

ベルヌーイ数の周辺

武隈良一

ベルヌーイの数は解析学，数論，差分方程式などにおいて頻繁にあらわれてくる。それは数学の各部門において重要な役割を果たすので，それに対して一通りの知識をもつことが必要である。しかし何分所どころにしかあらわれないので，まとまった知識とはなりにくい。また実際ベルヌーイの数に関するまとまった書物も二，三はあるが，あまり流布しておらないのが現状である。

本稿においても，もとよりベルヌーイの数に関する知識をまとめようとするものではない。むしろ，ベルヌーイの数がいかに滲透しているかを一，二の題目について述べてみようとするものである。

§1 においてはベルヌーイの数の起源について原典をしらべた結果を述べ，§2 においてはオイラーの定数，§3 においてはフェルマの問題においてベルヌーイの数がいかに重要な役割を果たしているかを最近の研究とともに述べるものである。

§1. ベルヌーイによる自然数の累乗の和の公式とベルヌーイの数

ヤコブス・ベルヌーイ (1654—1705) がいかにして自然数の累乗の和の公式をもとめたかを原典から直接読みとってみよう。原文は彼の死後出版された著書 *Artis Conjectandi* (推論法, 1713^{*}) の第2部順列論と組合せ論の第3章にある。

* この書物については [1] に詳述したことがある。[n] は後掲文献の番号をあらわす。

彼はまず次の組合せの表をあたえた。

	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
1	1	0	0	0	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0	0	0
3	1	2	1	0	0	0	0	0	0	0	0	0
4	1	3	3	1	0	0	0	0	0	0	0	0
5	1	4	6	4	1	0	0	0	0	0	0	0
6	1	5	10	10	5	1	0	0	0	0	0	0
7	1	6	15	20	15	6	1	0	0	0	0	0
8	1	7	21	35	35	21	7	1	0	0	0	0
9	1	8	28	56	70	56	28	8	1	0	0	0
10	1	9	36	84	126	126	84	36	9	1	0	0
11	1	10	45	120	210	252	210	120	45	10	1	0
12	1	11	55	165	330	462	462	330	165	55	11	1

この表を見ているといろいろの関係式が成立することが分る。ベルヌーイはこの数表についての驚くべき性質を12ほどあげているが、今日から見ればそれらは組合せ論においてよく知られたものである。これを利用して自然数の累乗の和を次のようにもとめている。(〔2〕の32頁,〔3〕の88頁)

まず自然数 $1, 2, \dots, n$ の和をもとめるのに、上の組合せの表の第 II 列の一般項は $n-1$ なので、それらの総和は

$$\int_{n-1} = 0+1+\dots+(n-1)$$

と書かれるが、この和が $\frac{n(n-1)}{1 \cdot 2}$ に等しいという。

(その理由は上の表において

$$\frac{0+1+2+\dots+(n-1)}{(n-1)+(n-1)+\dots+(n-1)} = \frac{1}{2}$$

が成立するからであるという。) それ故

$$\int_{n-1} = \int_n - \int_1 = \frac{nn-n}{2}$$

故に
$$\int n = \frac{nn-n}{2} + \int 1 = \frac{nn-n}{2} + n$$

故に
$$\int n = -\frac{1}{2}nn + \frac{1}{2}n$$

ともとまる。

次に自然数の平方の和をもとめるのに、上の組合せの表の第Ⅲ列の一般項は

$$\frac{n-1 \cdot n-2}{1 \cdot 2} = \frac{nn-3n+2}{2}$$

なので、その総和は

$$\int \frac{n^2-3n+2}{2} = \int \frac{1}{2}nn - \int \frac{3}{2}n + \int 1$$

となるが、この和が $\frac{n \cdot n-1 \cdot n-2}{1 \cdot 2 \cdot 3}$ に等しいこと（これが上の表における

既知性質）を用いると、

$$\int \frac{1}{2}nn - \int \frac{3}{2}n + \int 1 = \frac{n^3-3nn+2n}{6}$$

から

$$\begin{aligned} \int \frac{1}{2}nn &= \frac{n^3-3nn+2n}{6} + \int \frac{3}{2}n - \int 1 \\ &= \frac{n^3-3nn+2n}{6} + \frac{3nn+3n}{4} - n \\ &= -\frac{1}{6}n^3 + \frac{1}{4}nn + \frac{1}{12}n \end{aligned}$$

故に
$$\int nn = -\frac{1}{3}n^3 + \frac{1}{2}nn + \frac{1}{6}n$$

ともとまる。

同様に自然数の立方の和をもとめるのに、上の組合せの表の第Ⅳ列の一般項は

$$\frac{n-1 \cdot n-2 \cdot n-3}{1 \cdot 2 \cdot 3} = \frac{n^3-6nn+11n-6}{6}$$

なので、その総和が

$$\frac{n \cdot n-1 \cdot n-2 \cdot n-3}{1 \cdot 2 \cdot 3 \cdot 4} = \frac{n^4 - 6n^3 + 11nn - 6n}{24}$$

に等しいことを用いると

$$\int \frac{1}{6} n^3 - \int nn + \int \frac{11}{6} n - \int 1 = \frac{n^4 - 6n^3 + 11nn - 6n}{24}$$

