

小学校の算数から現在の未解決問題まで — 数学を楽しもう —

大島 利雄*

平成 10 年 8 月 5 日

1 はじめに

数学は、自然科学の中でも最も古くから存在し、しかも千年以上も前の天才が得た真理が価値ある成果として引き継がれ、現在の数学の中でもその価値を失わずに息づいている。

物事の本質が分かって理解できたときの喜びは、人間が生まれつき持っている感情であって、人類の高度な文化が発達するための原動力になってきた。数学における発見は物事の真理をより高い立場から統一的に見通すことを可能にし、数学は内在的に発展を遂げてきたのみならず、自然科学の基礎となって共に影響しあって発展してきた。現在もこれは変わらず将来も同様であろう。

数学の発展は、局所的には細分化と複雑化のように見えるが、本質はより高い立場からの統一化であって、それがあつたからこそ先人達の偉業の多くを私達も甘受することができるのである。

たとえば、私達が、日本の人口のような何桁もの大きな数を扱うことができ、それらの計算も出来るということは、私には真に不思議なことに思える。

今回はいくつかの数学の問題や疑問を取り上げることにするが、「数学」を「数楽」として存分に楽しむための材料にいただければ幸いである。

2 個数を教える関数

1996 年の算数オリンピックの問題に次のようなものがありました。

*東京大学数理科学研究科, e-mail: oshima@ms.u-tokyo.ac.jp

このノートは静岡県数学教育研究会夏期講座のために準備したものです。L^AT_EX で作成し、筆者が中心となって開発したプログラムで印刷しました。プログラムは <http://akagi.ms.u-tokyo.ac.jp/dvptest.html> から自由に得ることができます。

問題 1. ある整数を、0 より大きな整数の和で表す方法が何とおりあるかを考えます。
使う数が同じで順番だけが違うものは、1 とおりとして数えます。

(1) たとえば、6 を 3 個以下の整数の和で表す方法は、

$$\begin{array}{cccc} 6 & 5+1 & 4+2 & 3+3 \\ 4+1+1 & 3+2+1 & 2+2+2 & \end{array}$$

の 7 とおりあります。では、50 を 3 個以下の整数の和で表す方法は、何とおりありますか。

(2) 50 を 3 以下の整数の和で表す方法は何とおりありますか。

ちょっと面倒ですが計算してみましょう。(1) は

$$a_1 + a_2 + a_3 = 50, \quad a_1 \geq a_2 \geq a_3 \geq 0$$

となる整数の組 (a_1, a_2, a_3) の数を数えることになります。 $a_3 = 0, 1, \dots, [\frac{50}{3}] = 16$ に
対して、 $a_1 + a_2 = 50 - a_3$ より $a_2 = a_3, a_3 + 1, \dots, [\frac{50-a_3}{2}]$ ですから、その数は

$$\begin{aligned} \sum_{a_3=0}^{16} ([\frac{50-a_3}{2}] - a_3 + 1) &= \sum_{k=0}^8 ([\frac{50-2k}{2}] - 2k + 1) \\ &\quad + \sum_{k=1}^8 ([\frac{50-(2k-1)}{2}] - (2k-1) + 1) \\ &= \sum_{k=0}^8 (26-3k) + \sum_{k=1}^8 (27-3k) \\ &= 9 \times 26 + 8 \times 27 - 6 \times \frac{8 \times 9}{2} = 234 + 216 - 216 = 234 \end{aligned}$$

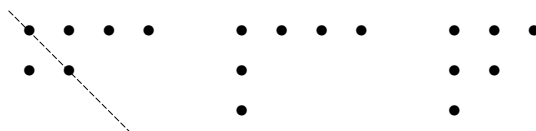
となります。(2) は上のようにしてやると大変なので、1 を b_1 個、2 を b_2 個、3 を b_3 個加えると 50 になると考えます。すなわち

$$\underbrace{1+\cdots+1}_{b_1 \text{ 個}} + \underbrace{2+\cdots+2}_{b_2 \text{ 個}} + \underbrace{3+\cdots+3}_{b_3 \text{ 個}} = 50, \quad b_1 + 2b_2 + 3b_3 = 50$$

このとき、 $b_3 = 0, \dots, [\frac{50}{3}] = 16$ で、 $b_2 = 0, \dots, [\frac{50-3b_3}{2}] = [\frac{50-b_3}{2}] - b_3$ ですから、
全く同じ計算となり 234 通りになります。

これが一致するのは偶然でしょうか？ 一般に「自然数 N を n 個以下の自然数の和で表す方法の数」と「自然数 N を n 以下の自然数の和で表す方法の数」とは等しくなるのでしょうか？

$N = 6, n = 3$ の場合に絵を描いて考えてみましょう。 $6 = 4 + 2, 6 = 4 + 1 + 1, 6 = 3 + 2 + 1$ は、それぞれ横の $\bullet$ の個数を加えると考えて

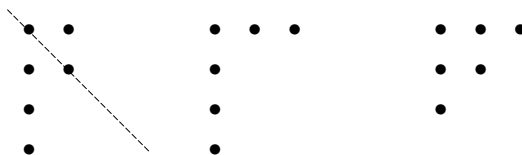


となります。

一般には、各行の個数が増えていかにように N 個の $\bullet$ を複数行に分けて並べることが、 N を自然数の和で表す方法の一つに対応します。そのうち、 n 個以下の自然数の和で表すことは、行が n 以下ということで、 n 以下の整数で表すことは、列が n 以下ということに対応します。

左上隅の $\bullet$ を通る -45 度の直線で対称に折り返してやることを考えます。これは、 N を自然数の和に表す表し方の中での対応を与えます。総個数は変わりませんが、 n 行以下に並べたものは n 列以下になります。先ほど予想した事実が、単に場合の数の一致だけでなく、より深い意味を持つことが解明できたことになります。

先ほどの例では



となり、それぞれ $6 = 2 + 2 + 1 + 1$, $6 = 3 + 1 + 1 + 1$, $6 = 3 + 2 + 1$ に対応します。具体的には

$$a_1 = b_1 + b_2 + b_3, \quad a_2 = b_2 + b_3, \quad a_3 = b_3$$

です。

自然数 N を自然数の和で表す表し方の個数 $p(N)$ というのは、分割数と呼ばれ、数学者の興味を引いてきました。 $p(N)$ は簡単な式には書けませんが、たとえば

問題 2. $n \rightarrow \infty$ のとき $p(n)$ はどの程度大きくなるのだろうか？

というのは最も基本的な疑問です ($p(10) = 42$, $p(100) = 190569292$)。

次数が無限の多項式 (形式べき級数という) を補助的に考えます。

$$(1 + x^1 + x^2 + x^3 + x^4 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots) \\ = \left(\sum_{b_1=0}^{\infty} x^{b_1} \right) \left(\sum_{b_2=0}^{\infty} x^{2b_2} \right) \left(\sum_{b_3=0}^{\infty} x^{3b_3} \right)$$

という積は x の次数の低いものから順に計算でき、 $1 + x + 2x^2 + 3x^3 + 4x^4 + \cdots$ となります。 x^6 の係数は、 $b_1 + 2b_2 + 3b_3 = 6$ を満たす非負整数の組 (b_1, b_2, b_3) の数となり、それは 6 を 3 以下の自然数の和で表す方法の数で 7 です。一般に上の式の x^N の係数は、 N を 3 以下の自然数の和で表す方法の個数となります (N を 3 個以下の自然数の和で表す方法の個数といっても同じ)。

自然数 k に対して

$$\frac{1}{1-x^k} = 1 + x^k + x^{2k} + x^{3k} + \dots$$

と置きましょう。実際 x が $|x| < 1$ を満たす数ならば、上の両辺は等しくなります。
 $\prod_{k=1}^{\infty} \frac{1}{1-x^k} = \prod_{k=1}^{\infty} (1 + x^k + x^{2k} + x^{3k} + \dots) = \prod_{k=1}^{\infty} \left(\sum_{b_k=1}^{\infty} x^{kb_k} \right)$ の x^n の係数は

$$b_1 + 2b_2 + 3b_3 + \dots = n$$

を満たす非負整数の列 $(b_1, b_2, b_3, \dots)$ の個数で、これは分割数 $p(n)$ となります。すなわち

$$\prod_{k=1}^{\infty} \frac{1}{1-x^k} = 1 + \sum_{n=1}^{\infty} p(n)x^n \quad (1)$$

が得られます。この関数 $\prod_{k=1}^{\infty} \frac{1}{1-x^k}$ を $p(n)$ の生成関数と呼びます。

$\prod_{k=1}^{\infty} \frac{1}{1-x^k}$ は $-1 < x < 1$ のとき正の値を取る微分可能関数となり、 $x=0$ での n 次の微係数は $n!p(n)$ となります。 $0 \leq x < 1$ で $f(x)$ が正の有限値を取ることは以下のようにして分かり、この範囲で $f(x)$ は単調増加です。

