
「ラングランズ・プログラム」とは何か？
やさしい入門編

「ラングランズ・プログラム」とは何か？
Agenda

Part 1

はじめに

Part 2

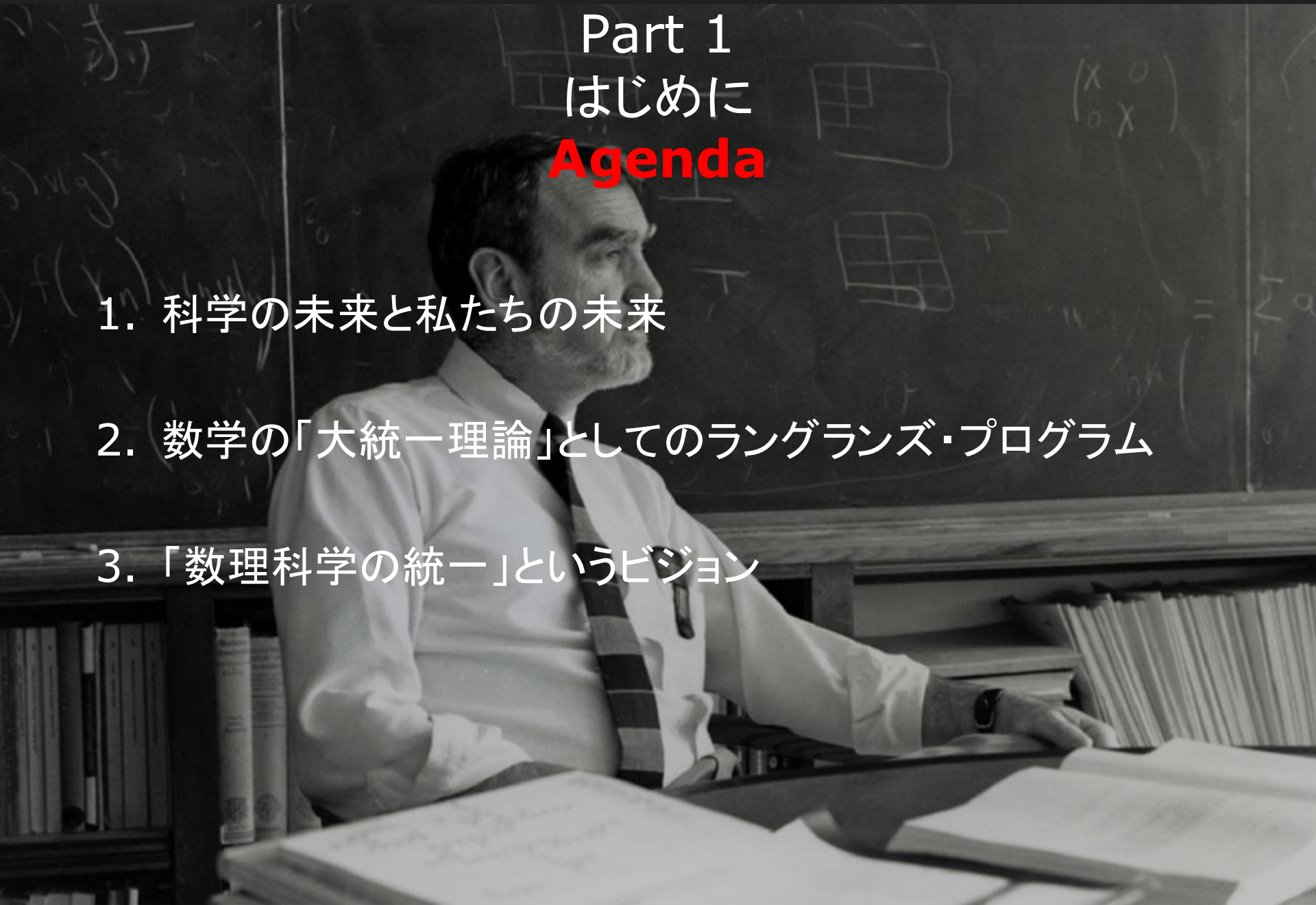
谷山・志村予想

Part 3

Langlands programの創世記

Part 4

Wiles による「フェルマーの最終定理」の証明

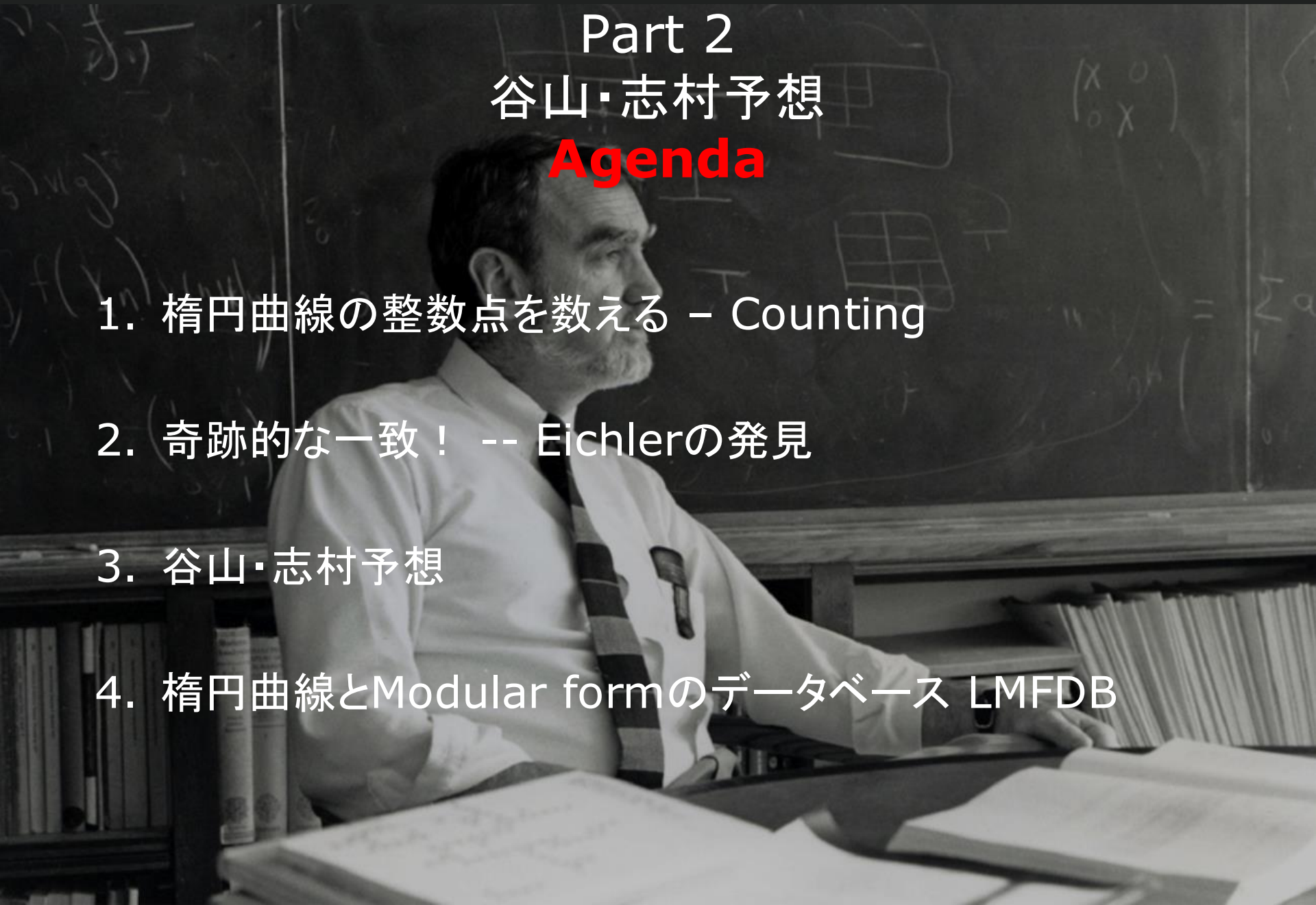


Part 1
はじめに
Agenda

1. 科学の未来と私たちの未来

2. 数学の「大統一理論」としてのラングランズ・プログラム

3. 「数理科学の統一」というビジョン

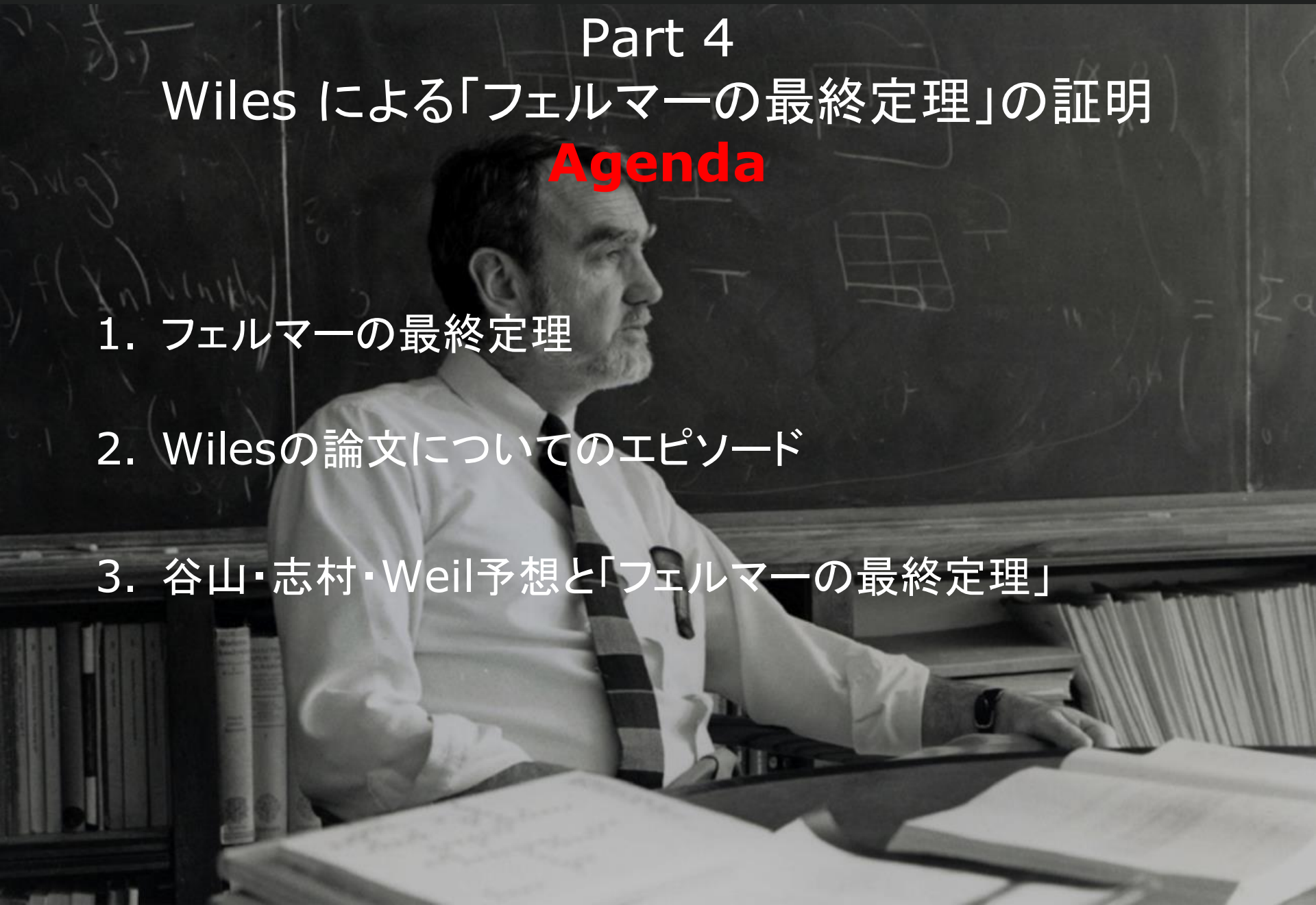


Part 2
谷山･志村予想
Agenda

1. 楕円曲線の整数点を数える – Counting
2. 奇跡的な一致！ -- Eichlerの発見
3. 谷山･志村予想
4. 楕円曲線とModular formのデータベース LMFDB

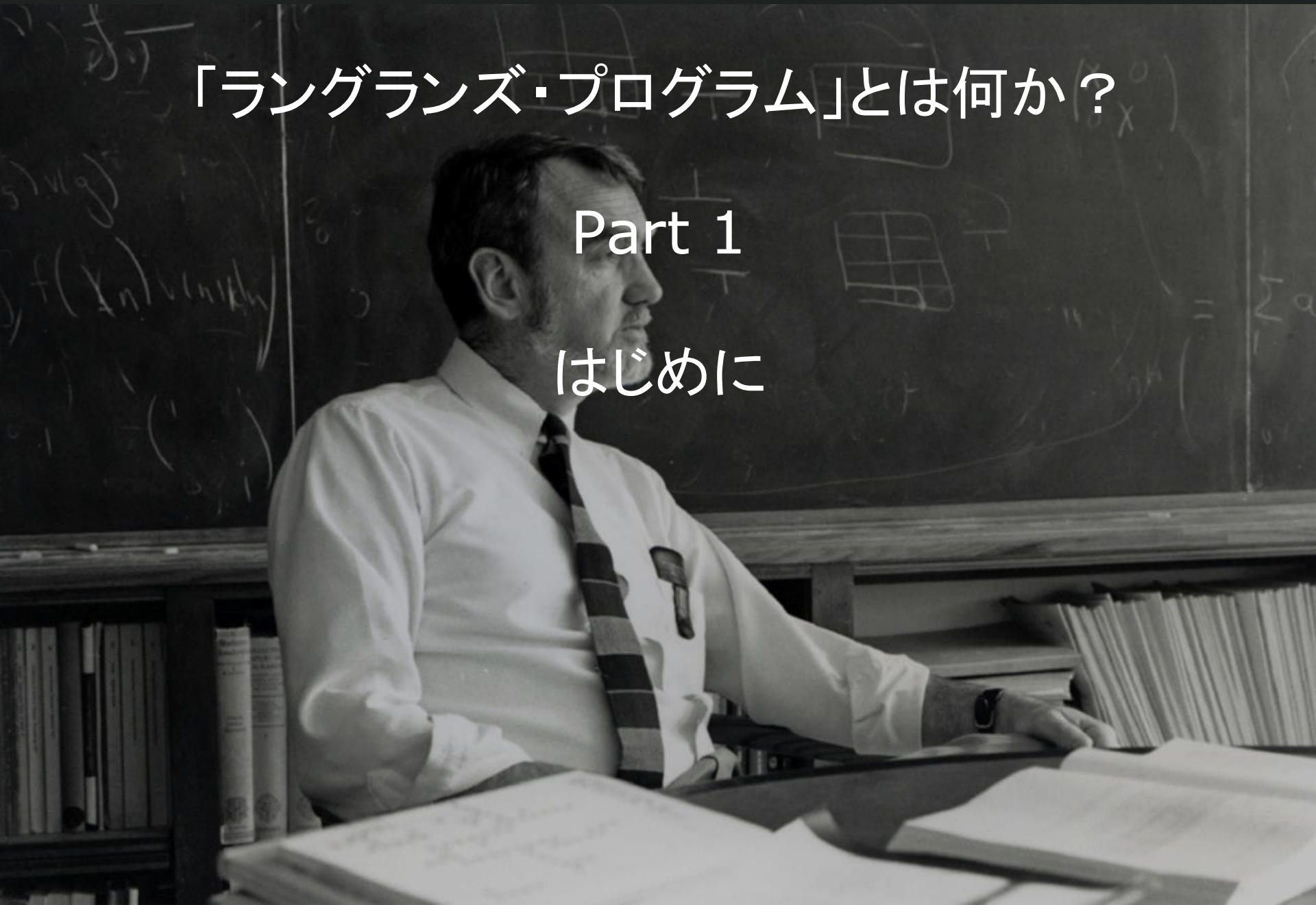
Part 3
Langlands programの創世記
Agenda

1. Weilへの手紙 --1967年
2. Eulerが考えたこと -- Euler product
3. Grothendieck – 1965年



Part 4
Wiles による「フェルマーの最終定理」の証明
Agenda

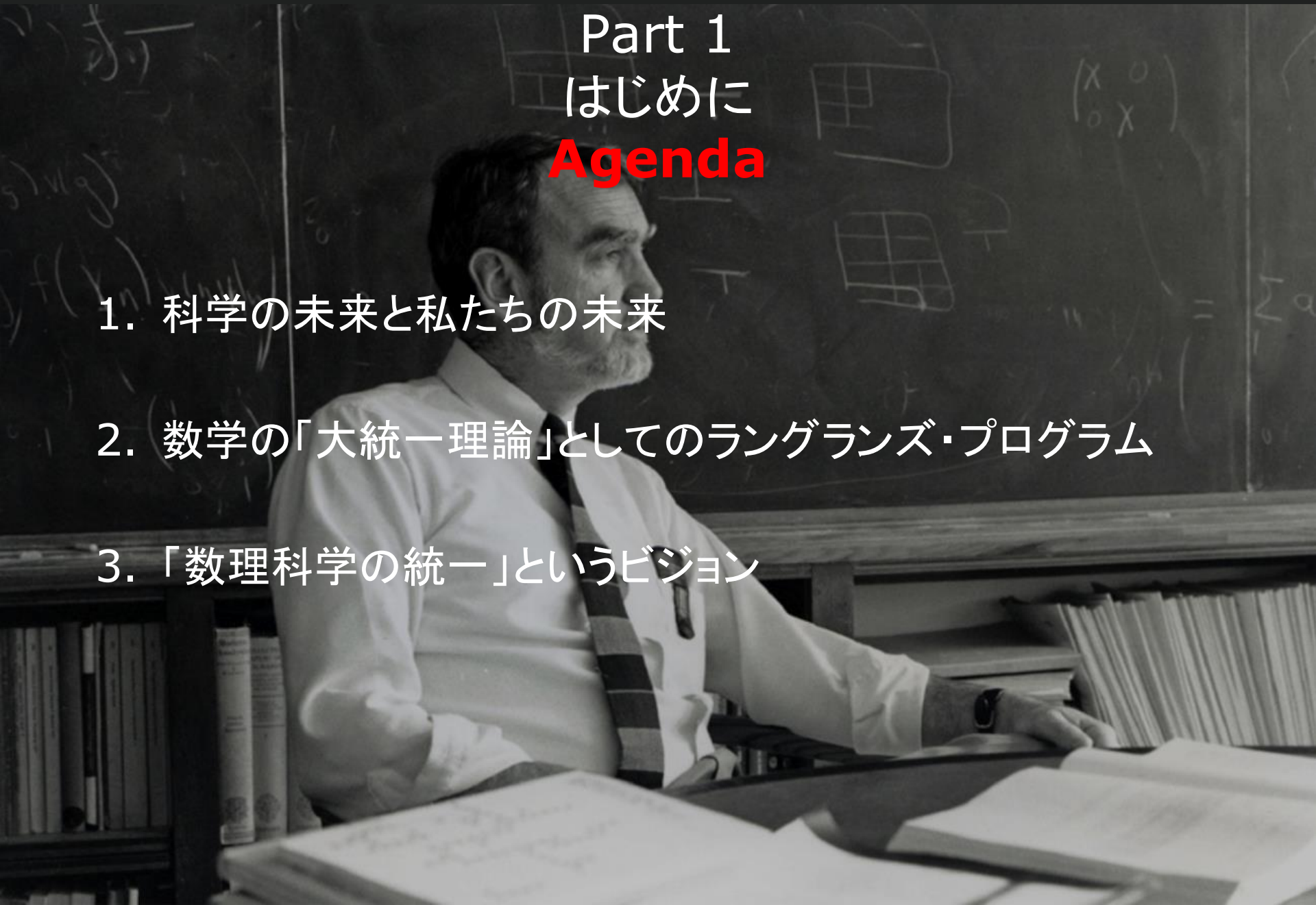
1. フェルマーの最終定理
2. Wilesの論文についてのエピソード
3. 谷山･志村･Weil予想と「フェルマーの最終定理」