から
$$\int n^3 = \frac{1}{4} n^4 + \frac{1}{2} n^3 + \frac{1}{4} nn$$

ともとまる。

このように一般項が $\frac{n-1 \cdot n-2 \cdot \dots \cdot n-r}{1 \cdot 2 \cdot \dots \cdot r}$ である数列の総和が

$$\frac{n \cdot n-1 \cdot n-2 \cdot \dots \cdot n-r}{1 \cdot 2 \cdot 3 \cdot \dots \cdot r+1}$$

に等しいという組合せの性質を用いて、自然数の累乗の和の公式を導いたのがベルヌーイである。4乗以上の和の公式は次の通りである。

$$\int n^4 = \frac{1}{5} n^5 + \frac{1}{2} n^4 + \frac{1}{3} n^3 * - \frac{1}{30} n$$

$$\int n^5 = \frac{1}{6} n^6 + \frac{1}{2} n^5 + \frac{5}{12} n^4 * - \frac{1}{12} nn$$

$$\int n^6 = \frac{1}{7} n^7 + \frac{1}{2} n^6 + \frac{1}{2} n^5 * - \frac{1}{6} n^3 * + \frac{1}{42} n$$

$$\int n^7 = \frac{1}{8} n^8 + \frac{1}{2} n^7 + \frac{7}{12} n^6 * - \frac{7}{24} n^4 * + \frac{1}{12} nn$$

$$\int n^8 = \frac{1}{9} n^9 + \frac{1}{2} n^8 + \frac{2}{3} n^7 * - \frac{7}{15} n^5 * + \frac{2}{9} n^3 * - \frac{1}{30} n$$

$$\int n^9 = \frac{1}{10} n^{10} + \frac{1}{2} n^9 + \frac{3}{4} n^8 * - \frac{7}{10} n^6 * + \frac{1}{2} n^4 * - \frac{1}{12} nn$$

$$\int n^{10} = \frac{1}{11} n^{11} + \frac{1}{2} n^{10} + \frac{5}{6} n^9 * - 1n^7 * 1n^5 * - \frac{1}{2} n^3 * \frac{5}{66} n$$

ここに*印は空欄をしめしている。

ここまでは組合せ論と自然数の累乗の和の関係を物語るもので、今日から見ればさしたることもないが、これより進んでベルヌーイはこの自然数の累乗の和の一般公式を次のように述べたことが驚くべきことである。

$$\begin{aligned} \int n^c &= 1^c + 2^c + \dots + n^c \\ &= \frac{1}{c+1} n^{c+1} + \frac{1}{2} n^c + \frac{c}{2} A n^{c-1} + \frac{c \cdot c - 1 \cdot c - 2}{2 \cdot 3 \cdot 4} B n^{c-3} \\ &\quad + \frac{c \cdot c - 1 \cdot c - 2 \cdot c - 3 \cdot c - 4}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} C n^{c-5} \\ &\quad + \frac{c \cdot c - 1 \cdot c - 2 \cdot c - 3 \cdot c - 4 \cdot c - 5 \cdot c - 6}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8} D n^{c-7} + \dots \end{aligned}$$

ここに n のべき指数は第 3 項以下 2 ずつ下って n 又は n^2 でおわる。 A , B , C , D ……は定数で $\int n$, $\int n^3$, $\int n^5$, $\int n^7$ ……における n の係数を表わす。すなわち

$$A = \frac{1}{6}, \quad B = -\frac{1}{30}, \quad C = \frac{1}{42}, \quad D = -\frac{1}{30} \dots\dots$$

となる。これらを求めるには、その係数を含む式のすべての項の係数の和が 1 であることから得られる。すなわち

$$\frac{1}{3} + \frac{1}{2} + A = 1 \quad \therefore A = \frac{1}{6}$$

$$\frac{1}{5} + \frac{1}{2} + \frac{1}{3} + B = 1 \quad \therefore B = -\frac{1}{30}$$

$$\frac{1}{7} + \frac{1}{2} + \frac{1}{2} - \frac{5}{6} + C = 1 \quad \therefore C = \frac{1}{42}$$

$$\frac{1}{9} + \frac{1}{2} + \frac{2}{3} - \frac{7}{15} + \frac{2}{9} + D = 1 \quad \therefore D = -\frac{1}{30}$$

というように。

この公式の説明においてどこに驚くべき点があるかについては、「推論法」の Robert Haussner による独訳 [4] に附せられている興味深い註が

次のように述べている。

「この主張は帰納的証明がやや科学的ではないので、ベルヌーイはおのずと不完全帰納法を用いていることになる。読者はこれらの言葉に奇異の感をもたれることと思うが、ベルヌーイはこの不完全帰納法から天才的なやり方で、 $S(n)$, $S(n^2)$, …… $S(n^{10})$ の公式から $S(n^c)$ の公式を導いたのである。この公式の n^{c-1} , n^{c-3} , n^{c-5} , …の係数から因数 $\frac{1}{2} \binom{c}{1}$, $\frac{1}{4} \binom{c}{3}$, $\frac{1}{6} \binom{c}{5}$, … をとりさった第 2 因数が定数として残り、それらは我々の知識から遠ざかるものである。

カントルの数学史 (第 III 卷序言 IX—X 頁) によると Schwering がこの研究を再び行なっており、それによると n^{c-1} 以下は次数が 2 ずつ低くならねばならぬという。このことはベルヌーイが上に述べた $c=10$ までの公式において一致するので、シュウェリングの研究はベルヌーイの思考過程と一致する。