$-\frac{d}{dy} \log(1-y) = \frac{1}{1-y}$ ですから、(平均値の定理から) $0 \leq y \leq \frac{1}{2}$ のとき $y \leq -\log(1-y) \leq 2y$ となります。 $0 \leq x < 1$ となる実数 x を一つ取ります。これに対して m を十分大きく取ると $0 \leq x^m \leq \frac{1}{2}$ となります。このとき

$$0 \leq \log \prod_{k=m}^N \frac{1}{1-x^k} \leq \sum_{k=m}^N 2x^k \leq \frac{1}{1-x}$$

$\prod_{k=m}^N \frac{1}{1-x^k}$ は N について単調増加で上から $e^{\frac{1}{1-x}}$ で押さえられているので、ある正の実数に収束します。

(1) より、 $0 < x < 1$ を満たす実数 x に対し

$$p(n) < \left(\frac{1}{x}\right)^n \frac{1}{\prod_{k=1}^{\infty} (1-x^k)} \quad (2)$$

が分かります。右辺は対数をとって n で割って $n \rightarrow \infty$ の極限を考えると $-\log x$ に収束します。よって特に

$$\lim_{n \rightarrow \infty} \frac{\log p(n)}{n} = 0$$

です。 $n \rightarrow \infty$ のときの良い $p(n)$ の評価を得るには、(2) で n に応じて x をうまくとれば良いと考えられます。 $x = e^{-t}$ とおいて

$$f(t) = \prod_{k=1}^{\infty} (1 - e^{-kt})$$

という関数の $(0 <) t \rightarrow 0$ の様子を調べるのが重要になります。さて、 $0 \leq y < 1$ のとき

$$-\log(1-y) = y + \frac{y^2}{2} + \frac{y^3}{3} + \frac{y^4}{4} + \cdots \quad (3)$$

となることを使うと（これは、 $\frac{1}{1-s} = 1 + s + s^2 + s^3 + \cdots$ を 0 から y まで積分すれば分かる）、

$$\begin{aligned} -\log f(t) &= \sum_{k=1}^{\infty} \left(e^{-kt} + \frac{e^{-2kt}}{2} + \frac{e^{-3kt}}{3} + \cdots \right) \\ &= \sum_{k=1}^{\infty} \sum_{\ell=1}^{\infty} \frac{e^{-k\ell t}}{\ell} = \sum_{\ell=1}^{\infty} \frac{e^{-\ell t}}{\ell(1-e^{-\ell t})} = \sum_{\ell=1}^{\infty} \frac{1}{\ell(e^{\ell t} - 1)} < \sum_{\ell=1}^{\infty} \frac{1}{\ell^2 t} = \frac{\pi^2}{6t} \end{aligned}$$

ここで、 $e^{\ell t} - 1 > \ell t$ ($t > 0$), $\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots^*$ を使った。従って

$$p(n) = e^{nt} e^{-\log f(t)} < \exp \left(nt + \frac{\pi^2}{6t} \right)$$

を得ます。ここで、 $t = \frac{\pi}{\sqrt{6n}}$ ととると

$$p(n) < \exp \left(\pi \sqrt{\frac{2n}{3}} \right)$$

が得られます。実際には Hardy-Ramanujan (1918 年) により

$$p(n) \sim \frac{1}{4\sqrt{3n}} \exp \left(\pi \sqrt{\frac{2n}{3}} \right) \quad (4)$$

が証明されています。これは、関数 $f(t) = \prod_{k=1}^{\infty} (1 - e^{-kt})$ のより深い解析に基づいています。たとえば

$$f\left(\frac{2\pi}{t}\right) = \sqrt{t} e^{\frac{\pi}{12}(\frac{1}{t}-t)} f(2\pi t) \quad (5)$$

$$\prod_{k=1}^{\infty} (1 - x^k) = 1 + \sum_{n=1}^{\infty} (-1)^n \left(x^{\frac{n(3n-1)}{2}} + x^{\frac{n(3n+1)}{2}} \right) \quad (6)$$

などの不思議な等式が成立します。この下の式に $p(n)$ の生成関数を乗じて x^n 次の項の係数を比べると

$$\sum_{k=-\infty}^{\infty} (-1)^k p\left(n - \frac{k(3k-1)}{2}\right) = 0 \quad (7)$$

*Euler による証明は、 $(\text{Arcsin } x)' = \sqrt{1-x^2}$, $\text{Arcsin } x = \sum_{n=0}^{\infty} \frac{(2n-1)!!}{(2n)!!} \frac{x^{2n+1}}{2n+1}$, $\int_0^1 \frac{x^{2n+1}}{\sqrt{1-x^2}} dx = \frac{(2n)!!}{(2n+1)!!}$, $\int_0^1 \frac{\text{Arcsin } x}{\sqrt{1-x^2}} dx = \left[\frac{(\text{Arcsin } x)^2}{2} \right]_0^1 = \frac{\pi^2}{8}$ より $\sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} = \frac{\pi^2}{8}$ となるので、 $S = \sum_{n=1}^{\infty} \frac{1}{n^2}$ とおくと $S = \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} + \sum_{n=1}^{\infty} \frac{1}{(2n)^2} = \frac{\pi^2}{8} + \frac{S}{4}$ より、 $S = \frac{\pi^2}{6}$ を得る。ここで、 $(2n)!! = (2n)(2n-2)(2n-4)\cdots(2)$, $(2n+1)!! = (2n+1)(2n-1)(2n-3)\cdots(1)$.

となります。ただし、 $n < 0$ のとき $p(n) = 0$ 、および $p(0) = 1$ と定めています。この漸化式は $p(n)$ を順に計算していくのに用いられます。

そのほか Ramanujan は、 $p(5m+4) \equiv 0 \pmod{5}$, $p(7m+5) \equiv 0 \pmod{7}$, $p(11m+6) \equiv 0 \pmod{11}$ などの不思議な関係式を発見しています。

3 物と関係の双対

1998 年のある大学の入試問題より

問題 3. 一列に並んでいる碁石に、一つずつ碁石を加えていく次のような操作を考える。

A. 隣り合った 2 つの碁石を選んでそれぞれ白黒を逆にし、その間に白石を挿入する。

B. 右端、あるいは、左端に白石を加え、加えた白石に隣り合った碁石の白黒を逆にする。

白石 1 つから始めて上の 1. または 2. の操作を続けることによって、白石のみが一列に n 個並んだ状態にすることが出来るための n の条件を求めよ。

挿入する位置を $\uparrow$ で表し、挿入された白石を $\circ$ で表すと

$$\begin{array}{llll} \circ \uparrow & \longrightarrow & \uparrow \bullet \circ & \longrightarrow & \circ \circ \circ \\ \circ \uparrow & \longrightarrow & \bullet \uparrow \circ & \longrightarrow & \circ \circ \bullet \\ \circ \uparrow & \longrightarrow & \bullet \circ \uparrow & \longrightarrow & \bullet \bullet \circ \end{array} \quad (8)$$

などから、 $n = 1, 3$ は可能で、 $n = 2$ は不可能であることがわかる。また

$$\uparrow \circ \circ \cdots \longrightarrow \uparrow \circ \bullet \circ \cdots \longrightarrow \circ \bullet \uparrow \circ \cdots \longrightarrow \circ \circ \circ \circ \cdots$$

より、 n のとき可能ならば $n+3$ のとき可能なことがわかる。よって $n \equiv 0, 1 \pmod{3}$ のときは可能である。

いろいろ試みてみると、 $n \equiv 2 \pmod{3}$ のときは出来ないようであるが、実際に証明するのは頭を悩ませるであろう。

別の見方をしてみよう。 $\bullet$ や $\circ$ は背後の隠れたものの関係を表していると想像してみる。 $\heartsuit$ と $\spadesuit$ が一列に並んでいて、その隣同士の関係を表していると考える。

$\heartsuit$ は「女子」で、 $\spadesuit$ は「男子」、 $\bullet$ は「異性」の関係、 $\circ$ は「同性」の関係としてみよう。たとえば $\heartsuit \spadesuit \heartsuit \spadesuit$ は、 $\heartsuit \bullet \spadesuit \circ \heartsuit \bullet \spadesuit$ より $\bullet \bullet \bullet \bullet$ に対応する。

このとき A. と B. では、「同性」の関係を挿入し、その隣りあった関係の「異性」と「同性」を逆にすることである。すなわち、「男子」または「女子」を一人選んで、それと異なる同性の二人に替えることに他ならない。たとえば(8)の例では、最初は

