n と $2n$ の間に素数がある

―ベルトラン・チェビシェフの定理のエルデーシュによる初等的証明―

一松 信（ひとつまつ しん）

§1. はじめに

整数の性質を解析学を利用して研究する解析的数論という分野があります。多くは高度の数学を必要としますが，その入口には高校数学の範囲で理解できる成果もあります。恐らく最も易しいのが，素数の逆数全体の和は発散するという結果でしょう。

その次くらいなのが標題に掲げた結果です。これはベルトランが素数表を眺めて予想し，後にチェビシェフが証明した定理です。チェビシェフの証明はガンマ関数を使った高度のものなので，この定理の証明は非常に難しいと書いた本もありました。

しかし現在では後に「放浪の数学者」といわれたハンガリー生れの鬼才エルデーシュが高校生のときに発見した初等的な証明があります。実力のある高校生なら十分に理解できる証明で，知っていて損はしないと思いますのでここに紹介します。

ただし，以下の証明はエルデーシュの原論文の通りでなく，私が手を入れて多少わかりやすくした(つもりの)証明です。これをめぐっていろいろな逸話もありますが，本題と関係ないので省略します。

§2. 証明の方針

いささか余分かもしれませんが，その証明のあらすじを前もって記します。意欲のある方はそれをヒントにして後述の証明を自分で再構成できるかもしれません。

エルデーシュはまず二項係数の中央の値

$$c_n={}_{2n}\mathrm{C}_n=\frac{(2n)!}{n!\,n!} \qquad \cdots\cdots(1)$$

を考えます。これは整数であり，素因数分解すると，n より大きく $2n$ 以下の素数があれば，それらはすべて1乗の形の積として実際に現れます。もしもその間に素数がなければ(1)は n 以下の素数の積で表されるはずです。実はさらに $\frac{2n}{3}$ 以下の素数の積になります。$\frac{2n}{3}$ より大きく n 以下の素数は，分子に2回，分母に2回現れて約分されるからです。

ところが n までの素数全体の積は n で評価されます。それが大体 e^n くらいというのが，素数定理の一つの表現なのですが，その証明は大変です。しかしもっと粗く 4^n あるいはその半分以下というのなら，後述のように数学的帰納法で容易に証明できます。

したがって標題の命題が成立しないとすると，大雑把にいって

$$c_n<4^{\frac{2n}{3}} \qquad \cdots\cdots(2)$$

ですが，これは c_n の大きさがほぼ 4^n という事実に反します。

ただし，このままの議論は正しくありません。(1)を素因数分解したとき，2や3といった小さい素数は大きな累乗として現れるでしょう。例えば

$$c_3=2^2\cdot5,\qquad c_7=2^3\cdot3\cdot11\cdot13$$

です。しかし後述するように，個々の素数の累乗はすべて $2n$ より小さく，しかも $\sqrt{2n}$ より大きい素数は1乗でしか現れません。そして2，3の倍数は素数でないので $\sqrt{n}$ までの素数は多く見積もっても $\frac{\sqrt{n}}{3}+2$ 個です(＋2は2と3自身を数えたもの)。

こういう点を補正すると，(2)を修正した正しい不等式(後述(9))が導かれます。それは n が大きくなると成立しないので，n が十分大きければ，n と $2n$ の間に必ず素数があると結論されます。

数学の理論としてはこれで十分なのですが，問題はそうなるような n の限界値です。これが，とてつもなく大きくて，現在の高速コンピュータでもその

限界までの数について検証不可能だと，標題のようには断言できません。幸いこの場合にはその限界はごく小さく，それ以下の数 n については直接に素数表にあたって検証できます。

以上の方針で順次補助定理から始めます。

§3. 二項係数の評価

補助定理 1　$n \geqq 1$ について

$$c_n = {}_{2n}\mathrm{C}_n \leqq 2^{2n-1} \quad \cdots\cdots(3)$$

証明　$c_1 = 2 \leqq 2^1$，$c_2 = 6 < 2^3$ である。n のとき正しいとすると

$$c_{n+1} = c_n \frac{(2n+1)(2n+2)}{(n+1)^2} = c_n \frac{2(2n+1)}{n+1} \quad \cdots(4)$$

であり，$\dfrac{2n+1}{n+1} < 2$　であるから

$$c_{n+1} \leqq 2^{2n-1} \times 2 \times 2 = 2^{2n+1} = 2^{2(n+1)-1}$$

であって，$n+1$ のときも正しい。よって，数学的帰納法で証明された。■

系 1　${}_{2n-1}\mathrm{C}_n = \dfrac{1}{2} c_n \leqq 2^{2(n-1)}$　((3)から明らか)

系 2　$(n+1)$ 以上 $(2n-1)$ 以下の素数の積は，2^{2n-2} より小さい。このとき該当する素数がなければ積を 1 と解釈する。

系 2 の証明　${}_{2n-1}\mathrm{C}_n = \dfrac{(n+1)(n+2)\cdots(2n-1)}{1\cdot 2\cdots(n-1)}$

