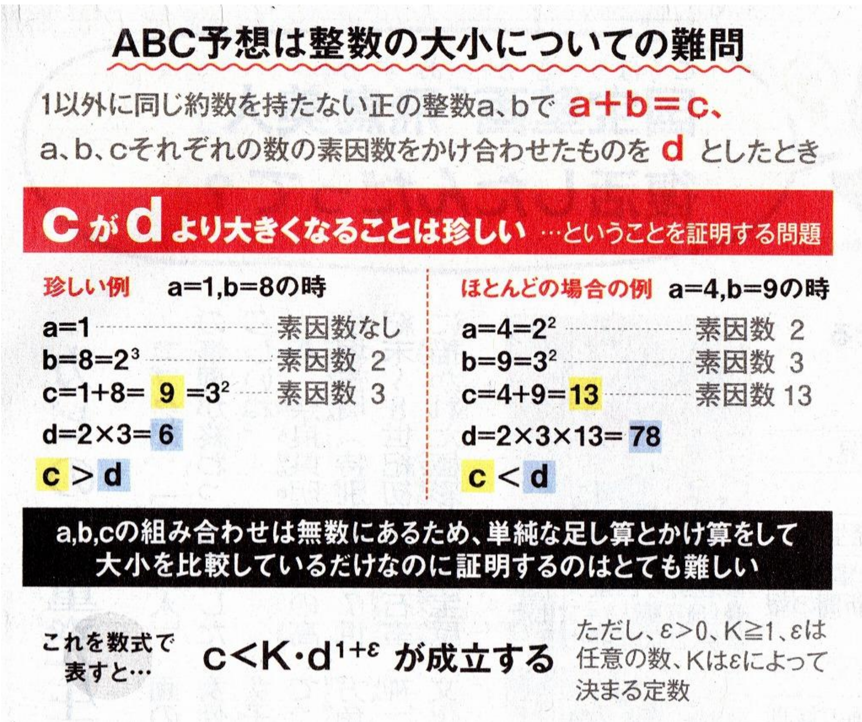
８６「ＡＢＣ予想について」

ここに記す内容は、加藤文元氏の著書「宇宙と宇宙をつなぐ数学（ITU 理論の衝撃）」及びネット上の動画「ＡＢＣ予想と新しい数学」を引用して作成したものです。

２０２０年４月４日朝日新聞記事



ＡＢＣ予想は次のように示される。

ＡＢＣ予想
$a+b=c$ を満たす、互いに素な自然数の組 $(a,\ b,\ c)$ に対し、$d=rad(abc)$ とする。 このとき、任意の正の実数 $\varepsilon>0$ に対して、$c>d^{1+\varepsilon}$ となる組 $(a,\ b,\ c)$ は、高々有限個しか存在しないであろう。（上記新聞記事のような $c<Kd^{1+\varepsilon}$ という表現もある）

ＡＢＣ予想は、京都大学望月教授が発表した**「宇宙際タイヒミュラー理論」**が打ち立てられたその成果の一つとして証明された。

「宇宙際タイヒミュラー理論」は、天動説に対する地動説，ニュートン物理学に対する相対性理論や量子力学のように、これまでの常識を全く覆してしまうような理論である。

ＡＢＣ予想が証明されれば、現代数学の景色が一変するといわれており、整数論などの数学分野に及ぼす影響は計り知れない。整数論における「モーデル予想」「シュピロ予想」「フライ予想」「ヴォイタ予想」（内容省略）そして「フェルマー予想」が自動的に証明される。

「宇宙際タイヒミュラー理論」は“自然数”と呼ばれる“普通の数”１，２，３・・・・の足し算と掛け算からなる「環」と呼ばれる数学的な対象に対して、その「足し算」と「掛け算」という２つの演算を分離し、その性質を再構成[復元]するという発想転換した斬新な理論である。

（「環」とはたし算とかけ算の２種類の演算を備えた数の集合で、「整数全体の集合」（整数環という）はその代表的なもので、整数環内ではたし算とかけ算が自由にでき計算結果が必ずその内部に存在する）

まず、ＡＢＣ予想について述べる。

素数とは、約数が１と自分自身のみである数。素因数分解とは、正の整数を素数の積の形で表すことをいう。

例えば、24 は $24 = 4 \times 6 = (2 \times 2) \times (2 \times 3) = 2^3 \times 3^1$ と素因数分解される。