しかし依然として不明な点は、ベルヌーイがいかにして、係数 A , B , C ……が定数であり、かつ交互に正負の数であることを知っていたかにある。もっともこのことをはじめて明らかにしたのは後年のオイラーで、彼は三角級数の助けを借りてこれを証明した。これについては彼の著書 *Institutiones Calculi differentialis* (1755) 第 2 卷第 5 章を見られたい。

それ故 A , B , C ……が交互に正又は負の値をとることを、その本来の定義を基礎として証明することは今日未だなされておらないのである。そして $S(n^c)$ に対する公式の現代における導入はそれらがただ定数であることをしめすばかりである。(つまり、オイラー以後いろいろな方法で導かれてはいるが、 A , B , C , D ……が交互に正又は負の定数であること、またこれらの数が上のように求まることをどのようにしてベルヌーイが知っていたかが問題であり、本来の定義からの直接の証明が問われているのである。——筆者注)

このA, B, C, D……にベルヌーイの数という名称を与えたのはド・モァヴル (Miscellanea analytica, London 1730) とオイラーである。

係数A, B, C, D……を順次に求めるベルヌーイの法則は次のように述べられる。すなわちいま, A, B, C, D……の代りに $B_1, -B_2, B_3, -B_4, \dots$ とおけば

$$\sum_{i=1}^m (-1)^i \binom{2m+1}{2i} B_i + m - \frac{1}{2} = 0$$

なる関係式が成立する。これを詳しく書くと $m=1, 2, 3$ に対して

$$(-1) \binom{3}{2} B_1 + 1 - \frac{1}{2} = 0$$

$$(-1) \binom{5}{2} B_1 + (+1) \binom{5}{4} B_2 + 2 - \frac{1}{2} = 0$$

$$(-1) \binom{7}{2} B_1 + (+1) \binom{7}{4} B_2 + (-1) \binom{7}{6} B_3 + 3 - \frac{1}{2} = 0$$

となる。この関係式はド・モァヴルの公式といわれるが、それは正しくない。何故ならド・モァヴルはベルヌーイが述べた法則をただ式に書きあらわしただけで、それが成立することの証明をしておらないからである。」

以上はハウスネルの註釋であるが、ベルヌーイ数の由来がうかがわれて興味深く感ぜられる。これによれば小著数学史の次の部分は誤りである。

「この和を求める際に次の式

$$\frac{x}{e^x - 1} = B_0 + B_1 \frac{x}{1!} + B_2 \frac{x^2}{2!} + B_3 \frac{x^3}{3!} + \dots + B_n \frac{x^n}{n!} + \dots$$

の右辺の級数の係数が問題となる。この係数をベルヌーイの数という。」〔5〕147頁。

これを次のように訂正しておこう。

「 $\int n^c = 1^c + 2^c + \dots + n^c$ を求める公式として

$$= \frac{1}{c+1} n^{c+1} + \frac{1}{2} n^c + \frac{c}{2} A n^{c-1} + \frac{c \cdot c-1 \cdot c-2}{2 \cdot 3 \cdot 4} B n^{c-3}$$

$$\begin{aligned}
& + \frac{c \cdot c-1 \cdot c-2 \cdot c-3 \cdot c-4}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} Cn^{c-5} \\
& + \frac{c \cdot c-1 \cdot c-2 \cdot c-3 \cdot c-4 \cdot c-5 \cdot c-6}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8} Dn^{c-7} + \dots
\end{aligned}$$

を与えている。ここに A, B, C, D……は後にオイラーによってベルヌーイの数とよばれた。」

§2. オイラーの定数

オイラーの定数というのは周知のように次の数列

$$u_n = 1 + \frac{1}{2} + \dots + \frac{1}{n} - \log n$$

の極限值

$$\begin{aligned}
r &= \lim_{n \rightarrow \infty} \left(1 + \frac{1}{2} + \dots + \frac{1}{n} - \log n \right) \\
&= 0.57721 \quad 56649 \quad 01532 \dots
\end{aligned}$$

を意味する。これはまたマスケロニ (Lorenzo Mascheroni 1750—1800) の定数ともよばれるが、実は彼はただ32桁まで計算したに過ぎない。(藤原松三郎, 微分積分学, I, p. 46)

さてこのオイラーの定数を計算するのにベルヌーイの数を必要とするが、最近 D. E. Knuth [6] によって小数点以下1271桁まで計算された。これについて以下に述べよう。

そもそもオイラーの定数は彼自身によって1735年に0.577218……と計算され、1781年には一層精密に0.5772156649015325……と計算された。この計算は後に多くの数学者によって一層精密になされたが、なかんずくガウスによって

$$r = 0.57721566490153286060653 \dots$$

と計算された。ガウス全集第3巻154頁には40桁まで示されている。

その後1870年前後にイギリスの数学者 J. W. L. Glaisher と W. Shanks

とがこの計算を続けたが、遂に数学者であり同時に海王星の存在を予言した天文学者として有名な J. C. Adams (1819—92)によって1878年から1887年に263桁まで計算された。これはシャンクスが得た110桁（ただしこれの101桁は誤り）をさらに進めたものである。アダムスの結果は1952年までそのままであったが、同年 Wrench によって328桁まで計算された。

