

素数を調べる ―その多様な姿―

広島大学・大学院理学研究科数学専攻 高橋浩樹

素数 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ... は、定義の簡明さにもかかわらず、その多様な性質を解き明かすことが極めて難しい対象です。ある数学者はこんなことを言ったそうです。

「素数に関する問題であれば、どんな人であろうと最も賢明な数学者を悩ませる問題を簡単に作ることができる」

ここではそんな素数について、「代数」「幾何」「解析」の各方面から調べてみることにします。なお公開講座当日は、時間の都合上ここで紹介する話題を部分的に取り上げることになると思いますが、どうかご了承ください。

1 素数と代数

1.1 素数と合成数の定義

自然数の集合を

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots\}$$

と表します。今回の主役である**素数**とは、

「1 とその数自身以外に約数を持たない 1 より大きな自然数」

です。いくつかの自然数の約数を書き下してみると、

(2 の約数)	= {1, 2}
(3 の約数)	= {1, 3}
(4 の約数)	= {1, 2, 4}
(5 の約数)	= {1, 5}
(6 の約数)	= {1, 2, 3, 6}
(7 の約数)	= {1, 7}
(8 の約数)	= {1, 2, 4, 8}
(9 の約数)	= {1, 3, 9}
(10 の約数)	= {1, 2, 5, 10}
(11 の約数)	= {1, 11}
(12 の約数)	= {1, 2, 3, 4, 6, 12}
(13 の約数)	= {1, 13}
(14 の約数)	= {1, 2, 7, 14}
(15 の約数)	= {1, 3, 5, 15}
(16 の約数)	= {1, 2, 4, 8, 16}
(17 の約数)	= {1, 17}
(18 の約数)	= {1, 2, 3, 6, 9, 18}
(19 の約数)	= {1, 19}
(20 の約数)	= {1, 2, 4, 5, 10, 20}

となることから, 2, 3, 5, 7, 11, 13, 17, 19 が素数であることが分かります. 他方, 1 より大きな素数でない自然数は**合成数**と呼ばれます. 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 は合成数ということになります. 素数の集合を

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

と表しましょう.

1.2 エラトステネスのふるい

n 以下の合成数は, $\sqrt{n}$ 以下の素数を約数に持ちます. なぜならば, 合成数 n の素因数分解を

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \quad (e_i \geq 1)$$

($j < k$ のとき, $p_j < p_k$) とすると, n は合成数なので $e_1 + e_2 + \cdots + e_r \geq 2$ であり,

$$p_1^2 \leq p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = n \quad \text{より}$$

$$p_1 \leq \sqrt{n}$$

となるためです.

$n = 100$ とすると, n 以下の合成数は $\sqrt{n} = \sqrt{100} = 10$ 以下の素数, すなわち 2, 3, 5, 7 のいずれかを約数に持つことになります. これらの素数の倍数を除くと, 残るのは素数だけになります.

素数探し I

1	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													

素数探し II

1	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									

問 素数を探しやすかったのはどちらの表だったでしょうか?

1.3 m を法とした計算

m を 1 より大きな自然数とします. 整数 a, b に対して,

$$a \equiv b \pmod{m} \iff m \mid a - b \quad (m \text{ は } a - b \text{ を割り切る})$$

と定義します. 例えば, $10 \equiv 3 \pmod{7}$, $(-1) \equiv 6 \pmod{7}$ となります.

m を法とした計算を具体的に見ていきましょう. 例えば, $m = 7$ のとき, $i = 5$, $j = 1 \sim 6$ に対する掛け算 $i \times j$ は

$$\begin{aligned} 5 \times 1 &= 5 = 0 \times 7 + 5 \equiv 5 \pmod{7} \\ 5 \times 2 &= 10 = 1 \times 7 + 3 \equiv 3 \pmod{7} \\ 5 \times 3 &= 15 = 2 \times 7 + 1 \equiv 1 \pmod{7} \\ 5 \times 4 &= 20 = 2 \times 7 + 6 \equiv 6 \pmod{7} \\ 5 \times 5 &= 25 = 3 \times 7 + 4 \equiv 4 \pmod{7} \\ 5 \times 6 &= 30 = 4 \times 7 + 2 \equiv 2 \pmod{7} \end{aligned}$$

となります. また, $i = 5$, $j = 1 \sim 6$ に対する i^j は,

$$\begin{aligned} 5^1 &= 5 &= 0 \times 7 + 5 &\equiv 5 \pmod{7} \\ 5^2 &= 25 &= 3 \times 7 + 4 &\equiv 4 \pmod{7} \\ 5^3 &= 125 &= 17 \times 7 + 6 &\equiv 6 \pmod{7} \\ 5^4 &= 625 &= 89 \times 7 + 2 &\equiv 2 \pmod{7} \\ 5^5 &= 3125 &= 446 \times 7 + 3 &\equiv 3 \pmod{7} \\ 5^6 &= 15625 &= 2232 \times 7 + 1 &\equiv 1 \pmod{7} \end{aligned}$$

となります. この計算は i^j が大きくなると計算が大変になるので, 次のように計算することによって労力を減らしてみましょう.

$$\begin{aligned} 5^1 &= 5 \times 5^0 \equiv 5 \times 1 \equiv 5 \pmod{7} \\ 5^2 &= 5 \times 5^1 \equiv 5 \times 5 \equiv 4 \pmod{7} \\ 5^3 &= 5 \times 5^2 \equiv 5 \times 4 \equiv 6 \pmod{7} \\ 5^4 &= 5 \times 5^3 \equiv 5 \times 6 \equiv 2 \pmod{7} \\ 5^5 &= 5 \times 5^4 \equiv 5 \times 2 \equiv 3 \pmod{7} \\ 5^6 &= 5 \times 5^5 \equiv 5 \times 3 \equiv 1 \pmod{7} \end{aligned}$$

問 次のページに $m = 2 \sim 11$ を法とした $i \times j$ と i^j の計算リストを掲載しています. いくつかの空白があるので, それを埋めてください. また, m が素数である場合と合成数である場合でどんな違いがあるのでしょうか?

mを法としたi×jの計算リスト

$m = 2$

	1
1	1

$m = 3$

	1	2
1	1	2
2	2	1

$m = 4$

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$m = 5$

	1	2	3	4
1	1	2	3	4
2	2	4		3
3	3		4	2
4	4	3	2	1

$m = 6$

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

$m = 7$

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5		6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$m = 8$

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

$m = 9$

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

$m = 10$

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	4	6	8	0	2	4	6	8
3	3	6	9	2	5	8	1	4	7
4	4	8	2	6	0	4	8	2	6
5	5	0	5	0	5	0	5	0	5
6	6	2	8	4	0	6	2	8	4
7	7	4	1	8	5	2	9	6	3
8	8	6	4	2	0	8	6	4	2
9	9	8	7	6	5	4	3	2	1

$m = 11$

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8		9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

mを法としたiの計算リスト

$m = 2$

i	i^1
1	1

$m = 3$

i	i^1	i^2
1	1	1
2	2	1

$m = 4$

i	i^1	i^2	i^3
1	1	1	1
2	2	0	0
3	3	1	3

$m = 5$

i	i^1	i^2	i^3	i^4
1	1	1	1	1
2	2	4		1
3	3	4	2	1
4	4	1	4	1

$m = 6$

i	i^1	i^2	i^3	i^4	i^5
1	1	1	1	1	1
2	2	4	2	4	2
3	3	3	3	3	3
4	4	4	4	4	4
5	5	1	5	1	5

$m = 7$

i	i^1	i^2	i^3	i^4	i^5	i^6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

$m = 8$

i	i^1	i^2	i^3	i^4	i^5	i^6	i^7
1	1	1	1	1	1	1	1
2	2	4	0	0	0	0	0
3	3	1	3	1	3	1	3
4	4	0	0	0	0	0	0
5	5	1	5	1	5	1	5
6	6	4	0	0	0	0	0
7	7	1	7	1	7	1	7

