素数が無限に多く存在することの証明

0　はじめに

素数が無限に多く存在することは有名である。

ここでは、この事実のいくつかの証明を紹介したい。これらの証明の多くは、良くはないが与えられた数以下の素数の個数に関する評価を与えている。$\pi(x)$ を x 以下の素数の個数とする。このとき、多くの証明は $\pi(x) > c \log\log x$ とか $\pi(x) > c \log x$ とかいった形の評価を与える。ここで c は正の定数である。

ここに挙げられた証明に関する論文などは MathSciNet で “infinitude of prime∗” で検索することにより見つけることができる。

もちろん、素数が無限に多く存在することの証明は他にもある。

（2018/11/3追記）2012年に arXiv に Romeo Meštrović, Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2012) `https://arxiv.org/abs/1202.3670` というプレプリントが公開され、2017年にさらに追記がなされた。この論文では素数が無限に多く存在することの 183 個の証明を紹介している。

1　ユークリッドの証明

$2 = p_1 < p_2 < \cdots < p_r$ をすべての素数と仮定する。$P = p_1 p_2 \cdots p_r + 1$ とし、 p を P の素因数とする。$p_1, p_2, \ldots, p_r$ はいずれも $P = p_1 p_2 \cdots p_r + 1$ の素因数ではないから、p はこれらの素数とは異なる素数である。これは $p_1, p_2, \ldots, p_r$ をすべての素数と仮定したことに矛盾する。 □

ユークリッドの証明は、素数が無限に多く存在することの証明としては最も有名なものだろう。この証明は非常に単純である。また、この証明を修正することで、素数の分布に関する情報を得ることができる。$R \geq 2$ に対し、$R < p \leq R^R + 1$ となる素数が存在する。

$2 = p_1 < p_2 < \cdots < p_r$ を R 以下のすべての素数とする。$P = p_1p_2\cdots p_r + 1$ とし、 p を P の素因数とする。$p_1, p_2, \ldots, p_r$ はいずれも $P = p_1p_2\cdots p_r + 1$ の素因数ではないから、p はこれらの素数とは異なる素数である。明らかに $p \leq R^r + 1 \leq R^R + 1$ である。$p_1, p_2, \ldots, p_r$ は R 以下の素数すべてであるから、 $p > R$ である。 □

ここで、$R^R + 1$ は $R^{R/2+1} + 1$ で置き換えられることがわかる。1 および 2 以外の偶数は素数ではありえないから、R 以下の素数の個数は $R/2+1$ 個を超えないからである。

もちろん、これは非常に弱い結果である。

ここで注意しなければならないのは、上に出てきた $p_1p_2\cdots p_r + 1$ という形の数自体は、必ずしも素数ではないということである。実際、 $2 \times 3 \times 11 \times 13 + 1 = 59 \times 509$ である。$p_1p_2\cdots p_r + 1$ の形の素数が無限に多く存在するか否かは未だに解決されていない問題である。$p_1p_2\cdots p_r + 1$ の形の合成数が無限に多く存在するか否かも知られていない。

ユークリッドの証明には、いくつもの変形がある。

参考

P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996, p. 3.

L. E. Dickson, *History of the Theory of Numbers, Vol. I: Divisibility and Primality*, Carnegie Institution of Washington, 1919 (reprint: Dover Publication, New York, 2005), p. 413.

2　クンマーの証明

$2 = p_1 < p_2 < \cdots < p_r$ をすべての素数と仮定する。$N = p_1p_2\cdots p_r > 2$ とおく、少なくとも素数は2つ以上はあり、N は素数すべての積なので $N-1 > p_r$ であるから、 $N - 1$ は素因数 p_i を持つ。p_i は $N - (N - 1) = 1$ を割りきらなければならないが、これは不可能である。 □

クンマーの証明は、ユークリッドの証明と本質的に同一のものである。ユークリッドが $p_1p_2\cdots p_r + 1$ の形の数を用いているのに対し、クンマーは $p_1p_2\cdots p_r - 1$ の形の数を用いている。ユークリッドの証明と同様に、クンマーの証明を修正し、任意の $R \geq 2$ に対し、$R < p \leq R^{R/2+1} - 1$ となる素数 p が存在することを証明することができる。