これを他方この r が有理数であるかどうかを決定する試みが数多くなされたこと（ただしこれは現在未解決）に比べれば、 r の値を求めることはあまり進んでいないといえる。それというのも高速度計算機により π は10万桁（1962）まで、 e は6万桁（1953）まで求まっているからである。その理由は r の値を求めることは相当に難かしいからという外はない。

さて r の値を求める技術は本質的にはアダムスや早期の数学者の用いたものと同じである。それらは周知のもので次の通りである。まずオイラーの総和公式

$$(1) \quad \sum_{i=1}^n f(i) = \int_1^n f(x) dx + \frac{1}{2} (f(n) + f(1)) \\ + \sum_{j=1}^k \frac{B_{2j}}{(2j)!} \left[f^{(2j-1)}(n) - f^{(2j-1)}(1) \right] + R_k$$

を用いる。ここに B_m は次の式

$$(2) \quad e^{Bx} = \frac{x}{e^x - 1}$$

によって記号的に定義されるベルヌーイ数である。この記号によれば

$$B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}$$

となる。また剰余は次の式

$$(3) \quad R_k = \frac{1}{(2k+1)!} \int_1^n P_{2k+1}(x) f^{(2k+1)}(x) dx$$

によって与えられ、 $P_{2k+1}(x)$ は周期ベルヌーイ多項式で、記号的に次の式

$$(4) \quad P_{2k+1}(x) = (\{x\} + B)^{2k+1} - (-1)^{k-1} (2k+1)! \sum_{r=1}^{\infty} \frac{2 \sin 2r\pi x}{(2r\pi)^{2k+1}}$$

で与えられる。ここに $\{x\}$ は x の分数部分である。

さていま $f(x) = \frac{1}{x}$ とおけば、(1)より

$$(5) \quad 1 + \frac{1}{2} + \cdots + \frac{1}{n} = \log n + \frac{1}{2} + \frac{1}{2n} + \frac{B_2}{2} \left(1 - \frac{1}{n^2}\right) + \cdots + \frac{B_{2k}}{2k} \left(1 - \frac{1}{n^{2k}}\right) - \int_1^n \frac{P_{2k+1}(x)}{x^{2k+2}} dx$$

となる。この(5)において $n \rightarrow \infty$ とすれば、

$$(6) \quad r = \frac{1}{2} + \frac{B_2}{2} + \cdots + \frac{B_{2k}}{2k} - \int_1^\infty \frac{P_{2k+1}(x)}{x^{2k+2}} dx$$

となる。(6)から(5)を引くと

$$(7) \quad r = 1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n - \frac{1}{2n} + \frac{B_2}{2n^2} + \cdots + \frac{B_{2k}}{(2k)n^{2k}} - \int_n^\infty \frac{P_{2k+1}(x)}{x^{2k+2}} dx$$

となる。この式の剰余について考えてみよう。まず

$$(8) \quad |P_{2k+1}(x)| \leq \frac{2(2k+1)!}{(2\pi)^{2k+1}} \sum_{r=1}^{\infty} \frac{1}{r^{2k+1}}$$

なるを以て、(8)にスターリングの公式を用いると

$$(9) \quad \left| \int_n^\infty \frac{P_{2k+1}(x)}{x^{2k+2}} dx \right| \leq \frac{4}{n} \sqrt{\frac{k}{\pi}} \left(\frac{k}{n\pi e}\right)^{2k}$$

となる。いま $k=250$, $n=10000$ とおくと

$$(10) \quad \left| \int_{10000}^\infty \frac{P_{501}(x)}{x^{502}} dx \right| < 10^{-1269}$$

となる。これを(7)に用いると少なくとも1269桁まで r を決定することができる。

そこでいよいよ r の実際の計算へと進もう。まず、 $1 + \frac{1}{2} + \cdots + \frac{1}{10000}$ は

$$(11) \quad S_{10000} = \frac{3}{2} + \frac{7}{12} + \cdots + \frac{19999}{99990000} = 9.787606036 \dots$$

と求まる。次に1000の自然対数は

$$(12) \quad \log 10000 = -252 \log(1-0.028) \\ + 200 \log(1+0.0125) + 92 \log(1-0.004672)$$

によって決定される。

この展開式は小数をあつかう計算機を用いるとき早く収束しようとする便宜のために作られたものである。まず $2^x 3^y 5^z \approx 1$, $y \geq 0$ を満足する (x, y, z) を求めると、次の3組のものが得られる。

$$(-1, 5, -3), (-4, 4, 1), (6, 5, -6)$$

すなわち

$$2^{-13} 5^{-3} = \frac{243}{250} = 1 - \frac{7}{250} = 1 - 0.028$$

$$2^{-43} 5^{-1} = \frac{81}{80} = 1 + \frac{1}{80} = 1 + 0.0125$$

$$2^6 3^5 5^{-6} = \frac{15552}{15625} = 1 - \frac{73}{15625} = 1 - 0.004672$$

となる。これを用いて(12)が得られる。しかし2進計算機の場合には $z \geq 0$ の条件が加わるので展開式を求めることは一層困難となるが、次の解が与えられている。

$$(12a) \quad \log 10000 = 160 \log 2^{-32} 3^7 5^9 - 864 \log 2^{-11} 3^4 5^2 + 292 \log 2^{-15} 3^8 5$$