$m = 9$

i	i^1	i^2	i^3	i^4	i^5	i^6	i^7	i^8
1	1	1	1	1	1	1	1	1
2	2	4	8	7	5	1	2	4
3	3	0	0	0	0	0	0	0
4	4	7	1	4	7	1	4	7
5	5	7	8	4	2	1	5	7
6	6	0	0	0	0	0	0	0
7	7	4	1	7	4	1	7	4
8	8	1	8	1	8	1	8	1

$m = 10$

i	i^1	i^2	i^3	i^4	i^5	i^6	i^7	i^8	i^9
1	1	1	1	1	1	1	1	1	1
2	2	4	8	6	2	4	8	6	2
3	3	9	7	1	3	9	7	1	3
4	4	6	4	6	4	6	4	6	4
5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6
7	7	9	3	1	7	9	3	1	7
8	8	4	2	6	8	4		6	8
9	9	1	9	1	9	1	9	1	9

$m = 11$

i	i^1	i^2	i^3	i^4	i^5	i^6	i^7	i^8	i^9	i^{10}
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9		5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

1.4 素数の無限性（ユークリッド『原論』）

ユークリッドが編纂した『原論』の第 IX 巻の命題 20 では、素数が無限に存在することを示しています。

「素数の個数はいかなる定められた素数の個数よりも多い」

原証明 A, B, C を素数とし、 $N = ABC + 1$ とする。 N が素数であれば、 A, B, C とは異なる素数が新たに 1 つ見つかったことになる。 N が合成数であれば、ある素数 P は N を割り切るが、 P は A, B, C とは異なる素数であることを主張する。なぜならば、もし P が A, B, C のいずれかと同じであれば、 A, B, C は $N - 1$ を割り切るので、 P も $N - 1$ を割り切る。これは不合理である。（ P は N と $N - 1$ を割り切ることになり、そのような自然数は 1 だけである。） Q.E.D.

原証明では 3 つの素数で説明されています。一般的には、定められた素数を全て掛け合わせた数に 1 を足すと、その数あるいはその数の素因数から新たな素数を見つけることができます。

ユークリッドの方法による素数探し

『原論』の証明の手順に従って、実際に素数を探してみましょう。ただし、 N の素因数 P は最小のものを選ぶことにします。最初の素数は $q_1 = 2$ とします。

$$\begin{aligned} N_1 &= q_1 + 1 = 3 \implies q_2 = 3 \\ N_2 &= q_1 q_2 + 1 = 7 \implies q_3 = 7 \\ N_3 &= q_1 q_2 q_3 + 1 = 43 \implies q_4 = 43 \\ N_4 &= q_1 q_2 q_3 q_4 + 1 = 1807 \implies q_5 = ? \end{aligned}$$

問 素数 q_5 は何でしょうか？（ヒント：20 以下の素数です。）

$N = ABC - 1$ として探してみましょう。最初の素数は $q'_1 = 3$ とします。

$$\begin{aligned} N_1 &= q'_1 - 1 = 2 \implies q'_2 = 2 \\ N_2 &= q'_1 q'_2 - 1 = 5 \implies q'_3 = 5 \\ N_3 &= q'_1 q'_2 q'_3 - 1 = 29 \implies q'_4 = 29 \\ N_4 &= q'_1 q'_2 q'_3 q'_4 - 1 = 869 \implies q'_5 = ? \end{aligned}$$

問 素数 q'_5 は何でしょうか？（ヒント：20 以下の素数です。）

1.5 有名な素数の探索

フェルマー素数

$2^m + 1$ という形の素数は、**フェルマー素数**と呼ばれます。このとき指数 m は 2^n の形である必要があります。(ヒント: 奇数 l に対し, $x^l + 1 = (x + 1)(x^{l-1} - x^{l-2} + \cdots - x + 1)$)

$F_n = 2^{2^n} + 1$ は n 番目のフェルマー数と呼ばれます。 $F_0 = 2^1 + 1 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65537$ は素数ですが,

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$$

となり合成数です。上記の 5 つの素数以外のフェルマー素数は知られていません。

メルセンヌ素数

$2^m - 1$ という形の素数は、**メルセンヌ素数**と呼ばれます。このとき指数 m は素数 p である必要があります。(ヒント: $x^l - 1 = (x - 1)(x^{l-1} + x^{l-2} + \cdots + x + 1)$)

2010 年 6 月の時点で、47 個のメルセンヌ素数 $M_p = 2^p - 1$ が知られています。具体的には、 $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609$ に対する M_p です。 $p = 43112609$ に対するメルセンヌ素数は,

$$M_{43112609} = 2^{43112609} - 1 = 316470269 \cdots 697152511$$

という約 1300 万桁の巨大素数です。

双子素数

p と $p + 2$ が共に素数となる組のことです。 $(3, 5)$, $(5, 7)$, $(11, 13)$ などがあります。現時点で知られている最大の**双子素数**は,

$$(65516468355 \times 2^{333333} - 1, 65516468355 \times 2^{333333} + 1)$$

という約 10 万桁の素数の組です。

三つ子素数

p , $p + 2$, $p + 4$ が全て素数となる三つ組は $(3, 5, 7)$ に限られます。(3 つの数のいずれかが 3 の倍数となるため) 一方, p , $p + 2$, $p + 6$ または p , $p + 4$, $p + 6$ が全て素数となる三つ組は, $(5, 7, 11)$, $(7, 11, 13)$, $(11, 13, 17)$ などがあります。

現時点で知られている最大の**三つ子素数**は,

$$(2072644824759 \times 2^{33333} - 1, 2072644824759 \times 2^{33333} + 1, 2072644824759 \times 2^{33333} + 5)$$