ある自然数 n を素因数分解し、そこに現れる「べき指数」（24 の場合であれば $2^3 \times 3^1$ における右肩の数「3」と「1」）をすべて 1 にしたものを n の根基（radical）と呼び、$\mathrm{rad}(n)$ と書く。$n = 24$ の場合は $2^1 \times 3^1 = 6$ が根基となり、$\mathrm{rad}(24) = 6$ である。つまり、素因数分解に現れる素数を、それぞれ１回だけ掛けて得られる数を考えるということで、n の根基とは、n の素因数分解に現れる異なった素数の積ということになる。

従って 6，12，18，24‥‥など 6 の倍数では、素因数分解した時の素数が 2 と 3 しか現れないので、$6 = \mathrm{rad}(6) = \mathrm{rad}(12) = \mathrm{rad}(18) = \mathrm{rad}(24) = \mathrm{rad}(36) = \mathrm{rad}(48) = \mathrm{rad}(72)$ となる。

以上を踏まえ、ＡＢＣ予想は「ＡＢＣトリプル」と呼ばれる自然数３つの組 $(a,\ b,\ c)$ についての予想である。

まず、２つの互いに素な自然数 $(a,\ b)$ を考える。$a,\ b$ は互いに素であるから、共通の素数はない。例えば、$(10,\ 21)$ とすると、$10 = 2 \times 5$，$21 = 3 \times 7$ なので、互いに共通の素数はなく、10，21 は互いに素であり条件に合致する。ここで $a,\ b$ を加えたものを $c\ (= a + b)$ として、このようにして得られた３つの自然数の組 $(\mathrm{a},\ \mathrm{b},\ \mathrm{c})$ をＡＢＣトリプルと呼ぶ。

次に、このＡＢＣトリプルについて、その３つの数の積 $a \times b \times c$ を考え、その根基を d とする。つまり、$d = rad(abc)$ である。d は言い換えれば、abc の素因数分解に現れる素数の積である。この２つの自然数 c と d の大小を比較するとき、多くの場合 $c < d$ となるが、例外的に $c > d$ となることがある。

例１

> $a = 5$，$b = 7$ のとき。$c = a + b = 5 + 7 = 12$ より、$abc = 5 \cdot 7 \cdot 12 = 2^3 \cdot 3 \cdot 5 \cdot 7$ となるので、$d = rad(abc) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ 、ここで $c = 12$，$d = 210$ だから $c < d$ となる。

例２

> $a = 11$，$b = 25$ のとき。$c = a + b = 11 + 25 = 36$ より、$abc = 11 \cdot 25 \cdot 36 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 11$ となるので、$d = rad(abc) = 2 \cdot 3 \cdot 5 \cdot 11 = 330$ 、ここで $c = 36$，$d = 330$ だから $c < d$ となる。

例３

> $a = 5$，$b = 27$ のとき。$c = a + b = 5 + 27 = 32$ より、$abc = 5 \cdot 27 \cdot 32 = 2^5 \cdot 3^3 \cdot 5$ となるので、$d = rad(abc) = 2 \cdot 3 \cdot 5 = 30$ 、ここで $c = 32$，$d = 30$ だから $c > d$ となる。

ＡＢＣトリプルについて $c,\ d$ を計算すると、例１，２のように多くの場合 $c < d$ となるが、例外的に例３のように $c > d$ となることがある。

ＡＢＣ予想は「d が c より小さいという例外的なＡＢＣトリプルはとても少ない」ということを予想したものである。少ないと言っても、例外的なＡＢＣトリプルは実際に存在しているのだから $c > d$ という不等式がすべてのＡＢＣトリプルに対して成り立つわけではない。

しかし、d の方を d^2 や d^3 というようにどんどん累乗していき、充分に大きな k をとれば、どんなＡＢ

Ｃトリプルについても、必ず$c < d^k$成り立つようにできる。

例えば大胆に$k = 2$ ($k = 1 + \varepsilon$なので$\varepsilon = 1$) としたものを“強いＡＢＣ予想”（確実に成り立つ）と呼んでいるが、これが正しければフェルマー予想は次のように簡単に証明される。

フェルマー予想とは、表現のしかたはいくつかあるが、要するに
『自然数$n \geqq 3$に対して、$x^n + y^n = z^n$ を満たす自然数 $x,\ y,\ z$ は存在しない』
というものである。以下、ＡＢＣ予想に基づくフェルマー予想の証明を示す。

フェルマー予想の証明

nを 3 以上の自然数として、$x^n + y^n = z^n$を満たす自然数の組$(x,\ y,\ z)$が存在したと仮定する。このとき$(x^n,\ y^n,\ z^n)$は（$x,\ y$はそれぞれ素数と考えてよいので）ＡＢＣトリプルとなる。