最後にベルヌーイ数 $B'_{2k} = 10^{-8k} B_{2k}$ は次の回帰公式から計算される。

$$(13) \quad \binom{2k+1}{2k} B'_{2k} + 10^{-8} \binom{2k+1}{2k-2} B'_{2k-2} + \dots + 10^{8-8k} \binom{2k+1}{2} B'_2 = \frac{(2k-1)}{2 \cdot 10^{8k}}$$

この式において、次の事実

$$(14) \quad \left| \frac{B_{2k}}{B_{2k-2}} \right| \approx \frac{2k(2k-1)}{4\pi^2}$$

を認めると、影響を及ぼすような打ち切り誤差が生じないことがわかる。その上実際には1300桁までが計算に用いられている。

B'_{2k} を求めるのに (13) を用いると、まずすべての正の項が一しょに加えられ、次にすべての負の項が一しょに加えられ、最後にこの両者が一しょにされる。これは計算に非常な速度を与える。また 0 をかけることを避ける注意が払われている。k が増加するとき B'_{2k} の値を求めることは次第に困難になる。それというのも項の数と 2 項係数の大きさが増大するからである。 B_n は交互に符号を変えるので、 r の計算における実際の誤差は

$$\frac{B'_{502}}{502} \approx +0.25 \times 10^{-1271}$$

より小さくなるので、ここに得られる値は 1271 桁まで正しいことになる。この結果はアダムスの値を容認するものであり、多くの調査によりこの結果の精密さが保証されている。ウレンチ博士は独立に 1039 桁まで検証した。

以上行なわれた計算は Burroughs 220 計算機によって行なわれたものである。 S_{10000} は約 1 時間で、対数の各々は約 6 分を要した。250 個のベルヌーイ数の計算は最も時間を要したところであり、それらの全計算には約 8 時間を費した。1270 D までのベルヌーイ数の表は Math. of Comp. の未発表数学表ファイルに送られている。また 1271 桁の実際の数値は [6] に記されている。

最後に r の連分数展開について述べよう。いま

$$r = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}$$

とあらわそう。すると $a_i \neq 0 (i > 1)$ なるときそしてこのときに限り r は無理数となり、また a_i の部分列が周期的なるときそしてこのときに限り r は 2 次無理数になる。この判定条件を用いることによって r が無理数であるかないかが分るのであるが、いまのところすべての a_i が分らぬのでなんともいえない。

また r の「最良有理近似数」はいろいろと与えられるが、手近のものとしては

$$\frac{228}{395} = 0.5772152$$

がある。これは小数第6桁まで正しい。

なお無理数を正則連分数に展開したときの部分分母を a_i とするとき、ほとんどすべての無理数に対して、

$$\lim_{n \rightarrow \infty} \sqrt[n]{a_2 a_3 \cdots a_{n+1}}$$

は一定値 K をもつ。この K は **ヒンチンの定数** とよばれ次の式で与えられる。

$$K = \prod_{r=1}^{\infty} \left\{ 1 + \frac{1}{r(r+1)} \right\}^{\log_2 r} = 2.68545 \dots$$

r においてこれを実際に計算してみると

$$\sqrt[371]{a_2 a_3 \cdots a_{372}} \approx 2.692$$

となり、これは K に近い。

以上でオイラーの定数は1271桁までも求めたので、当分の間はこれ以上に発展しないものと思われたが、昨年1963年に W. Sweeney [7] がベルヌーイ数を用いる在来の方法によらずさらに3566桁までも求めた。

彼の方法は指数積分の展開を用いるもので、この新しい方法はベルヌーイ数の高次のものの計算に要求される複雑なプログラミングを避けるものである。

指数積分とは次のものを表わす。

$$\begin{aligned} (1) \quad -E_i(-x) &= \int_x^{\infty} \frac{e^{-t} dt}{t} \\ &= -\gamma - \log x + x - \frac{x^2}{2 \cdot 2!} + \frac{x^3}{3 \cdot 3!} - \dots \\ &= -\gamma - \log x + S(x) \end{aligned}$$

またその漸近展開は

$$(2) \quad -E_i(-x) = \int_x^{\infty} \frac{e^{-t} dt}{dt}$$

$$\cong \frac{e^{-x}}{x} \left(1 - \frac{1}{x} + \frac{2!}{x^2} - \dots \right) = R(x)$$

と表わされるので、両式を等しいとおいて r を左辺へうつすと

$$(3) \quad r \cong S(x) - \log(x) - R(x)$$

となる。この式を用いて r を計算するのであるが、 $x = 2^{13} = 8192$ とおくと

$$(4) \quad R(x) = 0.22190 \dots \times 10^{-3561}$$

となる。 $x = 8192$ としたのは x として 2 の累乗をとると $\log x$ の計算がしやすいからである。

さて $\log 2$ の計算は次の式

$$(5) \quad \log 2 = \frac{1}{2} + \frac{1}{2 \cdot 2^2} + \frac{1}{3 \cdot 2^3} + \dots$$

によって非常に速く求められる。また r を求めるための計算機の活動は次の 2 つに分けて行なわれる。第 1 はまず次の式により $\log x$ を求める。

$$(6) \quad 13 \log 2 = 13 \left[\frac{5}{1 \cdot 1 \cdot 2^3} + \frac{11}{2 \cdot 3 \cdot 2^5} + \frac{17}{3 \cdot 5 \cdot 2^7} + \dots \right]$$