という約 1 万桁の素数の組です。

2 素数と幾何

2.1 素数の表現

●

●●

●●●

●●
●●

●●●●●

●●●
●●●

●●●●●●●●

●●●●
●●●●

●●●
●●●
●●●

●●●●●
●●●●●

●●●●●●●●●●●●●●

●●●●
●●●●
●●●●

●●●●●●●●●●●●●●●●

●●●●●●●●
●●●●●●●●

●●●●●
●●●●●
●●●●●

●●●●
●●●●
●●●●
●●●●

●●●●●●●●●●●●●●●●●●

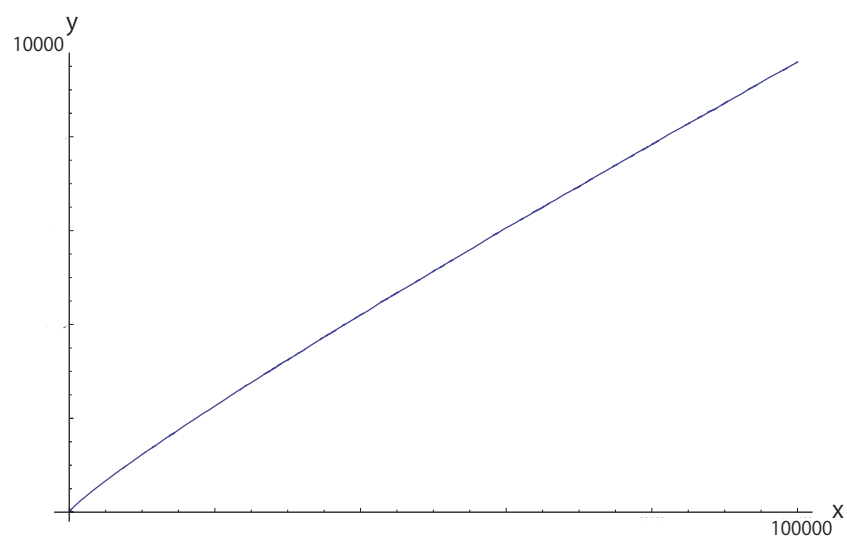
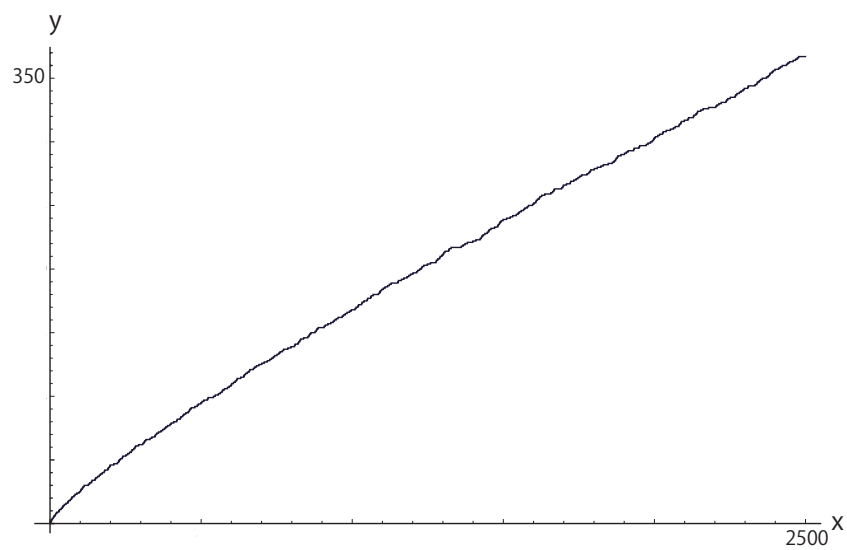
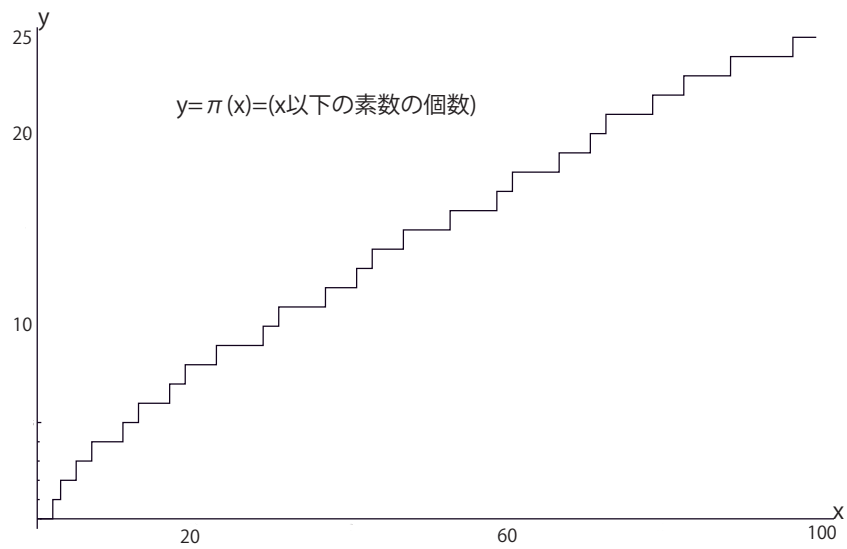
●●●●●●
●●●●●●
●●●●●●

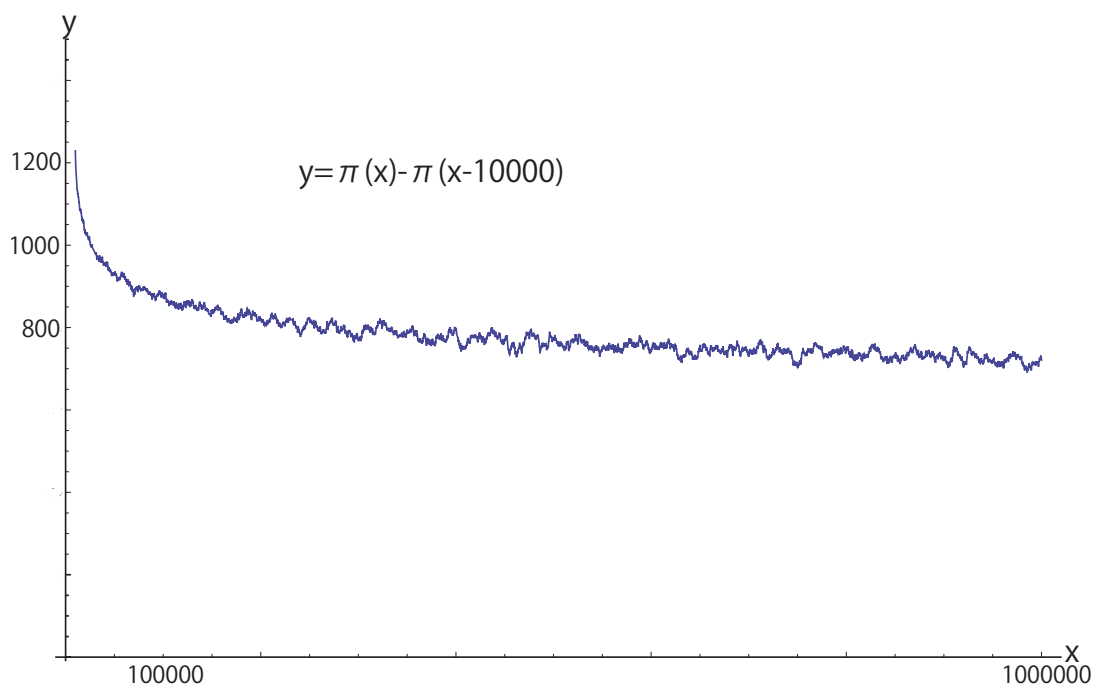
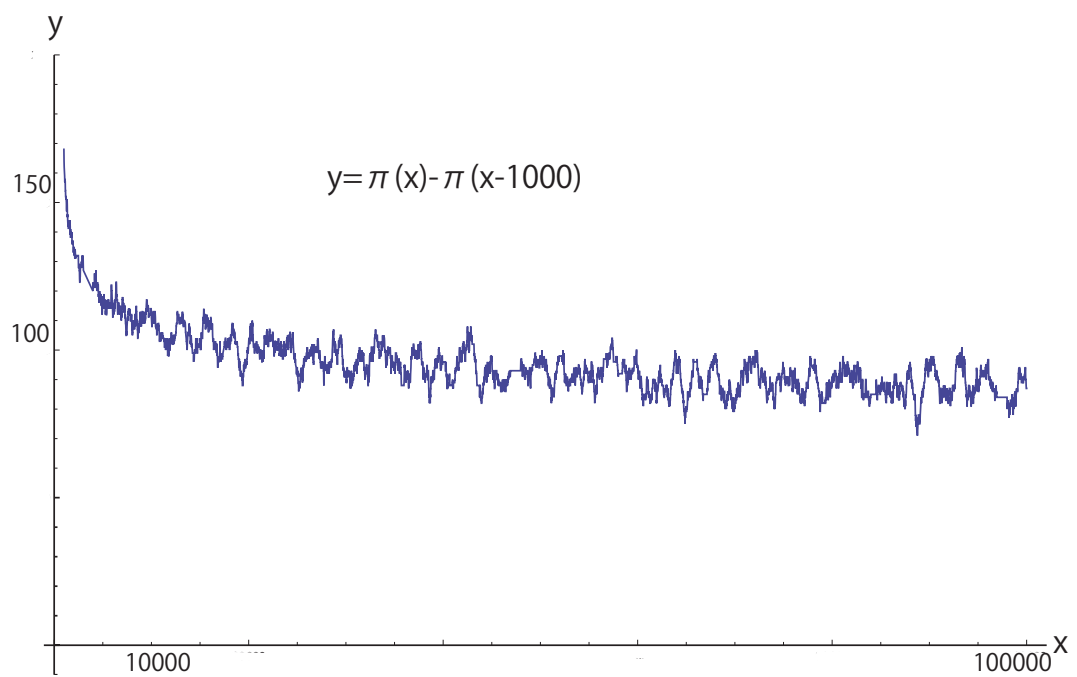
●●●●●●●●●●●●●●●●●●

●●●●●
●●●●●
●●●●●
●●●●●

●●
●●●
●●●●
●●●●●
●●●●●●
●●●●●●●
●●●●●●●●
●●●●●●●●●
●●●●●●●●●●
●●●●●●●●●●●
●●●●●●●●●●●●

