

MeBio 数学テキスト

順列は平方数にならない

—Erdős の証明—

目次

第1章	Bertrand の仮説	5
§ 1	きっかけ	5
§ 2	Bertrand の仮説と証明の方針	5
§ 3	左辺の下からの評価	6
§ 4	右辺第1項の上からの評価	7
§ 5	右辺第2項の上からの評価	8
§ 6	右辺第3項の上からの評価と仮説の証明	8
第2章	Sylvester–Schur の定理	11
§ 1	Sylvester–Schur の定理と証明の方針	11
§ 2	証明の第一段階	11
§ 3	系 2.3 の精密化	13
§ 4	7以下の k に対する直接証明	15
§ 5	Bertrand–Chebyshev の定理の証明と同様に出来る部分	17
§ 6	${}_n C_k$ の上からの評価	21
§ 7	残った場合	26
§ 8	復習	28
第3章	順列は平方数にならない	31
§ 1	容易にわかること	31
§ 2	$a_0 a_1 \cdots a_{n+k-1}$ の下からの評価	32
§ 3	$a_0 a_1 \cdots a_{n+k-1}$ の上からの評価	33
§ 4	矛盾を導く	35
§ 5	残った場合	36
参考文献		39

第 1 章

Bertrand の仮説

§ 1 きっかけ

東大の 2012 年の入試問題に「連続する $n(\geq 2)$ 個の自然数の積は n 乗数にならないことを示せ。」というのがあるが、これは非常に簡単な問題である。これを長男が立ち読みか何かしたときに、間違えて「連続する $n(\geq 2)$ 個の自然数の積は平方数にならないことを示せ。」という問題だと思ってしまい、それについて質問された。もちろん即答できるわけもなく、こんな難問が大学入試レベルだろうかと思んだのだが、実は間違いであると判明した。

しかし入試問題オリジナルと違っていても、この命題は実際に正しそうである。そこで証明できないだろうかと思って考えていたのだが、内容的に Bertrand の仮説に近いと調べていたら、 $n \leq 202$ の場合には成美清松 [8] が、一般の場合には Erdős [4] が本当に証明していたことを知った。しかも証明に本質的に役に立つのは、Bertrand の仮説 (Bertrand–Chebyshev の定理) およびその精密化である Sylvester–Schur の定理である。

Bertrand–Chebyshev の定理、Sylvester–Schur の定理の両方とも Erdős が簡略化に成功している ([2], [3])。そして上の問題を証明したのも Erdős である。そこで本稿ではそれらの定理を (ほぼ Erdős のラインに沿って) 証明してみよう。(多少変更している。)

§ 2 Bertrand の仮説と証明の方針

Bertrand の仮説 (1845 年) というのは次の命題のことである。

定理 1.1 あらゆる自然数 n に対し、 $n < p < 2n$ を満たす素数 p が存在する。

Chebyshev による証明 (1850 年) は難しかったのだが、Erdős が高校生のときに見つけた証明は非常に簡単である。(最近一松さんがそれをさらに改良した [5]。とはいえ本質的には同じ。)

現在の知識を何でも使ってよいのなら、この定理は非常に簡単に証明できるはずである。その点にも注意しながら、以下で「天書の証明」[1] の方法にほぼ沿った形で証明してみよう。

自然数 N と素数 p に対し、 p が N を割り切る最大回数を $\text{ord}_p N$ で表す。例えば $144 = 2^4 \cdot 3^2$ であるから $\text{ord}_2 144 = 4$ である。この記号を使うと $N = \prod_{p \leq N} p^{\text{ord}_p N}$ ということになる。ただし積は $p \leq N$ である素数 p を

動く。

ここで ${}_{2n}C_n$ を次のように表記する。

$${}_{2n}C_n = \prod_{p \leq \sqrt{2n}} p^{\text{ord}_p({}_{2n}C_n)} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^{\text{ord}_p({}_{2n}C_n)} \cdot \prod_{\frac{2}{3}n < p \leq n} p^{\text{ord}_p({}_{2n}C_n)} \cdot \prod_{n < p \leq 2n} p^{\text{ord}_p({}_{2n}C_n)} \quad (1.1)$$

n が小さいところには Bertrand の仮説の反例はない。それは必要に応じて確認しておく。十分大きな n に対して Bertrand の仮説の反例があるなら、その n に対して $\prod_{n < p \leq 2n} p^{\text{ord}_p({}_{2n}C_n)} = 1$ となる。しかし、もしそんなこと

が起これば右辺が小さすぎるのである。実例を挙げて方針を確認しておこう。

例 1.2 $n = 4095$ としてみよう. $\sqrt{2n} = \sqrt{8190} \doteq 90.49$, $\frac{2n}{3} = 2730$ である.

$$\begin{aligned} & 8190 C_{4095} \\ &= 2^{12} \cdot 3^6 \cdot 5^3 \cdot 7^3 \cdot 11^1 \cdot 13^1 \cdot 17^2 \cdot 19^2 \cdot 23^1 \cdot 29^1 \cdot 31^0 \cdot 37^2 \cdot 41^1 \cdot 43^0 \cdots 89^1 \\ &\times 97^0 \cdot 101^1 \cdot 103^1 \cdot 107^0 \cdots 2729^1 \\ &\times 2731^0 \cdot 2741^0 \cdots 4093^0 \\ &\times 4099^1 \cdot 4111^1 \cdots 8179^1 \end{aligned}$$

最初の $2^{12} \cdot 3^6 \cdot 5^3 \cdot 7^3 \cdots 89^1$ は $\sqrt{2n}$ 以下の素数に関する部分である. ここに関しては, 小さな素数は大きな冪で登場する可能性があるが, それでも $2^{12} = 4096 \leq 8190$, $3^6 = 729 \leq 8190$, $5^3 = 125 \leq 8190$, $7^3 = 343 \leq 8190$, $\cdots 89^1 = 89 \leq 8190$ というように各 p 成分それぞれがすべて $2n$ 以下であることが容易に示される. $\sqrt{2n}$ 以下の素数の個数は $\frac{\sqrt{2n}}{3} + 2$ 個以下だから (一松 [5]), この部分の積は $(2n)^{\frac{\sqrt{2n}}{3}+2}$ 以下ということになる.

(注: Erdős はもっと気前よく $\sqrt{2n}$ 以下の素数の個数は $\sqrt{2n}$ 個以下と評価している.)

2 つめの $97^0 \cdot 101^1 \cdot 103^1 \cdot 107^0 \cdots 2729^1$ は $\sqrt{2n} < p \leq \frac{2n}{3}$ の素数に関する部分である. この素数は高々 1 回しか表れない. 従ってこれらの積は $\prod_{p \leq \frac{2n}{3}} p$ 以下であるが, この部分の評価が数学的に最も重要であろう.

x 以下の素数の個数を $\pi(x)$ で表す. 素数定理 $\pi(x) \sim \frac{x}{\log x}$ の証明のためには, 第一 Chebyshev 関数 $\vartheta(x) = \sum_{p \leq x} \log p$ の $x \rightarrow \infty$ の際の漸近挙動が $\vartheta(x) \sim x$ であることを本質的に使う (亀井 [7]). ところが $\vartheta(x) \sim x$ は $\prod_{p \leq x} p \sim e^x$ と同値である. その証明は池原の定理により実現されるのだが, あまり初等的ではない. Erdős はもっと緩い条件の $\prod_{p \leq x} p < 4^{x-1}$ を初等的に証明して利用したわけである. これを認めると $\prod_{p \leq \frac{2n}{3}} p \leq 4^{\frac{2n}{3}-1}$ が得られる.

(注: 一松さん [5] は $\frac{1}{2} 4^{\frac{2n}{3}}$ 以下と評価しているが, 証明を見る限りそのまま $\frac{1}{4} 4^{\frac{2n}{3}}$ にできる. 何か深い意味があるのだろうか.)

3 つめの $2731^0 \cdot 2741^0 \cdots 4093^0$ は $\frac{2n}{3} < p \leq n$ の素数に関する部分である. この素数は現れない. 従ってこれらの積は 1 であるが, これが Erdős の証明がうまく機能する本質である.

4 つめの $4099^1 \cdot 4111^1 \cdots 8179^1$ が $n < p \leq 2n$ の素数に関する部分である. Bertrand の仮説は正しいのでここには素数が表れる (しかも数値的にここが圧倒的に大きい) のだが, もしもこの部分の積が 1 であれば, 右辺は小さすぎて左辺に等しくなれず, 矛盾するというのである.

§ 3 左辺の下からの評価

まず (1.1) の左辺がかなり大きいということから始めよう. Stirling の公式 $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$ を使うと ${}_{2n}C_n \sim \frac{1}{\sqrt{\pi n}} 4^n$ を示すことが出来るが, Bertrand の仮説の証明のためだけなら次の補題ぐらいの評価で十分である.

補題 1.3 (Erdős) ${}_{2n}C_n \geq \frac{4^n}{2n}$

証明 $(1+1)^{2n} = \sum_{k=0}^{2n} {}_{2n}C_k$ であるが ${}_{2n}C_n$ は右辺の $n+1$ 項の中の最大項であり, ${}_{2n}C_0$ と ${}_{2n}C_{2n}$ は2項合わせても値が2で最小だから, ${}_{2n}C_0 + {}_{2n}C_{2n}, {}_{2n}C_1, \dots, {}_{2n}C_n, \dots, {}_{2n}C_{2n}$ の相加平均よりも大きい. □

定理の証明にはこれで十分なのだが, 次の評価の方が少し精密である.

補題 1.4 (一松 [5]) $n \geq 4$ のとき ${}_{2n}C_n > \frac{4^n}{n}$

証明 $n = 4$ のとき 左辺 = ${}_8C_4 = 70$, 右辺 = $\frac{4^4}{4} = 64$ で成立する. $n+1 \geq 5$ については帰納法で

$$\begin{aligned} {}_{2n+2}C_{n+1} &= {}_{2n}C_n \times \frac{(2n+1)(2n+2)}{(n+1)(n+1)} \\ &> \frac{4^n}{n} \times \frac{(2n+1)(2n+2)}{(n+1)(n+1)} = \frac{4^{n+1}}{n+1} \times \frac{2n+1}{2n} \times \frac{2n+2}{2(n+1)} \\ &> \frac{4^{n+1}}{n+1} \end{aligned}$$

従って成立する. □

§ 4 右辺第1項の上からの評価

(1.1) の右辺第1項の上からの評価に移ろう.

補題 1.5 実数 a, b に対し $[a+b] - [a] - [b]$ は 0 または 1 である.

証明 $[a] = m, [b] = n$ とすると $m \leq a < m+1, n \leq b < n+1$ だから $m+n \leq a+b < m+n+2$ である. 従って $[a+b] = m+n$ または $m+n+1$ がいえる. □

補題 1.6 $p^{\text{ord}_p({}_{2n}C_n)} \leq 2n$

証明 $\text{ord}_p(2n)! = \sum_{k=1}^{\infty} \left[\frac{2n}{p^k} \right], \text{ord}_p n! = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]$ より $\text{ord}_p({}_{2n}C_n) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - \left[\frac{n}{p^k} \right] - \left[\frac{n}{p^k} \right] \right)$.

補題 1.5 より $\left[\frac{2n}{p^k} \right] - \left[\frac{n}{p^k} \right] - \left[\frac{n}{p^k} \right]$ の各項は 0 または 1 であるが, $k > \log_p 2n$ のときは $0 < \frac{2n}{p^k} < 1$ であるから明らかに 0 である. 従ってこの形式的無限和は実は高々 $[\log_p 2n]$ 個の 1 の足し算であり, $\text{ord}_p({}_{2n}C_n) \leq \log_p 2n$ つまり $p^{\text{ord}_p({}_{2n}C_n)} \leq 2n$ が従う. □

補題 1.7 n 以下の素数の数を $\pi(n)$ とすると, $\pi(n) \leq \frac{n}{3} + 2$.

証明 $n \leq 8$ のとき正しいことは確認出来る. $n \geq 9$ のとき $n-6 \geq 3$ であるが, 3 より大きい素数 p は $p \equiv 1, 5 \pmod 6$ を満たすから 4以降の連続 6 整数中には高々 2 つしかない. 帰納法により $\pi(n) \leq \pi(n-6) + 2 \leq \left(\frac{n-6}{3} + 2 \right) + 2 = \frac{n}{3} + 2$. □

系 1.8 $\prod_{p \leq \sqrt{2n}} p^{\text{ord}_p({}_{2n}C_n)} \leq (2n)^{\frac{\sqrt{2n}}{3} + 2}$

証明 補題 1.6, 補題 1.7 より明らか □

§ 5 右辺第2項の上からの評価

(1.1)の右辺第2項の上からの評価に移ろう.

補題 1.9 $\sqrt{2n} < p$ のとき $\text{ord}_p(2nC_n) \leq 1$

証明 $k \geq 2$ のとき $p^k > 2n$ であつて $\left[\frac{2n}{p^k} \right] = 0$ だから, 無限和は $k = 1$ に対応する項しかなく

$$\text{ord}_p(2nC_n) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - \left[\frac{n}{p^k} \right] - \left[\frac{n}{p^k} \right] \right) = \left[\frac{2n}{p} \right] - \left[\frac{n}{p} \right] - \left[\frac{n}{p} \right]$$

補題 1.5 よりこの式の値は0または1である. □

補題 1.10 n 以下の素数の積を $P_n = \prod_{p \leq n} p$ とすると, $P_n \leq 4^{n-1}$ である.

証明 帰納法で示す. $n = 2, 3, 4, 5$ に関して正しい. $n = 2m$ のとき $P_{2m} = P_{2m-1}$ であるから n が奇数 $2m-1$ のときのみ示せばよい. ${}_{2m-1}C_{m-1} = (m+1)(m+2)\cdots(2m-1)$ は $m < p \leq 2m-1$ であるすべての素数を因数に持つので

$$P_{2m} \leq P_m \times {}_{2m-1}C_{m-1}$$

帰納法の仮定より $P_m \leq 4^{m-1}$ である. また,

$$(1+1)^{2m-1} = {}_{2m-1}C_0 + {}_{2m-1}C_1 + \cdots + {}_{2m-1}C_{m-1} + {}_{2m-1}C_m + \cdots + {}_{2m-1}C_{2m-1}$$

で ${}_{2m-1}C_{m-1} = {}_{2m-1}C_m$ であるから ${}_{2m-1}C_{m-1} \leq \frac{2^{2m-1}}{2} = 4^{m-1}$ である. 従つて $P_{2m-1} \leq 4^{2m-2}$ が証明された. これより帰納法が進み, 題意は成立する. □

系 1.11 $\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\text{ord}_p(2nC_n)} \leq 4^{\frac{2n}{3}-1}$

証明 補題 1.9, 補題 1.10 より

$$\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\text{ord}_p(2nC_n)} \leq \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p \leq \prod_{p \leq \frac{2n}{3}} p \leq 4^{\frac{2n}{3}-1}$$

□

§ 6 右辺第3項の上からの評価と仮説の証明

(1.1)の右辺第3項の上からの評価は簡単である.

補題 1.12 $\frac{2n}{3} < p \leq n$ (かつ $n \geq 3$) のとき $\text{ord}_p(2nC_n) = 0$

証明 $0 < p \leq n < 2p \leq 2n < 3p$ かつ $p^2 \geq \frac{4}{9}n^2 > n$ だから

$$\text{ord}_p(2nC_n) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k} \right] - \left[\frac{n}{p^k} \right] - \left[\frac{n}{p^k} \right] \right) = \left[\frac{2n}{p} \right] - \left[\frac{n}{p} \right] - \left[\frac{n}{p} \right] = 2 - 1 - 1 = 0$$

□

系 1.13 $n \geq 3$ のとき $\prod_{\frac{2}{3}n < p \leq n} p^{\text{ord}_p(2n C_n)} = 1$ □

Bertrand の仮説の証明 Bertrand の仮説の反例があるとしてその数を n と置く. $n \geq 3$ としてよい. その場合, 補題 1.4, 系 1.8, 系 1.11, 系 1.13 より次の不等式が成り立つ.

$$\begin{aligned} \frac{4^n}{n} &\leq (2n)^{\frac{\sqrt{2n}}{3}+2} \cdot 4^{\frac{2n}{3}-1} \\ \Leftrightarrow 2 \cdot 4^{\frac{n}{3}+1} &\leq (2n)^{\frac{\sqrt{2n}}{3}+3} \\ \Leftrightarrow 2^{\frac{2n}{3}+3} &\leq (2n)^{\frac{\sqrt{2n}}{3}+3} \\ \Leftrightarrow \left(\frac{2n}{3} + 3\right) \log 2 &\leq \left(\frac{\sqrt{2n}}{3} + 3\right) \log 2n \\ &(\sqrt{2n} = x \text{ と置き換える}) \\ \Leftrightarrow \left(\frac{x^2}{3} + 3\right) \log 2 &\leq \left(\frac{x}{3} + 3\right) \log x^2 \\ \Leftrightarrow \frac{1}{2} \log 2 &\leq \frac{x+9}{x^2+9} \log x \end{aligned}$$

しかし最後の式は大きな x に対しては成立しない. 例えば $x \geq 9$ とすると

$$\frac{x+9}{x^2+9} \log x \leq \frac{2x}{x^2} \log x \leq \frac{2}{x} \log x$$

$f(x) = \frac{2 \log x}{x}$ は $x > e$ で単調減少であり, $f(32) = \frac{2}{32} \log 32 = \frac{5}{16} \log 2 < \frac{1}{2} \log 2$ であるから Bertrand の仮説は $x = \sqrt{2n} \geq 32$ ($\Leftrightarrow n \geq 512$) には反例を持たないことになる. $n < 512$ にも反例を持たないことは素数列

2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631

を考えれば容易にわかるので, これで証明が完了した. □

第 2 章

Sylvester–Schur の定理

§ 1 Sylvester–Schur の定理と証明の方針

Sylvester–Schur の定理とは次の命題のことである.