よって、$z^n < rad(x^n y^n z^n)^2$であるが、根基の定義から$rad(x^n y^n z^n)^2 = rad(xyz)^2$であり、$x,\ y < z$だから、$rad(xyz)^2 \leq (xyz)^2 < (z^3)^2 = z^6$となる。よって、$z^n < z^6$である。これは自然数$n$が 6 より小さいことを示しているが、$n$は 3 以上だったので、$n$の可能性は 3，4，5 しかないことになる。

$n = 3$，4，5 の場合は、すでに成り立たないことが個別に証明されているので「$x^n + y^n = z^n$を満たす自然数の組$(x,\ y,\ z)$が存在する」とした仮定が誤りである。以上より、フェルマー予想が証明された。

この場合は、$k = 2$として“強いＡＢＣ予想”で証明したが、これは$c > d^{1+\varepsilon}$という条件において、$\varepsilon = 1$の場合に該当し、真のεは 1 よりさらに小さいところにあるはずである。

例えば、$\varepsilon = 0.5$とすれば、$rad(xyz)^{1.5} \leq (xyz)^{1.5} < (z^3)^{1.5} = z^{4.5}$であり、$z^n < z^{4.5}$から$n$の可能性は 3，4 しかないことになり、5 が除外されるだけで、ＡＢＣ予想に基づくフェルマー予想の証明に本質的な差が出ることはない。(だから、ＡＢＣ予想が確実に成り立つ$\varepsilon = 1$の場合で証明しておけば反論の余地はない)

フェルマー予想は１７世紀に提起され、２０世紀の末に証明されるまで３６０年もかかった超難問である。ＡＢＣ予想を使えば、考えるべきnをごく限られたものに絞ることができ、超難問がわずか数行で証明できてしまうほどであるから、現代数学が一変するというのも頷ける。

表１は、３０という数から出発して、１ずつたしていったときの、素因数分解の様子を示している。これを見ると、例えば、素数である３１のところでは、素因数分解は３１になるが、その次の３２は突然２^5という高い「べき」が現れる。その後も１１や１７のような素数が現れたかと思えば、３６になると、また小さい素因数しか現れないようになったりと、不規則で変化に富んでいるのがわかる。

数	素因数分解
30	$2 \cdot 3 \cdot 5$
31	31
32	2^5
33	$3 \cdot 11$
34	$2 \cdot 17$
35	$5 \cdot 7$
36	$2^2 \cdot 3^2$

表１

このように、素因数の現れ方がいかに「気まぐれ」に見えるかがよくわかるだろう。ＡＢＣトリプルをいろいろと動かすと、dの素因数分解の中にときおり唐突に大きな素数が現れたり、逆にとても小さな素数しか現れなかったりす

ることがあり、その現れ方のパターンはとても気まぐれに見えるが、唐突に大きな素数が現れる場合は、そのＡＢＣトリプルは例外的にはなりにくくなる。実際、その場合には d が大きくなる傾向にあるからである。逆に、ＡＢＣの素因数がどれも小さいものばかりだと、d が小さくなる傾向にあるので、そのＡＢＣトリプルは例外的になりやすくなる。

したがって、素因数分解の中に現れる素数の種類や大きさは、ＡＢＣトリプルが例外的になるか否かに、非常にデリケートに関わってくる重大なことであることがわかる。ＡＢＣ予想においては、数の「たし算的側面」である c と、「かけ算的側面」である d を比べるということがテーマとなっている。

このかけ算的な側面とたし算的な側面が、まさに混ざっているということが、この予想の難しさの原点である。したがって、ＡＢＣ予想を解くためには、数の「たし算とかけ算の関係」という核心の部分にメスを入れなければならない。「宇宙際タイヒミュラー理論」は、まさにこの根本的な問題に挑戦する理論である。

「宇宙際タイヒミュラー理論」（以下、ＩＵＴ理論という）について

ＩＴＵ理論は、たし算とかけ算を分離して、互いに独立のものとして別々に扱うことを考える。例えば、たし算とかけ算の一方をそのままにして、他方を少し変形する、あるいは伸び縮みさせるというようなことを考える。

従来の数学では、たし算とかけ算は１つのパッケージの中で互いに分かち難く結びつき、複雑に絡まり合っている。よって、それを安直に分離しようとすると、たちまち矛盾が起こってしまう。

そこで、そのような矛盾が起こるのを回避するために、一つの数学ではなく「複数の数学の舞台」で考える。（この「舞台」を「宇宙」と呼ぶことにしたことから、宇宙際･･･という言葉が出てきた）

幾何学図形における「タテとヨコ」や複素平面における「長さと角度」など、２つをそれぞれ独立に扱うことのできない要素（次元）をもつ対象を「正則構造」と呼ぶものとする。

