社会人講座における素数定理の取扱いについて

梅 垣 敦 紀

本稿は，著者が 2014 年 9 月から 2015 年 3 月まで中日文化センターで開かれた「数学の世界に触れてみよう—体験を通して知る数学の歴史と理論—」という社会人講座の中で行ったルジャンドルが定式化した素数定理の紹介を再構成し，加筆したものである．

キーワード：素数定理，ルジャンドル，社会人講座，素数関数，対数

1 導入

本稿は，著者が 2014 年 9 月から 2015 年 3 月まで中日文化センターで行った「数学の世界に触れてみよう—体験を通して知る数学の歴史と理論—」という社会人講座の中で行った数値実験と数学理論の解説を振り返りつつ，再構成し加筆したものである．昨今の計算機の性能は凄まじく高くなっており，計算機を使うことさえできれば誰でも，前世紀までの数学者がかなりの年月をかけないと得られなかったデータを，ほんの数分，悪くても数時間で得ることができる．よって，計算機実験をしながら，数学者が何を見て，何に気付き，何を考え，何を得たのかを追体験してもらうことがこの講座の目標であった．当然のことながら，著者が計算実験を見せるだけでなく，誰もが同じ実験ができるように留意したつもりである．その際，特別なコンピュータを用意しなくても，適切なソフトウェアをインストールすれば良く，また，必要なソフトウェアはすべてフリーウェアであることを前提としているので，費用はまったく掛からない．

講座は半年を掛け，

1. 数学実験で見つかる数理現象とは？
2. 確率と統計の世界
3. 関数１（微分と積分）
4. 関数２（三角関数・指数関数）
5. 素数１（整数と素数）
6. 素数２（素数のもつ不思議な性質）

という 6 回の枠で行ったが，その中から本稿では第 5 回に行った「素数１（整数と素数）」を取り上げる．特に，この回の主眼は「素数定理」を把握することにある．素数定理とは，「x 以下の素数の個数を表す素数関数 $\pi(x)$ が x を大きくするにつれてどのように振る舞うか」を決定する定理である．最初にこの素数定理を予見し定式化したのは，ルジャンドルであり，19 世紀初頭のことであった．その後，19 世紀末にアダマールやド・ラ・ヴァレ・プーサンによって解決を見た大問題である．社会人講座ではこの素数定理の解説の前に準備として 4 回の講座を行ったが，その 4 回の内容については詳細を伝える機会があればそのときに譲ることにして，次節でそこまでに得られている知識を簡単にまとめることにする．

2　仮定する知識と計算機環境

あくまでも社会人講座であるため，現在のカリキュラムでいう中学くらいまでの知識は仮定しているが，高校の内容については，特段仮定していない．また，事実の証明についても，可能な限り正確さを期すが，完全な証明ではないものも含まれることを最初に注意しておく．(そのようなものでも，なるべく，証明の方針は大筋で外れてはいないように心掛けた.）本稿では講座の前半の知識を仮定しているため，この回までに説明したものの中から必要な事実を以下にすべて列挙しておく．

まず，高校の数列の極限や微分・積分についての知識は第 3 回および第 4 回の講座で触れた内容なので，本稿では仮定して，以下の定義は既知のものとしておく．

定義 2.1. 等式

$$\int_1^e \frac{1}{x}dx = 1$$

を満たす実数 e を**ネイピア数**（【英】Napier number）という．

社会人講座ではネイピア数の近似値

$$e \fallingdotseq 2.71828\ldots$$

を計算機実験で具体的に評価するために，この定義を採用した．さらに，ネイピア数を用いて指数関数も定義し，その微分も求めた．

定義 2.2. 実数 $y \in \mathbf{R}$ が実数 $x \in \mathbf{R}$ を用いて $y = e^x$ と表されるとき，x を y の**指数**（【英】expornent）という．さらに，x を変数と見るとき e^x を**指数関数**（【英】expornential function）という．

注意 2.2.1. この指数関数を

$$\exp(x) = e^x$$

と書くことも多い．

命題 2.3. 指数関数 e^x の導関数は $(e^x)' = e^x$ である．

また，次の等比数列の和の公式も既知とする．

命題 2.4. 初項 a_1，公比 $r \neq 1$ の等比数列 $\{a_n\}$ について，第 n 項までの和

$$S_n = \sum_{k=1}^{n} a_k$$

は

$$S_n = a_1\frac{1-r^n}{1-r}$$

で与えられる．特に，$|r| < 1$ のとき，n を無限大にしたときの極限は収束し，

$$\lim_{n\to\infty} S_n = \sum_{n=1}^{\infty} a_n = \frac{a_1}{1-r}$$

となる．

自然数に対する無限和について，次の 2 つの事実も認めるものとする．

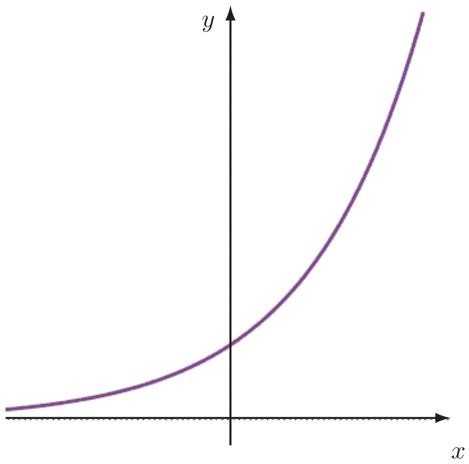
定理 2.5. $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n} = \infty$ が成り立つ．

定理 2.6. $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$ が成り立つ．

さらに，以下の計算実験では，OS が Windows 8.1 のコンピュータに，グラフ作画ツール gnuplot (version 5.0 patchlevel 1)（[PLOT] 参照）と計算ツール PARI/GP (version 2.7.4)（[PARI] 参照）を標準的にインストールした環境で行っているが，これより古い環境でも支障なく動く筈である．また，gunplot も PARI/GP も前述の通りフリーウェアであって，なおかつ，Windows 環境でなくても容易にインストールできる筈である．

