計算、証明、有限、無限

淵野 昌 (Sakaé Fuchino)

23年10月12日 (20時06分 (日本時間)) 版

以下の文章は、**現代思想 二〇二三年7月号「特集*〈計算〉の世界」**に寄稿した論説の拡張版である。雑誌掲載版では紙数の制限などのために削除した部分も復活させている。また、投稿後／校正後の加筆訂正も含まれる。**拡張版で加えられたテキストの主なものは、dark green (この文の foreground の色) で色付けしてある。**

このテキストの最新版は、https://fuchino.ddo.jp/misc/computation-2023-x.pdf として download することができる。

目次

1 計算と論理

「計算」と言ったときに多くの人が連想するのは、数の計算であろう。しかもこの場合の数は、自然数であることが多いのではないだろうか。たとえば、掛け

---

0) 本稿の内容は、(広い意味では) 筆者が研究代表者となっている科研費研究プロジェクト: 集合論的多世界宇宙の視点での連続体問題の解決、基盤研究 (C) (2020 – 2023) での研究とも、関連を持つものである。
後にも、本稿の何か所かで名前を挙げることになる酒井拓史氏からは、本稿の草稿に対する、複数の有益なコメントを頂いた。筆者はこのことに感謝する。

算 9999999 × 999999 など。この掛け算は、普通の「電卓」で計算すると桁あふれして、うまく計算できなかったり、指数表示による近似値が表示されるかもしれない。PC上の計算プログラムを使うと、9999989000001 という厳密な答を返してくれるかもしれない。

この計算を暗算でしてください、と言われたときにはどうしたらよいだろうか？ちょっと考えると、中学で習った式 $(a-b)(c-d) = ac - ad - bc + ad$ が応用できそうなことに気がつく。これを使うと、$9999999 = 100000000 - 1 = 10^8 - 1$, $999999 = 1000000 - 1 = 10^6 - 1$ に注意して、

$$9999999{\times}999999 = (10^8{\times}10^6) - (10^8{\times}1) - (1{\times}10^6) + (1{\times}1) \qquad (1)$$

と計算できることが分かる。この計算なら、普通の人が暗算で計算のできる、ぎりぎりの線に入っていると言えるだろう。しかも、この式 (1) を見ると、なぜ、計算機の教えてくれた答 9999989000001 で、最初に 9 が続いていて、10^8 の桁だけ 8 になっていて、その後 10^6 の桁未満で 0 が続いて、最後に一の桁が 1 になっているのかも、理解できる。

小学校で習う数の計算は、機械的な操作にすぎず、習ったことをそのまま実行する限り、どんな知性 (intelligence) も必要にならない。人間がそのような計算を苦痛に思うのは、規則に従って延々と機械的な操作を間違うことなくしなくてはいけなくなるからである。電卓や、PC などでの（普通の）計算 app の例では、速度や量に違いがあるとは言っても、基本的には、小学校で習った数の計算と同じことを機械的にやっているだけで、違いは、「パワーショベルが、どのオリンピック重量挙げ選手が持ちあげられるものより重いものを、持ち上げられる」、というのと同じような種類のものであろう。

ここでの暗算の例では、そこで挙げた代数の式（学校数学ないし受験数学では「公式」と言うのだろう）を思いつく、という理智の働きが必要になっているので、機械的な計算とは少し違うような気もする。そうは言っても、ここで挙げた数の

計算の例では、力づくの機械的な計算で結果を出すこともできたわけだが、すぐに見ることになるように、ここでのような「知性の働き」で計算を実行することはできるが、それなしの、闇雲な「計算」は、スーパーコンピュータをもってしても不可能だ、というような例もある。

「計算」を、もう少し一般化して、狭義の計算を特別な場合として含む、(数学の命題の)証明を考えてみると、そこでは、機械的な「計算手続き」を適用することで問題が解決できない場合の方が多く、そのような場合には、人間の「知性」を本質的に使わないと結果に至ることができない。しかも、この場合、ある命題を証明しようとしたとき、ある一定の時間をかけると結果が出る、という保証があるわけでもないことは、山のように残っている数学の未解決問題(ただ未解決というだけでなく、その解決が重要な意義を持つことになるはずの未解決の問題)を思い起こしてみると理解できるだろう。[1)]

一方、数学の証明でも、証明が一旦確立してしまったときには、それが正しいことをチェックする(つまり、狭義の「計算」での検算に相当する作業をする)ことは、機械的な「計算手続き」で実行できる。人間の数学者が使っている言葉が、かなり自然言語よりの、人間の「数学的直観」に訴えるものになっているため、現時点では、これを機械にかけてチェックできるような言葉に翻訳するのはそれほど容易でないが、この翻訳をアシストする未来のAIも実現寸前までのところに来ているかもしれない。

中学校以降の「数学」では、証明のことを計算と言っていることも少なくない。

---

1) こうは書いてみたが、実際には、数学の重要な問題は、既に過去にあらかた解けてしまっているのだろう、と考えている人も少なくないのかもしれない。そういう感想を持つ人が少なくないのは、現代の数学の内容やその意義が、予備知識のない人に対して、そう簡単には説明できない、という状況に起因するのだろう。このような誤解を解こうとして、一般の人に理解しやすそうな未解決問題を例として挙げて説明すると、説明された側は、数学の未解決問題とは、そのような例として説明された問題のような種類のものなのだろう、と誤解してしまう危険も小さくない。状況を理解してもらうのは至難の技であるように思える。

これは、「証明」と言うと拒否反応を示す人が一定数いる（というより、実際には大多数である）ことへの教育的配慮だろうか。式（方程式）を解く、というタイプの問題解決は、この、計算と呼ばれるが実は証明である、のパターンの一つだし（数理科学／技術での古典的な問題解決の多くが、この「方程式を解く」という作業に帰着されることは、これを認識していない人のために注意しておいてよいだろう）、微分や積分の「計算」もそのようなものであることが多いだろう。例えば、$\int_{-\infty}^{\infty} e^{-x^2}dx$ （ガウス積分[25]）の計算を考えてみよ。

　数学の証明は、人間の知性が必要になる、と言ったが、この「知性」と、知っている手法をすべてしらみつぶしに適用できるかどうか調べてみる、というアルゴリズミックな対処法の間に、効率の差以上の本質的な差があるかどうかは、不明にも思える。しかも後者なら、コンピュータに実装することもできるだろうし、実際、現在の数式処理のプログラムなら、先の例で触れたガウス積分やその変形なら、難なく「計算」できてしまうはずである。そのような意味で、「証明」も一般化された「論理計算」として「計算」に含めて考えることにしてみると、「知性」と「計算」の間の違いは限りなく小さなものに思えてくる。

　今、不用意に「論理計算」という表現を使ってしまったが、数学の「証明」では前提と結論に現れる命題たちが数学的な背景を持ったものになってはいるが、それらをつなぐ推論は、論理であり、この意味で、我々が数学的な証明の背景に思いえがく（人間の）数学的直観をとり去って、操作として眺めたときには、数学は、論理計算に他ならないものである。

　ここで言ったような意味で、論理も「計算」に過ぎないことを、最初に看破したのは、ライプニッツ (Gottfried Wilhelm Leibniz, 1646(寛永23年) ~ 1716(享保元年)) だった。ライプニッツによる、17世紀後半から、18世紀初めにかけての論理学の研究自身は、殆ど未発表で、残された草稿からその全容が明らかになり、18世紀や19世紀の論理学の研究を多くの点で先取りしていたことが判明するのは、20世紀になってからだったのだが、彼が、論理学のこのような研究をしていたこ

と自体は、18世紀や19世紀の論理学の研究者たちにも知られており、その意味では、彼等への精神的影響は少なくなかった、と評価してよいようである（この評価に関しては、[20]も参照されたい）。

一方、人間の知性も、（この拡張された意味を含む）機械的な「計算」に過ぎないことを、最初に見抜いたのは、チューリング（Alan Turing, 1912(明治45年)～1954(昭和29年)）だったと思ってよいだろう。このアイデアを背景になされた彼の1930年代の研究で導入された、仮想計算機械（チューリング・マシン）は、現代の計算機のプロトタイプと呼んでもよいものだった（[22]を参照）。[2] ただし、この「人間の知性が、「計算」に過ぎない」には、異論をはさむ人も少なくないかもしれない、例えば、ゲーデルはチューリングの研究を高く評価したが、この「人間の知性が、「計算」に過ぎない」という考え方に対しては、保留の意を表したことが知られている（例えば[24]の第II章第3節を参照）。

---

2) このように書いたところ、Turing の研究をしている Zhao Fan 氏から、このチューリングが「人間の知性も、（この拡張された意味を含む）機械的な「計算」に過ぎないことを、最初に見抜いた」は、現代では誤解だと解釈されることが多いし、自分もそう思う、というコメントを頂いた。確かに、これはいずれにしても言いすぎで、ここでの表現は、「人間の知性の出力が、（個々のインスタンスでの出力という意味でも、出力全体、という意味でも、この拡張された意味を含む）機械的な「計算」に完全に含まれていることを、最初に見抜いたのは…」とでもすべきだろう。しかも、こう言い直したとしても、チューリングが、彼の1936年の論文[22]で、既に、明確に、そのような見方を背景に議論していた、というのは、数学史研究の精度でいうと、臆測でしかない。しかし、この[22]と1950年の imitation game が論じられている[23]の間のどこかの時点で、チューリングが、これを確信したと思っても、間違ってはいないように、筆者には思える。[22]で「人間の心の動き」として分析されているのは、コンピュータ（現代の意味のコンピュータでなく、計算を実行する、という現在では無くなってしまった職業についている人間）の計算の際のそれ、のみである。