定理 2.1 「 n, k を $n \geq 2k$ を満たす自然数とする. 順列 ${}_n P_k = n(n-1)\cdots(n-k+1)$ は k より大きい素因数を持つ。」これは次のように言い換えてもよいことは明らかである.

「 n, k を $n \geq 2k$ を満たす自然数とする. 二項係数 ${}_n C_k$ は k より大きい素因数を持つ。」 □

$n = 2k$ の場合が Bertrand–Chebyshev の定理に同値な命題となる.

これが Bertrand–Chebyshev の定理と同じように証明できるかどうかを検証してみよう. Sylvester–Schur の定理に反例があったとする. つまり ${}_n C_k$ の素因数がすべて k 以下であるような (n, k) が存在するとする. その反例に対し ${}_n C_k$ を構成素数ごとに分解表記する.

$${}_n C_k = \prod_{p \leq k} p^{\text{ord}_p({}_n C_k)}$$

左辺を下から評価し, 右辺を上から評価して矛盾することを示すのであるが, $k \doteq n$ の場合と $k \ll n$ の場合とでは同じようには行かない. そのあたりの事情も含めて以下で証明していこう.

§ 2 証明の第一段階

まず, 最も単純な評価から得られる結論を考えてみる.

補題 2.2 $p^{\text{ord}_p({}_n C_k)} \leq n$

証明 $\text{ord}_p({}_n C_k) = \sum_{l=1}^{\infty} \left(\left\lfloor \frac{n}{p^l} \right\rfloor - \left\lfloor \frac{k}{p^l} \right\rfloor - \left\lfloor \frac{n-k}{p^l} \right\rfloor \right)$ であるが, 補題 1.5 よりこの和の各項は 0 または 1 である.

$l > \log_p n$ の場合 $\left\lfloor \frac{n}{p^l} \right\rfloor = 0$ であるから, 和は高々 $[\log_p n]$ 個の 1 の足し算でしかない. 従って $\text{ord}_p({}_n C_k) \leq \log_p n$ であり, 補題は成り立つ. □

系 2.3

- (1) $8 \leq k \leq \sqrt{n}$ には Sylvester–Schur の反例は存在しない.
- (2) $33 \leq k \leq n^{\frac{2}{3}}$ には Sylvester–Schur の反例は存在しない.

証明 ${}_n C_k$ が k 以下の素因数しか持たないのであれば

$${}_n C_k = \prod_{p \leq k} p^{\text{ord}_p({}_n C_k)} \leq \prod_{p \leq k} n = n^{\pi(k)}$$

($\pi(k)$ は k 以下の素数の個数であった.) 一方次の不等式が成り立っている.

$${}_n C_k = \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \frac{n-2}{k-2} \cdots \frac{n-k+1}{1} > \left(\frac{n}{k}\right)^k$$

$\pi(8) = 4, \pi(9) = 4$ で、それ以降 $\pi(k+2) \leq \pi(k) + 1$ が成り立つのだから、 $8 \leq k$ のとき $\pi(k) \leq \frac{k}{2}$ が帰納的に言える. これら3式より $\left(\frac{n}{k}\right)^k < n^{\frac{k}{2}}$ が成り立つことになるが、

$$\left(\frac{n}{k}\right)^k < n^{\frac{k}{2}} \iff n^{\frac{k}{2}} < k^k \iff \sqrt{n} < k$$

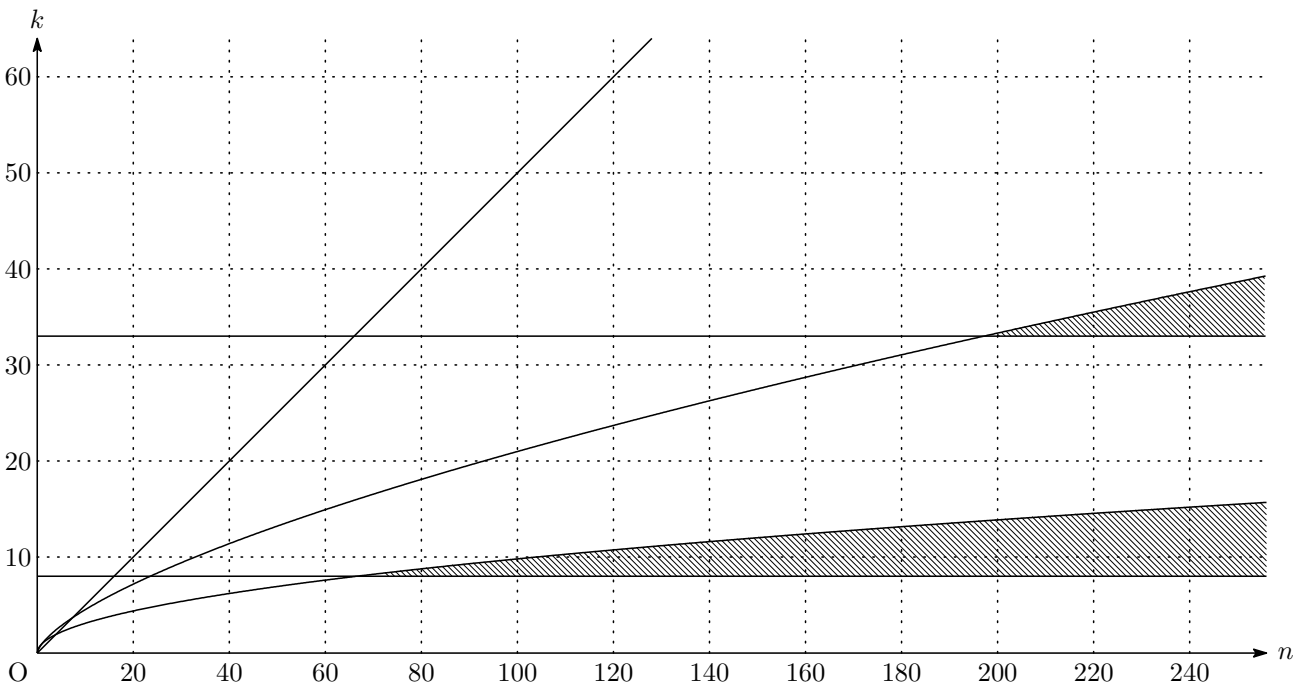
従って (1) が証明された.

また、 $\pi(33) = 11, \pi(34) = 11, \pi(35) = 11, \pi(36) = 11, \pi(37) = 12, \pi(38) = 12$ はすべて $\pi(k) \leq \frac{k}{3}$ を満たしており、これ以降 $\pi(k+6) \leq \pi(k) + 2$ が成り立つのだから、 $33 \leq k$ のとき $\pi(k) \leq \frac{k}{3}$ が帰納的に言える. これら3式より $\left(\frac{n}{k}\right)^k < n^{\frac{k}{3}}$ が成り立つことになるが、

$$\left(\frac{n}{k}\right)^k < n^{\frac{k}{3}} \iff n^{\frac{2k}{3}} < k^k \iff n^{\frac{2}{3}} < k$$

従って (2) が証明された. □

今わかったことは、次の図の斜線部分に Sylvester-Schur の定理の反例が存在しないということである.



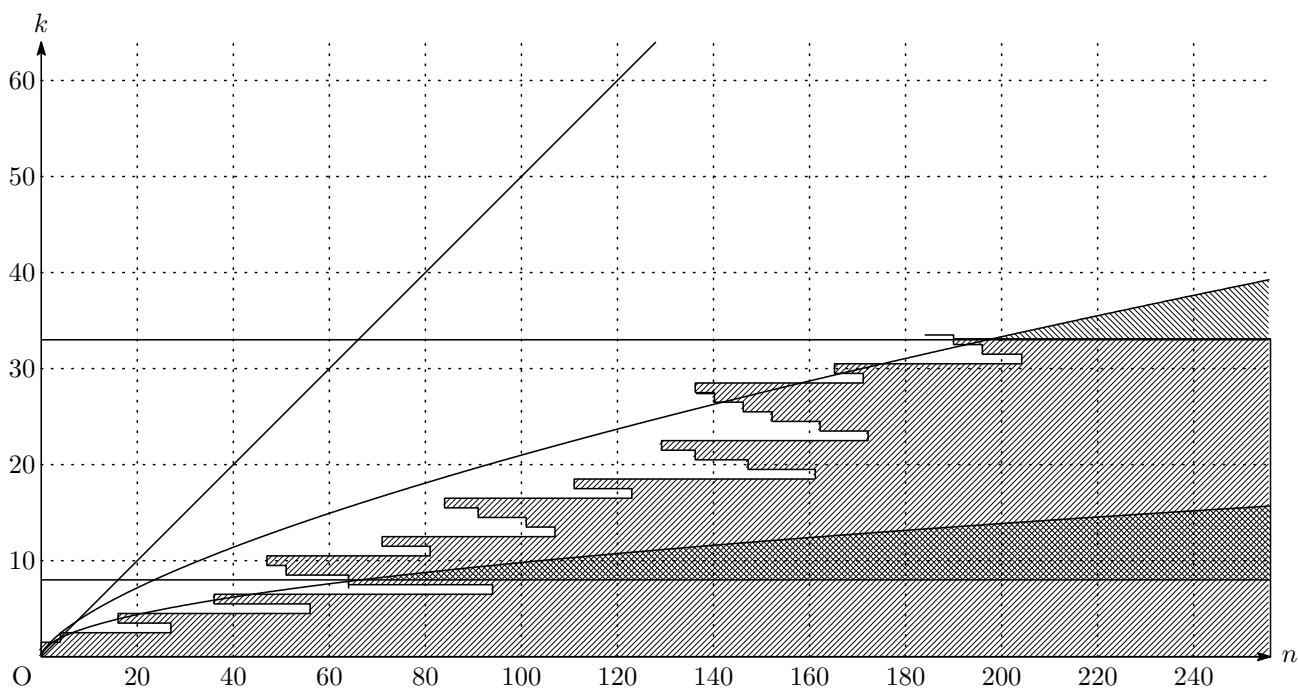
この斜線部分を $0 < 2k \leq n$ まで広げてやるのが目標である.

- (i) $8 \leq k \leq 32$ に関しては、示さないといけないことは上の図からもわかるとおり有限個の (n, k) に関する成立だけである。(図の下側の放物線 $k = \sqrt{n}$ は $(1089, 33)$ で $k = 33$ に交わる.) 地道に調べてもよいのだが、これでは多すぎるのもう少しばっさり減らしてから調べることにする.
- (ii) $1 \leq k \leq 7$ に関しては非常に初等的に証明することが出来る.
- (iii) $33 \leq k$ かつ $n^{\frac{2}{3}} \leq k \leq \frac{n}{2}$ に関しては次の節以降で証明する.

§ 3 系 2.3 の精密化

系 2.3 で証明したのは、 $\left(\frac{n}{k}\right)^k \geq n^{\pi(k)}$ つまり $n \geq k^{\frac{k}{k-\pi(k)}}$ には Sylvester-Schur の反例が存在しないということである。(1) では k が 8 以上のときを $k = 8$ の式で評価し、(2) では k が 33 以上のときを $k = 33$ の式で評価したに過ぎない。そこで $2 \leq k \leq 33$ (実は $2 \leq k \leq 89$) のそれ以外の k についても本当に調べてみると、次の表 2.1 のようになる。¹

これらのデータより、Sylvester-Schur の定理の反例が存在しない領域は次の斜線部まで拡張される。



$k \leq 33$ の反例の存在する可能性のある領域をつぶしていこう。

37 以上の素因数を持つ数列 (の部分列) は次のようになっている。

37, 43, 47, 53, 61, 67, 73, 79, 83, 89, 94(= 2 × 47), 97, 103, 109, 113, 118(= 2 × 59), 122(= 2 × 61),
 127, 131, 139, 134(= 2 × 67), 139, 142(= 2 × 71), 146(= 2 × 73), 149, 151, 157, 163, 167, 173, 179,

¹ 上の評価を $k > 33$ に対しても続けていくと反例の存在する領域が有界に押さえられないだろうかと思ったのだが無理である。

$$k^{\frac{k}{k-\pi(k)}} < 2k \iff \pi(k) < \frac{k \log 2}{\log k + \log 2}$$

であるが、素数定理より $\pi(k) \sim \frac{k}{\log k}$ なので、これは k を大きくしても実現されない。

表 2.1: $k^{\frac{k}{k-\pi(k)}}$ の評価

k	$\pi(k)$	$k - \pi(k)$	$\frac{k}{k - \pi(k)}$	$k^{\frac{k}{k-\pi(k)}}$	k	$\pi(k)$	$k - \pi(k)$	$\frac{k}{k - \pi(k)}$	$k^{\frac{k}{k-\pi(k)}}$
2	1	1	2.00	4.00	46	14	32	1.44	245.59
3	2	1	3.00	27.00	47	15	32	1.47	285.69
4	2	2	2.00	16.00	48	15	33	1.45	278.90
5	3	2	2.50	55.90	49	15	34	1.44	272.82
6	3	3	2.00	36.00	50	15	35	1.43	267.36
7	4	3	2.33	93.73	51	15	36	1.42	262.46
8	4	4	2.00	64.00	52	15	37	1.41	258.04
9	4	5	1.80	52.20	53	16	37	1.43	295.06
10	4	6	1.67	46.42	54	16	38	1.42	289.62
11	5	6	1.83	81.14	55	16	39	1.41	284.68
12	5	7	1.71	70.80	56	16	40	1.40	280.20
13	6	7	1.86	117.15	57	16	41	1.39	276.12
14	6	8	1.75	101.33	58	16	42	1.38	272.40
15	6	9	1.67	91.23	59	17	42	1.40	307.34
16	6	10	1.60	84.45	60	17	43	1.40	302.79
17	7	10	1.70	123.53	61	18	43	1.42	340.94
18	7	11	1.64	113.26	62	18	44	1.41	335.46
19	8	11	1.73	161.72	63	18	45	1.40	330.43
20	8	12	1.67	147.36	64	18	46	1.39	325.80
21	8	13	1.62	136.74	65	18	47	1.38	321.53
22	8	14	1.57	128.68	66	18	48	1.38	317.59
23	9	14	1.64	172.63	67	19	48	1.40	353.91
24	9	15	1.60	161.56	68	19	49	1.39	349.20
25	9	16	1.56	152.86	69	19	50	1.38	344.84
26	9	17	1.53	145.91	70	19	51	1.37	340.79
27	9	18	1.50	140.30	71	20	51	1.39	377.78
28	9	19	1.47	135.72	72	20	52	1.38	372.98
29	10	19	1.53	170.64	73	21	52	1.40	412.88
30	10	20	1.50	164.32	74	21	53	1.40	407.26
31	11	20	1.55	204.93	75	21	54	1.39	402.02
32	11	21	1.52	196.59	76	21	55	1.38	397.14
33	11	22	1.50	189.57	77	21	56	1.38	392.58
34	11	23	1.48	183.62	78	21	57	1.37	388.31
35	11	24	1.46	178.55	79	22	57	1.39	426.62
36	11	25	1.44	174.21	80	22	58	1.38	421.65
37	12	25	1.48	209.38	81	22	59	1.37	416.99
38	12	26	1.46	203.66	82	22	60	1.37	412.62
39	12	27	1.44	198.70	83	22	61	1.36	408.51
40	12	28	1.43	194.38	84	22	62	1.35	404.66
41	13	28	1.46	229.92	85	22	63	1.35	401.04
42	13	29	1.45	224.34	86	22	64	1.34	397.63
43	14	29	1.48	264.26	87	23	64	1.36	433.05
44	14	30	1.47	257.27	88	23	65	1.35	429.07
45	14	31	1.45	251.09	89	24	65	1.37	466.84

183(= 3 × 61), 188(= 2² × 47), 193, 199, 202(= 2 × 101), 206(= 2 × 103), 211, 215(= 5 × 43),
 219(= 3 × 73), 223, 229, …

この数列は、どの隣り合う数の差も6以下になっていることがわかる。これは $\{(n, k) \mid 6 \leq k \leq 36, 37 \leq n \leq 234\}$ には反例が存在しないことを表す。(37^{3/2} = 225.06 だから、この長方形の右上は $k < n^{2/3}$ の領域に達している.)