3　対数関数

指数関数 e^x を用いて，新しい関数を作ることを試みる．指数関数 $y = e^x = \exp(x)$ のグラフを描いてみると，



といった形状になる．このグラフを見ると，$y > 0$ を満たすどんな実数 $y \in \mathbf{R}_{>0}$ についても，ネイピア数 e を用いて $y = e^x$ となるような実数 $x \in \mathbf{R}$ が唯 1 つ存在することが視覚的にもわかる．より数学的に言えば，

$$\exp : \mathbf{R} \longrightarrow \mathbf{R}_{>0}, \qquad x \mapsto e^x$$

は全単射である．この x に注目して，x と y の立場を入れ換えて，以下のように定義する．

定義 3.1. 実数 $x \in \mathbf{R}_{>0}$ に対し，$x = e^y$ を満たす実数 y を

$$y = \log(x)$$

と表し，x の**対数**（【英】logarithm）と呼ぶ．

注意 3.1.1. 例えば，$1 = e^0$, $e = e^1$ なので，

$$\log(1) = 0, \quad \log(e) = 1$$

が成り立つ．また，定義から，実数 $a \in \mathbf{R}$ に対して

$$\log(e^a) = e^{\log a} = a$$

が成り立つ．

注意 3.1.2. $x = e^s$, $y = e^t$ とすると，

$$s = \log(x), \quad t = \log(y)$$

が成り立つ．このとき，

$$xy = e^s \times e^t = e^{s+t}$$

となって，$\log(xy) = s + t$ なので，

$$\log(xy) = \log(x) + \log(y)$$

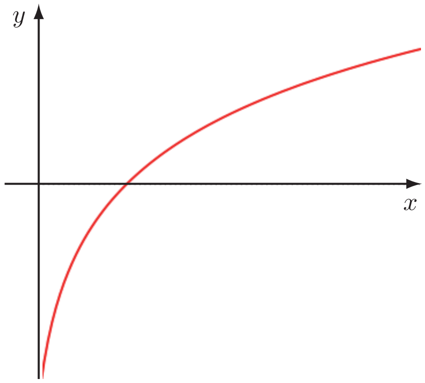
が成り立つ．

100 と 1000 を掛けるとき，それぞれを $100 = 10^2$, $1000 = 10^3$ と表せば，$2 + 3$ という加算を行うことにより，$10^{2+3} = 10^5 = 100000$ が計算できることを意味している．そもそも対数は桁数の大きな数同士を乗算する際，加算に置き換えて計算を楽にするために造られた概念である．例えば，$1234 \fallingdotseq e^{7.11801620}$, $5678 \fallingdotseq e^{8.64435433}$ であるが，この 2 つの積を計算する上で実際に乗算を行うより，$7.11801620 + 8.64435433 = 15.76237053$ という加算を実行する方が容易であろう．（この程度の桁数では乗算を選ぶかも知れないが，もっと大きな桁数で想像して欲しい．）ここで，$7006652 \fallingdotseq e^{15.76237053}$ となることを数表で知っていれば，$1234 \times 5678 = 7006652$ がわかるのである．この目的で，ネイピア数に名を残すネイピアは（現在の対数ではないが）20 年の年月をかけて巨大な数表を作成した．

さらに，この対数を使って対数関数を定義する．

定義 3.2. 正の実数 $x \in \mathbf{R}_{>0}$ に対して，$\log(x)$ を**対数関数**という．

この $y = \log(x)$ のグラフは



のようになる．特に，$y = e^x$ のグラフを直線 $y = x$ で折り返したグラフとなっている．この事実は，$y = \log(x)$ の定義からわかることである．実際，$y = \log(x)$ と

$$e^y = x$$

は同値であって，x と y の立場を入れ換える，即ち，x 軸と y 軸とを入れ換えたら同じグラフになる．これを同一の xy 平面上で考えれば，直線 $y = x$ で折り返していることに他ならない．(直線 $y = 2x$ と $y = \dfrac{1}{2}x$ のグラフを描いてみると，より状況が掴みやすいかも知れない.)

注意 3.2.1. また，注意 3.1.2 から，自然数 $n \in \mathbf{N}$ について

$$\log(x^n) = n\log(x)$$

が成り立つこともわかる．したがって，大体桁数に比例して増えていく関数だということがわかる．

桁数に比例するということは，増加するスピードは非常にゆっくりであるといえる．このグラフの x 軸の正の方向の先を考えると，非常にゆっくりではあるが確実に大きくなっていくので次が成り立つ．

命題 3.3. $\log(x)$ について，

$$\lim_{x\to\infty} \log(x) = \infty$$

が成り立つ．

注意 3.3.1. $x \to \infty$ のとき，$e^x = \exp(x)$ は急激に大きくなり，$\log(x)$ は非常にゆっくりと大きくなることに注意が必要である．

ネイピア数 e の定義（定義 2.1）に立ち返って，$\dfrac{1}{x}$ の原始関数を $F(x)$ とすれば，

$$\int_1^x \frac{1}{x}dx = \Big[F(x)\Big]_1^x$$

の値が 1 となるときの x の値が e であった．ここで，注意 3.1.1 で確認したように，

$$\int_1^e \frac{1}{x}dx = 1, \qquad \Big[\log(x)\Big]_1^e = 1$$

となって，「$F(x) = \log(x)$」とすると辻褄が合うことがわかる．実際にこの事実を以下で確認してみる．$y = e^x$ の $(x, y) = (a, e^a)$ での接線は命題 2.3 によって，

$$y - e^a = e^a(x - a)$$

と表すことができる．x と y を入れ換える（直線 $y = x$ で xy 平面を折り返すことに対応する）と，

$$x - e^a = e^a(y - a)$$

となって，

$$y - a = \frac{1}{e^a}(x - e^a)$$

となり，これが $\log(x)$ の $(x, y) = (e^a, a)$ での接線となる．即ち，$x = e^a$ での $\log(x)$ の微分係数は $\dfrac{1}{e^a}$ となっているから，次が成り立つ．

命題 3.4. $\log(x)$ の導関数について，

$$(\log(x))' = \frac{1}{x}$$

が成り立つ．

このことから，x が大きくなればなるほど微分係数は小さくなる，即ち，大きくなればなるほど $\log(x)$ の増加の仕方は非常に緩やかになるということである．しかし，微分係数がいくら小さい値であっても必ず正であることから，$\log(x)$ は単調増加する関数であって，$\displaystyle\lim_{x\to\infty} \log(x) = \infty$ が成り立つのである．