この論文では、現代の用語で universal Turing machine と呼ばれるものが考察されているが、これが、「メタの立場に視点を移行して考える」という人間にそなわっているように思える知性の働きに対応するものになっている、という議論が書いてあるわけでもない。

そのため、筆者の過剰解釈になってしまっている可能性も少なくないのではあるが、歴史家としてではなく、数学者としての筆者は、チューリングが、[22]の執筆の段階で、既に、これについての確信を得ていた、という見方にかけてみたいような気もしているのである。

昨今、いわゆる「AI翻訳」や[3)]、ChatGPTを初めとする“large language models”の台頭が、話題をさらっているが、そういった「知性的な」計算機を既に知っている我々にとっては、ライプニッツやテューリングのアイデアは、そんなに不思議なものに思えないかもしれない。しかし、彼等がこのような現代の計算機が想像もつかない時代に、ここで言ったようなアイデアに到達していたことは驚愕に値すると言ってよいだろう。

一方、狭義の計算と、証明の間には、有限の対象に対する考察に限定しても眩暈のするような乖離がある。これは次のような例を見てみると理解できるだろう。

チェビシェフの定理、あるいはベルトラン仮説と呼ばれる定理は、任意の自然数 n に対し、n と $2n$ の間に少なくとも一つは素数が存在することを主張するものである。この定理の、チェビシェフによる元々の証明は、少し複雑な、解析学を用いるものだが、もう少し簡単な、ラマヌジャンによる証明があり、更に初等的な、エルデシュが19才のときに発表した証明は、[1] に細説されている。初等的といっても、どうやってこの証明を見つけたのか分らないような ([1] で言うところの「天国にある本」に書いてあるような) 不思議な証明である。

Wikipedia [26] によると、2023年2月現在に知られている最大の素数は、

$$2^{82,589,933} - 1 \tag{2}$$

だということである。ここで、

3) ここでわざと「いわゆる「AI翻訳」」など括弧つきで、もってまわった言い方をしたのは、AI (artificial intelligence) という単語が本来指すべきものは、現在既に実現できているものではなく、むしろ近い未来に実現されるかもしれない本物の intelligence を指すための用語であるべきである、という理解に基づくものである。人間は動物と話すこともできるし、お人形と話すこともできる、という能力／習性を持っていることと、これらの現行の技術をAIとして売っている／売り出そうとしている会社たちの宣伝戦略のようなものの組み合わせで、いささか混乱が生じていると言えるのではないかと思うのだが、このことは、ここでの論考とは別の文脈に属す話題であるようにも思えるので、これに関連する議論の細説は、別の機会に譲りたいと思う。

$$2^{82,589,933} \quad \text{と} \quad 2^{82,589,934} \quad \text{の間にある素数のうち最小のもの} \qquad (3)$$

という指定を考えてみる (後者の数では、2の肩に乗った数字が1だけ大きいことに注意)。チェビシェフの定理から、そのような数は、実際に存在して、この数は、(3) での指定により一意に確定するし、それには、$2^{82,589,934}$ という上限すら存在する。それにもかかわらず、この数は、現在計算することができず (つまり (2) のような具体的な表現を「計算」することができない — もしできるなら、(2) が現在の最大の知られている最大の素数である、という事実に矛盾である)、更に、未来でもそうでない可能性も高い: もちろん (2) より大きな素数 (の具体的な表現) が将来見つかる可能性はあるが、発見されることになる素数が、(3) で指定したものであるとは限らないし、それが $2^{82,589,933}$ と $2^{82,589,934}$ の間に入っていることすら、あまりなさそうに思えるからである。

ちなみに、$2^{82,589,933}-1$ が素数なら、$2^{82,589,934}-1$ も素数かもしれない、と思う人もいるかもしれないが、この形の素数 (メルレンヌ数) に関する基礎理論 (例えば、[27] で、基礎事実が、証明も含めて確認できる) から、$2^{82,589,934}-1$ は素数でないことが直ちに証明できる。こう言うと、これも、証明はできるが、計算で具体的に確かめることはできない事例の一つ、であるような気がしてくるかもしれないが、実は、$2^{82,589,934}-1$ が素数でないことを例証する素因数分解 (の一部) は、(これが素数でないことの証明を応用して計算すると) 割合い簡単に求めることができる。例えば、この計算の一部になる 82589934 の素因数分解は、私が今この記事を書くのに使っている emacs で primes.el というパッケージを読み込んで、例えば `*scratch*` バッファで、

`(prime-factors 82589934)` [control-j]

`(2 3 7 1966427)`

として難無く求めることができる。この計算結果と、先程述べた証明から抽出し

た事実を用いると、$2^{82,589,934}-1$ は、$3\times 7\times 127\times \mathtt{rest}$ と因数分解できることが直ちに分かる(ただし、“rest”と書いた部分は、まだ更に因数分解が可能かもしれない)[4)]。

ここで見たように、現代のコンピュータの計算力で太刀打ちのできる計算と、証明によってのみ到達できる(一般化された意味での)計算の可能性の境界線は、複雑に入りくんでいるし、何がこの境界線のどちら側にあるのかは、個別に調べてみないと分らないことも多い。

ここで見たのは、計算できるはずだが、計算に必要な時間やメモリーのリソースが物理的に可能でないかもしれないものについて、数学的証明という形でのアプローチが可能であるようなものがある、という種類の状況を示す例だった[5)]。

計算のアルゴリズムはあるが、その計算や、同じ計算をするための他のどんなアルゴリズムについても、必要となる時間やリソースが物理的な制約の中に入りきらないようなものになってしまう、というような計算 (feasible でない計算)、も存在する。これは人工的にそのようなものを作れるだけではなく、数学的に自然なもので、そのようなものになってしまうものも、多く知られている。ここでは紙数の制限から、子細の説明は省略せざるを得ないが、Paris と Harrington によって見つけられた、有限 Ramsey 定理の変種に関連する関数(「相対的に巨大」な

---

4) こう書いたところ、草稿に目を通していただいた酒井拓史氏から、n が偶数のときには、$2^n\equiv 1 \mod 3$ となり、n が奇数のときには、$2^n\equiv 2 \mod 3$ になるので、$2^{82,589,934}-1$ が 3 で割れることは、すぐに分かる、というコメントを頂いた(この両方の事実は、組にして両方いっぺんに帰納法で証明できる)。実際、このことと、2^n-1 がメルセンヌ数のときには、n は素数になることから、$2^{n+1}-1$ は常に 3 で割切れ、特に、メルセンヌ数ではないことが分かる。またメルセンヌ数は常に、$\mod 3$ で 1 であることも分かる。

5) 「計算に必要な時間やメモリーのリソースが物理的に可能でない」という制約も、更に細かく見てみると、単に「現在の計算機では可能でない」というものから、計算するとしたら、物理的な制限の限界を考えても宇宙開闢から現在までの時間以上の時間が必要になる、とか、宇宙に存在する素粒子の全数より大きな数のメモリーが必要になる、というような、究極の物理的不可能性までの、グレイスケールのグレデイションを考える必要が出てくる。これについては、本文のすぐ後で書くことになる例も参照されたい。

一様集合の存在を保証する、色分けされるべき、集合族の台集合の最小のサイズを与える関数、[19] を参照されたい) $\sigma : \mathbb{N} \to \mathbb{N}$ がそのようなものの例の一つになっていることを注意しておく — 更に言うと、この関数はどの原始帰納的関数より速く増加することが示せる。[6)]

今まで考えた計算問題は、計算する対象の存在が確定しているようなものばかりだったが、そもそも計算できるかどうかが不明である、という問題もありえる。不完全性定理を応用すると、そのような不思議な状況を容易に作ることができる。不完全性定理の応用で得られる、そのような計算のうち一番直接的なものの一つは、

それがペアノ算術からの $0 = 1$ *の証明をコードしているような数* n (4)

の計算が挙げられるだろう。コンピュータで何らかのプログラムを実行するときには、このプログラムはコンピュータの中では、0と1の列、つまり自然数の二進法表示に相当するものとしてコードされているわけだが、(4) では、それと類似のコードで、数 n が記号列をコードしていて、その記号列がペアノ算術の公理系 (初等算術の体系) での、等式 $0 = 1$ の証明になっているような最小の数 n と言っているわけである。

ゲーデルの不完全性定理は、(4) でのような n が存在しないことがペアノ算術から証明できないことを主張するものである。しかし、もしこのような n があったとすると、それから、$0 = 1$ の本物の証明がデコードできてしまうので、ペアノ算術は (本当に) 矛盾していることになり、数学の基礎が根底から崩れてしまうことになる。これが起らないことの最終的な保証が存在しないことを、不完全性定理は示しているのだが、一方これが起らないことの状況証拠以上の保証があることも知られている (たとえばゲンツェンの定理がそのようなものの一つである)。

6) ここで、関数 $f : \mathbb{N} \to \mathbb{N}$ が、関数 $g : \mathbb{N} \to \mathbb{N}$ より速く増加する、と言っているのは、ある $N \in \mathbb{N}$ をとると、すべての $m > N$ に対し、$g(m) < f(m)$ が成り立つこと、である。

