2 \cdots p_k x) - P(a)}{b}$$

chia hết cho $bp_1p_2 \cdot \cdots p_k$ nên 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. Hơn nữa, mọi ước của Q đều là ước của P, bởi vì khi $t = a + bp_1 \cdot p_2 \cdots \cdot p_k x$ thì ta có đẳng thức $P(t) = bQ(x)$.

Như vậy đa thức $P(x)$ có ước nguyên tố khác với $p_1, p_2, \cdots, p_k$, mâu thuẫn.

Nhắc lại, 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 ta sẽ xét một số trường hợp riêng của định lí Dirichlet.

Chứng minh 11.

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

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 phải có tính chất đó. Nhưng $k \equiv 2 \pmod 3$), suy ra k phải có ước nguyên tố $q = 3n + 2$. 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 $6n + 5$.

Chứng minh 12.

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

Trước hết ta cần bổ đề sau đây:

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

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, mâu thuẫn vì p chia 3 dư 1.

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 nên nó có ước nguyên tố $q > 3$. Theo bổ đề, 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, mâu thuẫn.

Lập luận trên đây có thể mở rộng như sau:

Bổ đề *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*

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

Giả sử $p = mk + r, r = 1, 2, \cdots, m-1$. Cần chứng minh rằng $r = 1$. Từ giả thiết suy ra $x \equiv 1 \pmod{p}$, tức là x không chia hết cho p. Trước tiên ta chứng tỏ rằng

$$x^{r-1} \equiv 1 \pmod{p}. \quad (3)$$

Nếu $p < m$ thì $p = r$, và điều nói trên suy ra từ định lí Fermat. Nếu $p > m$ thì ta nâng hai vế lên lũy thừa $k = \frac{p-r}{m}$ và nhận được

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

Mặt khác theo định lí Fermat bé $x^{p-1} \equiv 1 \pmod{p}$, nên ta có

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

Do x không chia hết cho p nên suy ra (3).

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 $m \neq r-1$. Ta có

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

Từ đó suy ra rằng, p là ước chung của các số $x^m - 1$ và $x^{r-1} - 1$, nghĩa là ƯCLN của chúng là $x - 1$. Như vậy $x \equiv 1(\pmod{p})$. Từ đó $p(x) \equiv m \pmod{p}$, và do giả thiết, $p(x) \equiv 0 \pmod{p}$. Như vậy m chia hết cho p, mâu thuẫn.

Chứng minh 13.

Tồn tại vô hạn số nguyên tố dạng $mn + 1$, 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 $mn + 1$. Xác định số k bởi đẳng thức

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

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

Trong hai chứng minh tiếp theo, ta dùng phương pháp tổ hợp.

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 sử trong các số $1, 2, 3, \cdots, 2^n$ có $s \leq m$ 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 $p_1^{k_1}, p_2^{k_2}, \cdots, p_s^{k_s}$. Rõ ràng mỗi số mũ k_i đều không vượt quá n. Tuy nhiên số các số dạng $(1 + n)^r$ ít hơn 2^n, mâu thuẫn.

Do hàm mũ tăng nhanh hơn hàm lũy thừa nên với mọi 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.

Chứng minh 15.

Trước tiên ta chứng minh rằng trong các số $1, 2, 3, \cdots, n$ có không 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

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

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 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.

Chứng minh 16, Euler(1707-1783).

Với mỗi số nguyên tố p, chuỗi

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ...$$

hội tụ. Nếu các số nguyên tố là hữu hạn (gồm các số $p_1, p_2, p_3, ..., p_s$) thì khi nhân các chuỗi hội tụ trên đây, 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, chuỗi đang xét chính là tổng các số dạng $\frac{1}{n}$, mà chuỗi này phân kỳ, mâu thuẫn.

Chứng minh 17.

Với số nguyên tố p ta có

$$1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + ... = \frac{1}{p^2 - 1}.$$

Nếu tập hợp các số nguyên tố là hữu hạn $(p_1, p_2, ..., p_s)$ thì khi nhân các chuỗi 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 S là số hữu tỷ, số hạng tổng quát của chuỗi có dạng

$$\frac{1}{p_1^{2k_1} \cdot p_2^{2k_2}...p_s^{2k_s}},$$

trong đó k_i là các số nguyên không âm. Do định lí cơ bản của số học, 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, mâu thuẫn.

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 $\varphi(p) = 1$, trong đó φ là hàm Euler. Mặt khác $\varphi(p) = \varphi(p_1.p_2....p_s) = (p_1 - 1)(p_2 - 1)....(p_s - 1) > 1$, mâu thuẫn.

Chứng minh sau đây dựa vào khái niệm không gian tôpô. Nhắc lại rằng, một tập X khác rống gọi là được trang bị một cấu trúc của không gian tôpô nếu ta định nghĩa một lớp các tập con của X, được gọi là các *tập mở*, thỏa mãn các điều kiện: tập rỗng và X là tập mở; giao hữu hạn các tập mở là tập mở, hợp tùy ý các tập mở là tập mở. Phần bù của một tập mở gọi là tập đóng. Suy ra hợp của hữu hạn tập đóng là tập đóng.

Chứng minh 19, 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 $A_p = \{t_p \mid t \in Z\}$. Nó không chỉ là mở (bởi vì nó là cấp số cộng với công sai p,) mà còn là tập đóng vì phần bù của nó là hợp của những tập mở:

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

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. Mặt khác, 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.

Như vậy, chúng ta đã trình bày 19 chứng minh khác nhau của định lý Euclid. Con số 19 có vẻ không đẹp lắm, và có lẽ cần phải tìm thêm một chứng minh cho tròn số 20. Nhưng...đã hết giờ rồi, đành dành việc đó cho bạn đọc.