を素因数分解すると，$(n+1)$ 以上 $(2n-1)$ 以下の素数は分子に 1 回現れるだけで約分されないから積は左辺より小さい。左辺に系 1 を適用する。■

補助定理 2　n までの素数の積 P_n は $2^{2n-1} = \dfrac{1}{2} \times 4^n$ 以下である。

証明　$P_2 = 2 < 2^3$，$P_3 = 6 < 2^5$，$P_5 = 30 < 2^9$ など，小さい n については正しい。n より小さい場合は正しいとして数学的帰納法により n のときを示す。偶数 $2m$ は素数でないから $P_{2m} = P_{2m-1}$ であり，n を奇数 $2m-1$ としてよい。帰納法の仮定から

$$P_m \leqq 2^{2m-1} \quad (m < 2m-1)$$

である。他方 $(m+1)$ から $(2m-1)$ までの素数の積は，上述の系 2 により 2^{2m-2} より小さいから $n = 2m-1$ として

$$P_n = P_{2m-1} \leqq 2^{2m-1} \times 2^{2m-2} = 2^{2n-1}$$

である。■

補助定理 3　$n \geqq 4$ のとき

$$c_n = {}_{2n}\mathrm{C}_n > \frac{4^n}{n} \quad \cdots\cdots(5)$$

証明　$c_4 = 70 > \dfrac{4^4}{4} = 64$ である。$n \geqq 4$ の n について正しいとして $n+1$ のときを示す。(4)から

$$(n+1)c_{n+1} = 2(2n+1)c_n$$

であり，帰納法の仮定から

$$(n+1)c_{n+1} > 2(2n+1) \times \frac{4^n}{n} \quad \cdots\cdots(6)$$

であるが，$\dfrac{2n+1}{n} > 2$ なので(6)の右辺は，$2 \times 2 \times 4^n = 4^{n+1}$ より大きい。したがって数学的帰納法により証明された。■

§4. 素因数の累乗の評価

補助定理 4　$n!$ を素因数分解したとき，ある素数 p が p^r の形で含まれたとすると

$$r = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots\cdots + \left[\frac{n}{p^s}\right] + \cdots\cdots \quad \cdots\cdots(7)$$

である。ここに [　] はガウス記号を表すものとする。(7)の右辺は $n < p^{s+1}$ となる項以後は 0 となり，実質的に有限和である。

証明　n までの p の倍数は $\left[\dfrac{n}{p}\right]$ 個ある。$n!$ を $p^{[\frac{n}{p}]}$ で割ると，全体として p の倍数は除かれるが p^2 の倍数が残り，p の累乗指数が 1 つ減る。その個数は $\left[\dfrac{n}{p^2}\right]$ 個である。それを除くと p^3 の倍数が，累乗指数が 2 つ減って残る。この操作を反復すると有限回で p の項がすべて除かれ，割った p の全個数 r は(7)で与えられる。■

系 3　$c_n = {}_{2n}\mathrm{C}_n$ を素因数分解すると，$\sqrt{2n}$ より大きい素数は現れても p^1 の形である。それ以下の素数が p^k の形で現れれば，$p^k \leqq 2n$ である。

証明　$\left[\dfrac{2n}{p^s}\right] - 2\left[\dfrac{n}{p^s}\right] \quad \cdots\cdots(8)$

は 0 か 1 かである。実際 $\dfrac{n}{p^s}$ の小数部分が 0.5 未満ならば 0，0.5 以上ならば 1 である。

さて $\sqrt{2n} < p$ なら c_n に現れる(8)の値は $s=1$ のときだけで，$r=0$ か 1 である。それ以下の p につ

いては，$p^r \leqq 2n < p^{r+1}$ である $r(\geqq 2)$ が存在し，(8)は $s=1, 2, \cdots\cdots, r$ について現れる。各々の s に対して(8)は 0 か 1 なので，p^k の形で現れるとき $k \leqq r$ であり，$p^k \leqq p^r \leqq 2n$ である。∎

以上の諸結果をまとめると，次の事実が示されました。

定理 1　もしも n と $2n$ の間に素数がなければ，c_n は $\frac{2}{3}n$ 以下の素数の積で表される。n がある程度大きければ，$\sqrt{2n}$ 以上の素数は 1 乗の形で現れる。$\sqrt{2n}$ より小さい $\frac{\sqrt{2n}}{3}+2$ 個以下の各素数に対して，個々の p^k は $2n$ 以下である。したがって，補助定理 2，3 から

$$(2n)^{\frac{\sqrt{2n}}{3}+2} \times \frac{1}{2} \times 4^{\frac{2n}{3}} \geqq c_n > \frac{4^n}{n} \qquad \cdots\cdots(9)$$

が成立する。∎

(9)を整理して対数をとると(計算略)，不等式

$$\left(\frac{\sqrt{2n}}{3}+3\right)\log n \geqq \left(\frac{2n}{3}-\frac{\sqrt{2n}}{3}-1\right)\log 2 \qquad \cdots\cdots(10)$$

になります。ところが $n \to \infty$ とすると(10)の右辺のほうが左辺より大きくなって矛盾になります。その点を明確にし，さらに(10)が成立しない n の限界を定めるために，n を実変数 x にかえて，微分法を活用します。