4　素数

まず，素数の定義を確認しておく．

定義 4.1. 1 より大きな整数で 1 とそれ自身しか約数を持たないものを**素数**（【英】prime number）という．

したがって，素数全体の集合を $\mathbf{P}$ と書くことにすると，

$$\mathbf{P} = \{2, 3, 5, 7, 11, 13, \\ 17, 19, 23, 29, 31, \ldots\}$$

ということになる．すぐわかることであるが，偶数の素数は 2 しかない．したがって，2 以外の素数は必ず奇数となる．逆に考えれば，すべての自然数の集合

$$\mathbf{N} = \{1, 2, 3, 4, 5, \ldots\}$$

に対して少なくとも半分は素数ではないのである．以下では集合の記号を使って，ある自然数 $p \in \mathbf{N}$ に対して，p が素数であることを，$p \in \mathbf{P}$ とも書くことにする．

自然数の集合 $\mathbf{N}$ の中で $\mathbf{P}$ を特徴付ける性質は他にもないのであろうか？答えは「YES」であって，例えば，次のような例が知られている．

定理 4.2 (Jones, Sato, Wada, Wiens ([JSWW], 1976))**.** 26 変数多項式 f を

$$\begin{aligned}
&f(a,b,c,d,e,f,g,h,i,j,k,l,m,\\
&\qquad n,o,p,q,r,s,t,u,v,w,x,y,z)\\
=&(k+2)\big[1-(wz+h+j-q)^2\\
&-\{(gk+2g+k+1)(h+j)+h-z\}^2\\
&-(2n+p+q+z-e)^2\\
&-\{16(k+1)^3(k+2)(n+1)^2\\
&\qquad\qquad +1-f^2\}^2\\
&-\{e^3(e+2)(a+1)^2+1-o^2\}^2\\
&-\{(a^2-1)y^2+1-x^2\}^2\\
&-\{16r^2y^4(a^2-1)+1-u^2\}^2\\
&-\{((a+u^2(u^2-a))^2-1)(n+4dy)^2\\
&\qquad\qquad +1-(x+cu)^2\}^2\\
&-(n+l+v-y)^2\\
&-\{(a^2-1)l^2+1-m^2\}^2\\
&-(ai+k+1-l-i)^2\\
&-\{p+l(a-n-1)\\
&\quad +b(2an+2a-n^2-2n-2)-m\}^2\\
&-\{q+y(a-p-1)\\
&\quad +s(2ap+2a-p^2-2p-2)-x\}^2\\
&-\{z+pl(a-p)\\
&\quad +t(2ap-p^2-1)-pm\}^2\big]
\end{aligned}$$

で定めるとき，$a, \ldots, z \in \mathbf{Z}_{\geqq 0}$ に対して

$$f(a, \ldots, z) > 0 \Longleftrightarrow f(a, \ldots, z) \in \mathbf{P}$$

が成り立つ．

したがって，この定理によれば，定理中の多項式 f を用いて素数全体の集合 $\mathbf{P}$ を

$$\mathbf{P} = \{f(a, \ldots, z) \text{ がとる正の値 }\}$$

と書き表すこともできる．

しかしながら，素数の現れ方を理解するのは非常に難しい．11 と 13 のように p と $p+2$ がともに素数であるようなものは**双子素数**と呼ばれ，このような例はたくさん知られている反面（双子素数は無限に存在すると予想されているが，未だに証明されていない），887 から 907 までの間にある 19 個の自然数がすべて合成数であるように，ある素数 p から次の素数 $p+m$ までの間 m が大きい例もたくさん知られている．

いずれにせよ，素数というのは自然数の集合の中にまばらに分布している．一見，ランダムに存在しているようにも見えるのではあるが，物の見方を変えてみるとある意味では非常に規則正しく整列しているようにも見て取れる．その事実をきちんと把握してみたい．

5　素数とリーマンゼータ関数

紀元前から素数という対象は知られていた．例えば，紀元前6500年頃の骨片に11, 13, 17, 19本の線からなる刻み目が刻まれていて，これを最古の素数表と呼ぶ人もいる（この骨片はイシャンゴの骨（【英】Ishango bone）と呼ばれ，現在ブリュッセルの自然史博物館に所蔵されている）．

この真偽の程はわからないが，少なくともギリシア人は素数をきちんと定式化して認識していた．さらには，紀元前300年頃に成立したとされる，**ユークリッド**（【英】Euclid,【希】Ευκλείδης）の「原論」では次の定理が証明されている．

定理 5.1. 素数は無限個存在する．

注意 5.1.1. 「原論」では，この定理だけではなく,「自然数の素因数分解の一意性」も示されている．

Proof. 素数が有限個であると仮定する．このとき，

$$p_0, p_1, p_2, \ldots, p_n$$

がそのすべての素数だとして，

$$p = p_0 \times p_1 \times p_2 \times \cdots \times p_n + 1$$

という自然数を考える．すると，p をどの素数 p_i で割っても必ず1余ることになり，決して割り切れない．また，すべての $i = 1, \ldots, n$ に対して $p > p_i$ となるから，どの p_i についても $p \neq p_i$ が成り立つ．ゆえに，p は1と p 自身でしか割り切れない数だから素数であり，したがって，上の $p_0, p_1, p_2, \ldots, p_n$ がすべての素数であることに矛盾する．　□

この証明とどこかで出会ったことのある方も多いと思うが，この事実のもう1つ別の証明を紹介しておく．

そのために，ドイツの数学者であるオイラー（【独】Leonhard Euler）(1707–1783) やリーマン（【独】Georg Friedrich Bernhard Riemann）(1826–1866) が考えたリーマンゼータ関数を定義する．

定義 5.2.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

を**リーマンゼータ関数**という（**リーマン ζ 関数**とも書く）．

注意 5.2.1. この関数について，定理2.5から，

$$\lim_{s \to 1} \zeta(s) = \infty$$

となる．

定理 5.3 (Euler, 1737)**.** リーマンゼータ関数 $\zeta(s)$ について，$s > 1$ のとき，**オイラー積**（【英】Euler product）と呼ばれる

$$\begin{aligned} \zeta(s) &= \prod_{p \in \mathbf{P}} \frac{1}{1 - \dfrac{1}{p^s}} \\ &= \frac{1}{1 - \dfrac{1}{2^s}} \cdot \frac{1}{1 - \dfrac{1}{3^s}} \cdot \frac{1}{1 - \dfrac{1}{5^s}} \cdots \end{aligned} \tag{5.1}$$

