ABC予想って？（1）：超々入門

斬新・難解な証明の検証に8年もかかった！

ABC予想って？（1） 超々入門

1. 唐突な発表で登場したビッグニュース
2. 望月新一教授（京都大学）
3. 学術誌とは
4. レフェリー制
5. 論文の長さ、論文数
6. ABC予想とは
7. 弱い形のABC予想
8. 望月教授の論文が学術誌に採択されたことの京大の発表
9. フェルマーの最終定理とABC予想
10. ABC予想を使ってフェルマーの最終定理を証明する
11. ABC予想は足し算と掛け算の関係を述べている
12. 足し算と掛け算を分離して互いに独立なものとして扱う
13. 舞台と舞台の間の関係とは
14. 舞台と舞台の間の情報交換をどう行なうか
15. 群について（1） 定義
16. 群について（2） 巡回群
17. 群について（3） 対称群
18. 対称性通信と群
19. ICT理論がやろうとしていること
20. 文献

唐突な発表で登場したビッグニュース

2020年4月3日、京都大学は、未解明だった数学の難問「ABC予想」を証明したとする望月新一・京都大数理解析研究所教授の論文が、同研究所が編集・刊行する数学専門誌に掲載されることが決まったと発表しました。

時あたかも新型コロナウイルスの拡散が日本を含む世界中で大問題になっている最中なので、このような発表が行われたのは何か意図があったのかと疑ってしまいそうです。

望月教授はこの論文を8年前の2012年8月23日に自分のホームページに発表したのです（それは、筆者も記憶しています）が、斬新なアイデアと超難解な証明のために、証明が正しいことを検証するのに8年もかかったのだ、ということです。

ノーベル賞何個分にも匹敵する、今世紀最大の数学上の成果だと言われています。

専門が違う筆者には詳しい解説をする能力はありませんが、概要だけを理解しようとしてみました。

今回のパワーポイントの前半は参考文献の[1]を、次回は参考文献[2]を参考にしました。著者に謝意を表します。

望月新一・京都大数理解析研究所教授＝京都大提供

望月新一教授（京都大学）

望月新一教授は1969年3月東京生まれ。

5歳の時、父親の仕事の関係で渡米、16歳でプリンストン大に飛び級入学、19歳で同大大学院に進み、「数学界のノーベル賞」と言われるフィールズ賞受賞者のゲルト・ファルティングス教授に師事しました。

23歳で博士号を取得後、帰国し、京都大学数理解析研究所の助手に採用され、96年に助教授、2002年に32歳で教授に就任しました。

数論幾何学の業績は早くから認められ、45歳未満の研究者を対象に04年に創設された第1回日本学術振興会賞を受賞しました。

学術誌について

望月論文は京都大学数理解析研究所が発行する学術誌 Publications of RIMS に掲載が決定されました。

学術誌（Journal のほかに Bulletin, Memoirs, Notices, Transactions などの名称を冠す学術誌も多い）とは、学術的な研究成果を論文として発表する場であり、学会、大学や研究所などの研究機関のほかに Springer や Elsevier などの学術書専門の出版社などからも刊行されていますし、例外的なものでは O.L.クレレ個人によって1826年に創刊され現在も主要な数学の学術誌の1つとして続いている Journal für die reine und angewandte Mathematik もあります（アーベルやカントールやアイゼンシュタインらの論文も掲載されている）。

学術誌に掲載されるまでには最低1年以上の時間がかかるので、近年では、シンポジウム等で発表された論文を速報的に掲載する（ただし、査読は行われる）形式の Proceedings（会議録）とか Lecture Notes（講義録）といったものも多くなっており、Proceedings に掲載されたものを後にバージョンアップして Journal へ投稿することもありますが、そうしないケースも増えています。

レフェリー制

どの学術誌も論文の妥当性（内容が新規で正しいこと、掲載するだけの価値があること等）を審査する制度をもっています。これを査読といい、査読する人を査読者（レフェリー、referee）といいます。学術誌によっても違いますが、査読は2人あるいは3人以上のレフェリーが独立に行います。誰にレフェリーを依頼するかは学術誌の編集者（editor）や編集委員会が行います。編集委員は複数いて、投稿された論文に専門が近い人がレフェリーを選ぶことが多いです。レフェリーはほとんどの場合ボランティアです。