ある自然数 m が与えられたときには、この m が $0=1$ の証明をコードしているかどうかを判定するアルゴリズムは存在する。したがって、$0, 1, 2, 3, \ldots$ と、順に、これらの数が (4) での n になっていないかどうかを調べてゆくことはできる。このプロセスは無限に止らないと信じてよいだろうが、しかし、本当にいつか (4) のような n を出力して止まる、ということは絶対にない、という最終的な保証もないわけである。

2 無限の数の計算

前節で見てきたような、(有限の) 数の計算での、既に手におえなくなっているように感じられる複雑な状況を頭に置くと、「無限の数」の計算などは、全くお手上げ状態になってしまっているのではないか、と思う人もあるかもしれない。しかし、「無限の数」の計算を考えることは、十分にできて、[7] その計算は、場合によっては、有限の数での対応する状況よりずっと簡単になっていることもあるし、逆に複雑すぎて普通の数学の枠組の中におさまりきれなくなってしまうこともあり、その複雑さの度合のパタンは、有限の数における状況とは些か呈を異にするものとなる。

有限の数と無限の数の大きな違いの一つは、有限の数では、順序数 $(0, 1, 2, 3, \ldots$

---

7) ここで「無限の数の計算」と言っているのは、カントル (Georg Cantor, 1845 (弘化 2 年) ~ 1918 (大正 7 年))、により、1870 年代から 1880 年代に確立された、超限順序数と無限基数の理論のことを指している。ただし、超限順序数と無限基数の理論は、20 世紀から現在まで、大きな進歩を遂げているので、カントルのこれらの無限の数の導入が、数学史上の輝かしい瞬間の一つであることには異論はないにしても、カントルの名前を挙げて終りとしてしまうのは、「集合論的数学」に造詣のない人への説明としては、あまりに不完全であるように思える。少なくとも、1910 年代のハウスドルフによる、基数算術の古典理論の確立、1920 年代の、フォン・ノイマンによる順序数や基数 (自然数を含む) の再定式化、1970 年代のイェンセン (Ronald Jensen, 1936 (昭和 11 年) ~) による微細構造の理論の導入 (これは順序数算術を集合論の内部モデルの理論に関連づける理論と見ることができるだろう)、1980 年代以降のシェラハによる基数算術の理論、などは、言及すべき節目と言えるだろう。

と数え上げてゆくときの、数え上げの順番に着目したときの数）と、基数（集まりの中の要素の個数としての数）の算術的な差がないのに対し、無限の数では、順序数算術と基数算術が全く異るものになってしまうことである。

このことを見るために、まず、順序数の構成と順序数算術について、ここで許されている technicalities の範囲での直観的な言葉で、復習してみようと思う。

自然数 $0, 1, 2, 3, \ldots$ を考えて、これら全体を一つの集まりとして考えられる立場で議論する。公理的集合論では、このことは、無限公理と呼ばれる公理を仮定することに対応する。[8] 自然数全体からなる集まりを数学では、blackboard bold 体の $\mathbb{N}$ で表わすことが多いが、これを一つの新しい数と捉える立場で見るときには、ギリシャ文字の ω で表わす。聖書の黙示録にある、我は α なり ω なり、というときの ω である。集合としては、$\omega = \{0, 1, 2, 3, \ldots\}$ で、ω は、この集合上の順序 $0 < 1 < 2 < 3 < \cdots$ を表わす「数」となっていると考える。ここで ω の次の数 $\omega+1$ をとる。$\omega+1$ は、集合としては、$\omega+1 = \{0, 1, 2, 3, \ldots, \omega\}$ で、この集合上の順序 $0 < 1 < 2 < 3 < \cdots < \omega$ を表わす「数」となっている。同様に、$\omega+2, \omega+3, \omega+4, \ldots$ が作れるが、これらすべてが作られた後、ここでの「$\ldots$」の極限をとって $\omega+\omega$ が得られる。[9] $\omega+\omega$ は、順序型 $0 < 1 < 2 < 3 < \cdots < \omega < \omega+1 < \omega+2 < \omega+3 < \cdots$

---

8) ω の存在が無限公理なしでは証明できないことは、比較的簡単に示せる。例えば、[2] の付録 C 定理 25 を参照。

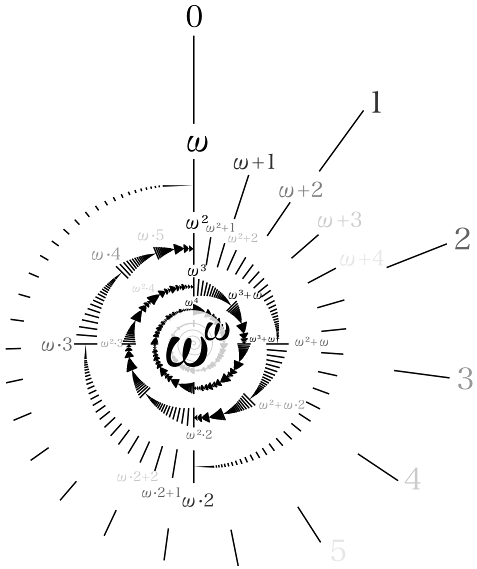
9) ここで、$\omega+\omega$ をフォン・ノイマン流のモダンな順序数の理論で得るには、ツェルメロの集合論では不十分で、ツェルメロ＝フレンケルの集合論が必要になる。このことは、ツェルメロ＝フレンケルの集合論で、$V_{\omega+\omega}$（累積的階層の $\omega+\omega$ 番目のもの）を考えると、$\omega+\omega \notin V_{\omega+\omega}$ だが、$V_{\omega+\omega}$ はツェルメロの集合論のモデルになっていること（および $\omega+\omega$ の定義の推移的なモデルでの絶対性）から結論できる。

一方、古いタイプのツェルメロの集合論で実行できる順序数の理論は、一般論としてはクラスのクラスを考えなくてはならなくなることから、基礎付けがうまくできなくなるので、色々と場合場合で補正して使わなくてはならなくなり、煩雑である。

ちなみに、ここで累積的階層と言っているのは、空集合から始めて、すべての順序数上の帰納法（再帰的定義）で、次々に冪集合を作ってゆくことで（極限ではそれまでに作ったものを全部合せる）構成される階層 V_α,（ただし α はすべての順序数を動く）のことである。

を表わす数である。これを、順序数の掛け算で $\varepsilon \cdot 2$ とも表わすことにすると、$\varepsilon \cdot 2+1, \varepsilon \cdot 2+2, \varepsilon \cdot 2+3, \ldots$ と続けて、これらの極限で $\varepsilon \cdot 3$ を得る。以上のようなプロセスを繰り返すことで $\varepsilon \cdot 3, \varepsilon \cdot 4, \varepsilon \cdot 5, \ldots$ が得られ、これらの極限として $\varepsilon \cdot \varepsilon$ あるいは、ε^2 が得られる、ここまでのプロセスを同様に繰り返すことで、$\varepsilon^2, \varepsilon^3, \ldots$ が得られ、これらの極限として $\varepsilon^{\varepsilon}$ が得られる、 etc.

　これらの順序数は、すべて可算である。つまり、これらの順序数は、どれも集合としては ε と one to one onto に対応づけることができる。たとえば、$\varepsilon+1$ が可算なことは、ε の要素としての 0 を $\varepsilon+1$ の要素としての ε に対応づけ、ε の要素としての $n+1$ を $\varepsilon+1$ の要素としての n に対応付ける写像が one to one onto になることから分かる。$\varepsilon+\varepsilon$ が可算なことは、ε の要素としての $2n$ を $\varepsilon+\varepsilon$ の要素としての n に対応させ、ε の要素としての $2n+1$ を $\varepsilon+\varepsilon$ の要素としての $\varepsilon+n$ に対応させることで得られる one to one onto の写像から分かる。ε^2 の可算性の証明はもう少しチャレンジングだが、有理数の全体 $\mathbb{Q}$ が可算であることの証明と同じアイデアで示せる。



[28] で引用されている、0 から ω^{ω} までの順序数の視覚化

これは，螺旋階段を下から見上げた構図だと思うと、腑に落ちるかもしれない。

　このように続けてゆくと、ある時点で極限をとったときに、それが最早、可算な順序数でなくなる。そのような順序数を、ε_1 と表わす。ε の存在を保証するのには、無限公理が必要になるのだったが、一旦 ε の存在を認めてしまうと、ε_1

の存在を保証する (証明する) ためには、新たな公理は必要にならない。ただし、$\omega+\omega$ の存在に関して既に注 9) で触れたように、フォン・ノイマンの意味での順序数として ω_1 がとれるためには、ツェルメロの集合論では不十分で、ツェルメロ＝フレンケルの集合論で議論していることが必要である。

ω が可算性の尺度となる順序数 (最初の無限順序数) だったように、ω_1 は最初の非可算性の尺度となる順序数 (最初の非可算な順序数) である。そこで、そのような集合の大きさ (濃度) の尺度となる順序数を基数とよび、ω や ω_1 を基数として考えるときには、それらを、ヘブライ語のアルファベットの最初の文字 $\aleph$ (aleph) を使って、それぞれ $\aleph_0, \aleph_1$ と表わす[10]。

順序数の生成は、ω_1 を超えて、$\omega_1+1, \omega_1+2, \ldots, \omega_1+\omega, \ldots, \omega_1+\omega_1, \ldots$ と続いてゆくが、ここで書いた順序数はすべて濃度 $\aleph_1$ である。つまり、集合として、ω_1 と one to one onto に対応づけすることができる。しかし、順序数の生成のプロセスのある時点で、極限をとったときに、もはや濃度が $\aleph_1$ でなくなっているときが来る。このことの証明も、ω_1 の存在の証明と同様にできる。ここで現れる最初の濃度が $\aleph_1$ でない順序数は、ω_2 と表わされ、それを基数と捉えるときには、$\aleph_2$ と表記する。