「ラングランズ・プログラム」とは何か？

Part 1

はじめに

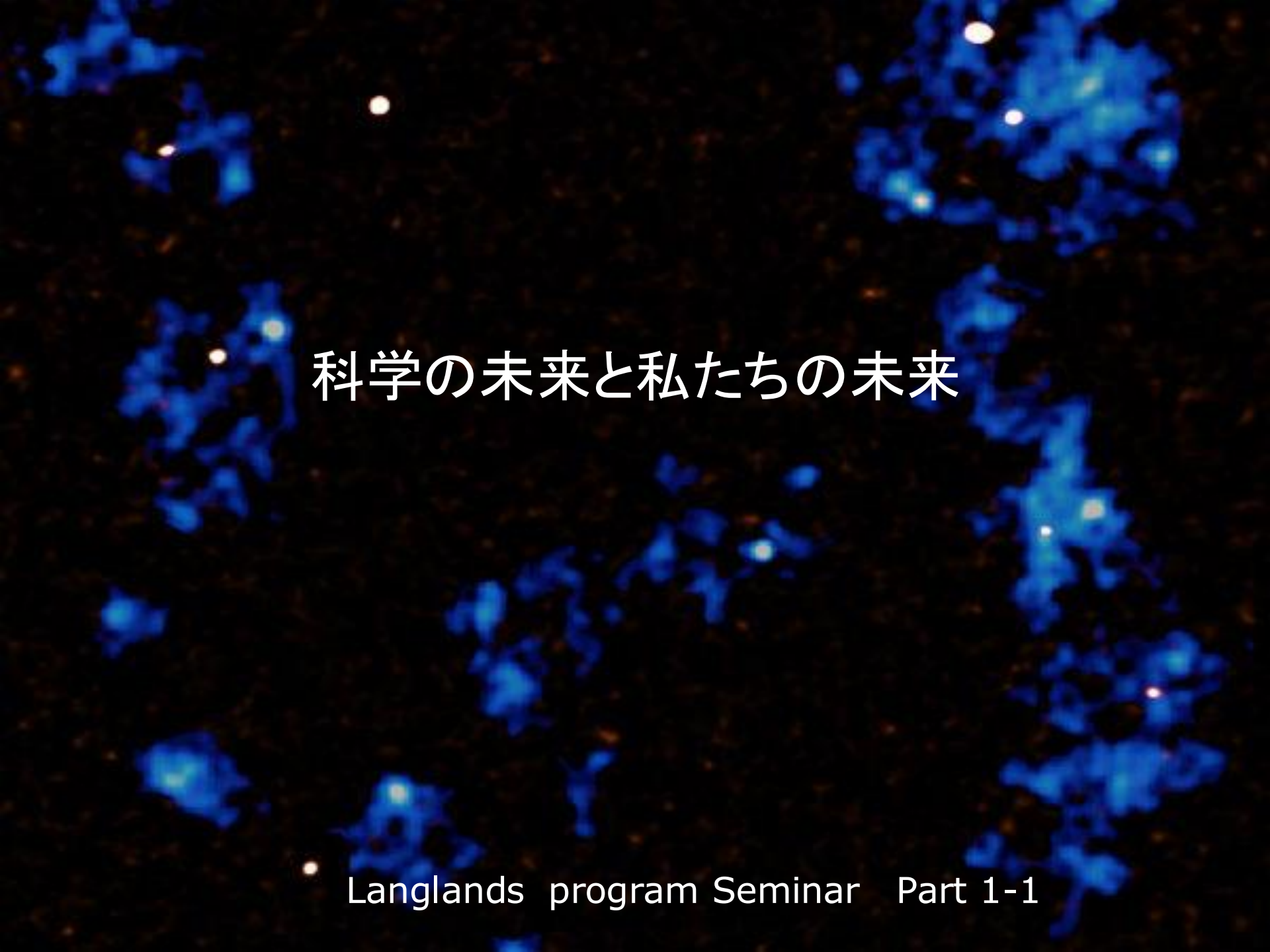


Part 1
はじめに
Agenda

1. 科学の未来と私たちの未来

2. 数学の「大統一理論」としてのラングランズ・プログラム

3. 「数理科学の統一」というビジョン


科学の未来と私たちの未来
Langlands program Seminar Part 1-1

今なぜ「数学」について語るのか？

2024年も終わりに近づいています。21世紀の最初の25年が終わろうとしています。

激動と言っていい現実の大きな変化の中で、これからの21世紀が私たちにとってどのような時代になるのか、多くの人が関心を高めていると思います。

考えるべき課題が山のように積み上がる中で、なぜ今、数学の世界について語るのでしょう？

それは、現在、数学の世界で進行している変化が、21世紀の科学の未来を大きく変える可能性を持つと考えられているからです。

ラングランズ・プログラム

今回のセミナーで取り上げる「ラングランズ・プログラム」は、まさに、現在の数学の変化をドライブしている中心的なプロジェクトです。

今年の5月、「ラングランズ・プログラム」の基本的な予想の一つである「幾何学予想」が証明されたのは、大きな事件でした。

“Proof of the geometric Langlands conjecture”
https://people.mpim-bonn.mpg.de/gaitsgde/GLC/

残念ながら、その重要性は、メディアではほとんど伝えられることはありませんでした。

技術の未来と私たちの未来

確かに、数学の世界での発見が、我々の未来に大きな影響を与えるという考えには、飛躍があると感じる人は多いでしょう。

でも、「飛躍がある」というのは、本当なのでしょうか？　あるいは、なぜ、「飛躍がある」のでしょう？

核の脅威にせよAI技術にせよ、技術の未来が、私たちの未来に大きく影響を与えるということについては、多くの人がさまざまに考え、さまざまな論争があります。

それは、現代の分断と対立の舞台そのものといっていいのかもしれません。

「数理科学の統一」というビジョン

科学の未来と私たちの未来についてはどうでしょう？

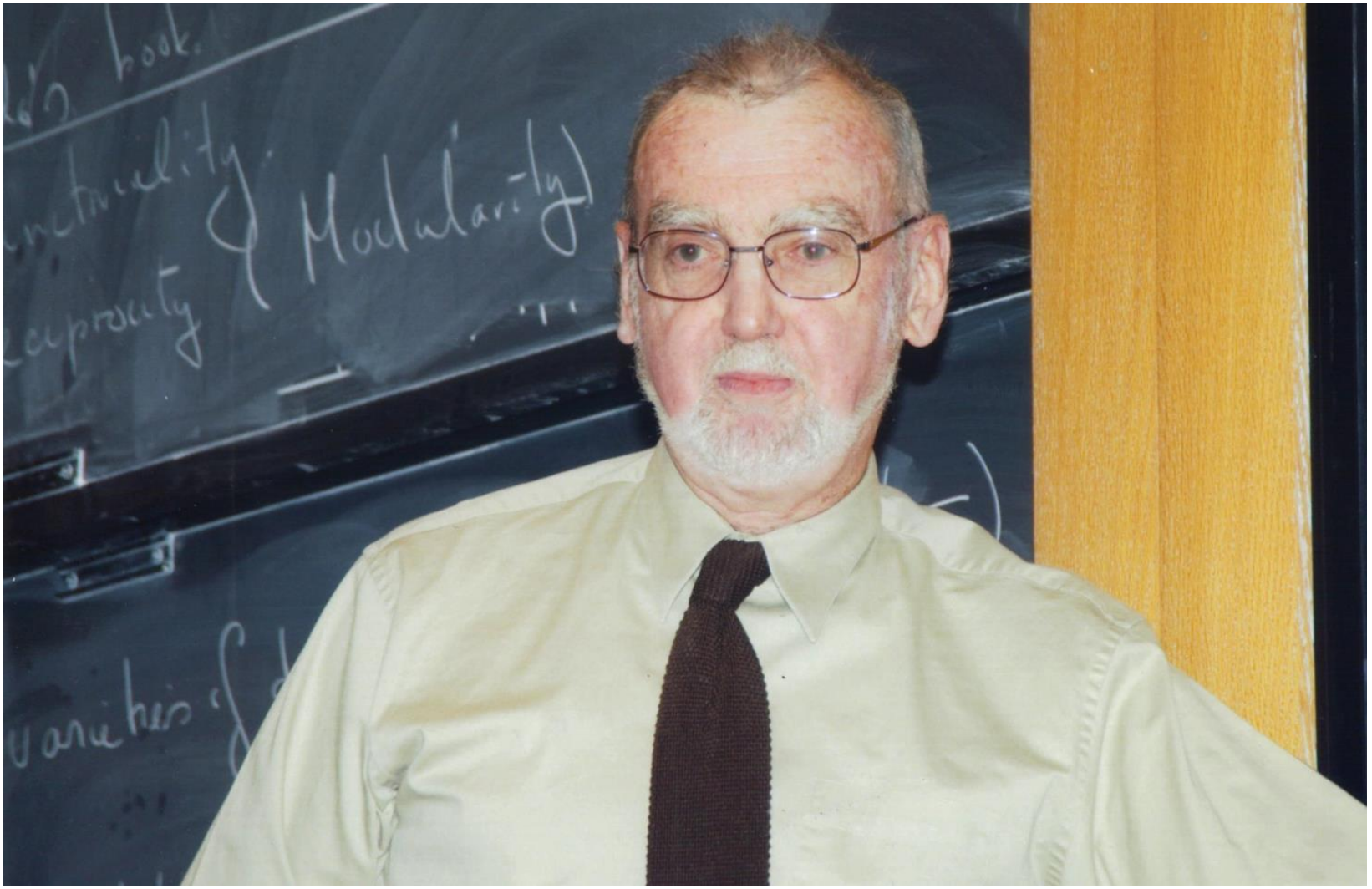
次に述べますように、「ラングランズ・プログラム」は、Frenkelのいうように、数学の各分野の「統一理論」を目指すものと考えることができるのですが、物理学のSuper String理論の深刻な行き詰まりの中で、数学と物理学を含めた「数理科学の統一理論」への期待と関心が高まっています。

科学が大きく変化するというビジョンのもとで、科学の未来と私たちの未来を議論することが、遠くない未来にはできるのではと考えています。

数学の「大統一理論」としての
ラングランズ・プログラム

Langlands program Seminar Part 1-2

LanglandsとLanglands program



Robert Langlands　1936~

ラングランズ･プログラムの意味するもの

素人の読者はもちろんや数学の専門家でさえ、ラングランズ・プログラムにおける抽象化は、やや理解しがたいものです。しかし、ラングランズの基本予想の証明または反証には、いくつかの明確な強い暗示があります。

このプログラムでは、解析的整数論と代数幾何の一般化との間に強力な関連性を仮定しているため、数体の抽象代数表現とそれらの解析的素数構成との間の「関手性」という考え方により、素数分布を正確に定量化できる強力な機能ツールが生まれます。これがさらに、ディオファントス方程式の分類や、さらに高度な代数関数の抽象化を可能にします。

英文 wiki の”implications” sectionから

さらに、仮定された対象物に対するこのような一般化代数の「相互性」が存在し、その解析関数が明確に定義されていることが示されれば、数学における非常に深い結果が証明できる可能性があります。

例としては、楕円曲線の有理解、代数多様体の位相的構成、そして有名なリーマン予想などがあります。このような証明では、一般化された解析級数の抽象的な解が利用されると予想されており、それぞれは数体における構造内の不変性に関連しています。

さらに、ラングランズ・プログラムとM理論との間には、両者の類似性が非自明な方法で結びついており、超弦理論における正確な解法の可能性を示唆しているという仮説が立てられています。

（これは、群論におけるmonstrous moonshine群の例と同様です。）

簡単に言えば、ラングランズ・プロジェクトは、幾何学的な形式に埋め込まれた解析関数による代数方程式の厳密解の高次一般化を通じて、数学の最も基本的な領域に触れる、深遠で強力な解決策の枠組みを示唆しています。

これにより、多くの離れた数学分野を強力な分析的手法の形式に統合することが可能になります。

Robert Langlands

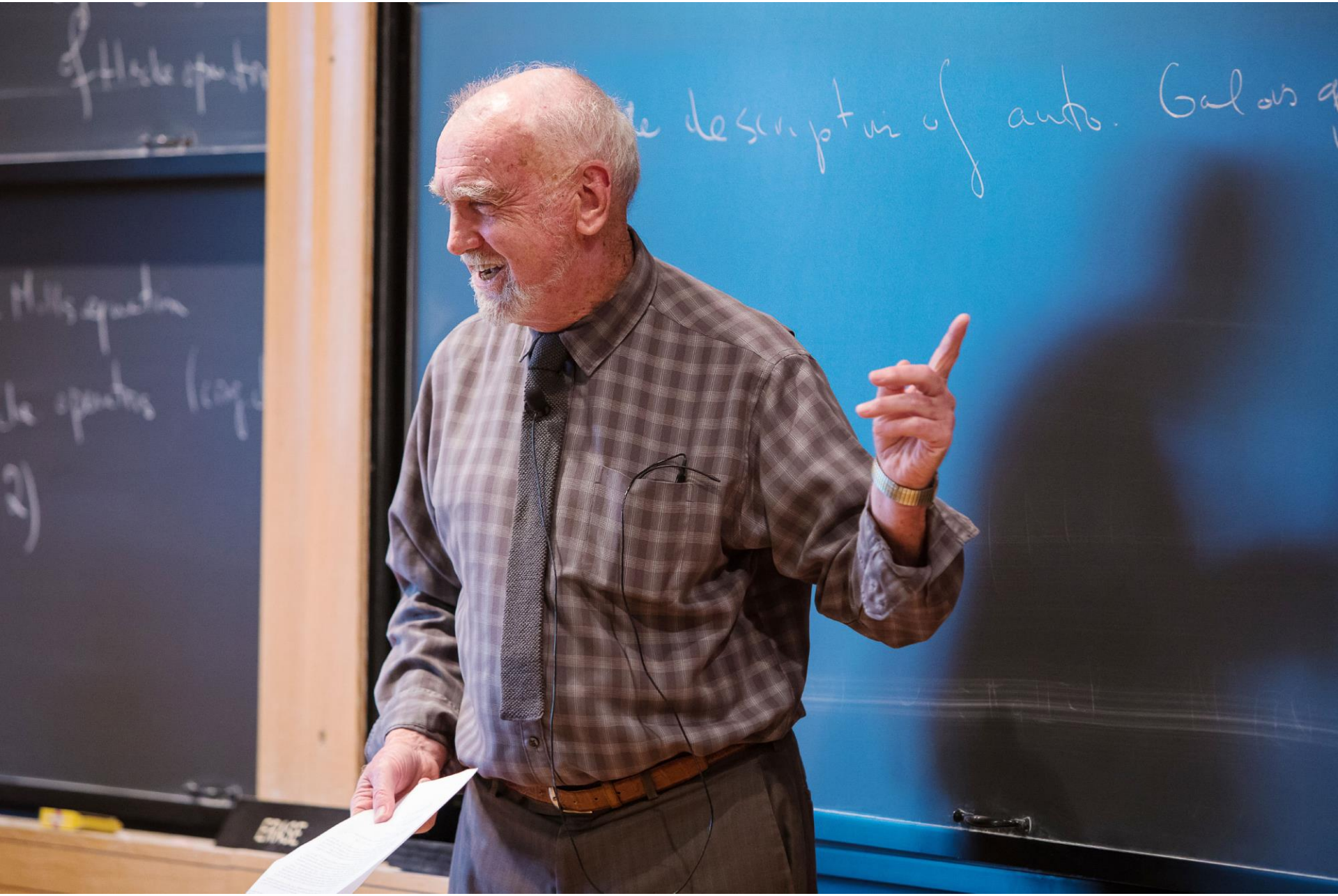
https://ja.wikipedia.org/wiki/ロバート・ラングランズ

https://en.wikipedia.org/wiki/Robert_Langlands

Langlands program

https://ja.wikipedia.org/wiki/ラングランズ・プログラム

https://en.wikipedia.org/wiki/Langlands_program



2016

Edward Frenkel “Love and Math”
『数学の大統一に挑む』から

ラングランズ・プログラムは、今や広大な研究分野となり、数論、調和解析、幾何学、表現論、数理物理学などさまざまな領域で、多くの数学者がこれに取り組んでいる。

数学者たちは、相当異質な対象を調べているにもかかわらず、よく似た現象を見る。

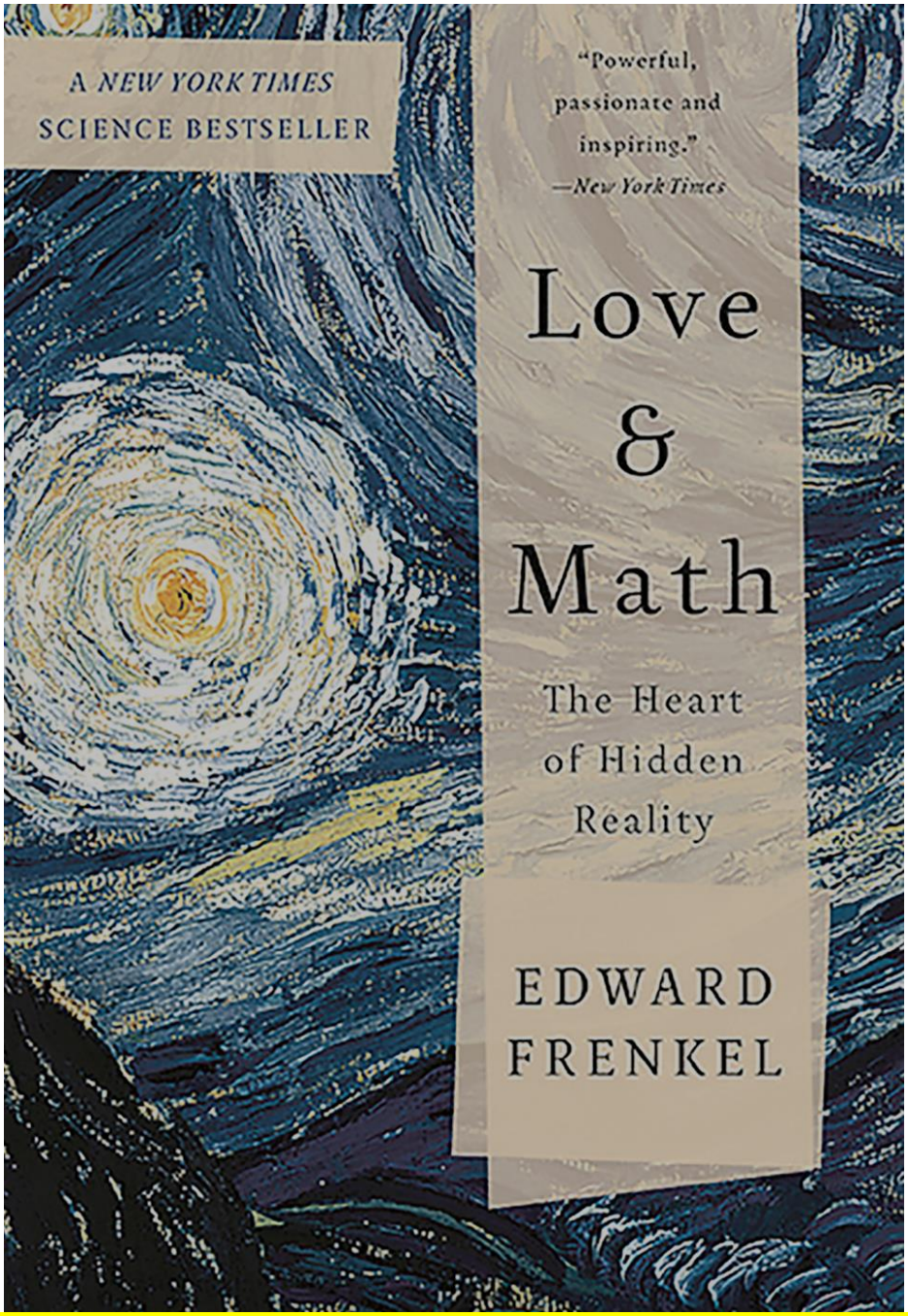
父はこれまでの話を読んで、「内容を詰め込みすぎだ」と言った。たしかに本章では、ヒッチン・モジュライ空間、ミラー対称性、Aブレーン、Bブレーン、保型層といった概念が登場した。これらすべての名前を覚えようとするだけでも、頭が痛くなってくるかもしれない。しかし信じてほしいが、ここで話した構成法を隅々まで理解している人は、専門家の中にさえ、まずめったにいないのだ。

数学の「大統一」への一歩

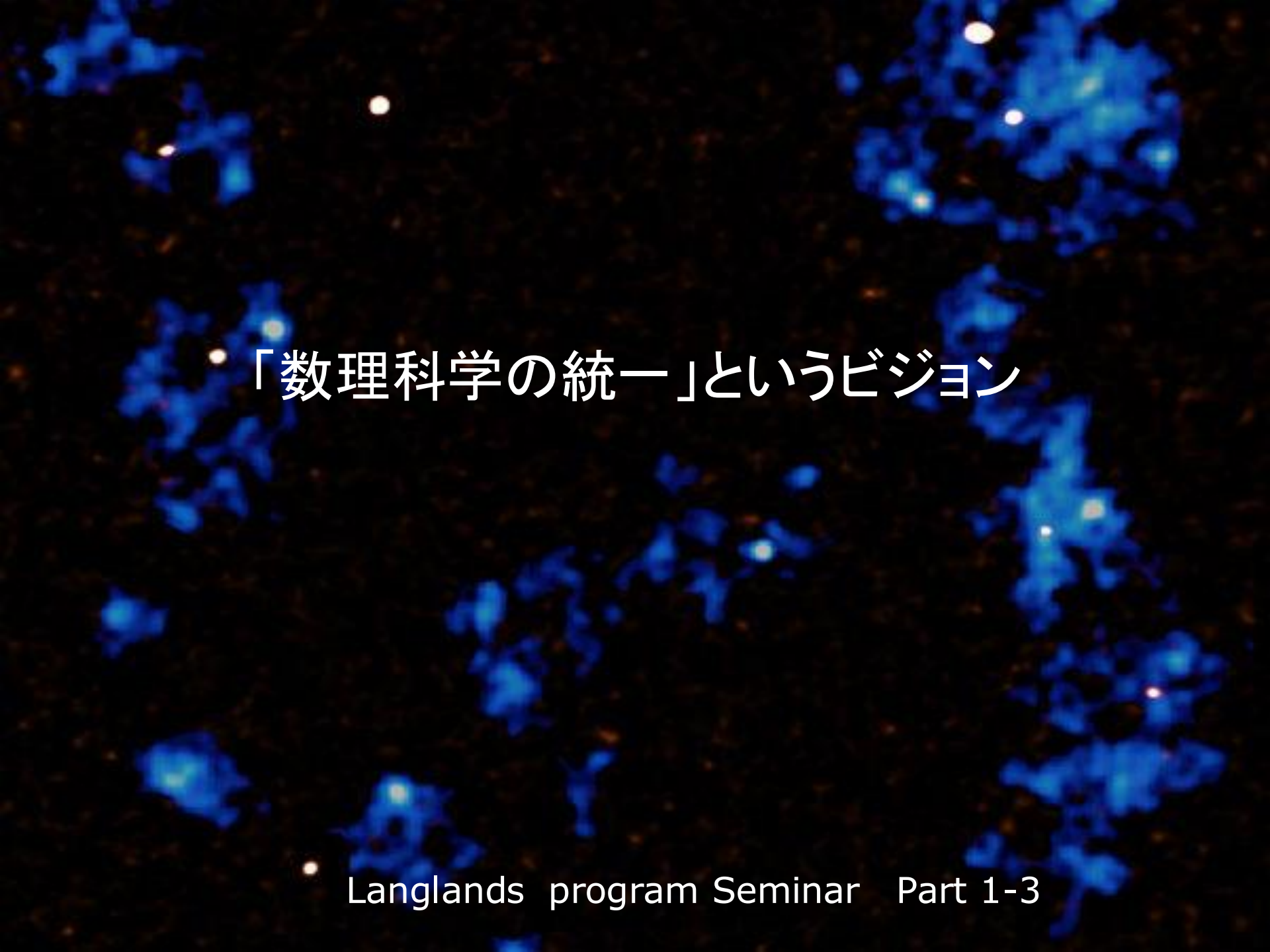
Frenkelは、Langlands program を、数学のさまざまな分野の「大統一」を目指す理論だという特徴づけをしています。それは、当たっていると思います。

今年五月の「幾何学的ラングランズ予想の証明 -- Proof of the geometric Langlands conjecture」の成功は、2024年、数学は「大統一」へ向けて、大きな一歩を踏み出したことを意味します。

Edward Frenkel
"Love and Math"



https://www.amazon.co.jp/-/en/Edward-Frenkel/dp/0465064957


「数理科学の統一」というビジョン
Langlands program Seminar Part 1-3

super string theory の行き詰まり

「大統一理論」というと、物理学での 電磁気力・弱い力・強い力・重力の四つの力を統一する理論、量子力学の「標準モデル」と重力の理論である一般相対性理論の統一を目指す理論を思い浮かべる人が多いと思います。

また、そうした統一理論を牽引してきた代表的な理論が、「超弦理論 super string theory」であることも、多くの人は知っていると思います。

ただ、僕にとっての2024年の最大のニュースの一つは、Langlands programの画期的な前進とともに、残念なことですが、super string theory の行き詰まりが明らかになってきたことでした。

super string theoryの創始者の一人である、Susskindがそれを率直に認めたことは、衝撃的でした。

https://youtu.be/2p_Hlm6aCok

WittenのBlackhole論

こうした中で新しい模索も始まっているように見えます。

僕は、2024年7月の北京でのWittenのブラックホール論の展開に興味を持っています。

講演資料

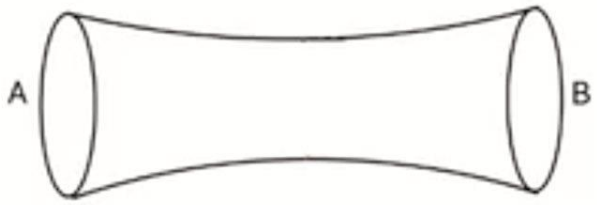
https://lsp.icbs.cn/upload/1143-1720859282-Edward%20Witten%EF%BC%8807-13%20final%20version%EF%BC%89-Black-Hole-BeijingLecture.pdf

INTERNATIONAL CONGRESS OF BASIC SCIENCE

国际基础科学大会

BIMSA bilibili

The answer is "yes," as was first found by Ryu and Takayanagi (2006), with later refinements by other authors. The simplest setup is to consider a universe with two "ends" (or asymptotic regions where an observer might live) with the universe overall in a state of minimum uncertainty (a pure state).