論文によってはそれを読んで判定をするのにかなりの日数を要す上、年に何回か（4回の場合が多いかも）しか発行されず、印刷・校正などにも時間がかかるので、掲載までに少なくとも1年以上かかってしまいます。今回の望月論文は500ページ（前段階の研究も含めると1000ページ以上）にも及ぶ大著であるだけでなくまったく新しい概念を使っているので8年という年月を要したようです。

論文の長さ、論文数

分野によって1つの論文の長さや共著者数は違い、それと関係あると思いますが、一人の研究者が書く論文の数はかなり違います。数学の場合、数ページから20・30ページくらいの論文が多く、単著のことが多いですが、短い研究報告的論文が多い分野（医学など）では共著者も多く（著者名だけで1ページ使った論文があるという笑い話もあるくらいです）、したがって、必然的に一人の研究者の論文数は多くなります。ある分野では論文数が数百篇を超える研究者も珍しくありません。

歴史上の数学者で膨大な数の、しかも後世に大きな影響力を与えた論文を書いたのはオイラー（L.Euler, 17世紀）やガウス（J.C.F.Gauß、18～19世紀）です。彼らは数学者としてだけでなく、物理学や天文学にも大きな業績を残しています。

長い論文が良いわけではなく、歴史に残るたった2ページの論文もありますし、共に19世紀初頭に生き20歳代で夭折したガロア（E.Galois、仏）やアーベル（N.H.Abel、ノルウェー）の論文数は多くはありませんが後世に与えた影響は絶大です。

ABC予想とは

1985年にオステルレ（J.Oesterlé）とマッサー（D.Masser）により提起された数論の予想。

$a+b=c$ を満たす互いに素な正の整数 a,b とその和 c に対して、それぞれの互いに異なる素因数の積を d とする。このとき、任意の実数 $\varepsilon > 0$ に対して、

$$c > d^{1+\varepsilon}$$

となるような a,b,c の組はたかだか有限個しか存在しないとする予想（「$c > d^{1+\varepsilon}$が任意の実数 $\varepsilon > 0$ に対して成り立つ」のではないことに注意）。

例えば、$a = 5,\ b = 7$ のとき、$c = 12 = 2^2 \times 3$ なので、$d = 2 \times 3 \times 5 \times 7 = 210$ であり、この場合には $c < d^{1+\varepsilon}$ が成り立っています。

上記のような a,b,c（a と b は互いに素、$c = a + b$）の組 (a,b,c) のことを**ABCトリプル**と呼び、abc の素因数分解に現れる素数（互いに相異なるもの1個ずつ）の積 d のことを abc の**根基**といい、$d = \mathrm{rad}(abc)$ と書くことにします。

弱い形のABC予想

固定されていない実数 $\varepsilon>0$ を伴う不等式 $c > d^{1+\varepsilon}$ は分かりにくいので、 ε を除いた式 $c > d = \mathrm{rad}(abc)$ が成り立つような (a,b,c) を例外的ABCトリプルと呼ぶことにした「弱い形のABC予想」について例を考えてみましょう。
例えば、$a = 1,\ b = 8 = 2^3$ のとき、$c = 9 = 3^2,\ abc = 2^3 \times 3^2$ なので、$d = \mathrm{rad}(abc) = 2 \times 3 = 6$ であり、$c > d$ であるから $(1,8,9)$ は例外的ABCトリプルです。
また、$a = 5,\ b = 27, c = 32$ も、$d = \mathrm{rad}(abc) = 30$ なので $(5,27,30)$ も例外的ABCトリプルです。
$c < 10000$ であるような (a,b,c) は約1500万通りありますが、そのうち例外的ABCトリプルは120個しかなく、$c < 100000$ の場合、約3億800万個の (a,b,c) のうち例外的ABCトリプルは276個しかありません。

