

新版 素数は“いくつ”あるか*

佐藤 篤†

§1 はじめに

1.1 素数とは

正の整数は、その (正の) 約数の個数から見れば、次の 3 種類に分けることができる:

- (i) ただひとつの約数をもつもの.
- (ii) ちょうど 2 個の約数をもつもの.
- (iii) 3 個以上の約数をもつもの.

全ての整数は 1 とその数自身を約数にもつから、(i) の場合に当たる数は 1 のみである. 素数とは (ii) の場合に当たる数のことであった. 例えば、100 以下の整数のうち、素数であるものは次の 25 個である:

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

なお、(iii) の場合に当たる数を合成数という.

次の定理からわかるように、素数とは整数の世界における元素のようなものである (証明は略):

定理 1.1 (初等整数論の基本定理) 任意の整数 $m \geq 2$ は、いくつかの素数の積として (順序の違いを除いて) ただひと通りに表される.

1.2 エラトステネスの篩

一般に正の整数 a, b に対して a が b を割り切るならば $a \leq b$ が成り立つから、整数 $m \geq 2$ が素数か否かを調べるためには m を $1 < n < m$ なる整数 n で割ってみればよい. いずれの n でも割り切れなければ m は素数である. m 未満の素数が既に与えられているときには、この手続きは

*第 3 回仙台数学セミナー (1995 年 8 月 21 日 - 25 日) 配布資料・数学ってなんだろう (猪狩惺 編著, 日本評論社, 1997 年) 原稿に加筆修正 [2015 年 9 月 5 日版]

†東北学院大学教養学部 (E-mail: atsushi@mail.tohoku-gakuin.ac.jp)

次のように簡略化できる:

(b) m が $p < m$ なる素数 p で割り切れなければ m は素数.

この判定法は, さらに次のように精密化できる:

(#) m が $p^2 \leq m$ なる素数 p で割り切れなければ m は素数.

これらの素数判定法を用いると, 100 以下の素数を次のようにして求めることができる:

(i) まず, 2 から 100 までの整数を全て書き出す:

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

このとき (b) より 2 は素数であることがわかる.

(ii) 2 以外の 2 の倍数は素数ではないから, それらを消す:

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

このとき (b) より 3 は素数であることがわかる.

(iii) 3 以外の 3 の倍数は素数ではないから, それらを消す:

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

このとき (b) より 5 は素数であることがわかる.

(iv) 5 以外の 5 の倍数は素数ではないから, それらを消す:

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

このとき (b) より 7 は素数であることがわかる.

(v) 7 以外の 7 の倍数は素数ではないから, それらを消す:

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

このとき (b) より 11 は素数であることがわかる. さらに, (♯) と $11^2 > 100$ により, 消されずに残っている

13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

も素数であることがわかる.

このようにして素数を求める方法をエラトステネスの^{ふるい}篩という.

練習問題 1.2 (b) と (♯) を証明せよ.

1.3 関数 $\pi(x)$

全体を通して, 実数 x に対し, x 以下の素数の個数を $\pi(x)$ で表す. 例えば, 10 以下の素数は 2, 3, 5, 7 の 4 個であるから, $\pi(10) = 4$. また, 先に述べたことから, $\pi(100) = 25$. さらに, $x < 2$ のときには $\pi(x) = 0$ であるから, $\pi(x)$ が実際に意味をもつのは $x \geq 2$ の場合である. 関数 $\pi(x)$ のグラフは, 図 1 (p. 4) のように, x が素数のときに 1 だけ飛び上がる階段のような形になる.

1.4 記号

全体を通して使う記号を列挙しておく.

(i) 整数 $k > 0$ に対し, k 番目の素数を p_k で表す:

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11, \quad \dots$$

(ii) 既に述べたように, 実数 x に対し, x 以下の素数の個数を $\pi(x)$ で表す.

(iii) 実数 x に対し, x 以下の整数のうちで最大のものを $[x]$ で表す. すなわち, $[x]$ とは不等式

$$[x] \leq x < [x] + 1$$

をみたす (ただひとつの) 整数である.

(iv) 整数 $a \neq 0$ が整数 b を割り切るとき, このことを “ $a \mid b$ ” と表す.

(v) $\log$ で自然対数を表す. また, 単に “対数” で自然対数を意味するものとする.

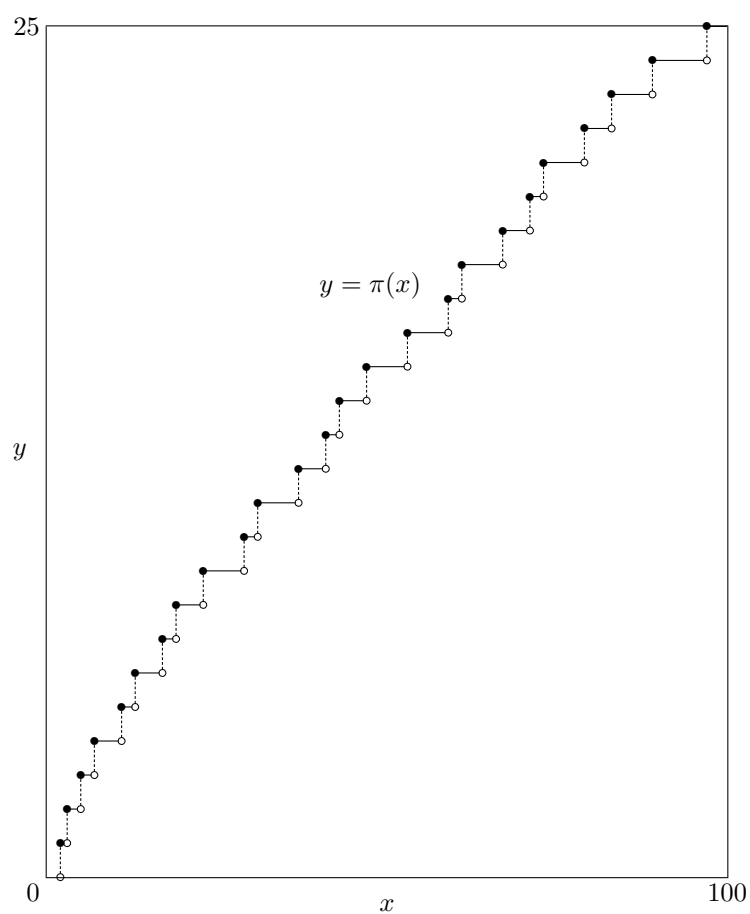


図 1: $\pi(x)$ のグラフ ($x \leq 100$)