2024/07 Witten 講演

講演ビデオ(Youtube)

https://youtu.be/VoozXnBxf8k

数理科学は大きな転換期に差し掛かっている

2024年、数理科学の両輪である数学と物理学の世界に起きた、明暗二つの事件は、21世紀の数理科学が、大きな転換期に差し掛かっていることを示しています。

きっと、これから、我々が恋に落ちる、愛すべき魅力的な新しい数理科学の時代が始まるのだと思います。

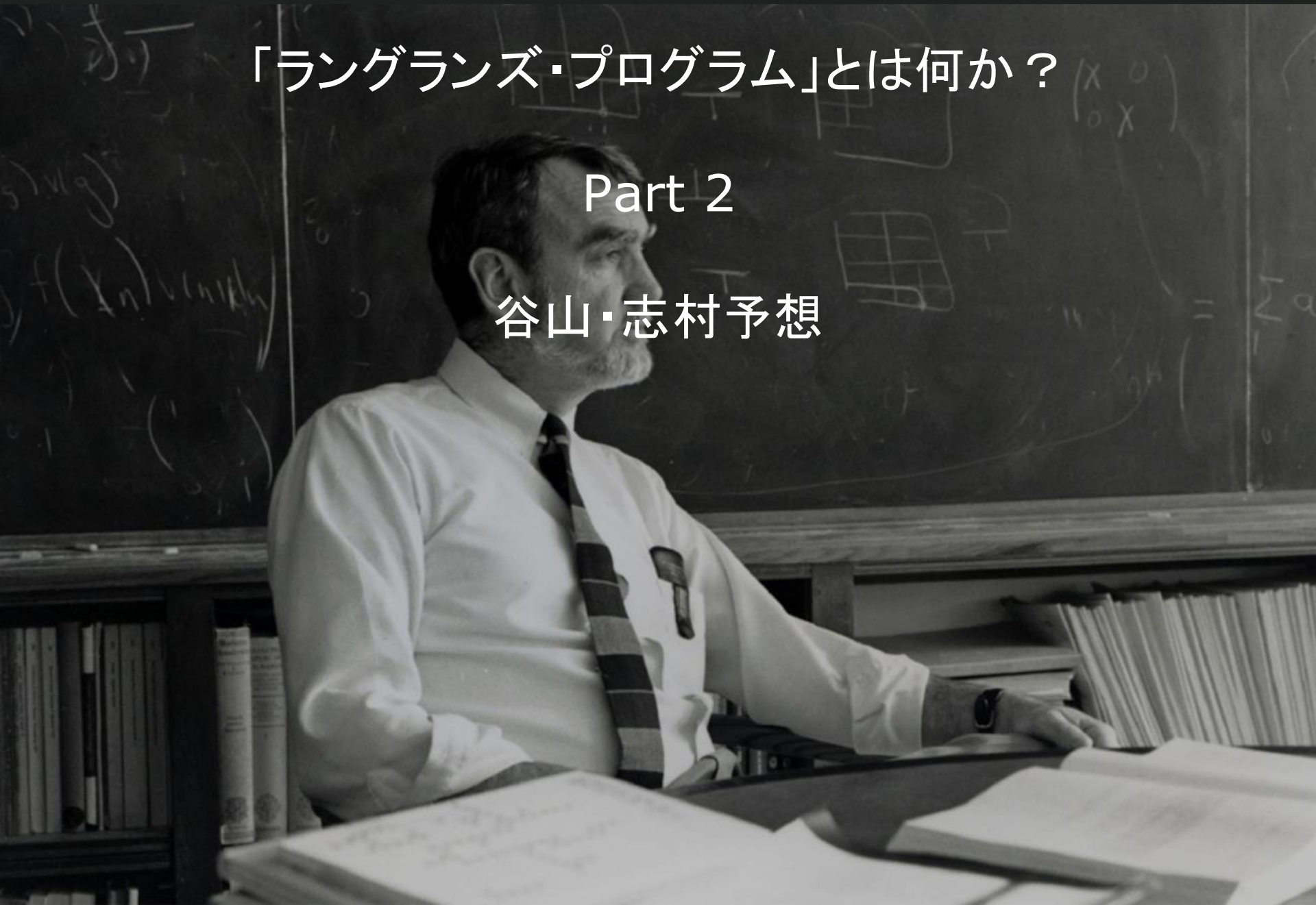
It's been too long since we took the time
No one's to blame, I know time flies so quickly
But when I see you, darling
It's like we both are falling in love again
It'll be just like starting over (over)
Starting over (over)

セミナーの構成

セミナーでは、次のような構成でラングラン・プログラムの概要を紹介したいと思います。

Part 1　はじめに ーー 科学の未来と私たちの未来
Part 2　谷山・志村予想
Part 3　Langlands Programの創世記
Part 4　Wiles による「フェルマーの最終定理」の証明


HITACHI
危い!



「ラングランズ・プログラム」とは何か？

Part 2

谷山・志村予想

Part 2　「谷山・志村予想」

この Part 2では、Langlands programが生まれるきっかけの一つになった、1955年の「谷山・志村予想」を紹介しようと思います。それは、有理数体上の楕円曲線とモジュラー形式のあいだに深い繋がりがあると言う予想でした。

「谷山・志村予想」には、先行する発見がありました。Part 2の冒頭で紹介しようと思っている、1954年のEichlerの発見は、一見すると数学的には全く無関係に思えるものが、実は繋がっているという驚くべきものでした。

「予想」から「定理」へ

「谷山・志村予想」は、Langlands programのより一般的な予想の特殊ケースと見なされていますが、もちろん、Langlands programに先行したものです。

この「予想」は、1995年ある制限の下で、Wilesによって証明されます。それが、Wilesの「フェルマーの最終定理」の証明の中核部分です。それについては、Part 4 で紹介します。

2001年、「谷山・志村予想」 は完全な形で証明され、現在ではそれはもはや「予想」ではなく「モジュラリティ定理（modularity theorem）」と呼ばれています。

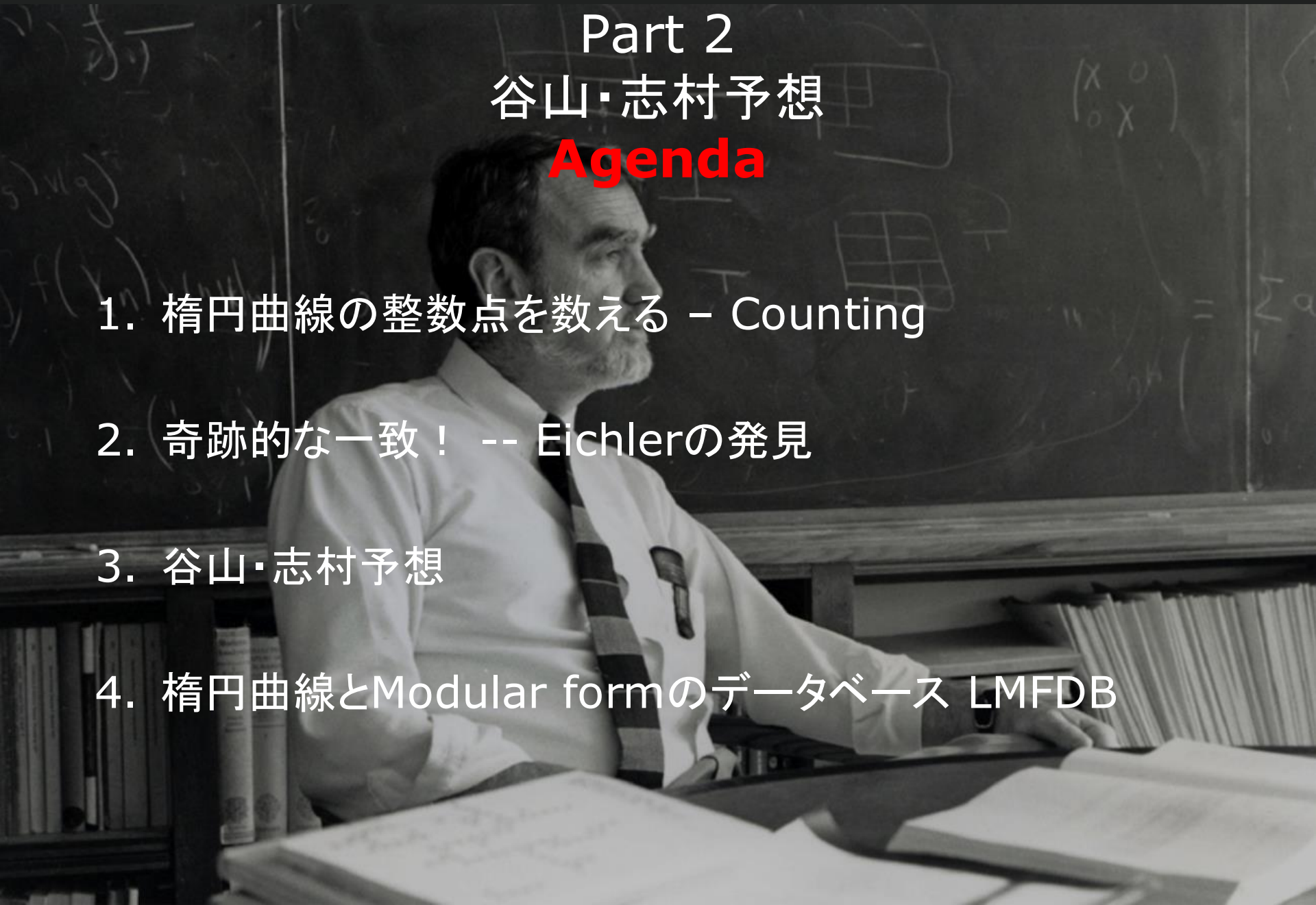
https://ja.wikipedia.org/wiki/谷山–志村予想

この節の文章は日本語として**不自然な表現、または文意がつかみづらい状態**になっています。
文意をわかりやすくするよう、修正が必要とされています。(2022年11月)

https://en.wikipedia.org/wiki/Modularity_theorem

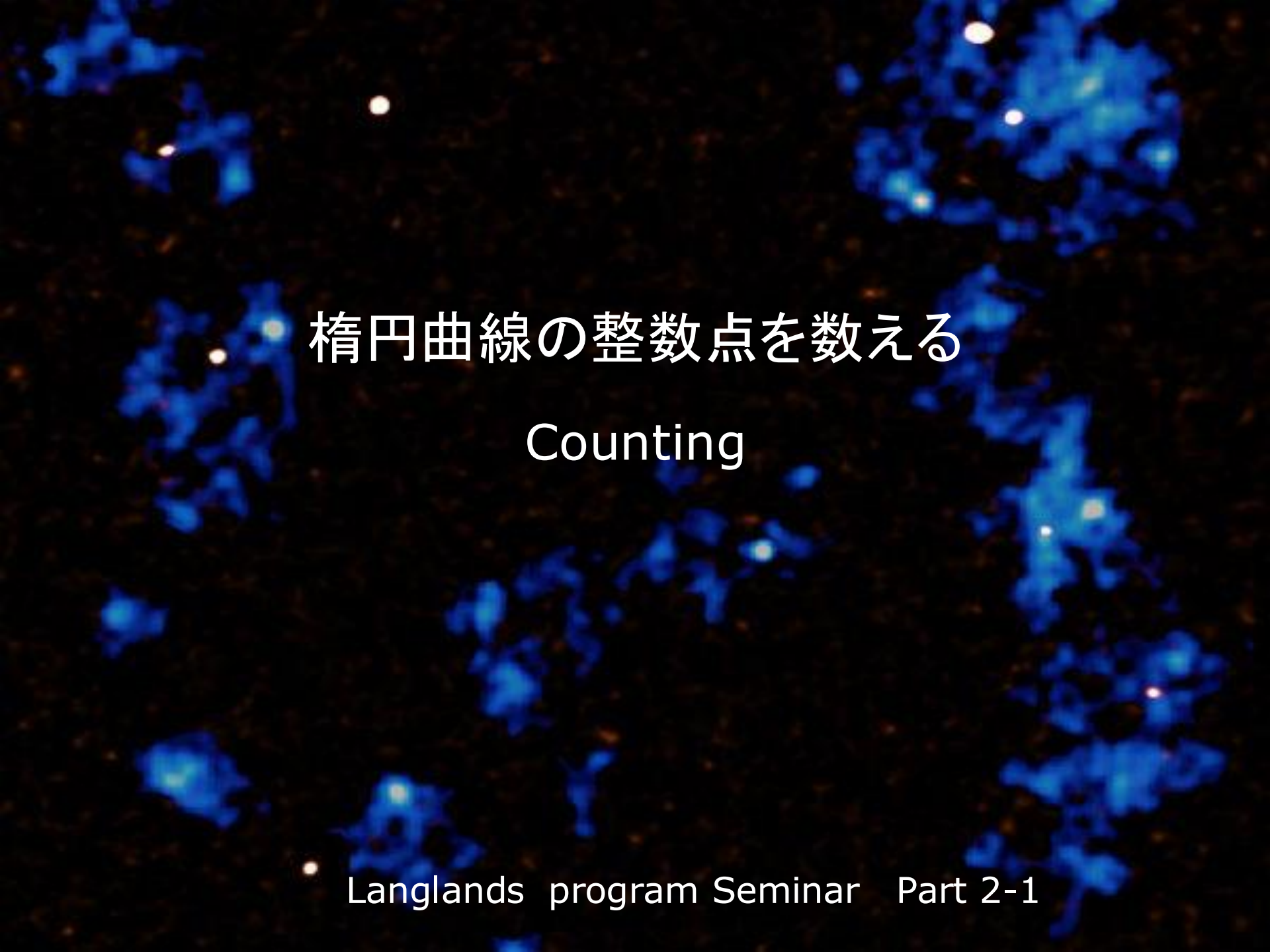
This section **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources in this section. Unsourced material may be challenged and removed.

Find sources: "Modularity theorem" – news · newspapers · books · scholar · JSTOR *(March 2021) (Learn how and when to remove this message)*



Part 2
谷山･志村予想
Agenda

1. 楕円曲線の整数点を数える – Counting
2. 奇跡的な一致！ -- Eichlerの発見
3. 谷山･志村予想
4. 楕円曲線とModular formのデータベース LMFDB


楕円曲線の整数点を数える
Counting
Langlands program Seminar Part 2-1

楕円曲線とは

このセッションで扱う楕円曲線は、$\mathbb{Q}$上で定義された次の形の整係数の二変数3次の方程式である。

$$a_1, a_2, a_3, a_4, a_5 \in \mathbb{Z}$$
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

この形式を、Weierstrassの標準形と呼ぶ。

[a_1, a_2, a_3, a_4, a_5] と係数を与えることで、一つの楕円曲線を指定することができる。

楕円曲線の例

例えば、次の式は $a_1 = 0, a_3 = 1, a_2 = -1, a_4 = 0, a_5 = 0$ で、係数が $[0, -1,\ 1,\ 0,\ 0]$ で与えられる楕円曲線である。

$$y^2 + y = x^3 - x^2$$

同様に、次の式は $a_1 = 1, a_3 = 1, a_2 = 0, a_4 = -1, a_5 = 0$ で、係数が $[1,\ 0,\ 1,\ -1,\ 0]$ で与えられる楕円曲線である。

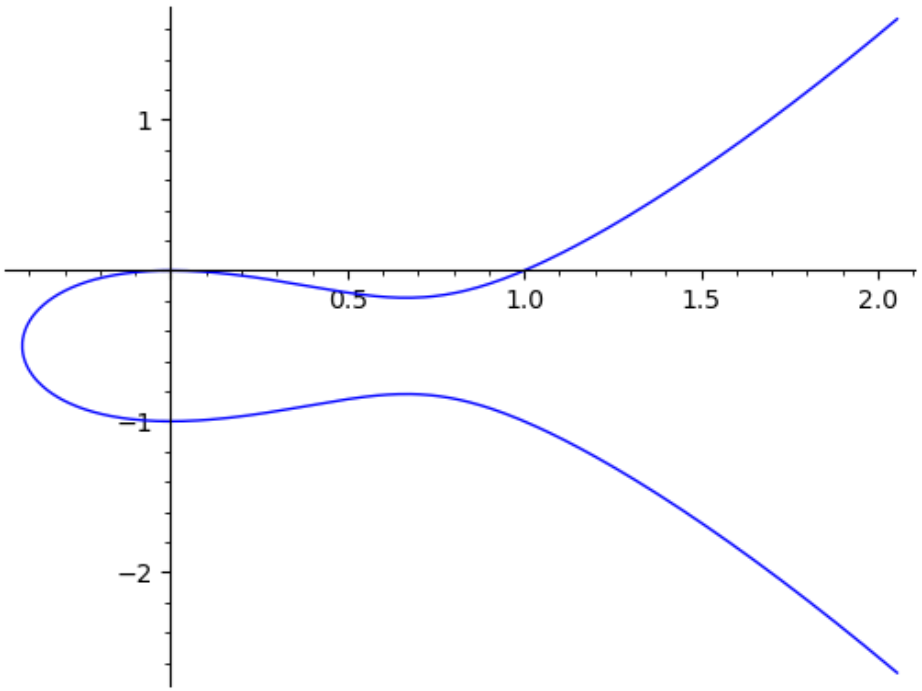
$$y^2 + xy + y = x^3 - x$$

楕円曲線の整数点を数える

このセッションでは、ある楕円曲線が与えられた時、そのグラフで x, y 座標がともに整数になる点である整数点(integral point)がいくつあるかという問題を考えてみよう。

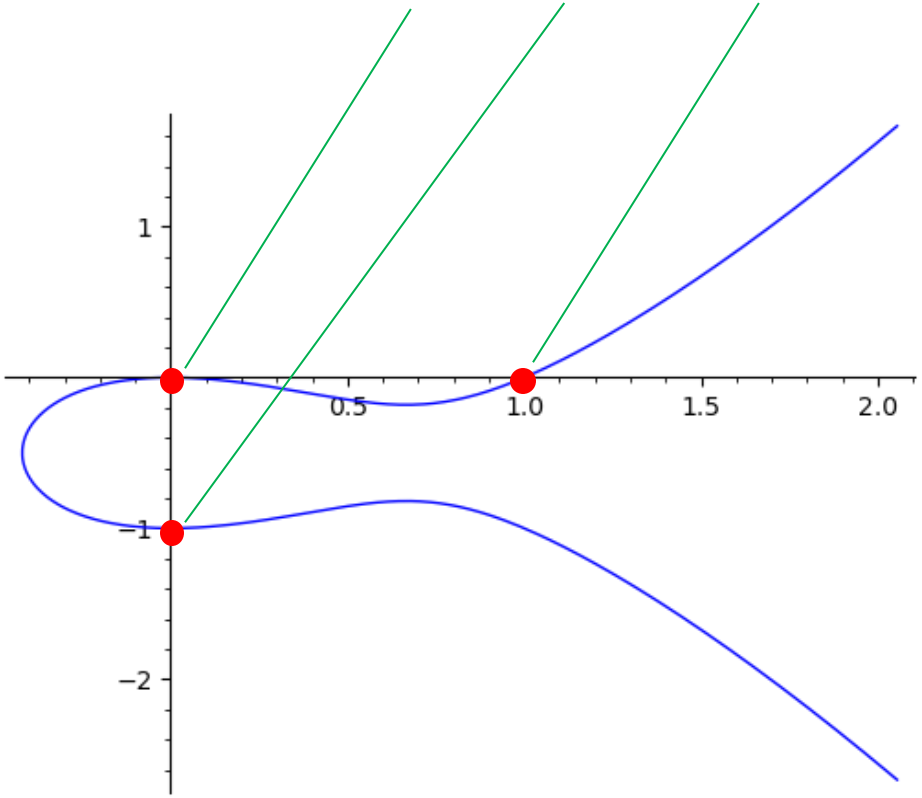
楕円曲線 $y^2 + y = x^3 - x^2$ の整数点を数える

式 $y^2 + y = x^3 - x^2$ で与えられる楕円曲線は、次のような形をしている。



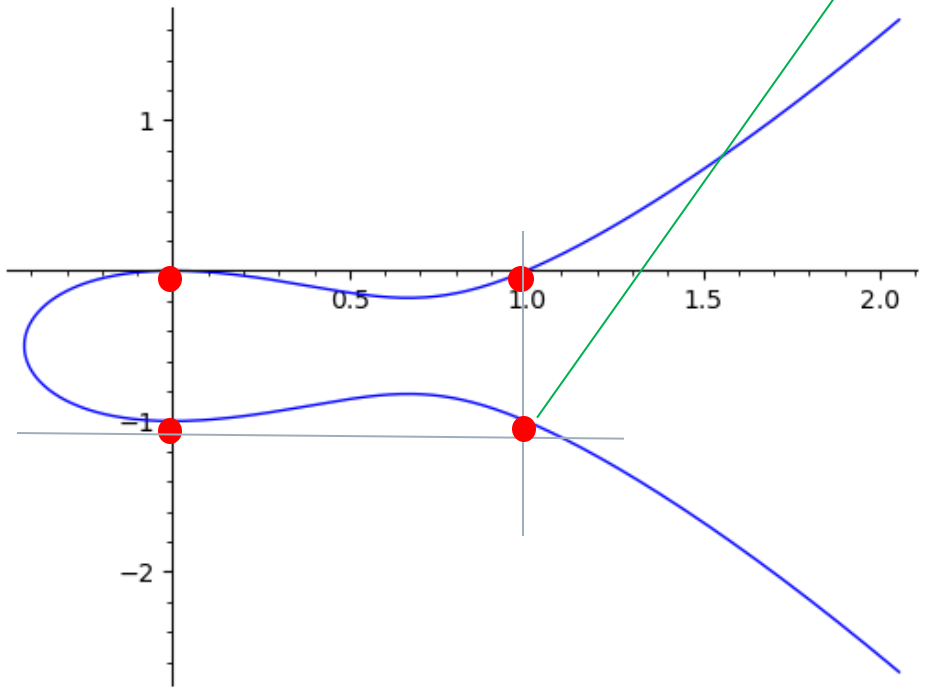
楕円曲線 $y^2 + y = x^3 - x^2$ の整数点を数える

式 $y^2 + y = x^3 - x^2$ で与えられる楕円曲線は、次のような形をしている。このグラフから、$(0,0), (0,-1), (1,0)$ が整数点であることがわかる。



