整数論と計算機

武 隈 良 一

表題の意味するものは，整数論の問題で計算機によって検証されるものについて述べようとするところにある。古来数多くの整数論の問題が論ぜられたが，実際の数についてこれらを検証することは容易ではなかった。それが電子計算機の出現により驚くべき効果をあげているのが現状である。その一端について述べようとするのが本稿の目的である。内容は次の通りである。

§1.　アルキメデスの家畜問題

問．太陽の神が白，黒，斑（ぶち），黄の4色の牡牛と牝牛からなる家畜の群をもっていた。

白牡牛は黄牡牛よりも黒牡牛の$\frac{1}{2}$と$\frac{1}{3}$だけ多く

黒牡牛は黄牡牛よりも斑牡牛の$\frac{1}{4}$と$\frac{1}{5}$だけ多く

斑牡牛は黄牡牛よりも白牡牛の$\frac{1}{6}$と$\frac{1}{7}$だけ多い。

白牝牛は黒牛全体の$\frac{1}{3}$と$\frac{1}{4}$との和に等しく

黒牝牛は斑牛全体の$\frac{1}{4}$と$\frac{1}{5}$との和に等しく

斑牝牛は黄牛全体の$\frac{1}{5}$と$\frac{1}{6}$との和に等しく

黄牝牛は白牛全体の$\frac{1}{6}$と$\frac{1}{7}$との和に等しい。

また，

白牡牛と黒牡牛との和は平方数に等しく

斑牡牛と黄牡牛との和は3角数に等しい。

このとき家畜の総頭数はいくらであるか。

解．白牡牛，黒牡牛，斑牡牛，黄牡牛の頭数をそれぞれ W, X, Y, Z, 白牝牛，黒牝牛，斑牝牛，黄牝牛の頭数をそれぞれ w, x, y, z とおくと題意により次の方程式が得られる。

$$W=\left(\frac{1}{2}+\frac{1}{3}\right)X+Z \cdots\cdots\cdots(1) \qquad X=\left(\frac{1}{4}+\frac{1}{5}\right)Y+Z \cdots\cdots\cdots(2)$$

$$Y=\left(\frac{1}{6}+\frac{1}{7}\right)W+Z \cdots\cdots\cdots(3)$$

$$w=\left(\frac{1}{3}+\frac{1}{4}\right)(X+x) \cdots\cdots(4) \qquad x=\left(\frac{1}{4}+\frac{1}{5}\right)(Y+y) \cdots\cdots(5)$$

$$y=\left(\frac{1}{5}+\frac{1}{6}\right)(Z+z) \cdots\cdots(6) \qquad z=\left(\frac{1}{6}+\frac{1}{7}\right)(W+w) \cdots\cdots(7)$$

$$W+X=U^2 \cdots\cdots\cdots\cdots\cdots\cdots(8) \qquad Y+Z=\frac{t(t+1)}{2} \cdots\cdots\cdots\cdots\cdots(9)$$

$$T=W+X+Y+Z+w+x+y+z \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(10)$$

ここにTは総頭数をあらわす。

(1), (2), (3) から

$$6W-5X=6Z,\ 20X-9Y=20Z,\ 42Y-13W=42Z$$

が得られるので，これを W, X, Y について解くと

$$W=\frac{742}{297}Z,\ X=\frac{178}{99}Z,\ Y=\frac{1580}{891}Z$$

となる。ここに W, X, Y, Z は正整数であり，Y の分母の $891=297\times3=99\times3\times3$ であり，Y の分子 1580 は 891 と互いに素であるから，Z は 891 の整数倍である。したがって Z=891K とあらわされる。これより

$$W=2226K,\ X=1602K,\ Y=1580K,\ Z=891K \cdots\cdots\cdots\cdots\cdots\cdots\cdots(\mathrm{I})$$

となる。これらの値を (4), (5), (6), (7) に代入すると

$$12w-7x=11214\mathrm{K},\ 20x-9y=14220\mathrm{K}$$

$$30y-11z=9801\mathrm{K},\ 42z-13w=28938\mathrm{K}$$

これを w, x, y, z について解くと

$$\left.\begin{array}{l}4657w=7206360\mathrm{K},\ 4657x=4893246\mathrm{K}\\ 4657y=3515820\mathrm{K},\ 4657z=5439213\mathrm{K}\end{array}\right\}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\text{(II)}$$

となる。ここに 4657 は素数である。

(II) の右辺における K の係数はいずれも 4657 で割り切れないから，$\mathrm{K}=4657k$ となる。この値を (I), (II) に代入すると

$$\left.\begin{array}{l}\mathrm{W}=10366482k=2\cdot3\cdot7\cdot53\cdot4657k\\ \mathrm{X}=\ 7460514k=2\cdot3^2\cdot89\cdot4657k\\ \mathrm{Y}=\ 7358060k=2^2\cdot5\cdot79\cdot4657k\\ \mathrm{Z}=\ 4149387k=3^4\cdot11\cdot4657k\end{array}\right\}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\text{(I')}$$

$$\left.\begin{array}{l}w=\ 7206360k=2^3\cdot3\cdot5\cdot7\cdot23\cdot373k\\ x=\ 4893246k=2\cdot3^2\cdot17\cdot15991k\\ y=\ 3515820k=2^2\cdot3\cdot5\cdot7\cdot11\cdot761k\\ z=\ 5439213k=3^2\cdot13\cdot46489k\end{array}\right\}\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\text{(II')}$$

が得られる。

ここに k は任意の正整数なので，(1) から (7) までを満足する解は無数にあるが，とくに $k=1$ のとき最小頭数の場合の答として次のものが得られる。

白牡牛	10366482	白牝牛	7206360
黒牡牛	7460154	黒牝牛	4893246
斑牡牛	7358060	斑牝牛	3515820
黄牡牛	4149387	黄牝牛	5439213