練習問題 1.3 $\log x$ の積分表示

$$\log x = \int_1^x \frac{dt}{t} \quad (x > 0)$$

を用いて, $0 < a \leq b$ なる実数 a, b に対して次の不等式が成り立つことを示せ:

$$\frac{b-a}{b} \leq \log \frac{b}{a} \leq \frac{b-a}{a}.$$

§2 素数は無数にある

標題の問いに対する最も安直な解答は次で与えられる:

定理 2.1 素数は無数に多く存在する.

2.1 ユークリッド原論にある証明

次に挙げるのはユークリッド原論にある証明である:

[定理 2.1 の証明] n 個の素数 $p_1, p_2, \dots, p_n$ に対し, それら以外にも素数が存在することを示せばよい. いま, $m = p_1 p_2 \cdots p_n + 1$ と置く. このとき, m はどの p_k ($k = 1, 2, \dots, n$) でも割り切れないから, m の素因数は $p_1, p_2, \dots, p_n$ 以外の素数である. この素因数が求めるものである. (証明終わり)

上の証明は既知の素数から新しい素数を構成する方法を示している訳ではない. しかしながら, この証明から次のことがわかる:

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \quad (n = 1, 2, 3, \dots).$$

この不等式から, 数学的帰納法を用いて, 次が成り立つことが証明できる:

$$p_n < 2^{2^n} \quad (n = 1, 2, 3, \dots).$$

また, 上の証明と同様のアイデアにより, 整数の列の中には素数をひとつも含まない任意の長さの範囲が存在することが示せる. 実際, $p_1 p_2 \cdots p_n + 2$ から始まる $p_n - 1$ 個の連続した整数

$$p_1 p_2 \cdots p_n + 2, \quad p_1 p_2 \cdots p_n + 3, \quad p_1 p_2 \cdots p_n + 4, \quad \dots, \quad p_1 p_2 \cdots p_n + p_n$$

は, いずれも $p_1, p_2, \dots, p_n$ のうちの少なくともひとつで割り切れ, 従って合成数である.

2.2 オイラーによる証明

1737 年, オイラーは次の定理を示した:

定理 2.2 任意の実数 $x \geq 2$ に対し, $n = \pi(x)$ とするとき,

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} \geq \log(\log x) - 1.$$

この定理から, 素数の逆数の総和

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots$$

は ∞ に発散することがわかり, 定理 2.1 の別証明が直ちに得られる.

定理 2.2 を示すために, 補助定理を 2 つ準備しておく.

補助定理 2.3

$$\left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n}\right)^{-1}$$

は $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ ($e_1, e_2, \dots, e_n \geq 0$) なる形の整数の逆数の総和に一致する.

[証明]

$$\begin{aligned}\left(1 - \frac{1}{p_1}\right)^{-1} &= 1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots, \\ \left(1 - \frac{1}{p_2}\right)^{-1} &= 1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots, \\ &\dots\dots\dots, \\ \left(1 - \frac{1}{p_n}\right)^{-1} &= 1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \cdots\end{aligned}$$

より

$$\begin{aligned}\left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n}\right)^{-1} \\ = \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots\right) \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots\right) \cdots \left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \cdots\right)\end{aligned}$$

が成り立つ. この等式の右辺を展開すると, 素因数分解の一意性により, $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ なる形の整数の逆数がちょうど 1 回ずつ現れる. (証明終わり)

補助定理 2.4 任意の整数 $m > 0$ に対し,

$$\log(m+1) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m} \leq 1 + \log m.$$

[証明] 練習問題 1.3 より, 実数 $a > 1$ に対して

$$\log \frac{a+1}{a} \leq \frac{1}{a} \leq \log \frac{a}{a-1}$$

が成り立つことがわかるから,

$$\begin{aligned}1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m} &\geq \log 2 + \log \frac{3}{2} + \cdots + \log \frac{m+1}{m} = \log(m+1), \\ 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m} &\leq 1 + \log 2 + \log \frac{3}{2} + \cdots + \log \frac{m}{m-1} = 1 + \log m.\end{aligned}$$

(証明終わり)

それではオイラーによる証明を述べる.

[定理 2.2 の証明] x 以下の整数 $m \geq 2$ の素因数分解には $p_1, p_2, \dots, p_n$ 以外の素数は現れないから, 補助定理 2.3 より,

$$\left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n}\right)^{-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{[x]} + \text{etc.} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{[x]}.$$

ここで “etc.” は $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ なる形の整数のうちで x よりも大きいものの逆数の総和である。また、補助定理 2.4 より、

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{[x]} \geq \log([x] + 1) \geq \log x.$$

従って

$$\left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n}\right)^{-1} \geq \log x$$

となり、この対数をとって

$$\log \left(1 - \frac{1}{p_1}\right)^{-1} + \log \left(1 - \frac{1}{p_2}\right)^{-1} + \cdots + \log \left(1 - \frac{1}{p_n}\right)^{-1} \geq \log(\log x)$$

となることがわかる。他方、練習問題 1.3 より、実数 $a > 1$ に対して

$$\log \left(1 - \frac{1}{a}\right)^{-1} = \log \frac{a}{a-1} \leq \frac{1}{a-1} = \frac{1}{a} + \left(\frac{1}{a-1} - \frac{1}{a}\right)$$