「女子」が二人並んでいると見なして

$$\begin{array}{ccccc}
 \heartsuit \circ \heartsuit & \longrightarrow & \heartsuit \bullet \heartsuit \circ \heartsuit & \longrightarrow & \heartsuit \bullet \heartsuit \bullet \heartsuit \bullet \heartsuit \\
 \uparrow & & \uparrow & & \\
 \heartsuit \circ \heartsuit & \longrightarrow & \heartsuit \bullet \heartsuit \circ \heartsuit & \longrightarrow & \heartsuit \circ \heartsuit \circ \heartsuit \bullet \heartsuit \\
 \uparrow & & \uparrow & & \\
 \heartsuit \circ \heartsuit & \longrightarrow & \heartsuit \bullet \heartsuit \circ \heartsuit & \longrightarrow & \heartsuit \bullet \heartsuit \circ \heartsuit \circ \heartsuit \\
 \uparrow & & \uparrow & &
 \end{array} \tag{9}$$

各段階は、 $\heartsuit$ を一つ選んで $\spadesuit \spadesuit$ に替えるか、 $\spadesuit$ を一つ選んで $\heartsuit \heartsuit$ に替えるかのどちらかである。「 $\heartsuit$ の数 - $\spadesuit$ の数」は3減るか3増えるかということになり、「 $\heartsuit$ の数 - $\spadesuit$ の数 $\bmod 3$ 」[†]の値は不変で、今の場合女子2人から始めたので2となる。

n 個並んだ全てが $\circ$ の状態とは、 $n+1$ 個が全て $\heartsuit$ か全てが $\spadesuit$ ということで、上記の操作でそのような状態になり得るとすると、それぞれ $n+1 \equiv 2 \pmod{3}$ と $-(n+1) \equiv 2 \pmod{3}$ である。 $n \equiv 2 \pmod{3}$ のときは、いずれも成り立たないので、 $\circ$ のみが n 個並んだ状態には出来ないことがわかる。

このように「 $\bullet$ と $\circ$ の世界」から「 $\heartsuit$ と $\spadesuit$ 」の世界に移って考えれば、任意に列に $\bullet$ と $\circ$ が並んだ状態から、最低何ステップで $\circ$ のみが並んだ状態にできるかも容易に分かる。すなわち、 $\heartsuit$ と $\spadesuit$ の世界に移ったとき、その個数の小さい方がステップ数となる。たとえば、 $\heartsuit$ の数の方が少なければ、各ステップで一つの $\heartsuit$ を2つの $\spadesuit$ に替えていけばよい。

別の問題を考察してみよう。

問題 4. 有限個の碁石が一行に並んでいるとする。全部が白石でないとする、次の操作 C を続けることにより、黒石が一つだけの状態にできることを示せ。

C . 黒の碁石を一つ指定して、それに隣り合った碁石の白黒を逆にする。

これも「 $\bullet$ と $\circ$ の世界」から「 $\heartsuit$ と $\spadesuit$ 」の世界に移って考えれば、 $\heartsuit$ と $\spadesuit$ とが並んだ列において C は隣り合った「女子」と「男子」が入れ替わることを意味している。また、 $\bullet$ が一つだけの状態とは、「女子」が全て左側に「男子」が全て右側に並んだ状態、あるいは、その逆の状態のことである。隣り合った二人を入れ替えていくことにより、このように「男子」と「女子」をそれぞれまとめた状態にできることは明らかである。

また、あるパターンから C の操作で別のパターンに移ったとすれば、逆の操作も可能である。

異なった「黒石が一つだけのパターン」が C の操作で移りあうためには、左右を入れ替えた (180 度回転した) パターンに限ることも分かる。

あるパターンから黒石が一つだけにするための操作を考えてみよう。 $\heartsuit$ を全て左側に持ってくることにしよう。各 $\heartsuit$ に対しその左側にある $\spadesuit$ の個数を数え、その数の和を N とする。

[†] $a \equiv b \pmod{c}$ とは、 $a - b$ が c の整数倍になること。

…♠♡… となっている 2 つを入れ替えると N が 1 つ減り、…♡♠… となっている 2 つを入れ替えると N が一つ増える。♡ が全て左側にあるパターンでない限り …♠♡… となっている部分があるので、その 2 つの入れ替える、という操作を続ければ最後には $N = 0$ すなわち、♡ が全て左側にある状態になる。左右を逆にした場合も同様の推論ができる。

たとえば、

問題 5. 黒石が一つのみの列で、その左側に白石が m 個、右側に白石が n 個並んだパターンを考える。 $m \neq n$ として、 C . を続けて m と n を入れ替えるのに最低何ステップかかるか。

の答えは $(m+1)(n+1)$ となる。次の 1998 年数学オリンピックの問題も一種の応用例である。

問題 6. 時計の文字盤の 1 から 12 のところに白または黒の碁石を置く。 C . の操作を続けることによって、「12 の場所に黒石、それ以外の 11 箇所は全て白石」にすることが出来るパターンは何通りあるか。

答えは、偶数の数字のところに黒石の個数と白石の個数の差が奇数、かつ、奇数の数字のところに黒石の個数と白石の個数の差が偶数の場合で、 $2^{10} = 1024$ 通りとなる。

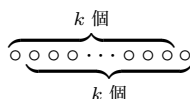
このような円の場合や、直線上でなくて枝分かれした場合、白黒の 2 色でなくて多色の場合、などこの問題はいろいろな拡張が考えられる。

4 初等幾何の 3 つの定理

碁石の問題を扱ったので、まず頭慣らしに簡単な定理から

定理 1. 有限個の碁石が一行に並んでいるとすると、それは全てが白、あるいは全てが黒のどちらかである。

証明. 碁石の個数 n に関する数学的帰納法で証明する。 $n = 1$ のときは明らかである。そこで、 $n = k$ のとき正しいと仮定しよう。 $k + 1$ 個の碁石が一行に並んでいるとき



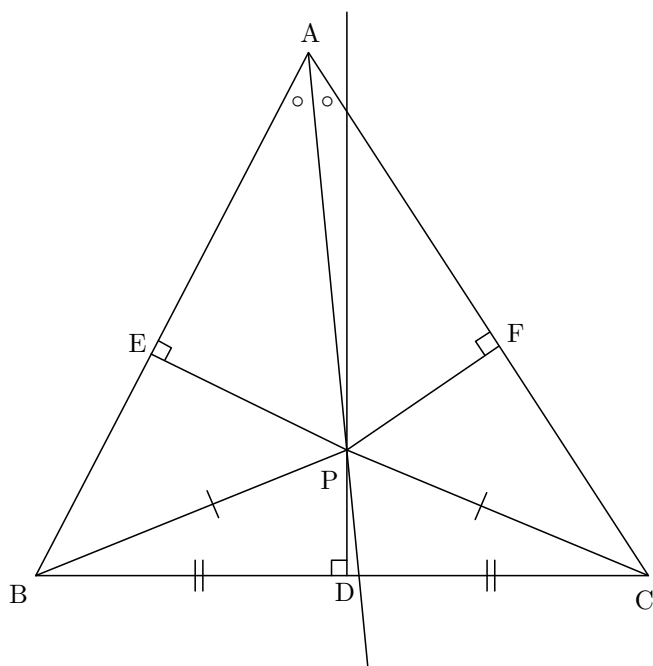
右の 1 個を忘れると左端から k 個並んでいると見なせるので、それらは全て白、あるいは全て黒である。左の 1 個を忘れた k 個も同様に、それらの色が食い違つてはおかしいので、やはり $k + 1$ 個は全て同じ色である。□

では初等幾何における3つの有名な定理を紹介しよう。

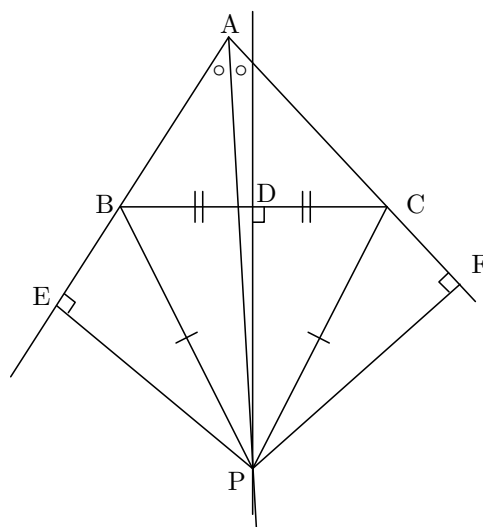
定理 2. 三角形の2つの辺は長さが等しい。

証明. $\triangle ABC$ の底辺 BC の中点を D とし、 BC の垂直二等分線と $\angle A$ の二等分線との交点を P とする。さらに P から AB, AC に下ろした垂線の足を、それぞれ E, F とおく。 $\triangle AEP$ と $\triangle AFP$ は斜辺の長さが等しい直角三角形で、さらに $\angle EAP = \angle FAP$ が成り立つので合同である。よって、 $AE = AF, PE = PF$ が分かる。