M-project

望月教授の論文が学術誌に採択されたことの京大の発表

望月教授の論文は
Inter-universal Teichmüller Theory I～IV
の４篇からなり、「宇宙際タイヒミューラー理論」と彼が呼ぶ一般理論を展開したものであり、ABC予想はその帰結の1つとして成り立つことが導かれる。
宇宙際は Inter-universal の和訳であり、「際」は、国際 (inter-national)や学際 (inter-college) などと同様に、「～の間の」という意味である。
また、ここで言う universe（宇宙）は宇宙空間の宇宙ではなく、ある一般的な「数学一式」からなる世界を指している。
タイヒミューラーは20世紀前半の数学者で、彼の名を冠したタイヒミューラー理論は望月教授の理論に深く関係する。

京都大学数理解析研究所の望月新一教授による次の４つの論文

[1] Inter-universal Teichmüller Theory I: Construction of Hodge Theaters.
[2] Inter-universal Teichmüller Theory II: Hodge-Arakelov-theoretic Evaluation.
[3] Inter-universal Teichmüller Theory III: Canonical Splittings of the Log-theta-lattice.
[4] Inter-universal Teichmüller Theory IV: Log-volume Computations and Set-theoretic Foundations.

は、2020 年 2 月 5 日付で、数理解析研究所が編集しヨーロッパ数学会出版局が発行する専門学術誌 Publications of the Research Institute for Mathematical Sciences (略称 PRIMS) にアクセプトされましたのでお知らせいたします.

論文の概要
本論文は、数学の数論（整数論）の分野において、「宇宙際タイヒミューラー理論」を展開し、その一つの帰結として「ABC 予想」とよばれる命題を証明したものです. 整数では足し算と掛け算ができますが、ABC 予想はその二つの演算の絡み合い方に関する命題で、1980 年代にヨーロッパの数学者たちによって提起されました. ABC 予想の成立を仮定すると他の数多くの未解決予想の証明が得られることから、数論における重要かつ困難な未解決問題として残されていました.

論文審査について
本論文の著者の望月新一教授は PRIMS の編集委員長でもあるため、本論文については、柏原正樹（数理解析研究所特任教授）および玉川安騎男（数理解析研究所教授）を共同編集委員長として、望月新一教授を完全に除外した特別編集委員会を構成し採否の審査を行いました.

PRIMS 特別編集委員会

フェルマーの最終定理とABC予想

ABC予想の凄さは、effectiveモーデル予想、シュビロ予想、フライ予想、双曲的代数曲線に関するヴォイタ予想などが自動的に導かれ、フェルマーの最終定理も簡単に証明できることからもわかります。

ファルマーの最終定理とは、

$n \geqq 3$ のとき、$x^n + y^n = z^n$ となる自然数の組 (x, y, z) は存在しない

という定理で、17世紀のフランスの数学者フェルマー（Pierre de Fermat）が古代ギリシアの数学者ディオファントスの著作『算術』を読んでいたとき、本文中の記述に関連した着想を余白への書き込んだものと言われており、フェルマーの死後360年経った1995年に英国の数学者ワイルズ（A. J. Wiles）によって完全に証明されました。

ABC予想を使ってフェルマーの最終定理を証明する

背理法による。

$n \geqq 3$ とし、$x^n + y^n = z^n$ となる自然数の組 (x, y, z) が存在したとする。x, y, z は互いに素であるとしてよい（そうでなかったら、共通因数で割ったものを考えればよい）。このとき、(x^n, y^n, z^n) はABCトリプルになるので、ABC予想（ε=1とした場合）により $z^n < \mathrm{rad}(x^n y^n z^n)^2$ が成り立つ。

根基の定義より、$\mathrm{rad}(x^n y^n z^n)^2 = \mathrm{rad}(xyz)^2$であり、$x, y < z$ だから $\mathrm{rad}(xyz)^2 \leqq (xyz)^2 < (z^3)^2 = z^6$ となり、したがって、$z^n < z^6$ が成り立つ。これは $n < 6$ であることを示しているが、$n \geqq 3$ という仮定から $n = 3, 4, 5$ の可能性しかない。しかし、これらの場合にはフェルマーの最終定理が成り立つことは昔から分かっていたので、矛盾が導かれた。