参考　P. Ribenboim, 上掲書, p. 4 および L. E. Dickson, 上掲書, p. 413。

3　スティルチェスの証明

素数が $p_1, p_2, \ldots, p_r$ しかないと仮定する。$N = p_1 p_2 \cdots p_r$ とし、$N = mn(m, n \geq 1)$ を N の分解の一つとする。各 p_i は、m と n のうちのちょうど片方のみを割り切るから、p_i はいずれも $m+n$ を割りきらない。つまり、$m+n$ はどのような素数でも割り切れない。しかし $m+n > 1$ だから、このようなことは不可能である。　□

参考　P. Ribenboim, 上掲書, p. 4 および L. E. Dickson, 上掲書, p. 414。

4　ゴールドバッハの証明

ゴールドバッハの予想（4 以上のすべての偶数は 2 つの素数の和で表される）で有名なゴールドバッハも素数が無限に多く存在することの証明を残している（ゴールドバッハが証明を書き残している例は他には確認されていない）。

まず、フェルマー数 $F_n = 2^{2^n} + 1(n \geq 0)$ は、どの 2 つも互いに素であることを示す。$F_m - 2 = 2^{2^n} - 1 = (2^{2^n-1} + 1)(2^{2^n-1} - 1) = F_0 F_1 \cdots F_{m-1}$ であるから、F_m と $F_n(m > n)$ を共に割り切る素数は $2 = F_m - (F_m - 2)$ を割りきらなければならないが、F_n は常に奇数だから、そのような素数はありえない。

よって q_1 を F_1 を割り切る素数とし、q_2 を F_2 を割り切る素数とし、以下同様にすると、$q_1, q_2, \ldots$ は素数の無限列となる。　□

1730 年にゴールドバッハがオイラーに宛てた手紙の中でフェルマー数を用いた証明を与えたことが記されている。

フェルマー数の最初の 5 つ $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ はいずれも素数である。しかし、$F_5 = 4294967297 = 641$ は合成数であり、その他のフェルマー数も、合成数であるものは多く知られているが、素数であるものは発見されていない。

参考　P. Ribenboim, 上掲書, p.p. 4–5 および L. E. Dickson, 上掲書, p. 413。

5　ショルンの証明

素数が m 個しか存在しないと仮定し、$n = m + 1$ とおく。n 個の整数 $(n!)i + 1 (i = 1, 2, \ldots, n)$ はどの 2 つも互いに素である。というのは、$1 \leq i < j \leq n$ とし $j = i+d$ とおくと $((n!)i+1, (n!)j+1) = ((n!)i+1, (n!)d) = 1$ となるからである。各 $i = 1, 2, \ldots, n$ に対し、p_i を $(n!)i + 1$ を割り切る素数とする。このとき $p_1, p_2, \ldots, p_n$ は相異なる素数である。よって少なくとも n 個の素数が存在することになり、当初の仮定に反する。　□

ショルンの証明は、任意の整数 n に対し、$(n!)n + 1$ 以下の素数は少なくとも n 個存在することを示している。

参考　P. Ribenboim, 上掲書, p.p. 5。

6　オイラーの証明

素数が無限に多く存在することの証明の多くは初等的であるのに対し、オイラーの証明はどちらかといえば解析的な考えを用いている。しかし、この方法は、素数の分布に関する大きな発展に結びついている。

$p_1, p_2, \ldots, p_n$ をすべての素数とする。いずれの素数も 1 より大きいから、等比級数 $\sum_{k=0}^{\infty} 1/p_i^k$ は $1/(1 - 1/p_i)$ に収束する。

したがって $\prod_{i=1}^{n} 1/(1 - 1/p_i) = \prod_{i=1}^{n} \sum_{k=0}^{\infty} 1/p_i^k = \sum_{k_i} 1/(\prod_{i=1}^{n} p_i^{k_i})$ である。$p_1, p_2, \ldots, p_n$ がすべての素数であるから、右辺に現れる積 $\prod_{i=1}^{n} p_i^{k_i}$ は正の整数をいずれも、少なくとも 1 回はとる。よってすべての整数の逆数の和は $\sum_{n=1}^{\infty} 1/n \leq \prod_{i=1}^{n} 1/(1-1/p_i)$ となって、収束しなければならない。しかし、これは $\sum_{n=1}^{\infty} 1/n$ は発散するという有名な事実（これは $\sum_{n=1}^{\infty} 1/n \geq 1 + 1/2 + (1/4 + 1/4) + (1/8 + 1/8 + 1/8 + 1/8) + \cdots$ により確かめられる）に反する。　□