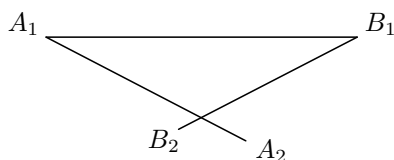
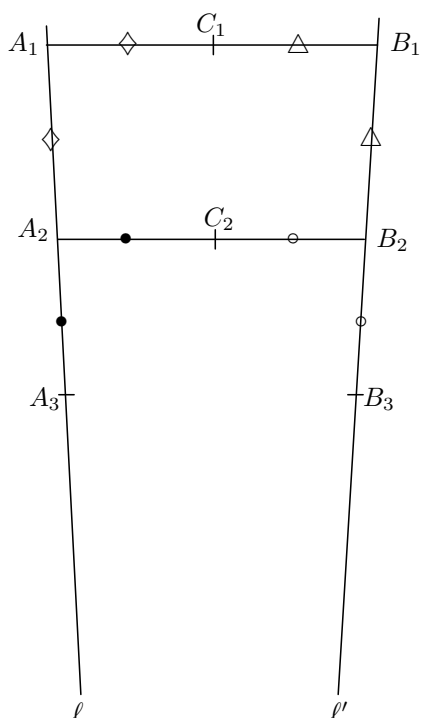
PD は BC の垂直二等分線であるから、 $PB = PC$ が成り立つ。 $\triangle PEB$ と $\triangle PFC$ は斜辺とその他の一辺の長さが等しい直角三角形であるから合同となる。特に $EB = FC$ である。よって $AE = AF$ とあわせて、 $AB = AC$ が得られる。□



注意: なお、右図のように BC の垂直二等分線と $\angle A$ の二等分線が $\triangle ABC$ の外で交わる場合も、証明は同様である。



定理 3. 平面上の相異なる直線は交わらない



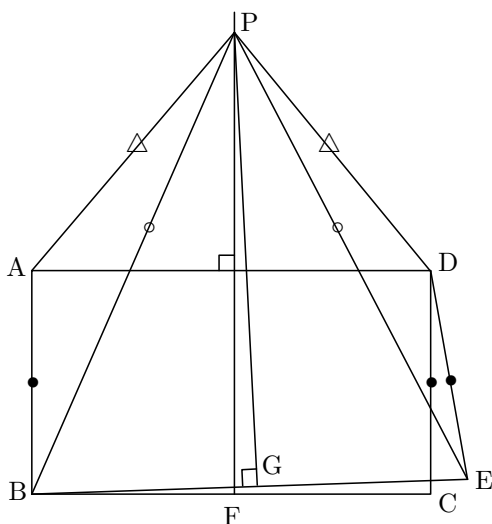
証明. 平面上の相異なる直線 ℓ, ℓ' 上に点 A_1, B_1 をとり、線分 A_1, B_1 上に点 C_1 をとり。左の図のように直線 ℓ 上に A_2 を、直線 ℓ' 上に B_2 を、 $A_1A_2 = A_1C_1, B_1B_2 = B_1C_1$ となるようにとる。

このとき、 $A_1B_1 = A_1A_2 + B_1B_2$ であるから、線分 A_1A_2 と線分 B_1B_2 がもし交わったとすると、そのときできる三角形の二辺の長さの和が他の一辺の長さより小さくなって矛盾である。従って、 A_1A_2 と B_1B_2 は交わらない。

線分 A_2B_2 上に点 C_2 を取って同様の議論を行う、ということをしていけば、直線 ℓ と ℓ' とが交わらないことが示される。□

注意: 「 A_nB_n ($n = 1, 2, \dots$) の長さが小さくなっていくので、有名な“アキレスと亀”の論理と同じでおかしい」という人がいたら、この証明を理解していないことになる。点 C_n をうまく取っていけば、そのようなことは容易に避けられるからである。

定理 4. 直角と鈍角は等しい。



証明. 長方形 $ABCD$ の一辺 DC の長さに等しい線分 DE を、右図のように長方形の外に引く。 BC の垂直二等分線と BE の垂直二等分線の交点を P とする。

BC の垂直二等分線は AD の垂直二等分線だから $PA = PD$ 。また P は BE の垂直二等分線上にあるから $PB = PE$ 。また、 $AB = DC = DE$ であるから、 $\triangle PAB$ と $\triangle PDE$ は三辺が等しいので合同である。

特に $\angle PAB = \angle PDE$ であるが、 $\angle PAD = \angle PDA$ であるから、 $\angle DAB = \angle ADE$ となる。□

5 ユークリッドの互除法とフィボナッチ数列

小学校の分数の計算で、たとえば $\frac{12}{27}$ という答えが出てきたら、約分して $\frac{4}{9}$ と既約分数に直すように教えられる。既約分数にして求めた答えが正解の既約分数と違っていれば、答えは間違いであることは皆知っている。では、ある分数が異なる既約分数に表せることは本当にはないのであろうか？

「もとの分数の分母と分子を素因数分解すれば明らかである」と言われるかも知れないが、素因数分解が一意的と言ってよいのであろうか？それは実は自明ではないのである。どうして自明でないのかが分かることは、ある程度の数学的素養を必要とするのかもしれない。

実際、小学生のときは習わないし、大学の数学科などに進まない限り、その証明は習うことがないかもしれない。素因数分解の一意性を突き詰めて考えていくと

問題 7. 自然数 m と n の積が素数 p で割り切れるならば、 m または n が p で割り切れる。

ということを示す必要があり、またこれが分かれば素因数分解の一意性も容易に得られる。そのためには、次の命題を使うとよい。

命題 1. 自然数 m と n が互いに素ならば、適当に整数 a と b を選ぶと $am + bn = 1$ を満たすようにできる。

証明. r と s のどちらも $am + bn$ の形に書けるならば、 $r + s$ や r の整数倍も同様な表示をもつことに注意する。 $am + bn$ の形に書ける自然数の中で最小のものを s とおく。

$s > 1$ と仮定しよう。 $0 < s \leq m$ であるが、 s が m の約数でないなら $0 < r = m - qs < s$ となる自然数 q が存在し、 r も $am + bn$ の形に書けることが言えるので、 s が最小であることに矛盾する。よって、 s は m の約数でなくてはならない。同様に s は n の約数でもあり、これは m と n が互いに素であることに矛盾する。□

問題 7 の証明. 仮定から、ある整数 c によって $mn = cp$ となっている。 m が p で割り切れないと仮定しよう。 m と p とは互いに素であるから $am + bp = 1$ となるように整数 a, b をとることができる。このとき、 $acp = amn = (1 - bp)n$ すなわち $n = (ac + bn)p$ となり n は p で割り切れる。□

上記の命題 1 の証明は、 a と b の存在を示しているが、それを具体的に求める方法を与えてはいない。このような証明は構成的でないという。構成的な証明を考えてみよう。

2 つの自然数が互いに素であることを示すには、その最大公約数が 1 であることと同じであり、最大公約数を求めるにはユークリッドの互除法がある。

(m, n) を $m \geq n > 0$ を満たす整数の組とする。 m を n で割った商を q 、余りを r とすると、

$$m = qn + r$$

である。 $r \neq 0$ ならば、 m と n の公約数は r の約数であり、逆に r と n の公約数は m の約数になるので、 m と n の最大公約数は、 n と r の最大公約数に等しい。このとき (m, n) を (n, r) で置き換えて同様の議論を繰り返していくと、有限回 (m 回以下) で割り切れる整数の組 (m', n') となり、 n' が m と n の最大公約数となる。たとえば、 $(m, n) = (119, 84)$ ならば、

$$119 \div 84 = 1 \cdots 35$$

$$84 \div 35 = 2 \cdots 14$$

$$35 \div 14 = 2 \cdots 7$$

$$14 \div 7 = 2$$

となるので、4 回の割算で最大公約数は 7 となることが分かる。 $17 = \frac{119}{7}$ と $12 = \frac{84}{7}$ は互いに素であるが、これにユークリッドの互除法を適用してみる。積の形に書くと

$$17 = 1 \cdot 12 + 5$$

$$12 = 2 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

すると、上から 3 行目の式から遡って見ていくと

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 \\ &= 5 \cdot (17 - 1 \cdot 12) - 2 \cdot 12 = 5 \cdot 17 - 7 \cdot 12 \end{aligned}$$

すなわち命題 1 が $(17, 12)$ の場合に具体的に得られた。一般の場合もユークリッドの互除法を使うと命題 1 の構成的証明が得られる。

実際、ユークリッドの互除法により、最後の段階で割り算の余りが 1 となるが、それはその直前に現れた 2 つの自然数の整数倍の和で表せる。その自然数は、前の段階の割り算の余りであるから、さらに一つ遡ったところで現れた 2 つの自然数の整数倍の和に書き直せる。これを続ければ、互いに素な元の自然数の整数倍の和で 1 を表す表示が具体的に得られる。

ユークリッドの互除法を使うと、2 つの自然数 (m, n) の最大公約数を容易に求めることが出来る。では何回程度割り算を行えば、最大公約数が求められるか考察してみよう。 $m = 2n$ ならば 1 回の割り算で終わりであるから、逆に割り算の回数が最も多い場合はどうなるかを考えてみる。