19以上の素因数を持つ数列(の部分列)は次のようになっている。

19, 23, 29, 31, 37, …

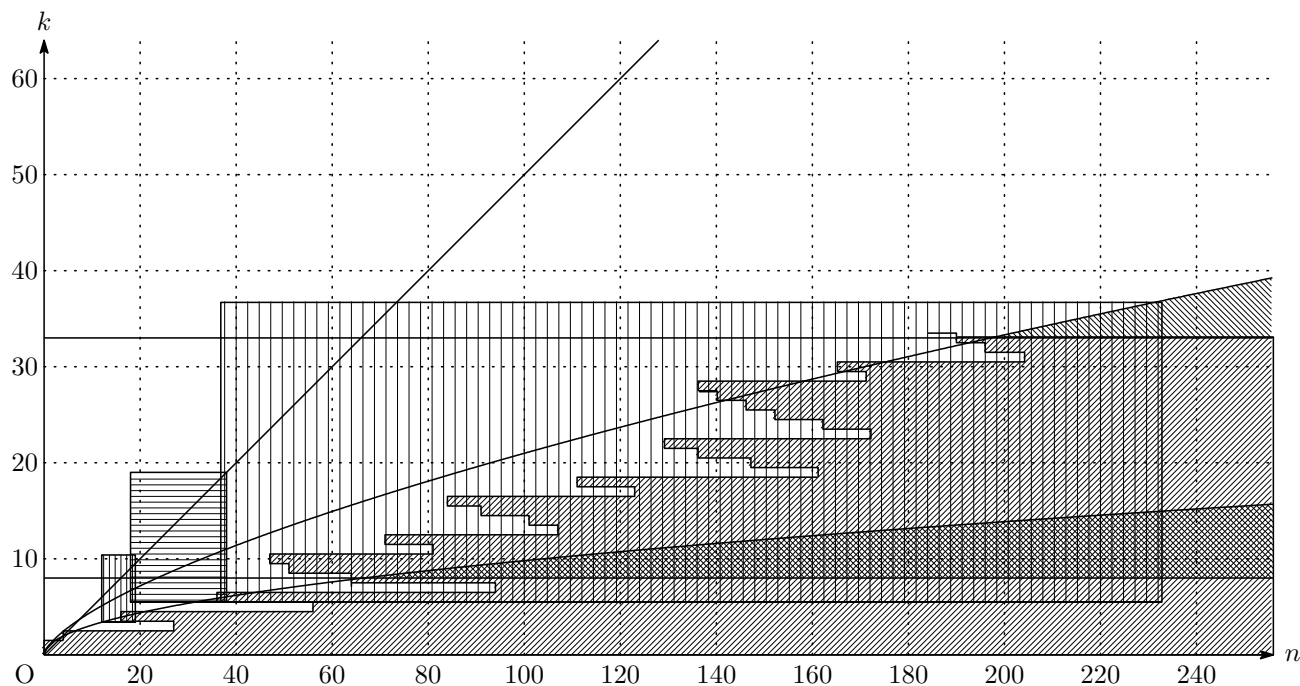
この数列は、どの隣り合う数の差も6以下になっていることがわかる。これは $\{(n, k) \mid 6 \leq k \leq 18, 19 \leq n \leq 37\}$ には反例が存在しないことを表す。

11以上の素因数を持つ数列(の部分列)は次のようになっている。

11, 13, 17, …

この数列は、どの隣り合う数の差も4以下になっていることがわかる。これは $\{(n, k) \mid 4 \leq k \leq 10, 11 \leq n \leq 19\}$ には反例が存在しないことを表す。

ここまでの状況を次の図に表す。斜線部分が反例の存在しない領域である。



以上より $k \leq 37$ で潰せていないのは $(n, k) = (10, 5) \sim (55, 5)$ と $(n, k) = (6, 3) \sim (27, 3)$ (の部分集合) になった。これが実際に潰れることを数値的に確認するのは非常に容易であるが、一般論としての証明もなかなか面白いので、以下でやってみよう。

§4 7以下の k に対する直接証明

$k = 1$ の場合「2以上の自然数 n は1より大きい素因数を持つ」という命題になって示すべきことは何もない。

命題 2.4 $k = 2$ の場合「4以上の自然数 n に対し $n(n-1)$ は2より大きい素因数を持つ」という命題になる。これは $n, n-1$ の一方が3以上の奇数だから明らかである。 □

命題 2.5 $k = 3$ の場合 6 以上の自然数 n に対し $n(n-1)(n-2)$ は 3 より大きい素因数を持つ.

証明 反例があったとすると, $n(n-1)(n-2)$ は 2 と 3 だけしか素因数に持てない. 従って奇数の約数は 3 の冪乗にならざるを得ないが, $n, n-1, n-2$ のうち 3 の倍数は一つなので, $n-1$ だけが奇数である. すると $n, n-2$ は 3 を因数に持たない偶数の約数となるから素因数は 2 だけを持つ, しかし 2 の冪乗の 2 数の差が 2 になるのは $\{2, 4\}$ の組み合わせだけである. これは $n \geq 2k = 6$ に反する. \square

命題 2.6 $k = 4$ の場合 8 以上の自然数 n に対し $n(n-1)(n-2)(n-3)$ は 4 より大きい素因数を持つ.

証明 反例があったとすると, $n(n-1)(n-2)(n-3)$ は 2 と 3 だけしか素因数に持てない. 従って奇数の約数は 3 の冪乗にならざるを得ないが, $n, n-1, n-2, n-3$ のうち奇数は 2 つあり, そのうちの一方は 3 の倍数ではない. これは矛盾. \square

命題 2.7 $k = 5$ の場合 10 以上の自然数 n に対し $n(n-1)(n-2)(n-3)(n-4)$ は 5 より大きい素因数を持つ.

証明 反例があったとすると, $n(n-1)(n-2)(n-3)(n-4)$ は 2, 3, 5 だけしか素因数に持てない. $n, n-1, n-2, n-3, n-4$ のうち奇数は 2 つまたは 3 つであるが, それらのうち 3 の倍数は高々一つ, 5 の倍数も高々一つである. 従って奇数の約数は $n-1, n-3$ の 2 個であり, そのうちの一方が 3 の冪乗, 他方が 5 の冪乗にならざるを得ない. すると $n, n-2, n-4$ は偶数となるが, これらのどれも 5 の倍数ではなく, $n, n-4$ の一方だけが 3 の倍数であるから, 残りの 2 つは 2 の冪乗である. 2 の冪乗の 2 数の差が 2 になるのは $\{2, 4\}$ の組み合わせだけなので $n \geq 10$ に反する. \square

命題 2.8 $k = 6$ の場合 12 以上の自然数 n に対し $n(n-1)(n-2)(n-3)(n-4)(n-5)$ は 6 より大きい素因数を持つ.

証明 反例があったとすると, $n(n-1)(n-2)(n-3)(n-4)(n-5)$ は 2, 3, 5 だけしか素因数に持てない. $n, n-1, n-2, n-3, n-4, n-5$ のうち奇数は 3 つあり, それらのうち 3 の倍数, 5 の倍数は高々一つずつしかない. すると少なくとも一つは 3 も 5 も素因数に持てなくなってしまう. これは矛盾. \square

命題 2.9 $k = 7$ の場合 14 以上の自然数 n に対し $n(n-1)(n-2)(n-3)(n-4)(n-5)(n-6)$ は 7 より大きい素因数を持つ.

証明 反例があったとすると, $n(n-1)(n-2)(n-3)(n-4)(n-5)(n-6)$ は 2, 3, 5, 7 だけしか素因数に持てない. $n, \dots, n-6$ に奇数が 4 つあったとすると, そのうち 7 の倍数は高々 1 つ, 5 の倍数は高々 1 つ, 3 の倍数は高々 2 つであるが, これら高々延べ 4 つは本当に 4 つでないで残りの奇数が因数を持てなくなってしまう. その場合 n と $n-6$ が 3 冪ということになるが, 差が 6 になる 3 冪の 2 数は $\{9, 3\}$ だけである. これは矛盾.

これより $n, \dots, n-6$ に奇数が 3 つあることになる. 7 の倍数は高々 1 つ, 5 の倍数は高々 1 つ, 3 の倍数は高々 1 つで, これら高々延べ 3 つは本当に合計 3 つでなければならない.

その場合 4 つの偶数について, 奇数因子を持たない純粋な 2 冪は高々 1 個である. (2 冪の差が 2, 4, 6 はいずれも不適になるため.) また, 2 冪でない偶数 (奇数因子を持つ偶数) のうち, 7 の倍数は 0 個, 5 の倍数は高々 1 個, 3 の倍数は高々 2 個となり, 合計高々 3 個になるので, 実際これらはすべて異なる必要がある. その場合 $n = 2^k \cdot 3$, $n-6 = 2^l \cdot 3$ となるが, $2^k - 2^l = 2$ は不適である. \square

以上で $k \leq 37$ に関しては完全に解決した.

§ 5 Bertrand–Chebyshev の定理の証明と同様に出来る部分

Sylvester–Schur の定理に反例があるとして、その (n, k) に対して

$${}_n C_k = \prod_{p \leq \sqrt{n}} p^{\text{ord}_p({}_n C_k)} \cdot \prod_{\sqrt{n} < p \leq k} p^{\text{ord}_p({}_n C_k)}$$

と分解表示する。今までの結果より、反例があるとする (n, k) は $k \geq 37, 2k \leq n < k^{\frac{3}{2}}$ を満たさないといけない。

$n \geq 2k$ であるから、補題 1.4 より左辺は ${}_n C_k \geq {}_{2k} C_k \geq \frac{4^k}{k}$ と評価される。右辺第 1 項に関しては補題 2.2 より $\prod_{p \leq \sqrt{n}} p^{\text{ord}_p({}_n C_k)} \leq n^{\sqrt{n}}$ がわかっている。右辺第 2 項に関しては補題 1.9, 補題 1.10 より $\prod_{\sqrt{n} < p \leq k} p^{\text{ord}_p({}_n C_k)} \leq 4^{k-1}$ がわかっている。これだけの評価から何か結論が得られるかやってみよう。成り立つことがわかる不等式は

$$\frac{4^k}{k} < n^{\sqrt{n}} \cdot 4^{k-1} \tag{2.1}$$

である。これは $4 < kn^{\sqrt{n}}$ と同値であるが、これから得られる情報は何もない。Bertrand–Chebyshev の定理の証明がうまくいったのは、 $\frac{n}{3} < p < n$ の素数が存在しないということから右辺の 4 の冪を左辺より小さく出来たからである。この場合もそれを狙ってみよう。

$l < p \leq k$ の範囲にある素数 p が ${}_n C_k$ の素因数に現れないのであれば、(2.1) の右辺の 4^{k-1} を 4^{l-1} に変更でき、それより n, k の範囲を有界に納めることが出来るようになる。この l を具体的に求めよう。

$\sqrt{n} < p \leq k$ を満たす素数 p が ${}_n C_k$ に現れない為の十分条件は、 $\left[\frac{n}{p} \right] = \left[\frac{k}{p} \right] + \left[\frac{n-k}{p} \right]$ が成り立つことである。仮に k が素数で $p = k$ ならばこの式は成り立つ。つまり $p = k$ は ${}_n C_k$ の素因数に現れない。 k 以下であって k に近い素数 p がこの条件を満たす十分条件 (必要条件ではない) は

$$\left[\frac{n}{p} \right] = \left[\frac{n}{k} \right] \text{ かつ } \left[\frac{k}{p} \right] = \left[\frac{k}{k} \right] \text{ かつ } \left[\frac{n-k}{p} \right] = \left[\frac{n-k}{k} \right] \tag{2.2}$$

が成り立つことである。

補題 2.10 $\frac{n}{N+1} < p \leq k \leq \frac{n}{N}$ であれば (2.2) が成り立つ。

証明 与式の逆数を考えると $\frac{N}{n} \leq \frac{1}{k} \leq \frac{1}{p} < \frac{N+1}{n} \dots \textcircled{1}$ 。これより $N \leq \frac{n}{k} \leq \frac{n}{p} < N+1$ だから

$$\left[\frac{n}{p} \right] = \left[\frac{n}{k} \right] = N \text{ である。}$$

$\textcircled{1}$ に k をかけて $\left(\frac{N}{n} k \leq \right) 1 \leq \frac{k}{p} < \frac{N+1}{n} k$ 。ここで $\frac{N+1}{n} k \leq \frac{N+1}{n} \times \frac{n}{N} = 1 + \frac{1}{N} < 2$ であるから $1 = \frac{k}{k} \leq \frac{k}{p} < 2$ ということになり $\left[\frac{k}{p} \right] = \left[\frac{k}{k} \right] = 1$ である。

$\textcircled{1}$ に $n-k$ をかけて $\frac{N}{n}(n-k) \leq \frac{n-k}{k} \leq \frac{n-k}{p} < \frac{N+1}{n}(n-k)$ 。ここで

$$\begin{aligned} \frac{N}{n}(n-k) &> \frac{N}{n} \left(n - \frac{n}{N+1} \right) = N - \frac{N}{N+1} > N-1 \\ \frac{N+1}{n}(n-k) &\leq \frac{N+1}{n} \left(n - \frac{n}{N} \right) = N - \frac{1}{N} < N \end{aligned}$$

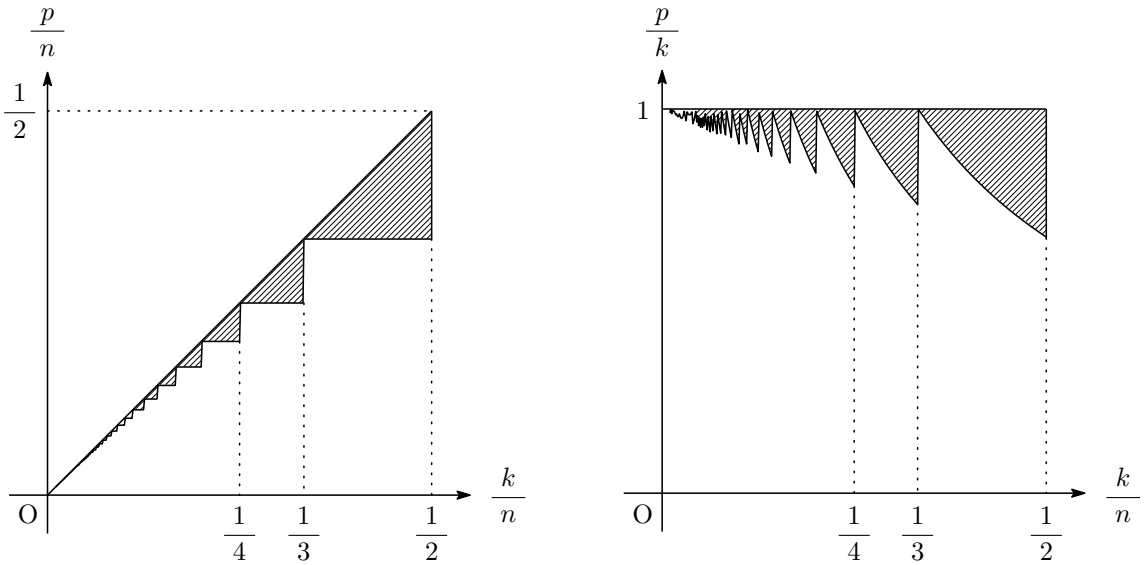
であるから $N - 1 < \frac{n - k}{k} \leq \frac{n - k}{p} < N$ ということになり $\left[\frac{n - k}{p} \right] = \left[\frac{n - k}{k} \right] = N - 1$ である. □

系 2.11 $\frac{n}{N + 1} < k \leq \frac{n}{N}$ であれば $\frac{n}{N + 1} < p \leq k$ である素数 p は ${}_n C_k$ の素因数にならない. □

$$\frac{n}{N + 1} < p \leq k \iff N \leq \frac{n}{k} < N + 1 \iff N = \left[\frac{n}{k} \right] \text{ だから}$$

$$\frac{n}{N + 1} < p \leq k \iff \frac{1}{\left[\frac{n}{k} \right] + 1} < \frac{p}{n} \leq \frac{k}{n}$$

となる. $\frac{k}{n}$ を横軸, $\frac{p}{n}$ を縦軸にとって, この領域を $0.1 < \frac{k}{n} \leq \frac{1}{2}$ で図示してみると次のようになる.