「タイヒミュラー理論」とは、このような正則構造を敢えて破壊することで、図形の変形を積極的に行う理論である。（本来のタイヒミュラー理論は、複素構造という正則構造を破壊する変形を施すものだが、内容が複雑なので省略する）

変形された図形は、また新しい正則構造を持つが、最初の図形とは少し異なっていて、その違いが正則構造の違いにより定量化される。図形の違いが定量化できれば、それらがどのくらい似ていて、どのくらい異なつているのかを、数学的に定量的に論じることができる。

例えば、長方形のタテを固定してヨコを伸び縮みさせれば、タテとヨコの比率が異なつた長方形ができるが、“比率”によりそれらの２つの長方形の形の違いを定量化できる。

ＩＴＵ理論は「たし算」と「かけ算」という、通常分けることのできない２つの要素（次元）を持つ正則構造を、タイヒミュラー理論の考え方を利用して変形し、それぞれ独立した舞台（宇宙）で論じ、それぞれの舞台（複数の宇宙）での違いを定量化するものであり、宇宙祭タイヒミュラー理論の名はこれに由来する。

図１はＩＵＴ的なジグソーパズルを示す。

ＩＵＴ的な数学とは、普通の数学ではぴったりはめることができない大きさの違うピースを互いにはめようと試みる。

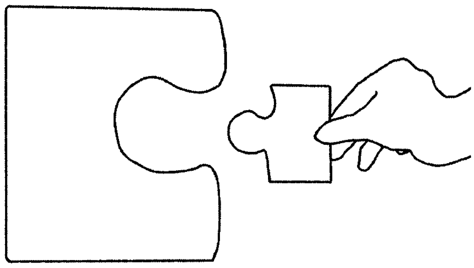


図１　ＩＵＴ的なジグソーパズル

同一平面上ではぴったりはまらないピースも、右側の小さい方のピースを手前側に近づければ（別の舞台に移せば）、正面からはぴったりはまったように見せることができる。ＩＵＴ理論は、異なる舞台の間の２つの量に次のような《等式》を考える。

$deg\boldsymbol{\Theta}$ “＝” $deg\,\boldsymbol{q}$ ---------------①

ここで、$\boldsymbol{\Theta}$ と $\boldsymbol{q}$ はそれぞれ違う舞台に属している《同じ》ものに由来し、それぞれの舞台の「かけ算」の構造によるものである。これらの間の等式を形式的に考えることで、「かけ算」が伸び縮みしている状況を表現する。

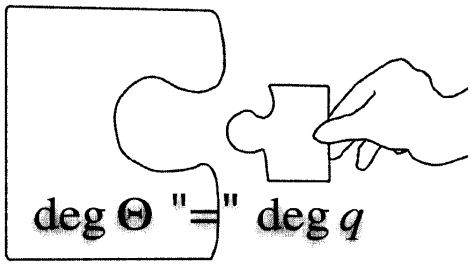


図２ 異なるサイズのピースをはめる

図２のように、それぞれ違う舞台に属しているものを《あてはまる》ものとして元に戻すと、何らかの不整合（ひずみ）が起こる。正面から見ればぴったりはまったように見えても、横から見ればそうではないということが起こる。

そこでＩＵＴ理論は、異なる舞台間の情報交換を行うことによって起こる“ひずみ”について、その大きさを計測することにより、 ①式は $deg\boldsymbol{\Theta} \leq deg\,\boldsymbol{q} + c$ ---------------②

のように表現することが可能になる。

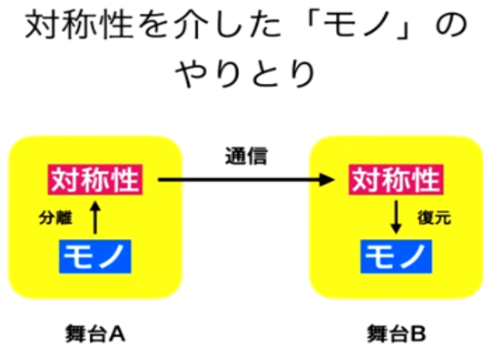


図３ 対称性通信

異なる舞台間の情報交換のために用いるのは「対称性」である。図３に示すように舞台Ａのモノから、対称性という属性を分離し、それを舞台Ｂに通信で伝え舞台Ｂでそれをモノに復元する。具体的には図４のような場合が考えられる。

ところが“１２０°回転を３回行う”といった単純な対称性の情報だけでは正確なカタチは再現できない場合があり、図５のように復元が違ってしまう場合がありうる。

図４ 対称性通信の具体例

したがって、より複雑な図形，より多くの情報があればさらに正確な復元が可能になるといえる。

ＩＵＴ理論では、より正確な復元を可能にするために「群論」（内容説明は省略）を用いて、対称性に関連した対象の「運動」や「操作」の概念を定量的に通信する。通信の結果としての「復元」が、どのくらい精密に行えるかは、通信によって伝達される対称性の複雑さによって決められる。