実際、素因数分解の一意性から、 オイラーは有名な式 $\sum_{n=1}^{\infty} 1/n^s = \prod_{i=1}^{n} 1/(1 - 1/p_i^s)$ を導いている。

オイラーの方法の興味深い点は、ζ 関数 $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ と素数のつながりを示唆していることにある。これは解析的整数論の最も重要な基礎の一つである。

さらにオイラーは素数の逆数の和が発散することも示している。

N 以下の整数は、 N 以下の素数の積で表されるから、上と同様にして、$\sum_{n=1}^{N} 1/n \leq \prod_{p \leq N} 1/(1 - 1/p)$ となることがわかる。

よって $\log\prod_{p\le N}1/(1-1/p)=-\sum_{p\le N}\log(1-1/p)$ となるが、$\log(1-1/p)=\sum_{m=1}^{\infty}1/(mp^m)\le\sum_{m=1}^{\infty}1/(p^m)=1/p+1/p(p-1)<1/p+1/(p-1)^2$ より、$\log\sum_{n=1}^{N}1/n\le\sum_{p\le N}1/p+1/(p-1)^2\le\sum_{p\le N}1/p+\sum_n 1/n^2$ となる。

したがって $\sum_{p\le N}1/p\ge\log\sum_{n=1}^{N}1/n-c\ge\log\log N-C$ となる定数 c,C が存在する。

参考　P. Ribenboim, 上掲書, p.p. 6–7 および L. E. Dickson, 上掲書, p. 413。

7　エルデシュの証明

$p_1=2,p_2=3,\ldots,p_j$ を x 以下のすべての素数とする。$n=n_1^2m$ （m は平方因子をもたない）とおく。このとき $m=2^{b_1}3^{b_2}\cdots p_j^{b_j}$（$b_i$ は 0 または 1）とかける。このような整数は多くても 2^j 個しかない。$n_1^2\le n\le x$ だから、各 m に対し、n_1 の可能性は多くても $x^{1/2}$ 通りである。よって $x\le 2^jx^{1/2}$ つまり $j\ge(\log x)/(2\log 2)$ となる。したがって、x 以下の素数は少なくとも $(\log x)/(2\log 2)$ 個存在する。 □

エルデシュの方法を用いて、素数の逆数の和が発散することを示すこともできる。

素数の逆数の和が収束すると仮定すると、$\sum_{p>M}1/p<1/2$ となる M が存在する。このとき、任意の整数 N に対し、$\sum_{p>M}N/p<N/2$ となる。

N 以下の整数を 2 つの集合に分割する。N_1 を N 以下の整数のうち、M より大きい何らかの素数で割り切れるものの個数とし、N_2 をそれ以外の N 以下の整数の個数とする。

このとき、$N_1\le\sum_{p>M}N/p<N/2$ であるが、一方で上と同様に $N_2<2^MN^{1/2}$ となる。よって N が十分大きいとき $N=N_1+N_2<N/2+2^MN^{1/2}<N$ となり、矛盾が生じる。 □

実際任意の正の整数 M に対して $N=2^{2M+2}$ ととれば $N_1\le\sum_{M<p\le N}N/p$ かつ $N_1=N-N_2\ge N-2^MN^{1/2}=2^{2M+1}=N/2$ より $\sum_{M<p\le 2^{2M+2}}1/p>1/2$ となることがわかる。

参考　G. H. Hardy and E. M. Wright, D. R. Heath-Brown, J. Silverman, A. Wiles, *An Introduction to the Theory of Numbers*, the 6th edition, Oxford University Press, 2008, Section 2.6.

8　チェビシェフの証明

チェビシェフは階乗の整数論的な性質を用いて、$x > 1$ のとき $x < p < 2x$ となる素数が存在するという有名な定理を証明した。エルデシュはこれに簡単な証明を与えている。

チェビシェフの方法は、素数が無限に多く存在することの証明に用いることができる。

$a(p, N)$ を素数 p が階乗 $N!$ を割り切る回数とする。

このとき、どの素数 $p \leq N$ に対しても、 $a(p, N) = \lfloor N/p \rfloor + \lfloor N/p^2 \rfloor + \cdots < N/(p-1)$ となり、p が N より大きい素数のとき、$a(p, N) = 0$ となる。

それで $\sum_{p \leq N} (\log p)/(p-1) > \sum_p a(p, N)(\log p)/N = (1/N) \log(N!) > (\log N) - 1$ となるから、$\sum_{p \leq N} (\log p)/(p-1)$ は N とともに正の無限大に発散する。これより、素数は無限に多く存在する。 □

参考　G. H. Hardy and E. M. Wright, D. R. Heath-Brown, J. Silverman, A. Wiles, *An Introduction to the Theory of Numbers*, the 6th edition, Oxford University Press, 2008, Section 22.7.