図からもわかるように, $\frac{k}{n}$ が $\frac{1}{3}$ と $\frac{1}{2}$ の真ん中あたりから $\frac{1}{2}$ までの間にある場合は, 削れる領域がかなりあって有効であるが, $\frac{1}{3}$ に近づけすぎると領域がほぼなくなりうまく機能しなくなる. $\frac{1}{3}$ 以下の部分にも削れる部分は存在するが, どのみち $\frac{1}{3}$ の付近を別の方法で処理しないといけなくなるのだから, この方法で考えるのはやめにする. そこで以下では $\frac{2n}{5} < k \leq \frac{n}{2}$ の場合を考えることにする.

系 2.12 $\frac{2n}{5} < k \leq \frac{n}{2}$ ($\iff 2k \leq n < \frac{5}{2}k$) であれば $\frac{n}{3} < p \leq k$ である素数 p は ${}_n C_k$ の素因数にならない. □

系 2.13 $\frac{2n}{5} < k \leq \frac{n}{2}$ ($\iff 2k \leq n < \frac{5}{2}k$) の範囲に Sylvester-Schur の定理に反例があれば, その (n, k) に対して

$${}_n C_k = \prod_{p \leq \sqrt{n}} p^{\text{ord}_p({}_n C_k)} \cdot \prod_{\sqrt{n} < p \leq \frac{n}{3}} p^{\text{ord}_p({}_n C_k)}$$

が成り立つ. 従って

$$\frac{4^k}{k} < n^{\sqrt{n}} \cdot 4^{\frac{n}{3}-1} \tag{2.3}$$

が成り立つ. □

$\frac{2n}{5} < k \leq \frac{n}{2}$ を使ってこの不等式 (2.3) を変形していく. $\frac{4^x}{x}$ が $x \geq 1$ で単調増加であることは容易にわかるので

$$\begin{aligned} & \frac{4^k}{k} < n^{\sqrt{n}} \cdot 4^{\frac{n}{3}-1} \\ \implies & \frac{4^{\frac{2n}{5}}}{\frac{2n}{5}} < n^{\sqrt{n}} \cdot 4^{\frac{n}{3}-1} \\ \iff & \frac{2n}{5} \log 4 - \log \frac{2n}{5} < \sqrt{n} \log n + \left(\frac{n}{3} - 1\right) \log 4 \\ \iff & \left(\frac{2}{15}n + 3\right) \log 2 < (\sqrt{n} + 1) \log n \\ \iff & \frac{2}{15}n \log 2 - \sqrt{n} \log n - \log n + \log 10 < 0 \end{aligned}$$

$f(x) = \frac{2}{15}x \log 2 - \sqrt{x} \log x - \log x + \log 10$ と置く. $f'(x) = \frac{2}{15} \log 2 - \frac{1}{2\sqrt{x}} \log x - \frac{1}{\sqrt{x}} - \frac{1}{x}$ である.

$f'(x)$ は単調増加関数で,

$$f'(2^{14}) = \frac{2}{15} \log 2 - \frac{14}{2^8} \log 2 - \frac{1}{128} - \frac{1}{16384} = \frac{302}{3840} \log 2 - \frac{127}{16384} > 0$$

より $f(x)$ は $x > 2^{14}$ で単調増加, また

$$f(2^{14}) = \frac{2^{15}}{15} \log 2 - 2^7 \log 2^{14} - \log 2^7 + \log 10 = \frac{5888}{15} \log 2 + \log 10 > 0$$

以上より $n \geq 2^{14} = 16384$ に関しては反例がないことが示された.

$n < 2^{14} = 16384$ に関しても反例がないことは次の数列を考えればわかる.

73 以上の素数列は次のようになっている.

- 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223
 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379
 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557
 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727
 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911
 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069
 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229
 1231 1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399
 1409 1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543
 1549 1553 1559 1567 1571 1579 1583 1597 1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693
 1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 1801 1811 1823 1831 1847 1861 1867
 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949 1951 1973 1979 1987 1993 1997 1999 2003 2011 2017
 2027 2029 2039 2053 2063 2069 2081 2083 2087 2089 2099 2111 2113 2129 2131 2137 2141 2143 2153 2161 2179
 2203 2207 2213 2221 2237 2239 2243 2251 2267 2269 2273 2281 2287 2293 2297 2309 2311 2333 2339 2341 2347
 2351 2357 2371 2377 2381 2383 2389 2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477 2503 2521
 2531 2539 2543 2549 2551 2557 2579 2591 2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683 2687
 2689 2693 2699 2707 2711 2713 2719 2729 2731 2741 2749 2753 2767 2777 2789 2791 2797 2801 2803 2819 2833

2837 2843 2851 2857 2861 2879 2887 2897 2903 2909 2917 2927 2939 2953 2957 2963 2969 2971 2999 3001 3011
3019 3023 3037 3041 3049 3061 3067 3079 3083 3089 3109 3119 3121 3137 3163 3167 3169 3181 3187 3191 3203
3209 3217 3221 3229 3251 3253 3257 3259 3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347 3359 3361
3371 3373 3389 3391 3407 3413 3433 3449 3457 3461 3463 3467 3469 3491 3499 3511 3517 3527 3529 3533 3539
3541 3547 3557 3559 3571 3581 3583 3593 3607 3613 3617 3623 3631 3637 3643 3659 3671 3673 3677 3691 3697
3701 3709 3719 3727 3733 3739 3761 3767 3769 3779 3793 3797 3803 3821 3823 3833 3847 3851 3853 3863 3877
3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001 4003 4007 4013 4019 4021 4027 4049
4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133 4139 4153 4157 4159 4177 4201 4211 4217 4219 4229
4231 4241 4243 4253 4259 4261 4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373 4391 4397 4409
4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547 4549 4561 4567 4583 4591
4597 4603 4621 4637 4639 4643 4649 4651 4657 4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759 4783
4787 4789 4793 4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937 4943 4951 4957
4967 4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059 5077 5081 5087 5099 5101 5107 5113
5119 5147 5153 5167 5171 5179 5189 5197 5209 5227 5231 5233 5237 5261 5273 5279 5281 5297 5303 5309 5323
5333 5347 5351 5381 5387 5393 5399 5407 5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501
5503 5507 5519 5521 5527 5531 5557 5563 5569 5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669
5683 5689 5693 5701 5711 5717 5737 5741 5743 5749 5779 5783 5791 5801 5807 5813 5821 5827 5839 5843 5849
5851 5857 5861 5867 5869 5879 5881 5897 5903 5923 5927 5939 5953 5981 5987 6007 6011 6029 6037 6043 6047
6053 6067 6073 6079 6089 6091 6101 6113 6121 6131 6133 6143 6151 6163 6173 6197 6199 6203 6211 6217 6221
6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311 6317 6323 6329 6337 6343 6353 6359 6361 6367 6373
6379 6389 6397 6421 6427 6449 6451 6469 6473 6481 6491 6521 6529 6547 6551 6553 6563 6569 6571 6577 6581
6599 6607 6619 6637 6653 6659 6661 6673 6679 6689 6691 6701 6703 6709 6719 6733 6737 6761 6763 6779 6781
6791 6793 6803 6823 6827 6829 6833 6841 6857 6863 6869 6871 6883 6899 6907 6911 6917 6947 6949 6959 6961
6967 6971 6977 6983 6991 6997 7001 7013 7019 7027 7039 7043 7057 7069 7079 7103 7109 7121 7127 7129 7151
7159 7177 7187 7193 7207 7211 7213 7219 7229 7237 7243 7247 7253 7283 7297 7307 7309 7321 7331 7333 7349
7351 7369 7393 7411 7417 7433 7451 7457 7459 7477 7481 7487 7489 7499 7507 7517 7523 7529 7537 7541 7547
7549 7559 7561 7573 7577 7583 7589 7591 7603 7607 7621 7639 7643 7649 7669 7673 7681 7687 7691 7699 7703
7717 7723 7727 7741 7753 7757 7759 7789 7793 7817 7823 7829 7841 7853 7867 7873 7877 7879 7883 7901 7907
7919 7927 7933 7937 7949 7951 7963 7993 8009 8011 8017 8039 8053 8059 8069 8081 8087 8089 8093 8101 8111
8117 8123 8147 8161 8167 8171 8179 8191 8209 8219 8221 8231 8233 8237 8243 8263 8269 8273 8287 8291 8293
8297 8311 8317 8329 8353 8363 8369 8377 8387 8389 8419 8423 8429 8431 8443 8447 8461 8467 8501 8513 8521
8527 8537 8539 8543 8563 8573 8581 8597 8599 8609 8623 8627 8629 8641 8647 8663 8669 8677 8681 8689 8693
8699 8707 8713 8719 8731 8737 8741 8747 8753 8761 8779 8783 8803 8807 8819 8821 8831 8837 8839 8849 8861
8863 8867 8887 8893 8923 8929 8933 8941 8951 8963 8969 8971 8999 9001 9007 9011 9013 9029 9041 9043 9049
9059 9067 9091 9103 9109 9127 9133 9137 9151 9157 9161 9173 9181 9187 9199 9203 9209 9221 9227 9239 9241
9257 9277 9281 9283 9293 9311 9319 9323 9337 9341 9343 9349 9371 9377 9391 9397 9403 9413 9419 9421 9431
9433 9437 9439 9461 9463 9467 9473 9479 9491 9497 9511 9521 9533 9539 9547 9551 9587 9601 9613 9619 9623
9629 9631 9643 9649 9661 9677 9679 9689 9697 9719 9721 9733 9739 9743 9749 9767 9769 9781 9787 9791 9803
9811 9817 9829 9833 9839 9851 9857 9859 9871 9883 9887 9901 9907 9923 9929 9931 9941 9949 9967 9973 10007
10009 10037 10039 10061 10067 10069 10079 10091 10093 10099 10103 10111 10133 10139 10141 10151 10159
10163 10169 10177 10181 10193 10211 10223 10243 10247 10253 10259 10267 10271 10273 10289 10301 10303
10313 10321 10331 10333 10337 10343 10357 10369 10391 10399 10427 10429 10433 10453 10457 10459 10463
10477 10487 10499 10501 10513 10529 10531 10559 10567 10589 10597 10601 10607 10613 10627 10631 10639
10651 10657 10663 10667 10687 10691 10709 10711 10723 10729 10733 10739 10753 10771 10781 10789 10799
10831 10837 10847 10853 10859 10861 10867 10883 10889 10891 10903 10909 10937 10939 10949 10957 10973
10979 10987 10993 11003 11027 11047 11057 11059 11069 11071 11083 11087 11093 11113 11117 11119 11131
11149 11159 11161 11171 11173 11177 11197 11213 11239 11243 11251 11257 11261 11273 11279 11287 11299

11311 11317 11321 11329 11351 11353 11369 11383 11393 11399 11411 11423 11437 11443 11447 11467 11471
 11483 11489 11491 11497 11503 11519 11527 11549 11551 11579 11587 11593 11597 11617 11621 11633 11657
 11677 11681 11689 11699 11701 11717 11719 11731 11743 11777 11779 11783 11789 11801 11807 11813 11821
 11827 11831 11833 11839 11863 11867 11887 11897 11903 11909 11923 11927 11933 11939 11941 11953 11959
 11969 11971 11981 11987 12007 12011 12037 12041 12043 12049 12071 12073 12097 12101 12107 12109 12113
 12119 12143 12149 12157 12161 12163 12197 12203 12211 12227 12239 12241 12251 12253 12263 12269 12277
 12281 12289 12301 12323 12329 12343 12347 12373 12377 12379 12391 12401 12409 12413 12421 12433 12437
 12451 12457 12473 12479 12487 12491 12497 12503 12511 12517 12527 12539 12541 12547 12553 12569 12577
 12583 12589 12601 12611 12613 12619 12637 12641 12647 12653 12659 12671 12689 12697 12703 12713 12721
 12739 12743 12757 12763 12781 12791 12799 12809 12821 12823 12829 12841 12853 12889 12893 12899 12907
 12911 12917 12919 12923 12941 12953 12959 12967 12973 12979 12983 13001 13003 13007 13009 13033 13037
 13043 13049 13063 13093 13099 13103 13109 13121 13127 13147 13151 13159 13163 13171 13177 13183 13187
 13217 13219 13229 13241 13249 13259 13267 13291 13297 13309 13313 13327 13331 13337 13339 13367 13381
 13397 13399 13411 13417 13421 13441 13451 13457 13463 13469 13477 13487 13499 13513 13523 13537 13553
 13567 13577 13591 13597 13613 13619 13627 13633 13649 13669 13679 13681 13687 13691 13693 13697 13709
 13711 13721 13723 13729 13751 13757 13759 13763 13781 13789 13799 13807 13829 13831 13841 13859 13873
 13877 13879 13883 13901 13903 13907 13913 13921 13931 13933 13963 13967 13997 13999 14009 14011 14029
 14033 14051 14057 14071 14081 14083 14087 14107 14143 14149 14153 14159 14173 14177 14197 14207 14221
 14243 14249 14251 14281 14293 14303 14321 14323 14327 14341 14347 14369 14387 14389 14401 14407 14411
 14419 14423 14431 14437 14447 14449 14461 14479 14489 14503 14519 14533 14537 14543 14549 14551 14557
 14561 14563 14591 14593 14621 14627 14629 14633 14639 14653 14657 14669 14683 14699 14713 14717 14723
 14731 14737 14741 14747 14753 14759 14767 14771 14779 14783 14797 14813 14821 14827 14831 14843 14851
 14867 14869 14879 14887 14891 14897 14923 14929 14939 14947 14951 14957 14969 14983 15013 15017 15031
 15053 15061 15073 15077 15083 15091 15101 15107 15121 15131 15137 15139 15149 15161 15173 15187 15193
 15199 15217 15227 15233 15241 15259 15263 15269 15271 15277 15287 15289 15299 15307 15313 15319 15329
 15331 15349 15359 15361 15373 15377 15383 15391 15401 15413 15427 15439 15443 15451 15461 15467 15473
 15493 15497 15511 15527 15541 15551 15559 15569 15581 15583 15601 15607 15619 15629 15641 15643 15647
 15649 15661 15667 15671 15679 15683 15727 15731 15733 15737 15739 15749 15761 15767 15773 15787 15791
 15797 15803 15809 15817 15823 15859 15877 15881 15887 15889 15901 15907 15913 15919 15923 15937 15959
 15971 15973 15991 16001 16007 16033 16057 16061 16063 16067 16069 16073 16087 16091 16097 16103 16111
 16127 16139 16141 16183 16187 16189 16193 16217 16223 16229 16231 16249 16253 16267 16273 16301 16319
 16333 16339 16349 16361 16363 16369 16381 16411

これらの中で隣り合う 2 数の差が 38 より大きいのは (15683, 15727), (16141, 16183) だけなのであるが、今考えているのは $2k \leq n < \frac{5}{2}k$ の領域なのでこれらは反例にならない。また、 $15703 = 41 \times 383$, $16161 = 3 \times 5387$ という素因数分解を持つ合成数を補えば、 $\{(n, k) \mid 38 \leq k \leq 8209, 73 \leq n \leq 16419\}$ には反例が存在しないことがわかる。

とまあ、一応証明は出来たのだが、これではちょっとみつともない。原因は (2.3) の右辺の評価 $\prod_{1 < p < \sqrt{n}} p^{\text{ord}_p({}_n C_k)} < n^{\sqrt{n}}$ が甘すぎるためである。この証明は取り下げることにして、次節で ${}_n C_k$ の上からの評価をもう少し精密に与えてみよう。

§ 6 ${}_n C_k$ の上からの評価

後で使うので、Chebyshev 関数およびその指数型を定義しておこう。

定義 2.14

(1) 実数 $x > 0$ (整数でなくてもよい) に対し $\Theta(x)$ を

$$\Theta(x) = \prod_{p \leq x} p$$

で定義する. (その対数は第一 Chebyshev 関数 $\vartheta(x) = \sum_{p \leq x} \log p$ である.)