問題 8. 自然数 k に対し、ユークリッドの互除法が丁度 k 回の割り算で終了する自然数の組 (m, n) で、 $m > n$ でかつ m が最小になるものを求めよ。

$k = 1$ のときは、明らかに $(2, 1)$ が求めるものである。同様に $k = 2$ のときは、 $(3, 2)$ であることも明らかである。 $(3 + 2, 3)$ ならば $k = 3$ となる。このように選んでいけば、この問題の解答が得られそうである。

すなわち、フィボナッチ数列を考える：

$$a_{n+2} = a_{n+1} + a_n \quad (n = 1, 2, \dots), \quad a_1 = a_2 = 1$$

具体的には、 $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \dots$

$n \geq 1$ のとき、 $a_{n+1} < a_{n+2} = a_{n+1} + a_n < 2a_{n+1}$ が分かるので

$$a_{n+2} \div a_{n+1} = 1 \cdots a_n \quad (n \geq 1)$$

となる。よって $k \geq 2$ とすると (a_{k+2}, a_{k+1}) には丁度 k 回の割り算が必要になる。特にフィボナッチ数列の連続した 2 項は互いに素であることが分かる。

逆に $a_{k+2} \geq m > n$ を満たす (m, n) で割り算の回数が k となるものは (a_{k+2}, a_{k+1}) に限ることを、 k に関する帰納法で示そう。 $k = 1, 2$ のときは明らかである。

割り算の回数が k 回となる (m, n) で $a_{k+2} \geq m > n$ となるものがあつたとしよう。 $k > 2$ と仮定する。 $m \div n = q_1 \cdots r_1$, $n \div r_1 = q_2 \cdots r_2$ とおくと、 (n, r_1) は $k - 1$ 回、 (r_1, r_2) は $k - 2$ 回の割り算が必要である。

帰納法の仮定より、 $n \leq a_{k+1}$ ならば、 $(n, r_1) = (a_{k+1}, a_k)$ がわかり、 $(m, n) = (a_{k+2}, a_{k+1})$ が得られる。一方 $n > a_{k+1}$ のとき $a_{k+2} \geq m$ なので $r_1 = m - n < a_{k+2} - a_{k+1} = a_k$ で、 (a_k, a_{k-1}) は $k - 2$ 回の割り算が必要であるから、帰納法の仮定に矛盾する。

フィボナッチ数列の第 n 項 a_n は[‡]

$$a_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

で与えられることに注意しよう。小さな n に対しては $n = 1$ から順に a_n を求めていくのが速いが $n \rightarrow \infty$ のときの a_n の様子を調べるには、この公式は都合がよい。

自然数の組 (m, n) で $m \geq n$ を満たすものを取り、 (m, n) に対するユークリッドの互除法が何回で終了するか考察してみよう。 $m \geq a_{k+2}$ を満たす最大の整数を k とすれば k 回以下で終了することが分かった。 $k \geq 1$, $\left(\frac{\sqrt{5}-1}{2}\right)^3 = 0.23606 \cdots$ に注意すると $\frac{\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} - 0.24}{\sqrt{5}} < a_{k+2}$ であるから $k + 2 < \frac{\log(\sqrt{5}m + 0.24)}{\log \frac{1+\sqrt{5}}{2}}$ となる。すなわち (m, n)

[‡] $a_{n+2} - \frac{1+\sqrt{5}}{2}a_{n+1} = \frac{1+\sqrt{5}}{2}(a_{n+1} - \frac{1+\sqrt{5}}{2}a_n)$ より、 $a_{n+2} - \frac{1+\sqrt{5}}{2}a_{n+1} = \left(\frac{1+\sqrt{5}}{2}\right)^n(a_2 - \frac{1+\sqrt{5}}{2}a_1) = \left(\frac{1+\sqrt{5}}{2}\right)^{n+1}$ となり、 $\sqrt{5}a_{n+1} = \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$ が得られる。

に対するユークリッドの互除法の割り算の回数は

$$\left\lceil \frac{\log(\sqrt{5}m + 0.24)}{\log \frac{1+\sqrt{5}}{2}} \right\rceil - 2 \quad (10)$$

回以下で終了する。

$(\log_{10} \frac{1+\sqrt{5}}{2})^{-1} = 4.78497 \dots$, $\frac{1}{2} \log_{10} 5 = 0.349485 \dots$, $4.78497 \times 0.349485 - 2 = -0.3277 \dots$ となることを使うと、 $m < 10^\ell$ ($\ell \geq 1$) のとき上の式の値は $4.785\ell - 0.327$ 以下になる。すなわち、 m が ℓ 桁の自然数ならば、ユークリッドの互除法の割り算の回数は、

$$[4.785\ell - 0.327] \quad (11)$$

回以下である。 $\ell = 1, 2, 3, 4, 5, 6, 7, 8, 9$ のとき確かめてみると、この値はそれぞれ 4, 9, 14, 18, 23, 28, 33, 37, 42 となるので、最良の評価となっていることが分かる[§]。

6 素数の分布

素数は常に数学者の興味を引いてきたが、現在の未解決問題で最大のものは素数の分布に関連して出された Riemann 予想であろう。分割数の場合の生成関数と同様、素数の分布に関連して Riemann の ζ 関数が考えられた。それは $s > 1$ のとき

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots \quad (12)$$

という収束級数で表される[¶]。この範囲で単調減少関数で、 $s = 1$ のときは、 $\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots = \infty$ と発散している。

全ての自然数 n は $n = q_1^{m_1} \dots q_k^{m_k}$ というように一意に素因数分解できる。ここで、 $q_1 < \dots < q_k$ は素数で $m_1, \dots, m_k$ は自然数である。たとえば、 $12 = 2^2 \cdot 3$, $60 = 2^2 \cdot 3 \cdot 5$ となる。素数を $\{p_1, p_2, p_3, \dots\}$ と小さい順に並べよう。 $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$ である。

$$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \dots$$

という数を考えると、 $n_1 = 0, 1, 2, \dots$, $n_2 = 0, 1, 2, \dots$, $n_3 = 0, 1, 2, \dots$, $n_k =$

[§] コンピュータを使うと容易に計算できるが[§] $a_{16} = 987$, $a_{17} = 1597, \dots$, $a_{20} = 6765$, $a_{21} = 10946, \dots$, $a_{25} = 75205$, $a_{26} = 121393, \dots$, $a_{30} = 832040$, $a_{31} = 1346269, \dots$, $a_{35} = 9227465$, $a_{36} = 14930352, \dots$, $a_{39} = 63245986$, $a_{40} = 102334155, \dots$, $a_{44} = 701408733$, $a_{45} = 1134903170, \dots$

[¶] $s > 1$ のとき、 $1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots \leq 1 + \sum_{k=1}^{\infty} \int_k^{k+1} \frac{dt}{t^s} = 1 + \int_1^{\infty} \frac{dt}{t^s} = 1 + \frac{1}{s-1} < \infty$ 。

$0, 1, 2, \dots$, と動かすことにより、全ての自然数が1回ずつ現れることが分かる。よって

$$\begin{aligned}\zeta(s) &= \lim_{k \rightarrow \infty} \sum_{n_1=1}^{\infty} \sum_{n_2=1}^{\infty} \cdots \sum_{n_k=1}^{\infty} p_1^{-sn_1} p_2^{-sn_2} \cdots p_k^{-sn_k} \\ &= \lim_{k \rightarrow \infty} \frac{1}{1-p_1^{-s}} \cdots \frac{1}{1-p_k^{-s}} \\ &= \prod_{k=1}^{\infty} \frac{1}{1-p_k^{-s}} = \prod_{p:\text{素数}} \frac{1}{1-p^{-s}}\end{aligned}\tag{13}$$

再び(3)を使うと

$$\log \zeta(s) = \sum_{p:\text{素数}} \sum_{\ell=1}^{\infty} \frac{p^{-\ell s}}{\ell} = \sum_{p:\text{素数}} p^{-s} + \sum_{p:\text{素数}} \sum_{\ell=2}^{\infty} \frac{p^{-\ell s}}{\ell}\tag{14}$$

この2項目は $s > \frac{1}{2}$ のとき収束するが、特に $s \geq 1$ のとき

$$\begin{aligned}\sum_{p:\text{素数}} \sum_{\ell=2}^{\infty} \frac{p^{-\ell s}}{\ell} &< \frac{1}{2} \sum_{p:\text{素数}} \sum_{\ell=2}^{\infty} p^{-\ell s} \\ &= \frac{1}{2} \sum_{p:\text{素数}} \frac{p^{-2s}}{1-p^{-s}} = \sum_{p:\text{素数}} \frac{1}{2p^s(p^s-1)} \\ &< \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \frac{1}{2} \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = \frac{1}{2}\end{aligned}$$

となるので、 $s > 1$ ならば

$$\log \zeta(s) - \frac{1}{2} < \sum_{p:\text{素数}} \frac{1}{p^s} < \log \zeta(s)\tag{15}$$