さて，$\mathrm{W}+\mathrm{X}=2^2\cdot3\cdot11\cdot29\cdot4657k$ は (8) により平方数であるから

$$k=3\cdot11\cdot29\cdot4657n^2=4456749n^2$$

となる。したがって (1) から (8) までを満足する値は次の通りになる。

$$\mathrm{W}-2\cdot3^2\cdot7\cdot11\cdot29\cdot53\cdot4657^2n^2=46200808287018n^2$$

$$X=2\cdot 3^3\cdot 11\cdot 29\cdot 89\cdot 4657^2n^2 \qquad =33249638308986n^2$$

$$Y=2^2\cdot 3\cdot 5\cdot 11\cdot 29\cdot 79\cdot 4657^2n^2 \qquad =32793026546940n^2$$

$$Z=3^5\cdot 11^2\cdot 29\cdot 4657^2n^2 \qquad =18492776362863n^2$$

$$w=2^3\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 23\cdot 29\cdot 373\cdot 4657n^2$$

$$=32116937723640n^2$$

$$x=2\cdot 3^3\cdot 11\cdot 17\cdot 29\cdot 15991\cdot 4657n^2=21807969217254n^2$$

$$y=2^2\cdot 3^2\cdot 5\cdot 7\cdot 11^2\cdot 29\cdot 761\cdot 4657n^2$$

$$=15669127269180n^2$$

$$z=3^3\cdot 11\cdot 13\cdot 29\cdot 46489\cdot 4657n^2 \qquad =24241207098537n^2$$

次に3角数とは 1, 3, 6, …, $\frac{t(t+1)}{2}$, … であるから, (9) より t のある値に対して

$$Y+Z=\frac{t^2+t}{2}$$

これより

$$(2t+1)^2=8(Y+Z)+1$$

となる。この Y, Z にいま求めた上の値を代入すると,

$$(2t+1)^2=410286423278424n^2+1$$

となるので, $2t+1=P$ とおくと

$$P^2-410286423278424n^2=1 \quad \cdots\cdots\cdots\cdots(11)$$

となり, このペルの方程式を解くと n が求まる。しかしこれを解くことは困難なので,

$$410286423278424=2^3\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353\cdot 4657^2$$

から $2\cdot 4657n=Q$ とおくと (11) は

$$\left.\begin{array}{l} P^2-2\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353Q^2=1 \\ \text{すなわち}\quad P^2-4729494Q^2=1 \end{array}\right\} \quad \cdots\cdots\cdots\cdots(12)$$

となるので, これを解くこととしょう。ただし, この場合には Q は $2\cdot 4657$ で割り切れぬばならぬ。

このペルの方程式 (12) を解いたのは A. Amthor (1880) [1, p. 344.] であ

る。彼はまず $\sqrt{D}=\sqrt{4729494}$ を連分数であらわすと，91 項の周期をもつことをしめし，(12) を満足する最小の解は次のものであることを見出した。

$$P=109931986732829734979866232821433543901088049 \text{ (45 桁)}$$

$$Q=50549485234315033074477819735540408986340 \text{ (41 桁)}$$

したがって

$$P_m+\sqrt{D}Q_m=(P+\sqrt{D}Q)^m$$

を満足する P_m と Q_m が (12) のすべての解であるが，そのうち Q_m が $2\cdot 4657$ で割り切れる最小の解は Q_m の $m=2329$ であることが見出された。この Q_{2329} を正確に求めることは不可能であったが，大体の値を求めこれより Amthor は

$$W=1598 \text{ (……以下 206541 桁の数……)}$$

であり，総頭数 T は

$$T=7766 \text{ (……以下 206541 桁の数……)}$$

であることを導いた [2, p. 325.]。

計算機による解. Amthor の結果は 1965 年に計算機によって実際に求められた [3]。

(10) により

$$T=C\left(\frac{Q_{2329}}{2\cdot 4657}\right)^2$$

となり，ここに C は次の数をあらわす。

$$C=2\cdot 3\cdot 11\cdot 29\cdot 41\cdot 107\cdot 4657\cdot 5743=224571490814418$$

この T を求めるのに用いられた計算機は，IBM 7040 と IBM 1620 (II) であり，次の 3 つの段階 (A), (B), (C) をへて最終的な数字が得られた。

(A) P_i, Q_i を求めるのに i の値として次のものを計算した。

1, 2, 4, 8, 9, 18, 36, 72, 144, 145, 290, 291, 582, 1164, 2328, 2329.

かくして Q_{2329} が求められた。このために行なわれる計算の式は次の通りである。

$$P_{2n}=2P_n^2-1,\ Q_{2n}=2P_nQ_n,\ P_{n+1}=PP_n+(DQ)Q_n,$$

$$Q_{n+1}=PQ_n+QP_n.$$

ここに Q_{2329} は 2・4657 で割り切れるが，以上の計算に 2 時間 25 分を要した。

(B) n を平方すること。これには 1 時間と 18 分を要した。

(C) (B) の 結果は 2 進法であらわされるので，これを 10 進法であらわす。この結果 n^2 が求められたが，計算に 3 時間と 48 分を要した。そして n^2 に 224571490814418 を掛けるのに 18 分を要した。

(T の最初の 30 桁と最後の 12 桁は A. H. Bell が 1889 年に求めたものと一致した。)

以上で所要の時間は合計 7 時間 49 分であり，求められた 206545 桁の数を全部しめすことは紙面が狭いので，最初の 50 桁と最後の 50 桁だけをしるしておこう。

77602714064868182695302328332138866642323224059233……………………
05994630144292500354883118973723406626719455081800.

史話. 劇作家，批評家として，近代ドイツ文学の礎石をきずいた有名なレッシング (G. E. Lessing 1729–1781.) がヴォルフェンビュッテルの図書館の司書をしていたころ，1773 年 にアルキメデスの手記を発見した。これは 22 行の対連（2 行の対句）からなる詩を含む手紙で，アレキサンドリアのエラトステネスにあてたものである。この詩のなかに家畜の問題が述べられている [4, s. 1.]。

§ 2. 等差数列をなす素数

問. n 個の素数で等差数列をなすものを求めよ。

計算機による解.