楕円曲線 $y^2 + y = x^3 - x^2$ の整数点を数える

グラフからだけではわかりにくいかもしれないが、$(1, -1)$も、
$y^2 + y = x^3 - x^2$ の上にあることは、すぐに確かめることができる。



楕円曲線 $y^2 + y = x^3 - x^2$ の整数点を数える
これで全部か？

グラフと簡単なチェックで、$y^2 + y = x^3 - x^2$ 上に、整数点 $(0,0), (0,-1), (1,0), (1,-1)$ があることはわかった。

問題は、この曲線上の整数点がこの4つだけであるか？ということである。

もちろん、そうは言えない。

では、どうするか？　総当たりで確かめる？

一つの考えは、全ての整数$x, y \in \mathbb{Z}$についてペア(x, y)を考え、それが、楕円曲線の方程式を満たすか否かをチェックして、このテストに合格するペアの数を数えることである。

ただ、こうした総当たりでは（といっても現実に可能なのは有限回のチェックでしかない）、次のような二つの重要な問題に対して、その両方に答えを与えることができない。

1. 整数点は、一つも存在しないのか？
2. 整数点は、無限個存在するのか？

問題の設定を変える

最初の問題の設定は、「楕円曲線の整数点を数える」というものだったが、整数のペア全体を対象とした総当たりでは、あまり役にたつ情報は得られそうもない。

ここでは、違う形に問題を設定することにする。

それは、前回のセッションで、方程式 $ax = b$ や $x^2 = q$ の解を有限体$\mathbb{F}_p$ の中で探したように、「有限体 $\mathbb{F}_p$ の中で、楕円曲線の整数点を数える」という問題を考えようということである。

素数pごとに有限体$\mathbb{F}_p$ は異なるので、$p = 2,3,5, \ldots$ ごとに整数点を数える必要がある。

やってみよう！

$P = 2$の時、$\mathbb{F}_2$ の中で、
楕円曲線 $y^2 + y = x^3 - x^2$ の整数点を数える

$y^2 + y = x^3 - x^2$ を $y(y+1) = x^2(x+1)$と変形する。
$x, y \in \mathbb{F}_2$ だから $x, y \in \{0,1\}$である。

$x = 0$の時、右辺は0になる。左辺の$y(y+1) = 0$。

よって、 $y = 0$ または、$y + 1 = 0$

$y = 1$ の時、$y + 1 = 1 + 1 = 2 = 0 \ (mod\ 2)$

$(0,0), (0,1)$ は、この楕円曲線の整数点である。

$x = 1$ の時、右辺は $1^2(1-1) = 0$

よって、 左辺 $y(y+1) = 0\ (mod\ 2)$

$y = 0$ または、$y + 1 = 0$

ここから、$y = 0$ または、$y = 1$

$(1,0),(1,1)$ は、この楕円曲線の整数点である。

$p = 2$の時、

この楕円曲線の$\mathbb{F}_2$での整数点は、次の4つである。

$(0,0),(0,1),(1,0),(1,1)$

$P = 3$の時、$\mathbb{F}_3$ の中で、
楕円曲線 $y^2 + y = x^3 - x^2$ の整数点を数える

$y^2 + y = x^3 - x^2$ を $y(y+1) = x^2(x-1)$と変形する。

$x, y \in \mathbb{F}_3$ だから $x, y \in \{0,1,2\}$である。

$x = 0$の時、右辺は0になる。$y(y+1) = 0$。

よって、 $y = 0$ または、$y + 1 = 0$

$y = 2$ の時、$y + 1 = 2 + 1 = 3 = 0 \ (mod\ 3)$

$(0,0),(0,2)$ は、この楕円曲線の整数点である。

$x = 1$ の時、右辺は $1^2(1-1) = 0$

よって、 左辺 $y(y+1) = 0\ (mod\ 3)$

$y = 0$ または、$y + 1 = 0$

ここから、$y = 0$ または、$y = 2$

$(1, 0), (1, 2)$ は、この楕円曲線の整数点である。

$x = 2$ の時、右辺は $2^2(2-1) = 4 = 1\ (mod\ 3)$

よって、 左辺 $y(y+1) = 1\ (mod\ 3)$

$y = 0$は、$0 = 1\ (mod\ 3)$ となってこの式を満たさない。

$y = 1$は、$2 = 1\ (mod\ 3)$ となってこの式を満たさない。

$y = 2$も、$6 = 0 = 1\ (mod\ 3)$ となってこの式を満たさない。

$p = 3$の時、

この楕円曲線の$\mathbb{F}_3$での整数点は、次の4つである。

$(0,0),(0,2),(1,0),(1,2)$

$P = 5$の時、$\mathbb{F}_5$ の中で、
楕円曲線 $y^2 + y = x^3 - x^2$ の整数点を数える

$y^2 + y = x^3 - x^2$ を $y(y+1) = x^2(x-1)$と変形する。

$x, y \in \mathbb{F}_5$ だから $x, y \in \{0,1,2,3,4\}$である。

$x = 0$の時、右辺は0になる。$y(y+1) = 0$。

よって、 $y = 0$ または、$y + 1 = 0$

$y = 4$ の時、$y + 1 = 4 + 1 = 5 = 0 \ (mod\ 5)$

$(0,0),(0,4)$ は、この楕円曲線の整数点である。

$x = 1$ の時、右辺は $1^2(1-1) = 0$

よって、 左辺 $y(y+1) = 0$

$y = 0$ または、$y + 1 = 0\ (mod\ 5)$

ここから、$y = 0$ または、$y = 4$

$(1, 0), (1, 4)$ は、この楕円曲線の整数点である。

$x = 2$ の時、右辺は $2^2(2-1) = 4$

よって、 左辺 $y(y+1) = 4\ (mod\ 5)$

$y = 0$は、$0 = 4\ (mod\ 5)$ となってこの式を満たさない。

$y = 1$は、$2 = 4\ (mod\ 5)$ となってこの式を満たさない。

$y = 2$は、$6 = 4\ (mod\ 5)$ となってこの式を満たさない。

$y = 3$は、$12 = 2 = 4\ (mod\ 5)$ となってこの式を満たさない。

$y = 4$は、$20 = 0 = 4\ (mod\ 5)$ となってこの式を満たさない。

$x = 3$ の時、右辺は $3^2(3-1) = 18 = 3\ (mod\ 5)$

よって、 左辺 $y(y+1) = 3\ (mod\ 5)$

$y = 0$は、$0 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 1$は、$2 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 2$は、$6 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 3$は、$12 = 2 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 4$は、$12 = 2 = 3\ (mod\ 5)$ となってこの式を満たさない。

$x = 4$ の時、右辺は $4^2(4-1) = 48 = 3\ (mod\ 5)$

よって、 左辺 $y(y+1) = 3\ (mod\ 5)$

$y = 0$は、$0 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 1$は、$2 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 2$は、$6 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 3$は、$12 = 2 = 3\ (mod\ 5)$ となってこの式を満たさない。

$y = 4$は、$12 = 2 = 3\ (mod\ 5)$ となってこの式を満たさない。

$p = 5$の時、

この楕円曲線の$\mathbb{F}_5$での整数点は、次の4つである。

$(0,0),(0,4),(1,0),(1,4)$

ここまでのまとめ

$p = 2$の時、
この楕円曲線の$\mathbb{F}_2$での整数点は、次の4つである。
$(0,0),(0,1),(1,0),(1,1)$

$p = 3$の時、
この楕円曲線の$\mathbb{F}_3$での整数点は、次の4つである。
$(0,0),(0,2),(1,0),(1,2)$

$p = 5$の時、
この楕円曲線の$\mathbb{F}_5$での整数点は、次の4つである。
$(0,0),(0,4),(1,0),(1,4)$

手計算は、手間がかかる
コンピュータを使ってみる

手計算は、手間がかかる。

この計算は、コンピュータで簡単にできる。

$x, y \in \mathbb{F}_p$では、$x, y \in \{0, 1, \dots, p-1\}$だから、たかだか$p$個の値を取る$x$と同じく$p$個の値を取る$y$を総当たりで組み合わせて、この例の場合だったら、$y^2 + y = x^3 - x^2 \ (mod\ p)$ が成り立っているかチェックすればいい。

ここでは、Sage というパッケージを使った。

整数論の処理には、とても便利である。高度なこともできる。

https://www.sagemath.org/

SageMath is a free open-source mathematics software system licensed under the GPL. It builds on top of many existing open-source packages: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R and many more. Access their combined power through a common, Python-based language or directly via interfaces or wrappers.

Mission: *Creating a viable free open source alternative to Magma, Maple, Mathematica and Matlab*.

Learn how to use SageMath:

Sage for Undergraduates by Gregory Bard (Spanish: Sage para Estudiantes de Pregrado)

Mathematical Computation with Sage by Paul Zimmermann et al.
(French: Calcul mathématique avec Sage, German: Rechnen mit Sage)

Sage on CoCalc

or: SageMathCell

Install 10.4

Releases · Clone from GitHub

Help/Documentation

Video · Forums · Tutorial · FAQ · **Questions?**

Feature Tour

Quickstart · Research · Graphics

Library

Testimonials · Books · Publications · Press Kit

Search

Search...

```
def my_loop2 ():

    print("Elliptic Curve: ", "y^2 + y == x^3 - x^2")
    p_loop = [2,3,5,7,11,13,17,19,23,29,31,37]
    for p in p_loop:
      solutions = []

      for x in Zmod (p):
          for y in Zmod (p):
              if y^2 + y == x^3 - x^2:
                  solutions.append((x, y))

      print(" ")
      print("Prime:", p)
      print("Solution")

      for x, y in solutions:
           print("(", x, ",", y, ")" , end = " ")

      n_of_sol = len(solutions)
      print("\nNumber of solutions: ", n_of_sol )
```

こんなプログラムを作った

```
def my_loop2 ():

    print("Elliptic Curve: ", "y^2 + y == x^3 - x^2")
    p_loop = [2,3,5,7,11,13,17,19,23,29,31,37]
    for p in p_loop:
      solutions = []
```

ここが仕事をしている部分。簡単である。

```
      for x in Zmod (p):
          for y in Zmod (p):
              if y^2 + y == x^3 - x^2:
                  solutions.append((x, y))

      print(" ")
      print("Prime:", p)
      print("Solution")

      for x, y in solutions:
           print("(", x, ",", y, ")" , end = " ")

      n_of_sol = len(solutions)
      print("\nNumber of solutions: ", n_of_sol )
```

プログラムの出力

Elliptic Curve: y^2 + y == x^3 - x^2

Prime: 2
Solution
(0 , 0) (0 , 1) (1 , 0) (1 , 1)
Number of solutions: 4

Prime: 3
Solution
(0 , 0) (0 , 2) (1 , 0) (1 , 2)
Number of solutions: 4

Prime: 5
Solution
(0 , 0) (0 , 4) (1 , 0) (1 , 4)
Number of solutions: 4

Prime: 7

Solution

(0 , 0) (0 , 6) (1 , 0) (1 , 6) (4 , 2) (4 , 4) (5 , 1) (5 , 5) (6 , 3)

Number of solutions: 9

Prime: 11

Solution

(0 , 0) (0 , 10) (1 , 0) (1 , 10) (5 , 3) (5 , 7) (7 , 5) (8 , 5) (10 , 4) (10 , 6)

Number of solutions: 10

Prime: 13

Solution

(0 , 0) (0 , 12) (1 , 0) (1 , 12) (2 , 5) (2 , 7) (8 , 2) (8 , 10) (10 , 6)

Number of solutions: 9

Prime: 17

Solution

(0 , 0) (0 , 16) (1 , 0) (1 , 16) (2 , 8) (7 , 7) (7 , 9) (8 , 2) (8 , 14) (9 , 1) (9 , 15) (11 , 4) (11 , 12) (12 , 4) (12 , 12) (13 , 7) (13 , 9) (15 , 7) (15 , 9)

Number of solutions: 19

Prime: 19

Solution

(0 , 0) (0 , 18) (1 , 0) (1 , 18) (2 , 6) (2 , 12) (3 , 7) (3 , 11) (8 , 5) (8 , 13) (9 , 1) (9 , 17) (13 , 9) (14 , 1) (14 , 17) (15 , 8) (15 , 10) (16 , 1) (16 , 17)

Number of solutions: 19

Prime: 23

Solution

(0 , 0) (0 , 22) (1 , 0) (1 , 22) (3 , 10) (3 , 12) (4 , 1) (4 , 21) (6 , 6) (6 , 16) (7 , 10) (7 , 12) (10 , 8) (10 , 14) (12 , 4) (12 , 18) (14 , 10) (14 , 12) (19 , 3) (19 , 19) (20 , 7) (20 , 15) (22 , 9) (22 , 13)

Number of solutions: 24

Prime: 29

Solution

(0 , 0) (0 , 28) (1 , 0) (1 , 28) (5 , 6) (5 , 22) (6 , 2) (6 , 26) (8 , 6) (8 , 22) (10 , 5) (10 , 23) (13 , 7) (13 , 21) (16 , 3) (16 , 25) (17 , 6) (17 , 22) (18 , 7) (18 , 21) (19 , 1) (19 , 27) (20 , 1) (20 , 27) (22 , 8) (22 , 20) (25 , 14) (28 , 7) (28 , 21)

Number of solutions: 29

Prime: 31

Solution

(0 , 0) (0 , 30) (1 , 0) (1 , 30) (4 , 10) (4 , 20) (6 , 7) (6 , 23) (9 , 9) (9 , 21) (10 , 12) (10 , 18) (11 , 12) (11 , 18) (14 , 2) (14 , 28) (16 , 13) (16 , 17) (22 , 13) (22 , 17) (24 , 6) (24 , 24) (25 , 13) (25 , 17)

Number of solutions: 24

Prime: 37

Solution

(0 , 0) (0 , 36) (1 , 0) (1 , 36) (3 , 15) (3 , 21) (7 , 8) (7 , 28) (9 , 7) (9 , 29) (10 , 3) (10 , 33) (12 , 5) (12 , 31) (13 , 5) (13 , 31) (15 , 6) (15 , 30) (17 , 10) (17 , 26) (23 , 4) (23 , 32) (24 , 1) (24 , 35) (27 , 17) (27 , 19) (29 , 9) (29 , 27) (32 , 8) (32 , 28) (35 , 14) (35 , 22) (36 , 8) (36 , 28)

Number of solutions: 34

カウント数

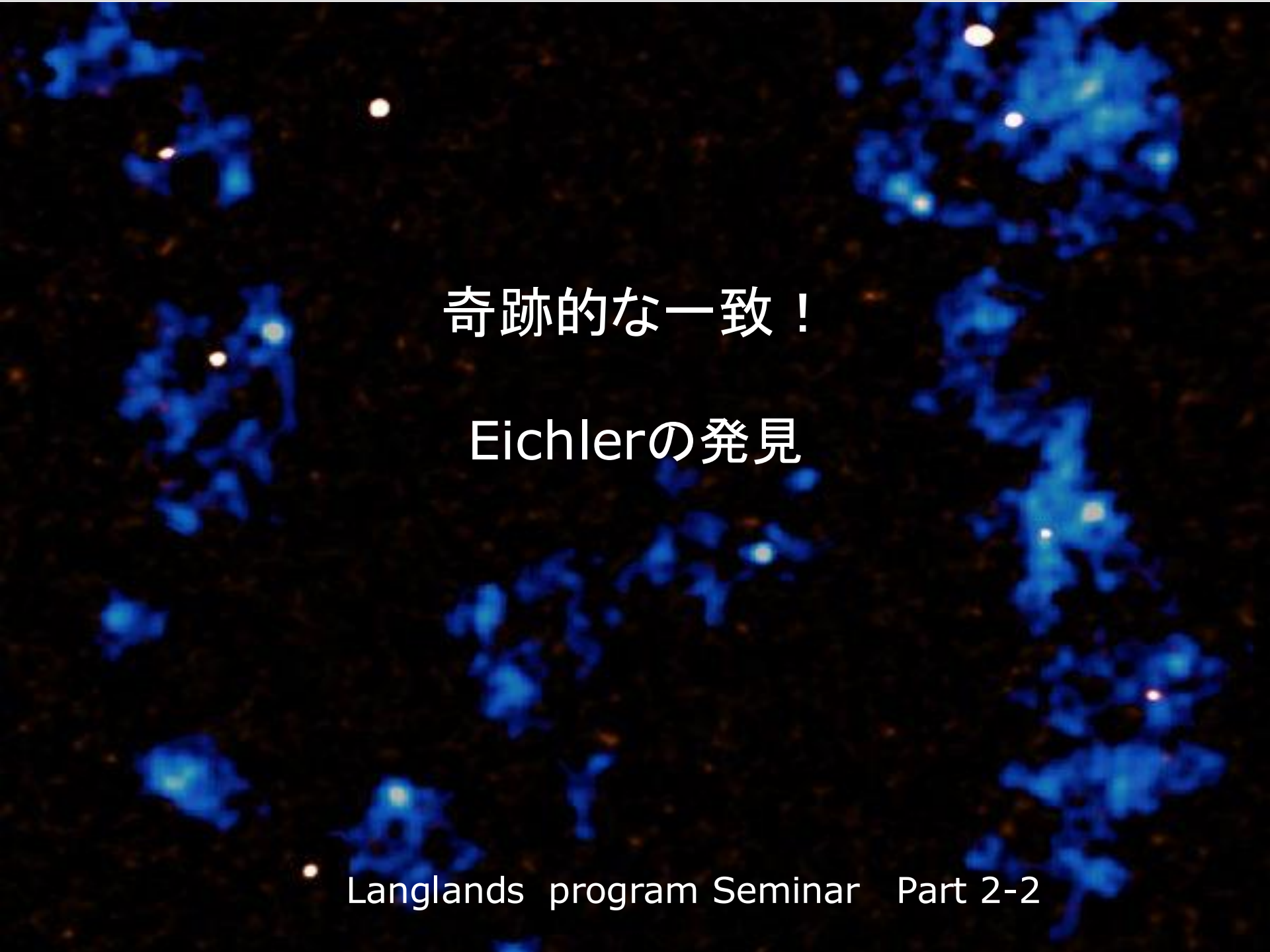
pの値が増えると、整数点の数も増大する。ここでは

カウント数 ＝ p – 整数点の数

と調整して、$a(p)$と表すことにする。

Elliptic Curve: y^2 + y == x^3 - x^2

a(2) = -2
a(3) = -1
a(5) = 1
a(7) = -2
a(11) = 1
a(13) = 4
a(17) = -2
a(19) = 0
a(23) = -1
a(29) = 0
a(31) = 7
a(37) = 3


奇跡的な一致！
Eichlerの発見
Langlands program Seminar Part 2-2

Martin Eichler

アイヒラーと志村五郎は、ある種のモジュラー形式から楕円曲線を構成する方法を開発した。

すべての楕円曲線は対応するモジュラー形式を持つという逆の概念は、後にフェルマーの最終定理を証明する鍵となった。

https://en.wikipedia.org/wiki/Martin_Eichler

There are five fundamental operations in mathematics , addition, subtraction, multiplication, division and modular forms.