回転対称性だけでなく、鏡像対称性，並進対称性というように対称性の種類を増やしていけば通信の正確さを増すことが可能になる。

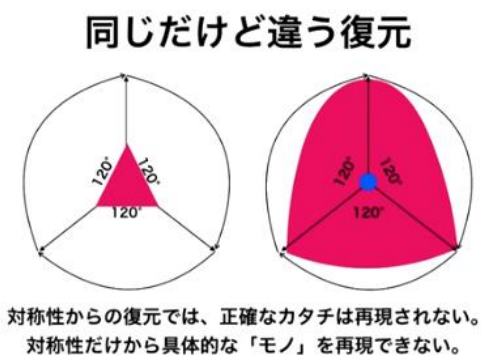


図５ 復元が違ってしまう例

モノに付随している属性はモノそのものではない。だからそれはモノが越えられない障壁を越えることができる。

対称性のもつ有用な特徴をうまく使いながら、異なった舞台の間での通信が可能になるのである。

対称性だけを頼りに図形を復元する幾何学を「遠アーベル幾

何学」と呼ぶ。(アーベルはノルウェーの数学者) これは"アーベル"が可換、つまり単純であることを意味していることから"遠アーベル"とは単純から遠く離れている、つまり充分複雑であることを示している。整理すると、

ＩＵＴ理論
❖たし算とかけ算の絡み合う正則構造を打破するため、複数の数学舞台を設定する
❖複数の舞台間の関係を構築するために「対称性通信」をする(伝達)
❖対称性通信で障壁を超え「遠アーベル幾何学」を応用して対象を復元する(復元)
❖通信のひずみを定量的に計測する(計測)

前出②式 $deg\boldsymbol{\Theta} \leq deg\,\boldsymbol{q} + c$ の証明を行う。(以下の説明だけでは理解しにくいと思われるが、、、)
ここで、$\boldsymbol{\Theta}$ はテータ関数(後述)、$deg\boldsymbol{\Theta}$ はテータ関数の次数と考えておけばよい。

この中の $\boldsymbol{q}$ という量が一律に小さいということを証明するため、$\boldsymbol{q}$ をある種の不等式で抑えることを考える。$\boldsymbol{q}$ が充分小さければ、自然数をＮとしたとき、$\boldsymbol{q^N}$ も小さいと考えられる。
この $\boldsymbol{q^N}$ が $\boldsymbol{q}$ とほぼ等しいという式が導ければよい。舞台Ａにおける $\boldsymbol{q}$ のコピーを $\boldsymbol{q_A}$，舞台Ｂにおける $\boldsymbol{q}$ のコピーを $\boldsymbol{q_B}$ とする。この状態で舞台Ａと舞台Ｂの間で対称性通信をしながら、一斉に同じ計算を行う。計算の手順の一つ一つを、連絡を取り合いながら実行していくので、その結果も同じになるものと期待できる。そうすることで、舞台Ａにおける $\boldsymbol{q_A}$のＮ乗と、舞台Ｂにおける $\boldsymbol{q_B}$ のＮ乗はほぼ等しいという結論を得ることができるはずである。

つまり、２つの舞台間で形式的に、$\boldsymbol{q_B^N} \cong \boldsymbol{q_A}$ (≅はそれぞれ対応しているという意味) という関係を取り決めておき、図２に示すように、異なるサイズのピースの片方を見かけ上変更して式的にはめ込む。

その状況のもとで、互いに通信しあいながら計算を行い $\boldsymbol{q_B^N} \fallingdotseq \boldsymbol{q_A^N}$ という結果を得る。そうすることにより、舞台Ａの人にとっては、この２つの式を併せて考えれば、$\boldsymbol{q_A^N}$ と$\boldsymbol{q_A}$ は「ほぼ等しい」という望みどおりの結果を得ることができる。

このように、形式的にピースはめて関係づけることを「テータリンク」と呼ぶ。

相互の通信において、お互いの計算を同期させるために重要な通信内容は、$\boldsymbol{q}$ のＮ乗という量を計算する仕方である。これをそのまま伝えようとしても、そのままでは不定性が大きくなり意味のある通信ができない。その理由は「 $\boldsymbol{q^N}$ 」という値だけだと、その対称性があまり豊かではないためである。