ABC予想は足し算と掛け算の関係を述べている

整数論の難しさや深さは、「足し算と掛け算の関係」に由来すると考えられています。足し算と掛け算の関係は難しくて、まだ完全には理解できていません。例えば、素数の分布に関するリーマン予想（リーマンのゼータ関数 $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$ の零点は、負の偶数と、実部が 1/2 の複素数に限られるという予想。リーマン予想は素数の分布についての予想を含んでいる）、双子素数予想（双子素数とは、差が 2 である２つの素数の組のことであり、双子素数は無限に存在するかという予想）、ゴールドバッハ予想（３より大きいどんな偶数も２つの素数の和として表すことができるという予想）などはいずれも素数が絡んでいますが、素数は足し算と掛け算の関係が絡んでいます（例えば、すべての整数は素数の積である一方、素数の和である場合もあります（ゴールドバッハ予想））。

一方、ABC予想では、c は a と b の和 $(c=a+b)$ であり、d は a と b と c の互いに異なる素因数の積であり、$c>d^{1+\varepsilon}$ は足し算としての側面を表す c と掛け算としての側面を表す d の間の関係を述べた初めての例です。

足し算と掛け算を分離して互いに独立なものとして扱う

「1つの数学という宇宙だけでなく、複数の数学（宇宙）がある世界を考える」

宇宙際（Inter-universal）の宇宙とは、そのような数学の宇宙のことです。望月教授の IUT理論（*Inter-universal Teichmüller Theory*）は、従来からある「数学」という学問の統一体（多数の対象や分野や概念の集合体）である「宇宙」を1つだけでなく複数考え、それらの間の関係について論じる理論であり、これまでの数学の歴史にはなかった斬新な考え方を提案する理論です。このように、宇宙とはある数学を展開する舞台ですから、今後、「宇宙」と「舞台」を同義語として使います。。

整数の世界において足し算と掛け算という切り離すことができない構造（それを「正則構造」と呼ぶことにします）をタイヒミューラー理論との類似性（アナロジー）で 捉えようとするものです。このような正則構造を上手く破壊して、いくつもの異なる正則構造に変形する理論がタイヒミューラー理論ですが、その理論と類似する変形を施して「足し算と掛け算」という正則構造を破壊（すなわち、分離）して考えようというものです。

舞台と舞台の間の関係とは

例えば、足し算を固定しておいて、掛け算だけをタイヒミューラー的に変形する（伸び縮みさせる）ことを考えます。したがって、本来は足し算と掛け算は切っても切れない関係にあるのに、これを別々に扱うのです。

舞台１における掛け算というピース（断片）を変形（伸び縮み）させて舞台２における掛け算にリンク（関連付け）させよう（等しいとみなそう）というわけです。これを式で

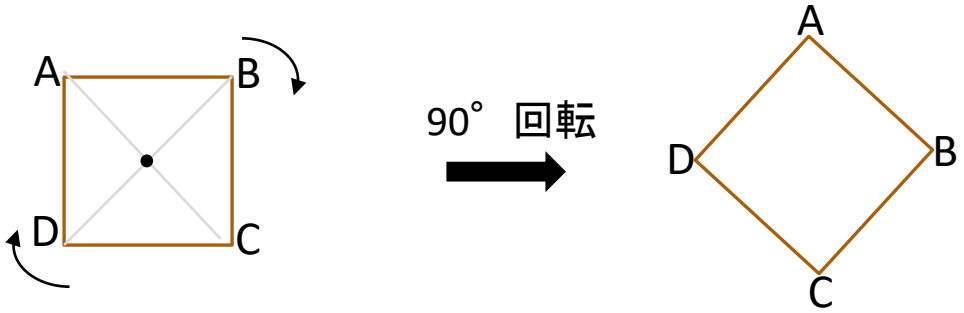
$$\deg \Theta \text{ “}=\text{“ } \deg q$$