$n=3$ のとき直ちに見出されるものとして，(1, 2, 3) と (1, 3, 5) があるがこれらは除外しておく。

最初の素数が 3 のとき，(3, 5, 7) と得られるが，このとき 公差は 2 でありこれは 6 で割り切れない。

最初の素数が3でないものとして，(7, 13, 19) が得られるが，このとき公差6は $6=2\cdot3$ で割り切れる。

$n=4$ のとき，(1, 7, 13, 19) が得られるが，このとき公差6は $6=2\cdot3$ で割り切れる。また次のものが得られる。

$$7+12m,\ 17+12m,\ 1877+12m\ (0\leqq m\leqq3)$$

これらは公差が $6=2\cdot3$ で割り切れる。

$n=5$ のとき，最初の素数を5とすれば，(5, 11, 17, 23, 29) と得られるが，このとき公差6は $30=2\cdot3\cdot5$ で割り切れない。また (5, 17, 29, 41, 53) も得られるが，このとき公差12は $30=2\cdot3\cdot5$ で割り切れない。

最初の素数が5でないものは，容易に見つからなかったが，ついに以下のものを見出した。

$$33893+510m=33893+2\cdot3\cdot5\cdot17m\ (0\leqq m\leqq4)$$

これでみると，公差510は $30=2\cdot3\cdot5$ で割り切れている。(これらより小さい素数で5個ならんだものがあるかどうかは検証しておらない。)

これらより大きい素数なら若干見出される。すなわち

$$\left.\begin{array}{l}34019+2\cdot3\cdot5\cdot19m\\33331+2\cdot3\cdot5\cdot21m\\33191+2\cdot3\cdot5\cdot22m\\32183+2\cdot3\cdot5\cdot28m\\28439+2\cdot3\cdot5\cdot56m\end{array}\right\}(0\leqq m\leqq4)$$

であるが，公差はみな $30=2\cdot3\cdot5$ で割り切れる。

$n=6$ のとき次のものが得られる。$(0\leqq m\leqq5)$

$$7+30m=7+2\cdot3\cdot5m$$

$$107+30m=107+2\cdot3\cdot5m$$

$$11+60m=11+2\cdot3\cdot5\cdot2m$$

$$53+60m=53+2\cdot3\cdot5\cdot2m$$

$$13+90m=13+2\cdot3\cdot5\cdot3m$$

$$503+90m=503+2\cdot3\cdot5\cdot3m$$

$$239+120m=239+2\cdot3\cdot5\cdot2\cdot2m$$

$$281+120m=281+2\cdot3\cdot5\cdot2\cdot2m$$

$$73+150m=73+2\cdot3\cdot5\cdot5m$$

$$397+180m=397+2\cdot3\cdot5\cdot2\cdot3m$$

$$13+210m=13+2\cdot3\cdot5\cdot7m$$

最初のものの公差は $30=2\cdot3\cdot5$ で割り切れ，最後のものの公差は $210=2\cdot3\cdot5\cdot7$ で割り切れている。

$n=7$ のとき，最初の素数が7であれば，$7+150m(0\leqq m\leqq6)$ が得られる。このとき公差は $210=2\cdot3\cdot5\cdot7$ で割り切れない。

最初の素数が7でないならば次のものが得られる $(0\leqq m\leqq6)$。

$$47+210m=47+2\cdot3\cdot5\cdot7m$$

$$829+210m=829+2\cdot3\cdot5\cdot7m$$

$$193+420m=193+2\cdot3\cdot5\cdot7\cdot2m$$

$$2267+630m=2267+2\cdot3\cdot5\cdot7\cdot3m$$

$$1061+840m=1061+2\cdot3\cdot5\cdot7\cdot4m$$

$$1319+1680m=1319+2\cdot3\cdot5\cdot7\cdot8m$$

これらにおいては公差はみな $210=2\cdot3\cdot5\cdot7$ で割り切れる。

$n=8$ のとき，　$619+210m,\ (0\leqq m\leqq7)$

$n=9$ のとき，　$409+210m,\ (0\leqq m\leqq8)$

$n=10$ のとき，$199+210m,\ (0\leqq m\leqq9)$

と見出される。

$n=11$ のとき，$a+2310bm,\ (0\leqq m\leqq10)$

なる形の a, b を求めようとしているが，まだ見つかっておらない。ここに $2310=2\cdot3\cdot5\cdot7\cdot11$ である。

$n=12$ のとき，これは既に W. A. Golubieff によって次の形で見出されている[5, p. 232.]。

$$23143+30030m=23143+2\cdot3\cdot5\cdot7\cdot11\cdot13m\ (0\leqq m\leqq11)$$

$n=13$ のとき，これは既に V. Seredinsky によって次の形で見出されている [13, p. 121.]。

$$4943+30030\times2m\ (0\leqq m\leqq12)$$

$n=14$ 以上については，まだ見つかっておらない。さらに進んで100個つづいた素数の等差数列の存在も知られておらないが，もしあったとしても，その公差は30桁以上であることが証明される [13, p. 121.]。

史話. この問題に対してこれまでに知られていることを述べておこう [6, p. 425.]。

まず Waring, E. がその著書 Meditationes Algebraicae (1770) において次のように述べている。

3つの素数が等差数列をなすとすれば，その公差は $6=2\cdot3$ で割り切れる。ただし (1, 2, 3) と (1, 3, 5) は除外する。

5つの素数は，最初の素数が5でないとき，その公差は $30=2\cdot3\cdot5$ で割り切れる。

7つの素数は，最初の素数が7でないとき，その公差は $210=2\cdot3\cdot5\cdot7$ で割り切れる。

11個の素数は，最初の素数が11でないとき，その公差は $2310=2\cdot3\cdot5\cdot7\cdot11$ で割り切れる。以下同様。

これらを証明したのは次の定理である。

カントール (Cantor, M) **の定理** (1861). 2から p までのすべての素数の積を $P=2\cdot3\cdot\cdots\cdots\cdot p$ とするとき，公差が P で割り切れなければ，p 個の素数で等差数列になるものはない。ただし p 個の素数のなかに p はないものとする。

この定理により最初に述べた計算機による解の状態がうなずかれることと思う。ただし，素数の個数 n が素数でない場合に担当する定理は得られておらない。

また，計算機による解のなかで既に知られているものは次の通りである。

$$n=6,\quad \left.\begin{array}{r} 7+30m \\ 107+30m \end{array}\right\} \begin{array}{l} \text{Lemaire, G. (1909).} \\ (0 \leqq m \leqq 5) \end{array}$$

$$n=7,\quad \left.\begin{array}{r} 7+150m \\ 47+210m \end{array}\right\} \begin{array}{l} \text{Lemaire, G. (1909).} \\ (0 \leqq m \leqq 6) \end{array}$$

$$71+2310m \quad \text{Devignot, (1910).}$$

存在の証明．以上により等差数列をなす素数のあつまりが実在することは分ったが，存在することの証明はまだ一般になされていない。わずかに $n=3$ の場合になされているだけである。それが内山氏の次の定理（1961）[7] である。