という等式が成り立つ．

注意 5.3.1. 定理中の

$$\zeta(s) = \prod_{p \in \mathbf{P}} \frac{1}{1 - \dfrac{1}{p^s}}$$

の右辺 $\displaystyle\prod_{p \in \mathbf{P}} \frac{1}{1 - \dfrac{1}{p^s}}$ は,「すべての素数 $p \in \mathbf{P}$ について

$$\frac{1}{1 - \dfrac{1}{p^s}}$$

を掛け合わせる」ことを意味する．総和の記号 $\sum$ の掛け算版だと理解して欲しい．

Proof. 簡単のため $s=2$ のときを考える．$\zeta(2)=\sum_{n=1}^{\infty}\frac{1}{n^2}$ だから，

$$\zeta(2)=1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\frac{1}{6^2}+\frac{1}{7^2}+\frac{1}{8^2}+\frac{1}{9^2}+\frac{1}{10^2}+\cdots$$

であって，両辺に $\frac{1}{2^2}$ を掛けると，

$$\frac{1}{2^2}\zeta(2)=\frac{1}{2^2}+\frac{1}{4^2}+\frac{1}{6^2}+\frac{1}{8^2}+\frac{1}{10^2}+\cdots$$

となり，辺々引くと，

$$\left(1-\frac{1}{2^2}\right)\zeta(2)=1+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\frac{1}{9^2}+\cdots$$

となる．同様に，この式から，この式の両辺に $\frac{1}{3^2}$ を掛けたもの

$$\frac{1}{3^2}\left(1-\frac{1}{2^2}\right)\zeta(2)=\frac{1}{3^2}+\frac{1}{9^2}+\frac{1}{15^2}+\frac{1}{21^2}+\cdots$$

を引くと，

$$\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{2^2}\right)\zeta(2)=1+\frac{1}{5^2}+\frac{1}{7^2}+\frac{1}{11^2}+\cdots$$

となる．この操作をすべての素数 $p\in\mathbf{P}$ について繰り返せば，

$$\prod_{p\in\mathbf{P}}\left(1-\frac{1}{p^2}\right)\zeta(2)=1$$

が得られる． □

オイラー積に現れる因子 $\frac{1}{1-\frac{1}{p^s}}$ を形式的に $s=1$ として和の形に書き換えてみる．命題 2.4 において，$a_1=1,\, r=\frac{1}{p}$ とすると，

$$\frac{1}{1-\frac{1}{p}}=\sum_{k=0}^{\infty}\frac{1}{p^k}=1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots$$

となることがわかる．リーマンゼータ関数の定義とオイラー積から，形式的に $s=1$ とすると

$$\sum_{n=1}^{\infty}\frac{1}{n}=\prod_{p\in\mathbf{P}}\frac{1}{1-\frac{1}{p}}=\prod_{p\in\mathbf{P}}\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right) \tag{5.2}$$

が成り立つ．このオイラー積に現れる因子 $\frac{1}{1-\frac{1}{p}}$ は任意の素数 p に対して有限の値であることに注意して欲しい．素数全体の集合 $\mathbf{P}$ が有限集合ならば，オイラー積の値は有限でならなければならず，注意 5.2.1 の

$$\lim_{s\to 1}\zeta(s)=\infty$$

に矛盾してしまうので，$\mathbf{P}$ は無限個の素数を含んでいなくてはならない．これは，定理 5.1 の別証明となっている．

さらに，上述の (5.2) 式に注目すると，左辺に現れる項 $\frac{1}{n}$ の 1 つ 1 つについて，ある素数の組 $\{p_1,\ldots,p_m\}$ を用いて

$$\frac{1}{n}=\frac{1}{p_1^{t_1}}\times\frac{1}{p_2^{t_2}}\times\cdots\times\frac{1}{p_m^{t_m}}$$

と表せることを意味している．即ち,「自然数 n が素因数分解ができ，なおかつ，それが一意的である」ことも示唆している．

このように，定理 5.3 のオイラー積の等式 (5.1) は，非常に重要な自然数の事実を 2 つも含んだ意義深い等式なのである．

6　エラトステネスの篩

さらに，**エラトステネス**（【英】Eratosthenes,【希】Ερατοσθένης）(B.C. 275–B.C. 194) **の篩**と呼ばれる素数のリストを求めるアルゴリズムが知られていた．これは,『k 以下の素数のすべてを求めたいときには，k までの自然数のリストを作り，$\sqrt{k}$ 以下のすべての素数の倍数を消去すれば，残った数はすべて素数となる』というもので，具体的に表わせば次のようになる．このアルゴリズムにおいては,『←』は代入を表し,『=』は比較演算子を表すことに注意しておく．

アルゴリズム 6.1 (エラトステネスの篩)**.**

【入力】自然数 $k \in \mathbf{N}$

【出力】k 以下の素数のリスト

1. ［初期化］すべての $i = 1, \ldots, k$ について $a_i \leftarrow 1$ とおく．i が素数でないものは $a_i = 0$ としたいので，まず 1 を除外して，$a_1 \leftarrow 0$ とする．2 は素数だから $p \leftarrow 2$ とおいて，$t \leftarrow p$ とおく．
2. ［篩］$t \leftarrow t+p$ とおく．$t \geqq k$ ならば p の倍数をすべて消去したことになるので step 3 へ，$t < k$ ならば $a_t \leftarrow 0$ とおいて step 2 へ．
3. ［p の取り直し］$p \leftarrow p+1$ とおく．$a_p = 1$ である（p より小さいすべての素数で割り切れない）ことと p が素数であることは必要十分だから，$a_p = 0$ ならばstep 3へ，$a_p = 1$ ならばstep 4へ．
4. ［終了確認］$p > \sqrt{k}$ ならばすべての素数について篩い落としたことになるので step 5 へ，$p \leqq \sqrt{k}$ ならば p の倍数をすべて消去するために $t \leftarrow p$ とおいて step 2 へ．
5. ［出力］すべての $i = 1, \ldots, k$ について，$a_i = 1$ となる i が素数であるから，i を出力する．