が成り立つことがわかるから、

$$\begin{aligned} & \log \left(1 - \frac{1}{p_1}\right)^{-1} + \log \left(1 - \frac{1}{p_2}\right)^{-1} + \cdots + \log \left(1 - \frac{1}{p_n}\right)^{-1} \\ & \leq \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} + \left(\frac{1}{p_1-1} - \frac{1}{p_1}\right) + \left(\frac{1}{p_2-1} - \frac{1}{p_2}\right) + \cdots + \left(\frac{1}{p_n-1} - \frac{1}{p_n}\right). \end{aligned}$$

ここで

$$\begin{aligned} & \left(\frac{1}{p_1-1} - \frac{1}{p_1}\right) + \left(\frac{1}{p_2-1} - \frac{1}{p_2}\right) + \cdots + \left(\frac{1}{p_n-1} - \frac{1}{p_n}\right) \\ & \leq \left(\frac{1}{2-1} - \frac{1}{2}\right) + \left(\frac{1}{3-1} - \frac{1}{3}\right) + \left(\frac{1}{4-1} - \frac{1}{4}\right) + \cdots \\ & = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots = 1 \end{aligned}$$

であるから、

$$\log \left(1 - \frac{1}{p_1}\right)^{-1} + \log \left(1 - \frac{1}{p_2}\right)^{-1} + \cdots + \log \left(1 - \frac{1}{p_n}\right)^{-1} \leq \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} + 1.$$

これより求める不等式を得る。

(証明終わり)

この他にもオイラーは、実数 $s > 1$ に対し、正の整数を s 乗したものの逆数の総和

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

($s > 1$ ならば、この無限和は収束する) を研究し、この無限和が

$$\left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \left(1 - \frac{1}{5^s}\right)^{-1} \cdots = \left(1 - \frac{1}{p_1^s}\right)^{-1} \left(1 - \frac{1}{p_2^s}\right)^{-1} \left(1 - \frac{1}{p_3^s}\right)^{-1} \cdots$$

なる無限積に一致することを示した (証明は補助定理 2.3 のそれと同様). また, $\sin(\pi x)$ の無限積への分解

$$\sin(\pi x) = \pi x(1-x^2) \left(1 - \frac{x^2}{2^2}\right) \left(1 - \frac{x^2}{3^2}\right) \left(1 - \frac{x^2}{4^2}\right) \cdots$$

を利用して, 次のような結果を得ている:

$$\begin{aligned} 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots &= \frac{\pi^2}{6}, \\ 1 + \frac{1}{2^4} + \frac{1}{3^4} + \cdots &= \frac{\pi^4}{90}, \\ 1 + \frac{1}{2^6} + \frac{1}{3^6} + \cdots &= \frac{\pi^6}{945}, \\ 1 + \frac{1}{2^8} + \frac{1}{3^8} + \cdots &= \frac{\pi^8}{9450}, \\ &\dots\dots\dots \end{aligned}$$

ただし, ここでは π は円周率を表す.

さらに, オイラーは s が 0 以下の整数のときにも上のような無限和を考え, 次のような結果 (!) も得ている:

$$\begin{aligned} 1 + 1 + 1 + \cdots &= -\frac{1}{2}, \\ 1 + 2 + 3 + \cdots &= -\frac{1}{12}, \\ 1 + 2^2 + 3^2 + \cdots &= 0, \\ 1 + 2^3 + 3^3 + \cdots &= \frac{1}{120}, \\ &\dots\dots\dots \end{aligned}$$

これらの奇妙な計算結果は後のリーマンの仕事によって (適当な意味で) 正当化されることになる.

§3 素数は “どのくらい” たくさんあるか

先に述べたように, 関数 $\pi(x)$ のグラフは階段状であって, それを支配している何の法則も見出せないように思われる. ところが, x の範囲を徐々に広げれば, 図 2 (p. 9) のような美しい曲線が現れる.

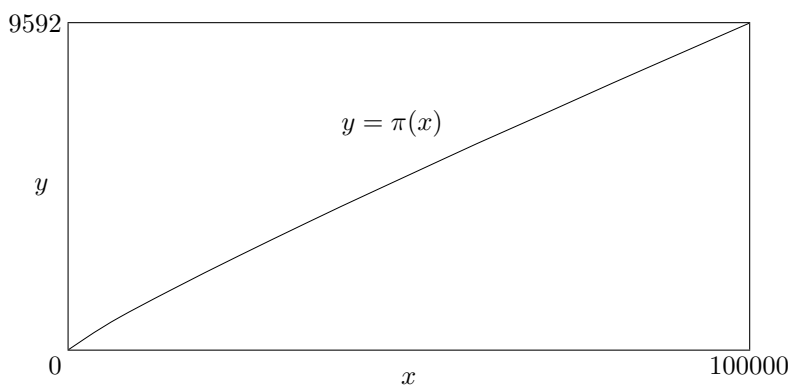
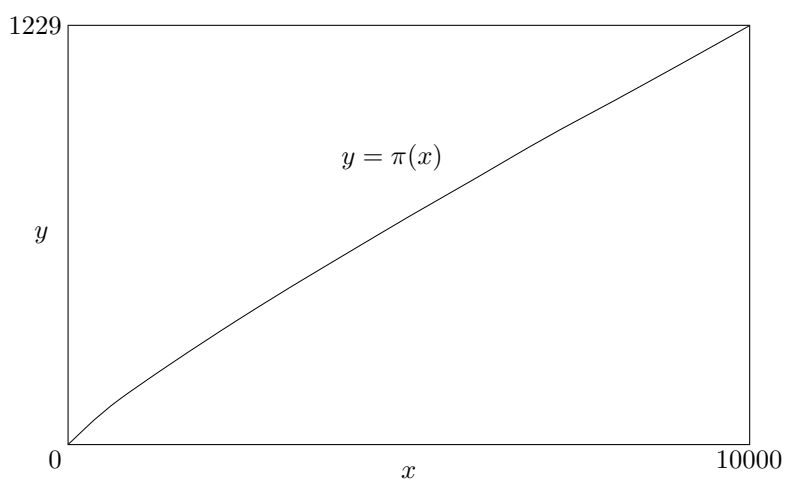
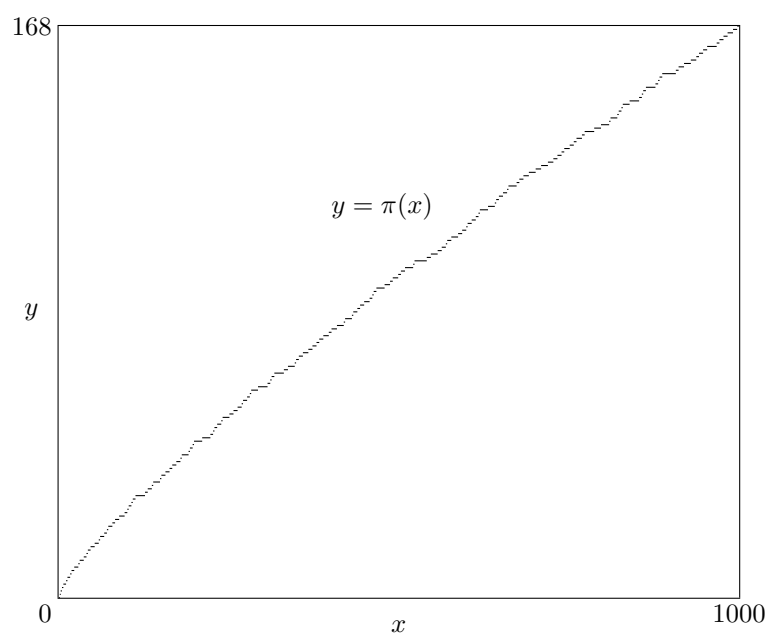