定理．a を正整数，b を任意の整数とし，$N(x, a, b)$ を

$$p_1+p_3=ap_2+b$$

を満足する解の個数とする。ここに p_1, p_2, p_3 は $2 \leqq p_j \leqq x$ $(j=1, 2, 3)$ を満足する素数とする。このとき次式が成立する。

$$N(x, a, b)=C(a, b)T(x, a, b)+O(x^2(\log x)^{-A}) \qquad (x \to \infty,\ A>3)$$

ここに O-定数は a, b と A に従属しており，

$$C(a, b)=\prod_{p|a,\ p|b} \frac{p}{p-1} \prod_{\substack{p|a,\ p\nmid b \\ \text{or} \\ p\nmid a,\ p|b}} \frac{p(p-2)}{(p-1)^2} \prod_{p\nmid ab}\left(1+\frac{1}{(p-1)^3}\right)$$

$$T(x, a, b)=\sum(\log n_1 \log n_2 \log n_3)^{-1}$$

この和は $n_1+n_3=an_2+b$ のすべての整数解 n_1, n_2, n_3 の上を動く。$2 \leqq n_j \leqq x$ $(j=1, 2, 3)$。

系．$a=1$, $b=0$ とすれば $n=3$ の場合の証明になる。

なお，これより先き Chowla, S が 1944 年に等差数列をなす 3 つの素数の存在を証明している。

結論的にいえば，n 個の素数で等差数列をなすものは存在すると予想されるが，それを経験的に求めても $n=13$ ぐらいまでしか分っておらず，$n=3$ を除いて一般にその存在は証明されておらないのが現状である。

§ 3.　$\dfrac{p^p-1}{p-1}$について

問. pを素数とするとき，$\dfrac{p^p-1}{p-1}$は素数であるか。

問. $\dfrac{11^{11}-1}{10}$は素数であるか。

後者の問題は前者において$p=11$の特別の場合であるが，これらについて内山三郎氏（信州大理教授）から筆者宛への旧書簡（1961. 5. 19.）に次のようにある。

「……$\dfrac{11^{11}-1}{10}=28531167061$ が素数か否かという問題は以前伊藤昇氏（現名大教養教授）が北大在任当時教室の学生に出されたものです。この数は比較的大きいため Factor Table も使用できずに最近まで放置せられていたようなので，私が2～3の人に電子計算機を用いてみることを依頼した訳なのです。そして東大理学部の PC-I（一松信氏），有隣電機精機 K. K. の FACOM-222（岡本彬氏）によって独立に

$$\text{上記の数}=15797\times1806113$$

と分解されること，そして両因数は共に素数であること（このことは素数表からも分りますが）が立証（＝計算）されました。

上記の数は $(p^p-1)/(p-1)$,（p＝素数）の形の数の特別なもので最近 PC-I により $p=13$ のときも計算されています。もっともこの時は小さな素因数 53 がありますので『問題』は容易かも知れません。

$$(13^{13}-1)/12=53\times264031\times1803647$$

各因子は素数。

$(p^p-1)/(p-1)$ は或る種の有限群の order で，これが素数である場合の方がむしろ興味あるものだそうです（伊藤氏による）。整数論的な意味はよく分りませんが，多分この形の数の素因子の個数はあまり多くはないのではないかと思われますが実相は不明です。……猶 $(p^p-1)/(p-1)$ は既約多項式 $F_p(x)$（p 次の円分方程式，degree は $p-1$）の $x=p$ の値になっている訳です。……」

さてこの問題の由来について述べよう [8]。E. T. Bell は1934年に

$$e^{e^x-1}=\sum_{n=0}^{\infty}B(n)\frac{x^n}{n!}$$

を考えた。この母函数によって定義される B(n) は次のものの個数である。

(a) n の異なるものを n 個の似た箱のなかへ入れる仕方の個数である。ただし箱には何にも入らないものがあってもよい。

(b) 暗号解読のとき起ることであるが，n 個の文字を n 個以下に分割して単語（無意味のこともある）の列にする仕方は何通りあるか。

(c) n 個の単語がならんでいる詩において，これに韻をふませるために n 個以下に分割する方法は何通りあるか。

(d) n 個の素数が与えられたとき，これらを適当にまとめて，合成数と素数の積にする方法は何通りあるか。

これらはみな同じことの異なる表現である。(d) について例をあげると，3 個の素数が与えられたとき

$$(p_1p_2p_3)=(p_1p_2)p_3=(p_1p_3)p_2=(p_2p_3)p_1=(p_1)(p_2)(p_3)$$

となるので，$B(3)=5$ となる。

この $B(n)$ については，いろいろな式と性質が与えられている。

$$B(n)=\frac{1}{e}\sum_{t=0}^{\infty}\frac{t^n}{t!}$$

$$B(n)=\sum_{r=1}^{n}\sum_{k=0}^{r}\frac{(-1)^k}{r!}\binom{r}{k}(r-k)^n=\sum_{r=1}^{n}S(n,r)$$