9　シュリニヴァサンの証明

上に述べた通り、どの 2 つも互いに素な整数からなる無限列が存在するならば、素数は無限に多く存在する。As mentioned above, any infinite sequence of pairwise coprime integers shows the infinite of primes.

数列 $x_i (i = 0, 1, \ldots)$ が $x_i \mid x_{i+1}$ かつ $\gcd(x_i, x_{i+1}/x_i) = 1$ を満足するならば、数列 $a_i = x_{i+1}/x_i (i = 0, 1, \ldots)$ は、どの 2 つも互いに素な整数からなる。

$f(x) = x^2 + x + 1$ とする。このとき $f(n^2) = n^4 + n^2 + 1 = (n^2 + n + 1)(n^2 - n + 1) = f(n)f(-n)$ であるが $n^2 + n + 1$ は常に奇数なので $\gcd(n^2 + n + 1, n^2 - n + 1) = \gcd(n^2 + n + 1, 2n) = 1$ である。

よって $x_i = f(2^{2^m})$ によって定まる数列 $x_m (m = 0, 1, \ldots)$ は上記の条件を満たす。

数列 $x_m = 2^{p^m} - 1 (m = 0, 1, \ldots)$ も上記の条件を満たす。$q \mid x_m$ ならば $x_{m+1}/x_m = ((x_m+1)^p - 1)/((x_m+1) - 1) = 1 + (x_m+1) + \cdots + (x_m+1)^{p-1} \equiv p$

$(\mathrm{mod}\ q)$ となる。よって q が $x_m, x_{m+1}/x_m$ を共に割り切るのは $q = p$ の場合のみである。しかし フェルマーの小定理より $x_m = (2^m)^p - 1 \equiv 1\ (\mathrm{mod}\ p)$ より p が x_m を割り切ることはできない。したがって $\gcd(x_m, x_{m+1}/x_m) = 1$ である。 □

$2^{p^m} - 1$ の素因数は p^m を法として 1 と合同である。したがって、上のことから p^m を法として 1 と合同な素数は無限に多く存在することがわかる。

より一般に、シュリニヴァサンはすべての正の整数 k に対して、k を法として 1 と合同な素数が無限に多く存在することを示している。これは本質的には k を法として 1 と合同な素数が無限に多く存在することのルーカスによる証明の変形である。

参考 S. Srinivasan, On infinitude of primes, *Hardy Ramanujan J.* **7** (1984), 21–26.

10 トゥエの証明

n, k を $(1+n)^k < 2^n$ となる正の整数とし、$p_1 = 2, p_2 = 3, \ldots, p_r$ を 2^n 以下のすべての素数とする。$1 \le m \le 2^n$ となるすべての整数は $m = 2^{e_1}3^{e_2}\cdots p_r^{e_r}$ の形に書くことができる。$m \le 2^n$ なので $e_i \le n$ である。このような $e_1, e_2, \ldots, e_r$ の選び方は多くても $(n+1)^r$ 通りであるから $(1+n)^k < 2^n \le (1+n)^r$ つまり $r > k$ である。任意の正の整数 k に対し、$1 + 2k^2 < 2^{2k}$ より $(1+2k^2)^k < 2^{2k^2}$ である。よって任意の正の整数 k に対し、$n = 2k^2$ ととれば n, k は冒頭の条件を満たす。したがって $2^n = 4^{k^2}$ より小さい素数の個数は少なくとも $k+1$ 個ある。 □

参考 P. Ribenboim, 上掲書, p. 7 および L. E. Dickson, 上掲書, p. 414。

11 ペロットの証明

まず、$\sum_{n=1}^{\infty}(1/n^2)$ は 2 より小さな値に収束する。実際、この和は $\pi^2/6$ に収束することはオイラーの有名な結果である。