2.2 素数のグラフ





問 素数の個数の増え方には、どのような法則がありそうでしょうか？

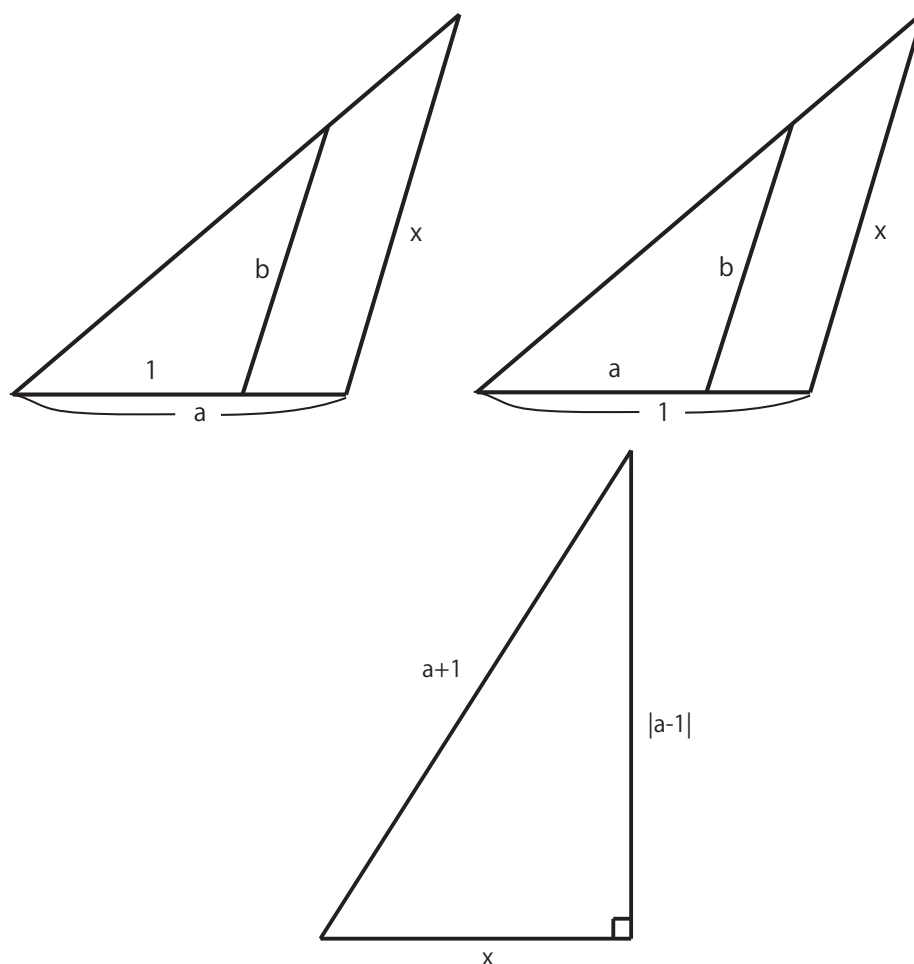
2.3 フェルマー素数と作図

1796年3月30日の朝、19歳のガウスが目覚めたとき、正17角形の作図の方法がひらめいたそうです。一般的に述べると、以下ようになります。

「 p を素数とする。 p がフェルマー素数であるときに限り、正 p 角形は定木とコンパスで作図可能である。」

フェルマー素数 $2^{2^n} + 1$ の 2 と $\sqrt{a} = a^{1/2}$ の 2 が関係しています。

問 以下の図の x は, a, b を用いてどのように表せるでしょうか？



$p = F_0 = 2^{2^0} + 1 = 3$ のとき,

$$\cos \frac{2\pi}{p} = -\frac{1}{2}.$$

$p = F_1 = 2^{2^1} + 1 = 5$ のとき,

$$\cos \frac{2\pi}{p} = \frac{-1 + \sqrt{p}}{4}.$$

$p = F_2 = 2^{2^2} + 1 = 17$ のとき,

$$\cos \frac{2\pi}{p} = \frac{-1 + \sqrt{p} + \sqrt{2p - 2\sqrt{p}} + 2\sqrt{p + 3\sqrt{p} - \sqrt{2p - 2\sqrt{p}} - 2\sqrt{2p + 2\sqrt{p}}}}{16}.$$

3 素数と解析

素数の集合 $\mathbf{P}$ の中で小さい方から i 番目の素数を p_i と名付けましょう. すると, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$, $p_{10} = 29$, $\dots$ となります.

3.1 素数の無限性 (オイラー)

$$S_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots + \frac{1}{n-1} + \frac{1}{n}$$

について調べましょう.

$$\frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^k+2^k} \geq 2^k \cdot \frac{1}{2^k+2^k} = \frac{1}{2}$$

となることに注意すると,

$$\begin{aligned} S_{2^m} &= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \dots + \left(\frac{1}{2^{m-1}+1} + \dots + \frac{1}{2^m}\right) \\ &\geq 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots + \frac{1}{2} = 1 + \frac{1}{2} \cdot m \end{aligned}$$

より, $n \rightarrow \infty$ のとき $S_n \rightarrow \infty$ となることが分かります.

前章で登場した興味深い関数

$$\pi(x) = (x \text{ 以下の素数の個数})$$

を S_n を用いて調べてみましょう. n 以下の自然数の最大の素因数は $p_{\pi(n)}$ であることに注意すると,

$$\begin{aligned} S_n &= 1 + \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_1^2} + \frac{1}{p_3} + \frac{1}{p_1 p_2} + \dots + \frac{1}{p_{\pi(n)}} + \dots + \frac{1}{n} \\ &< \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \frac{1}{p_1^4} + \frac{1}{p_1^5} + \dots\right) \\ &\quad \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \frac{1}{p_2^3} + \frac{1}{p_2^4} + \frac{1}{p_2^5} + \dots\right) \\ &\quad \dots\dots\dots \\ &\quad \left(1 + \frac{1}{p_{\pi(n)}} + \frac{1}{p_{\pi(n)}^2} + \frac{1}{p_{\pi(n)}^3} + \frac{1}{p_{\pi(n)}^4} + \dots\right) \\ &= \frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}} \cdot \frac{1}{1 - \frac{1}{p_3}} \cdot \dots \cdot \frac{1}{1 - \frac{1}{p_{\pi(n)}}} \\ &= \prod_{i=1}^{\pi(n)} \frac{1}{1 - \frac{1}{p_i}} \end{aligned}$$

という不等式が成立します. n を大きくすると, S_n はいくらでも大きくなるので, $\pi(n)$ も同様にいくらでも大きくなる必要があります. なぜならば, もし $\pi(n)$ が有界であったとすると, 最後の積は十分大きな n ではある一定の値になってしまうからです. 以上により, 素数は無限個存在することが示せました. (ずいぶんまわりくどい証明に思いませんか?)