ここに $S(n,r)$ は第 2 種スターリング数である。また

$$B(n+1)=(B+1)^n$$

が成立する。ここに右辺の B^m は展開の後に $B(m)$ によっておきかえられる。

定差公式　$B(n)=\triangle^n B(1)$

が計算機のために最も簡単な形で見出され，$B(n)$ の計算に際して用いられた。

$B(n)$ の数論的性質の研究に際しては，素数 p に対して

$$B(n+p)\equiv B(n)+B(n+1)\quad(\mathrm{mod.}\ p)$$

が成立することが基本事項である。これに加うるに

$$B(n+p^m)\equiv B(n+1)+mB(n) \pmod{p}$$

の成立を注意しておこう。

さて $B(n)$ の実際の値を少し書いてみよう。

$B(0)=1,\quad B(5)=52,\quad B(10)=115975,$

$B(1)=1,\quad B(6)=203,\quad B(11)=678570,$

$B(2)=2,\quad B(7)=877,\quad B(12)=4213597,$

$B(3)=5,\quad B(8)=4140,\quad B(13)=27644437,$

$B(4)=15,\quad B(9)=21147,\quad B(14)=190899322,$

これらの $B(n)$ の mod. p に関する剰余をならべると，

$p=2$ のとき，1, 1, 0, 1, 1, 0, ……

となり周期は 3 である。この 3 は $\dfrac{2^2-1}{2-1}$ に等しい。

$p=3$ のとき，1, 1, 2, 2, 0, 1, 2, 1, 0, 0, 1, 0, 1, ……

となり周期は 13 である。この 13 は $\dfrac{3^3-1}{3-1}$ に等しい。

一般に次の定理が成立する。

定理. $B\left(n+\dfrac{p^p-1}{p-1}\right)\equiv B(n) \pmod{p}$

すなわち $B(n)$ は $N_p=\dfrac{p^p-1}{p-1}$ という合同周期をもっている。

これを証明したのは G. T. Williams [9] であり，これを実際に $p=2, 3, 5$ の場合に確めた。

しかし N_p が素数でないときは N_p が最小の周期ではなく N_p の約数が最小周期になるかも知れない。その意味で N_p が素数であるか否かが問題となるのである。

$p>5$ に対しては Jack Levine と R. E. Dalton が次の定理を得ている [8]。

定理. $B(n)$ の数列の mod. p に関する最小周期は，$p=7, 11, 13, 17$ のとき N_p である。また $p<50$ の残りの素数，すなわち 19, 23, 29, 31, 37, 41, 43 に対しては，それらの素数 N_p の知られている素因数（これは 40 桁以下

のものである）は周期にならない。

この定理によると $17<p<50$ の素数に対しては N_p が最小周期であるかどうかは不明である。それというのもまず N_p が素数であるか否かを調べることは大変な計算を必要とし，また素因数が見つかったとしても $B(n)$ の値を n の相当大きなところまで求めておくことが必要であるからである。

実際[8]においては，$B(n)$ が $n=74$ まで求められ，$B(n)$ (mod. p) の値が $0 \leqq n \leqq p$, $p \leqq 50$ まで求められ，N_p の値が $p<50$ まで求められている。このうち最後のものを少し紹介しておこう。

$N_5=781=11\times 71$

$N_7=1,37257=29\times 4733$

$N_{11}=2,85311,67061=15797\times 1806113$

$N_{13}=2523,95922,16021=53\times 264031\times 1803647$

$N_{17}=51702,51636,78960,47761$

$\quad=10949\times 1749233\times 2699538733$

$N_{19}=1099,12203,09223,96438,40221$（素因数は知られてない。）

$N_{23}=94911,21818,11268,72883,43196,77753$

$\quad=461\times 1289\times 1597216194112486480522357$

$N_{29}=9,\cdots\cdots,02981$（41 桁の数）

$\quad=59\times 16763\times 84449\times 2428577\times 14111459\times$（17 桁の数）

$N_{31}=$（45 桁の数にして素因数は知られてない。）

$N_{37}=57$ 桁の数

$\quad=149\times 1999\times 7993\times$（40 桁以上の数）

$N_{41}=65$ 桁の数

$\quad=83\times$（40 桁以上の数）

$N_{43}=69$ 桁の数

$\quad=173\times 6709\times$（40 桁以上の数）

$N_{47}=77$ 桁の数

$\quad=1693\times$（40 桁以上の数）

§ 4.　一般化されたフェルマの問題

フェルマの問題とは周知のように

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

を満足する正整数解（今後単に解とよぶ）が存在しないことを証明せよという問題である。これを拡張すると次のようになる。

問．$x_1^n+x_2^n+\cdots\cdots+x_m^n=x_{m+1}^n$ において $n\leqq m$ ならば解があり，$n>m$ ならば解はない。ここに n, m は自然数である。

これを**一般化されたフェルマの問題**というが，これについて述べよう [12, p. 332.]。

その前に (1) について以前に [10, p. 15.] 述べたことがあるが，その後の発展について補っておこう。

それはフェルマの問題の第 1 の場合に，「素数 p が次の合同式

$$\frac{2^{p-1}-1}{p}\equiv 0\ (\mathrm{mod.}\ p)\quad\cdots\cdots(2)$$

を満足しないならば，$x^p+y^p=z^p$（p は奇素数）は解をもたない。」

と証明されているが (2) を満足する素数は 200,183 までの間に $p=1093$ と 3511 だけであることが知られている。

いま 2 の代りに a をとって (2) と同様な合同式を考えたとき，それを満足する奇素数 p があるか否かについては次の結果が Hans Riesel (1964) によって得られている [11]。

（第 1 表）

奇素数 $p<500,000$ とす。

a	p	a	p
2	1093, 3511	7	5, 491531
3	11	8	3, 1093, 3511
4	1093, 3511	9	11
5	20771, 40487	10	3, 487
6	66161		

（第2表）

奇素数 $p<10,000$ とす。

a	p	a	p
11	71	39	8039
12	2693	40	11, 17, 307
13	863	41	29
14	29, 353	42	23
16	1093, 3511	43	5, 103
17	3	53	3, 47, 59, 97
18	5, 7, 37, 331	59	2777
19	3, 7, 13, 43, 137	67	7, 47
20	281	71	3, 47, 331
22	13, 673	73	3
23	13	79	7, 263, 3037
24	5	83	4871
26	3, 5, 71	89	3, 13
27	11	97	7
28	3, 19, 23	101	5
30	7	107	3, 5, 97
31	7, 79, 6451	109	3
32	5, 1093, 3511	127	3, 19. 907
33	233	131	17
35	3, 1613, 3571	137	29, 59, 6733
37	3	149	5
38	17, 127	150	13