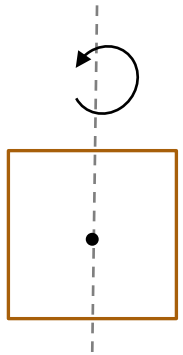
と書いて表すことにします。Θ と q はそれぞれの舞台に属している“同じもの”（例えば、掛け算）がサイズや形を変えたものです。deg は多分 degree（程度）の略記でしょう。

例えば、舞台２における足し算に合うように舞台１における掛け算 q を変形したものが Θ であるとき、この変形において「ひずみ」が起こるかもしれません。IUT 理論では、このひずみの大きさが計測でき、上記の ” = “ は次のような不等式で表すことができます：$\deg \Theta \leqq \deg q + c$

舞台と舞台の間の情報交換をどう行なうか

IUT 理論では、舞台と舞台の間の情報交換の方法として「対称性」を使うのだそうです。例えば、正方形は重心を中心にして回転させても回転の前後で図形として区別できません。



また、  を点線を軸にして3次元的に180度回転させても同じ図形になります。

これを鏡映と言います。 この回転対称性と鏡映対称性は本質的に異なるものです（なぜかを考えてみて下さい頂点に番号を付けて回転前と回転後の数字の並びを比べてください）。

対象 X が操作 s によって変わらないとき、X は操作 s に関して対称であると言います。

群について（1）定義

文献[1]では、このあと、群 (group) の話が登場します。群の基本については第19回講座

『和ってなに？積ってなに？ いろんな和と積：どこが同じで、どこが違う』 を参照してください。

説明なしに数学的定義だけを述べると、群とはある集合 G と、G の上で定義された2項演算 ・ によって定義された $(G, \cdot)$ （・が分かっているときは単に G と書く）で、次の性質が成り立っているものです：

(1) G は演算・で閉じている。すなわち、任意の $a, b \in G$ に対して $a \cdot b \in G$ である。

(2) 演算・は結合律を満たす。すなわち、任意の $a, b, c \in G$ に対して $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ が成り立つ。

(3) G には単位元 e が存在する。すなわち、任意の $a \in G$ に対して $a \cdot e = a = e \cdot a$ が成り立っている。

(4) Gの任意の元 a に対して $a \cdot a^{-1} = e = a^{-1} \cdot a$ が成り立つような逆元 $a^{-1} \in G$ が存在する。

特に、任意の $a, b \in G$ に対して $a \cdot b = b \cdot a$ が成り立っているとき、G は可換であるとかアーベル群であるという。

群について（2）巡回群

群の中でも、たった1個の元（それを a としましょう）に演算・を施すことによって G の元すべてが得られるとき、G を**巡回群** (cyclic group) といいます：$\mathbb{N}$

n個のa

$G = \{ a^n \mid n \in \mathbb{N} \}$ （a^n は $\overbrace{a \cdot a \cdot \cdots \cdot a}$ のことです）　このとき、$G =< a >$ と書きます。

例えば、・が足し算のとき、整数の集合 $\mathbb{Z}$ は 0 を単位元として $\mathbb{Z} =< 1 >$ です。なぜなら、1 を n 個足すと正の整数 n が得られ、1 の逆元は -1 $(1 + (-1) = 0)$ ですから、-1 を n 回足せば $-n$ が得られ、すべての整数は 1 を何個か足すことによって得られます。

元が2個の群はすべて巡回群です。なぜなら、1 を単位元として $G = \{1, a\}$ とするとき、G が群になるためには、・は右下の表に示したような関係が成り立たなければならないからです。

・	1	a
1	1	a
a	a	1

例えば、ある人が「何もしない」「右を向く」「左を向く」「後ろを向く」ことをそれぞれ e, r, l, b で表すと、例えば $r \cdot b \cdot l = r \cdot r = b$ という関係が成り立ち、$Z_4 = \{e, r, l, b\}$ は ・ の下で巡回群になります：$Z_4 =< r >$.