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = 1+\frac{1}{4}+\sum_{n=3}^{\infty}\frac{1}{n^2} < \frac{5}{4}+\sum_{n=3}^{\infty}\frac{1}{n(n-1)} = \frac{5}{4}+\sum_{n=3}^{\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right) = \frac{5}{4}+\frac{1}{2} = \frac{7}{4}$$

より、$\sum_{n=1}^{\infty}(1/n^2) < 7/4$ となることはすぐにわかる。

$\delta = 2 - \sum_{n=1}^{\infty}(1/n^2)$ とおくと、上の評価より $\delta > 1/4$ となる。

さて X を任意の正の実数とし $p_1, p_2, \ldots, p_r$ を X 以下のすべての素数とする。 X 以下の整数 m で、平方数で割り切れないものの個数は多くても 2^r である。X 以下の整数 m で、d^2 で割り切れるものの個数は多くても X/d^2 であるから、X 以下の整数 m で、何らかの平方数で割り切れるものの個数は多くても $\sum_{d=2}^{\infty}(X/d^2) = X(\sum_{d=1}^{\infty}(1/d^2) - 1) = X(1-\delta)$ である。よって $X \leq 2^r + X(1-\delta)$ つまり $2^r \geq \delta X \geq N/4$ である。したがって $r > (\log X/\log 2) - 2$ となる。 □

ペロットの証明は X 以下の整数のうち各平方数 d^2 で割り切れないものを取り除くことにより X 以下の、平方数で割り切れない整数の個数を数えている。この議論は本質的には、ある条件を満たす整数の個数を評価するために発展した篩の理論の基本的な考えである。

参考　P. Ribenboim, 上掲書, p. 8 および L. E. Dickson, 上掲書, p. 413。

12　オーリックの証明

$p_1 < p_2 < \cdots < p_r$ がすべての素数であると仮定する。t を任意の正の整数とし $N = p_r^t$ とおく。

任意の N 以下の正の整数 m は r 個の非負の整数 $(f_1, f_2, \ldots, f_r)$ により $m = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$ の形に書くことができる。$E = (\log p_r)/(\log p_1)$ とおく。$p_1^{f_i} \leq p_i^{f_i} \leq m \leq N = p_r^t$ よりすべての i に対して $f_i \leq tE$ である。よって N は $1 \leq f_i \leq tE$ となる r 個の整数の組 $(f_1, f_2, \ldots, f_r)$ の選び方の個数を超えないので $p_r^t = N \leq (tE+1)^r \leq t^r(E+1)^r$ である。これは t が大きいときには成り立たない。 □

参考　P. Ribenboim, 上掲書, p. 9 および L. E. Dickson, 上掲書, p. 414。

13　Boije af Gennäs の証明

X を任意の正の実数とし、 $2, 3, \ldots, p_n$ を X 以下のすべての素数とする。$e_i (i = 1, 2, \ldots, n)$ を任意の正の整数とし $P = 2^{e_1} 3^{e_2} \cdots p_n^{e_n}$ とおく。δ と P/δ が互いに素で、かつ $Q = P/\delta - \delta > 1$ となるような δ をとる。Q は X 以下の素数では割り切れないから Q は X より大きな素数の積である。特に X より大きな素数が存在する。 □

参考 L. E. Dickson, 上掲書, p. 414。

14 バーネスの証明

1976 年にバーネスは連分数とペル方程式の理論を用いた、新しい素数の無限性の証明を発表した。

$p_1 = 2, p_2 = 3, \ldots, p_t$ がすべての素数であると仮定し、$P = \prod_{i=1}^{t} p_i, Q = \prod_{i=2}^{t} p_i$ とおく。

このとき $x = (P + \sqrt{P^2+4})/2 = Q + \sqrt{Q^2+1}$ は連分数 $x = [p, p, \ldots]$ により表される。

このとき Q^2+1 は $p_1 = 2$ 以外の素数で割り切れないので 2 の累乗でなければならない。Q^2+1 は平方数でもありえないので $Q^2+1 = 2^{2l+1}$ つまり $Q^2 - 2(2^l)^2 = -1$ でなければならない。よって $Q/2^l$ は $\sqrt{2}$ の連分数展開 $[1, 2, 2, \ldots]$ の偶数番目の近似分数なければならない。$[1, 2, 2, \ldots]$ の m 番目の近似分数を B_m とおく。それで $B_0 = 1, B_1 = 2, B_{m+1} = 2B_m + B_{m-1}$ となり m が偶数のとき、常に B_m は奇数でなければならない。したがって Q も奇数でなければならず、よって $l = 0$ つまり $Q = 1$ でなければならない。これは矛盾である。 □

もちろん、$Q^2+1 > 2$ であり Q^2+1 は 4 では決して割り切れないから Q^2+1 は 2 の累乗ではありえない。

参考 C. W. Barnes, The infinitude of primes; a proof using continued fractions, *L'Enseignement Math.* (2) **22** (1976), 313–316.