実験 1. エラトステネスの篩を体感してみる．

この実験を行うために，PARI/GP というフリーウェアを用いる．起動すると 9 ページの図 1 のような画面が現れる．

このソフトウェアは整数論と呼ばれる数学の分野の研究者が中心となって開発を進めているもの（[Coh] 参照）なので，素数に関する計算が非常に早く動作するように設計されている．アルゴリズムに基づいて手続きを繰り返すのは，コンピュータに任せた方が良いので，プログラムを書いて関数を作ってしまった方が便利である．プログラムといっても，そんなに大したことではなく，メモ帳などのテキストエディタを用いて

```
era(k)={
a=Vec(x=[]);a0=Vec([1]);
for(i=1,k,a=concat(a,a0));
a[1]=0;p=2;t=p;
while(p*p<=k,
  t=t+p;
  while(t<=k,a[t]=0;t=t+p);
  p=p+1;
  while(a[p]==0,p=p+1);
  t=p;
);
for(i=1,k,if(a[i]==1,a[i]=i));
print1(a);
}
```

というテキストファイルを準備しておくだけである.（とはいえ，一文字でも入力を間違えてしまうと，正しく動作しないのはコンピュータの厄介なところでもある.）このリストとアルゴリズムは，2〜4 行目がstep 1に，6･7 行目がstep 2に，8･9 行目がstep 3に，5 行目と10･11 行目がstep 4に，12･13 行目がstep 5に対応していることを注意しておく．準備ができたら，`Desktop` 上に「`era.gp`」というファイル名で保存しておく．ここで，PARI/GP

のコマンドプロンプトから

```
gp> \r $HOME/Desktop/era.gp
```

とすれば，今作ったファイルを読み込むことができる.（但し,「gp> 」の部分は自動的に表示されるので，自ら入力する必要はない．このような入力待ち状態に表示される文字列をプロンプトと呼ぶ.）さらに，

```
gp> era(100)
```

とすれば，エラトステネスの篩を用いて，100までの整数の中で素数だけをリストアップすることができる．実際に実行してみると，図2のように表示される筈である．素数を表示させるのは勿論であるが，ここでは敢えて，素数が出現する不規則さを体感するために，素数でない整数に対しては0を表示させている．era(k) の k の値をどんどん大きくして「era(300)」,「era(500)」, ... などの表示を見てみると，素数が出現する様子はとても不規則であることが観察できる．以下の節では，このような不規則な素数の列について，何か規則性を見付けることができないのかもう少し詳細に調べてみる．

図 1：PARI/GP 起動画面

```
Reading GPRC: gprc.txt ...Done.

                   GP/PARI CALCULATOR Version 2.7.4 (released)
          amd64 running mingw (x86-64/GMP-6.0.0 kernel) 64-bit version
                compiled: Jun  5 2015, gcc version 4.9.2 (GCC)
                            threading engine: single
                 (readline v6.2 enabled, extended help enabled)

                     Copyright (C) 2000-2015 The PARI Group

PARI/GP is free software, covered by the GNU General Public License,
and comes WITHOUT ANY WARRANTY WHATSOEVER.

Type ? for help, \q to quit.
Type ?12 for how to get moral (and possibly technical) support.

parisize = 8000000, primelimit = 500000
(12:14) gp >
```

図 2：出力サンプル

```
[0, 2, 3, 0, 5, 0, 7, 0, 0, 0, 11, 0, 13, 0, 0, 0, 17, 0, 19, 0, 0, 0, 23, 0, 0,
0, 0, 0, 29, 0, 31, 0, 0, 0, 0, 0, 37, 0, 0, 0, 41, 0, 43, 0, 0, 0, 47, 0, 0, 0
, 0, 0, 53, 0, 0, 0, 0, 0, 59, 0, 61, 0, 0, 0, 0, 0, 67, 0, 0, 0, 71, 0, 73, 0,
0, 0, 0, 0, 79, 0, 0, 0, 83, 0, 0, 0, 0, 0, 89, 0, 0, 0, 0, 0, 0, 0, 97, 0, 0, 0
]
```

7　素数の個数

有限集合 S に対して，$\#S$ を S に属する要素の個数とする．x 以下の素数の個数を数える関数

$$\pi(x) = \#\{p : \text{素数} \mid p \leqq x\}$$

を考える.（この関数は，素数関数（【英】prime counting function）と呼ばれることがある.）例えば，この関数は $\pi(10) = \#\{2, 3, 5, 7\} = 4$ という値を取る．小さい値ならば具体的に計算するのは簡単であるが，大きな x に対して $\pi(x)$ を計算するのは非常に骨が折れる作業になる．実際，x が大きいときにエラトステネスの篩（アルゴリズム 6.1）を手で実行するのは嫌だと想像できる筈である．

実験 2. $\pi(x)$ の値を計算してみる．

この $\pi(x)$ の値を求めるために，改めて PARI/GP を用いる．$\pi(x)$ を自作して

```
pi(k)={
s=0;
for(j=1,k,
  if(isprime(j)==1,
    s=s+1,s=s));
print1("pi("k")="s"\n")
}
```

という関数を定義して計算すれば，より具体的に素数を数えている気分が味わえるが，PARI/GP には「primepi(x)」という関数が最初から定義されているので，これを用いて

```
gp> primepi(100)
```

とすれば，気軽に $\pi(100)$ の値が計算できる．『100』という値を変えてもっと大きな値に対しても $\pi(x)$ の値を計算してみると，

x	$\pi(x)$	$\dfrac{x}{\pi(x)}$
10	4	2.50
100	25	4.00
1000	168	5.95
10000	1229	8.14
100000	9592	10.43
1000000	78498	12.74

といった表ができあがる．今の表を良く調べてみると，x の値を 1 桁ずつ（10 倍ずつ）増やすごとに $\dfrac{x}{\pi(x)}$ がおおよそ 2 から 3 の間で増えていることに気が付くであろう．注意 3.2.1 で確認したように，桁が増えるごとに一定の大きさで増加する関数は $\log(x)$ だと知っているので，この現象に基づいて，次のように予想できる筈である．