図 2: $\pi(x)$ のグラフ ($x \leq 1000, 10000, 100000$)

表 1: $x = 10^k$ ($k = 1, 2, \dots, 8$) に対する $\pi(x)$, $\text{Li}(x)$, $x/\log x$ の値

x	$\pi(x)$	$\text{Li}(x)$	$x/\log x$
10	4	5.12...	4.34...
100	25	29.08...	21.71...
1000	168	176.56...	144.76...
10000	1229	1245.09...	1085.73...
100000	9592	9628.76...	8685.88...
1000000	78498	78626.50...	72382.41...
10000000	664579	664917.35...	620420.68...
100000000	5761455	5762208.33...	5428681.02...

3.1 ガウスによる予想

1792 年, 当時 15 歳であったガウスは, その前年にもらった対数表の中の素数の表を調べるうちに実数 x の近辺のおおよそ $\log x$ 個に 1 個が素数であることに気づき, $\pi(x)$ は関数

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t}$$

と漸近的に等しいであろうという予想を立てた. これよりも少し精度は落ちるが, この予想は

$$(*) \quad \lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1$$

と書いてもよい. ガウスはその生涯に渡って素数の分布に興味を抱き続け, 膨大な計算を残している. また, ガウスよりも少し遅れて, ルジャンドルも 1798 年に出版された著書の中でほぼ同様の予想を述べている.

先のグラフに $x/\log x$ のグラフを重ねると図 3 (p. 11) のようになる.

3.2 整数が素数である “確率”

ガウスの予想は彼ならではの洞察力と計算力に基づくものであるが, 大胆な推論を許せば我々がその根拠を納得することも可能である. 以下, 多少怪しい議論をすることになるが, これはあくまで推測なので細かいことは気にしない.

いま, x を “十分大きい” 実数とし, $2 \leq m \leq x$ なる整数 m が素数である “確率” を求めることを考える.

p を素数とすると, 整数の列の中には p の倍数が $1/p$ の頻度で現れるから, 無作為に選ばれた整数が p の倍数でない “確率” は $1 - 1/p$ であると考えられる. 整数 $m \geq 2$ が素数であるとは,