15 ブラウンの証明

t 個の素数 $p_1, p_2, \ldots, p_t$ しか存在しないと仮定し $m/n = \sum_{i=1}^{t} 1/p_i$ とおく。さて $1/2 + 1/3 + 1/5 > 1$ であるから $m/n > 1$ である。よって $m > n \geq 1$ である。したがって m は素因数 p_i を持たなければならないが、このとき $p_i \mid p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_t$ となり、これは不可能である。 □

参考 L. E. Dickson, 上掲書, p. 414。

16 ハリスの証明

A_0, A_1, A_2 を、どの 2 つも互いに素な正の整数とし $n \geq 3$ に対して $A_n = A_0A_1 \cdots A_{n-3}A_{n-1} + A_{n-2}$ とする。

このとき $A_0, A_1, \ldots, A_n$ はどの 2 つも互いに素であることが次のようにしてわかる。$p \mid \gcd(A_n, A_{n-2})$ のとき $p \mid A_n - A_{n-2} = A_0A_1 \cdots A_{n-3}A_{n-1}$ より、ある $i \geq 1, i \neq 2$ に対し $p \mid \gcd(A_{n-i}, A_{n-2})$ となる。同様に $p \mid \gcd(A_n, A_{n-j})$ for some $j \geq 1, j \neq 2$ のとき $p \mid A_n - A_0A_1 \cdots A_{n-3}A_{n-1} = A_{n-2}$ より $p \mid \gcd(A_{n-j}, A_{n-2})$ となる。以上より数学的帰納法より $A_0, A_1, \ldots, A_n$ はどの 2 つも互いに素である。$n \geq 3$ に対し $A_n > 1$ となるから $A_0, A_1, \ldots$ は 1 より大きく、かつどの 2 つも互いに素である整数の無限列を含んでいる。よって素数の個数は無限個である。 □

なお $A_0 = b_0, A_1 = b_0b_1 + 1, A_2 = b_0b_1b_2 + b_0 + b_2$ and $b_n = A_0A_1 \cdots A_{n-3}$ により数列 $b_i (i = 0, 1, \ldots)$ を定めると A_n は連分数 $[b_0, b_1, b_2, \ldots]$ の近似分数の分子となる。

参考 V. C. Harris, Another proof of the infinitude of primes, *Amer. Math. Monthly* **63** (1956), 711.

17 チェルノフの証明

チェルノフの証明は単純な数え上げの議論のみを用いる。k 個の素数 $p_1, p_2, \ldots, p_k$ しか存在しないと仮定する。N が正の整数ならば k 個の正の整数の組 $(e_1, e_2, \ldots, e_k)$ で $p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k} \leq N$ すなわち $e_1 \log p_1 + e_2 \log p_2 + \cdots + e_k \log p_k \leq \log N$ となるものは少なくとも N 個存在する（実際には素因数分解の一意性よりちょうど N 個となる）。そのような 整数の組の個数は $(\log N)^k/(k! \log p_1 \log p_2 \cdots \log p_k)$ 以下であるから $N \leq c(\log N)^k$ となる正の整数 c が（ N に無関係に）存在する。これは N が大きいとき成り立たない。よって素数は無限に多く存在する。 □

この証明では素因数分解の一意性は必要とされない。また、議論を少し変更することにより $p_1, p_2, \ldots, p_k$ を N 以下のすべての素数としてもよいことがわかる。このとき $c = 1/(k! \log 2)$ ととることができ、 $N \leq (\log N)^k/(k! \log 2)$ となる。したがって $k > c' \log N$ となる正の絶対定数 c' が存在する。つまり N 以下の素数の個数は少なくとも $c' \log N$ であることがわかる。

参考 Paul R. Chernoff, A “Lattice Point” Proof of the Infinitude of Primes. *Math. Mag.* **38** (1965), 208.