以上の表は Riesel の表の抜きがきであるが，Riesel の原表において a が素数である次の場合

$$a=47, 61, 103, 113, 139$$

が計算されておらないのが惜しい。

さて一般化されたフェルマの問題はもちろん証明されてはいないが，n および m の小さな値について調べてみよう。

(I) $n=2$, $m=2$ のとき，$x^2+y^2=z^2$ となるが，この方程式の解はピタゴラスの数として周知の通りである［1, p. 165.］。

(II)　$m=2,\ n\geqq 3$ のとき，これはフェルマの問題である（未解決）。

(III)　$m=3,\ n=2$ のとき，$x^2+y^2+z^2=u^2$. これは [3, p. 69.] に解かれてあるが，次の一般の場合に帰着する。

(IV)　m は任意，$n=2$ のとき，

$$x_1^2+x_2^2+\cdots\cdots+x_n^2=y^2$$

これは会田安明（1747–1817）によって次の解が得られている [1, p. 318.]。それは彼の著書「算法整数術」（1807）にあり，結果は次の通りである [14, p. 515.]。

$$x_1=-a_1^2+a_2^2+\cdots\cdots+a_m^2.$$

$$x_2=2a_1a_2,\ x_3=2a_1a_3,\ \cdots\cdots,\ x_m=2a_1a_m$$

$$y=a_1^2+a_2^2+\cdots\cdots+a_m^2.$$

ここに a_i は任意の整数を表わす。

(V)　$m=3,\ n=3$ のとき，$x^3+y^3+z^3=u^3$.

これについてはいろいろの解が得られているが [1, p. 560.], [14, p. 516.], ここでは Ramanujan (1887–1920) のものを 1 つ掲げておこう [12, p. 201.]。

$$x=3a^2+5ab-5b^2,\quad y=4a^2-4ab+6b^2$$

$$z=5a^2-5ab-3b^2,\quad u=6a^2-4ab+4b^2.$$

電子計算機による解は次の通りである。ただし $x\leqq y\leqq z$ とする。

x	y	z	u	x	y	z	u	x	y	z	u
1	6	8	9	6	8	10	12	10	なし	なし	なし
2	12	16	18	6	20	36	38	11	15	27	29
2	17	40	41	6	32	33	41	12	16	20	24
3	4	5	6	6	36	48	54	12	19	53	54
3	10	18	19	7	14	17	20	13	なし	なし	なし
3	18	24	27	7	42	56	63	14	28	34	40
3	36	37	46	7	54	57	70	15	20	25	30
4	17	22	25	8	34	44	50	15	42	49	58
4	24	32	36	8	48	64	72	⋮	⋮	⋮	⋮
5	30	40	45	9	12	15	18	54	72	90	108
				9	30	54	57				

これはほんの一部にすぎないが，$0<x, y, z<100$ の完全な表を作りつつある。これまでに知られたものでは次のものがある。

$$149^3+256^3+363^3=408^3$$

(VI)　$m\geqq 4$, $n=3$ のとき，［1, p. 563.］においていろいろと論ぜられているが，ここでは具体的な例をあげておこう。

$m=5$, の前に
$$m=4,\quad 13^3=1^3+5^3+7^3+12^3$$
$$20^3=11^3+12^3+13^3+14^3$$
$$217^3=1^3+2^3+52^3+216^3$$
$$m=5,\quad 9^3=1^3+3^3+4^3+5^3+8^3$$
$$16^3=4^3+6^3+7^3+9^3+14^3$$
$$25^3=1^3+2^3+4^3+12^3+24^3$$
$$440^3=230^3+243^3+256^3+269^3+282^3$$
$$m=6,\quad 13^3=1^3+5^3+6^3+7^3+8^3+10^3$$
$$1155^3=435^3+506^3+577^3+648^3+719^3+790^3$$
$$m=7,\quad 14^3=2^3+3^3+5^3+7^3+8^3+9^3+10^3$$

これらを求めるためにいろいろと苦心がなされたことと思われるが，計算機によって幾多の例が得られるはずである。

しかし問題点は不定方程式の解の公式を求め得たとしても，それによってすべての解が得られるかどうかを常に検証しておく必要がある。また解のすべてが素数であるもの，解が等差数列をなすもの，解はすべて異なる自然数からなるものを求めるというように，他の条件の加わった解を求めることも興味深い問題である。(このことは一般の不定方程式についてもいえる。)

(VII)　$m=3$, $n\geqq 4$ のとき，$x^n+y^n+z^n=u^n$ となる。$n=4$ のとき Euler の研究があるが不完全である［1, p. 648.］。

これを $n\geqq 4$ のすべての n について不能であることを証明したのは O. Schier (1881) である［1, p. 682.］。

(VIII)　$m\geqq 4$, $n=4$ のとき，［1, p. 649.］,［13, p. 57.］,［13, p. 394.］にお

いていろいろと論ぜられているが，ここでは具体的な例をあげておこう。

$m=4$, $353^4=30^4+120^4+272^4+315^4$

$651^4=240^3+340^4+430^4+599^4$

$m=5$, $5^4=2^4+2^4+3^4+4^4+4^4$

$15^4=4^4+6^4+8^4+9^4+14^4$

$65^4=1^4+8^4+12^4+32^4+64^4$

$85^4=2^4+13^4+32^4+34^4+84^4$

$$(4x^4+y^4)^4=(4x^4-y^4)^4+(4x^3y)^4+(4x^3y)^4+(2xy^3)^4+(2xy^3)^4$$

$m=6$, $13^4=2^4+6^4+8^4+2^4+7^4+12^4$

$91^4=14^4+24^4+34^4+49^4+58^4+84^4$

$325^4=7^4+8^4+10^4+28^4+108^4+324^4$

$m=7$, $325^4=3^4+8^4+10^4+20^4+26^4+108^4+324^4$

$m=9$, $75^4=8^4+12^4+16^4+18^4+20^4+28^4+40^4+45^4+70^4$

(IX)　$m=4$, $n\geqq5$ のとき，$x^n+y^n+z^n+u^n=v^n$ となる。この式の不能はまだ証明されていない。

(X)　$m\geqq5$, $n=5$ のとき，[1, p. 682.], [13, p. 395.] においていろいろと論ぜられている。

$m=5$,　具体的例のないのが遺憾である（まさか不能ではあるまい。）

$m=6$, $12^5=4^5+5^5+6^5+7^5+9^5+11^5$

$30^5=5^5+10^5+11^5+16^5+19^5+29^5$

$m=7$, $92^5=2^5+9^5+11^5+22^5+51^5+58^5+89^5$

$m=12$, $32^5=3^5+6^5+7^5+8^5+10^5+11^5+13^5+14^5+15^5+16^5+18^5+31^5$

(XI)　$n=6$.