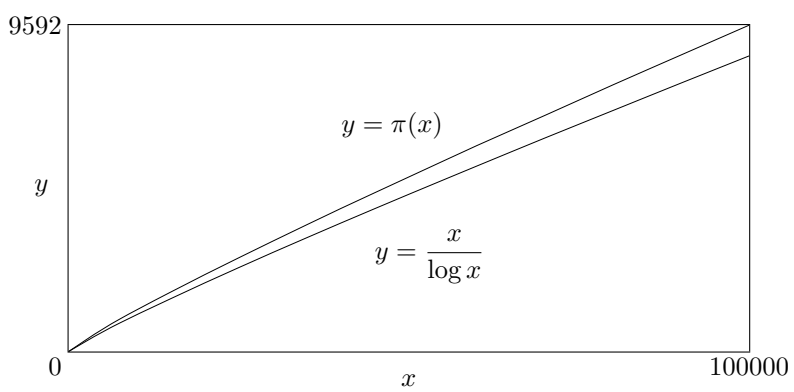
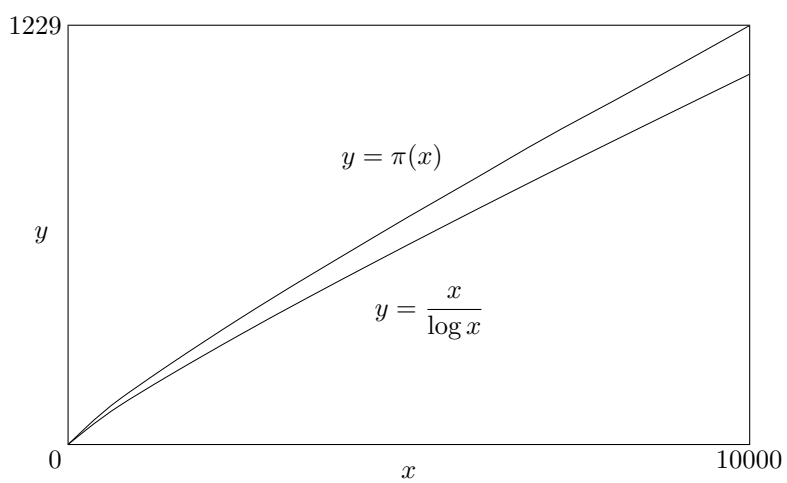
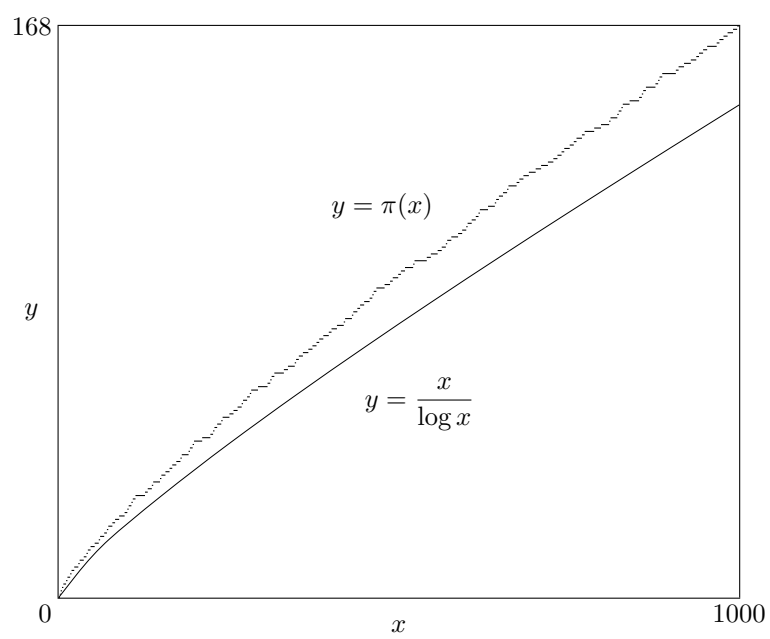


図 3: $\pi(x)$ と $\frac{x}{\log x}$ のグラフ ($x \leq 1000, 10000, 100000$)

m が $2 (= p_1)$ の倍数でなく, $3 (= p_2)$ の倍数でなく, $5 (= p_3)$ の倍数でなく, ... ということであるから, これらの事象が互いに独立であると仮定すると, m が素数である“確率”は

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \cdots = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \cdots$$

ということになる. ただし, いま考えているのは $m \leq x$ なる場合だから, 上の積において x より大きい素数 p に対しては $1 - 1/p$ を掛ける必要はない (m は x より大きい素数の倍数ではあり得ない). つまり, $n = \pi(x)$ とするとき, 求める“確率”は

$$\left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

であると考えることができる (この議論はエラトステネスの篩の考え方に他ならない).

ところで, 定理 2.2 の証明で述べたように

$$\left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n}\right)^{-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{[x]} + \text{etc.}$$

が成り立つが, この式において“etc.”の部分が無視できるほどに小さいと仮定してみる:

$$\left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n}\right)^{-1} \doteq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{[x]}.$$

ここで $\doteq$ は“ほぼ等しい”ということを意味する記号である. 補助定理 2.4 より, この式の右辺はほぼ $\log x$ に等しいことがわかるから,

$$\left(1 - \frac{1}{p_1}\right)^{-1} \left(1 - \frac{1}{p_2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n}\right)^{-1} \doteq \log x.$$

以上の議論により, $2 \leq m \leq x$ なる整数 m が素数である“確率”はおおよそ $1/\log x$ であるということができる. このことから

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

であることが推測される.

なお, m を x に“近い”整数に限定すると, 上の議論はより精密になる. すなわち, x に“近い”整数が素数である“確率”はほぼ $1/\log x$ であるということができる. このことから

$$\pi(x) \doteq \text{Li}(x)$$

であることが推測される. これがガウスの元々の予想であった.

以上の議論は必ずしも全てが正当化できる訳ではない. しかしながら, 表 2 (p. 13) を見る限りでは, あながち的外れともいえない.

表 2: “十分大きい” 実数の近辺における素数の割合と自然対数の逆数

範囲	素数の個数	素数の割合	範囲の上限の自然対数の逆数
10000 — 20000	1033	0.1033	$1/\log 20000 = 0.100974 \dots$
20000 — 30000	983	0.0983	$1/\log 30000 = 0.097003 \dots$
30000 — 40000	958	0.0958	$1/\log 40000 = 0.094369 \dots$
40000 — 50000	930	0.093	$1/\log 50000 = 0.092423 \dots$
50000 — 60000	924	0.0924	$1/\log 60000 = 0.090891 \dots$
60000 — 70000	878	0.0878	$1/\log 70000 = 0.089635 \dots$
70000 — 80000	902	0.0902	$1/\log 80000 = 0.088575 \dots$
80000 — 90000	876	0.0876	$1/\log 90000 = 0.087661 \dots$
90000 — 100000	879	0.0879	$1/\log 100000 = 0.086858 \dots$
100000 — 200000	8392	0.08392	$1/\log 200000 = 0.081926 \dots$
200000 — 300000	8013	0.08013	$1/\log 300000 = 0.079292 \dots$
300000 — 400000	7863	0.07863	$1/\log 400000 = 0.077524 \dots$
400000 — 500000	7678	0.07678	$1/\log 500000 = 0.076205 \dots$
500000 — 600000	7560	0.0756	$1/\log 600000 = 0.075161 \dots$
600000 — 700000	7445	0.07445	$1/\log 700000 = 0.074300 \dots$
700000 — 800000	7408	0.07408	$1/\log 800000 = 0.073570 \dots$
800000 — 900000	7323	0.07323	$1/\log 900000 = 0.072938 \dots$
900000 — 1000000	7224	0.07224	$1/\log 1000000 = 0.072382 \dots$
1000000 — 2000000	70435	0.070435	$1/\log 2000000 = 0.068924 \dots$
2000000 — 3000000	67883	0.067883	$1/\log 3000000 = 0.067050 \dots$
3000000 — 4000000	66330	0.06633	$1/\log 4000000 = 0.065781 \dots$
4000000 — 5000000	65367	0.065367	$1/\log 5000000 = 0.064830 \dots$
5000000 — 6000000	64336	0.064336	$1/\log 6000000 = 0.064072 \dots$
6000000 — 7000000	63799	0.063799	$1/\log 7000000 = 0.063446 \dots$
7000000 — 8000000	63129	0.063129	$1/\log 8000000 = 0.062913 \dots$
8000000 — 9000000	62712	0.062712	$1/\log 9000000 = 0.062450 \dots$
9000000 — 10000000	62090	0.06209	$1/\log 10000000 = 0.062042 \dots$