3.2 リーマンゼータ関数

次の**リーマンゼータ関数**は、 S_n の極限を発展させたものといえるでしょう。

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \cdots + \frac{1}{n^x} + \cdots \quad (x > 1)$$

自然数の**素因数分解の一意性**により、自然数 n は

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_r^{e_r} \cdots \quad (e_i \geq 0)$$

という形に一意的に表されます。有限個の i を除いて $e_i = 0$ となります。ここで

$$\frac{1}{n^x} = \frac{1}{(p_1^{e_1})^x (p_2^{e_2})^x (p_3^{e_3})^x \cdots (p_r^{e_r})^x \cdots} = \frac{1}{(p_1^x)^{e_1}} \frac{1}{(p_2^x)^{e_2}} \cdots \frac{1}{(p_r^x)^{e_r}} \cdots$$

となることに注意すると、リーマンゼータ関数が以下のような関数たちの無限積で表されることが分かります。

$$\begin{aligned} \zeta(x) &= \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \cdots + \frac{1}{n^x} + \cdots \\ &= \left(\frac{1}{(2^x)^0} + \frac{1}{(2^x)^1} + \frac{1}{(2^x)^2} + \frac{1}{(2^x)^3} + \frac{1}{(2^x)^4} + \frac{1}{(2^x)^5} + \cdots \right) \\ &\quad \left(\frac{1}{(3^x)^0} + \frac{1}{(3^x)^1} + \frac{1}{(3^x)^2} + \frac{1}{(3^x)^3} + \frac{1}{(3^x)^4} + \frac{1}{(3^x)^5} + \cdots \right) \\ &\quad \left(\frac{1}{(5^x)^0} + \frac{1}{(5^x)^1} + \frac{1}{(5^x)^2} + \frac{1}{(5^x)^3} + \frac{1}{(5^x)^4} + \frac{1}{(5^x)^5} + \cdots \right) \\ &\quad \left(\frac{1}{(7^x)^0} + \frac{1}{(7^x)^1} + \frac{1}{(7^x)^2} + \frac{1}{(7^x)^3} + \frac{1}{(7^x)^4} + \frac{1}{(7^x)^5} + \cdots \right) \\ &\quad \left(\frac{1}{(11^x)^0} + \frac{1}{(11^x)^1} + \frac{1}{(11^x)^2} + \frac{1}{(11^x)^3} + \frac{1}{(11^x)^4} + \frac{1}{(11^x)^5} + \cdots \right) \\ &\quad \cdots \cdots \\ &= \prod_{p:\text{素数}} \frac{1}{1 - \frac{1}{p^x}} = \prod_{p:\text{素数}} \frac{p^x}{p^x - 1}. \end{aligned}$$

このリーマンゼータ関数の表示を**オイラー積**表示といいます。素数たちが作る関数が協力しあって、ゼータ関数を構成しているわけです。

前節での素数の無限性の証明では、 $n \rightarrow \infty$ とすると $S_n \rightarrow \infty$ となることが利用されました。これをリーマンゼータ関数の言葉に翻訳すると、 $x \rightarrow 1 + 0$ とすると $\zeta(x) \rightarrow \infty$ となることに対応します。

リーマンゼータ関数の他にもさまざまなゼータ関数が発見されており、多くのゼータ関数が歴代の数論研究者たちを魅了し悩ませ続けてきました。有意義に解決すれば賞金 100 万ドルが手に入ること有名なクレイ数学研究所の 7 つのミレニアム問題のうちの 2 つは、このゼータ関数に関する問題です。**リーマン予想**はリーマンゼータ関数の零点に関する予想、**BSD 予想**は楕円曲線のゼータ関数の $x = 1$ での振る舞いに関する予想です。

リーマン予想を説明するためには、リーマンゼータ関数を**複素関数**に拡張する必要があります。

まず、実関数 p^x を複素関数 p^{x+iy} に拡張しましょう。大学1年生で学ぶ指数関数、三角関数の**マクローリン展開**：

$$\begin{aligned} e^x &= \frac{x^0}{0!} + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!} \\ \cos x &= \frac{x^0}{0!} - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \frac{x^8}{8!} - \frac{x^{10}}{10!} + \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)!} \\ \sin x &= \frac{x^1}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \frac{x^9}{9!} - \frac{x^{11}}{11!} + \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!} \end{aligned}$$

を用いて、 e^x , $\cos x$, $\sin x$ を複素関数に“自然に”拡張することができます。すなわち両辺の x を複素数 $z = x + iy$ に置き換えるのです。こうすると、

$$e^z = e^{x+iy} = e^x e^{iy} = e^x (\cos y + i \sin y)$$

が成立します。特に $z = 0 + iy$ のとき、

オイラーの公式 $e^{iy} = \cos y + i \sin y.$

さらに $y = \pi$ とすると、

オイラーの等式 $e^{i\pi} = -1 + i \cdot 0 \iff e^{i\pi} + 1 = 0$

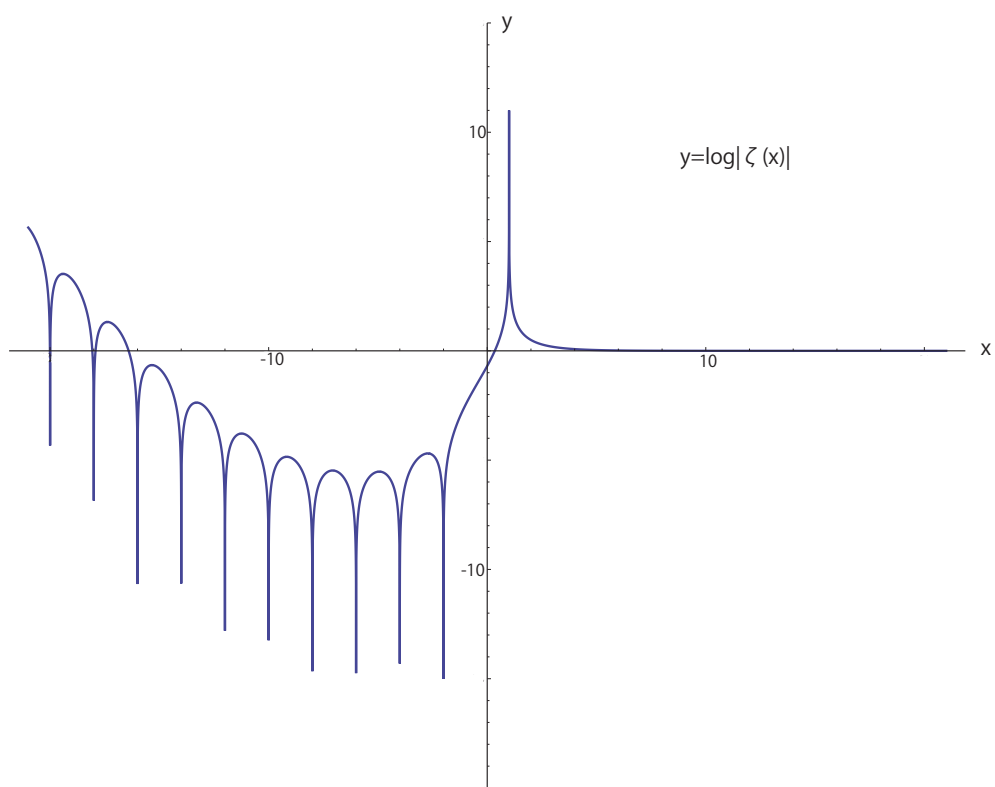
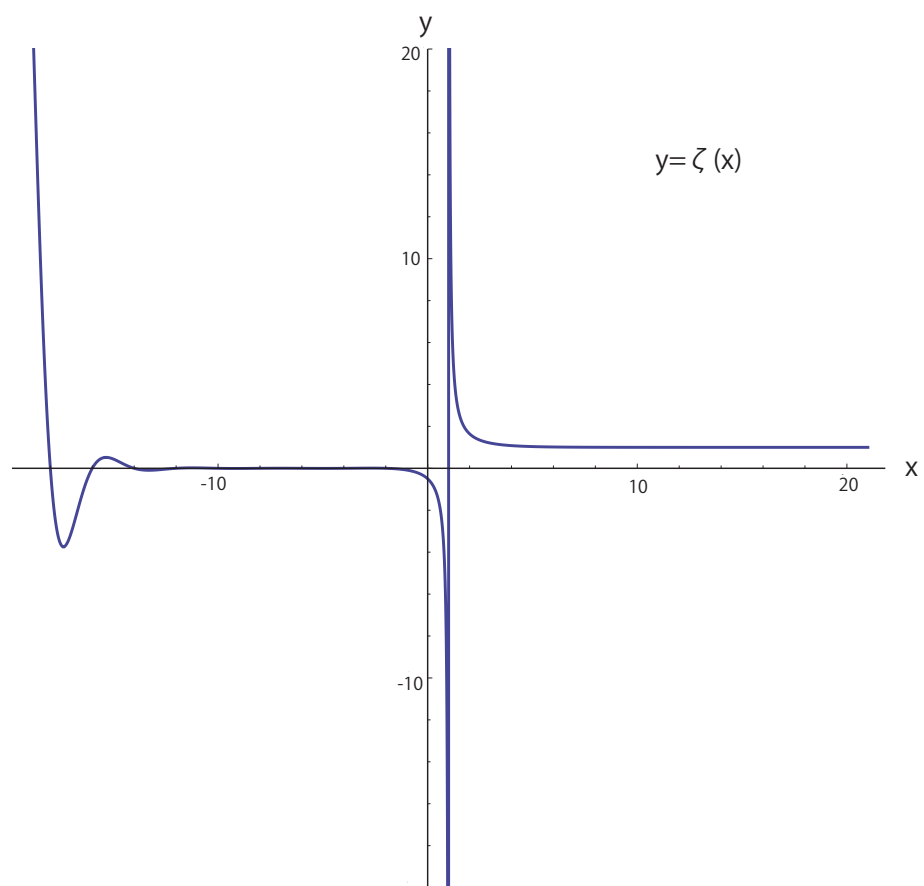
が成立します。そこで