このように順序数の生成を続けてゆくと、節目になる基数が $\omega_0, \omega_1, \omega_2, \omega_3, \ldots$ と得られる (ただし、ω_0 は ω をこの基数の列のメーンバーとして見るときの別名である)。基数の極限も基数になることが示せるので、これらの極限として ω_ω (基数としての表記は $\aleph_\omega$), 更に $\omega_{\omega+1}, \omega_{\omega+2} \ldots$ と無限に続いてゆくことになる。これにより、すべての順序数 α に対して、α 番目の基数 ω_α (または $\aleph_\alpha$) が対応することになる。順序数の全体の中で一つの基数 ω_α が現れると、次の基数 $\omega_{\alpha+1}$

10) 無限基数をヘブライ語の $\aleph$ (aleph) を使って表わすのは、カントルが導入した伝統である。基数算術では、ヘブライ語のアルファベットの二番目と三番目の文字 $\beth$ (beth), $\gimel$ (gimel) も用いられることがあって、これらの記号は LaTeX での amssymb の数学記号の基本セットの中にも含まれている。

までには濃度 $\aleph_{\alpha+1}$ のギャップがあるのだが、全体として見たときには、基数たちは、順序数たちの中にぎっしりと詰っている（基数の全体は順序数の全体の中の closed unbounded な部分クラスをなす）。

以上の順序数の生成の説明の中にも既に出てきたように、順序数の間の和や積や冪を考えることができる。一般には、順序数 α と β の和 $\alpha+\beta$ は、順序型 α のうしろに順序型 β をつなげて得られる順序型に対応する順序数である。一方、順序数 α と順序数 β の積 $\alpha\cdot\beta$ は、順序型 α のコピーを β 個ならべたとき（つまり β の要素のそれぞれを α のコピーで置き換えて、辞書式に並べたとき）に得られる順序型に対応する順序数である。この定義は、有限の数（自然数）の和と積の定義を拡張するものになっており、実際、有限の数の和や積の再帰的定義を拡張する（超限再帰的）定義により導入することもできる。しかし、無限順序数の四則演算は有限の数のそれとは、かなり性格を異にするものとなる。例えば、和に関しては、次のようなことが成り立つ。（有限なものも含めた）任意の順序数 α, β について、β が 0 でないなら、$\alpha < \alpha+\beta$ である。これは、有限の数の和でと同じだが、一方、$\alpha < \beta$ で β が α より十分に大きいときには、$\alpha+\beta=\beta$ となる。例えば $(2^{82,589,933}-1)+\omega=\omega$ だし、$\omega+\omega^2=\omega^2$ である。特に、順序数の和は可換ではない（つまり、足し合せの順序を変えたときに、出てくる答が必ずしも同じにならない）。同様のことは順序数の積についても言える。

無限基数の四則演算は、（無限の基数に対しては）順序数のそれらの演算とは異るものになる。κ と λ を基数とする（つまり、有限の順序数（$=$ 有限の基数）であるか、または、ある順序数 α に対し、$\aleph_\alpha$ という形で表わせる順序数であるとする）。このとき、基数の和 $\kappa+\lambda$ を、互いに素な集合で（つまり、共通部分が空の集合で）それぞれの濃度が κ と λ の集合 X, Y をとったときの、和集合 $X\cup Y$ の濃度となる基数のこととする。同様に、X と Y を同様にとるとき（こちらの場合には、互いに素である必要はない）$\kappa\cdot\lambda$ は、積集合 $X\times Y := \{\langle x,y\rangle : x\in X, y\in Y\}$ の濃度となる基数のこととし、κ^λ は、$\{f : f : Y\to X\}$ の濃度となる基数のこと

とする。特に、この定義から、2^{λ} は、冪集合 $\mathcal{P}(Y)$ の濃度となることがわかる。

　これらの定義も有限の数の和、積、冪の組合せ論的特徴付けの拡張になっているので、有限の κ, λ に対しては、通常の和、積、冪と一致する。定義から、基数の和と積は可換になることは明らかなので、既にそのことから、順序数の和と積とは異るものになることが分かるが、実は、基数の和と積は、無限の基数の場合には、有限の場合よりずっと簡単な計算で求まるものになる。κ と λ の少なくとも片方が無限基数の場合には、$\kappa+\lambda=\kappa\cdot\lambda=\max\{\kappa,\lambda\}$ となるからである。

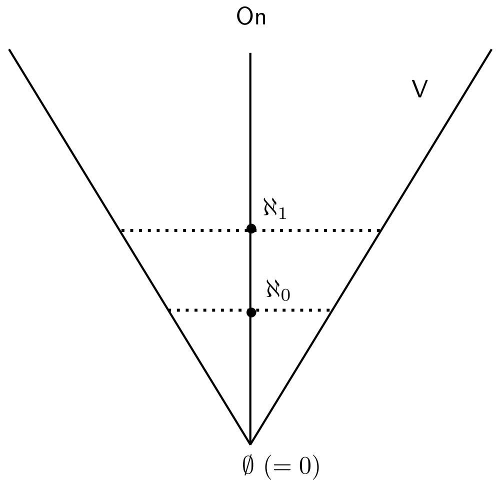
　このように、無限基数の和と積は、ほとんどトリヴィアルなものとなるが（とはいっても、これらの演算は、具体的に与えられた集合の濃度を決定するときに基本となるものでもあるが）、一方、無限基数の冪は、ひどく扱いづらいものである。まず、無限基数の冪は、選択公理なしでは定義できない。κ^{λ} は、それぞれ濃度が κ と λ の集合 X, Y をとったときの、集合

$$\{f : f : Y \to X\} \tag{5}$$

の濃度、と定義したが、そもそも、このような集合が濃度を持つ（つまり、この集合と、ある基数 $\aleph_{\alpha}$ との間に one to one onto な写像が存在する）ことを示すためには、選択公理が必要になるからである。

　現代の集合論では、更に基礎の公理と呼ばれる、古典的な数学では用いられることのない公理を仮定するが、この公理の下では、（選択公理を仮定していなくても）集合の全体からなる集合論の宇宙は、冪集合をとる操作を（空集合から始めて）超限回繰り返すことで得られるフォン・ノイマン累積的階層の全体の和と一致し、順序数の全体からなるクラス On は、集合論の宇宙をつらぬく、この累積的階層

の背骨としての役割を果たすものとなり、基数たちはこの背骨の節目となる。



順序数の全体 On は累積的階層によって生成される集合論の宇宙 V をつらぬく背骨になる。基数 $\aleph_0, \aleph_1, \ldots$ はこの背骨の節目である。

しかし、選択公理や基礎の公理を仮定したとしても、それで事が解決するわけではない。既に注意したように、κ を基数とするとき、2^κ は、濃度が κ の集合（例えば簡単のために κ 自身）の冪集合（κ に対する $\mathcal{P}(\kappa)$）の濃度だが、現在では、この濃度は κ より真に大きく、ケゥニッヒの定理（König's Theorem これは Julius (Gyula) König による定理で、無限グラフに関する Kőnig の補題の Dénes Kőnig は彼の息子である。[11]）からの制限を受ける他は、集合論の通常の公理系からは殆ど何も制約を受けないことが分っている。[12] 特に、$\kappa = \aleph_0$ の場合には、$2^{\aleph_0}$ は、自然数の全体の集合の冪集合 $\mathcal{P}(\mathbb{N})$ の濃度になるが、$\mathcal{P}(\mathbb{N})$ は実数の全体 $\mathbb{R}$ と等濃度

---

11) 親子で、二人ともハンガリー人だが、Julius König (1849(嘉永 2 年) ~ 1913(大正 2 年)) の名前はウムラウトで書き、Dénes Kőnig (1884(明治 17 年) ~ 1944(昭和 19 年)) の名前はハンガリアンウムラウトで書くことが多いようである。

12) ここで「殆ど何も制約を受けない」と書いたが、実は、極限基数 κ (極限順序数 α に対し $\kappa = \aleph_\alpha$ となっているような基数) で、後述の (6) を満たさないもの（つまり、弱到達不可能基数でないもの）に関しては、それより小さい基数での基数の冪の振舞いが、2^κ の値に複雑な影響を与えることが知られている。既に注 7) で触れた、シェラハの基数算術は、このことに関連した様々な結果を導く理論である。

であり、[13] 等式、$2^{\aleph_0}=\aleph_1$ は連続体仮説として知られているもので、ここで言ったことは、$2^{\aleph_0}=\aleph_\alpha$ となる順序数 α が、通常の集合論の公理系からは、$\alpha \geq 1$ であること（と、ここでは説明を省略した König の定理からの帰結である、α の共終数が非可算になること）以外、何も決定できない、という、連続体仮説の集合論からの独立性と呼ばれる結果の一般化である。これはコーエン (Paul Cohen, 1934(昭和9年) ~ 2007(平成19年)) らによって1960年代に証明された結果である。