-- Martin Eichler

Eichlerが気づいたこと

Eichlerは、ある無限級数の係数を計算する中で、それが楕円曲線と深い関係にあることに気づく。

このセッションでは、Eichlerの驚くべき発見を紹介する。

天下りだが、Eichlerがどのような無限級数の係数を計算したのかを振り返ってみよう。

Eichlerが計算した級数

次のような、qについての無限積の形の式を考える

$$q \cdot (1-q)^2 \cdot (1-q^{11})^2 \cdot (1-q^2)^2 \cdot (1-q^{22})^2 \cdot (1-q^3)^2 \cdot (1-q^{33})^2 \cdot (1-q^4)^2 \cdot (1-q^{44})^2 \cdot (1-q^5)^2 \cdot \cdots\cdots$$

この式には、あるパターンがある。

最初に、この式をよく眺めて、そのパターンを考えてほしい。

次のような、qについての無限積の形の式を考える

$$q\cdot(1-q)^2\cdot(1-q^{11})^2\cdot(1-q^2)^2\cdot(1-q^{22})^2\cdot(1-q^3)^2\cdot$$
$$(1-q^{33})^2\cdot(1-q^4)^2\cdot(1-q^{44})^2\cdot(1-q^5)^2\cdot\cdots\cdots$$

この式には、あるパターンがある。

最初に、この式をよく眺めて、そのパターンを考えてほしい。

この式は、次のようにかける。

$$q \cdot \cdots \cdot \left(1-q^{k}\right)^{2} \cdot \left(1-q^{11k}\right)^{2} \cdot \cdots$$
$$= q \prod_{k=1}^{\infty} \left(1-q^{k}\right)^{2} \cdot \left(1-q^{11k}\right)^{2}$$

こうした積の形を eta product というのだが、それについては今回のセミナーでは触れない。後で見る係数の計算で出てくる「数の分割数」に、それは関係している。

積から和へ

この積の形を和の形にすることを考える。カッコを外していけばいい。

$$q\prod_{k=1}^{\infty}\left(1-q^{k}\right)^{2}\cdot\left(1-q^{11k}\right)^{2}$$

は、20次まで計算すると次のようになる。

$$q-2q^{2}-q^{3}+2q^{4}+q^{5}+2q^{6}-2q^{7}-2q^{9}-2q^{10}+q^{11}-2q^{12}+4q^{13}+4q^{14}-q^{15}-4q^{16}-2q^{17}+4q^{18}+O(q^{20})$$

計算の詳細は、次のページ。

積から和へ
計算少し詳しく (ただし11次まで)

$$q\prod_{k=1}^{\infty}\left(1-q^{k}\right)^{2}\left(1-q^{11k}\right)^{2}$$

$$=q\prod_{k=1}^{\infty}\left(1-q^{k}\right)^{2}\cdot\prod_{k=1}^{\infty}\left(1-q^{11k}\right)^{2}$$

$$=q(1-q)^{2}\cdot(1-q^{2})^{2}\cdot(1-q^{3})^{2}\cdot(1-q^{3})^{2}\cdot(1-q^{4})^{2}\cdots$$
$$\cdot(1-q^{11})^{2}\cdot(1-q^{22})^{2}\cdot(1-q^{33})\cdot(1-q^{44})^{2}\cdot\cdots$$

qの20次までの項の係数の計算なら、次の計算から係数を求めるので十分である。

$$q(1-q)^2 \cdot (1-q^2)^2 \cdot (1-q^3)^2 \cdot (1-q^3)^2 \cdot (1-q^4)^2$$
$$\cdot (1-q^5)^2 \cdot (1-q^6)^2 \cdot (1-q^7)^2 \cdot (1-q^8)^2 \cdot (1-q^9)^2$$
$$\cdot (1-q^{10})^2 \cdot (1-q^{11})^2 \cdot (1-q^{12})^2 \cdot (1-q^{13})^2 \cdot (1-q^{14})^2$$
$$\cdot (1-q^{15})^2 \cdot (1-q^{16})^2 \cdot (1-q^{17})^2 \cdot (1-q^{18})^2 \cdot (1-q^{19})^2$$
$$\cdot (1-q^{20})^2$$
$$\cdot (1-q^{11})^2 \cdot (1-q^{22})^2 \cdot (1-q^{33}) \cdot (1-q^{44})^2 \cdot \dots$$

$$q(1-q)^2\cdot(1-q^2)^2\cdot(1-q^3)^2\cdot(1-q^4)^2$$
$$\cdot(1-q^5)^2\cdot(1-q^6)^2\cdot(1-q^7)^2\cdot(1-q^8)^2\cdot(1-q^9)^2$$
$$\cdot(1-q^{10})^2\cdot(1-q^{11})^2\cdot(1-q^{12})^2\cdot(1-q^{13})^2\cdot(1-q^{14})^2$$
$$\cdot(1-q^{15})^2\cdot(1-q^{16})^2\cdot(1-q^{17})^2\cdot(1-q^{18})^2\cdot(1-q^{19})^2$$
$$\cdot(1-q^{20})^2\cdot(1-q^{11})^2$$

q^1の係数　　1

q^2の係数　　$(1-q)^2$の $-2q$ から -2

q^3の係数　　$(1-q)^2$のq^2から 1;

$(1-q^2)^2$の $-2q^2$から-2;

あわせて $1+(-2)=-1$

q^4の係数　　$(1-q)^2(1-q^2)^2$の$-2q\cdot-2q^2=4q^3$から 4

$(1-q^3)^2$の $-2q^3$から -2

あわせて $4+(-2)=2$

$(1-q^k)^2$をk項と呼ぼう

$$q(1-q)^2\cdot(1-q^2)^2\cdot(1-q^3)^2\cdot(1-q^4)^2$$
$$\cdot(1-q^5)^2\cdot(1-q^6)^2\cdot(1-q^7)^2\cdot(1-q^8)^2\cdot(1-q^9)^2$$
$$\cdot(1-q^{10})^2\cdot(1-q^{11})^2\cdot(1-q^{12})^2\cdot(1-q^{13})^2\cdot(1-q^{14})^2$$
$$\cdot(1-q^{15})^2\cdot(1-q^{16})^2\cdot(1-q^{17})^2\cdot(1-q^{18})^2\cdot(1-q^{19})^2$$
$$\cdot(1-q^{20})^2\cdot(1-q^{11})^2$$

q^5の係数

1項・2項の $q^2\cdot -2q^2=-2q^4$ から -2

1項・3項の $-2q\cdot -2q^3=4q^4$ から 4

2項の q^4 から 1

4項の $-2q^4$ から -2

あわせて $(-2)+4+1+(-2)=1$

$$q(1-q)^2\cdot(1-q^2)^2\cdot(1-q^3)^2\cdot(1-q^4)^2$$
$$\cdot(1-q^5)^2\cdot(1-q^6)^2\cdot(1-q^7)^2\cdot(1-q^8)^2\cdot(1-q^9)^2$$
$$\cdot(1-q^{10})^2\cdot(1-q^{11})^2\cdot(1-q^{12})^2\cdot(1-q^{13})^2\cdot(1-q^{14})^2$$
$$\cdot(1-q^{15})^2\cdot(1-q^{16})^2\cdot(1-q^{17})^2\cdot(1-q^{18})^2\cdot(1-q^{19})^2$$
$$\cdot(1-q^{20})^2\cdot(1-q^{11})^2$$

q^6の係数

1項・2項の $-2q\cdot q^4=-2q^5$ から -2

1項・3項の $q^2\cdot-2q^3=-2q^5$ から -2

1項・4項の $-2q\cdot-2q^4=4q^5$ から 4

2項・3項の $-2q^2\cdot-2q^3=4q^5$ から 4

4項の $-2q^4$ から -2

あわせて $(-2)+(-2)+4+4+(-2)=2$

$$q(1-q)^2\cdot(1-q^2)^2\cdot(1-q^3)^2\cdot(1-q^4)^2$$
$$\cdot(1-q^5)^2\cdot(1-q^6)^2\cdot(1-q^7)^2\cdot(1-q^8)^2\cdot(1-q^9)^2$$
$$\cdot(1-q^{10})^2\cdot(1-q^{11})^2\cdot(1-q^{12})^2\cdot(1-q^{13})^2\cdot(1-q^{14})^2$$
$$\cdot(1-q^{15})^2\cdot(1-q^{16})^2\cdot(1-q^{17})^2\cdot(1-q^{18})^2\cdot(1-q^{19})^2$$
$$\cdot(1-q^{20})^2\cdot(1-q^{11})^2$$

q^7の係数

1項・2項の $q^2\cdot q^4=q^6$ から 1

1項・2項・3項の $-2q\cdot-2q^2\cdot-2q^3=-8q^6$ から -8

1項・4項の $q^2\cdot-2q^4=-2q^6$ から -2

1項・5項の $-2q\cdot-2q^5=4q^6$ から 4

2項・4項の $-2q^2\cdot-2q^4=4q^6$ から 4

3項の q^6 から 1

6項の $-2q^6$ から -2

あわせて $1+(-8)+(-2)+4+4+1+(-2)$

$=$ *-2*

Modular Form

こうして得られた式

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + O(q^{20})$$

を、Modular Form という。

Modular Form

Modular form function

$$f(q) = \sum_{n=0}^{\infty} a_n q^n$$

$q = e^{2\pi i z}$として $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$

$\mathfrak{H} = \{z \in \mathbf{C} : \mathrm{im}(z) > 0\}$. Weight 2 modular forms:

複素平面の上半面

$$f : \mathfrak{H} \to \mathbf{C} : f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z) \text{ for}$$

整数からなる2×2の行列 $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) : c \equiv 0\,(N) \right\}$

Modular Form

こうして得られた式

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + O(q^{20})$$

を、Modular Form という。

この式の、素数乗の項とその係数に注目してほしい。

Modular Form

こうして得られた式

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + O(q^{20})$$

を、Modular Form という。

この式の、素数乗の項とその係数に注目してほしい。

素数p乗の項の係数をb(p)と表すと、次のようになる。

b(2) = -2
b(3) = -1
b(5) = 1
b(7) = -2
b(11) = 1
b(13) = 4
b(17) = -2
b(19) = 0

実は、これと全く同じ数字の並びを、我々は以前に見ているのだ。

それは、楕円曲線 $y^2 + y = x^3 - x^2$ の整数点をカウントした時だ。

この楕円曲線の有限体 $\mathbb{F}_p$ での整数点を数えるプログラムの出力を振り返ってみよう。

楕円曲線上の
整数点を数える

a(2) = -2
a(3) = -1
a(5) = 1
a(7) = -2
a(11) = 1
a(13) = 4
a(17) = -2
a(19) = 0

Modular Form
の係数

b(2) = -2
b(3) = -1
b(5) = 1
b(7) = -2
b(11) = 1
b(13) = 4
b(17) = -2
b(19) = 0

Eichlerが発見したこと

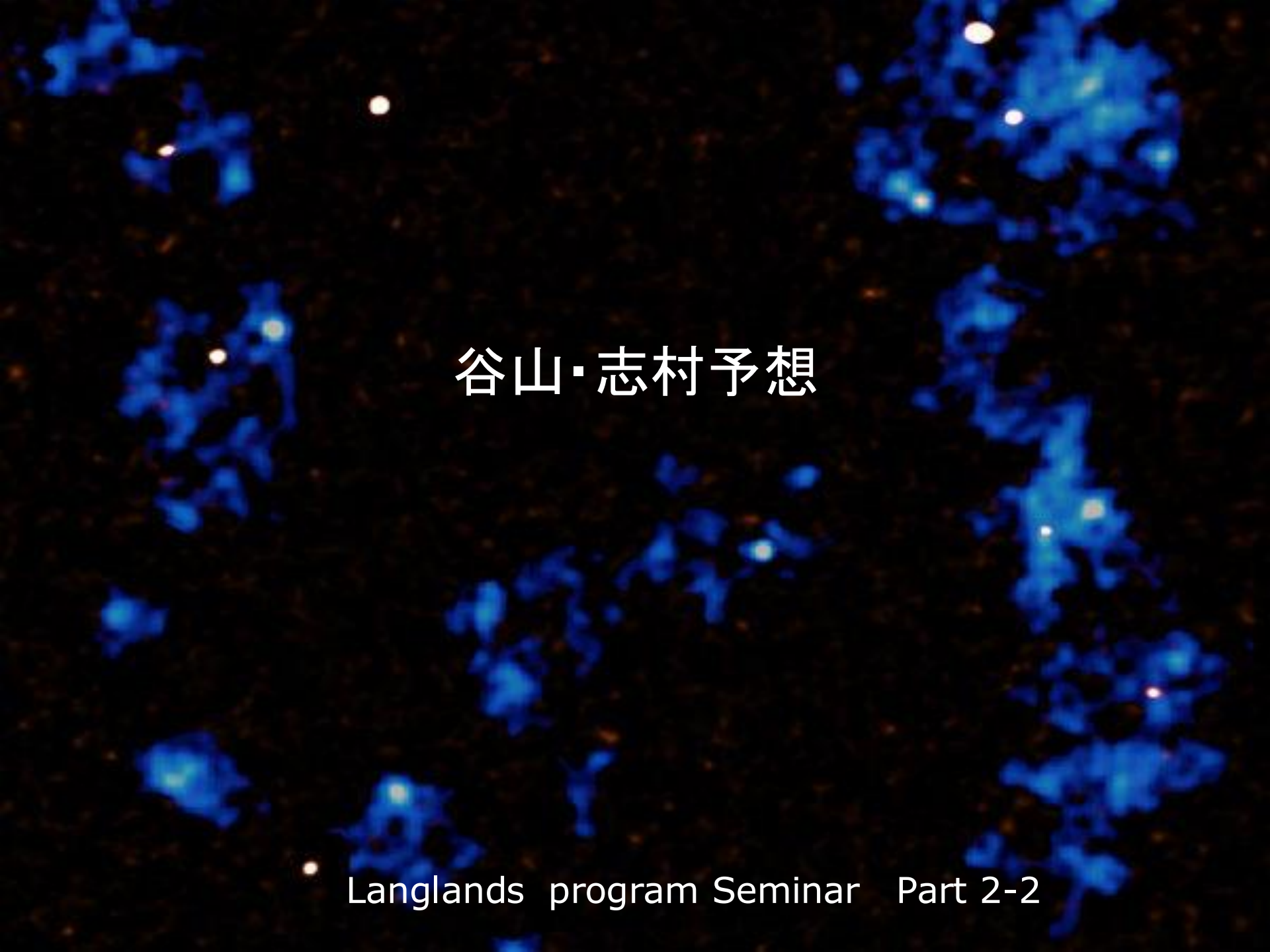
Eichlerは、楕円曲線 $y^2 + y = x^3 - x^2$の整数点の数が、
Modular form

$$q\prod_{k=1}^{\infty}\left(1-q^k\right)^2\cdot\left(1-q^{11k}\right)^2$$

$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + \cdots$$

の係数と、正確に対応していることを発見したのである。

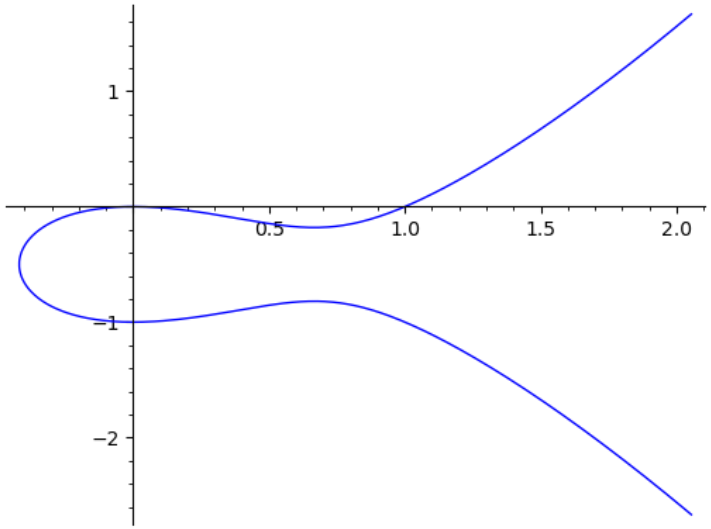
なんと不思議な関係なのだろう！


谷山･志村予想
Langlands program Seminar Part 2-2

Eichlerが発見したこと

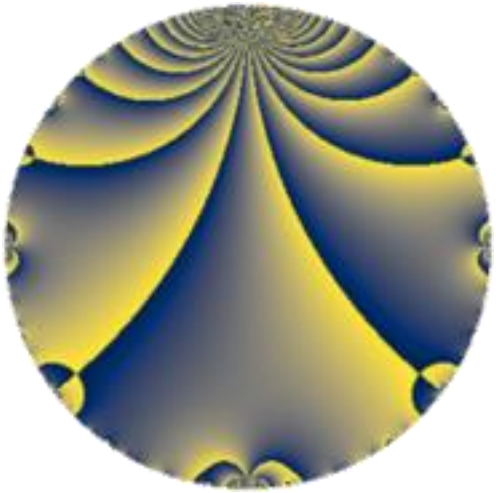
楕円曲線

$$y^2 + y = x^3 - x^2$$



Modular Form

$$q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$$



両者は、展開されたmodular form

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + \cdots$$

の係数を通じて、つながっている。

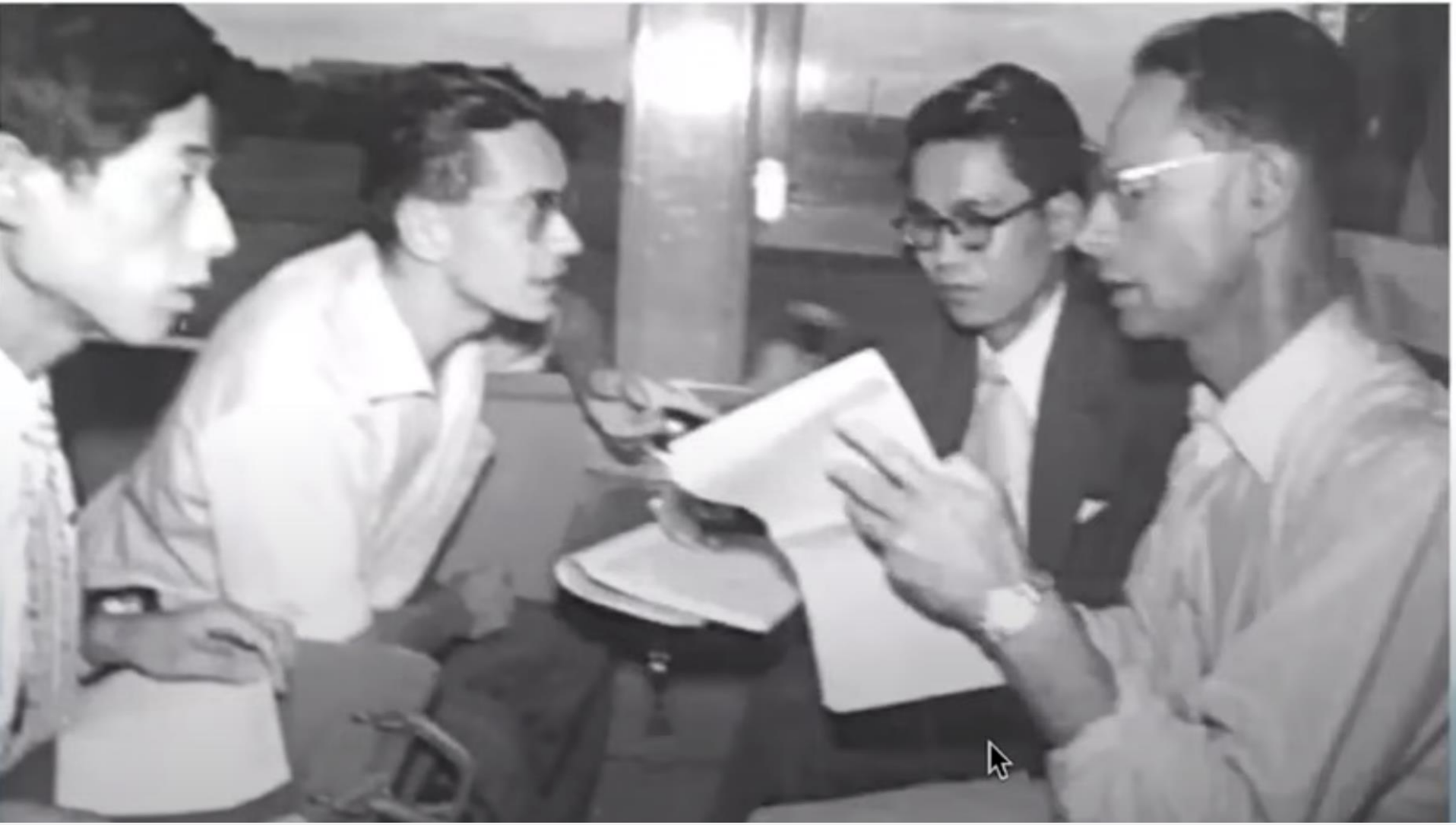
楕円曲線上の
整数点を数える

a(2) = -2
a(3) = -1
a(5) = 1
a(7) = -2
a(11) = 1
a(13) = 4
a(17) = -2
a(19) = 0

Modular Form
の係数

b(2) = -2
b(3) = -1
b(5) = 1
b(7) = -2
b(11) = 1
b(13) = 4
b(17) = -2
b(19) = 0

1955年 「代数的整数論に関する国際会議」 東京・日光



志村五郎　　**Jean-Pierre Serre**　　谷山豊　　**André Weil**

谷山･志村予想

それは、大雑把にいうと Eichlerの発見を一般化したもので、「有理数体上の楕円曲線はモジュラー形式と特別な関係がある。」というものである。

この予想は、2001年に、Richard Taylor, Christophe Breuil らによって証明された。

https://www.ams.org/journals/jams/2001-14-04/S0894-0347-01-00370-8/viewer/

現在では「予想」ではなく、「モデュラリティ定理 modularity theorem」と呼ばれている。

Modularity theorem

Theorem A. *If $E_{/\mathbf{Q}}$ is an elliptic curve, then E is modular.*

有理数体上の任意の楕円曲線は、ある整数Nに対して古典モジュラー曲線X0(N)から整数係数を持つ有理写像を介して得ることができる。

この写像はレベルNのmodular parametrizationと呼ばれる。

もしNが、そのようなparametrizationを見つけることができる最小の整数であるならば、（モジュラー性の定理自体によって、これは現在、conductorと呼ばれる数であることが知られている）parametrizationは、重み2とレベルNの特定の種類のモジュラー形式、整数q展開を持つ正規化new formによって生成される写像の観点から定義することができる。

Wilesの貢献

「1990年代初頭の時点では、ほとんどの数学者は谷山・志村予想は証明できないと信じていた。

しかし、A.Wilesはそうではなかった。彼は楕円曲線の集合とモジュラー楕円曲線の集合の対応関係を、それぞれの数が同じであることを示すことによって確立しようとした。

ワイルズはガロア表現を「数え」、モジュラー形式の数と比較することでこれを達成した。1993年、Wilesは7年に及ぶ途方もない努力の末、semistable elliptic curvesと呼ばれる特殊な曲線のクラスについて谷山-志村予想を（ほぼ）証明した（これはsquarefree conductorsを持つ楕円曲線に対応する; Knapp 1999）。」

Weisstein, Eric W. “Taniyama–Shimura Conjecture”. MathWorld. https://mathworld.wolfram.com/Taniyama-ShimuraConjecture.html

楕円曲線とModular formとの対応について
具体的なサンプル

Eichlerの「奇跡的な発見」のあと、多くの人が楕円曲線とModular formの対応の研究に加わった。

「谷山・志村予想」の背景には、こうした関心の大きな広がりがあった。

今回のセッションの後半では、初等的な方法で確かめることのできる、楕円曲線とModular formとの対応についての具体的なサンプルを、一つ紹介しようと思う。

ここで取り上げているのは、

Modular form

$$q\prod_{n=1}^{\infty}(1-q^{n})(1-q^{2n})(1-q^{7n})(1-q^{14n})$$

と、楕円曲線

$$y^2 + xy + y = x^3 - x$$

の対応である。

興味のある方は、自分の手で確認してほしい。

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$$

の係数を計算する。

qの係数	1項の 1; 1
q^2の係数	1項の $-q$; -1
q^3の係数	2項の $-q^2$; -2
q^4の係数	1項·2項の $-q\cdot-q^2$; 1
q^5の係数	1項の $-q^4$; -1
	2項の $-q^4$; -1
	1項·1項の $-q\cdot-q^3$; 1
	1項·2項の $-q^2\cdot-q^2$; 1
	あわせて 1＋(ー1) 0