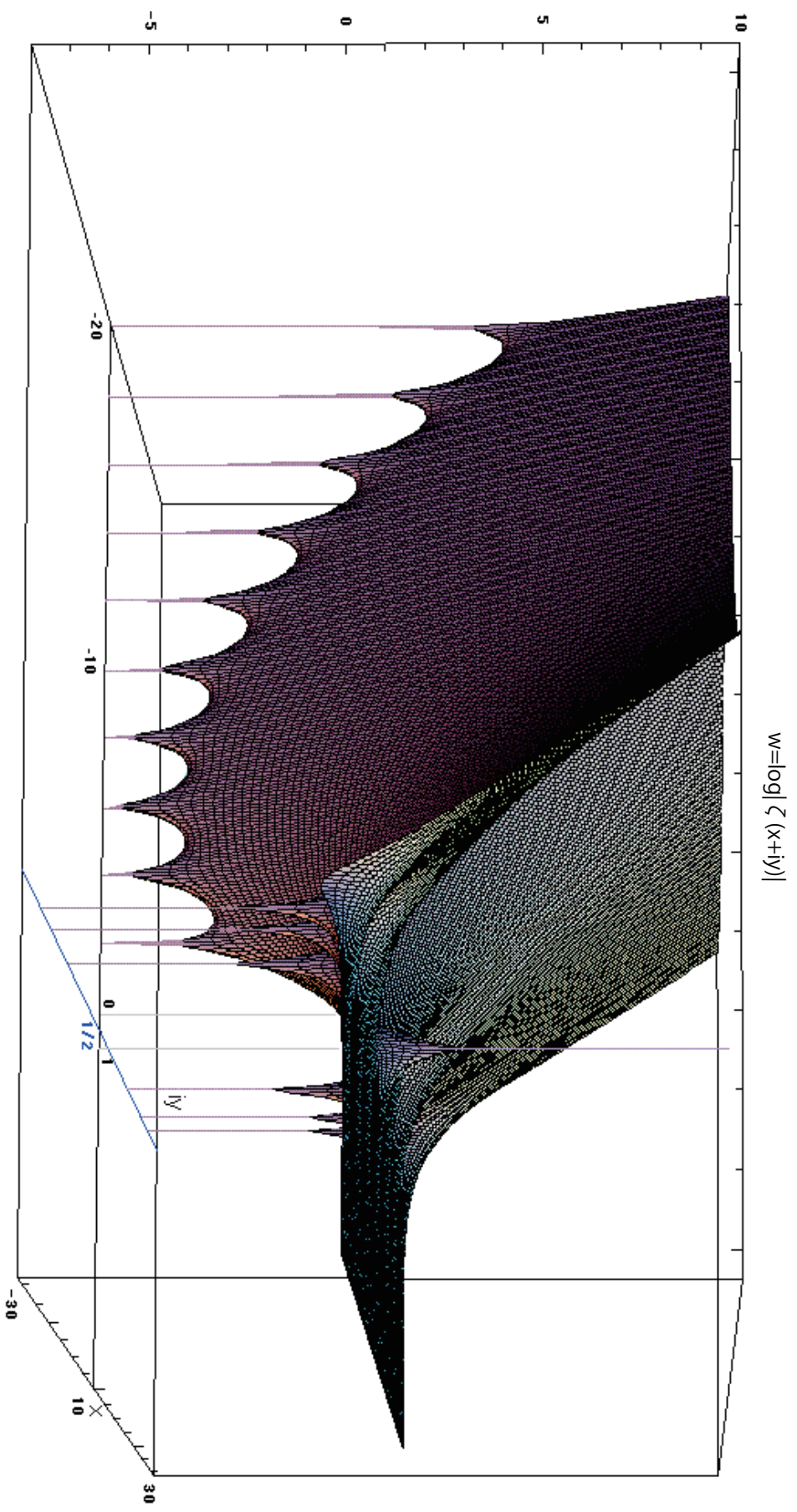
$$\begin{aligned} p^{x+iy} &= (e^{\log p})^{x+iy} \\ &= e^{(\log p)x + i(\log p)y} = e^{(\log p)x} e^{i(\log p)y} \\ &= e^{(\log p)x} \{ \cos((\log p)y) + i \sin((\log p)y) \} \end{aligned}$$

と定義することにより、リーマンゼータ関数の定義域は複素変数 $z = x + iy$ ($x > 1$) にまで広がることになります。($x > 1$ のときには、無限和が収束するため)

さらに $x \leq 1$ となる複素数もリーマンゼータ関数の定義域に含めるようにできます。これは、数学の専門科目「複素関数論」で学ぶ解析接続と呼ばれる関数の“自然な”拡張によるものです。すなわち、複素数 z について微分可能であるような滑らかな関数に解析的に接続するというものです。上記のテイラー展開による関数の拡張は、解析接続のひとつの方法です。こうしてリーマンゼータ関数の定義域は、 $z = 1$ を除く全ての複素数にまで広がることになります。

次ページに、リーマンゼータ関数の3つのグラフ（実関数、実関数の対数グラフ、複素関数の対数グラフ）を掲載しています。一目見て、ゼータ関数が奇妙な性質を持っていることが分かるでしょうか？





3.3 リーマン予想

前ページのグラフでは、リーマンゼータ関数の零点（対数グラフでは関数の値が $-\infty$ となる z ）は、実数軸における負の偶数と直線 $x = \frac{1}{2}$ 上にあるように見えます。前者はリーマンゼータ関数の自明な零点、それ以外の零点は非自明な零点と呼ばれています。