ハウスドルフ (Hausdorff 1868(明治元年) ~ 1942(昭和17年)) は、連続体仮説を一般化した、すべての基数 κ に対して $2^\kappa=\kappa^+$ が成り立つ[14]、ということを主張する、一般連続体仮説と呼ばれる公理を導入した。これはハウスドルフが1908年(明治41年) の論文で導入した概念である。一般連続体仮説を仮定すると、基数の冪は、冪の底が2でなく、無限基数である場合も含めて、すべて一意に記述できることがハウスドルフによって示されているが（これが先に注7) で、「基数算術の古典理論」と表現したものである)、現代の興味は、むしろ一般連続体仮説を仮定しないとき（通常の集合論の公理系だけからの推論で）何が言えるのか、また、何が可能なのか（つまり通常の集合論の公理系を（例えば基数算術に関して）どう拡張することが可能なのか）、という問題であり、これについては、上記のシェラハのモニュメンタルな研究成果も含め、現在でも多くの研究がなされている。

実は、基数算術の背後には、もう一つの大きなテーマが隠れている。それは、巨大基数の理論と呼ばれるものである。[15] 自然数 $0, 1, 2, \ldots, n, n+1, \ldots$ に対して、ε は強い超越性を持っていることが分かる。ε の存在を言うために、新しい公理(無限公理) が必要になることは、この超越性の一つの顕れと考えることができる

13) $\mathbb{R}$ から $\mathcal{P}(\mathbb{N})$ への one to one onto な対応は、各実数の二進法による無限小数点表示を考えて、これから自然に定義できる $\mathcal{P}(\mathbb{N})$ の要素への対応を調節することで得られる。

14) κ^+ は κ の次の基数を表わす。$\kappa=\aleph_\alpha$ として $\kappa^+=\aleph_{\alpha+1}$ である

15) 巨大基数については、[18] も参照されたい。

だろう。基数 κ が与えられたときに κ^+ を作ることも、基数の集合が与えられたときに、その極限となる基数を作ることも、新しい公理を必要としないので、これらの操作により、ω から出発して到達可能な、$\aleph_1, \aleph_2, \ldots, \aleph_\omega, \ldots$ は ω の持っているような特別な超越性は持っていないと考えてよいだろう。選択公理の下では、κ から 2^κ を作る操作についても同様である。[16] 自分自身より小さい基数たちに対する、強い超越性を持つ、極限基数の存在を、主張する公理群は、巨大基数公理とよばれており、様々な種類のものが研究されている。[17]

巨大基数のうち、一番小さい（超越性の弱い）ものは、到達不可能基数と呼ばれるものである。基数 κ が到達不可能基数であるとは、$\kappa > \omega$ となる極限基数で、

$$\kappa \text{ は、長さが } \kappa \text{ 未満の順序数たちの上昇列の極限として表わせない} \qquad (6)$$

$$\kappa \text{ は基数の冪算に関して閉じている} \qquad (7)$$

という性質を満たすことである。ω は、(6) も (7) も満たすので、到達不可能基数の概念は、ω の自然な拡張となっていると考えることができる。この二つの性質のうち (6) のみを満たす $\kappa > \omega$ となる極限基数は、今日では弱到達不可能基数と呼ばれていて、これもハウスドルフが導入した概念である。[18]

---

16) ただし、$\aleph_1, \aleph_2, 2^{\aleph_0}$ などが、ある種の潜在的な超越性を持つことは可能で、そのことの表明となっていると解釈のできる様々な命題が、研究されてもいる。例えば、筆者らの [9]、[10]、[11]、[12] は、この $\aleph_1, \aleph_2, 2^{\aleph_0}$ がある種の潜在的な超越性を持つことと、連続体問題との関わりについての、研究である。

17) 巨大基数は、その超越性から、存在を保証をする公理は集合論の公理系からは証明できないものになるし、ある巨大基数の存在を仮定したときにも、それより「大きい」種類の巨大基数の存在の主張は、この仮定から独立となる。

18) [6] では、ハウスドルフの書いた集合論の教科書 [15]、[16] や、それらに倣って書かれた古めの一般向けの集合論の教科書の多くが、その後の集合論や数理論理学で得られた知見をもって見たときには、現代の集合論への入門書としては大変に問題のあるものになっている、という点を強調したため、その主張の影に隠れてしまって、十分に書ききれていなかったかもしれないが、ハウスドルフの、無限の算術としての集合論への貢献は、偉大であった、としか形容しようのないものである。

一般連続体仮説の下では、到達不可能基数の概念と弱到達不可能基数の概念は同値となるが、一般には、弱到達不可能基数の方が、到達不可能基数より弱いものとなる。[19]

巨大基数の全体は、(7) のような、それ未満の基数での基数算術に関しての閉包性で特徴づけられるような、小さな巨大基数[20]に対し、その少し上くらいの基数から、それ以下への反映の原理[21]として記述のできる「中程度の大きさの巨大基数」、集合論の宇宙全体から、それ以下への反映原理[21]として記述される「大きな巨大基数」に分類されるが、小さな巨大基数と中程度の巨大基数の間、あるいは中程度の巨大基数と大きな巨大基数の間には、自然数たちと ω の間に存在する絶対的な断絶のような、否や、それとは比べられないくらいの想像を超える大きな断絶が横たわっている。

しかし、注 21) で述べたような意味での「反映原理」という観点からは、一階の述語論理のコンパクト性定理を、無限から有限への反映原理と捉えることもできるので、その意味では、大きな巨大基数も、ω の概念の一般化になっている、と

---

19) しかし、到達不可能基数の概念と弱到達不可能基数の概念の無矛盾性の強さ (consistency strength) は、同じである (つまり、それらの各々が集合論の通常の公理系の上で無矛盾である、という命題たちは互いに同値になる) — このことは、これらの概念が無矛盾同値 (equi-consistent) である、とも表現される。無矛盾性の強さについては、第 5 節の初めを参照されたい。

20) 「小さな巨大基数」というのは、形容矛盾に聞こえるかもしれないが、巨大基数の理論では、「大きな巨大基数」という用語とともに、よく使う言い方である。英語では、巨大数は large cardinal なので、「大きな巨大基数」は large large cardinal になってしまい、もっと変なのであるが。ちなみに、「小さな巨大基数」は定義の確定した概念ではないのだが、ここで言っているものより精密と言える、「その存在が、ゲーデルの $\mathsf{V} = \mathsf{L}$ と矛盾しないような巨大基数」である、という「定義」が想定されていることも多い。

21) ここで言っている「反映原理」は、自分自身より (累積的階層に関して) 上の世界で起こっている現象 (のうちの指定された種類のもの) に対応する現象が、(累積的階層に関して) 自分自身より下の世界でも起こっていることの主張、として表現できるような種類の命題のことである。より技術的には、このことは、集合論のユニヴァースから内部モデルへの非自明な初等的埋め込みの存在に関する命題として記述されることも多い。

考えることも可能であろう。

3　指数関数的増加が咆哮し、階乗関数的増加が牙をむく

今度のパンデミックでは、色々と教えられることが多かった。日本の大多数の人が、数学や統計などの初歩を理解していないらしい、ということも、改めて教えられたことの一つだった。日本の場合、テレビや新聞などのメディアが、平均的な日本人の知的レヴェルを代表している、と考えてよさそうに思えるが、この日本でのメディアでのナレーションは、パンデミックの始まりから、「先週より何人増えた」、「先週より何人減った」、「はじめて何千人台を越えた」等々というようなものに終始した。ちなみに、ドイツのメディアは、パンデミックの初期から incidence number の表示を採用して、Moderator（ニュースキャスタ）が「パンデミックが始まって以来、我々は色々と新しいことを勉強することになりましたが…」などとコメントしたりしていたが、これは必ずしも、ドイツの平均の知性が日本のそれより高いことを示しているわけではなく、ドイツでは（コマーシャルでない）メディアが知的エリートをターゲットにしていて日本ではそうでない、という違いに過ぎないだろう。日本との違い、ということでは、意思決定権を持っている人たちが知的エリートでもあることが、少なくなく、そうでない人たちも知的エリートのふりをしたがる、というドイツ文化での事情が、この知的エリートをターゲットにしたメディアを可能にしている、というだけのことだろう。事実、ドイツでは、（これが広く観察されたのは、主にパンデミック以前のことではあるが）このメディアの言っていることを理解する能力のない人達が、これを „Lügenpresse“（嘘吐きメディア）と呼んで憎悪を剥き出しにする、という現象が見られた。

しかし、この「先週より何人増えた」等は、線形近似による現状分析、というより、むしろスーパーの買物での値段の計算と同レベル、と言うほかない。しかも、ここで、先週の今日の何月何日の人数に比べて、というような、生の数値を

言っているのは、平均的な人々に平均値についての理解も欠如していることを示唆している。

日本の高校では、線形（アファイン）関数だけでなく二次関数や二次の分数関数も習うはずである。引力や、ある点から放射された光りを含む放射線の強度など、距離の自乗に反比例する関数で表現できる現象は多いが、これに対する感覚は、既にこのスーパーの買物の計算能力を超えたものになっているように思える。

このことで思い出すことがある。昔、まだガラ系の携帯しかなかった時代に北海道旅行をしたときのことである。観光バスの中で SMS をチェックしていると、はす向かいの席に坐っていた老人に、自分は心臓のペースメーカーをつけているので、電源を切ってほしい、と言われたのだった。もちろん、自分がやっていることに恐怖を覚える人がいたときには、理由がどうであれやめるべきなので、携帯の電源をすぐに切ったのだが、「電磁波の強度は距離の自乗に反比例するので・・・」という説明をすべきか、どうか、ちょっと迷った末、何も言わないことにしたのだった。