$m=5$,　$x^n+y^n+z^n+u^n+v^n=w^n$ の不能の証明はまだなされていない（$n\geqq6$）。

$m=6, 7, \ldots 15$ のときの具体的例はまだ得られてない。

$$m=16,\quad 28^6=1^6+2^6+4^6+5^6+6^6+7^6+9^6+12^6+13^6+15^6+16^6+18^6+20^6+21^6+22^6+23^6$$

以上で本節を打切るが，具体的例を掲げたのは計算機によりこれ以外の多くの例を求めてもらいたいからである。しかし n が 4 またはそれ以上になると容易な業ではない。

§ 5.　$x^n+y^n=u^n+v^n$

良く知られているように，$x^n+y^n=u^n+v^n$ をみたす正整数解（今後たんに解とよぶ）には次のものがある。

$n=2$ のとき，　$1^2+8^2=4^2+7^2$

$n=3$ のとき，　$1^3+12^3=9^3+10^3$

$n=4$ のとき，$133^4+134^4=59^4+158^4$

このうち最後のものは Euler によって 1772 年に求められている [1, p. 644.]。

これより進んで Sierpiñski は次の問題を提出した [15, p. 116.]。

問 1. $n\geqq 5$ とするとき，$x^n+y^n=u^n+v^n$ をみたす解は存在するであろうか。

問 2. $x^4+y^4=u^4+v^4=\alpha^4+\beta^4$ をみたす解は存在するであろうか。すなわちある整数が 3 通りの方法で 4 乗の和にあらわされであろうか。

この 2 問は今日未解決である。ここでは $n=3$, $n=4$ の場合について，これまでに知られていることを少しく述べておこう。

$n=3$ の場合

$$x^3+y^3=u^3+v^3$$

これについては和算家馬場正統編集の書物（1830，文政十三年）に次の解がある [14, p. 520.]。

$$x=c(c^6-4),\qquad y=6c^3+c^6-4$$

$$u=-6c^3+c^6-4,\quad v=12c+c(c^6-4)$$

その他の解もあるが [1, p. 555], それらに深入りすることなく, 実際に知られている解について述べよう。

$$1^3+12^3=9^3+10^3 \qquad 9^3+34^3=16^3+33^3$$

$$2^3+16^3=9^3+15^3 \qquad 10^3+27^3=19^3+24^3$$

$$2^3+34^3=15^3+33^3 \qquad 1043^3+2987^3=1140^3+2976^3$$

$$3^3+36^3=27^3+30^3$$

この外にもちろん存在するであろうが, 計算機で系統的にもとめたものがほしい。

$n=4$ の場合

$$N=x^4+y^4=u^4+v^4$$

これについての解は Euler (1772) によって次のように求められた。

$$\begin{cases} x=a^7+a^5b^2-2a^3b^4+3a^2b^5+ab^6 \\ y=a^6b-3a^5b^2-2a^4b^3+a^2b^5+b^7 \\ u=a^7+a^5b^2-2a^3b^4-3a^2b^5+ab^6 \\ v=a^6b+3a^5b^2-2a^4b^3+a^2b^5+b^7 \end{cases}$$

しかし, これはある意味で不完全な解である [12, p. 201.]。

計算機による解が最近得られているので, それをしるそう [16, p. 450.]。

i	N_i	x	y	u	v
1	635, 318, 657	158	59	134	133
2	3, 262, 811, 042	239	7	227	157
3	8. 657, 437, 697	292	193	257	256
4	68, 899, 596, 497	502	271	497	298
5	86, 409, 838, 577	542	103	514	359
6	160, 961, 094, 577	631	222	558	503
7	2, 094, 447, 251, 857	1203	76	1176	653
8	4, 231, 525. 221, 377	1381	878	1342	997
9	26, 033, 514, 998. 417	2189	1324	1997	1784
10	37, 860, 330, 087, 137	2461	1042	2141	2026
11	61, 206, 381, 799, 697	2797	248	2524	2131
12	76, 773, 963, 505, 537	2949	1034	2854	1797

13	109,737,827,061,041	3190	1577	2986	2345
14	155,974,778,565,937	3494	1623	3351	2338
15	156,700,232,476,402	3537	661	3147	2767
16	621,194,785,437,217	4883	2694	4397	3966
17	652,057,426,144,337	5053	604	5048	1283
18	680,914,892,583,617	4849	3364	4303	4288
19	1,438,141,494,155,441	6140	2027	5461	4840
20	1,919,423,464,573,697	6619	274	5942	5093
21	2,089,568,089,060,657	6761	498	6057	5222
22	2,105,144,161,376,801	6730	2707	6701	3070
23	3,263,864,585,622,562	7557	1259	7269	4661
24	4,063,780,581,008,977	7604	5181	7037	6336
25	6,315,669,699,408,737	8912	1657	7559	7432
26	6,884,827,518,602,786	9109	635	9065	3391
27	7,191,538,859,126,257	9018	4903	8409	6842
28	7,331,928,977,565,937	9253	1104	8972	5403
29	7,362,748,995,747,617	9043	5098	8531	6742
30	7,446,891,977,980,337	9289	1142	9097	4946
31	7,532,132,844,821,777	9316	173	9197	4408

このうち $i=1$ は Euler (1772), $i=2$ は A. S. Werebrusow (1912), $i=3$ も Werebrusow (1914), $i=7$ は A. Desboves (1879) によって既に求められている。

最後に問 2 は解決されていないが,

$$x^4+y^4+z^4=u^4+v^4+w^4=\alpha^4+\beta^4+\gamma^4$$

をみたすものとして次のものがある [16, p. 451.]。

$$29^4+17^4+12^4=28^4+21^4+7^4=27^4+23^4+4^4$$

$$159^4+58^4+1^4=134^4+133^4+1^4=154^4+83^4+71^4$$

§ 6.　$a^3+b^3+c^3=a+b+c$

M. Wunderlich [17, p. 482-486] によってこの式を満足する解について述べよう。ことの起りは, J. C. P. Miller と M. F. C. Woollet (1955) によって広大な計算が行なわれたにもかかわらず