ついで $S(x)$ を次の式により求める。

$$(7) \quad S(x) = \left(x + \frac{x^3}{3 \cdot 3!} + \dots \right) - \left(\frac{x^2}{2 \cdot 2!} + \frac{x^4}{4 \cdot 4!} + \dots \right) \\ = x + \sum D_{2n+1} - \sum D_{2n}$$

これらの D は次の式で表わされる。

$$(8) \quad C_{2n} = \frac{x^{2n+1}}{(2n)!} = \frac{x^2}{2n(2n-1)} D_{2n-2}$$

$$(9) \quad D_{2n+1} = \frac{C_{2n}}{(2n+1)^2}, \quad D_{2n} = \frac{C_{2n}}{2nx}$$

計算機の第 2 の活動は次の処置を行なうことにある。 $\log 8192$ は $n = 12, 300$ にはじまる次の回帰公式から値が求まる。

$$(10) \quad \log 8192 = 13B_1, \quad B_n = \frac{1}{2} \left(\frac{1}{n} + B_{n+1} \right)$$

また $S(x)$ は $n=30,000$ にはじまる次の回帰公式から値が求まる。

$$(11) \quad S(x) = xA_1, \quad A_n = 1 - \frac{nx}{(n+1)^2} A_{n+1}$$

以上を完全に計算することは IBM 7094 のエンジニア・モデルによって 58分 でなされた。このうち第1の活動はほぼ20分 でなされ、第2の活動はほぼ35分 を要した。残りの時間は、結果の重なりあわない印刷やパンチに費された。

§3. フェルマの問題

フェルマの問題とは周知のように

$$(1) \quad x^p + y^p = z^p, \quad (x, y, z) = 1, \quad (p \text{ は奇素数})$$

に正の整数解(今後単に解とよぶ)がないことを証明せよという問題である。

この問題は1637年に提出されて以来今日にいたるも未解決である。今日まで解決された経路を以下に述べることは到底紙数が許さないが、ベルヌーイ数に関連した部分を中心にその概観を述べてみよう。

最初この問題は $p+xyz$ の場合と p/xyz の場合において研究された。前者を第1の場合といい、後者を第2の場合という。

第1の場合において今世紀の始め A. Wieferich (1909) が次の結果を発表してセンセーションを起こした。

定理. 1. 素数 p が次の合同式

$$(2) \quad \frac{2^{p-1} - 1}{p} \equiv 0 \pmod{p}$$

を満足しないならば、フェルマの方程式(1)は解をもたない。

ところが(2)を満足する素数は $p=1093$ と 3511 だけらしい。したがってこの2つの素数以外の場合には(1)が解をもたないことになる。らしいといったのは、その検証がすべての素数についてなされる訳ではないからである。 p が大きくなれば(2)の左辺(これをフェルマの商という)の計算は複雑になるので容易ではないが、今日では計算機により 200,183 までの間にはこの2

つの素数以外に(2)を満足するものがないことが調らべられている。〔8〕

(2)はその後多くの人によって拡張され次の定理にまで発展した。

定理. 2. 素数 $q \leq 43$ の少なくとも 1 つに対して, $q^{p-1} \not\equiv 1 \pmod{p^2}$ であれば(1)に解はない。

D. H. Lehmer と E. Lehmer は 1941 年にこの定理を用いて, $p < 253, 747, 889$ のとき(1)に解がないことを確めた。〔9〕

第 1 の場合はこのように p の相当大きな値に対して解の存在しないことが確かめられているが, 第 2 の場合はこれ程うまうまいか。それというのも, 第 2 の場合は問題が一層困難となり, その上各々の素数について 1 つずつ調べていかねばならないからである。

そこでいっそのこと 2 つの場合に分けることを止め, $p + xyz$ という制限を撤廃して研究しようとする方針がとられた。このときベルヌーイ数に關係のある正則素数が問題となる。

定義. $B_1, B_2, \dots, B_{(p-3)/2}$ のどの分子 (既約分数として) も p で割切れないとき p を正則素数 (regular prime) といい, 割切れるとき不正則素数 (irregular prime) という。

この正則素数に対して 1850 年に Kummer は次の定理を得ている。

定理. 3. p が正則素数なるとき(1)は解をもたない。

この有名な定理は数論における最も深い結果の 1 つである。E. Landau (1877—1938) は自著 Vorlesungen über Zahlentheorie (1927) の第 3 巻において上の定理を証明するのに必要な代数的整数論の知識を詳しく述べている。ランダウ流の (定理証明定理証明……とかく) 書き方を以てしても上の定理の証明には 50 頁は優に必要である。それは円体の類数 h をまとまった形に導くのに議論が長くかかるからである。その議論は無限級数の極限として代数体の類数を求めることにあり, またこの極限が円体に應用されたとき無限の形で与えられることにある。

ところで不正則素数は 37, 59, 67, 101, 103, 131, 149, 157 であること

をクummerは知っていた。それでこの場合にも(1)が解をもたないことを証明するために新しい判定法を工夫したが、これは 37, 59, 67 にしか適用されなかった。その結果クummerは 100 以下の素数と 100 以上の正則素数について(1)が解をもたないことをしめすに止まった。