一方、核反応などでの連鎖反応や、人口爆発、感染症の拡大でのダイナミズムは、指数関数的なものである。指数関数は、どんな多項式関数よりも速く増加する。あるいは肩に載っている変数に負の係数がかかっているときには、どんな正の多項式分数関数より速く減少する（0 に近づく）のであるが、このことは、二次関数や二次分数関数の増減についての感覚さえおぼつかない人たちに理解ができるとは到底思えない。しかも日本の場合、多分19世紀末に日本に輸入されたと思われる、「幾何級数的」という死語になっているべき表現が（ガラパゴス化して？）、「指数関数的」(exponential) という表現と拮抗しているために、分りにくさを助長しているように思える。

コンピュータサイエンスの素養のある人は、遅くても $P \neq NP$ 問題について学んだ段階で、この本質的な関数の増加の速さの違いを認識するはずであるが、これも、ひょっとすると「はずである」と、現実の間の、乖離が存在するかもしれ

ない。

今回のパンデミックは、今、終息に向っているように見えるが、このパンデミックでは、幸いに、この指数関数的な展開が感じられたのは、ほんの何回かで、数日間から一週間くらい、ごく短い期間の展開についてのことに止まったと言えると思う。そうだったのは、微分方程式の抵抗項に対応するファクターがそれほど小さくなかったことが幸いしているのだろうが、これは、population の感染症の感染拡大に対する構造的な安定性というよりは、たまたま大丈夫だった、ということにすぎないようにも思える。一方、我々は、そういう不幸中の幸いのみに頼っていると、どんな壊滅的状況が起こり得るかということも、特に、昨今の自然災害や非自然災害の多くで、経験を積みつつある、ところでもある。

そう考えると、この増加の度合いが線形性の言葉（以下）でしか理解のできない平均的な人々(?)の事態の認識能力の欠如は、democratic な意思決定ということの下では、ひどく危険なことに思える。[22)]

日常で遭遇する速い増加ということに関して、指数関数がノンプラスウルトラか、ということこれは、全くそんなことはない。組合せの数を考えるときに出てくる、階数関数が、指数関数型の関数に対して、それらのどれよりも速く増加する関数になっている。第1節で触れた、Paris-Harrington タイプの関数も、組合せ論的な関数であり、階数関数型の関数のさらに彼方に鈍い光りを放っている。

4　実数の計算

いわゆる「科学技術」に関連する計算では、実数値の数値計算が問題になることが多いだろう。実数値の数値計算は、いずれにしても近似計算でしかありえな

22) autocratic な意思決定が、旧式の democratic な意思決定よりまし、というわけでも必ずしもないことも、このパンデミックと同じ時期の様々な世界の動向が教えてくれた教訓であるように思える。

い。実数は、一般には無限桁の小数表現が必要になるが、我々が扱えるのは、どう頑張っても有限桁で、その桁数も極めて限られたものにならざるを得ないからである。

一方、例えば、物理での計算では、この計算に入力すべき観測値自身も、測定方法やその誤差などから来る制限や、量子力学的な理論的な制限から、限られた桁数のものでしかありえないので、計算値で意味のある桁数も、結果的に小さなものにしかなり得ない。

[21] によれば、NASA による軌道計算での最高精度の計算で使っている π の値は、3.141592653589793（小数点以下 15 桁）だということである。[21] には、人類が宇宙に送った人工物で、一番地球から遠くに到達したのは、Voyager 1 で、これは、現在地球から約 14.8×10^9 マイルほど離れた地点にいるが、地球を中心に、この半径の円を描いた時、π を小数点以下 15 桁までで打ち切ったことによる円周の長さの計算値の誤差は一インチ以下だ、という説明がある。

ただし、π 自身は関連する計算では最後に定数として値にかかる形でしか関与しない可能性が高いが（物理学で出てくる公式を思い起こしてみると、π^n や π^{-n}、$n > 1$ の形で π が現れるものは皆無と言っていいだろう）、値を出す途中の繰り返し計算では、誤差の集積をさけるために、もう少し多くの桁数の計算が必要になっている可能性もあるような気がするのだが。

科学技術での計算に従事している人の視点からは、無限桁の実数表示の全体としての数学の意味での実数の全体（連続体）は、無駄な高精度のように感じられるかもしれない。しかし、もし我々がある桁数に制限された実数だけからなる数の体系の理論しか持っていなかったとしたら、現在の科学技術計算がそのベースとしているような解析学は、決して生まれていなかっただろう。

この場合、物理学的現実を見ているときに有効な桁数の小ささと、物理学やその背後にある数学での理想化された無限桁小数表示としての実数の関係を、どう考えるべきなのか、数学での連続体は方便に過ぎないのか、それとも物理的実存

の背後に、ある種の極限として控えている何らかの実体と考えるべきなのか、後者だとしたら、その実存は古典的な数学で既に必要なものはすべて捉えきれているのか、それとも集合論的数学で初めて見ることができるようになる数学的現象が、実は、物理的な現象にまで影を落としている可能性もあるのか？など、このことは、少なくとも、数学、数理哲学、科学哲学の視点から見て、非常にエキサイティングで、重要にも思える問題たちに、連なっているようにも思える。

5 Speed-up 定理たち

自然数の理論から、有限桁の小数点表示で表わされる実数たちの理論、すべての実数の理論、無限集合を含む集合論の理論、巨大基数の存在を仮定する集合論の理論たち、と、考察の対象を広げていったとき、対応する公理的な背景理論もどんどん強いもので置き換えてゆく必要が出てくる。このことにより、これらの理論を展開するための公理系の無矛盾性の強さ (consistency strength) も真に大きくなってゆく。[23] ここで無矛盾性の強さと言っている概念の標準的な定義の一つは、理論T'の無矛盾性の強さが理論Tより (無矛盾性の強さに関して真に) 強い、とは、理論T'で理論Tの無矛盾性が証明ができることである。第二不完全性定理により、ここで考えている理論Tが無矛盾なら、TではT自身の無矛盾性は証明できないので、T'はTでは証明のできないことの証明ができる (特に$T \subseteq T'$のときには真の拡張になっている) 理論となっていることがわかる。

ツェルメロの集合論では、自然数論のモデルが構成できるので、自然数論の矛盾性が証明できる。つまり、ツェルメロの集合論の無矛盾性の強さは、自然数論より大きい。ツェルメロ＝フレンケルの集合論では、ツェルメロの集合論のモデ

23) ただし、自然数の理論から有限桁の小数点表示で表わされる実数たちの理論への移行は、理論の背景となる公理系の取り方によっては、無矛盾性の強さが大きくならないようにできている場合もありえる。

ル $V_{\omega+\omega}$ が存在するので[24]、ツェルメロの集合論の無矛盾性が示せる、到達不可能基数 κ の存在の主張を集合論の公理系に加えた公理系では、集合論のモデル V_κ が存在するので、この公理系では集合論の無矛盾性が証明できる、等々。

無矛盾性の強さと言うと聞こえがいいが、T' が T より無矛盾性の強さが強い、ということは、T' の方が、T より、矛盾している「確率」が高い、ということでもある。このような背景から、「できるだけ（無矛盾性の強さの）弱い理論体系で展開できる数学が安全で、そのようなものが望ましい」という結論を導き出すことも可能なように思える。実際、そのような立場で数学を考えるべきだ、と主張する数学者たちは少なからずいたし、現在でもいるかもしれない。クローネカ (Leopold Kronecker 1823(文政6年)〜1891(明治24年)) は、そのような立場をとった有名な数学者のうちの最初の人たちの一人で、彼は、この立場から、かつての弟子だったカントルの集合論や、カントル自身に対して、猛烈な批判や攻撃を続けたし、「整数は神が御造りになった。それ以外は全部、人の捏造したものにすぎない[25]」という有名な言葉を残してもいる。もちろんクローネカはゲーデルより前の時代の人なので、ここで言ったような、不完全性定理による議論を知りようはなかっわけなのだが。

逆に、あえて、この矛盾している「確率」の高い、強い公理系の下で数学を展開することに、何らかの積極的な意味を見出すことはできるのだろうか？実は、不思議なことに、不完全性定理の証明の変形から、この無矛盾性の強さの大きな公理系で数学を展開することの意義を説明することができる。それは、二つの理論 T と T' について、T が数論を含んでいて、T' の無矛盾性の強さが T のそれより真に大きいときには、T で証明できる命題 φ で、これを T で証明すると、物理的に不

24) 注9) を参照。

25) „Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk" — 886 年にクローネカがベルリンでの科学者会議に講演で言ったとされる言葉。

可能な長さの証明しか存在しないが、T'での証明は、実現可能な長さのものになるようなものが存在する、というものである。これは、ゲーデルの Speed-up 定理と呼ばれるものを巷の言葉で言いなおしてみたものなのだが、この定理の証明を見てみると分かるように、そのようなφは存在することが言えるだけでなく、多少人工的な形はしているが、具体的に与えることもできる。ゲーデルの Speed-up 定理（や類似のその他の speed-up theorems）については、[4]や、そこで挙げた文献を参照されたい。

実は、T' の無矛盾性の強さが T のそれより真に大きくなくても、T' が、T の真の拡張になっているときには、speed-up 現象が起ることが知られている（Ehrenfeucht-Mycielski Speed-up 定理、この定理の証明は、[13]に書いた）。