そのためにＩＵＴ理論では「 $\boldsymbol{q^N}$ 」を、そのまま数として通信するのではなく、「テータ関数」と呼ばれる、非常に豊かな対称性と結びついた関数の特殊値と解釈することで、不定性を少なくするよう考える。このテータ関数と結びついた対称性とは、点付きの「楕円曲線」という、遠アーベル幾何学の対象である双曲的代数曲線の幾何学 (多項式で定義される曲面を扱う幾何学の１つ) と関連付けられるため、まさに遠アーベル幾何学の手法を用いて復元されるのである。このようにして復元されたテータ関数の特殊値をとることで、望み通り「 $\boldsymbol{q^N}$ 」の計算に必要なデータを受け取ることができる。

それでもなお残る不定性について、その「ひずみ」を定量的に計測して数式で示すことを可能にするのがこのＩＵＴ理論の優れたところである。

通信の結果得られた $\boldsymbol{q_A^N}$ と$\boldsymbol{q_A}$ は「ほぼ等しい」、つまり $\boldsymbol{q_A^N} \fallingdotseq \boldsymbol{q_A}$ と数式で表現する時、≒は軽微だが不定性があることを示し、これから $\boldsymbol{q_A^N} < \boldsymbol{q_A} + \boldsymbol{c}$ という不等式が得られる。

これは目指す②式 $deg\boldsymbol{\Theta} \le deg\,\boldsymbol{q} + c$ と一致する。左辺の $\boldsymbol{\Theta}$（テータ）は、テータ関数の値の集まりを表す記号である。舞台Ａの $\boldsymbol{q_A}$ は舞台Ｂに通信されると $\boldsymbol{\Theta}$ になり、これが舞台Ｂでは $\boldsymbol{q_B^N}$ に対応するものだということになる。よって、$deg\,\boldsymbol{q}$ は小さいという結論が得られる。

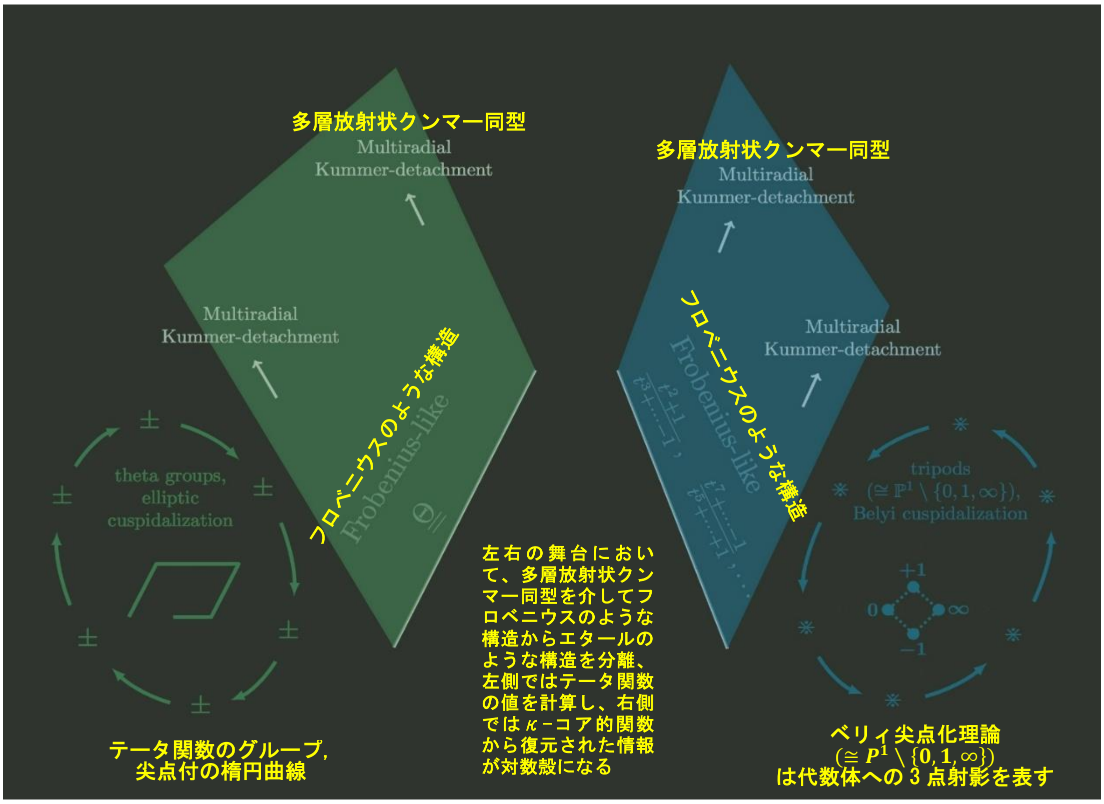
これだけでは、ＡＢＣ予想の証明にはまだ不充分であり、実際にはこれまでの計算と「数体の復元」と呼ばれる、もう一つの類似の計算について考えなければならない。さらにそれらの計算を無限個一斉に行わなければならないのである。