である。素数が多いほど、 $\zeta(s)$ が大きくなるので、 $\zeta(s)$ を調べると素数がどの程度あるか分かるに違いない。これが Riemann の発想であった。

たとえば、 $s \rightarrow 1+0$ としてみると

$$\sum_{p:\text{素数}} \frac{1}{p} = \infty\tag{16}$$

が得られるので、少なくとも素数は無限個存在しなくてはならない。

n 番目の素数 p_n は $p_n > n$ を満たす。そこで、 $p_n \geq n^\lambda$ となる 1 より大きな λ が存在するか調べてみよう。もしこれが成り立ったとしてみよう。 N 以下の素数の個数を $\pi(N)$ と書く。 $p_{\pi(N)} \leq N$ であるから $\pi(N) \leq N^{\frac{1}{\lambda}}$ となり、 $\pi(2^n) \leq 2^{\frac{n}{\lambda}}$ である。特に 2^{n-1} 以上 2^n 未満の素数の個数は $2^{\frac{n}{\lambda}}$ 以下である。従って

$$\sum_{\substack{p:\text{素数} \\ 2^{n-1} \leq p < 2^n}} \frac{1}{p} \leq \frac{\pi(2^n)}{2^{n-1}} \leq \frac{2^{\frac{n}{\lambda}}}{2^{n-1}} = 2^{1-n(1-\frac{1}{\lambda})}$$

を $n = 2, 3, \dots$ に関して加えあわせると

$$\sum_{p:\text{素数}} \frac{1}{p} \leq \sum_{n=2}^{\infty} 2^{1-n(1-\frac{1}{\lambda})} = \frac{2^{\frac{2}{\lambda}-1}}{1-2^{1-\frac{1}{\lambda}}} < \infty$$

となって矛盾する。すなわち、1 より大きな任意の実数 λ に対して、適当に n を選べば n 番目の素数 p_n は n^λ より小さくなる。

もう少し良い評価を出してみよう。ある整数 C に対して $\pi(N) \leq C \frac{N}{(\log N)^\lambda}$ が成り立っていたとする。 $\pi(2^n) \leq C \frac{2^n}{(n \log 2)^\lambda}$ であるから、同様にして

$$\sum_{p:\text{素数}} \frac{1}{p} \leq \sum_{n=2}^{\infty} \frac{2C}{(n \log 2)^\lambda} \quad (17)$$

となる。右辺は $\lambda > 1$ のとき有限の値になってしまう。従って、 $\lambda > 1$ ならば正数 C を如何に大きくとっても $\pi(n) > \frac{Cn}{(\log n)^\lambda}$ となる n が存在することがわかる。特に、 $\pi(n) \leq C \frac{n}{(\log n)^\lambda}$ が成り立つとすれば、 $\lambda \leq 1$ でなくてはならない。

実は Gauss が予想した素数定理

$$\pi(n) \sim \frac{n}{\log n} \quad (18)$$

があり、これは J. Hadamard と C. de la Vallée-Poussin によりほとんど同時に証明された (1896 年)。この証明には $s \rightarrow 1$ のとき $\zeta(s) \sim \frac{1}{s-1}$ となること^{||} が用いられた。

Riemann は $(s-1)\zeta(s)$ という関数が $\sum_{n=0}^{\infty} c_n s^n$ という無限級数で書けることを証明した (c_n はある実数)。この無限級数は任意の複素数 s について収束するので $\zeta(s)$ の定義域は $s = 1$ を除く複素数の全体にまで広がる。さらに、 $\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s)$ ^{**} とおくと

$$\xi(s) = \xi(1-s) \quad (\text{Riemann の } \zeta(s) \text{ の関数等式}) \quad (19)$$

が成立することを示した。素数の分布の詳しい様子は、 $\zeta(s)$ の $\text{Re } s \leq 1$ での振る舞いと関係することを Riemann は見抜き、有名な **Riemann 予想**

$$\zeta(s) \text{ が } 0 < \text{Re } s < 1 \text{ において零になるのは } \text{Re } s = \frac{1}{2} \text{ のときに限る} \quad (20)$$

を提出した (1859 年)。この予想が証明されれば

$$\pi(x) = \text{Li } x + O(\sqrt{x} \log x) \quad (21)$$

が成立することが知られている。ここで

$$\begin{aligned} \text{Li } x &:= \lim_{\delta \rightarrow +0} \left(\int_0^{1-\delta} \frac{dt}{\log t} + \int_{1+\delta}^x \frac{dt}{\log t} \right) \\ &= \frac{x}{\log x} + \frac{1!x}{(\log x)^2} + \cdots + \frac{(k-1)!x}{(\log x)^k} + O\left(\frac{x}{(\log x)^{k+1}}\right) \end{aligned}$$

^{||} $s > 1$ のとき $\int_1^\infty \frac{dt}{t^s} < 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots < 1 + \int_1^\infty \frac{dt}{t^s}$ より、 $\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1}$ 。

^{**} $x > 1$ のときは $\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt$ で与えられる。 $\Gamma(x+1) = x\Gamma(x)$, $\Gamma(n+1) = n!$ を満たす。

である。

この Riemann 予想は、現在の数学における最大の未解決問題とみなされているが、大変難しく解決の見通しは立っていない。 $0 < \operatorname{Re} s < 1$ には $\zeta(s)$ の零となる点が無限個あることが知られているが、Hardy は無限個の零点が $\operatorname{Re} s + \frac{1}{2}$ の上にあることを示した (1914 年)。最近の電子計算機による計算では、このうち実軸に近いものから数えて数千万個までは全て $\operatorname{Re} s = \frac{1}{2}$ の上にあることが確かめられている。一方、現在

$$\pi(x) = \operatorname{Li} x + O\left(x \exp\left(-c \frac{(\log x)^{\frac{3}{5}}}{\log(\log x)^{\frac{1}{5}}}\right)\right)$$

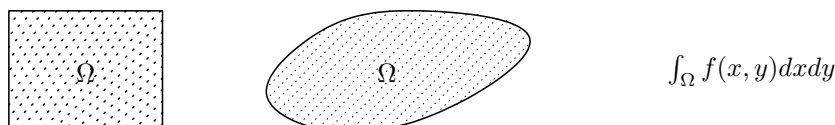
となる正数 c が存在することが知られている。最後に、元の問題に対して

$$p(n) = n \log n + n \log \log n + O(n) \quad (22)$$

という評価が得られていることを述べておく。

7 モザイクのぼかしから元の画像が復元できるか

x - y 平面の画像が関数 $f(x, y)$ で表されているとしよう (たとえば、 $f(x, y)$ は光の 3 原色に分解した赤の明るさ)。 x - y 平面の有界な凸集合 Ω を考え、これを「窓」と考えて、窓を通すと $\int_{\Omega} f(x, y) dx dy$ という情報 (「明るさ」) が得られるとする。「この Ω を動かして得られる「明るさ」の情報から、もとの画像 $f(x, y)$ が決まるか」という問題を考察する。



動かすというのは、回転と平行移動の組み合わせのことで、上の問題を正確に述べれば

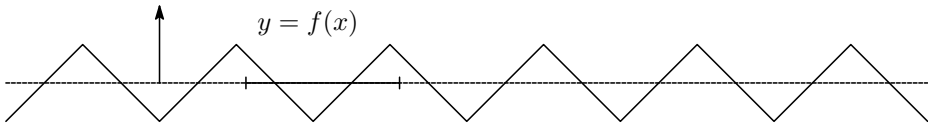
問題 9. 2 変数の関数 $f(x, y)$ に対して

$$h_f(x, y, \theta) = \int_{\Omega} f(x + s \cos \theta - t \sin \theta, y + s \sin \theta + t \cos \theta) ds dt$$

と定義する。このとき、関数 $f(x, y)$ は $h_f(x, y, \theta)$ によって一意に決まるか?