(2) $x > 0$ に対し $\Psi(x)$ を

$$\Psi(x) = \text{l.c.m}\{1, 2, \dots, [x] - 1, [x]\}$$

で定義する. (その対数は第二 Chebyshev 関数 $\psi(x) = \log(\text{l.c.m}\{1, 2, \dots, [x] - 1, [x]\})$ である.)

命題 2.15 $\Psi(x)$ と $\Theta(x)$ には次の関係がある.

$$\Psi(x) = \prod_{l=1}^{\infty} \Theta(\sqrt[l]{x}) = \Theta(x) \cdot \Theta(\sqrt{x}) \cdot \Theta(\sqrt[3]{x}) \cdots$$

対数型で述べると $\psi(x) = \sum_{l=1}^{\infty} \vartheta(\sqrt[l]{x}) = \vartheta(x) + \vartheta(\sqrt{x}) + \vartheta(\sqrt[3]{x}) + \cdots$ となる.

証明 各素数 p に対し, 明らかに $\text{ord}_p \Psi(x) = [\log_p x]$. また $\text{ord}_p \Theta(x) = \begin{cases} 1 & (p \leq x) \\ 0 & (p > x) \end{cases}$ であるから

$$\text{ord}_p \prod_{l=1}^{\infty} \Theta(\sqrt[l]{x}) = \sum_{l=1}^{\infty} \text{ord}_p \Theta(\sqrt[l]{x}) = \#\{h \in \mathbb{N} \mid p \leq x^{1/h}\} = \#\{h \in \mathbb{N} \mid h \leq \log_p x\} = [\log_p x]$$

□

補題 2.16 k に関わらず

$${}_n C_k \leq \Psi(n) \tag{2.4}$$

が成り立つ.

証明 補題 2.2 で見たように, 各素数 p に対し $\text{ord}_p({}_n C_k) = \sum_{l=1}^{\infty} \left(\left[\frac{n}{p^l} \right] - \left[\frac{k}{p^l} \right] - \left[\frac{n-k}{p^l} \right] \right) \leq [\log_p n]$ である. $\text{ord}_p \Psi(n) = [\log_p n]$ だからこの補題は成立する. □

次に必要なのは $\Psi(n)$ の上からの評価である. それに関しては $\psi(x) \sim x$ より $\Psi(x) \sim e^x$ が知られている (これから素数定理が証明される) が, ここでは初等的に $\Psi(n) \leq 4^n$ を示そう.

(風あざみ氏 [6] によると $\Psi(n) \leq \frac{4^n}{2n}$ も示すことが出来る.)

補題 2.17

- (1) $\Psi(2m) \leq \Psi(m) \cdot {}_{2m} C_m$
- (2) $\Psi(2m+1) \leq \Psi(m+1) \cdot {}_{2m+1} C_{m+1}$

証明

- (1) 各素数 p に対し $\text{ord}_p \Psi(2m) \leq \text{ord}_p \Psi(m) + \text{ord}_p ({}_{2m} C_m)$ が示されればよい. $\text{ord}_p \Psi(m) \leq \text{ord}_p \Psi(2m) \leq \text{ord}_p \Psi(m) + 1$ であることは容易にわかる.

- (i) $\text{ord}_p \Psi(2m) = \text{ord}_p \Psi(m)$ であれば問題はない.
- (ii) $\text{ord}_p \Psi(2m) = \text{ord}_p \Psi(m) + 1$ となるのは $m < p^h \leq 2m$ となる $h \in \mathbb{N}$ が存在することが必要十分である. その場合

$$\text{ord}_p({}_{2m}C_m) = \sum_{l=1}^{\infty} \left(\left[\frac{2m}{p^l} \right] - 2 \left[\frac{m}{p^l} \right] \right) \geq \left[\frac{2m}{p^h} \right] - 2 \left[\frac{m}{p^h} \right] = 1$$

であるからやはり成立する.

- (2) 各素数 p に対し $\text{ord}_p \Psi(2m+1) \leq \text{ord}_p \Psi(m+1) + \text{ord}_p({}_{2m+1}C_{m+1})$ が示されればよい.
 $\text{ord}_p \Psi(m+1) \leq \text{ord}_p \Psi(2m+1) \leq \text{ord}_p \Psi(m+1) + 1$ であることは容易にわかる.

- (i) $\text{ord}_p \Psi(2m+1) = \text{ord}_p \Psi(m+1)$ であれば問題はない.
- (ii) $\text{ord}_p \Psi(2m+1) = \text{ord}_p \Psi(m+1) + 1$ となるのは $m+1 < p^h \leq 2m+1$ となる $h \in \mathbb{N}$ が存在することが必要十分である. その場合

$$\begin{aligned} \text{ord}_p({}_{2m+1}C_{m+1}) &= \sum_{l=1}^{\infty} \left(\left[\frac{2m+1}{p^l} \right] - \left[\frac{m+1}{p^l} \right] - \left[\frac{m}{p^l} \right] \right) \\ &\geq \left[\frac{2m+1}{p^h} \right] - \left[\frac{m+1}{p^h} \right] - \left[\frac{m}{p^h} \right] = 1 - 0 - 0 = 1 \end{aligned}$$

であるからやはり成立する.

□

命題 2.18 $n \geq 2$ に対し $\Psi(n) \leq 4^n$ が成り立つ.

証明 帰納法で証明する. $n = 1, 2$ の場合は明らかに成り立つ.

- (1) $n = 2m$ の場合

補題 2.17 より $\Psi(2m) \leq \Psi(m) \cdot {}_{2m}C_m$ が成り立っている. 帰納法の仮定により $\Psi(m) \leq 4^m$ である. また ${}_{2m}C_m \leq (1+1)^{2m} = 4^m$ もわかる. 従って $\Psi(n) = \Psi(2m) \leq 4^m \cdot 4^m = 4^{2m} = 4^n$ がいえた.

- (2) $n = 2m+1$ の場合

補題 2.17 より $\Psi(2m+1) \leq \Psi(m+1) \cdot {}_{2m+1}C_{m+1}$ が成り立っている. 帰納法の仮定により $\Psi(m+1) \leq 4^{m+1}$ である. また ${}_{2m+1}C_{m+1} = {}_{2m+1}C_m$ および ${}_{2m+1}C_m + {}_{2m+1}C_{m+1} \leq (1+1)^{2m+1} = 2 \cdot 4^m$ より ${}_{2m+1}C_{m+1} \leq 4^m$ もわかる. 従って $\Psi(n) = \Psi(2m+1) \leq 4^{m+1} \cdot 4^m = 4^{2m+1} = 4^n$ がいえた.

□

補題 2.16, 命題 2.18 より任意の k に対して ${}_n C_k \leq 4^n$ が得られるが, こんな不等式なら最初から成立するのはわかっているし, Sylvester-Schur の定理の証明にも何の役にも立たない. ${}_n C_k$ の各 p 成分の個数を細かく見る必要がある.

補題 2.19 次が成り立つ.

$${}_n C_k \leq \Theta(n) \cdot \Theta(\sqrt{n}) \cdot \Theta(\sqrt[3]{n}) \cdot \Theta(\sqrt[4]{n}) \cdot \Theta(\sqrt[5]{n}) \cdot \Theta(\sqrt[6]{n}) \cdots \quad (2.5)$$

証明 素数 p に対し $\text{ord}_p({}_n C_k) = \sum_{l=1}^{\infty} \left(\left[\frac{n}{p^l} \right] - \left[\frac{k}{p^l} \right] - \left[\frac{n-k}{p^l} \right] \right)$ であるが,

$$\left[\frac{n}{p^l} \right] - \left[\frac{k}{p^l} \right] - \left[\frac{n-k}{p^l} \right] = \begin{cases} 0 \text{ または } 1 & (l \leq \log_p n) \\ 0 & (l > \log_p n) \end{cases}$$

一方

$$\text{ord}_p \Theta(\sqrt[l]{n}) = \begin{cases} 1 & (p \leq \sqrt[l]{n}) \\ 0 & (p > \sqrt[l]{n}) \end{cases} = \begin{cases} 1 & (l \leq \log_p n) \\ 0 & (l > \log_p n) \end{cases}$$

従って $\text{ord}_p({}_n C_k) \leq \text{ord}_p(\Theta(n) \cdot \Theta(\sqrt{n}) \cdot \Theta(\sqrt[3]{n}) \cdot \Theta(\sqrt[4]{n}) \cdot \Theta(\sqrt[5]{n}) \cdot \Theta(\sqrt[6]{n}) \cdots)$ が成り立ち、命題は成立する。□

この右辺は $\Psi(n)$ であって、これでは補題 2.16 と何の違もない。しかし、この補題の証明を少し変更すると次が得られる。

命題 2.20 ${}_n C_k$ が $u (u < n)$ より大きな素因数を持たないとすると。

$${}_n C_k \leq \Theta(u) \cdot \Theta(\sqrt{n}) \cdot \Theta(\sqrt[3]{n}) \cdot \Theta(\sqrt[4]{n}) \cdot \Theta(\sqrt[5]{n}) \cdot \Theta(\sqrt[6]{n}) \cdots \tag{2.6}$$

証明 (2.6) は (2.5) の右辺の第 1 因子 $\Theta(n)$ から $u < p \leq n$ である素因子を取り除いたものであるが、その p に関しては $\text{ord}_p({}_n C_k) = 0$ なのであるから $\text{ord}_p({}_n C_k) \leq \text{ord}_p(\Theta(u) \cdot \Theta(\sqrt{n}) \cdot \Theta(\sqrt[3]{n}) \cdot \Theta(\sqrt[4]{n}) \cdot \Theta(\sqrt[5]{n}) \cdot \Theta(\sqrt[6]{n}) \cdots)$ であることはやはり成り立つ。 u 以下の p に関しては (2.6) と (2.5) に違いはない。□

定理 2.21 命題 2.20 において $u \geq n^{\frac{2}{3}}$ が成り立っていれば

$${}_n C_k \leq \Psi(u) \cdot \Psi(\sqrt{n}) \left(\leq 4^{u+\sqrt{n}} \right) \tag{2.7}$$

が成り立つ。

証明 命題 2.15 より (2.6) の偶数項だけを掛け合わせれば $\Psi(\sqrt{n})$ になる。

$$\Theta(\sqrt{n}) \cdot \Theta(\sqrt[4]{n}) \cdot \Theta(\sqrt[6]{n}) \cdots = \Psi(\sqrt{n})$$

奇数項に関しては $n^{\frac{1}{3}} \leq u^{\frac{1}{2}}, n^{\frac{1}{5}} \leq u^{\frac{3}{10}} < u^{\frac{1}{3}}, n^{\frac{1}{7}} \leq u^{\frac{3}{14}} < u^{\frac{1}{4}}, \dots$ などがすべて成り立つので

$$\Theta(u) \cdot \Theta(\sqrt[3]{n}) \cdot \Theta(\sqrt[5]{n}) \cdot \Theta(\sqrt[7]{n}) \cdots \leq \Theta(u) \cdot \Theta(\sqrt[2]{u}) \cdot \Theta(\sqrt[3]{u}) \cdot \Theta(\sqrt[4]{u}) \cdots = \Psi(u)$$

以上より定理は成り立つ。□

これを使って前節で挫折した証明を完遂しよう。

定理 2.22 $2k \leq n < \frac{5}{2}k \left(\iff \frac{2n}{5} < k \leq \frac{n}{2} \right)$ には Sylvester-Schur の定理の反例はない。

証明 反例 (n, k) があつたとする。系 2.11 より $\frac{n}{3} < p \leq k$ である素数 p は ${}_n C_k$ の素因数にならない。従って命題 2.20 より

$${}_n C_k \leq \Theta\left(\frac{n}{3}\right) \cdot \Theta(\sqrt{n}) \cdot \Theta(\sqrt[3]{n}) \cdot \Theta(\sqrt[4]{n}) \cdot \Theta(\sqrt[5]{n}) \cdot \Theta(\sqrt[6]{n}) \cdots \tag{2.8}$$

2章 §4 までで $k \leq n^{\frac{2}{3}}$ または $k \leq 37$ には反例がないことを示しているのだから、反例がある場合 $k > n^{\frac{2}{3}}$ かつ $k > 37$ である。また $\frac{n}{3} < n^{\frac{2}{3}} \iff n^{\frac{1}{3}} < 3 \iff n < 27$ であるが、今の場合には $n \geq 2k > 74$ なのであるから $\frac{n}{3} < n^{\frac{2}{3}}$ は成り立たない。つまり $\frac{n}{3} \geq n^{\frac{2}{3}}$ である。従って $u = \frac{n}{3}$ は定理 2.21 の仮定を満たし、

$${}_n C_k \leq \Psi\left(\frac{n}{3}\right) \cdot \Psi(\sqrt{n}) \left(\leq 4^{\frac{n}{3}+\sqrt{n}} \right) \tag{2.9}$$

が成り立つ. また ${}_nC_k$ は補題 1.4 より ${}_nC_k \geq 2^k C_k \geq \frac{4^k}{k}$ と下から評価される.

以上より $\frac{4^k}{k} \leq 4^{\frac{n}{3} + \sqrt{n}}$ が得られた. これが大きな n に対しては成立しないことを見よう.

$$\begin{aligned} \frac{4^k}{k} &\leq 4^{\frac{n}{3} + \sqrt{n}} \\ \implies \frac{4^{\frac{2n}{3}}}{\frac{n}{2}} &< 4^{\frac{n}{3} + \sqrt{n}} \\ \iff 2 \cdot 4^{\frac{n}{15}} &< n \cdot 4^{\sqrt{n}} \\ \iff \log 2 + \frac{2n}{15} \log 2 &< \log n + 2\sqrt{n} \log 2 \\ \iff \frac{2n}{15} \log 2 - 2\sqrt{n} \log 2 - \log n + \log 2 &< 0 \end{aligned}$$

$f(x) = \frac{2x}{15} \log 2 - 2\sqrt{x} \log 2 - \log x + \log 2$ と置く. $f(x) \sim \frac{2x}{15} \log 2$ であるからこの不等式はいずれ成り立たないのは明らかであるが, 必要なのはその評価である.

$$f'(x) = \frac{2}{15} \log 2 - \frac{1}{\sqrt{x}} \log 2 - \frac{1}{x}$$

だから非常に大雑把に見て $x > 15^2 = 225$ のとき

$$f'(x) > \frac{2}{15} \log 2 - \frac{1}{15} \log 2 - \frac{1}{225} = \frac{1}{225} (15 \log 2 - 1) > 0$$

であることがわかる. つまり単調増加である.

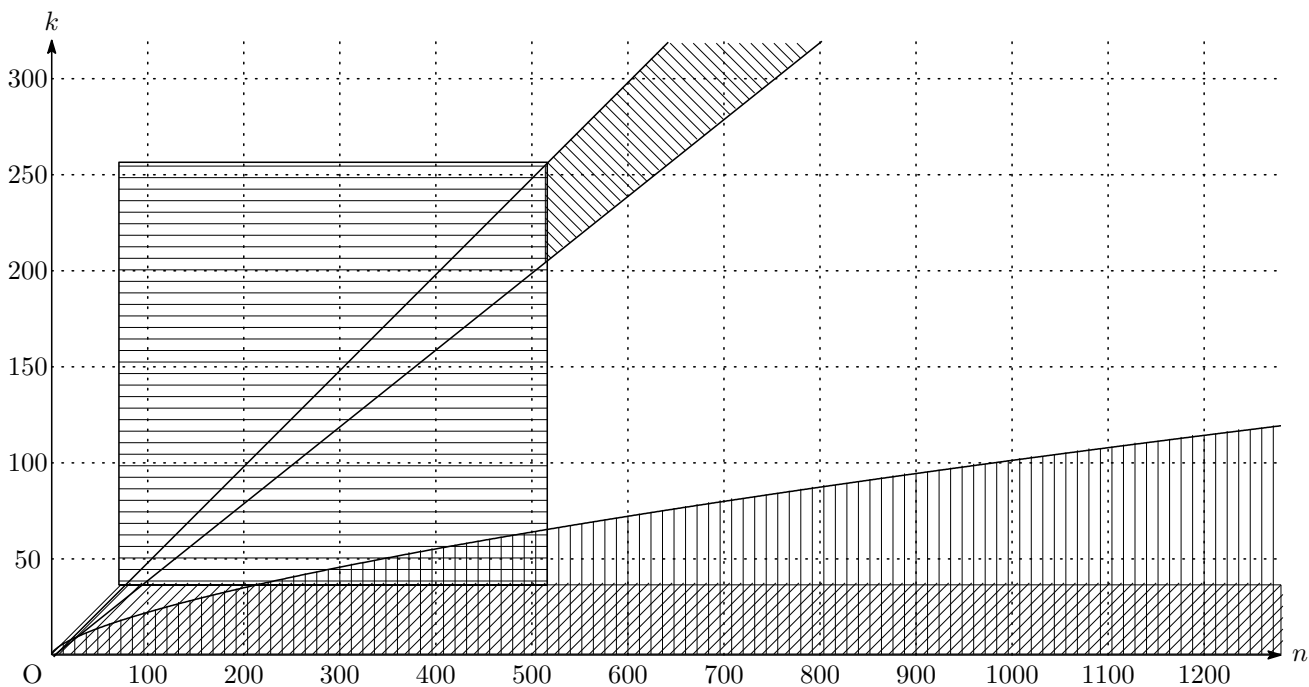
また $f(512) = \frac{2 \times 512}{15} \log 2 - 32\sqrt{2} \log 2 - 9 \log 2 + \log 2 > (68 - 46 - 9 + 1) \log 2 > 0$ であるから $x \geq 512$ なら $f(x) > 0$ といえる. 従って $n < 512$ でなければならない.