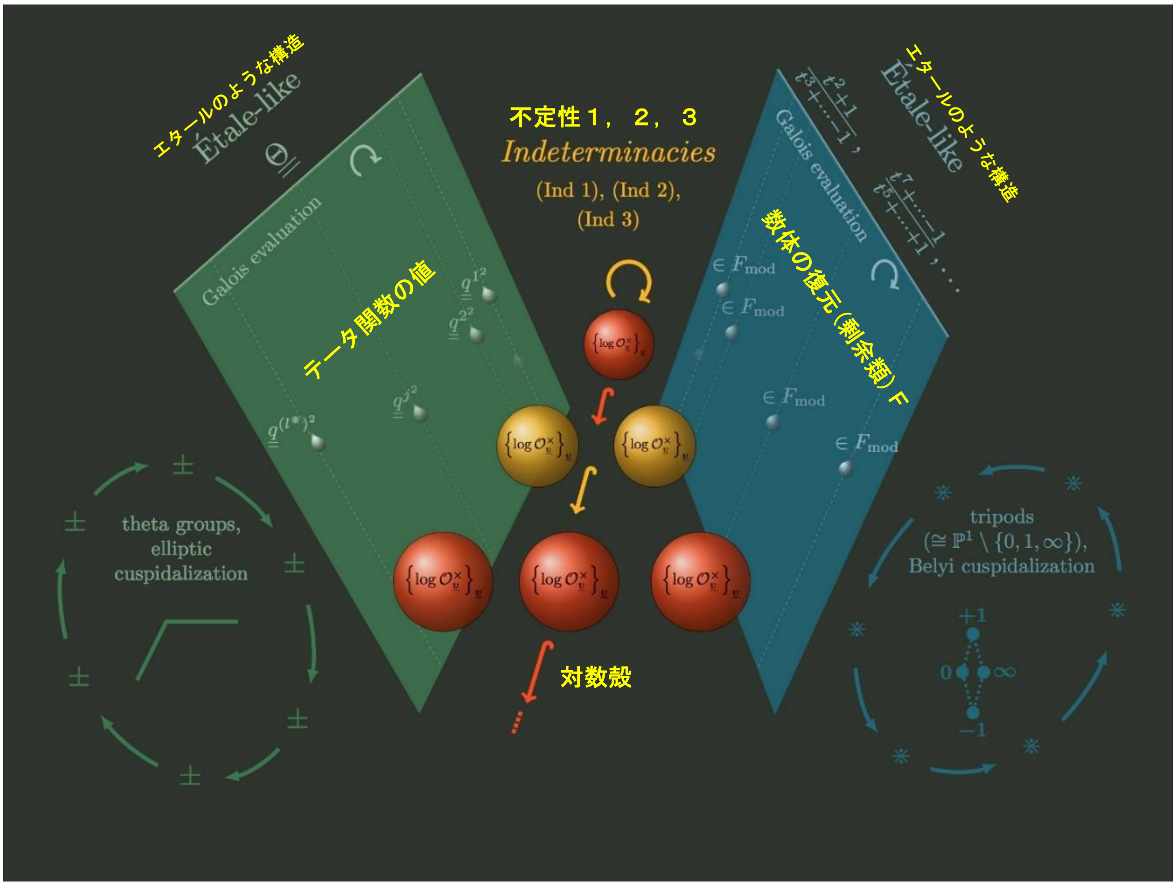
「$\boldsymbol{q^N}$」の計算に必要なデータとして、テータ関数の特殊値を復元する必要があるが、そのデータは「局所的」なデータである。全体を解明するためには、これらデータを集め統合することによって「大域的」なデータとしなければならない。ここで数学的な「局所」と「大域」という概念が必要となるが、その詳細は省略する。端的にいえば局所（部分）で成立するものを、無限個束ねることによって大域（全体）で成立するようにすることである。