ゲーデルや Ehrenfeucht-Mycielski の Speed-up 定理たちから、たとえば、数論と集合論、集合論と集合論に巨大基数の存在公理を付加したもの、というような、妥当な公理系の組T、T'で、T'がTの拡張になっていて、T'の無矛盾性の強さがTのそれより真に大きいようなものが与えられたとき、とりあえず拡張された方の公理系T'で数学を展開してみる、という方針が妥当なものであると議論することができるだろう。この方針をとったときに、Speed-up 定理たちが示唆しているように、T'で、Tで得られるより、容易に、ずっと短く、したがって簡単である可能性も高い証明が得られる可能性があるからである。

そのような試みから、Tの言語でも書き下せる命題φが、T'で証明できたときには、次のような①〜②(γ)(2)のシナリオの可能性が考えられる。

①: 得られたφの証明が、実は、ほとんどそのまま、あるいは多少の変更でTの証明に書き換えることができる場合。この場合には、この変更をしさえすればTでの結果が得られるわけなので、もし、読者が、T'での数学を認めない立場だったとしても、T'はこの場合、Tでの数学研究の tool として用いられたと解釈することができる。

②: 得られたφのT'証明が、straightforward にはTでの証明に翻訳できない

場合。この場合には、更にいくつかの可能なシナリオが考えられる。

②(α): T'でとは全く異るTでの証明が可能な場合。これは、T'を集合論として、Tをペアノ算術としたとき、第1節で触れたチェビシェフの定理の、エルデシュによる証明が、ちょうどそのようなものの例になっている。この場合、Tでの証明は、T'でのそれとは全く異るとしたので、T'で得られている証明は、Tの証明に何等貢献していないようにも思えるが、実際には、T'で得られている証明を見て、Tでも証明できるに違いない、と思うことは、心理的にはTでの証明を試みるときの大きな支えになりえるので、そのような心理的なサポートとして生身の数学者の研究に対して、大きな貢献があったと解釈することもできる。

②(β): φは、Tでも証明できるが、その証明の長さはfeasibleなものでなくなってしまう場合。これが、まさにゲーデルのSpeed-up定理が、そのようなことがあり得ることを指摘しているような場合である。

この場合には、(1) Tでの証明の長さがfeasibleなものでありえないことを何等かの超数学的な手法で証明できる場合、がありえるが、(2) そうでない場合、には、Tでの証明の試みは暗礁に乗りあげたような状態になってしまう。

②(γ): φは、Tでは証明できない場合。これは、やはり、T'を集合論として、Tをペアノ算術としたとき、第1節で触れたParis-Harringtonの定理での有限組合せ論の命題がそのようなものになっている。この定理での場合のように、(1) 実際に超数学的手法で、(1) φがTでは証明できないことが証明できる、という可能性もあるが、ここでも、(2) そのような証明が得られずに、Tでの証明の試みが袋小路に入ってしまったような状態になってしまうこともあり得る。

ここで見たシナリオたちのうち、②(β) (2) と、②(γ) (2) で起ってしまうの停滞は、T'を認めず、Tの中だけで考えるという立場で研究していたとしても、起こるしかないものだが、そのような立場で、超数学的な考察も拒否しているのなら、②(β) (1) や、②(γ) (1) の形で状況が打開される可能性からも、見放さ

れてしまうことになる。①や②(α)では、T-純粋主義者は、T'での研究結果の助けなしでもφの証明を見出せているかもしれないが、証明を発見するまでにT'での証明を経由した場合に比べて、ずっと時間がかかってしまっている可能性もある。

Tだけを認める立場にとっての、T'の理という観点から議論してみたが、Tと、T'が、与えられたときに、もっと積極的にT'での数学を推奨する理由も、複数あげることができる。その一つは、既に述べたように、短い証明が得られる可能性があることであるが、ただ短かくて簡単な証明が得られる可能性がある、というだけでなく、強い方の体系で得られる証明によって、定理の意味がより明確になる可能性がある、ということも挙げられる。

このことの、歴史上の例の一つには、三次や四次の方程式の解法があげられるだろう。タルタガリアやカルダーノの中世の数学では、これは、一種の秘法として、現代の言葉で整理しなおすと、冪根の表現を含む代数的な表現で表わせる数の作る体での一階の理論として研究された。当時は、これらの偉大な数学者たちが一生を捧げる課題だったが、現代では、この理論は、体の拡大や、対応する自己同型群の間の相互作用を記述するガロアの理論やその拡張、という、高階の理論(集合論の中で展開できる理論)での、もっと大きな文脈の中の一つの現象として、より整理された形で理解できるだろう。

もう一つの例として、ここでは、古典的な集合論的数学について触れておきたいと思う。ツェルメロ(Ernst Zermelo, 1871(明治4年)~1953(昭和28年))が集合論の公理系を考察したのは、1908年(明治41年)の[29]だった。これは、現在Zermelo の集合論 ZC と呼ばれるもの(と全く一致するわけではないが、これ)に大体対応するものである。この前後にヨーロッパでは、ZC で展開されていると考えられる集合論的数学が様々な分野で試みられている。

一方、現在集合論の公理系として標準的に考察されるツェルメロ-フレンケル集合論 ZFC と呼ばれる体系は、既に触れたように、ZC より無矛盾性の強さの大き

な体系で、この体系が確立するのは、ツェルメロ、フレンケル、フォン・ノイマン、スコーレムといった人達の研究を経た、1940年代のことだった。筆者が前のパラグラフで「集合論的数学」と呼んだ研究分野は、この間、この集合論の前線での研究とはほとんど没交渉に発展したため、はっきりと公理的な枠組で議論していないことが多いので不明の場合もあるが、殆どの場合ZCでの議論を継承しているように見える。

しかし、まさにこのことが、少なくとも筆者にとっては、この古典的な集合論的数学の歴史的論文をひどく読みにくいものにしている。1970年代ごろから、この集合論的数学で、もっとモダンな、現代集合論をベースとした研究が興ってきているのだが、この新しいタイプの集合論的数学は、旧来の集合論的数学（また、旧来のカテゴリー論的数学）の視点からは、それらに、うまく融合しきれていないものになっているような気がする。このような背景を鑑みて、ここで記述したような、旧式の集合論的数学から、もっとモダンな集合論的数学への移行を促す、という意味あいもこめて、筆者は「集合論的数学」という題で、旧来の集合論的数学の様々な結果の再構成を含むテキストの執筆の準備を始めているところである（[8]）。

制限された体系のみで数学を行おうとする保守的な立場と、どんどん強い公理系での数学に移行してゆこうとする傾向のある前進的な数学、というのを、ここでは、対立する立場としてのみ記述したが、実際には、これらの二つの対極にある立場や、その中間にある様々な立場たちは、全体として相補的に共存して数学の進歩を支えてゆくべきものであると思う。

しかし、実際には、遅くともクローネカ以来、どの時代にも、この保守的な立場から、他の立場の数学を強く批判する人々が出てくる傾向があるように思えるのだが、ここでも既に分析したように、制限された体系だけで数学を実行しようとする、という意味での純粋主義者の「ぶ」は、客観的には、あまり良いものにはなっていない、としか言いようがないようにも思える。

6　有限から無限、無限から有限へ

ここまで読み進められた読者の中には、ひょっとすると、筆者が、雑多な無関連な話題について気儘なコメントをした、というような印象を持たれてしまった方もいるかもしれない。しかし、筆者がここで述べたかったことは、むしろ、これまでに話題にした、多様な視点、観点からの様々な「計算」たちが、全体として、大きな文脈に結びつけられており、これらを研究する立場からも、テクニックの共有やアナロジーによるアイデアの交換、場合によっては、第2節で触れたコンパクト性定理のような、(この定理の場合には有限と無限との間での) システマティックな遷移原理(transfer principle)などによって、高度に synagetic な状況が成立している、ということである。

特に、このシナジェティックな状況は、有限組合せ論と無限組合せ論の間では、古くから認識されていたと思うが[26)]、ここで話題としてとりあげた広い意味での有限や無限の「数の計算」での現象も超えて、もっと大きな絵の中でも成り立っていることだと思う。

最後に、ここでシナジーと言ったことの例となるような、筆者自身の研究で最近起こった事例について、話してみしたいと思う。

[14] は、筆者が 2022 年の夏に、これまでにも多くの共同研究を行なってきた酒井拓史氏との共著で書き上げた論文である。現在投稿前ではあるが、文献表にも書いた URL で、プレプリントアーカイヴに upload されている。この論文では、大きな巨大基数で起っている現象のアナロジーを小さな巨大基数の世界に移したときに何になるか、というタイプの設問に対する答が得られていて、このアナロジーの説明が、論文の初めの方に偽の等式

26)　第2節の終りで触れた、一階の述語論理のコンパクト性定理は、有限組合せ論と無限組合せ論の間の transfer を記述する定理と看倣すことができ、そう見たときには、この定理は、ここで言った、有限組合せ論と無限組合せ論の間のシナジーの説明の一つになっていると考えることができる。

$$\frac{\text{weakly compact cardinals}}{\text{strongly compact cardinals}} = \frac{x}{\text{extendible cardinals}}. \tag{8}$$