$38 < k, n < 512$ に反例が存在しないことは次の素数列からわかる. (2章 §5 の数列には合成数も含まれていたの
で, その数列の中に k' より大きな数が含まれていたとしても k' より大きな素因数の存在の証拠にはならなかった
のだが, 今回は素数列だからもっと強い結論が得られるのである.)

- 41, 79, 113, 151, 181, 211, 241, 277, 313, 349, 383, 421, 457, 491, 523

以上により定理は証明された. □

現状を図示しておこう. 斜線部の (n, k) が反例の存在しないと確定した領域である.



§ 7 残った場合

残っているのは $\frac{5}{2}k \leq n < k^{\frac{3}{2}}$ の場合である. Erdős はこれを $\frac{5}{2}k \leq n < 4k$ と $4k \leq n < k^{\frac{3}{2}}$ の2つに分割して扱っているが, 分割しないとどうなるかやってみよう.

先程の $2k \leq n < \frac{5}{2}k$ の場合でも今回の場合でも, 証明の元となる不等式は定理 2.21 の ${}_nC_k \leq 4^{k+\sqrt{n}}$ である. ただこのままだと何の結果も得られないので, $2k \leq n < \frac{5}{2}k$ の場合は $4^{k+\sqrt{n}}$ の k を $\frac{n}{3}$ に置き換えて $\frac{4^k}{k} < {}_nC_k \leq 4^{\frac{n}{3}+\sqrt{n}}$ の評価を得た, 今回は右辺の評価を厳しくすることは難しいが, 代わりに左辺の $\frac{4^k}{k}$ を厳しくすることが出来る. それは以下の通り.

$$\frac{5k}{2} \leq n \text{ より}$$

$$\begin{aligned} {}_nC_k &= \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} = \frac{2k(2k-1)\cdots(k+1)}{k(k-1)\cdots 1} \times \frac{n(n-1)\cdots(n-k+1)}{2k(2k-1)\cdots(k+1)} \\ &> 2kC_k \times \left(\frac{n}{2k}\right)^k > \frac{4^k}{k} \times \left(\frac{n}{2k}\right)^k \geq \frac{4^k}{k} \times \left(\frac{5}{4}\right)^k \\ &= \frac{5^k}{k} \end{aligned}$$

これを ${}_nC_k \leq 4^{k+\sqrt{n}}$ に代入する. $\frac{5}{2}k \leq n < k^{\frac{3}{2}} \left(\iff n^{\frac{2}{3}} < k \leq \frac{2n}{5} \right)$ にも注意して

$$\begin{aligned} & \frac{5^k}{k} < 4^{k+\sqrt{n}} \\ \iff & \left(\frac{5}{4}\right)^k < k \cdot 4^{\sqrt{n}} \\ \iff & k \log \frac{5}{4} < \log k + \sqrt{n} \log 4 \\ \implies & n^{\frac{2}{3}} \log \frac{5}{4} < \log \frac{2n}{5} + 2\sqrt{n} \log 2 \end{aligned}$$

数値計算するとこの不等式から $n \leq 67955$ が得られるのだが, これではやはり大きすぎるのである. 区間を分割するとどうなるかやってみよう.

命題 2.23 $\frac{5}{2}k \leq n < 4k \left(\iff \frac{n}{4} < k \leq \frac{2}{5}n \right)$ には Sylvester-Schur の定理の反例はない.

証明 上で述べた議論とまったく同様に $\frac{5^k}{k} < {}_nC_k \leq 4^{k+\sqrt{n}}$ が成り立っている. 今の場合は

$$\begin{aligned} & \frac{5^k}{k} < 4^{k+\sqrt{n}} \\ \iff & \left(\frac{5}{4}\right)^k < k \cdot 4^{\sqrt{n}} \\ \iff & k \log \frac{5}{4} < \log k + \sqrt{n} \log 4 \\ \implies & \frac{n}{4} \log \frac{5}{4} < \log \frac{2n}{5} + 2\sqrt{n} \log 2 \end{aligned}$$

$f(x) = \frac{x}{4} \log \frac{5}{4} - 2\sqrt{x} \log 2 - \log \frac{2x}{5}$ と置く. $f'(x) = \frac{1}{4} \log \frac{5}{4} - \frac{1}{\sqrt{x}} \log 2 - \frac{1}{x}$ である.

$$\begin{aligned} f'(2^{10}) &= \frac{1}{4} \log \frac{5}{4} - \frac{1}{32} \log 2 - \frac{1}{1024} = \frac{1}{32} \log \frac{5^8}{2^{17}} - \frac{1}{1024} \\ &> \frac{1}{32} \log 2.9 - \frac{1}{1024} > 0 \end{aligned}$$

であり, $f'(x)$ は明らかに単調増加だから $x > 2^{10}$ において $f'(x) > 0$, つまり $f(x)$ が単調増加である. また

$$\begin{aligned} f(2^{10}) &= 2^8 \log \frac{5}{4} - 2^6 \log 2 - \log \frac{2^{11}}{5} \\ &= 256 \log 5 - 512 \log 2 - 64 \log 2 - 11 \log 2 + \log 5 \\ &= 257 \log 5 - 587 \log 2 \\ &> 257 \times 1.60 - 587 \times 0.70 = 411.2 - 410.9 = 0.3 > 0 \end{aligned}$$

だから $x \geq 2^{10}$ においては $f(x) > 0$ である. 今の場合は $f(n) < 0$ より $n < 2^{10}$ が必要となる.

この範囲に反例がないことは定理 2.22 の素数列をさらに続けてやればよい.

- 41, 79, 113, 151, 181, 211, 241, 277, 313, 349, 383, 421, 457, 491, 523, 557, 593, 631, 661, 691, 727, 761, 797, 829, 863, 887, 919, 953, 991, 1021, 1051

以上により命題は証明された。 □

次の命題で最後に残った領域を片づけよう。

命題 2.24 $4k \leq n < k^{\frac{3}{2}}$ ($\iff n^{\frac{2}{3}} < k \leq \frac{n}{4}$) には Sylvester-Schur の定理の反例はない。

証明 この場合は ${}_nC_k \leq 4^{k+\sqrt{n}}$ における ${}_nC_k$ の評価を厳しく出来る。 $4k \leq n$ より

$$\begin{aligned} {}_nC_k &= \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} = \frac{2k(2k-1)\cdots(k+1)}{k(k-1)\cdots 1} \times \frac{n(n-1)\cdots(n-k+1)}{2k(2k-1)\cdots(k+1)} \\ &> {}_{2k}C_k \times \left(\frac{n}{2k}\right)^k > \frac{4^k}{k} \times \left(\frac{n}{2k}\right)^k \geq \frac{4^k}{k} \times 2^k \\ &= \frac{8^k}{k} \end{aligned}$$

これを ${}_nC_k \leq 4^{k+\sqrt{n}}$ に代入する。 $4k \leq n < k^{\frac{3}{2}}$ ($\iff n^{\frac{2}{3}} < k \leq \frac{n}{4}$) にも注意して

$$\begin{aligned} \frac{8^k}{k} &< 4^{k+\sqrt{n}} \\ \iff 2^k &< k \cdot 4^{\sqrt{n}} \\ \iff k \log 2 &< \log k + \sqrt{n} \log 4 \\ \implies n^{\frac{2}{3}} \log 2 &< \log \frac{n}{4} + 2\sqrt{n} \log 2 \end{aligned}$$

そこで $f(x) = x^{\frac{2}{3}} \log 2 - 2\sqrt{x} \log 2 - \log \frac{x}{4}$ と置くと

$$f'(x) = \frac{2}{3}x^{-\frac{1}{3}} \log 2 - \frac{1}{\sqrt{x}} \log 2 - \frac{1}{x} = \frac{1}{3}x^{-\frac{1}{3}} \left(2 \log 2 - 3x^{-\frac{1}{6}} \log 2 - 3x^{-\frac{2}{3}} \right)$$

$g(x) = 2 \log 2 - 3x^{-\frac{1}{6}} \log 2 - 3x^{-\frac{2}{3}}$ は単調増加であり、

$$g(2^6) = 2 \log 2 - \frac{3}{2} \log 2 - \frac{3}{2^4} = \frac{8 \log 2 - 3}{16} = \frac{4 \log 4 - 3}{16} > 0$$

であるから $x > 2^6$ において $f'(x) > 0$ つまり $f(x)$ は単調増加である。また

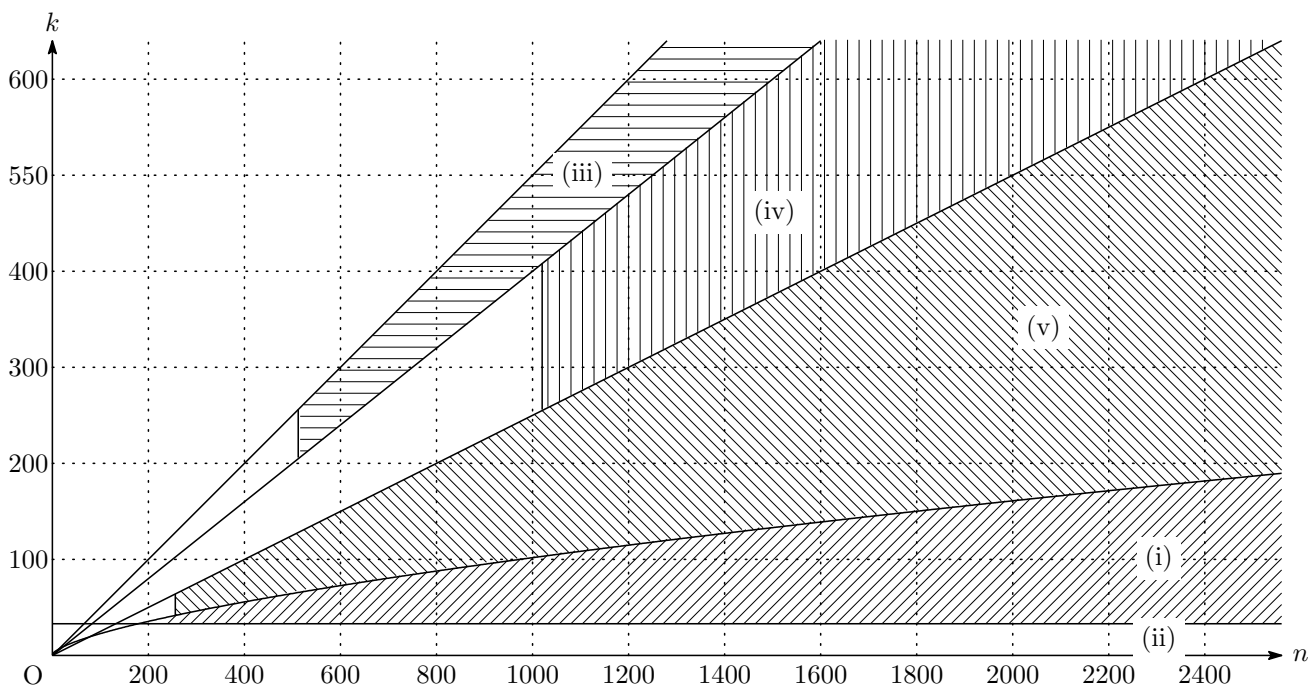
$$\begin{aligned} f(2^8) &= 2^{\frac{16}{3}} \log 2 - 2^5 \log 2 - \log 2^6 = (2^{\frac{16}{3}} - 2^5 - 6) \log 2 = \{2^5(2^{\frac{1}{3}} - 1) - 6\} \log 2 \\ &> \{2^5(1.25 - 1) - 6\} \log 2 > 0 \end{aligned}$$

だから $x \geq 2^8$ においては $f(x) > 0$ である。今の場合は $f(n) < 0$ より $n < 2^8$ が必要となるが、この範囲に反例がないことは定理 2.22 で証明済みである。以上により命題は証明された。 □

結論 Sylvester-Schur の定理は成立する。

§ 8 復習

(n, k) の各領域に対してどのような手法で証明したのかをまとめておく。



(i)~(v) の各領域は次のように証明したのであった. (iii)~(v) は $\frac{4^k}{k} \left(\frac{n}{2k}\right)^k < {}_n C_k < 4^{k+\sqrt{n}}$ がベースになっている.

- (i) $33 \leq k \leq n^{\frac{2}{3}}$ の場合. $\left(\frac{n}{k}\right)^k < {}_n C_k < n^{\pi(k)}$ により n の多項式として評価.
- (ii) $k \leq 33$ の場合. (i) と同様の評価. および直接証明.
- (iii) $2k \leq n < \frac{5}{2}k$ の場合. $\frac{4^k}{k} < {}_n C_k < 4^{\frac{n}{3}+\sqrt{n}}$ により評価.
- (iv) $\frac{5}{2}k \leq n < 4k$ の場合. $\frac{5^k}{k} < {}_n C_k < 4^{k+\sqrt{n}}$ により評価.
- (v) $4k \leq n < k^{\frac{3}{2}}$ の場合. $\frac{8^k}{k} < {}_n C_k < 4^{k+\sqrt{n}}$ により評価.

そうして残りの有限部分は直接実例により証明したのであった.

第 3 章

順列は平方数にならない

n を 1 以上の整数, k を 2 以上の整数として $A_k(n) = n(n+1)(n+2)\cdots(n+k+1)$ と定義する. この章の目標は次の定理を証明することである.

定理 3-1

$$A_k(n) = n(n+1)(n+2)\cdots(n+k-1) = y^2 \quad (3.1)$$

は自然数解を持たない. □

Erdős は右辺の y^2 を y^m ($m \geq 2$) にしても自然数解が存在しないことを証明している. ちなみに (3.1) の左辺を組み合わせ ${}_nC_k$ に変更したら解を持つようになる.

例えば ${}_nC_2 = y^2$ は $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(2n-1+2\sqrt{2}y) = 1$ と変形でき, 基本単数が $1+\sqrt{2}$ であることより

$$(n, y) = \left(\frac{(1+\sqrt{2})^{2m} + (1-\sqrt{2})^{2m} + 1}{2}, \frac{(1+\sqrt{2})^{2m} - (1-\sqrt{2})^{2m}}{8\sqrt{2}} \right)$$

という一般解を持つことがわかる. 最初の方は $(n, y) = (9, 6), (50, 35), (289, 204), (1682, 1189), \dots$ となっている. また (n, y) が解になっているとき, 「次の解」は $(3n+4y-1, 2n+3y-1)$ であることも容易にわかる.

また ${}_{50}C_3 = 140^2$ であるが, $k \geq 4$ のとき ${}_nC_k = y^m$ は整数解を持たないだろうというのは未解決なようだ. もっと一般に $k \geq 4$ のとき $\text{ord}_p({}_nC_k) = 1$ となる k より大きい素数 p が存在すると予想されているが, 証明はされていない.

§ 1 容易にわかること

補題 3.1 $k \geq n$ のとき (3.1) は解を持たない.

証明 $k \geq n$ とする. Bertrand-Chebyshev の定理より

- $n+k+1$ が偶数の場合 $\frac{n+k-1}{2} < p < n+k-1$ を満たす素数 p が存在するが, $n - \frac{1}{2} \leq \frac{n+k-1}{2}$ よりこの p は $n \leq p \leq n+k-1$ を満たす.
- $n+k+1$ が奇数の場合 $\frac{n+k}{2} < p < n+k$ を満たす素数 p が存在するが, $n \leq \frac{n+k}{2}$ よりこの p は $n \leq p \leq n+k-1$ を満たす. ($n+k$ は偶数だから素数ではない.)