予想 7.1. $\pi(x)$ について，

$$\frac{x}{\pi(x)} \sim \log(x),$$

即ち，

$$\pi(x) \sim \frac{x}{\log(x)}$$

が成り立つ．

ここで,「$\sim$」という記号は，x が限りなく大きくなるとき $\dfrac{\pi(x)}{\frac{x}{\log(x)}}$ も $\dfrac{\frac{x}{\log(x)}}{\pi(x)}$ も有界となる（ある定数で押さえることができる）ことを意味するものである．簡単に言えば，x が大きくなればなるほど，$\pi(x)$ という関数は $\dfrac{x}{\log(x)}$ という関数と同じくらいの速さで大きくなることを意味する記号である．

さらに，命題 3.3 によって，

$$\lim_{x\to\infty} \log(x) = \infty$$

だったので，x が大きくなれば $\log(x)$ も無限に大きくなることと，その無限に大きくなるなり方が非常に遅いことを確認しておく．

PARI/GP には一応グラフを描く機能も備わっていることを注意しておく．例えば，

```
graphpi(k)={
vx=Vec(x=[]);
vy=Vec(y=[]);
for(j=1,k,
    vx0=Vec([j]);
    vy0=Vec([primepi(j)]);
    vx=concat(vx,vx0);
    vy=concat(vy,vy0));
plothraw(vx,vy);
}
```

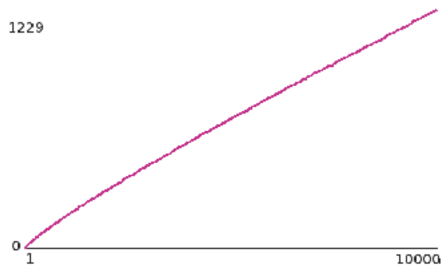
という内容を「prime2.gp」というテキストファイルとして保存してから，

```
gp> \r $HOME/Desktop/prime2.gp
```

としてこのファイルを読み込んで，

```
gp> graphpi(10000)
```

を実行すれば，$\pi(x)$ の様子を見ることができる．



（上で「一応グラフを描く機能も備わっている」と述べたのは，見易さには欠けるからである．この点を補うためにも，次節で述べる通り，グラフを描く専門のソフトに任せた方が便利である.）このグラフが本当に $\dfrac{x}{\log(x)}$ のグラフに近いのかどうかに興味がわくだろう．次節で，計算実験を行い，この予想を検証する．

8　素数の分布

18 世紀になると対数表など色々な数表が作られるようになった．かなり大きな素数の表もフェルケル（【墺】Anton Felkel）の例に見られる（[Fel] 参照）．

このような時代背景のもと，フランスの数学者**ルジャンドル**（【仏】Adrien-Marie Legendre）(1752–1833) は $\pi(x)$ をより詳細に調べた結果，予想 7.1 を次の予想に置き換えた．

予想 8.1 (Legendre ([Leg], 1808))**.**

$$\pi(x) \sim \frac{x}{\log(x) - 1.08366}$$

が成り立つ．

実験 3. $\pi(x)$ と $\dfrac{x}{\log(x) - 1.08366}$ をグラフに図示して比較してみる．

PARI/GP にもグラフを描く機能があることを紹介したが，確認した通りお世辞にも綺麗だとは言い難いので，その部分はグラフを描く専門のソフトに任せることにする．そのために，PARI/GP で計算したデータを別のファイルに出力するのに，テキストエディタで

```
k=30000;\
forstep(i=0,k,100,\
 s=primepi(i);\
 write1(\
 "$HOME/Desktop/pi-x.txt",\
 i" "s"\n"));
```

を入力し（この際，テキストエディタによっては，バックスラッシュ (\) を入力しても「¥」で表示されることがあるが気にしないでよい），「prime3.gp」というファイル名で保存する．

```
gp> \r $HOME/Desktop/prime3.gp
```

として実行してみると，デスクトップに「pi-x.txt」というファイルができている筈である．このファイルの中身を眺めてみると，

```
0 0
100 25
200 46
300 62
.....
29900 3238
30000 3245
```

といったように x の値が 0 から 30000 まで 100 刻み毎に $\pi(x)$ の値が書き込まれている筈である.（色々なフリーウェアの高機能な部分を「良いとこ取り」するために，このように中間データを次のフリーウェアで使いやすい形で保存しておくというのはよくやることであり，実際，効果も大きい場合が多い.）

このデータを用いて，改めてグラフを描いてみる．そのために gnuplot を使う.（3, 4 ページの指数関数と対数関数のグラフも gnuplot を用いて描いている.）gnuplot を起動すると 13 ページの図 3 のような画面が現れる筈である．最後に現れる

```
gnuplot>
```

はプロンプトなので，これに続けて入力してグラフを描いていく．まず，$\pi(x)$ のデータは先ほど作った「pi-x.txt」というファイルに出力されているので，これを利用して，

```
gnuplot> plot\
> "../Desktop/pi-x.txt"\
> using 1:2
```

と入力してみる.（ここでは 3 行にわたって書いているが，これはあくまで紙面の都合であって，1 行で書いてしまって構わない．その場合はバックスラッシュ (\) をタイプせず,

```
plot "../Desktop/pi-x.txt" using 1:2
```

のように入力すればよい．バックスラッシュは複数行にわたって入力する際に必要なだけであって，2, 3 行目にある「> 」はバックスラッシュを入力後，エンターキーを入力すると即時に表示されるプロンプトなので自ら入力する必要はない.）

最後の「using 1:2」の部分は,「データの 1 列目と 2 列目の値を x 軸，y 軸にとってプロットする」という意味である．したがって，1 列目には x の値，2 列目には $\pi(x)$ の値が書かれているので，それに対応する点がグラフ上にプロットできる．このままではわかりにくいので，もう一度 gnuplot を再起動して

```
gnuplot> plot \
> "../Desktop/pi-x.txt"\
> using 1:2 with steps
```

と入力してみる．今度は点と点が線で結ばれて階段状のグラフになる．さらに，この階段グラフと予想 8.1 の $\dfrac{x}{\log(x)-1.08366}$ とを見比べるために同時に 2 つのグラフを描いてみる．それには,

```
gnuplot> plot\
> "../Desktop/pi-x.txt"\
> using 1:2 with steps,\
> x/(log(x)-1.08366)
```