表 3: $m = 1, 2, \dots, 20$ に対する ${}_2mC_m$ の素因数分解

m	${}_2mC_m$ の素因数分解	m	${}_2mC_m$ の素因数分解
1	2	11	$2^3 \cdot 3 \cdot 7 \cdot 13 \cdot 17 \cdot 19$
2	$2 \cdot 3$	12	$2^2 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
3	$2^2 \cdot 5$	13	$2^3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19 \cdot 23$
4	$2 \cdot 5 \cdot 7$	14	$2^3 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19 \cdot 23$
5	$2^2 \cdot 3^2 \cdot 7$	15	$2^4 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
6	$2^2 \cdot 3 \cdot 7 \cdot 11$	16	$2 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$
7	$2^3 \cdot 3 \cdot 11 \cdot 13$	17	$2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 19 \cdot 23 \cdot 29 \cdot 31$
8	$2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13$	18	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 29 \cdot 31$
9	$2^2 \cdot 5 \cdot 11 \cdot 13 \cdot 17$	19	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 23 \cdot 29 \cdot 31 \cdot 37$
10	$2^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	20	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 31 \cdot 37$

§4 $\pi(x)$ と $x/\log x$ の比較

1850 年, チェビシエフは次の不等式を成り立たせるような正の定数 A と B が存在することを示した:

$$A \frac{x}{\log x} \leq \pi(x) \leq B \frac{x}{\log x} \quad (x \geq 2).$$

本節では, チェビシエフの考えを簡単な形にして,

$$A = \frac{\log 2}{4} = 0.17 \dots, \quad B = 8 \log 2 = 5.54 \dots$$

の場合に対する不等式の証明を述べる.

4.1 準備

チェビシエフのアイデアは, 二項係数

$${}_2mC_m = \frac{(2m)!}{(m!)^2} = \frac{(m+1)(m+2) \cdots (2m)}{1 \cdot 2 \cdots m}$$

の素因数分解の形に注目したという点にある.

定理 4.1 $m > 0$ を整数とし,

$${}_2mC_m = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots \quad (e_1, e_2, e_3, \dots \geq 0)$$

を二項係数 ${}_2C_m$ の素因数分解とする. このとき:

$$(i) p_n^{e_n} \leq 2m \quad (n = 1, 2, 3, \dots).$$

$$(ii) m < p_n \leq 2m \text{ ならば, } e_n = 1.$$

この定理を示すために, 補助定理をひとつ準備しておく.

補助定理 4.2 $l > 0$ を整数とし,

$$l! = p_1^{d_1} p_2^{d_2} p_3^{d_3} \cdots \quad (d_1, d_2, d_3, \dots \geq 0)$$

を l の階乗 $l!$ の素因数分解とする. このとき,

$$d_n = \left\lfloor \frac{l}{p_n} \right\rfloor + \left\lfloor \frac{l}{p_n^2} \right\rfloor + \left\lfloor \frac{l}{p_n^3} \right\rfloor + \cdots \quad (n = 1, 2, 3, \dots).$$

練習問題 4.3 $k = 1, 2, 3, \dots$ に対し, $1, 2, \dots, l$ の中には p_n^k の倍数がちょうど $\lfloor l/p_n^k \rfloor$ 個存在することをを用いて, 上の補助定理を証明せよ.

[定理 4.1 の証明] (i) ${}_2C_m = (2m)!/(m!)^2$ であるから, 上の補助定理より,

$$\begin{aligned} e_n &= \left(\left\lfloor \frac{2m}{p_n} \right\rfloor + \left\lfloor \frac{2m}{p_n^2} \right\rfloor + \left\lfloor \frac{2m}{p_n^3} \right\rfloor + \cdots \right) - 2 \left(\left\lfloor \frac{m}{p_n} \right\rfloor + \left\lfloor \frac{m}{p_n^2} \right\rfloor + \left\lfloor \frac{m}{p_n^3} \right\rfloor + \cdots \right) \\ &= \left(\left\lfloor \frac{2m}{p_n} \right\rfloor - 2 \left\lfloor \frac{m}{p_n} \right\rfloor \right) + \left(\left\lfloor \frac{2m}{p_n^2} \right\rfloor - 2 \left\lfloor \frac{m}{p_n^2} \right\rfloor \right) + \left(\left\lfloor \frac{2m}{p_n^3} \right\rfloor - 2 \left\lfloor \frac{m}{p_n^3} \right\rfloor \right) + \cdots. \end{aligned}$$

ここで, 各 $k = 1, 2, 3, \dots$ に対し,

$$\frac{2m}{p_n^k} - 1 < \left\lfloor \frac{2m}{p_n^k} \right\rfloor \leq \frac{2m}{p_n^k}, \quad \frac{m}{p_n^k} - 1 < \left\lfloor \frac{m}{p_n^k} \right\rfloor \leq \frac{m}{p_n^k}$$

より

$$-1 < \left\lfloor \frac{2m}{p_n^k} \right\rfloor - 2 \left\lfloor \frac{m}{p_n^k} \right\rfloor < 2$$

となることがわかるから,

$$\left\lfloor \frac{2m}{p_n^k} \right\rfloor - 2 \left\lfloor \frac{m}{p_n^k} \right\rfloor$$

(これは整数) は 0 または 1 になる. さらに, $k > \log(2m)/\log p_n$ (すなわち $2m < p_n^k$) ならば

$$\left\lfloor \frac{2m}{p_n^k} \right\rfloor = \left\lfloor \frac{m}{p_n^k} \right\rfloor = 0$$

であるから,

$$e_n \leq \frac{\log(2m)}{\log p_n}.$$

これより求める不等式を得る.