そして $2p > n+k-1$ よりこの p は $A_k(n)$ を一回だけ割るので, $A_k(n)$ は平方数にならない. □

補題 3.2 (3.1) が解を持てば $n > k^2$ である.

証明 解を持つ場合 $k < n$ だから Sylvester–Schur の定理より $A_k(n)$ は k より大きい素因数 p を持つ. $n, n+1, \dots, n+k-1$ の中に p の倍数は一つしかないので, その数は p で 2 回以上割れないといけない. その数を $n+i$ ($0 \leq i \leq k-1$) とすると, $n+i \geq p^2 \geq (k+1)^2$ が成り立つので $n \geq k^2 + 2k + 1 - i > k^2$ である. \square

$n+i$ ($0 \leq i \leq k-1$) を, 平方因子を持たない因数 a_i と平方因子 x_i^2 に分解する.

$$n+i = a_i x_i^2$$

$A_k(n) = n(n+1)\cdots(n+k-1) = (a_0 a_1 \cdots a_{k-1})(x_0 x_1 \cdots x_{k-1})^2$ であるが, $A_k(n)$ が平方数なのだから $a_0 a_1 \cdots a_{k-1}$ は平方数でなければならない.

補題 3.3 a_0, a_1, \dots, a_{k-1} はすべて異なる.

証明 $0 \leq i < j \leq k-1$ に対して $a_i = a_j$ だとする.

$$(n+j) - (n+i) = a_j x_j^2 - a_i x_i^2 = a_i (x_j^2 - x_i^2) = a_i (x_j + x_i)(x_j - x_i)$$

ところが 左辺 $= j - i < k - 1$, 右辺 $\geq a_i \cdot 2x_i \cdot 1 \geq a_i \sqrt{x_i} = \sqrt{n+i} \geq \sqrt{n} > k$ より矛盾する. \square

§2 $a_0 a_1 \cdots a_{n+k-1}$ の下からの評価

a_0, a_1, \dots, a_{k-1} はすべて異なる平方因子を持たない自然数である. 平方因子を持たない自然数を小さいものから並べた数列を $\{b_i\}$ とする. ($b_1 = 1, b_2 = 2, b_3 = 3, b_4 = 5, b_5 = 6, b_6 = 7, b_7 = 10, b_8 = 11, b_9 = 13, \dots$)

補題 3.4 $k \geq 7$ に対し $b_k > \frac{4}{3}k$ が成り立つ.

証明 $b_7 = 10 > \frac{4}{3} \times 7, b_8 = 11 > \frac{4}{3} \times 8, b_9 = 13 > \frac{4}{3} \times 9$ より $k = 7, 8, 9$ に対して成り立つ. また $\{b_k\}$ には 4 の倍数は含まれないから $k \geq 7$ に対し $b_{k+3} \geq b_k + 4 > \frac{4}{3}k + 4 = \frac{4}{3}(k+3)$ が成り立ち, 帰納法により証明が完了する. \square

補題 3.5 $k \geq 19$ に対し $b_1 \cdot b_2 \cdots b_k > \left(\frac{4}{3}\right)^k k!$ が成り立つ.

証明 $k = 19$ のとき

$$\begin{aligned} \text{左辺} &= 1 \cdot 2 \cdot 3 \cdot 5 \cdot 6 \cdot 7 \cdot 10 \cdot 11 \cdot 13 \cdot 14 \cdot 15 \cdot 17 \cdot 19 \cdot 21 \cdot 22 \cdot 23 \cdot 26 \cdot 28 \cdot 30 = 2.94 \times 10^{19}, \\ \text{右辺} &= \left(\frac{4}{3}\right)^{19} 19! = 2.88 \times 10^{19} \end{aligned}$$

より成り立つ. $k \geq 20$ の場合は

$$b_1 \cdot b_2 \cdots b_{k-1} \cdot b_k \geq \left(\frac{4}{3}\right)^{k-1} (k-1)! \cdot \frac{4}{3}k = \left(\frac{4}{3}\right)^k k!$$

なので, 帰納法により証明できた. \square

§ 3 $a_0 a_1 \cdots a_{n+k-1}$ の上からの評価

$\text{ord}_p(a_0 a_1 \cdots a_{n+k-1})$ は $n, n+1, \dots, n+k-1$ のうちの p の倍数の個数以下である. k が p の倍数でない場合には, 例えば $p, p+1, \dots, 2p$ の $p+1$ 個の自然数に p の倍数が 2 つあるように, p の倍数は最大で $\left\lfloor \frac{k}{p} \right\rfloor + 1$ 個存在するから

(i) $\frac{k}{p} = 2l$ つまり $p = \frac{k}{2l}$ の場合 $\text{ord}_p(a_0 a_1 \cdots a_{n+k-1}) \leq 2l = \left\lfloor \frac{k}{p} \right\rfloor$.

(ii) $2l < \frac{k}{p} < 2l+1$ つまり $\frac{k}{2l+1} < p < \frac{k}{2l}$ の場合 $\text{ord}_p(a_0 a_1 \cdots a_{n+k-1}) \leq 2l+1 = \left\lfloor \frac{k}{p} \right\rfloor + 1$ である

が, $a_0 a_1 \cdots a_{n+k-1}$ は平方数なので $\text{ord}_p(a_0 a_1 \cdots a_{n+k-1}) \leq 2l = \left\lfloor \frac{k}{p} \right\rfloor$ が成り立つ.

(iii) $\frac{k}{p} = 2l+1$ つまり $p = \frac{k}{2l+1}$ の場合 $\text{ord}_p(a_0 a_1 \cdots a_{n+k-1}) \leq 2l+1 = \left\lfloor \frac{k}{p} \right\rfloor$ であるが, $a_0 a_1 \cdots a_{n+k-1}$

は平方数なので $\text{ord}_p(a_0 a_1 \cdots a_{n+k-1}) \leq 2l = \left\lfloor \frac{k}{p} \right\rfloor - 1$ が成り立つ.

(iv) $2l+1 < \frac{k}{p} < 2l+2$ つまり $\frac{k}{2l+2} < p < \frac{k}{2l+1}$ の場合 $\text{ord}_p(a_0 a_1 \cdots a_{n+k-1}) \leq 2l+2 = \left\lfloor \frac{k}{p} \right\rfloor + 1$ である.

補題 3.6 次が成り立つ.

$$a_0 a_1 \cdots a_{k-1} \leq \prod_{p < k} p^{\left\lfloor \frac{k}{p} \right\rfloor} \prod_{k > p > \frac{1}{2}k} p \prod_{\frac{1}{3}k > p > \frac{1}{4}k} p \cdots$$

証明 上で述べたことより $\text{ord}_p(a_0 a_1 \cdots a_{n+k-1})$ が $\left\lfloor \frac{k}{p} \right\rfloor$ を超えている可能性のあるのは $\frac{k}{2l+2} < p < \frac{k}{2l+1}$ の場合で, その場合でも超えている回数は高々 1 回である. □

命題 3.7 $\prod_{k > p > \frac{1}{2}k} p \prod_{\frac{1}{3}k > p > \frac{1}{4}k} p \cdots$ は ${}_{k-1}C_{\left\lfloor \frac{k-1}{2} \right\rfloor}$ を割り切る.

証明 左辺の区間は重なっていないので, 各区間に入っている素数 p に対して $\text{ord}_p \left({}_{k-1}C_{\left\lfloor \frac{k-1}{2} \right\rfloor} \right)$ が 1 以上であることを示せばよい.

(i) $k = 2m$ の場合

$${}_{k-1}C_{\left\lfloor \frac{k-1}{2} \right\rfloor} = \frac{(2m-1)!}{(m-1)!m!} \text{ であり, } \text{ord}_p \left({}_{k-1}C_{\left\lfloor \frac{k-1}{2} \right\rfloor} \right) = \sum_{\nu=1}^{\infty} \left(\left\lfloor \frac{2m-1}{p^\nu} \right\rfloor - \left\lfloor \frac{m-1}{p^\nu} \right\rfloor - \left\lfloor \frac{m}{p^\nu} \right\rfloor \right) \text{ である.}$$

素数 p が $\frac{2m}{2l-1} > p > \frac{2m}{2l}$ を満たすとき

$$\begin{aligned} \frac{2m}{2l-1} > p > \frac{2m}{2l} &\iff (2l-1)p < 2m < 2lp \iff (2l-1)p \leq 2m-1 < 2lp-1 \\ \iff 2l-1 \leq \frac{2m-1}{p} < 2l - \frac{1}{p} &\implies \left\lfloor \frac{2m-1}{p} \right\rfloor = 2l-1 \end{aligned}$$

$$\begin{aligned} \frac{2m}{2l-1} > p > \frac{2m}{2l} &\iff l - \frac{1}{2} < \frac{m}{p} < l \iff l - \frac{1}{2} - \frac{1}{p} < \frac{m-1}{p} < l - \frac{1}{p} \\ \implies \left\lfloor \frac{m-1}{p} \right\rfloor = \left\lfloor \frac{m}{p} \right\rfloor &= l-1 \end{aligned}$$

$$\text{従って } \left[\frac{2m-1}{p} \right] - \left[\frac{m-1}{p} \right] - \left[\frac{m}{p} \right] = (2l-1) - (l-1) - (l-1) = 1$$

(ii) $k = 2m - 1$ の場合

$${}_{k-1}C_{\left[\frac{k-1}{2}\right]} = \frac{(2m-2)}{(m-1)!(m-1)!} \text{ であり, } \text{ord}_p \left({}_{k-1}C_{\left[\frac{k-1}{2}\right]} \right) = \sum_{\nu=1}^{\infty} \left(\left[\frac{2m-2}{p^\nu} \right] - \left[\frac{m-1}{p^\nu} \right] - \left[\frac{m-1}{p^\nu} \right] \right)$$

である. 素数 p が $\frac{2m-1}{2l-1} > p > \frac{2m-1}{2l}$ を満たすとき

$$\begin{aligned} \frac{2m-1}{2l-1} > p > \frac{2m-1}{2l} &\iff (2l-1)p < 2m-1 < 2lp \iff (2l-1)p \leq 2m-2 < 2lp-1 \\ \iff 2l-1 \leq \frac{2m-2}{p} < 2l - \frac{1}{p} &\implies \left[\frac{2m-2}{p} \right] = 2l-1 \end{aligned}$$

$$\begin{aligned} \frac{2m-1}{2l-1} > p > \frac{2m-1}{2l} &\iff (2l-1)p < 2m-1 < 2lp \iff (2l-1)p \leq 2m-2 < 2lp-1 \\ \iff 2l-1 \leq \frac{2m-2}{p} < 2l - \frac{1}{p} &\iff l - \frac{1}{2} \leq \frac{m-1}{p} < l - \frac{1}{2p} \implies \left[\frac{m-1}{p} \right] = l-1 \end{aligned}$$

$$\text{従って } \left[\frac{2m-2}{p} \right] - \left[\frac{m-1}{p} \right] - \left[\frac{m-1}{p} \right] = (2l-1) - (l-1) - (l-1) = 1$$

(i)(ii) より証明できた. □

系 3.8

$$a_0 a_1 \cdots a_{k-1} \leq {}_{k-1}C_{\left[\frac{k-1}{2}\right]} \prod_{p < k} p^{\left[\frac{k}{p}\right]}$$

□

命題 3.9

$$a_0 a_1 \cdots a_{k-1} \leq 2^{k-2} \prod_{p < k} p^{\left[\frac{k}{p}\right]}$$

証明 自然数 n に対して ${}_n C_{\left[\frac{n}{2}\right]} \leq 2^{n-1}$ が示されればよい.

(i) $n = 1, 2$ の場合明らかになり立つ.

(ii) $n = 2m + 1 (\geq 3)$ の場合, $2m - 1$ まで成り立っているとして

$$\begin{aligned} {}_n C_{\left[\frac{n}{2}\right]} &= {}_{2m+1} C_m = \frac{(2m+1)!}{(m+1)!m!} = \frac{2m+1}{m+1} \times \frac{2m}{m} \times \frac{(2m-1)!}{m!(m-1)!} \\ &\leq 4 \cdot {}_{n-2} C_{\left[\frac{n-2}{2}\right]} \leq 4 \cdot 2^{n-3} = 2^{n-1} \end{aligned}$$

(iii) $n = 2m + 2 (\geq 4)$ の場合, $2m$ まで成り立っているとして

$$\begin{aligned} {}_n C_{\left[\frac{n}{2}\right]} &= {}_{2m+2} C_{m+1} = \frac{(2m+2)!}{(m+1)!(m+1)!} = \frac{2m+2}{m+1} \times \frac{2m+1}{m+1} \times \frac{(2m)!}{m!m!} \\ &\leq 4 \cdot {}_{n-2} C_{\left[\frac{n-2}{2}\right]} \leq 4 \cdot 2^{n-3} = 2^{n-1} \end{aligned}$$

以上により命題は証明された. □

§ 4 矛盾を導く

前節までで $k \geq 19$ に対し $n(n+1)\cdots(n+k-1)$ が平方数であれば (そのとき $n > k^2$ も成立しているが)

$$\left(\frac{4}{3}\right)^k k! \leq 2^{k-2} \prod_{p < k} p^{\left[\frac{k}{p}\right]} \tag{3.2}$$

が成立するという結論が得られた. これが大きな k に対しては不可能であることを示そう.

$k! = \prod_{p < k} p^{\left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \cdots}$ であるが, これを $k! \geq \prod_{p < k} p^{\left[\frac{k}{p}\right]}$ と評価したのでは先の不等式が $\left(\frac{4}{3}\right)^k \leq 2^{k-2}$ という

自明なものになってしまっても何も得られない. $p = 2, 3$ のところだけ第2項まで取って $\left(\frac{4}{3}\right)^k \times 2^{\left[\frac{k}{2^2}\right]} \times 3^{\left[\frac{k}{3^2}\right]} \leq 2^{k-2}$ にしても有効な評価は得られない.

$$\left(\frac{4}{3}\right)^k \times 2^{\left[\frac{k}{2^2}\right] + \left[\frac{k}{2^3}\right]} \times 3^{\left[\frac{k}{3^2}\right] + \left[\frac{k}{3^3}\right]} \leq 2^{k-2}$$

にしておけば $k \geq 80$ のときに成立しないことが数値的に確認出来る. Erdős では次のように評価している.

定理 3.10 次が成り立つ.

$$p^{\text{ord}_p k!} > \frac{1}{kp} p^{\frac{k}{p-1}}$$

証明 $k = c_0 p^s + c_1 p^{s-1} + \cdots + c_s$ ($0 \leq c_i \leq p-1$) のように p 進数表示されたとすると,

$$\begin{aligned} & \text{ord}_p k! \\ &= \left[\frac{k}{p} \right] + \left[\frac{k}{p^2} \right] + \cdots \\ &= (c_0 p^{s-1} + c_1 p^{s-2} + \cdots + c_{s-1}) + (c_0 p^{s-2} + c_1 p^{s-3} + \cdots + c_{s-2}) + \cdots + c_0 \\ &= c_0 (p^{s-1} + p^{s-2} + \cdots + 1) + c_1 (p^{s-2} + p^{s-3} + \cdots + 1) + \cdots + c_{s-1} \\ &= c_0 \cdot \frac{p^s - 1}{p - 1} + c_1 \cdot \frac{p^{s-1} - 1}{p - 1} + \cdots + c_{s-1} \cdot \frac{p - 1}{p - 1} + c_s \cdot \frac{1 - 1}{p - 1} \\ &= \frac{(c_0 p^s + c_1 p^{s-1} + \cdots + c_s) - (c_0 + c_1 + \cdots + c_s)}{p - 1} \\ &\geq \frac{k - (s + 1)(p - 1)}{p - 1} \\ &= \frac{k}{p - 1} - (s + 1) \end{aligned}$$

従って $p^{\text{ord}_p k!} \geq p^{\frac{k}{p-1} - (s+1)} = \frac{p^{\frac{k}{p-1}}}{p^{s+1}} \geq \frac{1}{kp} p^{\frac{k}{p-1}}$ □

この評価はかなりよい. 例えば $k = 100, p = 2$ の場合, 左辺 $= 2^{97}$, 右辺 $= \frac{2^{100}}{200}$ である. また $k = 100, p = 3$ の場合, 左辺 $= 3^{48}$, 右辺 $= \frac{3^{50}}{300}$ である.