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$$

α: 1 2 3 4 5 6 7 8 9 10 11 12 13 ⋯

β: 2 4 6 8 10 12 14 16 18 20 22 24 26 ⋯

γ: 7 14 21 28 ⋯ ⋯

δ: 14 28 ⋯ ⋯

係数が小さいところだけを考える

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$$

α:	1	2	3	4	5	6	7	8	9	10	11	12	13 …
β:	2	4	6	8	10	12	14	16	18	20	22	24	26 …
γ:	7	14	21	28	…	…							
δ:	14	28	…	…									

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$$
$$= q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 + \cdots$$

b(2) = -1
b(3) = -2
b(5) = 0
b(7) = 1
b(11) = 0

この級数

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$$

$$= q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 + \cdots$$

に対応する楕円曲線が存在する。

簡単なプログラムで、楕円曲線

$$y^2 + xy + y = x^3 - x$$

の整数点をカウントしてみよう。

```
def my_loop2xy():

    print("楕円曲線: ", "y^2 + x*y + y == x^3 - x")
    p_loop = [2,3,5,7,11,13]
    for p in p_loop:
      solutions = []

      for x in Zmod (p):
          for y in Zmod (p):
              if y^2 + x*y + y == x^3 - x:
                  solutions.append((x, y))

      print(" ")
      print("素数 p =:", p)
      print("有限体 F_p 上の整数点")

      for x, y in solutions:
           print("(", x, ",", y, ")" , end = " ")

      n_of_sol = len(solutions)
      print("\n整数点の数: ", n_of_sol )
      print("カウント数: ", p - n_of_sol )
```

楕円曲線: y^2 + x*y + y == x^3 - x

素数 p =: 2
有限体 F_p 上の整数点
(0 , 0) (0 , 1) (1 , 0)
整数点の数: 3
カウント数: -1

素数 p =: 3
有限体 F_p 上の整数点
(0 , 0) (0 , 2) (1 , 0) (1 , 1) (2 , 0)
整数点の数: 5
カウント数: -2

素数 p =: 5
有限体 F_p 上の整数点
(0 , 0) (0 , 4) (1 , 0) (1 , 3) (4 , 0)
整数点の数: 5
カウント数: 0

素数 p =: 7

有限体 F_p 上の整数点

(0 , 0) (0 , 6) (1 , 0) (1 , 5) (3 , 5) (6 , 0)

整数点の数: 6

カウント数: 1

素数 p =: 11

有限体 F_p 上の整数点

(0 , 0) (0 , 10) (1 , 0) (1 , 9) (2 , 4) (4 , 8) (4 , 9) (6 , 6) (6 , 9) (7 , 7) (10 , 0)

整数点の数: 11

カウント数: 0

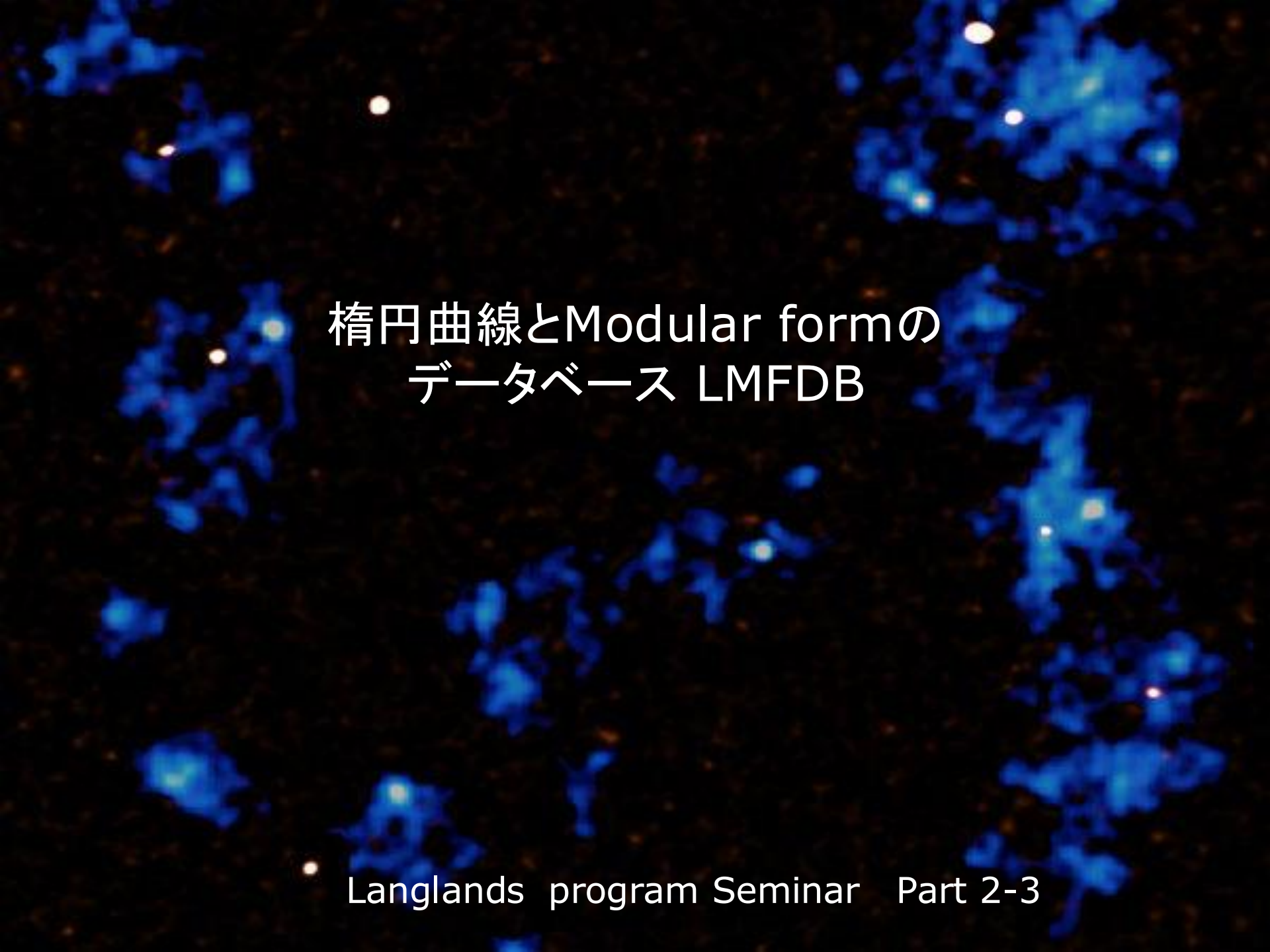
楕円曲線 $y^2 + xy + y = x^3 - x$ の整数点のカウント

a(2) = -1
a(3) = -2
a(5) = 0
a(7) = 1
a(11) = 0
a(13) = -4

楕円曲線とModular formとの対応

$y^2 + xy + y = x^3 - x$ の場合

a(2) = -1	b(2) = -1
a(3) = -2	b(3) = -2
a(5) = 0	b(5) = 0
a(7) = 1	b(7) = 1
a(11) = 0	b(11) = 0
a(13) = -4	b(13) = -4


楕円曲線とModular formの
データベース LMFDB
Langlands program Seminar Part 2-3

楕円曲線とModular formの
データベース LMFDB

このセッションでは、楕円曲線とModular formのデータベースであるLMFDBを紹介しようと思う。

The LMFDB Collaboration,
The L-functions and modular forms database,
https://www.lmfdb.org

正確にいうと、楕円曲線ではなく、L-function と modular formsのデータベースなのであるが、L-function については、次回のセミナーで扱うことにする。

LMFDB

⌂

Citation · Feedback · Hide Menu

The L-functions and modular forms database (LMFDB)

Introduction

Overview Random

Universe Knowledge

L-functions

Rational All

Modular forms

Classical Maass

Hilbert Bianchi

Varieties

Elliptic curves over $\mathbb{Q}$

Elliptic curves over $\mathbb{Q}(\alpha)$

Genus 2 curves over $\mathbb{Q}$

Higher genus families

Abelian varieties over $\mathbb{F}_q$

Fields

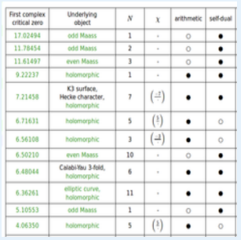
Number fields

p-adic fields

Representations

Dirichlet characters

A database

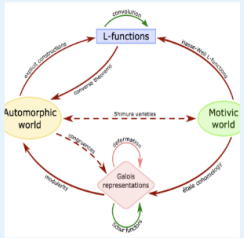


The LMFDB is a database of mathematical objects arising in number theory and arithmetic geometry that illustrates some of the mathematical connections predicted by the Langlands program.

Click a heading on the left to browse, or go to a random page.

今回は、最初にここを開くといい。

Learn more



Information is available regarding the source, reliability, and completeness of the database.

Knowls provide explanations when you need them.

Overview LMFDB universe Knowledge Data

Announcements

The first LuCaNT conference took place July 10-14, 2023 at ICERM. Thanks to everyone who attended! Conference proceedings will be published soon.

Check out the recently updated abstract groups database [beta].

Check out the new modular curves database [beta].

Citations and acknowledgments

- How to cite the LMFDB
- Source code repository
- Editorial board
- Acknowledgments

https://www.lmfdb.org/

これまでのセッションで見てきたこと

これまでのセッションで、具体的には二つの楕円曲線

$$y^2 + y = x^3 - x^2$$
$$y^2 + xy + y = x^3 - x^2$$

を取り上げて、それぞれが次のようなmodular formと対応関係にあることを見てきた。

$$q\prod_{k=1}^{\infty}\left(1-q^k\right)^2\cdot\left(1-q^{11k}\right)^2$$

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$$

ただ、今回のセミナーでとったその対応関係の確認の仕方は、無限積の形のmodular formを展開してその係数を得て、それを楕円曲線の整数点の数と比較するというものだった。

q^{11}の係数の計算のような次数の低い項の係数でも、手間がかかる。振り返ってみると、セッションの少ない時間を、その計算に当てている。

それに「対応する」という楕円曲線の選択も天下りだった。

こうした問題は、どのように解決されたのだろう？

時間とともに進む認識

これまでのセッションで、すでに繰り返し述べてきたことだが、楕円曲線とmodular form との対応関係については、時間と共に我々の認識は、進んできた。

- Eichlerによる最初の対応の発見
- 多くの数学者による多くの対応の発見
- 「すべての楕円曲線はmodularである」という谷山・志村予想の成立
- …
- …
- WilesらのグループによるModularity Theoremの証明（谷山・志村予想」の解決）

LMFDBとは何か？

LMFDBは、ある意味で言うと、さきの「多くの数学者による多くの対応の発見」をまとめたデータベースである。

もっとも、そうしたまとめはLMFDBの特徴づけとしては正確なものではない。

なぜなら、現代では、「楕円曲線とmodular formとの対応」は、Modularity Theoremですでに証明済みの数学的事実だからだ。わざわざ、それをデータベースで確認する必要はない。

Langlands ProgramとLMFDB

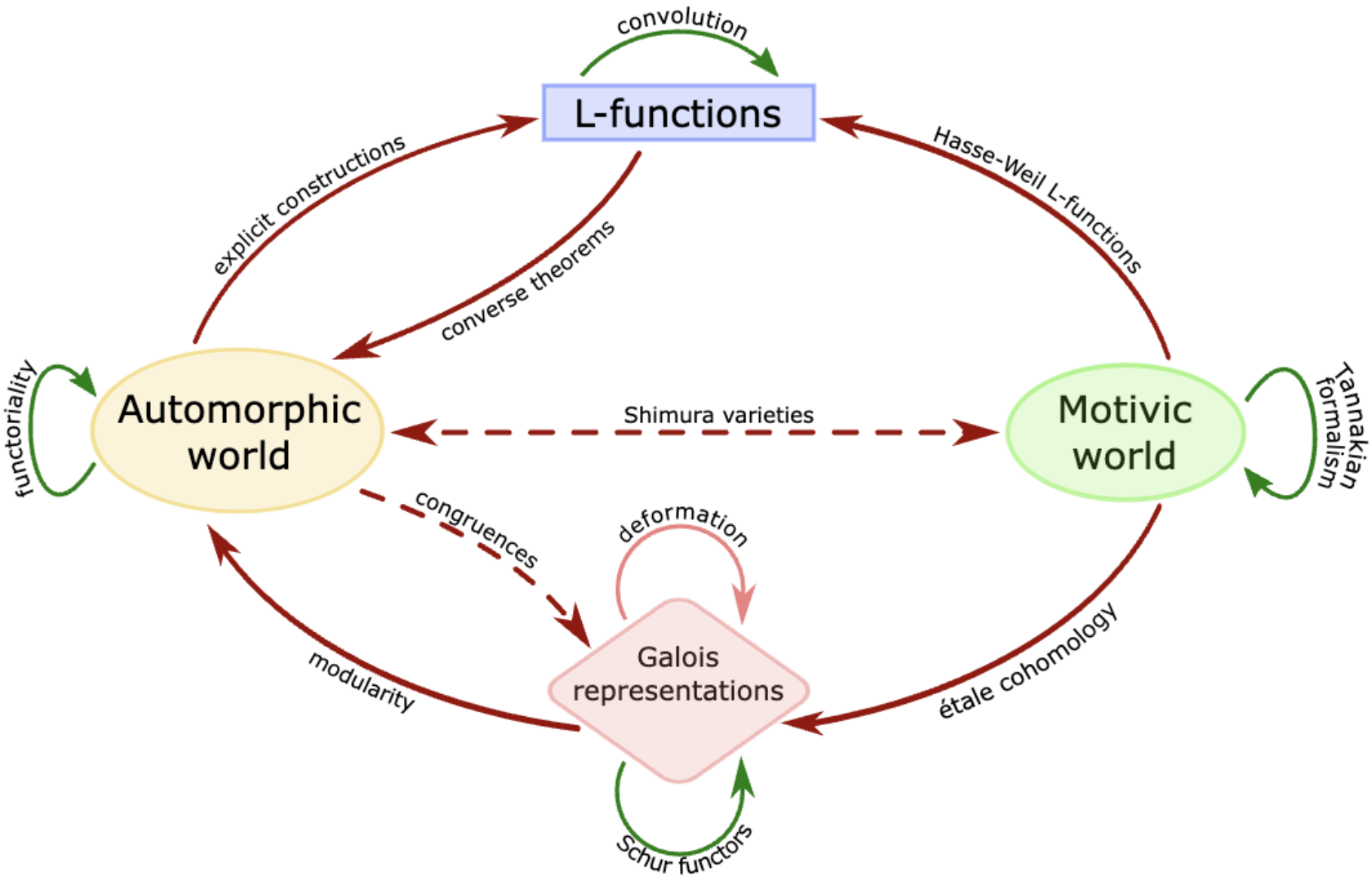
現代の数学者がLMFDBを参照する動機の一つは、Langlands Programに深く関係している。

LMFDB全体の概念構成を示した、LMFDB Universe という図（次のページ）には、次のようなコメントがある。

「図の上半分はLanglands programに基づくもので、Motivic世界のオブジェクトは、L関数を介してAutomorphic世界のオブジェクトに対応することを予言している。」

残念ながら、今回のセミナーでは、こうした話題に深入りすることはできない。

LMFDB Universe



LMFDBを見る一つの楽しみ
日本人数学者の活躍

本題からはまったく外れるのだが、LMFDBを見る一つの楽しみは、いろんなところに日本人数学者の名前がみれることである、

先の図でも、左側の「Automorphic World」と右側の「Motivic World」を直接結んでいる “Shimura varieties”の “Shimura”は志村五郎のことである。

ちょっとわかりにくいが、「Motivic World」の “Tannakian formalism” の “Tannakian” は淡中忠郎のことである。

他にももっとたくさんある。日本人数学者が、大きな活躍をしてきたことがよくわかる。


HITACHI
危い!

「ラングランズ・プログラム」とは何か？

Part 3

Langlands Programの創世記

Part 3 Langlands programの創世記

セミナーのPart 3は、Langlands programの紹介です。ただし、1970年代から現代に至るその膨大なprogramの展開 と広いリーチを満遍なく説明することは、僕の手に余ります。

The Work of Robert Langlands

Introduction

Robert P. Langlands was born in New Westminster, British Columbia, in 1936. He graduated from the University of British Columbia with an undergraduate degree in 1957 and an M.Sc. in 1958, and from Yale University with a Ph.D. in 1960. He has held faculty positions at Princeton University and Yale University, and is currently a Professor Emeritus at the Institute for Advanced Study in Princeton, New Jersey. He has won several awards recognizing his outstanding contributions to the theory of automorphic forms.

With the intention that the works be published eventually, perhaps posthumously if there is still an audience, Robert Langlands's papers and some of his correspondence and lectures are being collected on this site in a uniform format. This site has absorbed an earlier site created by Bill Casselman and most of the comments not directly attributed to Langlands himself are from Casselman's pen. The collection of papers is essentially complete; letters will be added as they turn up. The young Langlands made no systematic effort to retain copies of his correspondence.

This material is being put into TEX at the Institute for Advanced Study in Princeton, New Jersey and will appear here as it becomes ready. We would like to thank Alice Garber, Dorothea Phares, Marietta Chiorello, Elly Gustafsson, Michelle Huguenin, and Carol Warfield of the present and former staff at the Institute, as well as Mark Goresky, for helping with this project. Above all we thank Bill Casselman for the initial suggestion, for a good deal of the original work, and for continuing advice. At present Anthony Pulido is responsible for the site. Questions and comments should be addressed to him.

https://publications.ias.edu/rpl/

The Work of Robert Langlands

1. Ph.D. thesis
2. Representation theory of real groups
3. Eisenstein series and automorphic forms
4. Functoriality
5. First tests and first consequences of functoriality
6. Base change
7. Endoscopy
8. Beyond endoscopy
9. Shimura varieties
10. Percolation
11. Mathematical physics
12. The geometric theory
13. Miscellaneous
14. Letters
15. Informal material
16. Visual material

Bibliography [pdf]

「Langlands programの創世記」は、どういう時代だったのか

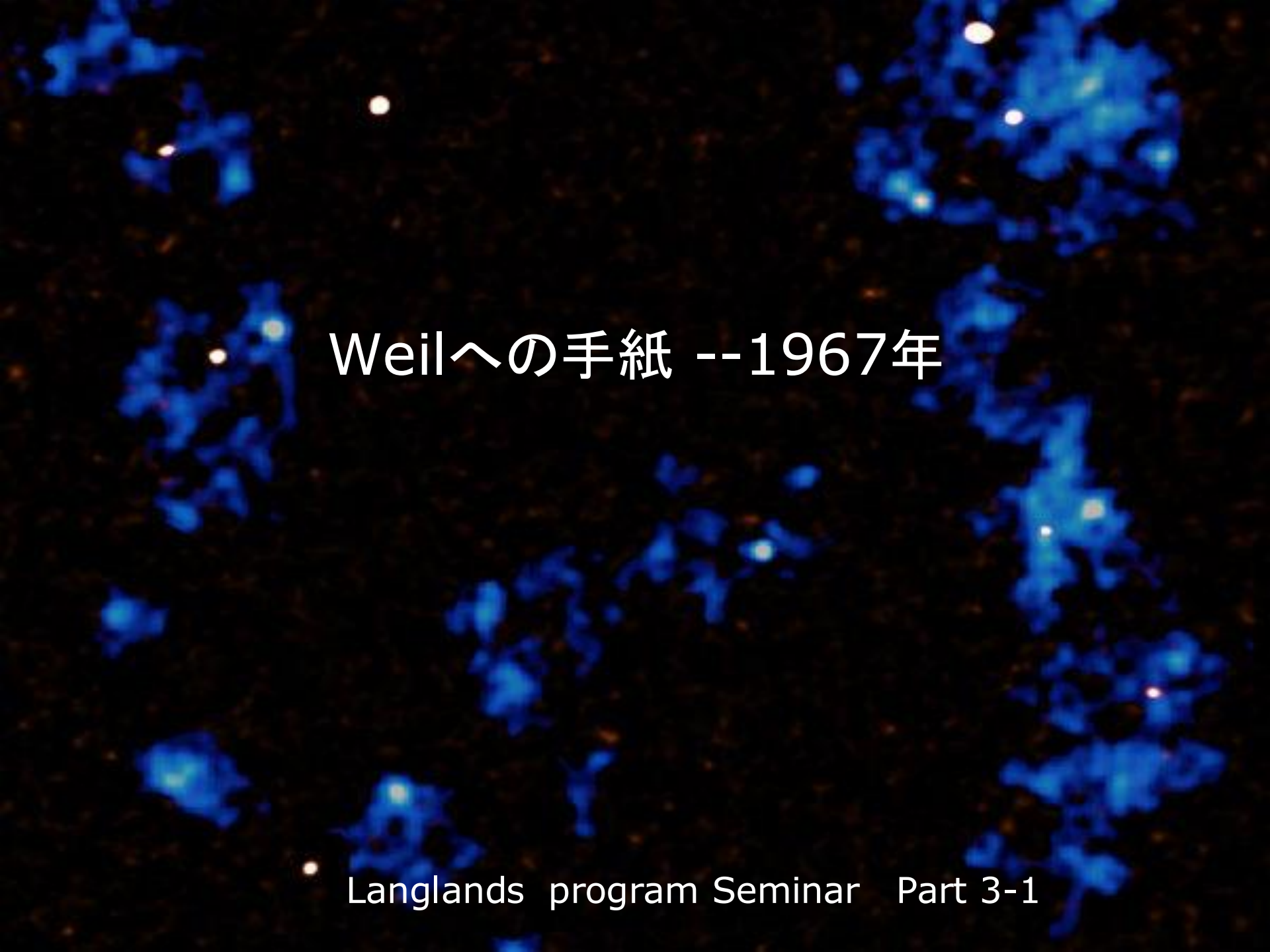
今回のセミナーでは、その最も最初期のビジョンを、振り返ってみようと思います。

ただ、Langlands program の「最初期」といっても、それは数学的には高度に完成されたものでした。その意味を数学的にきちんと伝えることは、難しいのです。

このPart 3 では、数学的には初等的に説明可能なオイラー積の導出と、この「Langlands programの創世記」は、 どういう時代だったのかをエピソードを中心にお話ししたいと思います。

Part 3
Langlands programの創世記
Agenda

1. Weilへの手紙 --1967年
2. Eulerが考えたこと -- Euler product
3. Grothendieck – 1965年


Weilへの手紙 --1967年
Langlands program Seminar Part 3-1

Langlands Program の始まり

1967年1月、当時無名だったラングランズは、高名な数学者アンドレ・ヴェイユに手書きの手紙を書く。

https://publications.ias.edu/sites/default/files/handwritten-ltw_rpl_3.pdf

このラングランズの手紙は、後に「ラングランズ予想」として知られることになる数学における、一連の深い予想の最初の定式化を示している。

Langlands Programは、このヴェイユへの手紙からはじまる。

Professor Weil:

In response to your invitation to come and talk I wrote the ~~following~~ enclosed letter. After I wrote it I realized there was hardly a statement in it of which I was certain. If you are willing to read it as pure speculation I would appreciate that; if not — I am sure you have a waste basket handy.

