素数は無限に多く存在する証明

n を自然数とする。パスカル三角形を考えれば，二項係数は中央に近いほど大きいから

$$n\,{}_{2n}C_n = n\left({}_{2n-1}C_{n-1} + {}_{2n-1}C_n\right) \geqq \sum_{k=0}^{2n-1} {}_{2n-1}C_k = (1+1)^{2n-1} = 2^{2n-1}$$

よって，$${}_{2n}C_n \geqq \frac{2^{2n-1}}{n} \quad \cdots①$$

ルジャンドルの定理

$n!$ を素因数分解したときの素因数 p の指数は，次のように表される。

$$\sum_{k=1}^{\infty}\left\lfloor \frac{n}{p^k}\right\rfloor = \left\lfloor \frac{n}{p}\right\rfloor + \left\lfloor \frac{n}{p^2}\right\rfloor + \left\lfloor \frac{n}{p^3}\right\rfloor + \cdots$$

ただし，$\lfloor x \rfloor$ は x を超えない最大の整数を表す。

p を $2n$ 以下の素数とする。${}_{2n}C_n$ を素因数分解したときの p の指数を a_p とし，$p^k \leqq 2n$ を満たす最大の整数 k を k_p とする。${}_{2n}C_n = \dfrac{(2n)!}{(n!)^2}$ にルジャンドルの定理を用いれば

$$a_p = \sum_{k=1}^{k_p}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right)$$

m を整数，$0 \leqq x < 1$ として $\dfrac{n}{p^k} = m + x$ とおくと，$0 \leqq 2x < 2$ であるから

$$\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor = \lfloor 2m + 2x\rfloor - 2m = 2m + \lfloor 2x\rfloor - 2m = \lfloor 2x\rfloor = 0, 1$$

よって，$$a_p = \sum_{k=1}^{k_p}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right) \leqq \sum_{k=1}^{k_p} 1 = k_p$$

これより $$p^{a_p} \leqq p^{k_p} \leqq 2n \quad \cdots②$$

${}_{2n}C_n$ の素因数は $2n$ 以下であるから，$2n$ 以下の素数の個数を s とすると，②より

$${}_{2n}C_n = \prod_{p<2n} p^{a_p} \leqq (2n)^s$$

これと，①より

$$\frac{2^{2n-1}}{n} \leqq {}_{2n}C_n \leqq (2n)^s \quad \text{よって} \quad 2^{2n} \leqq (2n)^{s+1}$$

両辺の自然対数をとって整理すると

$$s \geqq \frac{2n\log 2}{\log 2n} - 1 \quad \cdots③$$

右辺は，$n \to \infty$ とすると正の無限大に発散するから，素数は無限に多く存在する。

$n \geqq 2$ として n 以下の素数の個数を $\pi(n)$ とする。③より

$$\pi(2n) \geqq \frac{2n\log 2}{\log 2n} - 1 \qquad \cdots ④$$

関数 $y = \dfrac{x}{\log x}$ は $x \geqq e$ で増加するから

$$\pi(2n-1) = \pi(2n) \geqq \frac{(2n)\log 2}{\log(2n)} - 1 > \frac{(2n-1)\log 2}{\log(2n-1)} - 1$$

よって

$$\pi(n) \geqq \frac{n\log 2}{\log n} - 1$$

チェビシェフの証明

素数が m 個(有限個)しか存在しないと仮定し，それらを小さい順に $2, 3, 5, \cdots, p_m$ とする。

ここで， $n \geqq p_m$ として， $n!$ を考える。このとき， $n!$ は素因数に $2, 3, 5, \cdots, p_m$ しか持たないが，

$n!$ の任意の素因数 p の指数を r とすると，ルジャンドルの定理により

$$r = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \leqq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{\dfrac{n}{p}}{1 - \dfrac{1}{p}} = \frac{n}{p-1}$$

よって

$$p^r \leqq p^{\frac{n}{p-1}} = \left(p^{\frac{1}{p-1}} \right)^n$$

したがって

$$n! < \left(\prod_{k=1}^{m} p_k^{\frac{1}{p_k - 1}} \right)^n \qquad \cdots ①$$

また,

$$\log(n!) = \log 2 + \log 3 + \cdots + \log n > \int_1^n \log x \, dx = [x\log x - x]_1^n = n\log n - n + 1 > n\log n - n \qquad \cdots ②$$

①，②より

$$n\log n - n < n \sum_{k=1}^{m} \frac{1}{p_k - 1} \log p_k$$

両辺を n で割って整理すると

$$\log n < 1 + \sum_{k=1}^{m} \frac{1}{p_k - 1} \log p_k$$

この不等式は任意の $n \geqq p_m$ に対して成り立つが，n が十分大きいとき左辺は右辺を超えるから矛盾する。ゆえに，素数は無限に存在する。