これは、「 $h_f \equiv 0$ ならば $f \equiv 0$ か」ということと同じである。

まず 1 次元の場合を考えてみる。「窓」は幅 1 の線分とすると、 $h_f(x) = \int_0^1 f(x+t) dt$ である。



上記のような周期 1 の関数 $f(x)$ を考えると、 $h_f \equiv 0$ となるので h_f から f の復元は無理である。

一方「2 次元（またはそれ以上の次元）の場合 Ω が円（一般次元の球）でない限り h_f から f が決まる」という予想があり、これを **Pompeiu 問題** という。この予想は、1920 年代からあったが、現在まだ未解決である。しかしながら、具体的な Ω に関しては h_f から f が決まることが分かっている。たとえば、 Ω が長方形ならばよい。

円の場合どうして駄目なのか考えてみよう。 Ω を半径 1 の円とし、まず $f(x, y)$ が y に依らない $\cos \lambda x$ という関数であったとしよう。このとき

$$\begin{aligned} h_f(x, y, \theta) &= 2 \int_{-1}^1 \sqrt{1-t^2} \cos \lambda(x+t) dt = \operatorname{Re} \left(2 \int_{-1}^1 \sqrt{1-t^2} e^{i\lambda(x+t)} dt \right) \\ &= \operatorname{Re} \left(2e^{i\lambda x} \int_{-1}^1 \sqrt{1-t^2} e^{i\lambda t} dt \right) = \operatorname{Re} \left(4e^{i\lambda x} \int_0^1 \sqrt{1-t^2} \cos \lambda t dt \right) \\ &= 4 \cos \lambda x \int_0^1 \sqrt{1-t^2} \cos \lambda t dt = \frac{2\pi}{|\lambda|} \cos \lambda x \cdot J_1(|\lambda|) \end{aligned}$$

となる^{††} (J_1 は 1 次の Bessel 関数)。

$I(\lambda) = \int_0^1 \sqrt{1-t^2} \cos \lambda t dt$ とおくと、 $I(\lambda_0) = 0$ となる λ_0 が存在すれば、 $f(x, y) = \cos \lambda_0 x$ のとき $h_f \equiv 0$ となってしまう。

$I(0) = \frac{\pi}{4}$ であり、一方

$$\begin{aligned} I\left(\frac{5}{3}\pi\right) &= \left(\int_0^{\frac{3}{10}} + \int_{\frac{3}{10}}^{\frac{3}{5}} + \int_{\frac{3}{5}}^{\frac{4}{5}} + \int_{\frac{4}{5}}^{\frac{9}{10}} + \int_{\frac{9}{10}}^1 \right) \sqrt{1-t^2} \cos \frac{5}{3}\pi t dt \\ &\leq \left(1 - \sqrt{1 - \frac{3^2}{5^2}} \right) \int_0^{\frac{3}{10}} \cos \frac{5}{3}\pi t dt + \sqrt{1 - \frac{4^2}{5^2}} \int_{\frac{3}{5}}^{\frac{4}{5}} \cos \frac{5}{3}\pi t dt \\ &= \left(\frac{1}{5} - \frac{3\sqrt{2}}{5 \cdot 3} \right) \frac{3}{5\pi} < 0 \end{aligned}$$

となっている。よって $0 < \lambda < \frac{5\pi}{3}$ の範囲で $I(\lambda) = 0$ となるところがある ($0 \leq \lambda \leq \pi$ のときは、 $I(\lambda) > 0$ が容易に分かるので $\pi < \lambda < \frac{5\pi}{3}$ としてよい)。実際 $J_1(\lambda) = 0$ はこの間にただ一つの根 λ_0 を持つことが分かっており、 $\lambda_0 = 3.8317059 \dots$ である。また、 $J_1(\lambda)$ は正負に振動する関数で、無限個の零点をもつことが知られている。

この関数を原点の周りで回転した $f(x, y) = \cos \lambda_0(x \cos \theta + y \sin \theta)$ も全ての θ に対して、 $h_f \equiv 0$ を満たすので、

$$f(x, y) = \frac{1}{2\pi} \int_0^{2\pi} \cos \lambda_0(\sqrt{x^2 + y^2} \cos \theta) d\theta = J_0(\lambda_0 \sqrt{x^2 + y^2}) \quad (23)$$

^{††} $e^{is} = \cos s + i \sin s$ であるが、 $e^{is} \cdot e^{it} = e^{i(s+t)}$ となることに注意。

に対しても、 $h_f \equiv 0$ が成り立つ (J_0 は 0 次の Bessel 関数)。この $f(x, y)$ は原点を中心として回転不変な関数である。

以上の結果にも関わらず、以下の命題が成立する。

命題 2. Ω を x - y 平面の有界な (空でない) 領域とする。十分大きな R に対して

$$x^2 + y^2 \geq R^2 \text{ ならば } f(x, y) = 0$$

を満たす (有界な台をもつという) 連続関数に対しては、

$$H_f(x, y) = \int_{\Omega} f(x + s, y + t) ds dt \quad (24)$$

から f を復元できる (復元公式は(33))。

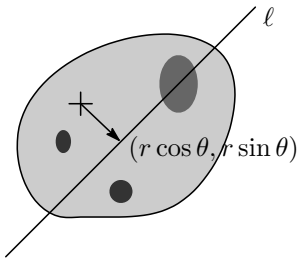
なおこの命題は、2次元でなくても任意の次元で成立する。特に1次元の場合は $h_f(x) = \int_0^1 f(x+t)dt = \int_x^{x+1} f(t)dt$ のとき、 $h'_f(x) = f(x+1) - f(x)$ となるので、 $f(x) = \sum_{n=1}^{\infty} h'_f(x-n)$ である。

Pompeiu 問題は解かれていないが、「円から非常に離れた凸領域」では復元可能なことと、「決められた円に十分近い凸領域で復元不可能な領域は円に限る」ということは証明されている。しかしながら、予想の解決からはかなり遠い。

さて、 Ω の代わりに直線を持ってきたらどうなるであろうか。原点からその直線に下ろした垂線の足を $(r \cos \theta, r \sin \theta)$ とすると

$$R_f(r, \theta) = \int_{-\infty}^{\infty} f(r \cos \theta - t \sin \theta, r \sin \theta + t \cos \theta) dt \quad (25)$$

という積分変換を考えることになる。これは **Radon 変換** と呼ばれているものの一例である。



$$f \mapsto (\ell \mapsto R_f(\ell) = \int_{\ell} f(\ell(t)) dt)$$

$$\ell(t) = (r \cos \theta - t \sin \theta, r \sin \theta + t \cos \theta)$$

ℓ を X 線 (あるいは超音波) の伝わった軌跡とし、 $f(x, y)$ はそれが伝わった場合の減少の割合を表す関数とすると、強さは $e^{-R_f(\ell)}$ 倍に減少する。よって、平面上であらゆる方向から X 線 (あるいは超音波) を当てると f の Radon 変換 R_f が得られる。この R_f から元の f を復元することができれば、すなわち Radon 変換の逆変換が分かれば、もとの平面の各点の状況が得られる。X 線や超音波を用いて頭部や腹部の断層写真を得ることができるのは (例: CT スキャン) この原理に基づいている。

最後に $R_f(r, \theta)$ から f を復元する公式を挙げておこう。平行移動して考えると、 R_f から $f(0, 0)$ が分かればよいことになる。それは

$$f(0, 0) = \frac{1}{4\pi^2} \int_0^{2\pi} \int_0^\infty \frac{2R_f(0, \theta) - R_f(r, \theta) - R_f(-r, \theta)}{r^2} dr d\theta \quad (26)$$

で与えられる^{††}。ただし、 $|f(x, y)|$ は $x^2 + y^2 \rightarrow \infty$ のとき十分速く 0 に収束するものとする（有界な台を持つならよい）。

この公式は「物の世界」と「波動の世界」との対応（双対性）を与える **Fourier 変換** の理論から求められる。 f の Fourier 変換 $\mathcal{F}f$ を

$$\mathcal{F}f(\xi, \eta) = \frac{1}{2\pi} \int_{-\infty}^\infty \int_{-\infty}^\infty f(x, y) e^{-i(x\xi + y\eta)} dx dy \quad (27)$$

と定義すると、その逆変換公式（ f の **Fourier 積分表示**）は

$$f(x, y) = (\mathcal{F}\mathcal{F}f)(-x, -y) = \frac{1}{2\pi} \int_{-\infty}^\infty \int_{-\infty}^\infty \mathcal{F}f(\xi, \eta) e^{i(x\xi + y\eta)} d\xi d\eta \quad (28)$$

で与えられる。これを用いると

$$\begin{aligned} \mathcal{F}f(p \cos \theta, p \sin \theta) &= \frac{1}{2\pi} \int_{-\infty}^\infty \int_{-\infty}^\infty f(r \cos \theta - t \sin \theta, r \sin \theta + t \cos \theta) \\ &\quad \cdot e^{-i(p \cos \theta (r \cos \theta - t \sin \theta) + p \sin \theta (r \sin \theta + t \cos \theta))} dt dr = \frac{1}{2\pi} \int_{-\infty}^\infty R_f(r, \theta) e^{-ipr} dr \end{aligned} \quad (29)$$

なので、 $f(0, 0) = \frac{1}{2\pi} \int_{-\infty}^\infty \int_{-\infty}^\infty \mathcal{F}f(\xi, \eta) d\xi d\eta$ を極座標による積分に直して

$$\begin{aligned} f(0, 0) &= \frac{1}{2\pi} \int_0^{2\pi} \int_0^\infty \left(\frac{1}{2\pi} \int_{-\infty}^\infty R_f(r, \theta) e^{-ipr} dr \right) p dp d\theta \\ &= \lim_{\epsilon \rightarrow +0} \frac{1}{4\pi^2} \int_0^{2\pi} \int_0^\infty \int_0^\infty \left(R_f(r, \theta) + R_f(-r, \theta) \right) \frac{e^{-ip(r-i\epsilon)} + e^{ip(r+i\epsilon)}}{2} p dr dp d\theta \\ &= \lim_{\epsilon \rightarrow +0} -\frac{1}{16\pi^2} \int_0^{2\pi} \int_{-\infty}^\infty \left(R_f(r, \theta) + R_f(-r, \theta) \right) \left(\frac{1}{(r-i\epsilon)^2} + \frac{1}{(r+i\epsilon)^2} \right) dr d\theta \end{aligned}$$