$$a^3+b^3+c^3=3 \qquad\qquad (1)$$

をみたす解は次のただ2通りであった。

$$(a=b=c=1),\ (a=b=4,\ c=-5)$$

ついで，この解は Aubrey Kempner によって次の式

$$a^3+b^3+c^3=a+b+c \qquad\qquad (2)$$

をみたすことが注意された。

したがって(2)はこの2つの解以外のものをもつかどうかが興味をもたれ，そのさい(1)の解が非常に少ないので(2)の解は存在しても，有限個に過ぎないと予想された。

いま c の符号を変え(2)を6で割ると

$$\frac{a^3-a}{6}+\frac{b^3-b}{6}=\frac{c^3-c}{6}$$

すなわち

$$\frac{(a-1)a(a+1)}{6}+\frac{(b-1)b(b+1)}{6}=\frac{(c-1)c(c+1)}{6}$$

となる。ここにあらわれる形の数

$$\frac{(a-1)a(a+1)}{6},\quad a\geqq 2 \qquad\qquad (3)$$

はギリシアの時代から研究されている「ピラミッド数」である[1, Chap. 1.]。また(3)よりピラミッド数は次のように定義される。

$$P_n=\binom{n+2}{3},\quad n\geqq 1$$

2項定理によればこれはパスカルの三角形の第4行にあらわれる数である。すなわち

1, 4, 10, 20, 35, 56, 84, ……

したがって(2)に対する予想は次のように述べられる。すなわち

$$P_x+P_y=P_z \qquad\qquad (4)$$

をみたす解は有限個にすぎないと。

この予想と(4)をみたす解の表について述べるのが本節の目的である。

結果は予想を裏切って S. Chowla が(4)，したがって(2)が無限個の解をもつことを証明した。そして特に

$2P_x = P_y$

をみたす解は $x=3,\ y=4$ のみであることを証明した。

また(4)をみたす最初の88個の解が下表のように計算機によって求められた。それは Colorado の C. D. C. 1604 計算機により6時間を要した。

ここに注目すべきは S. Chowla は無限個の解の存在を証明したにもかかわらず，計算機で見出された解の大多数を正しいものと検証しておらないことである。それは彼が(2)を Pell の方程式にみちびくことによって無限個の解の存在を証明したので，特別の形の無限個の解にふれたことになり，それらは次の表にあらわれるものとは偶然にも1つも一致しなかった。以下に88個の解の一部をしめそう。

x	y	z	x	y	z
3	3	4	……	……	……
8	14	15	4115	8034	8379
20	54	55	4015	8910	9174
30	55	58	7104	7847	9442
39	70	74	7062	8094	9592
61	102	109	2951	10184	10266
84	90	110	1328	10568	10575
34	118	119	7842	10168	11532
48	138	140	7294	10618	11660
119	154	175	8274	10149	11725
……	……	……	9050	11100	12824

この表にあらわれる解にふれたものは Sierpiñski (1961) であるが，彼とても解の無限個の存在を証明したのち，$x=8,\ y=14,\ z=15$ と $x=2912,\ y=4838,\ z=5167$ の2つの解だけを導きだした。

ここで2つの未解決の問題が提出される。1つは(2)のすべての解を与えるパラメトリック表示を見出すこと，他は素数定理と類似の漸近密度函数を見出すことである。

後者をより明確に述べると次のようになる。

n に対して，$P_a + P_b = P_n$

をみたす正整数 a, b が存在するような n で，$n \leqq x$ なるものの個数を $\phi(x)$ であらわす。このとき $\phi(x) \sim g(x)$ になるような連続函数が存在するであろうか。すなわち

$$\lim_{x\to\infty}\frac{\phi(x)}{g(x)}=1$$

を満足するものを求めている。

さてピラミッド数はさらに拡張され，それは第 r 番目次数 n の図形数 (the r th figurate number of order n) とよばれる次のものとなる。

$$f_{n.r}=\binom{r+n-1}{n} \cdots\cdots (5)$$

これによるとピラミッド数 P_x は $f_{3,x}$ である。そこで問題はさらに拡張され

$$f_{n,x}+f_{n,y}=f_{n,z}$$

の解を求める方向に進められるが，それに深入りすることは次の機会にゆずろう。　(1966. 9. 22.)

引 用 文 献

[1] Dickson, L. E. History of the Theory of Numbers, vol. 2, Chelsea, New York, (1952).

[2] Heath, T. L. The works of Archimedes with the method of Archimedes. (1897), (Dover 版).

[3] Williams, H. C., German. R. A. and C. R. Zarnke, Solution of the Cattle Problem of Archimedes. Math. of Comp. vol. 19. No. 92 (1965). pp. 671–674.

[4] Dörrie, E. Triumph der Mathematik. (1933).

[4a] Antin, D. tr. 100 Great Problems of Elementary Mathematics. (1940). (Dover 版).

[4b] 高津巌訳，数学の勝利。(1942)。

[5] Erdös, P. Some unsolved problems. Pub. Math. Inst. Hungarian Acad. Sci. vol. 6. (1961).

[6] Dickson, L. E. History of the Theory of Numbers, vol. 1. Chelsea, New York, (1952).

[7] Uchiyama, S. Three Primes in Arithmetical Progression. Proc. Japan

Acad. vol. 37. (1961) pp. 329–330.

[8] Jack Levine and R. E. Dalton, Minimum Periods, Modulo p, of First-Order Bell Exponential Integers. Math. of Comp. 16 (1962) pp. 416–423.

[9] G. T. Williams, Numbers generated by the function $e^{e^x}-1$. Amer. Math. Monthly. 52 (1945) pp. 323–327.

[10] 武隈良一，ベルヌーイ数の周辺。人文研究。第 28 輯 (1964) pp. 1–22.

[11] H. Riesel, Note on the Congruence $a^{p-1} \equiv 1$ (mod. p^2). Math. of Comp. vol. 18 (1964) pp. 149–150.

[12] Hardy, G. H. and E. M. Wright, An introduction to the theory of numbers. fourth ed. (1960).

[13] Sierpiñski, Elementary theory of numbers. (1964).

[14] 加藤平左衛門，和算の研究，整数論，(1964).

[15] W. Sierpiñski, A selection of problems in the theory of numbers. (1964).

[16] L. J. Lander and T. R. Parkin, Equal sums of biquadrates. Math. of Comp. vol. 20. No. 95. (1966).

[17] M. Wunderlich, Certain properties of pylamidal and figurate numbers. Math. of Comp. vol. 18. No. 80. (1962).