として説明してある (分母が大きな巨大基数の世界で、分子が小さな巨大基数の世界を表徴するものになっている)。著者たちのこの論文での主要結果の一つは、この等式での x が何かを決定したことである。これは、大きな無限の研究と小さな無限の研究の間での、アイデアの交流を通じての、新しいアナロジーの確立、と言えるが、更に、この研究では、Michael Rathijen の導入した shrewd cardinals と呼ばれる小さな巨大基数が、登場人物の一人となっている。Rathijen 氏は、証明論と呼ばれる研究分野の、代表的な研究者の一人で、筆者は、彼とは、ベルリンに住んでいた頃からの旧知である。氏の研究分野である証明論は、有限と無限のグレデイションに関しては、有限と無限のちょうど間くらいのグレーゾーンに位置するもので、だから、筆者の研究の位置とはかなり離れていると言える。それで、筆者自身は証明論に興味もあり勉強を試みてもいる、とはいえ、このような、研究上のクロスオーヴァーを持つことになるとは思っていなかったので、自分でもちょっとびっくりしたのだった。しかも、[14] で実際に用られているのは、筆者が大変親しくしている、しかし、やはり研究分野の違いから、研究上の交流は今までそれほどなかった Andrés Villaveces 氏が、抽象モデル理論の文脈で strongly unfoldable cardinals として導入して、後に Philipp Lücke 氏が shrewd cardinals と同じものであることを示すことになった、という背景を持つ、shrewd cardinals の特徴付けだった。

論文をプレプリントアーカイヴに upload した後、抽象モデル理論の若手のホープの一人である、Will Boney 氏がメールを送ってくれて、論文をほめてくれたのだが、彼とも面識はあったが、共同研究などをしたことはなかったので、未来の共同研究の可能性とともに、ここで我々の行なった無限の数 (巨大基数) の研究のシナジェティックな他の数学の研究分野との結びつきを強く感じたのだった。

わざわざ、自画自賛に見えてしまうかもしれない危険を犯してまで、自分の最

近の研究まで例に挙げて説明を試みてみたのは、ひとつには、「… などの研究をしてもしょうがない」という種類のコメントを言ったり、書いたりする人が少なくないので、それに対して注意を促しておいてもよいような気がしているからでもある。

ここで述べた有限と無限に関する研究たちにおける synergetic な状況でもそうだが、もっと一般的に、科学で考察される、多様な概念たちや現象たち、それを考察する研究たちの間にはりめぐらされた、アナロジーや、アイデアの共有や、連想のシナジー、まだ見えていない関連性のネットワークなどからなる、大きな文脈に様々な研究分野が有機的に複雑に絡みあった状況においては、「何が意味があって何に意味がない」、というようなことをわざわざ議論することは、あまり建設的であるとは思えない。もし本当に研究してもしようがない、と判断されることになるものがあれば、それはいずれは自然消滅するはずなので、自然消滅にまかせていればよいだけだと思う。

この、色々な場所で聞かれる、「… は研究してもしょうがない」発言は、むしろ、自分の「専門分野」に凝り固まった人々の、動物的な縄張り本能の発露のようなものに過ぎないのかもしれない。[27]

どの分野でも研究が進みすぎてしまって、全体を見渡すような研究は、今日では、もう常人にはできなくなってしまった、と言う人も少なくないかもしれないが、逆に、インターネットやコンピュータ上の様々な tools のおかげで、現在、大きな視点からのユニバーサルな研究が我々にもできる可能性は、過去に比べて格段に大きくなっている、とも言えるのではないかとも思う。そのようなスケールの大きな研究は、現実では、必ずしも、いつも十分にでききれる、とは限らない

---

27) 「理系」、「文系」という受験産業の用語を初めとして、日本の文化の中には、人が動物的「職人的専門意識／縄張り意識」を高めるための手立てが沢山仕組まれている、と言えるかもしれない。この『動物的「職人的専門意識／縄張り意識」』は、ゲーム感覚で、遊び半分に運用している限りにおいては、「競争意識を持ってお互いに切磋琢磨する」、というような積極的な意味付けも可能なのかもしれないが。

かもしれないが、少なくとも、そういうものを目指す心構えは忘れないようにしたいと思うし、そのような努力の結果に得られるであろう広い視野で見たときに、初めて見えてくることになる素晴しい風景を、眺望できることを切望するものでもある。

この作文の投稿版を『現代思想』誌に渡した直後に、Joel Hamkins が、MathOverflow に [30] を投稿した。彼がそこで書いているのは、主に計算論と集合論の間の "natural affinity" であるが、彼が書いていることも、私がここで書いた意味での「研究たちの間にはりめぐらされた、アナロジーや、アイデアの共有や、連想のシナジー」が決して私の個人的な感想にすぎないわけではないことの、一つの証明になっている、と言えるだろう。

参考文献

[1] Martin Aigner, Günter M. Ziegler: Proofs from THE BOOK, 6.Edition, Springer, (1998/2018). 日本語訳: 蟹江 幸博 訳、天書の証明、丸善出版 (2002/2022).

[2] デデキント著: 渕野 昌 訳・解説、数とは何かそして何であるべきか、ちくま学芸文庫、(2013/2021).

[3] Herbert B. Enderton: A Mathematical Introduction to Logic, Second Edition, Academic Press (2001). 日本語訳：嘉田 勝 訳、『論理学への数学的手引き』、1月と7月 (2020).

[4] 渕野 昌: 数学と集合論 — ゲーデルの加速定理の視点からの考察、科学基礎論研究、Vol.46, No.1 (2018), 33–47.
https://fuchino.ddo.jp/papers/speedup-th.pdf

[5] ______: 無限と有限の硲（はざま）にて、数学基礎論若手の会での講演 2021/12/03 (zoom, org.: 倉橋 太志 (神戸大))
講演の slides: https://fuchino.ddo.jp/wakate-fuchino-2021-12-pf.pdf

[6] ______: ハウスドルフの集合論と位相空間論の誕生 —— 現代、ないし（仮想的）近未来の視点からの考察、数理科学 2022 年 6 月号・特集「集合・位相の考え方 —— 数学の基礎をなす概念」、7–18.
出版後の拡張版が、https://fuchino.ddo.jp/misc/hausdorff-x.pdf から download 可能.

[7] ______: 論理、この厄介なもの、現代思想、 2022 年 4 月号、Vol.50, No.4, 214–229. https://fuchino.ddo.jp/misc/logic-2022-x.pdf

[8] ______: 集合論的数学、 monograph, in preparation.

[9] Sakaé Fuchino, André Ottenbreit Maschio Rodrigues and Hiroshi Sakai, Strong Löwenheim-Skolem theorems for stationary logics, I, Archive for Mathematical Logic, Volume 60, issue 1-2, (2021), 17–47.

[10] ______________________, Strong Löwenheim-Skolem theorems for stationary logics, II — reflection down to the continuum, Archive for Mathematical Logic, Volume 60, issue 3-4, (2021), 495–523.

[11] ______________________, Strong Löwenheim-Skolem theorems for stationary logics, III — mixed support iteration, to appear in the Proceedings of the Asian Logic Conference 2019.

[12] Sakaé Fuchino and André Ottenbreit Maschio Rodrigues, Reflection principles, generic large cardinals, and the Continuum Problem, to appear in the Proceedings of the Symposium on Advances in Mathematical Logic 2018, (2022), 1–26.

[13] Sakaé Fuchino, Axiomatic set theory and the foundation of mathematics, 2019年の前期と後期に、神戸と Katowice (Poland) で行なった講義の講義録.
https://fuchino.ddo.jp/kobe/logic-ss2019.pdf

[14] Sakaé Fuchino, and Hiroshi Sakai: Weakly extendible cardinals and compactness of extended logics, preprint. https://arxiv.org/abs/2212.14218

[15] Felix Hausdorff: Grundzüge der Mengenlehre, Veit & Comp., Leipzig (1914).

[16] ——————: Mengenlehre, de Gruyter (1927/1935).

[17] ——————: Gesammelte Werke, Band III, (全集 第III巻)、Springer-Verlag, (2008).

[18] Akihiro Kanamori, The Higher Infinite, Springer–Verlag (1994/2003).

[19] Jeff Paris, and Leo Harrington: A mathematical Incompleteness in Peano Arithmetic, Handbook of Mathematical Logicm ed.: J. Barwise (1977).

[20] Volker Peckhaus: Leibnitz's Influence on 19th Century Logic, Stanford Encyclopedia of Philosophy, (2018).
https://plato.stanford.edu/entries/leibniz-logic-influence/

[21] Mark Rayman: How Many Decimals of Pi Do We Really Need?, NASA/JPL Edu (2016/2022).
https://www.jpl.nasa.gov/edu/news/2016/3/16/how-many-decimals-of-pi-do-we-really-need/

[22] Alan Turing: On Computable Numbers with an Application to the Entscheidungsproblem, Proceedings of London Math Soc, Series 2, Vol.42, (1937), 230–265.

[23] ＿＿＿＿＿: Computing Machinery and Intelligence, Mind, Vol.49, (1950), 433-460.

[24] Hao Wang: From Mathematics to Philosophy, Routledge Revivals, (1974).

[25] Wikipedia: Gaussian integral,
`https://en.wikipedia.org/wiki/Gaussian_integral`

[26] Wikipedia: Largest known prime number,
`https://en.wikipedia.org/wiki/Largest_known_prime_number`

[27] Wikipedia: Mersenne prime,
`https://en.wikipedia.org/wiki/Mersenne_prime`

[28] Wikipedia: Ordinalzahl,
`https://de.wikipedia.org/wiki/Ordinalzahl`

[29] Ernst Zermelo: Untersuchungen über die Grundlagen der Mengenlehre. I, Mathematische Annalen 65 (1908), 261–281.

雑誌投稿後に加えられた補足文献

[30] Joel David Hamkins, Theorems in set theory that use computability theory tools, and vice versa, MathOverflow,
`https://mathoverflow.net/a/444997` (version: 2023-04-18)