と入力すればよい．コンマ（,）で関数を区切れば同時に複数のグラフを描くことができるのである．この操作によって，13 ページの図 4 のようなグラフを描くことができる．今の要領で，より大きな x まで $\pi(x)$ のグラフを描くことができる．x を 10 万くらいまで大きくして実験を繰り返せば繰り返すほど，ルジャンドルの予想（予想 8.1）をかなり正しいと感じるようになる筈である．

彼の予想からおよそ 90 年後にフランスの数学者アダマールとベルギーの数学者ド・ラ・ヴァレ・プーサンが独立にリーマンゼータ関数 $\zeta(s)$ を調べることにより以下の事実を証明した．

定理 8.2 (Hadamard [Had], de la Vallèe-Poussin [Pou], 1896)**.** 上記の予想 7.1 は正しい．特に，

$$\frac{x}{\log(x)-1}$$

が $\pi(x)$ の最良近似である．

この事実から，ルジャンドルの予想 8.1 は真の意味では正しくないことわかる．しかしながら，そのことを責めたい訳ではない．コンピュータのない時代に，本稿では気軽に手に入れている実験データを手計算で得ることは非常に大変なことである．ルジャンドルは当時としては精密な計算実験を行い，正しい帰結を得るための大きな礎石を遺したと評価するべきである．

図 3：GNUPLOT 起動画面

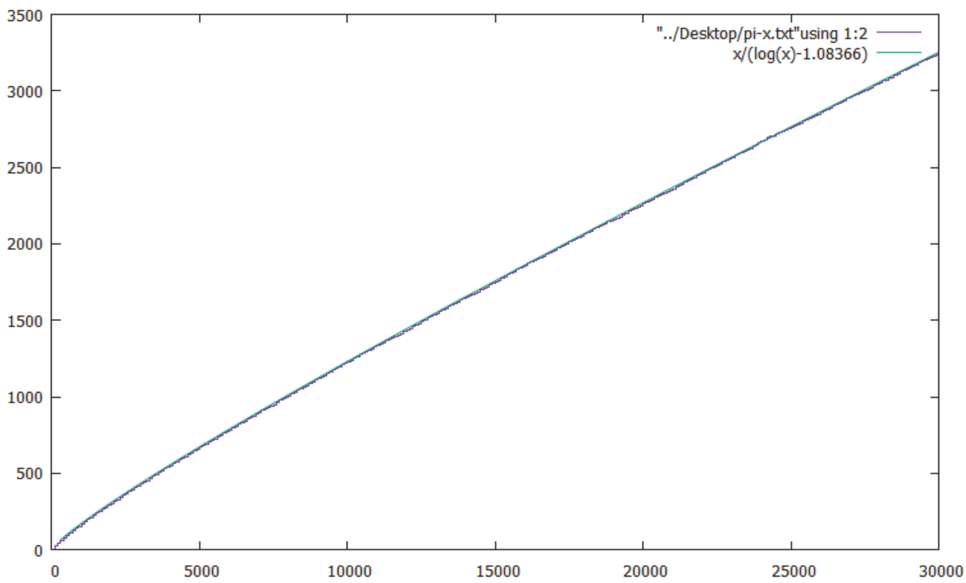
```
        G N U P L O T
        Version 5.0 patchlevel 1    last modified 2015-06-07

        Copyright (C) 1986-1993, 1998, 2004, 2007-2015
        Thomas Williams, Colin Kelley and many others

        gnuplot home:     http://www.gnuplot.info
        faq, bugs, etc:   type "help FAQ"
        immediate help:   type "help"  (plot window: hit 'h')

Terminal type set to 'wxt'
gnuplot>
```

図 4：$\pi(x)$ **と** $\dfrac{x}{\log(x)-1.08366}$ **のグラフ**



9　ルジャンドルが見ていた世界

最後に，予想 8.1 の式に現れる定数 1.08366 に着目して，ルジャンドルが予想のために用いたデータがどのようなものであったかを推測してみることにする．具体的には，整数 k を中心に $k-200$ から $k+200$ の範囲で $\pi(x)$ を求めて

$$f_1(x)=\frac{x}{\log(x)-1.08366}$$

と

$$f_2(x)=\frac{x}{\log(x)-1}$$

のグラフと比較すれば，どの範囲の k まで $f_1(x)$ に近いのかがわかる筈である．実際，$k=10000$ のときには図 5 のようになり，十分に 1.08366 の効果があるのが見て取れる．但し，紫の線が $\pi(x)$ で緑と水色の線がそれぞれ $f_1(x)$，$f_2(x)$ を表している．

このような作業を繰り返すと $k=200000$ のときは15ページの図 6 のようになり，$f_1(x)$ に近い最後であって，ここから $k=250000$ 前後では $\pi(x)$ は $f_1(x)$ のグラフの上に位置するようになり，$k=300000$ 以上では $\pi(x)$ は $f_1(x)$ より下に少しずつ離れて行ってしまう．したがって，ルジャンドルはどれだけ良くても高々20万までの素数表しか調べていなかったと見るのが妥当であろう．

では，いつ $f_2(x)$ に近付いていくのかと言えば，k が 1000 億程度でも 15 ページの図 7 のようになり，$f_1(x)$ と $f_2(x)$ のちょうど中間ぐらいに位置している．これはまだまだ k が小さいのであって，数学では「素数が無限個存在する」と容易に表現してしまうように，計算実験するのは大変だが k を無限に大きくすれば $f_2(x)$ に近付く（筈）という数学らしい現象が見て取れる．