定理 3.10 を $p = 2, 3$ の場合にだけ適用し, $3 < p < k$ の p に対しては $\text{ord}_p k! \geq \left\lfloor \frac{k}{p} \right\rfloor$ という自明な関係を使うと $k! \geq \frac{2^k}{2k} \cdot \frac{3^{\frac{k}{2}}}{3k} \prod_{3 < p < k} p^{\lfloor \frac{k}{p} \rfloor}$ が得られる. これを (3.2) に代入すると

$$\begin{aligned} & 2^{k-2} \prod_{p < k} p^{\lfloor \frac{k}{p} \rfloor} \geq \left(\frac{4}{3}\right)^k k! \\ \implies & 2^{k-2} \prod_{p < k} p^{\lfloor \frac{k}{p} \rfloor} \geq \left(\frac{4}{3}\right)^k \cdot \frac{2^k}{2k} \cdot \frac{3^{\frac{k}{2}}}{3k} \prod_{3 < p < k} p^{\lfloor \frac{k}{p} \rfloor} \\ \iff & 2^{k-2} \cdot 2^{\lfloor \frac{k}{2} \rfloor} \cdot 3^{\lfloor \frac{k}{3} \rfloor} \geq \left(\frac{4}{3}\right)^k \cdot \frac{2^k}{2k} \cdot \frac{3^{\frac{k}{2}}}{3k} \\ \implies & \left(\frac{3}{2}\right)^6 k^{12} \geq \left(\frac{2^9}{3^5}\right)^k \\ \implies & \left(\frac{3}{2}\right)^6 k^{12} \geq 2^k \end{aligned}$$

この最後の不等式は $k \geq 100$ だと成立しないことが容易にわかる. (実際には $k \geq 80$ で成立しない.)

以上により $n(n+1)\cdots(n+k-1)$ は $k \geq 100$ の場合平方数にならないことが証明された.

§ 5 残った場合

$k < 202$ の場合に (3.1) が解を持たないことは, 成美清松さんが 1917 年に証明している. ここではその証明を, これまでの記述に合うような形で (表記法は大幅に変更して) 述べてみたい. (有限の未解決部分を消去するだけだから, 原論文の一般性を多少犠牲にしているところもある.)

証明の方針はやはり, 解があったとすると補題 3.3 の「 a_0, a_1, \dots, a_{k-1} はすべて異なる」という部分が矛盾するというものである. k が大きい場合の Erdős の証明は, a_0, a_1, \dots, a_{k-1} がすべて異なると $a_0 a_1 \cdots a_{k-1}$ が大きくなりすぎるというものであったが, 今回は各 i ごとに $a_i = \prod_{p < k} p^{\nu_{p,i}}$ と表したときに k 個の $\{(\nu_{2,i}, \nu_{3,i}, \nu_{4,i}, \dots)\}$

がすべて異なることは出来ないというものである.

ただし本当に k が小さい場合を直接証明しておかないといけない. まずそれを片付けておこう.

定理 3.11 $k = 2$ の場合 $n(n+1) = y^2$ は自然数解を持たない.

証明 $n, n+1$ は互いに素であるからそれぞれが平方数でなければならない. これは $(n, n+1) = (0, 1)$ しかあり得ない. □

定理 3.12 $k = 3$ の場合 $n(n+1)(n+2) = y^2$ は自然数解を持たない.

証明 今までのように $n+i = a_i x_i^2$ ($i = 0, 1, 2$) と, 平方因子 x_i^2 と平方因子を持たない因子 a_i に分解する. 補題 3.3 より a_0, a_1, a_2 はすべて異ならないといけませんが, 今の場合 a_i は 1 か 2 でしかあり得ないのでこれは不可能である. □

定理 3.13 $k = 4$ の場合 $n(n+1)(n+2)(n+3) = y^2$ は自然数解を持たない.

証明 これは代数的に解く.

$$\begin{aligned} n(n+1)(n+2)(n+3) &= y^2 \\ \iff (n^2+3n)(n^2+3n+2) &= y^2 \\ \iff (n^2+3n+1)^2 - 1 &= y^2 \\ \iff (n^2+3n+1+y)(n^2+3n+1-y) &= 1 \end{aligned}$$

この式は $(n^2+3n+1+y, n^2+3n+1-y) = (\pm 1, \pm 1)$ を意味するので, $y = 0$ になってしまう. □

定理 3.14 $k = 5$ の場合 $n(n+1)(n+2)(n+3)(n+4) = y^2$ は自然数解を持たない.

証明 a_i は k 未満の素因数しか持たないので $a_i = 2^{\nu_{2,i}} \cdot 3^{\nu_{3,i}}$ ($i = 0, 1, 2, 3, 4$) と表される. ここで各 $\nu_{p,i}$ は 0 か 1 のいずれかの値を取る. しかしその場合可能な数は $2^0 3^0, 2^0 3^1, 2^1 3^0, 2^1 3^1$ の 4 通りしかないので, $\{a_i\}$ のうちに等しいものが存在することになる. □

定理 3.15 $k = 6$ の場合 $n(n+1)(n+2)(n+3)(n+4)(n+5) = y^2$ は自然数解を持たない.

証明 a_i は k 未満の素因数しか持たないので $a_i = 2^{\nu_{2,i}} \cdot 3^{\nu_{3,i}} \cdot 5^{\nu_{5,i}}$ ($i = 0, 1, 2, 3, 4$) と表される. すべての $\nu_{5,i}$ が 0 の場合は $\{a_i\}$ は 4 通りしか可能性がなく必ず重複している. $\nu_{5,i}$ のなかに 1 が含まれる場合, $\nu_{5,0} = \nu_{5,5} = 1$ しかあり得ず, その場合 $\nu_{5,1} = \nu_{5,2} = \nu_{5,3} = \nu_{5,4} = 0$ である. その上で a_1, a_2, a_3, a_4 が異なっているとすれば, 全体として $\{a_1, a_2, a_3, a_4\} = \{2^0 3^0, 2^0 3^1, 2^1 3^0, 2^1 3^1\}$ のはずであるが, その場合

$$(n+1)(n+2)(n+3)(n+4) = a_1 a_2 a_3 a_4 x_1^2 x_2^2 x_3^2 x_4^2 = 2^2 3^2 x_1^2 x_2^2 x_3^2 x_4^2$$

ということになる. これは定理 3.13 に矛盾する. □

定理 3.16 $k = 7$ の場合 $n(n+1)(n+2)(n+3)(n+4)(n+5)(n+6) = y^2$ は自然数解を持たない.

証明 定理 3.15 に準ずる. □

定理 3.17 $k = 8$ の場合 $n(n+1)(n+2)(n+3)(n+4)(n+5)(n+6)(n+7) = y^2$ は自然数解を持たない.

証明 a_i のうち, 7 も 5 も因数に持たないものが連続で 4 つ存在することが容易にわかる. その 4 つに同じものがない場合は定理 3.15 と同様矛盾が導ける. □

この調子で $k = 100$ まで示すのは気が遠くなる作業であるが, そこはうまく処理できるのである. 例えば $k = 100$ の場合は次のようにする.

a_0, a_1, \dots, a_{99} は 100 未満の素因数しか持たないので

$$a_i = \prod_{p \leq 99} p^{\nu_{p,i}} = 2^{\nu_{2,i}} \cdot 3^{\nu_{3,i}} \cdot 5^{\nu_{5,i}} \cdot 7^{\nu_{7,i}} \cdot \dots \cdot 97^{\nu_{97,i}}$$

と表される. 各 $\nu_{p,i}$ は 0 または 1 である.

これら 100 個の a_i のうち, $\nu_{97,i} = 1$ であるものは高々 2 個しか存在しない. それは 97 に限らず $100 - 1$ をちょうど 1 回割る素数, つまり $100 - 1 \geq p > \frac{100 - 1}{2}$ を満たす素数 p に関してはそうである, 今の場合は $p = 97, 89, 83, 79, 73, 71, 67, 61, 59, 53$ の 10 個の素数ということになる.

$100-1$ をちょうど2回割る素数, つまり $\frac{100-1}{2} \geq p > \frac{100-1}{3}$ を満たす $p = 47, 43, 41, 37$ の4個の素数は3つの a_i に登場する可能性があるが, $\prod a_i$ は平方数でなければならないので, やはりこれらも高々2回しか登場しない.

同様に考えて

$$\begin{aligned} \frac{100-1}{3} \geq p > \frac{100-1}{5} & \text{ を満たす } p = 31, 29, 23 \text{ の3個の素数は高々4回,} \\ \frac{100-1}{5} \geq p > \frac{100-1}{7} & \text{ を満たす } p = 19, 17 \text{ の2個の素数は高々6回,} \\ \frac{100-1}{7} \geq p > \frac{100-1}{9} & \text{ を満たす } p = 13 \text{ の1個の素数は高々8回,} \\ \frac{100-1}{9} \geq p > \frac{100-1}{11} & \text{ を満たす } p = 11 \text{ の1個の素数は高々10回,} \\ \left(\frac{100-1}{11} \geq p > \frac{100-1}{13} \right. & \text{ を満たす素数はない)} \\ \frac{100-1}{13} \geq p > \frac{100-1}{15} & \text{ を満たす } p = 7 \text{ の1個の素数は高々14回} \end{aligned}$$

登場する.

仮にこれら延べ $14 \times 2 + 3 \times 4 + 2 \times 6 + 1 \times 8 + 1 \times 10 + 0 \times 12 + 1 \times 14 = 84$ 個がまったく重複なく $a_0 \sim a_{99}$ の中に登場したとしても, 少なくとも残り16個は7以上の素因子を持たない. つまり $a_i = 2^{\nu_2, i} \cdot 3^{\nu_3, i} \cdot 5^{\nu_5, i}$ の形をしている. しかしこのような数は $2^3 = 8$ 通りしか存在しないので, すべてを異ならせることは不可能である.

これを他の k に対しても実行してみよう.

補題 3.18 k 未満の素数 p が a_0, a_1, \dots, a_{k-1} に現れる回数は高々 $2 \left\lfloor \frac{k-1+p}{2p} \right\rfloor$ である.

証明 素数 p が $\frac{k-1}{2l-1} \geq p > \frac{k-1}{2l+1}$ を満たす場合, p は $k-1$ を $2l-1$ 回以上 $2l+1$ 回未満割り切るので $0, 1, 2, \dots, k-1$ の中に p の倍数は $2l+2$ 個未満存在する. 従って p が a_0, a_1, \dots, a_{k-1} に登場する回数も $2l+2$ 回未満であるが, 登場回数は偶数でなければいけないので $2l$ 回以下ということになる. そして

$$\begin{aligned} \frac{k-1}{2l-1} \geq p > \frac{k-1}{2l+1} \\ \iff \frac{k-1}{p} \geq 2l-1 \text{ かつ } 2l+1 > \frac{k-1}{p} \\ \iff \frac{k-1}{2p} + \frac{1}{2} \geq l > \frac{k-1}{2p} - \frac{1}{2} \\ \iff l = \left\lfloor \frac{k-1}{2p} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{k-1+p}{2p} \right\rfloor \end{aligned}$$

以上により証明された. □

定義 3.19

(1) 7より大きい自然数 k に対し, $H_7(k) = \sum_{7 \leq p < k} 2 \left[\frac{k-1+p}{2p} \right]$ と定義する. 上の補題より a_0, a_1, \dots, a_{k-1}

のうち 2, 3, 5 以外の素因数を持つものは高々 $H_7(k)$ 個である.

(2) 5より大きい自然数 k に対し, $H_5(k) = \sum_{5 \leq p < k} 2 \left[\frac{k-1+p}{2p} \right]$ と定義する. 上の補題より a_0, a_1, \dots, a_{k-1}

のうち 2, 3 以外の素因数を持つものは高々 $H_5(k)$ 個である.

□

$7 \leq k \leq 100$ に対して $H_7(k)$, $k - H_7(k)$, $H_5(k)$, $k - H_5(k)$ を計算すると次頁の表 3.1 のようになる.

この表で $k - H_7(k) > 8$ であるような k に関しては (3.1) は自然数解を持たない. また $k - H_5(k) > 5$ であるような k に関しても (3.1) は自然数解を持たない. 従って $9 \leq k \leq 100$ に関しては (3.1) は自然数解を持たないことになるが, §4 までで $k > 100$ に関しては解を持たないことを示しており, $2 \leq k \leq 8$ に関してはこの節の前半で直接証明しているので, すべての $k \geq 2$ に関して解を持たないことが証明できた,

表 3.1: $7 \leq k \leq 100$ に対する $H_7(k)$, $H_5(k)$

k	$H_7(k)$	$k - H_7(k)$	$H_5(k)$	$k - H_5(k)$	k	$H_7(k)$	$k - H_7(k)$	$H_5(k)$	$k - H_5(k)$
7	0	7	2	5	54	38	16	48	6
8	2	6	4	4	55	38	17	48	7
9	2	7	4	5	56	40	16	52	4
10	2	8	4	6	57	40	17	52	5
11	2	9	4	7	58	42	16	54	4
12	4	8	6	6	59	42	17	54	5
13	4	9	6	7	60	44	16	56	4
14	6	8	8	6	61	44	17	56	5
15	6	9	8	7	62	46	16	58	4
16	6	10	10	6	63	46	17	58	5
17	6	11	10	7	64	48	16	60	4
18	8	10	12	6	65	48	17	60	5
19	8	11	12	7	66	50	16	64	2
20	10	10	14	6	67	50	17	64	3
21	10	11	14	7	68	52	16	66	2
22	12	10	16	6	69	52	17	66	3
23	12	11	16	7	70	54	16	68	2
24	14	10	18	6	71	54	17	68	3
25	14	11	18	7	72	56	16	70	2
26	14	12	20	6	73	56	17	70	3
27	14	13	20	7	74	58	16	72	2
28	14	14	20	8	75	58	17	72	3
29	14	15	20	9	76	58	18	74	2
30	16	14	22	8	77	58	19	74	3
31	16	15	22	9	78	62	16	78	0
32	18	14	24	8	79	62	17	78	1
33	18	15	24	9	80	64	16	80	0
34	20	14	26	8	81	64	17	80	1
35	20	15	26	9	82	64	18	80	2
36	22	14	30	6	83	64	19	80	3
37	22	15	30	7	84	66	18	82	2
38	24	14	32	6	85	66	19	82	3
39	24	15	32	7	86	68	18	86	0
40	26	14	34	6	87	68	19	86	1
41	26	15	34	7	88	70	18	88	0
42	28	14	36	6	89	70	19	88	1
43	28	15	36	7	90	72	18	90	0
44	30	14	38	6	91	72	19	90	1
45	30	15	38	7	92	76	16	94	-2
46	30	16	40	6	93	76	17	94	-1
47	30	17	40	7	94	78	16	96	-2
48	32	16	42	6	95	78	17	96	-1
49	32	17	42	7	96	80	16	100	-4
50	34	16	44	6	97	80	17	100	-3
51	34	17	44	7	98	82	16	102	-4
52	36	16	46	6	99	82	17	102	-3
53	36	17	46	7	100	84	16	104	-4

参考文献

- [1] M. アイグナー, G.M. ツィーグラー, 「天書の証明」, シュプリンガー・フェアラーク東京 (2002)
- [2] P.Erdős, "Beweis eines Satzes von Tschebyschef", Acta Litt. Sci. Szeged 5 (1932), 194-198
https://www.renyi.hu/~p_erdos/1932-01.pdf
- [3] P.Erdős, "A Theorem of Sylvester and Shur", London Math.Soc., vol 9(1934), pp282-288
https://www.renyi.hu/~p_erdos/1934-01.pdf
- [4] P.Erdős, "Notes on the product of consecutive integers", London Math.Soc., vol 14(1939), pp194-198
https://www.renyi.hu/~p_erdos/1939-03.pdf
- [5] 一松信 「 n と $2n$ の間に素数がある」, 数研通信 70 号 (2011 年 5 月)
http://www.chart.co.jp/subject/sugaku/suken_tsushin/70/70-1.pdf
- [6] 風あざみ, 「Sylvester-Shur の定理について」, 2016/10/14
<http://puit578.web.fc2.com/sylvester.pdf>
- [7] 亀井真人 「素数定理と明示公式」 p.30-47
http://www1.kcn.ne.jp/~mkamei/math/201519_zeta.pdf
- [8] Seimatsu Narumi, "An Extension of a Theorem of Liouville's", Tohoku Math. Journal, 11(1917), 128-142
https://www.jstage.jst.go.jp/article/tmj1911/11/0/11_0_128/_pdf