となる。一方 $\epsilon \neq 0$ ならば $\int_{-\infty}^\infty \frac{dr}{(r-i\epsilon)^2} = 0$ であるから上の $R_f(r, \theta) + R_f(-r, \theta)$ を $R_f(r, \theta) + R_f(-r, \theta) - 2R_f(0, \theta)$ に置き換えることができ、置き換えたあとでは非積分関数の $\epsilon \rightarrow +0$ の極限が存在するので(26) が得られる。

実際に断層写真を得る場合は、平面上の全ての直線での Radon 変換の情報を得ることは不可能なので、有限個の直線で近似し、また上の(26) もコンピュータを使って近似的に計算される。

^{††} $(R \cos \phi, R \sin \phi)$ から $\ell(t)$ に下ろした垂線の足は、 $((r - R \cos(\theta - \phi)) \cos \theta, (r - R \cos(\theta - \phi)) \sin \theta)$ であるから、 $F(x, y) = f(R \cos \phi + x, R \sin \phi + y)$ とおくと、 $R_F(r, \theta) = R_f(r - R \cos(\theta - \phi), \theta)$ となり、これによって $f(R \cos \phi, R \sin \phi) = \frac{1}{4\pi^2} \int_0^{2\pi} \int_0^\infty \frac{2R_F(0, \theta) - R_F(r, \theta) - R_F(-r, \theta)}{r^2} dr d\theta$ と求まる。

上記の Radon 変換の逆変換を求めるには、平面上の全ての直線上の積分の情報を用いた。本当に全ての直線上での積分値が必要であろうか？たとえば、 x 軸に平行な直線と y 軸に平行な直線だけではどうであるか考えてみよう。

2	9	4
7	5	3
6	1	8

そこで、

2	9	4
7	5	3
6	1	8

 という 3 次の魔法陣を考えてみる。この魔法陣は x - y 平面上にあって、各辺は x 軸または y 軸に平行であり、その小矩形の一辺の長さが 1 で、数字 5 の入っている小矩形の中心が x - y 平面の原点であると考ええる。

関数 $f(x, y)$ は、 (x, y) が小矩形の内部にあるときは、そこに書いてある数字の値、それ以外では 0 という値をとる関数とする。このとき、 x 軸または y 軸に平行でいずれかの小矩形の内部を通る直線上での $f(x, y)$ の積分値は 15 で、9 つの小矩形に全て数字 5 を書き込んだ場合と同じ結果となる。この例は、 x 軸に平行な直線と y 軸に平行な直線上の積分値だけでは、元の関数を復元できないことを示している。

$e^{i\theta} = \cos \theta + i \sin \theta$ を用いて、Fourier 変換を三角関数で書き直してみる。

$$\mathcal{F}_c f(\xi, \eta) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \cos(\xi x + \eta y) dx dy \quad (30)$$

$$\mathcal{F}_s f(\xi, \eta) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \sin(\xi x + \eta y) dx dy \quad (31)$$

$\mathcal{F}_c f$ を f の **Fourier 余弦変換**、 $\mathcal{F}_s f$ を f の **Fourier 正弦変換** と言うが、 $\mathcal{F}f = \mathcal{F}_c f + i\mathcal{F}_s f$ となるので、元の f はこれらを使って

$$\begin{aligned} f(x, y) &= \mathcal{F}_c \mathcal{F}_c f + \mathcal{F}_s \mathcal{F}_s f \\ &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \mathcal{F}_c f(\xi, \eta) \cos(\xi x + \eta y) d\xi d\eta \\ &\quad + \frac{1}{2\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \mathcal{F}_s f(\xi, \eta) \sin(\xi x + \eta y) d\xi d\eta \end{aligned} \quad (32)$$

と表せる。これは(27), (28)を言い換えただけである。

$f(x, y)$ が x - y 平面における剛体の各点での密度を表しているとする、 $f(x, y)$ は力学的な意味の物質を記述している関数である。上の(32)は、そのような x - y 平面の物質が (ξ, η) をパラメータとする x - y 平面上の波動 $\cos(\xi x + \eta y)$, $\sin(\xi x + \eta y)$ を集めたものとみなすことができることを示す、大変興味深い式である。このとき $\mathcal{F}_c f(\xi, \eta)$, $\mathcal{F}_s f(\xi, \eta)$ はその波動の強さ (振幅密度) を表している。また、 $\mathcal{F}\mathcal{F}f(x, y) = f(-x, -y)$ となることに注意すると、 x - y 平面と ξ - η 平面とはその役割が対等で、「物質」と「波動」の空間は、その役割を逆にしてもよいことがわかる。

x - y 平面の有界領域 Ω の特性関数 $\chi_\Omega(x, y)$ は (x, y) が Ω の点であるとき 1、そうでないとき 0 と定義される。これを用いると、 Ω を (x, y) だけ平行移動した「窓」から

覗いた $f(x, y)$ の平均 $H_f(x, y)$ ((24) を参照) は

$$H_f(x, y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \chi_{\Omega}(s, t) f(x + s, y + t) ds dt$$

と書けるが、 H_f の Fourier 変換は

$$\begin{aligned} \mathcal{F}H_f(\xi, \eta) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \chi_{\Omega}(s, t) f(x + s, y + t) e^{i(\xi x + \eta y)} ds dt dx dy \\ &= \frac{1}{2\pi} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \chi_{\Omega}(s, t) f(u, v) e^{i(\xi(u-s) + \eta(v-t))} du dv ds dt \\ &= 2\pi \mathcal{F}\chi_{\Omega}(-\xi, -\eta) \cdot \mathcal{F}f(\xi, \eta) \end{aligned}$$

となるので ($x = u - s$, $y = v - t$ とおいた)、(28) を用いて

$$f(x, y) = \mathcal{F}\left(\frac{\mathcal{F}H_f(-\xi, -\eta)}{2\pi \mathcal{F}\chi_{\Omega}(\xi, \eta)}\right)(x, y) \quad (33)$$

により f が H_f から復元できる。これは命題 2 の具体的な証明を与えている。ただし、「 f の台が有界でないと $\mathcal{F}f$ の積分は一般には収束しない」などの理由から、台が有界でない一般の f に対してはこの公式を適用することはできない。

($\pm L, \pm L$) を 4 頂点とする正方形の内部を Ω とした場合は、

$$\mathcal{F}\chi_{\Omega}(\xi, \eta) = \mathcal{F}_c\chi_{\Omega}(\xi, \eta) = \frac{2}{\pi} \frac{\sin L\xi}{\xi} \frac{\sin L\eta}{\eta} \quad (34)$$

となるので、具体的な逆変換公式は次のようになる。

$$f(0, 0) = \frac{1}{4} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \frac{\xi\eta \cos(\xi x + \eta y)}{\sin L\xi \cdot \sin L\eta} H_f(x, y) dx dy d\xi d\eta \quad (35)$$

$f(x, y)$ も有界領域の特性関数とすると、「Radon 変換とは、直線がこの領域で切り取られる線分の長さ (最初の問題では、決まった形の領域との共通部分の面積)」に他ならないので、その逆変換を求めることは、「その情報から、もとの有界領域の形を知る」という幾何学的問題を考えていることになる。

また、 $f(x, y)$ が剛体の密度を表していると考えたとき、 $\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) dx dy$ は全質量となる。上で考えた一辺の長さ $2L$ の正方形を Ω とすると、 $f = \frac{\chi_{\Omega}}{4L^2}$ は全質量が 1 となる。「物質」の世界で理想的なものは質点であるが、原点における質量 1 の質点とは、この f の $L \rightarrow 0$ の極限と考えられる。これは数学的には δ 関数として定義されているが、それを「波動」の集まりとみたときは、((34) の両辺を $4L^2$ で割って $L \rightarrow 0$ とすれば分かるように) すべての「波動」を同じ振幅密度 $\frac{1}{2\pi}$ で集めたものと考えることができる。この δ 関数は点に対して値を対応させる関数でなく、普通の関数の概念を拡張して「関数に対して値を対応させる関数」という枠組み、すなわち超関数として扱うことができるが、それについては別の機会に譲りたい。

8 最後に

このノートの記事には、著者の計算ミスや思い違いが含まれているかもしれない。筋道は正しいと思われるので、読者自ら計算を行ってチェックしたり、さらにその先に発展している問題を考えて楽しんでいただけると有り難い。