そこで 100 以上の不正則素数について問題は残ったが、これに手をつけたのは Vandiver である。彼はまず次の定理を証明した。

定理. 4. (Vandiver, 1929. [11])

(1) 円体 $k(\zeta)$ の類数の第 2 因数 h_2 が p と素である。

(2) ベルヌーイの数 B_{nl} , $n=1, 2, \dots, \frac{1-3}{2}$ のどの 1 つも l^3 で割切れない。

この 2 つの仮定があるとき(1)は解をもたない。

この定理とこれに関連ある二、三の定理を用いることによって Vandiver は 1928 年から 1936 年にかけて 619 までの不正則素数について(1)が解をもたないことを複雑な計算の結果確かめた。この労苦はおそらく大変なものであったと思われるが、計算機出現以前の時代としては止むを得ないことである。以上が戦前における発展の経路であるが、その詳細は [10] において見ることが出来る。

次に戦後に計算機が出現してからは不正則素数に対する計算が容易に（といっても戦前に比べてであるが）なったのでそれについて述べよう。不正則素数に対してフェルマの問題が成立するか否かを確かめるには次の定理を用いるのである。

定理. 5. (Vandiver, [11])

$B_1, B_2, \dots, B_{(p-3)/2}$ のうちに分子が p で割切れるものがあるとして、それらを B_{a_1}, \dots, B_{a_s} とする。正の整数 k, t と素数 q とを

$$q=1+kp, \quad q < p^2-p, \quad t^k \equiv 1 \pmod{q}$$

を満足するようにとることができたとして

$$d = 1^{p-a} + 2^{p-2a} + \dots + \left(\frac{p-1}{2}\right)^{p-2a}$$

$$Q_a = t^{-kd/2} \prod_{b=1}^{(p-1)/2} (t^{bk} - 1)^{b^{p-1-2a}}$$

とおく。このとき $Q_{a_i}^k \equiv 1 \pmod{q}$ ($i=1, 2, \dots, s$)

ならば(1)に解はない。

Lehmer—Lehmer—Vandiver [12] はこの定理を用いて1954年に1997までの不正則素数について(1)が解をもたないことを証明した。次いで Vandiver [13] は同年2503までの不正則素数について, Selfridg—Nicol—Vandiver [14] は1955年に4001までの不正則素数について証明した。しかもこれらの計算はみな SWAC (Los Angeles) を用いてなされた。

以上で今日までのフェルマの問題の発展を述べたが, これを概括すると, 第1の場合には $p < 253,747,889$ まで, 第2の場合には $p < 4001$ まで解決されたことになる。また定理4の第1の仮定 $(h_2, p) = 1$ は証明されていないが, これは正しいであろうと予想されている。そして実は第1の場合にはこの仮定だけが必要なので, もしも $(h_2, p) = 1$ という予想が証明されれば, 第1の場合には解決されることになる。これに反して第2の場合にはベルヌーイ数に関する第2の仮定を必要とするので一寸問題は複雑になる。以上の結果からみれば1637年以来300年以上経た今日可成の成果をあげていることが分ろう。

さて問題を前進させて, まず正則素数と不正則素数との割合を考えてみよう。すると $3 \leq p \leq 4001$ の間では正則素数は334個あり, 不正則素数は216個あることが分っている。また正則素数は有限個あるか無限個あるかという問題も起こる。もし後者が証明されればクムマーの定理は非常に有力なものとなるが, おそらくは前者ではないかといわれている。その理由の1つとして Vandiver は600の附近には不正則素数が以外に多いことをあげている。547, 557, 577, 587, 593, 607 がそれである。また他の理由として1915年 Jensen によって次の定理が証明されている。

定理. 6. $4n+3$ なる形の不正則素数は無限にある。

したがって将来に残された問題は次のいずれかを証明することにある。

- (1) 正則素数は有限個しか存在しない。
- (2) 正則素数と不正則素数はともに無限個存在して、その割合は一定である。

ただしこれが解決されたからといってすぐにフェルマの問題の解決へと直結されるものではない。定理6により不正則素数は無限に存在するので計算機を用いて確かめていってもそれは徒勞というほかはない。

最後に定理6の証明を〔15〕によって述べてみよう。まず次の補題を証明する。

補題 $S_i(a) = 1^i + 2^i + \dots + (a-1)^i \dots\dots\dots (1)$

ならば

$$S_{2n}(2^k) \equiv 2^k b_{2n} \pmod{2^{k+1}}, n > 1, k > 1 \dots\dots\dots (2)$$

である。

証明、まずよく知られたベルヌーイ和の公式 ([16] p.254) により

$$S_{2n}(2^k) = \binom{2n+1}{1} \frac{b_{2n} 2^k}{2n+1} + \binom{2n+2}{2} \frac{b_{2n-1} 2^{2k}}{2n+1} + \dots + \frac{2^{k(2n+1)}}{2n+1}$$

となる。ここに一般項は $\binom{2n}{r} \frac{2^{kr+k-1}}{r+1} (2b_{2n-r})$ とかかれるので、 $\frac{2^{kr+k-1}}{r+1} \equiv 0$