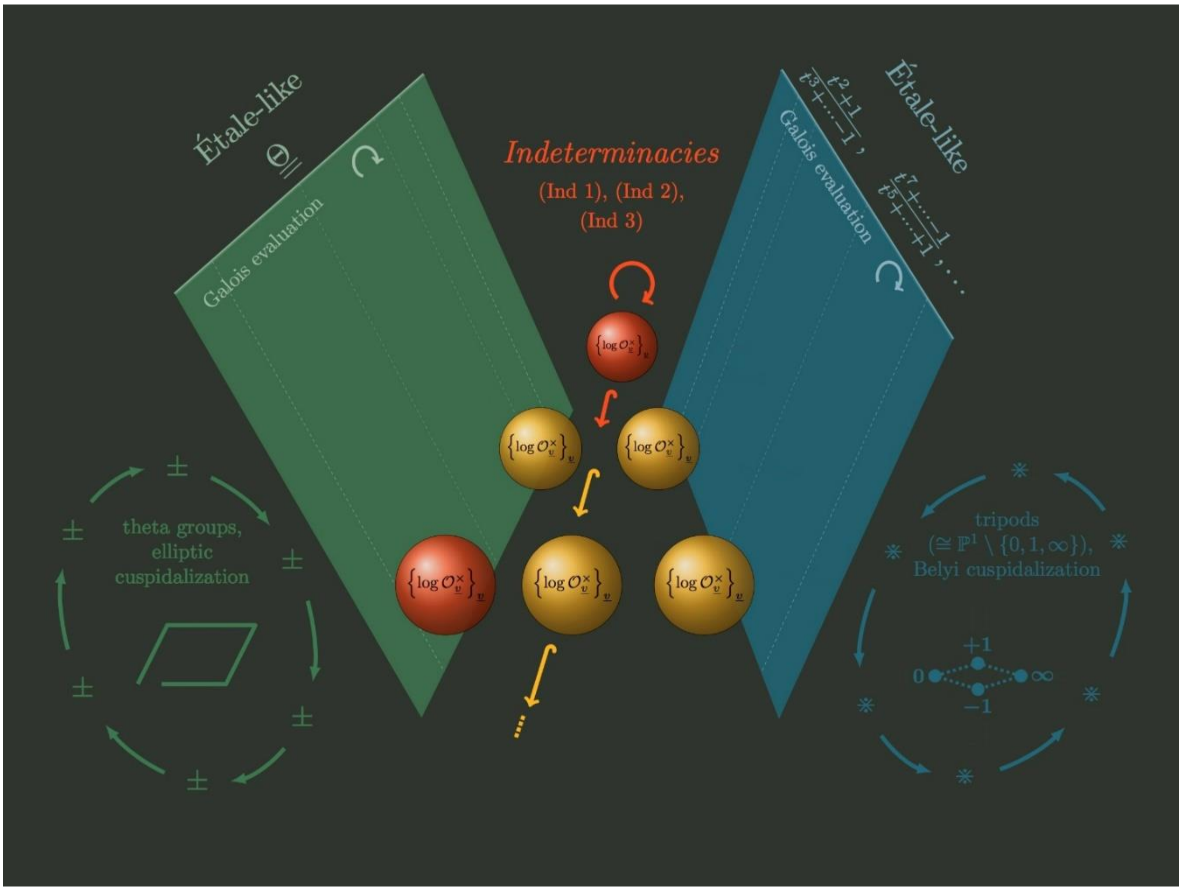
数の体系は「局所的側面」と「大域的側面」が絶妙に関連しているので、局所的な側面を束ねて大域的な性質に結実させるのは一般的には非常に困難である。無限個ある局所理論は、それぞれ完全に独立してやればよいというわけではなく、「たし算構造」と「かけ算構造」が大域的に“つながる”ようお互いに同期をとりながら関連性を保持しながら実行されなければならない。

この複雑な仕組みを映像的に示したものが、望月教授のホームページで紹介されている。

この動画では、左側で「$\boldsymbol{q}$」と「$\boldsymbol{\Theta}$」による不等式の理論が展開される。「$\boldsymbol{q}^{j^2}$」と書かれているのが、テータ関数の値、それぞれの素点ごとに、舞台間通信で得られたこれらの値が、下にある「対数殻（log shell)」と呼ばれるものの中に溜まっていく。一方、右側では対称性通信を通じて「$\boldsymbol{\kappa}$（カッパ）コア的関数」というものから復元された数体の情報が落ちて、下の対数殻にポロポロと落ちていく、といった状況が表現されている。　（２０２０．０５．１５）




エタールのような構造
Étale-like
不定性１，２，３
Indeterminacies
(Ind 1), (Ind 2),
(Ind 3)
エタールのような構造
Étale-like
Galois evaluation
テータ関数の値
Galois evaluation
数体の復元（剰余類）F
theta groups,
elliptic
cuspidalization
tripods
$(\cong \mathbb{P}^1 \setminus \{0, 1, \infty\})$,
Belyi cuspidalization
対数殻


Étale-like
Indeterminacies
(Ind 1), (Ind 2),
(Ind 3)
Étale-like
Galois evaluation
Galois evaluation
theta groups,
elliptic
cuspidalization
tripods
$(\cong \mathbb{P}^1 \setminus \{0, 1, \infty\})$,
Belyi cuspidalization