§5. 微分法による評価

補助定理 5　$x > e$ のとき $\frac{\log x}{x}$ は減少関数であり，$x \to \infty$ のとき 0 に近づく。

証明　$f(x)=\frac{\log x}{x}$ とおくと

$$f'(x)=\frac{1-\log x}{x^2}$$

であるから，$x > e$ ならば $1-\log x < 0$，$f'(x) < 0$ であって，$f(x)$ は減少する。

$x \to \infty$ のときの極限値はロピタルの定理によってもよいが，次のように指数関数に直すほうがわかりやすい。$\log x = t$ とおくと $f(x)=\frac{t}{e^t}$ である。ところが，$t > 0$ のとき

$$e^t > 1+t+\frac{t^2}{2} \qquad \cdots\cdots(11)$$

である。なぜなら(11)の (左辺)−(右辺)$=g(t)$ とおくと

$$g(0)=0,\ g'(t)=e^t-(1+t),\ g'(0)=0,$$
$$g''(t)=e^t-1>0\ (t>0)$$

から，$g'(t)$ は増加で $t>0$ のとき $g'(t)>0$，したがって $g(t)$ も増加で，$t>0$ のとき $g(t)>0$ である。

これから $t \to +\infty$ のとき

$$\frac{e^t}{t} > \frac{1}{t}+1+\frac{t}{2} > \frac{t}{2} \to +\infty$$

である。その逆数 $\frac{t}{e^t}$ は 0 に近づく。∎

さて n を x にかえて(10)に $\frac{3}{x}$ を掛けると

$$\left(\sqrt{\frac{2}{x}}+\frac{9}{x}\right)\log x + \left(\sqrt{\frac{2}{x}}+\frac{3}{x}\right)\log 2 \geqq 2\log 2 \qquad \cdots\cdots(12)$$

となります。$y=\sqrt{x}$ とすると

$$\frac{\log x}{\sqrt{x}}=\frac{2\log y}{y}$$

は $y>e$，すなわち $x>e^2$ で減少であり，(12)の左辺は $x>e^2$ で減少関数です。したがって，ある x_0 で(12)の左辺が右辺の定数より小さければ，$x \geqq x_0$ において(12)は成立しないので矛盾になります。

その限界を精密に求める必要はありませんが，見当をつけるために，(12)に定数 $\log_2 e$ を掛けて，(12)の対数を 2 を底とする $\log_2$ に置き換えます。

$x_0=128=2^7\ (>e^2)$ を代入すると，(12)の左辺は

$$\left(\sqrt{\frac{2}{128}}+\frac{9}{128}\right)\times 7+\sqrt{\frac{2}{128}}+\frac{3}{128}$$
$$=\frac{63+3}{128}+\frac{7+1}{8}=1\frac{66}{128}<2=2\log_2 2$$

であって，(12)が成立しません。限界 x_0 は 128 で十分で，下記の定理 2 は $n \geqq 128$ で成立します。

128 以下なら，素数表を見ると

2，3，5，7，13，23，43，83，163，……

と次々に前の 2 倍以下の素数があります。したがって，次のように断言できます。

定理 2　任意の正の整数 n に対して，n と $2n$ の間に素数がある。

証明　$n<128$ のときは素数表を調べれば正しいことが確認できる。$n \geqq 128$ のときは，存在しないとすると，不等式(9)およびそれと同値の(12)が成立するはずだが，上述のとおり $n=x_0 \geqq 128$ では(12)が成立しないので矛盾である。∎

上記の評価をもっと粗くしても，限界 x_0 が少し大きくなるだけで大筋は変りません。そういった変形はいろいろ可能です。

§6. 発展とむすび

標題の命題は証明できましたが，上記の議論はそれ以上の内容を含んでいます。まず不等式(12)(同じことだが(9)，(10))の両辺の比較から，n と $2n$ との間にある素数の積の大きさを下から評価できます。それを精密化すると，少なくとも１つだけでなく，少なくとも何個といった個数の評価もできます。

またその積は $P_{2n} \div P_n$ ですから，補助定理２の証明と同様の帰納法により，多少技巧がいりますが

$$P_n \geqq (\sqrt{2})^n$$

を示すことができます。これは素数がどの位多くあるかという定量的評価の１つです。

さらにこれはもっと高度の数学を必要としますが，上記の議論と同様な考え方で，n が十分大きければ，n と $1.5n$ との間に素数があることを証明した論文もありました。

一言しておくと，もしも現在大きな話題になっているリーマン予想が正しければ，ある正の定数 k があって，n と $n+k\sqrt{n}$ との間に素数があるという命題が証明されます(今のところはこれは予想)。それに比べれば $2n$ とか $1.5n$ とかは随分粗い結果ですが，高度の数学を使わず，高校数学の範囲でも，工夫次第でかなりの結果が導びかれるという一例を紹介しました。

高校生の頃にこういった研究成果を上げたエルデーシュは特別な天才なのでしょうが，読者がご指導されている高校生の中からも面白い結果を考える方が現れることを期待します。

(京都大学名誉教授)