$\pmod{2^{k+1}}$ か又は $\frac{2^{kr-2}}{r+1}$ が奇数の分母をもつ分数としてあらわされること

をしめそう。これを証明するには

$$2^{kr-1} > r+1, (r > 1) \dots\dots\dots (3)$$

をしめせば十分である。それというのも $r=1$ に対応する項は $n > 1$ のとき消えるからである。ところで2項定理により

$$1 + (2r-1) < 2^{2k-1}$$

にして、 $r > 1$ のとき $2r > r+1$ なるを以て(3)が成立、したがって(2)が得られる。

定理 6 の証明. 59 は $4n+3$ なる形の最小不正則素数である。いま p_s をこの形の不正則素数とすると、 $59 \leq p \leq p_s$ を満足するこの形のすべての不正則素数を決定することができる。そこでこの形の不正則素数で $l > p_s$ なるものをいかにして決定するかをしめそう。そのために算術級数 (等差数列) における Dirichlet の定理を用いると次の式

$$q \equiv 1 \left(\text{mod } \prod_{i=1}^s p_i (p_i - 1) \right) \dots\dots\dots (4)$$

を満足する素数 q を見出すことができる。次に B_q の分母は因数 2 と 3 をもつので $q \equiv 1 \pmod{6}$

にして、 $2q+1=2(6t+1)+1=12t+3$ は合成数である。しかも 2 と 3 だけがその因数なので Staudt—Clausen の定理 ([16] p. 257) により分母はまさしく 6 である。また $q+hv > 0$ として重要な関係式 ([16] p. 266)

$$\frac{B_q}{q} \equiv \frac{(-1)^{hv} B_{q+hv}}{q+hv} \pmod{1} \dots\dots\dots (5)$$

$$\text{ただし } v = (1-1)/2$$

を用いると、(4)により $B_1 \equiv \frac{B_q}{q} \pmod{p}$

$$\text{ただし } p = p_1, p_2, \dots, p_s$$

となる。故に B_q の分子は p のおのおのと素である。いま $n=q, k=2$ とすれば(2)より

$$1^{2q} + 2^{2q} + 3^{2q} \equiv 4b_{2q} \pmod{8}$$

また

$$2^{2q} \equiv 0 \pmod{8}; 3^{2q} \equiv 1 \pmod{8}; b_{2q} = B_q$$

なるを以て

$$2B_q \equiv 1 \pmod{4}$$

となる。これより B_q の分子は $4l+3$ なる形をもつことが推論される。故にこの分子がこの形の素数でこれまでの p のいずれとも異なる l によって割

切れる。(5)において q は素なるを以てそれは $\frac{1-1}{2}$ の倍数ではない。なぜなら $\frac{1-1}{2}=q$ ならば $2q+1=1$ となり、これは $q \equiv 1 \pmod{6}$ から不可能である。それ故 $q+hv$ が $1, 2, \dots, \frac{1-3}{2}$ のなかにあるように h を正, 負, 又は 0 にとると, 1 は B_{q+hv} の約数となり, したがって定義により, 1 は p_s より大なる不正則素数となる。これで定理 6 が証明された。

(1964. 5. 10)

引用文献

- [1] 武隈良一, 古典確率論における諸問題 (Ⅱ) (商学討究, 第10巻第1号, 1959年7月, 73頁—106頁)
- [2] James Bernoulli, *Doctrine of Permutations and Combinations, and some other useful mathematical tracts* (1795), (小樽商大手塚文庫 P.1571)
- [3] D. E. Smith, *A source book in mathematics* (1929)
- [4] Jakob Bernoulli, (R. Haussner 訳) *Wahrscheinlichkeitsrechnung (I, II)* Ostwald's Klassiker der exakten Wissenschaften Nr. 107 (1899) 155—156.
- [5] 武隈良一著, 数学史, 第4刷 (昭和37年) 培風館。
- [6] Donald E. Knuth, Euler's Constant to 1271 Places. *Math. of Comp.* 16 (1962) 275—281.
- [7] W. Sweeney, On the Computation of Euler's Constant. *Math. of Comp.* 17 (1963) 170—178.
- [8] E. H. Pearson, On the Congruences $(p-1)! \equiv -1$ and $2^{p-1} \equiv 1 \pmod{p^2}$. *Math. of Comp.* 17 (1963) 194—195.
- [9] D. H. Lehmer and E. Lehmer, On the first case of Fermat's last theorem. *Bull. Amer. Math. Soc.* 47 (1941) 139—142.
- [10] H. S. Vandiver, Fermat's last theorem. *Amer. Math. Monthly.* 53 (1946) 555—578.
- [11] H. S. Vandiver, On Fermat's last theorem. *Trans. Amer. Math. Soc.* 31 (1929) 613—642.
- [12] D. H. Lehmer, E. Lehmer and H. S. Vandiver, An application of high-speed computing to Fermat's last theorem. *Proc. Nat. Acad. Sci. U. S. A.* 40 (1954) 25—33.

- [13] H. S. Vandiver, Examination of methods of attack on the second case of Fermat's last theorem. Proc. Nat. Acad. Sci. U. S. A. 40 (1954) 732—735.
- [14] J. L. Selfridge, C. A. Nicol and H. S. Vandiver, Proof of Fermat's last theorem for all prime exponents less than 4002. Proc. Nat. Acad. Sci. U. S. A. 41 (1955) 970—973.
- [15] H. S. Vandiver, Is there an infinity of regular primes? Scripta Math. 21 (1956) 306—309.
- [16] Uspensky and Heaslet, Elementary Number Theory (1939)