(ii) 容易.

(証明終わり)

また, 次の不等式も平易だが重要である:

補助定理 4.4 任意の整数 $m > 0$ に対し,

$$2^m \leq {}_{2m}C_m \leq 2^{2m}.$$

練習問題 4.5 上の補助定理を証明せよ.

4.2 $\pi(x)$ は $x/\log x$ より “大きい”

補助定理 4.6 任意の整数 $m > 0$ に対し,

$$\frac{\log 2}{2} \cdot \frac{2m}{\log(2m)} \leq \pi(2m).$$

[証明] $n = \pi(2m)$ と置く. このとき定理 4.1 の (i) より, ${}_{2m}C_m$ の素因数分解は

$${}_{2m}C_m = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \quad (e_1, e_2, \dots, e_n \geq 0)$$

なる形であることがわかる. 再び定理 4.1 の (i) より

$$p_1^{e_1} \leq 2m, \quad p_2^{e_2} \leq 2m, \quad \dots, \quad p_n^{e_n} \leq 2m$$

であるから,

$${}_{2m}C_m \leq (2m)^n.$$

これと補助定理 4.4 より,

$$2^m \leq (2m)^n.$$

この対数をとって

$$m \log 2 \leq n \log(2m)$$

を得る.

(証明終わり)

定理 4.7 任意の実数 $x \geq 2$ に対し,

$$\frac{\log 2}{4} \cdot \frac{x}{\log x} \leq \pi(x).$$

[証明] $2m \leq x < 2m + 2$ となるような整数 $m > 0$ をとると, 上の補助定理より,

$$\pi(x) \geq \pi(2m) \geq \frac{\log 2}{2} \cdot \frac{2m}{\log(2m)}.$$

ここで

$$2m \geq \frac{x}{2}, \quad \log(2m) \leq \log x$$

であるから,

$$\frac{\log 2}{2} \cdot \frac{2m}{\log(2m)} \geq \frac{\log 2}{2} \cdot \frac{x/2}{\log x} = \frac{\log 2}{4} \cdot \frac{x}{\log x}.$$

(証明終わり)

4.3 $\pi(x)$ は $x/\log x$ より “小さい”

補助定理 4.8 任意の整数 $m > 0$ に対し,

$$(\pi(2m) - \pi(m)) \log m \leq 2m \log 2.$$

[証明] $n = \pi(m)$, $n' = \pi(2m)$ と置く. $n = n'$ ならば上の不等式は明らかに成り立つから, 以下 $n < n'$ とする. このとき, 定理 4.1 の (ii) より,

$$p_{n+1} \mid {}_{2m}C_m, \quad p_{n+2} \mid {}_{2m}C_m, \quad \dots, \quad p_{n'} \mid {}_{2m}C_m.$$

従って

$$p_{n+1}p_{n+2} \cdots p_{n'} \mid {}_{2m}C_m$$

となり,

$$m^{n'-n} \leq p_{n+1}p_{n+2} \cdots p_{n'} \leq {}_{2m}C_m.$$

これと補助定理 4.4 より,

$$m^{n'-n} \leq 2^{2m}.$$

この対数をとって

$$(n' - n) \log m \leq 2m \log 2$$

を得る.

(証明終わり)

補助定理 4.9 任意の整数 $m > 0$ に対し,

$$\pi(2m) \log(2m) - \pi(m) \log m \leq 4m \log 2.$$

[証明] 上の補助定理より

$$\pi(2m) \log(2m) - \pi(m) \log m = (\pi(2m) - \pi(m)) \log m + \pi(2m) \log 2 \leq (2m + \pi(2m)) \log 2$$

となるが, 明らかに $\pi(2m) \leq 2m$ であるから $2m + \pi(2m) \leq 4m$ となり, 求める不等式が得られる.

(証明終わり)

補助定理 4.10 任意の整数 $l > 0$ に対し,

$$\pi(2^l) \leq 4 \log 2 \frac{2^l}{\log 2^l}.$$

[証明] 上の補助定理において $m = 1, 2, 4, \dots, 2^{l-1}$ とすると,

$$\begin{aligned}\pi(2) \log 2 - \pi(1) \log 1 &\leq 4 \cdot 1 \log 2, \\ \pi(4) \log 4 - \pi(2) \log 2 &\leq 4 \cdot 2 \log 2, \\ \pi(8) \log 8 - \pi(4) \log 4 &\leq 4 \cdot 4 \log 2, \\ &\dots\dots\dots, \\ \pi(2^l) \log 2^l - \pi(2^{l-1}) \log 2^{l-1} &\leq 4 \cdot 2^{l-1} \log 2.\end{aligned}$$

これより,

$$\pi(2^l) \log 2^l \leq 4(1 + 2 + 4 + \dots + 2^{l-1}) \log 2.$$

ここで

$$1 + 2 + 4 + \dots + 2^{l-1} = 2^l - 1 \leq 2^l$$

であるから,

$$\pi(2^l) \log 2^l \leq 4 \cdot 2^l \log 2.$$

(証明終わり)