Yours truly,
R Rayleen

If you are willing to read it as pure speculation I would appreciate that; if not — I am sure you have a waste basket handy."

もし、あなたが、この手紙を純粋な思索として読んでいただけるなら、ありがたいです。
もしそうでないなら、あなたはきっと近くにゴミ箱を用意していることでしょう。

この手紙は、公開以来、整数論、数論的代数幾何、群の表現論といった数学の分野に大きな影響を与え、一見無関係に見える数学のいくつかの分野が、実は深く絡み合っていることを明らかにした。

ラングランズは、異なる分野の数学的対象間の驚くべきつながりを提案し、数論、表現論、保型形式の分野に革命をもたらした。

300年以上未解決だった「フェルマーの最終定理」は、1994年に**アンドリュー・ワイルズによって証明されるのだが、そこでは、ラングランズの予想が重要な役割を果たした。**

それについては、今回のセミナーのPart 4で触れようと思う。

Langlands Programの「創世記」

Julia Muellerは、この手紙をLanglands予想の「創世記」として、その内容を次の二点に要約している。

- 新しいAutomorphic L-functionの発見
- ”Functoriarity”予想

以下、その要約を紹介しよう。

“On the Genesis of Robert P. Langlands’ Conjectures and his Letter to Andre Weil”
https://www.ams.org/journals/bull/2018-55-04/S0273-0979-2018-01609-1/supplementary-information/S0273-0979-2018-01609-1-original-version.pdf

Langlandsの
新しいAutomorphic L-functionの発見

「(1) Automorphic Representation -- 保型表現(およびいくつかの付加的な表現論的データ)に付随するAutomorphic L-function -- 保型L-関数 についての一般的な包括的な概念の発見。

これは、ヘッケのL-関数とアルティンのL-関数を同時に一般化するものである。このような一般化は、1936年のヘッケの研究以来、手の届かないものとなっていた。

Automorphic Representation -- 保型表現とL-functionの両方を支えるL-群(およびその双対群)の概念は、ラングランズがAutomorphic L-function -- 保型L関数を発見する上で決定的な要因となった。」

Functoriarity予想
Reciprocity Lawの拡大

「(2) The Principal of Functoriarity -- 関手原理と Principal of nonabelian class field theory -- 非可換類体論の原理は、予想ではあるが、L-群が適切な作用素の概念を介して関連しているグループ上のAutomorphic Representation -- 保型表現の間の関係を説明している。

さらに、Functorial Conjecture -- 関手性予想の特別なケースは、Artinのabelian reciprocity law -- アーベル相互法則を一般化し、Artinの非アーベル体拡大における reciprocity conjecture -- 相互法則予想を予想ではあるが主張しており、これは、非アーベル類体論の一般的な定式化と見なすことができる。」

二つのトピックの関連 について
Langlandsのautomorphic L-関数の特徴

「トピック（2）はトピック（1）と関連しており、ほぼ同時に発見された。

ラングランズが発見したautomorphic L-関数 L (s, π, ρ) は、automorphic representation π に依存するだけでなく、正規に関連付けられた双対群すなわちL-群の有限次元の補助表現 ρ にも依存する。」

(a) $L_p(s, \pi_p, \rho_p) = [\det(1 - \rho_p(c(\pi_p))p^{-s}]^{-1}$, p unramified.
(b) $L(s, \pi, \rho) = \prod_p L_p(s, \pi_p, \rho_p) = \prod_p [\det(1 - \rho_p(c(\pi_p))p^{-s}]^{-1}$, which verges in some right half-plane.

「ラングランズは当初、自身のL関数をArtin-Hecke級数と名付けたが、これはρとπの表現を通じて、これら2つのL-関数を単一の定義に大幅に一般化したためである。

これは、ラングランズのL-関数がArtinのL-関数に類似したオイラー積として定義されており、したがって本質的には算術的であるが、解析的特性も備えており、それはHeckeのL-関数により近いものである。

代数と解析学を組み合わせたこの独特な特徴は、ラングランズのL-関数において中心的な役割を果たしている。」

$$L(s,\pi,\rho)=\prod_{p}\frac{1}{\det\left(1-\frac{\rho_p(c(\pi_p))}{p^s}\right)}$$

Suppose we have an automorphic form ϕ on $\bar{G}_{\mathbb{Q}} \backslash \bar{G}_{\mathbb{A}}$ which is an eigenfunction of the Hecke algebra for almost all p. Then, for almost all p, we have a homomorphism of the Hecke algebra into the complex numbers and thus a semi-simple conjugacy class α_p in $\mathcal{O}_p \backslash^{L}G \subseteq \mathcal{O} \backslash^{L}G$. If π is a complex representation of $\mathcal{O} \backslash^{L}G$ define the Artin-Hecke L series as

$$L(s,\pi,\phi) = \prod_p \frac{1}{\det\left(1 - \frac{\pi(\alpha_p)}{p^s}\right)}$$

(Product is taken over almost all p)

$$L(s,\pi,\phi) = \prod_p \frac{1}{\det\left(1 - \frac{\pi(\alpha_p)}{p^s}\right)}$$

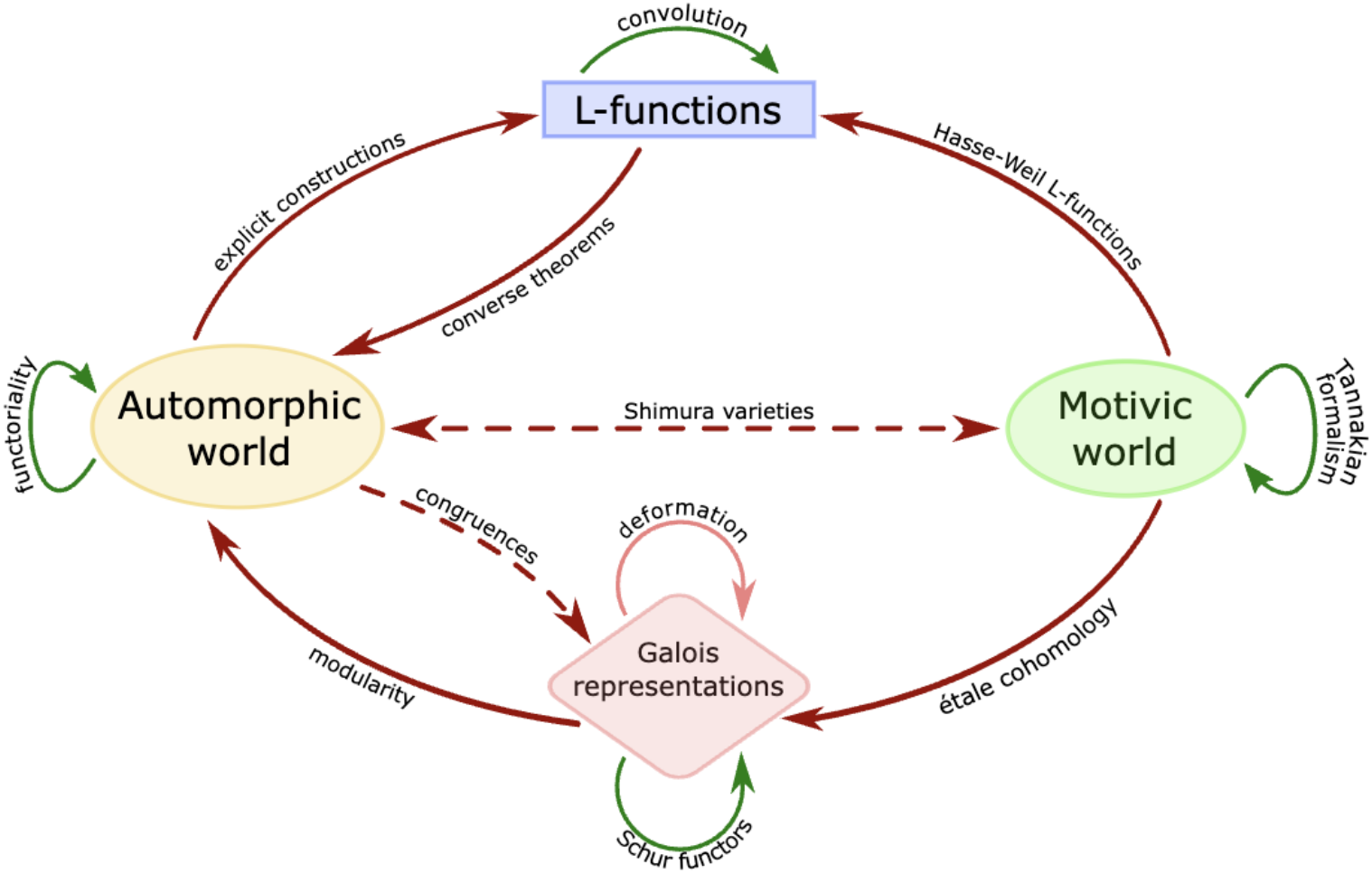
https://publications.ias.edu/sites/default/files/letter-to-weil-1967-01_rpl_3.pdf

LanglandsからWeilへの質問

The first question is whether or not these products define functions meromorphic in the entire complex plane with poles of the usual type and whether or not for each φ there is an automorphic form ψ so that $L(s,\varphi,\pi)/L(s,\psi,\bar{\pi})$ is an elementary function for all π. $\bar{\pi}$ is the representation contragredient to π.

アルティン-ヘッケ L-函数が複素平面全体で有理型であり、通常の極を持つ函数を定義するかどうか？そして各保型形式 φ に対して、すべての π に対して L(s, φ, π)/L(s, ψ, π̃) が初等函数となるような保型形式 ψ が存在するかどうか？

現代のLanglands Programのビジョン
LMFDB Universeから



1967年のWeilへの手紙には、既に、現代のLanglands Programの基本的構成要素が全て含まれていることが分かる。

Reciprocity予想

Langlandsのプログラムの出発点は、Quadratic reciprocity -- 平方剰余の相互法則を一般化したEmil Artinのreciprocity law -- 相互法則である。

Artinのreciprocity law -- 相互法則は、ガロア群が可換である代数的数体のガロア拡張に適用され、このガロア群の一次元表現にL-関数を割り当て、これらのL-関数は、あるディリクレL-級数や、Hecke characters -- ヘッケ指標から構成されるより一般的な級数（つまり、リーマンゼータ関数のある類似体）と同一であるとしている。

これらの異なる種類のL-関数の間の正確な対応が、Artinのreciprocity lawを構成している。

Langlandsの洞察は、ディリクレL-関数の適切な一般化を見出すことであり、これによってLanglandsのより一般的な設定においてArtinの主張を定式化することが可能になった。

Heckeは先に、ディリクレL-関数とautomorphic form --保型形式（複素数平面の上半分の平面上の正則函数で、ある関数方程式を満たすもの）とを関連付けていた。

Langlandsは次に、これらを一般化して、（有理数の） adele ring -- アデール環上の一般線形群GL(n)のある無限次元の既約表現である、automorphic cuspidal 表現とした。(この環はp進数のすべての完備化を含んでいる）。

Langlandsは、これらのautomorphic representationにautomorphic L-関数を対応づけ、そして、ある数体のガロア群の有限次元表現から生じるすべてのArtin L-関数は、automorphic cuspidal 表現から生じるものと等しいと予想した。

これはLanglandsのreciprocity conjectureとして知られている。

大雑把に言えば、この予想は、簡約群のautomorphic representationと、Langlands group -- ラングランズ群からLanglands dual group -- L-群への準同型との対応関係を与える。

ラングランズ群とL-群の定義が定まっていないこともあり、この予想には多くのバリエーションがある。

https://en.wikipedia.org/wiki/Langlands_program

Functoriarity予想

Langlandsの研究で新しかったのは、数学の各分野間のつながりが提案されたこと、そしてその豊かな組織的な構造が仮説として示されたこと（いわゆるFunctoriarity予想）である。

Functoriarity予想とは、L-群の適当な同型が、大域的な場合には automorphic form -- 保型形式相互の対応を与え、局所的な場合には、その representation -- 表現相互の対応を与えると予想されるというものである。

大雑把に言えば、Langlands のReciprocity予想は、reductive group – 簡約群の一方がトリビアルである場合のFunctoriarity予想の特殊な場合である。

https://en.wikipedia.org/wiki/Langlands_program

幾何学予想

幾何学的Langlands programは、Vladimir Drinfeldのアイデアに従ってGérard Laumonが提案したもので、既約表現以上のものを関連付けようとする通常のLanglands programの幾何学的再定式化から生まれたものである。

簡単な例では、代数曲線のétale基本群の l-adic表現と、その曲線上のvector bundleのmoduli stack上の l-adic sheavesの派生categoryのobjectとの関係である。

2024年5月、Dennis Gaitsgoryが率いる9人の共同プロジェクトが、Hecke eigensheaf を証明の一部として活用したGeometric Langlands予想の証明を発表した。

Langlandsのautomorphic L-関数

Langlandsのautomorphic L-関数については、次回のセッションでもう少し触れようと思う。

今回のセミナーの前半で、簡単なサンプルで計算をしたのだが、無限積の形で表現された級数を、無限和の整係数の級数に展開して、各項の係数を求めようとした。

同じようなことをイメージに持って貰えばいいと思う。

楕円曲線 $y^2 + y = x^3 - x^2$の場合(Eichler)

$$q\prod_{k=1}^{\infty}\left(1-q^k\right)^2\cdot\left(1-q^{11k}\right)^2$$

$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + O(q^{20})$$

楕円曲線 $y^2 + xy + y = x^3 - x^2$の場合

$$q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n})$$

$$= q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 + \cdots$$

Eulerが考えたこと

Euler product

Langlands program Seminar Part 3-2

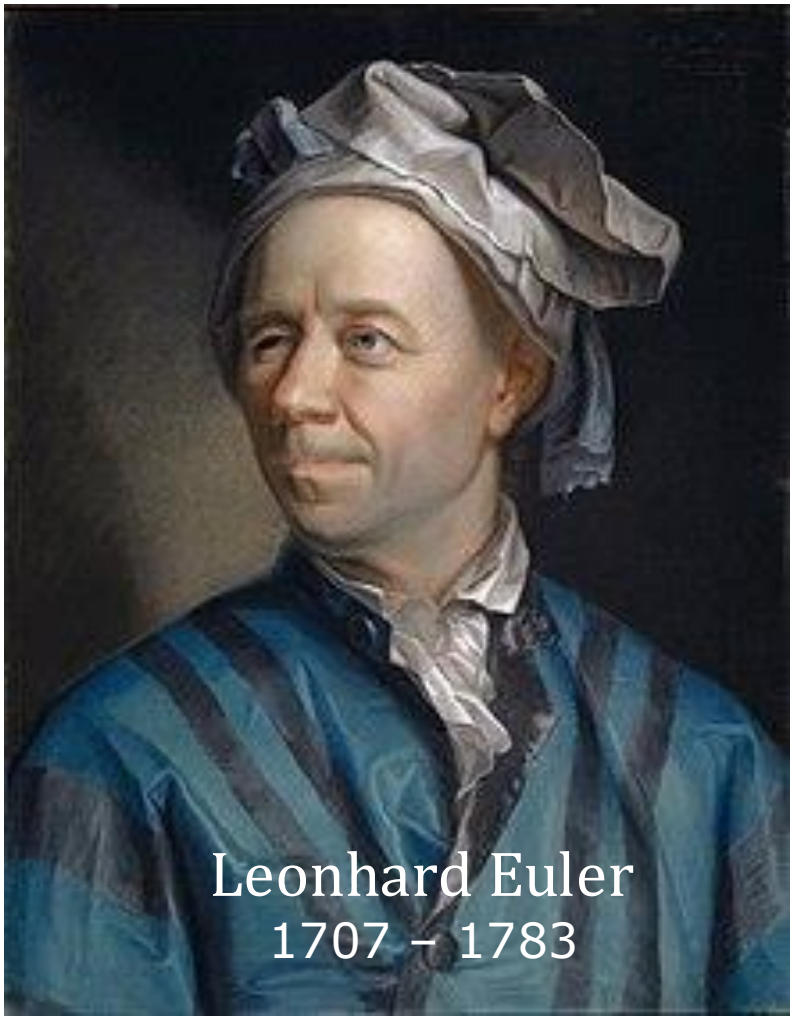
Eulerが考えたこと -- Euler product

Langlandsのautomorphic L-functionの源流は、Eulerにある。

1737年、Eulerは次の式が成り立つことを証明した。

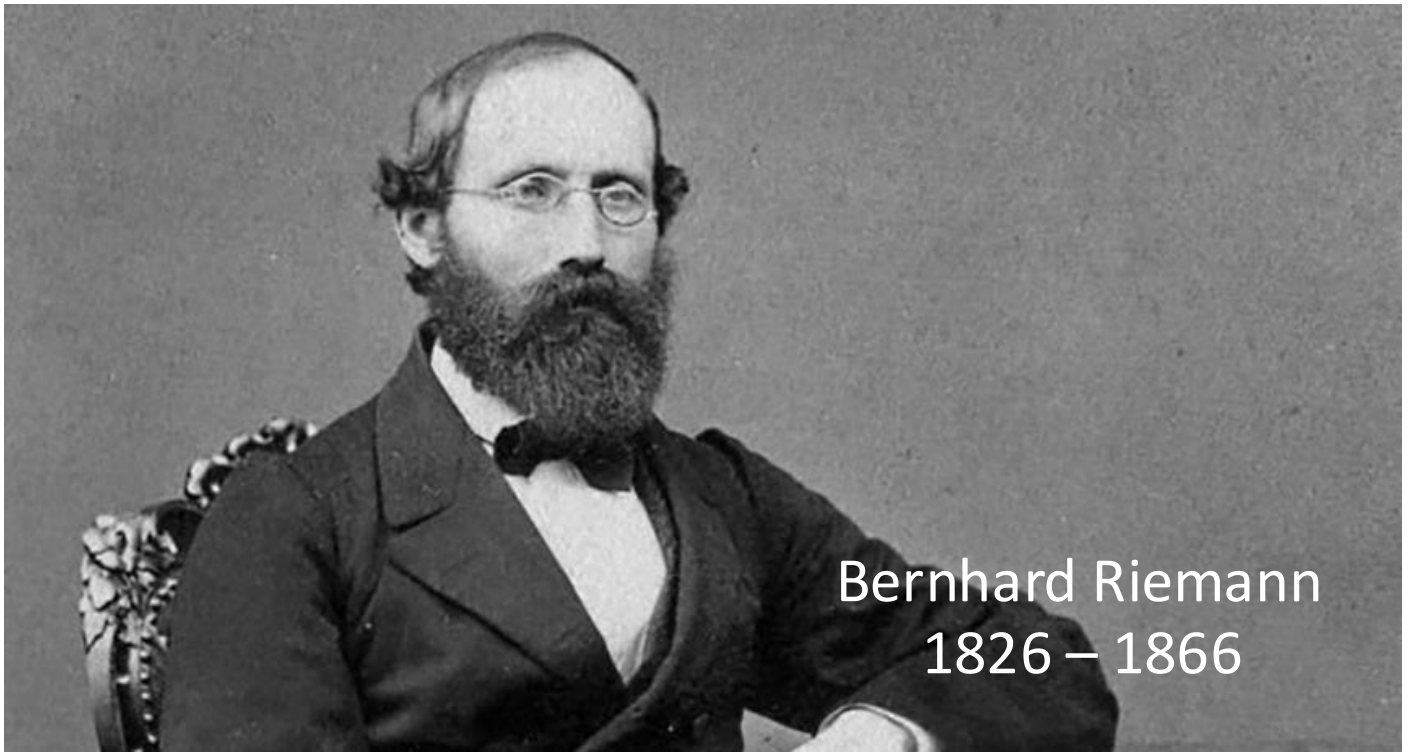
$$\zeta(s) = \sum_{n} \frac{1}{n^s} = \prod_{p\ prime} \frac{1}{1 - p^{-s}}$$

これを、$\zeta(s)$のEuler product表示という。



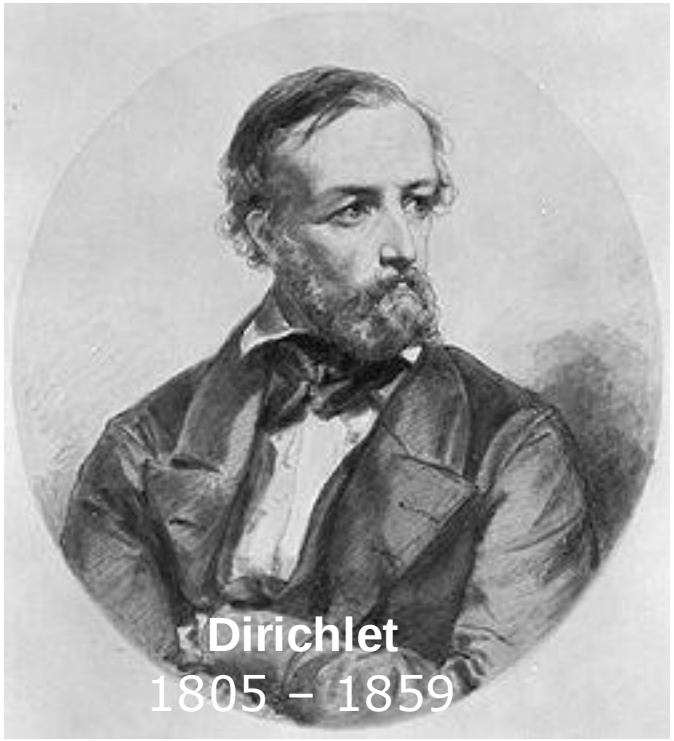
Euler–Riemann ζ-function

$$\zeta(s) = \sum_n \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \cdots$$