リーマン予想 $\zeta(s)$ の全ての非自明な零点は、直線 $x = \frac{1}{2}$ 上にある。

実はこの予想は、リーマンが $\pi(x)$ がどのような関数で近似されるかを研究している際に考察したことです。リーマンが示そうとした

素数定理

$$\pi(x) \sim \int_2^x \frac{dt}{\log t}$$

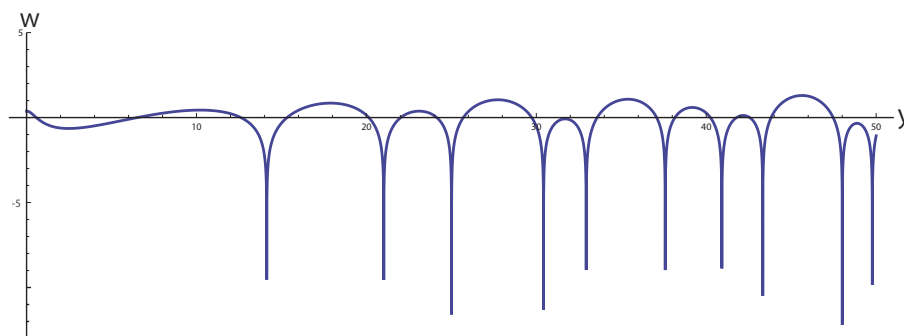
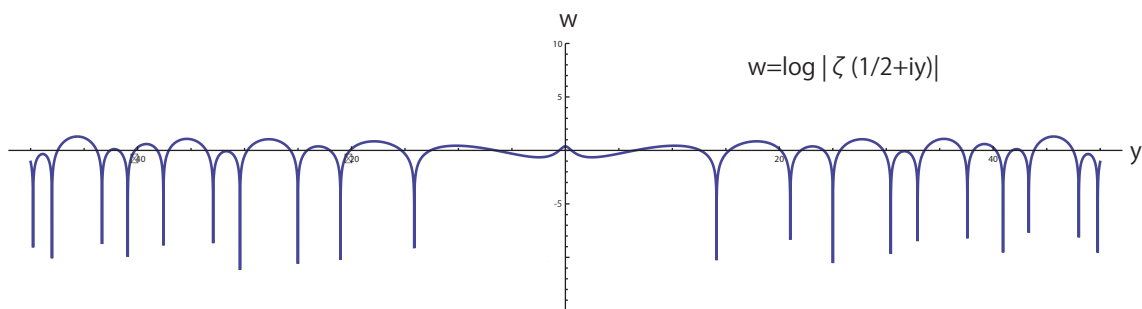
は、リーマン予想より弱い事実（非自明な零点は直線 $x = 1$ 上にない）から導けることが分かり、素数定理はアダマールとプーサンによって証明されました。なお、 $f(x) \sim g(x)$ は、「 $x \rightarrow \infty$ のとき、 $\frac{f(x)}{g(x)} \rightarrow 1$ 」という記号です。

もしリーマン予想が正しいならば、次のような $\pi(x)$ の究極の近似等式が得られることになるのです。

$\pi(x)$ の予想

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(\sqrt{x} \log x).$$

なお、 $f(x) = g(x) + O(h(x))$ は、「 $x \rightarrow \infty$ のとき、 $\frac{f(x) - g(x)}{h(x)}$ が有界である」という記号です。実はこの予想は、リーマン予想と同値であることが知られています。



3.4 リーマンゼータ値

フェルマーの最終定理 $x^n + y^n = z^n$, x, y, z, n : 整数, $n > 2$ ならば, $xyz = 0$.

1994年9月19日プリンストン大学のワイルズは、フェルマーの最終定理の証明の最後の一步を思いもかけず閃光のようにひらめきました。それは、ワイルズがメイザーとともにリーマンゼータ値の分子の謎を解明した約10年後のことでした。実は、この謎解きがあったからこそ、あの輝かしい成功があったと言えるのです。ここでは、そのリーマンゼータ値の分子の謎について紹介しましょう。

$$\begin{aligned}
 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} \text{ etc.} &= \frac{p^2}{6} = P \\
 1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \frac{1}{5^4} \text{ etc.} &= \frac{p^4}{96} = Q \\
 1 + \frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{4^6} + \frac{1}{5^6} \text{ etc.} &= \frac{p^6}{945} = R \\
 1 + \frac{1}{2^8} + \frac{1}{3^8} + \frac{1}{4^8} + \frac{1}{5^8} \text{ etc.} &= \frac{p^8}{9450} = S \\
 1 + \frac{1}{2^{10}} + \frac{1}{3^{10}} + \frac{1}{4^{10}} + \frac{1}{5^{10}} \text{ etc.} &= \frac{p^{10}}{93555} = T \\
 1 + \frac{1}{2^{12}} + \frac{1}{3^{12}} + \frac{1}{4^{12}} + \frac{1}{5^{12}} \text{ etc.} &= \frac{691 p^{12}}{6425 \cdot 93555} = V.
 \end{aligned}$$

オイラーによるゼータ値の計算 (1735 年頃)

リーマンゼータ値 k : 正の偶数 $\zeta(k) = \frac{2^{k-1}}{k!} |B_k| \pi^k$, $\zeta(1-k) = -\frac{B_k}{k}$.

ベルヌーイ数

$$\begin{aligned}
 B_0 &= 1 & B_1 &= \frac{1}{2} & B_2 &= \frac{1}{6} & B_4 &= -\frac{1}{30} & B_6 &= \frac{1}{42} & B_8 &= -\frac{1}{30} & B_{10} &= \frac{5}{66} \\
 B_{12} &= -\frac{691}{2730} & B_{14} &= \frac{7}{6} & B_{16} &= -\frac{3617}{510} & B_{18} &= \frac{43867}{798} & B_{20} &= -\frac{174611}{330} \\
 B_{22} &= \frac{854513}{138} & B_{24} &= -\frac{236364091}{2730} & B_{26} &= \frac{8553103}{6} & B_{28} &= -\frac{23749461029}{870} \\
 B_{30} &= \frac{8615841276005}{14322} & B_{32} &= -\frac{7709321041217}{510} & B_{34} &= \frac{2577687858367}{6} \\
 B_{36} &= -\frac{26315271553053477373}{1919190} & B_{38} &= \frac{2929993913841559}{6} \\
 B_{40} &= -\frac{261082718496449122051}{13530} & B_{42} &= \frac{1520097643918070802691}{1806} \\
 B_{44} &= -\frac{27833269579301024235023}{690} & B_{46} &= \frac{596451111593912163277961}{282} \\
 B_{48} &= -\frac{5609403368997817686249127547}{46410} & B_{2k+1} &= 0 \quad (k \geq 1)
 \end{aligned}$$

以下のリストから分かるように、ゼータ値の分母の素数の出現は規則的ですが、分子の素数の出現にはどのような規則があるのか見当が付きません。ワイルズはメイザーとともに、 (p, k) の出現を p 円分体のイデアル類群の k -部分という対象に結びつけることに成功したのです。

$\zeta(1 - k)$ の分母

k	分母	素 因 数 分 解
2	12	$2^2 \cdot 3$
4	120	$2^3 \cdot 3 \cdot 5$
6	252	$2^2 \cdot 3^2 \cdot 7$
8	240	$2^4 \cdot 3 \cdot 5$
10	132	$2^2 \cdot 3 \cdot 11$
12	32760	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$
14	12	$2^2 \cdot 3$
16	8160	$2^5 \cdot 3 \cdot 5 \cdot 17$
18	14364	$2^2 \cdot 3^3 \cdot 7 \cdot 19$
20	6600	$2^3 \cdot 3 \cdot 5^2 \cdot 11$
22	276	$2^2 \cdot 3 \cdot 23$
24	65520	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$
26	12	$2^2 \cdot 3$
28	3480	$2^3 \cdot 3 \cdot 5 \cdot 29$
30	85932	$2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31$
32	16320	$2^6 \cdot 3 \cdot 5 \cdot 17$
34	12	$2^2 \cdot 3$

$\zeta(1 - k)$ の分子

k	$\pm$	分子	素因数分解
2	+	1	
4	-	1	
6	+	1	
8	-	1	
10	+	1	
12	-	691	691
14	+	1	
16	-	3617	3617
18	+	43867	43867
20	-	174611	$283 \cdot 617$
22	+	77683	$131 \cdot 593$
24	-	236364091	$103 \cdot 2294797$
26	+	657931	657931
28	-	3392780147	$9349 \cdot 362903$
30	+	1723168255201	$1721 \cdot 1001259881$
32	-	7709321041217	$37 \cdot 683 \cdot 305065927$
34	+	151628697551	151628697551