定理 4.11 任意の実数 $x \geq 2$ に対し,

$$\pi(x) \leq 8 \log 2 \frac{x}{\log x}.$$

[証明] $2^{l-1} \leq x < 2^l$ となるような整数 $l > 0$ をとると, 上の補助定理より

$$\pi(x) \leq \pi(2^l) \leq 4 \log 2 \frac{2^l}{\log 2^l}.$$

ここで

$$2^l \leq 2x, \quad \log 2^l \geq \log x$$

であるから,

$$4 \log 2 \frac{2^l}{\log 2^l} \leq 4 \log 2 \frac{2x}{\log x} = 8 \log 2 \frac{x}{\log x}.$$

(証明終わり)

4.4 チェビシエフが示したこと

チェビシエフ自身は

$$A = \log \frac{2^{1/2} 3^{1/3} 5^{1/5}}{30^{1/30}} = 0.92 \dots, \quad B = \frac{6}{5} A = 1.10 \dots$$

の場合に対して、実数 x が “十分大きい” ならば不等式

$$A \frac{x}{\log x} \leq \pi(x) \leq B \frac{x}{\log x}$$

が成り立つことを証明した。同時に、極限

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x}$$

が存在するならば、その値は 1 でなければならないということも示している。

これらの結果は予想 (*) に対して十分な状況証拠を与えるが、チェビシェフのアイデアでは予想そのものを証明することはできない。

§5 そして素数定理へ

チェビシェフ以降の歴史をかいつまんで紹介しておく。

5.1 リーマンの研究

1859 年に発表されたリーマンの論文 “与えられた数より小さい素数の個数について” によって、素数分布の研究は飛躍的な進歩を遂げることになる。

リーマンはオイラーが研究した無限和

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

において s を複素数としたものを考え (s の実部が 1 より大きいならば、この無限和は収束する)、その性質を研究している。リーマンの業績にちなんで、この無限和はリーマンのゼータ関数と呼ばれる (“ゼータ関数” という名前は、リーマンがこの無限和をギリシア文字の ζ ^{ゼータ} を用いて $\zeta(s)$ と表したことに由来する)。

さらに、リーマンはゼータ関数を素数分布の研究に応用し、いくつかの作業仮設の下に関数 $\pi(x)$ を $\text{Li}(x)$ と $\zeta(s)$ を用いて正確に表す公式 (リーマンの明示公式) を得ている。

論文の標題からも推察されるようにリーマンの目標は予想 (*) の証明にあったと思われるが、リーマンの早世 (1866 年に 39 歳で死去) によりその目標は達成されなかった。

リーマンの作業仮設に厳密な証明をつける試みは既にリーマンの生存中に始まり、1895 年には明示公式も証明された。最後にただひとつ残った仮設はリーマン予想と呼ばれ、これは今日でも未解決である。リーマン予想の内容をここで述べることはしないが、その後の研究により、この予想は “ $\text{Li}(x)$ は $\pi(x)$ をどの程度近似しているか” という問題に密接に関係していることがわかっていく。

5.2 素数定理の証明

予想 (*) は 1896 年にアダマールとド・ラ・ヴァレ・プーサンによって独立に証明された:

定理 5.1 (素数定理)

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1.$$

彼らの与えた証明はいずれもリーマンが提供してきた道具と複素解析学 (複素数を変数とする微積分学) を駆使したものである.

また, 1949 年にはセルバーグとエルデスによって (これも独立に) この定理の “初等的” (ゼータ関数や複素解析学を用いないということ. “易しい” という意味ではない) な証明が与えられた. セルバーグは, この業績によって 1950 年に “数学のノーベル賞” と呼ばれるフィールズ賞を受けている.

付録 A 文献案内

本稿で扱った話題に関連する文献をいくつか紹介しておく (筆者が参考にした文献を全て挙げている訳ではない).

- [1] G. H. ハーディー・E. M. ライト (示野信一・矢神毅 訳), 数論入門 I・II, シュプリンガー数学クラシックス, 丸善出版, 2012 年.

世界中で広く読まれている整数論の古典の第 5 版 (1979 年刊) の邦訳. 原著初版は 1938 年刊.

- [2] 木田祐司・牧野潔夫, UBASIC によるコンピュータ整数論, 日本評論社, 1994 年.

関数 $\pi(x)$ を計算するアルゴリズムや素数判定法に詳しい. 本稿にある数値例の計算には木田氏作の UBASIC を用いた.

- [3] P. リーベンボイム (吾郷孝視 訳編), 素数の世界 その探索と発見 (第 2 版), 共立出版, 2001 年.

素数に関する色々な話題に詳しい. 原著初版は 1991 年刊.

- [4] H. ラーデマッヘル・O. テープリッツ (山崎三郎・鹿野健 訳), 数と図形, ちくま学芸文庫, 筑摩書房, 2010 年.

整数論や初等幾何学に関する様々なトピックが平易に述べられている. 原著初版は 1930 年刊だが, 古さを感じさせない.

- [5] 高木貞治, 初等整数論講義 (第 2 版), 共立出版, 1971 年.

1931 年刊の初版以来, 広く読まれている名著. 具体的な数値例の計算に詳しい.

[6] D. ザギエ (雨宮一郎 訳), 最初の五千万の素数, 数学セミナー 1985 年 8 月号, 日本評論社, pp. 38–48 (数学のたのしみ 28 (2001 年), 日本評論社, pp. 92–112 に再掲載).

1975 年にボン大学で行われた著者の就任講演. 本稿は, この論説から初学者向けの部分を抜粋したものに過ぎない.

付録 B 人名

ユークリッド (Euclid)	330?–275? B.C.
エラトステネス (Eratosthenes)	275–194 B.C.
オイラー (L. Euler)	1707–1783
ルジャンドル (A. M. Legendre)	1752–1833
ガウス (C. F. Gauss)	1777–1855
チェビシェフ (P. L. Chebyshev)	1821–1894
リーマン (G. F. B. Riemann)	1826–1866
アダマール (J. S. Hadamard)	1865–1963
ド・ラ・ヴァレ・プーサン (C. J. de la Vallée-Poussin)	1866–1962
エルデス (P. Erdős)	1913–1996
セルバーグ (A. Selberg)	1917–2007