群について（3）対称群

もう一つ、特殊な群として対称群というものがあります。「番号づけられて並んでいるものを並べ替える」操作のことを**置換**（permutation）といい、置換という操作を元とする群を**対称群**（symmetric group）といいます。もう少し数学的に言うと、集合 $I_n = \{1, 2, \dots, n\}$ に対し、I_n から I_n への全単射全体の集合は写像の合成を積として群になりますが、これを **n次の対称群**といい、S_n 等の記号で表します。S_n の元の個数は $n!$ です。

位数（集合の元の個数のこと）が n の集合 X の元の並び $(x_1, \dots, x_n)$ を $(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$ に移すよう写像 σ のことを **n 次の置換**といい

$$\sigma = \begin{pmatrix} x_1 & \dots & x_n \\ \sigma(x_1) & \dots & \sigma(x_n) \end{pmatrix} \qquad \text{あるいは} \qquad \sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$$

で表します。

例えば、前出の 正方形の回転（90度の回転 σ と鏡映 τ）の全体は位数8の群 $D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \sigma^3\}$ であり、頂点 A, B, C, D の置換全体からなる群は位数24の4次の対称群 S_4 になります。

Z_4 は可換（アーベル群）ですが、D_4 は可換ではありません。

対称性通信と群

遠アーベル幾何学という分野では、数論幾何学とか代数幾何学に現れる対象（スキームとか多様体と呼ばれるもの）を、その対称性だけから復元するということが行なわれており、復元が正確にできるためには、その対称性の群が十分に豊かで複雑であること（したがって、非可換である方がよいので、このことを**遠アーベル的**というのだそうです）が要求されるのだそうです。

例えば、同じ4個のものを置換する方法の種類を考えたとき、Z_4 よりは D_4 の方がより複雑で、D_4 よりは S_4 の方が複雑です（例えば、$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ は D_4 のどの元とも違うものであり、それは正方形の90度回転や鏡映だけでは表すことができない置換であるということです）。

IUT 理論においても、舞台と舞台の間の通信（情報交換）の方法として「対称性」を使うのだそうです。

しかし、対称性を満たす通信を使っても精度の高い情報交換ができるとは限らないのですが、IUT理論ではその精度を定量的に計測することができる、ということがミソであるということです。通信に対称性の群を使うだけでなく、その通信をより精確にために受信して復元するという段階において遠アーベル幾何学が用いられるのだそうです。つまり、可換から十分遠い群を使うことによって復元によって得られる情報が多くなって、復元がより精確になるというわけです。

ICT理論がやろうとしていること

文献[1]はここ（第7章）までが全体の90%で、残りの部分（第8章）でIUT理論の本質を前出の不等式 $\deg \Theta$ “＝“ $\deg q$ を不等式 $\deg \Theta \leqq \deg q + c$, さらには $N\log(q) \leqq \log(q) + c$ を出して説明しようとしていますが、あまりにも”お話し”過ぎて、数学を多少なりとも理解する者には少しも理解した気にならならないので、今回はここでやめておきます。

次回以降は文献[2]に基づいて述べますが、[1]とは逆に、こちらは大学の数学科程度の知識が必要になるという、専門的すぎる極端さです。

[1][2]の2冊とも Kindle で読んだのですが、数学書は Kindle で読むべきではないと知りました。1画面の内容が少ないし、数式がきれいに表示されません。

参考文献

[1] 加藤文元、『宇宙と宇宙をつなぐ数学　IUT理論の衝撃』、角川学芸出版、2019年

[2] 黒川信重・小山信也、『ABC予想入門』、PHPサイエンス・ワールド新書、2013年

[1]は一般読者向けの概念的・思想的な（数式は現れない）説明がメインで、数学の知識がある人は物足りなさを覚えるであろう。数学者のものの考え方、重要とされる未解決問題とはどういうものか等も述べた「読み物」である。勿論、ABC問題の“概要”の説明はあるが、残念ながらあまりにも概略すぎる。

[2]も冒頭で未解決問題についてかなりのページを費やして説明している。内容は[1]に比べかなり本格的で、大学の数学科の卒業生でないと理解できないであろう。