問 素数 101 が最初に現れるのは k がいくつのときでしょうか？（分子は難しい.）

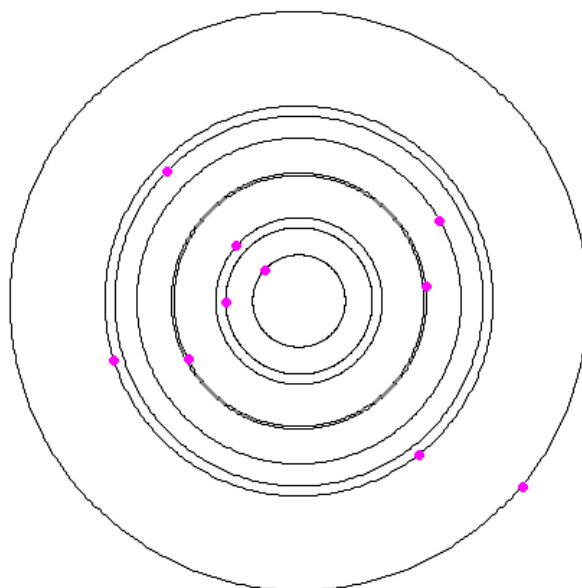
ディリクレ L 関数

(mod m の指標 $\chi(ab) = \chi(a)\chi(b)$ に対するゼータ関数 $L_{\pm m}(x)$)

$$L_1(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \frac{1}{9^x} + \frac{1}{10^x} + \frac{1}{11^x} + \frac{1}{12^x} + \cdots$$

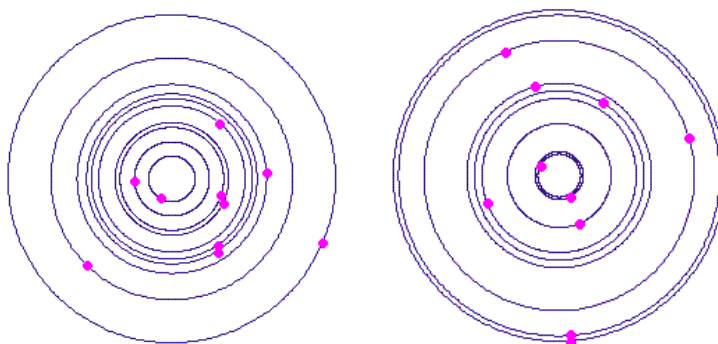
$$L_{-4}(x) = \frac{1}{1^x} + \frac{0}{2^x} + \frac{-1}{3^x} + \frac{0}{4^x} + \frac{1}{5^x} + \frac{0}{6^x} + \frac{-1}{7^x} + \frac{0}{8^x} + \frac{1}{9^x} + \frac{0}{10^x} + \frac{-1}{11^x} + \frac{0}{12^x} + \cdots$$

$$L_5(x) = \frac{1}{1^x} + \frac{-1}{2^x} + \frac{-1}{3^x} + \frac{1}{4^x} + \frac{0}{5^x} + \frac{1}{6^x} + \frac{-1}{7^x} + \frac{-1}{8^x} + \frac{1}{9^x} + \frac{0}{10^x} + \frac{1}{11^x} + \frac{-1}{12^x} + \cdots$$



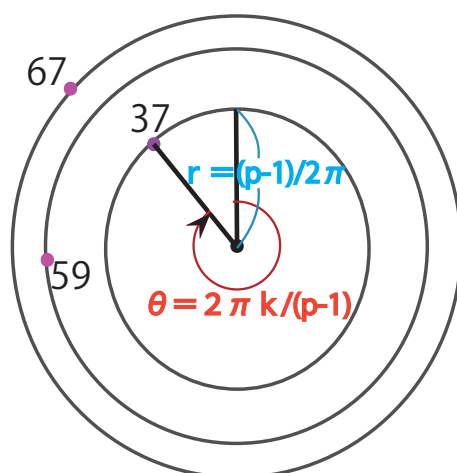
$\zeta(x) = L_1(x)$ のゼータ値の分子に現れる素数 (p, k)

$(37, 32)(59, 44)(67, 58)(101, 68)(103, 24)(131, 22)(149, 130)(157, 62)(157, 110)(233, 84)$



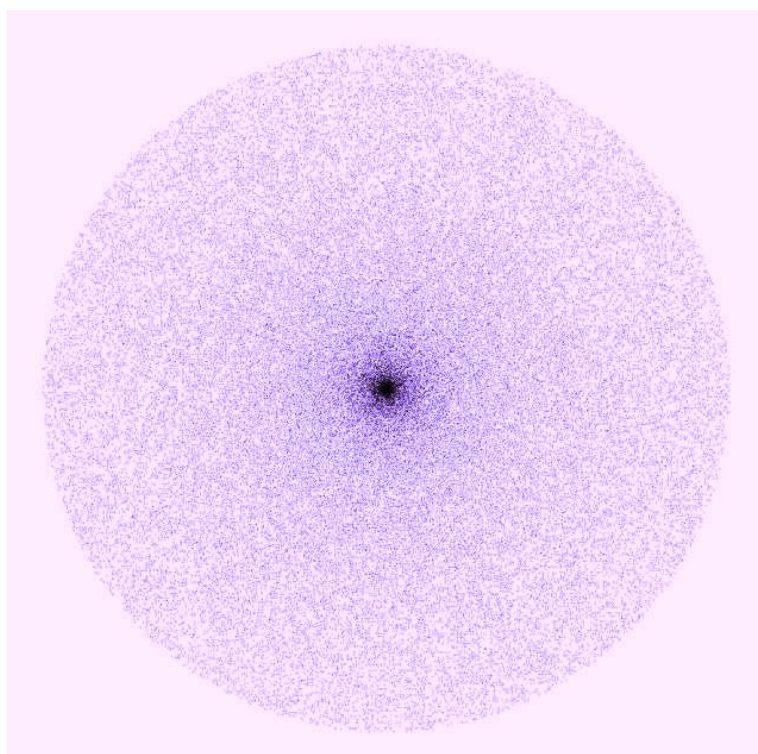
$L_{-4}(x), L_5(x)$ の L 値の分子に現れる素数 (p, k)

$(19, 11)(31, 23)(43, 13)(47, 15)(61, 7)(67, 27)(71, 29)(79, 19)(101, 63)(137, 43)$
 $(17, 14)(19, 8)(41, 18)(61, 42)(67, 6)(73, 70)(107, 22)(107, 100)(127, 62)(131, 64)$



(p, k) の表示方法

数論研究者たちは、多様なゼータ関数について様々な側面から研究を続けています。将来おそらくそれらのゼータ関数の研究によって素数の不思議が解明され、さらにその解明が新たな研究の大きな目標を与えてくれることを期待しています。無限の素数宇宙の探検は、いつまでも終わることはないでしょう。



$\zeta(x) = L_1(x)$ の 200 万までの分子の素数 (p, k)

未解決問題 フェルマー素数，メルセンヌ素数，双子素数，三つ子素数，ゼータ値の分子に現れない素数は，それぞれ無限個あるのでしょうか？

問の答え

p.2 I の場合, 2,7: ずれなし, 3,5: 右に 1 のずれ,
II の場合, 2,3: ずれなし, 5: 左に 2 のずれ, 7: 右に 2 のずれ
(I の方がパターンが分かりやすいかもしれません.)

p.3 空白の数字: 1,1,2,3,3,2,1

$i \times j: 0$ は m が素数の時は現れませんが, m が合成数のときは現れます.

m が素数の時, 全ての各行と各列に $1 \sim m-1$ 全てが現れます.

i^j : ある行に $1 \sim m-1$ 全てが現れるのは m が素数の時だけです. そのような i は素数 m の原始根と呼ばれます. 原始根に関してはアルティン予想という未解決予想があり, 一般リーマン予想から導かれます. (アルティン予想の一部: 平方数でも -1 でもない整数は, 無限個の素数の原始根になるだろう.)

p.6 13,11

p.10 このページのグラフが $1000 \frac{1}{\log(x-500)}, 10000 \frac{1}{\log(x-5000)}$ に近似していることから, $\int_2^x \frac{1}{\log t} dt$ で近似できるのではないかと推測できます.

p.11 $ab, \frac{b}{a}, 2\sqrt{a}$

p.19 分母 100 番目, 分子 68 番目 (分子は予測だけでは難しいと思われます.)

リーマン予想と $\pi(x)$ の関係

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$$

$$\pi(x) = \mathrm{Li}(x) - \sum_{\zeta(\rho)=0, \rho \notin \mathbf{R}} \mathrm{Li}(x^\rho) + O(\sqrt{x}).$$