図 5：$k=10000$ のとき

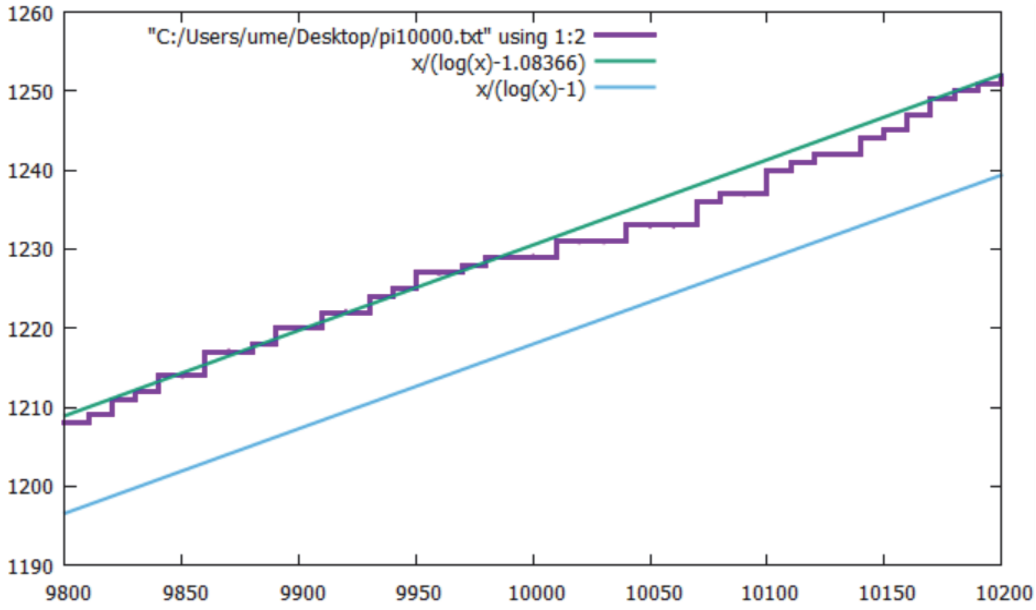


図 6：$k = 200000$ **のとき**

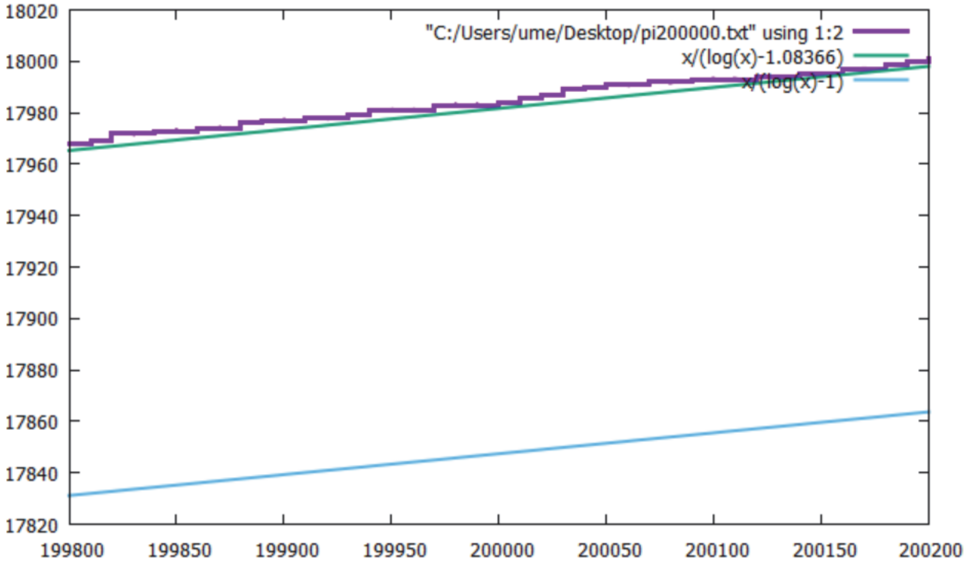
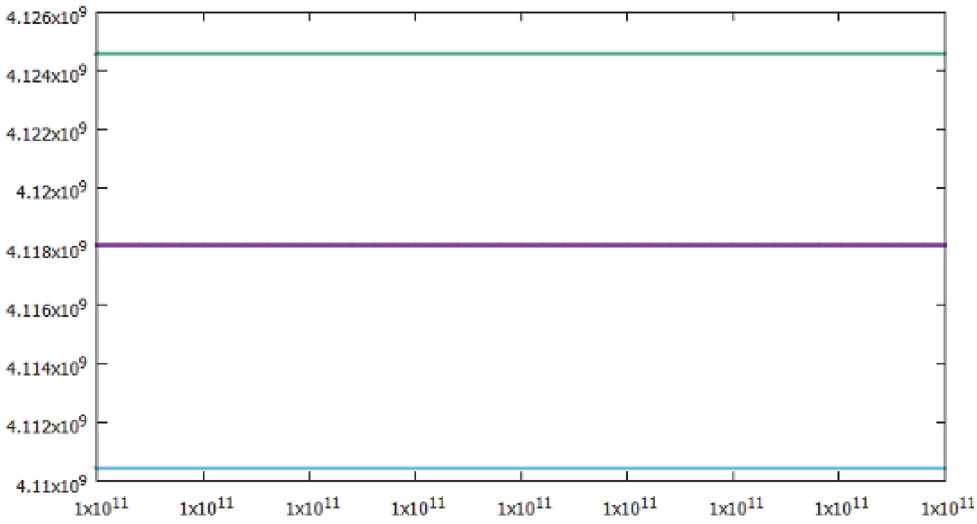


図 7：$k = 100000000000$ **のとき**



参考文献

[Fel] Felkel, Anton, *Tafel aller einfachen Factoren der durch 2, 3, 5 nicht theilbaren Zahlen von 1 bis 10 000 000*, Vienna, 1776

[Leg] Legendre, Adrien-Marie, *Essai sur la théorie des nombres*, Reprint of the second (1808) edition, Cambridge University Press, Cambridge, 2009

[Pou] de la Vallée-Poussin, C. J., Recherches analytiques de la théorie des nombres premiers, *Annales de la Societe*

Scientifique de Bruxelles, 1896

[Had] Hadamard, J., Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, *Bulletin de la Société Mathématique de France*, **24**, 1896, 199-220

[Coh] Cohen, H., *A Course in Computational Algebraic Number Theory*, GTM 138, 1993, Springer-Verlag

[JSWW] Jones James P.; Sato, Daihachiro; Wada, Hideo; Wiens, Douglas, Diopahntine representation of the set of prime numbers, *Amer. Math. Manthly*, **83**, 1976, no. 6, 449–464

[PARI] PARI/GP ホームページ
`http://pari.math.u-bordeaux.fr`

[PLOT] gunplot ホームページ
`http://gnuplot.info`

Title: **Introduction to prime number theorem presented at a course of adult education**

Author: **UMEGAKI, Atsuki**