Dirichlet のL-関数

$$L(s) = \sum_n \frac{a_n}{n^s} = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \frac{a_5}{5^s} + \frac{a_6}{6^s} + \frac{a_7}{7^s} + \cdots$$



こうした係数[$a_1, a_2, a_3, a_4, \cdots$]で定義される無限級数をDirichletは考えた。

これは、Eulerのζ級数の一般化である。

Euler product formulaの導出

$$\zeta(s) = \sum_n \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \cdots$$

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \frac{1}{12^s} + \frac{1}{14^s} + \cdots$$

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{1^s} + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{1}{13^s} + \cdots$$

分母が2で割れる項は、取り除かれている。

$$\left(1-\frac{1}{2^s}\right)\zeta(s)=\frac{1}{1^s}+\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{9^s}+\frac{1}{11^s}+\frac{1}{13^s}+\cdots$$

$$\frac{1}{3^s}\left(1-\frac{1}{2^s}\right)\zeta(s)=\frac{1}{3^s}+\frac{1}{9^s}+\frac{1}{15^s}+\frac{1}{21^s}+\frac{1}{27^s}+\frac{1}{33^s}+\frac{1}{39^s}+\cdots$$

$$\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=1+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+\frac{1}{17^s}+\cdots$$

分母が2と3で割れる項が、取り除かれている。

$$\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=1+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+\frac{1}{17^s}+\cdots$$

$$\frac{1}{5^s}\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=\frac{1}{5^s}+\frac{1}{25^s}+\frac{1}{35^s}+\frac{1}{55^s}+\frac{1}{85^s}+\cdots$$

$$\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=1+\frac{1}{7^s}+\frac{1}{11^s}+\frac{1}{17^s}+\cdots$$

分母が2と3と5で割れる項が、取り除かれている。

$$\cdots\left(1-\frac{1}{11^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=1$$

$$\zeta(s)=\frac{1}{\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{11^s}\right)\cdots}$$

$$\zeta(s)=\prod_{p\ prime}\frac{1}{1-\frac{1}{p^s}}$$

Rieman Hypothesis

リーマンゼータ関数ζ(s)は、sの引数が1以外の任意の複素数であり、その値も複素数である関数である。

負の偶数ではゼロとなる。つまり、sが-2、-4、-6、...のいずれかの場合、ζ(s) = 0となる。これらは「自明なゼロ」と呼ばれる。
ゼータ関数は、s の他の値に対してもゼロとなり、これらは非自明零点と呼ばれる。

リーマン予想

リーマンゼータ関数の非自明零の実部はすべて 1/2 である。

Dirichlet L-function

Dirichlet L-級数を、次の形の関数とする。

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

ただし、$\chi(n)$は整数から複素数への巻数で、次のような性質を持つものとする。

- $a \equiv b \ (mod\ N)$ なら$\chi(a) = \chi(b)$
- $\chi(ab) = \chi(a)\chi(b)$
- $\chi(1) = 1$
- aとNが互いに素でなければ $\chi(a) = 0$

こうした$\chi(n)$をDirichlet character – ディリクレ指標と言う。

全ての整数nに対して$\chi(n) = 1$なら、$L(s,\chi)$は$\zeta(s)$と一致する。

Dirichlet L-級数 $L(s,\chi)$を、全複素平面上でmeromorphic function -- 有理型関数に拡大したものを、Dirichlet L-function と呼び、再び、$L(s,\chi)$と表す。

この時、$L(s,\chi)$は、$Re(s) > 1$で次のEuler積表示をもつ。

$$L(s,\chi) = \prod_{p\ prime} \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

Appendix

Hecke's degree-1 L-series.

$$L(s,\chi) = \sum_{U} \chi(U) N(U)^{-1} = \prod_{P} \frac{1}{1 - \frac{\chi(P)}{N(P)}}$$

Hecke's degree-2 L-series

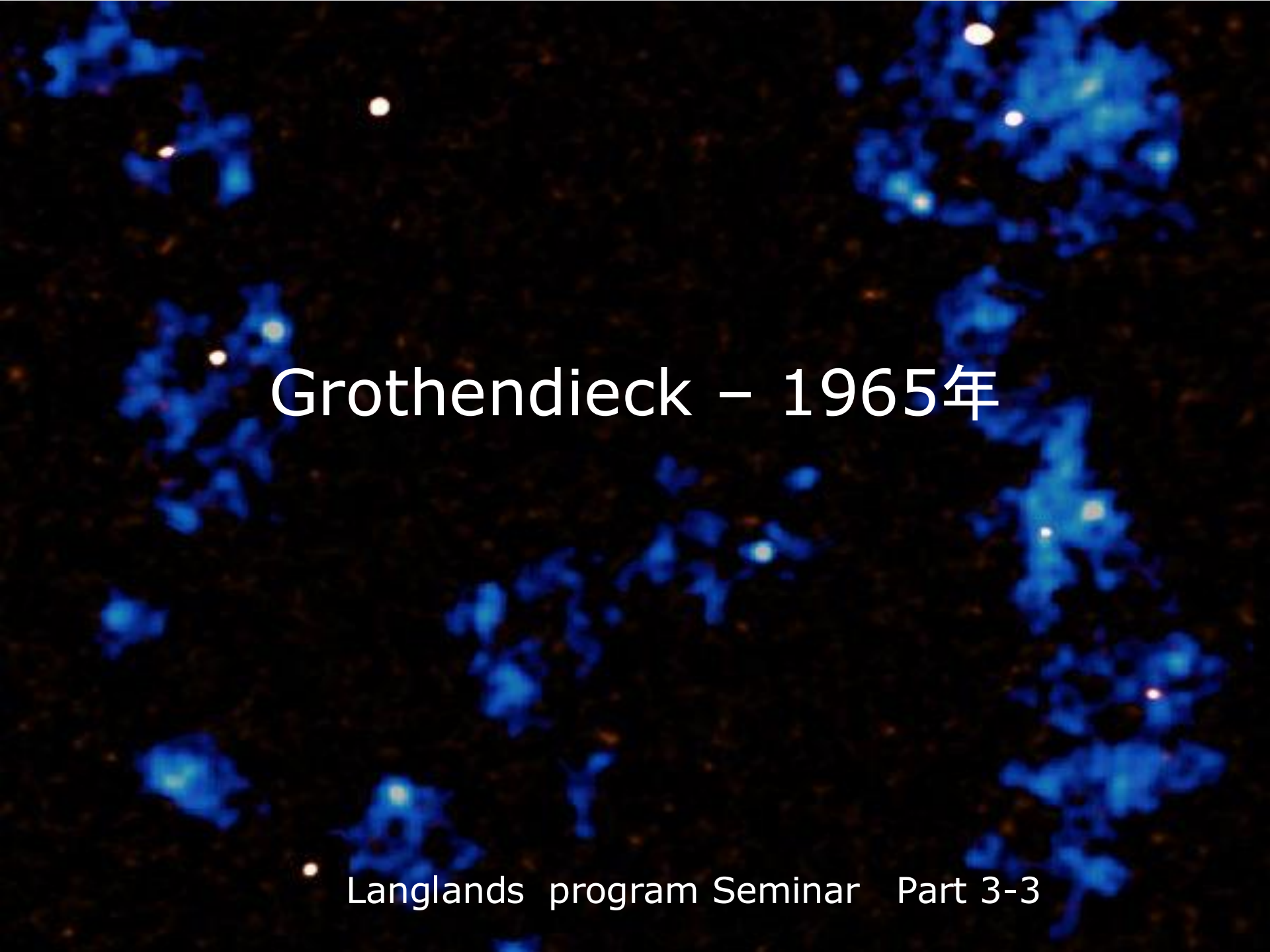
$$L(s,f) = \sum_{n} a_n n^{-1} = \prod_{p} \frac{1}{1 - \frac{a_p}{p^s} + p^{k-1-2s}}$$

Artin L-functions

$$L(s,r) = \prod_{P} L_P(s,r) = \prod_{P} \frac{1}{det\left(1 - \frac{r(Frob_P)}{(NP)^s}\right)}$$

Langlands' automorphic L-functions.

$$L(s,\pi,\rho) = \prod_{p} \frac{1}{\det\left(1 - \frac{\rho_p(c(\pi_p))}{p^s}\right)}$$



Langlands program Seminar Part 3-3

Alexander Grothendieck

(1928-2014)

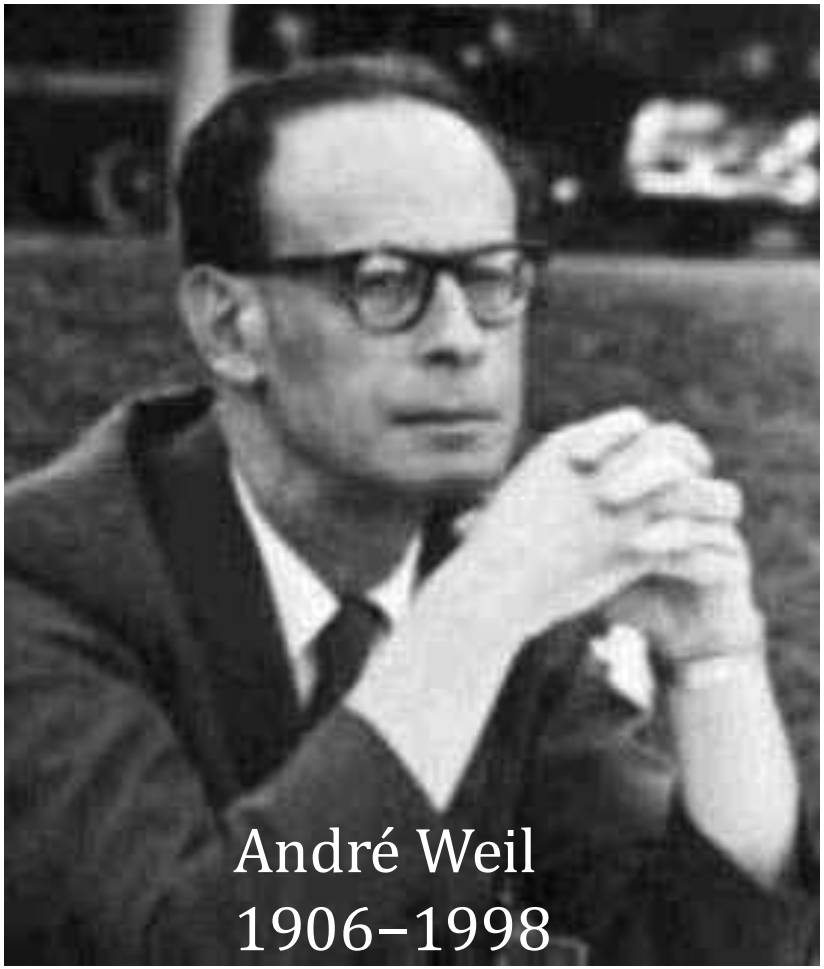
Alexander Grothendieck

In the eyes of many, Alexandre Grothendieck was the most original and most powerful mathematician of the twentieth century. He was also a man with many other passions who did all things his own way, without regard to convention.

多くの人々にとって、アレクサンドル・グロタンディークは20世紀で最も独創的で最も影響力のある数学者であった。また、彼は数多くの情熱を持った人間であり、あらゆることを独自のやり方で行い、慣習を気にすることなく行動した。

「アメリカ数学会　グラタンディック追悼号」 から
https://www.ams.org/journals/notices/201603/rnotip242.pdf

Weil Conjecture



「ヴェイユ予想」は、アンドレ・ヴェイユによって1949年に提出された「予想」である。

この「予想」を証明するため、数十年にわたって数学者は努力し、その成功の過程が、現代の代数幾何学と数論の枠組みを構築することになった。

グロタンディックは、この予想の解決に大きな貢献し、1966年、フィールズ賞を授与されている。

最終的にこの予想を解いたのはデリーニュで、1974年のことである。

ヴェイユ予想

「ヴェイユ予想」は、代数多様体上の点の数を数えることで導かれる生成関数（局所ゼータ関数として知られる）に関するものである。

有限体上の多様体Vは、有限個の（元の体の座標を持つ）有理点と、元の体の任意の有限拡大体の座標を持つ点を持つ。生成関数は、拡大体の点の数N_k（q^k個の要素を持つ）から導かれる係数を持つ。

ヴェイユは、滑らかな多様体に関するこのようなゼータ関数は

(1) 有理関数であり、

(2) ある種の関数方程式を満たし、

(3) その零点は制限された場所にある

と予想した。

(2)と(3)の部分は、意識的にリーマン・ゼータ関数をモデルにしている。それは素数に対する一種の生成関数であり、関数方程式に従い、（予想によると）そのゼロは「リーマン仮説」によって制限されている。そ

(1)の有理性はバーナード・ドワーク（1960年）によって、(2)の関数方程式はアレクサンダー・グロタンディーク（1965年）によって、そして（3）の「リーマン仮説」との類似はピエール・ドゥリーニュ（1974年）によって証明された。

https://en.wikipedia.org/wiki/Weil_conjectures

Weil conjectures

1 Introduction

https://youtu.be/2n8xpH5enDg

Grothendieck's Mathematical Work

以下、「アメリカ数学会　グラタンディック追悼号」 から
https://www.ams.org/journals/notices/201603/rnotip242.pdf

グロタンディークの数学における最大の功績は、代数幾何学におけるものであり、1956年から1968年までの12年間に最も集中的に取り組んだ成果であった。

それ以前にも、1950年から1954年にかけては関数解析の分野で主要な業績を残している。その後、モンペリエでは多くのアイデアに取り組み、そのうちのいくつかは 著書『Esquisse d'un programme』にまとめられている。しかし、その多くは未だに出版されていない。

これらすべての仕事を網羅するには多くの専門家が必要であり、本稿では代数幾何学への彼の最も顕著な貢献と考えられる4つのみを概説する。

最も驚くべきことは、それぞれにおいて新しい抽象理論を創出し、それが彼が着手した当時の代数幾何学における主要な問題の解決に導いたと言うことである。

彼の業績の多くの重要な部分、特に初期の位相ベクトル空間に関する研究、IHESでの双対性理論、平坦化、結晶コホモロジー、motive、toposの理論、そして最後にモンペリエ時代の「dessin d'enfants」やその他の業績を省略した。

先の「アメリカ数学会　グラタンディック追悼号」 は、次の4つを彼の主要な業績として取り上げている。

- K-theory and the Grothendieck-Riemann-Roch Theorem for Morphisms $f : X \to Y$
- Formal Schemes, Nilpotents and the Fundamental Group
- Functors and the Hilbert, Picard, and Moduli Schemes
- Étale Cohomology

ここではWeil conjecture と関連の深いÉtale Cohomology 論について、その要約を紹介する。

Étale Cohomology

1954年のアンドレ・ヴェイユの講演で、標数 pの多様体のコホモロジー論への関心は刺激された。

代数的にコホモロジーを定義するという問題は、それまであまり関心を引いていなかった。なぜなら、複素数上の多様体に対しては、古典的位相幾何学が利用可能だったからである。

しかし、ヴェイユの話の頂点は、有限体上の多様体V上の有理点はFrobenius automorphismの固定点であるため、Lefschetz Fixed Point Formula（レフシェッツ固定点公式）で固定点を数えることができるかもしれないという説明であった。

この公式は、automorphism φの固定点の数は、コホモロジー上のφによって誘導される写像のtraceの交互和

$$\sum_i (-1)^i Trace_{H_i(V)}(\varphi^*)$$

に等しいと主張する。

しかし、コホモロジー群の定義が必要であった。ザリスキ・トポロジーはこれには役に立たなかった。

ヴェイユが予想した性質を持つ定義が存在するはずだということが、「ヴェイユ予想」として知られるようになった。

$H^1(V, \mathbb{Z}/n)$ は、n-torsion divisor class の群から構成できるので、次元 1のコホモロジーについては問題がなかった。したがって、曲線のコホモロジーは理解できた。

実際、ヴェイユの予想は、既知の曲線のケースに基づいていた。

そのために、ゼータ関数が解析されていて、それらの曲線上では E. Artin、H. Hasse、そしてヴェイユ自身によって、リーマン仮説の類似が証明されていた。

コホモロジーを定義するためのGrothendieckのアイデアは、トポロジーの開集合を、Zariskiの開集合の非分岐被覆に置き換えて定義することであった。

これがうまくいくかも知れないというヒントは、すでにあった。以前、Serreはlocal isotrivialityと呼ばれるものを定義していた。

ある多様体上のバンドル Bが局所的にisotrivialであるのは、Xのすべての点pに対して、pのZariski開集合近傍の有限被覆U'が存在し、BからU' へのプルバックがトリビアルである場合である。

さらに、河田とテートは、曲線のコホモロジー群を、その基本群のコホモロジーの観点から回復できることを示した。

M. Artinは1961年、Grothendieckがハーバード大学を訪れた際に、このアイデアを取り上げた。

彼は、有限でない、つまりすべてのエタール写像を使って、複素数上に、古典的位相幾何学と同じように、ねじれ係数を持つコホモロジーが得られることを示すことに成功した。

振り返ってみると、エタール・トポロジーは、ザリスキ・トポロジーよりも強く、古典的トポロジーよりも弱いので、試してみる自然なものだった。

そのことは、当時は、まったく明らかではなかった。

なぜなら、エタール・トポロジーは、通常の意味でのトポロジーではないからである。開集合はエタール写像に置き換えられるが、この写像は基底空間にはinjectiveには写像されない。

このような設定でsheaf理論ができるという考えは斬新だった。

そして、妥当な理論を持つためには、ねじれ係数を扱う必要がある。定点定理に必要な非ねじれ係数を持つコホモロジーは、ℓ-adic コホモロジーとして逆極限によって定義される。

それからグロテンディークは、1次元の既知の場合から始めて、fibrationを連続的に用いて、一連の定理、特に適切な基底変換の定理を証明した。この定理は、次元の帰納法によって多様体のコホモロジーを制御することを可能にするものである。

この定理を証明するために、Grothendieckは、Serreが。Artin、Grothendieck、Verdierが導入していた方法を採用し、1963-64年にかけてIHESで完全な理論を共同で開発した。

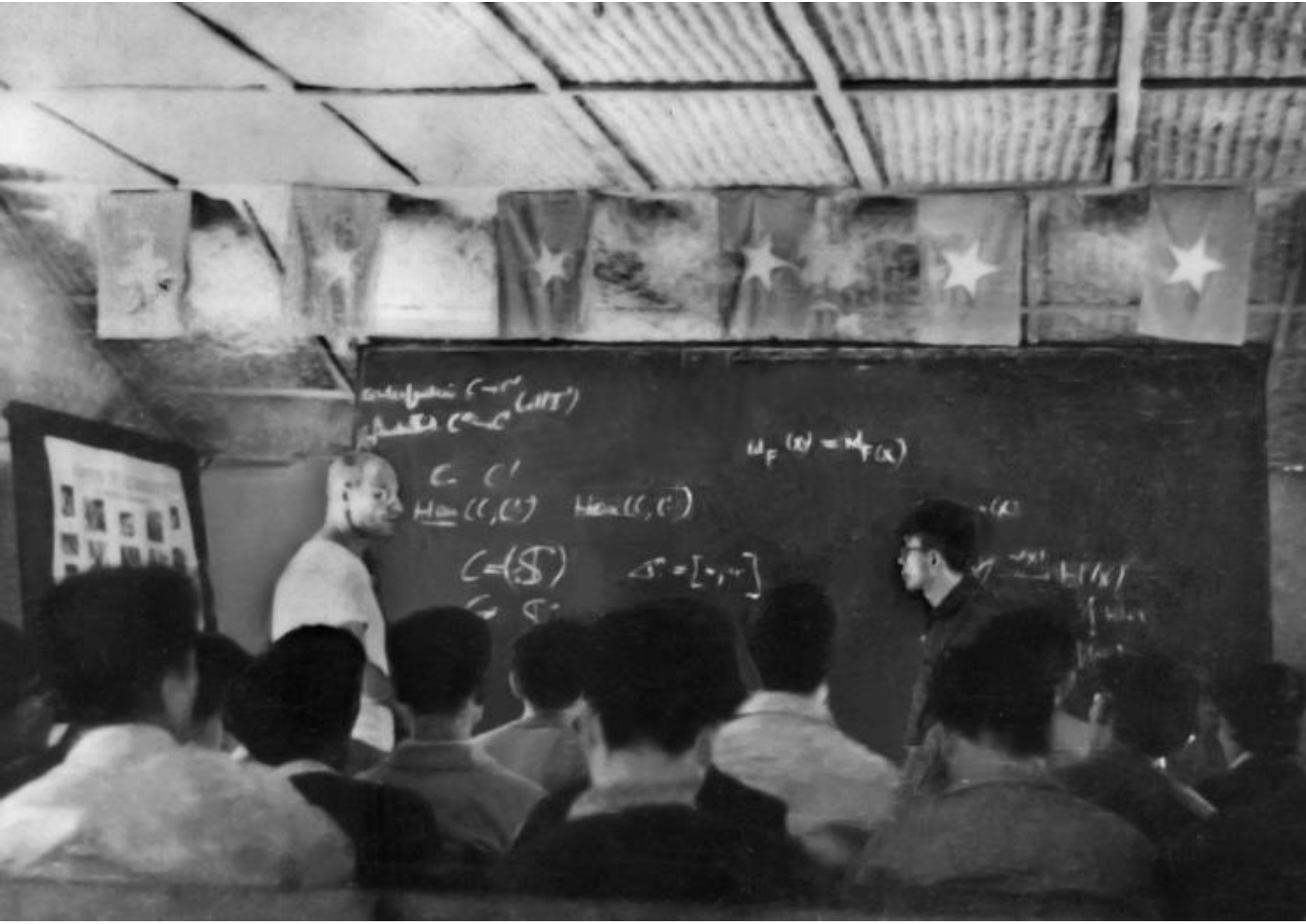
Grothendieckはその後、任意の構成可能なsheafのコホモロジーについてL-級数を定義した。これによって1964年、彼はL-球数の有利性を証明し、基底変換定理とVerdierの双対性定理を用いて、次元1の場合に還元する関数方程式を見つけることができた。

有限体上の多様体に対するRiemann Hypothesisは1974年にDeligneによって証明された。

Grothendieck – 1967年

Grothendieck visited North Vietnam in late 1967, during the Vietnam War, and spent a month teaching mathematics to the Hanoi University mathematics department staff, including Hoàng Xuân Sính, who took the notes for the lectures. Because of the war, Grothendieck's lectures were held away from Hanoi, first in the nearby countryside and later in Đại Từ.

Grothendieck – 1967年

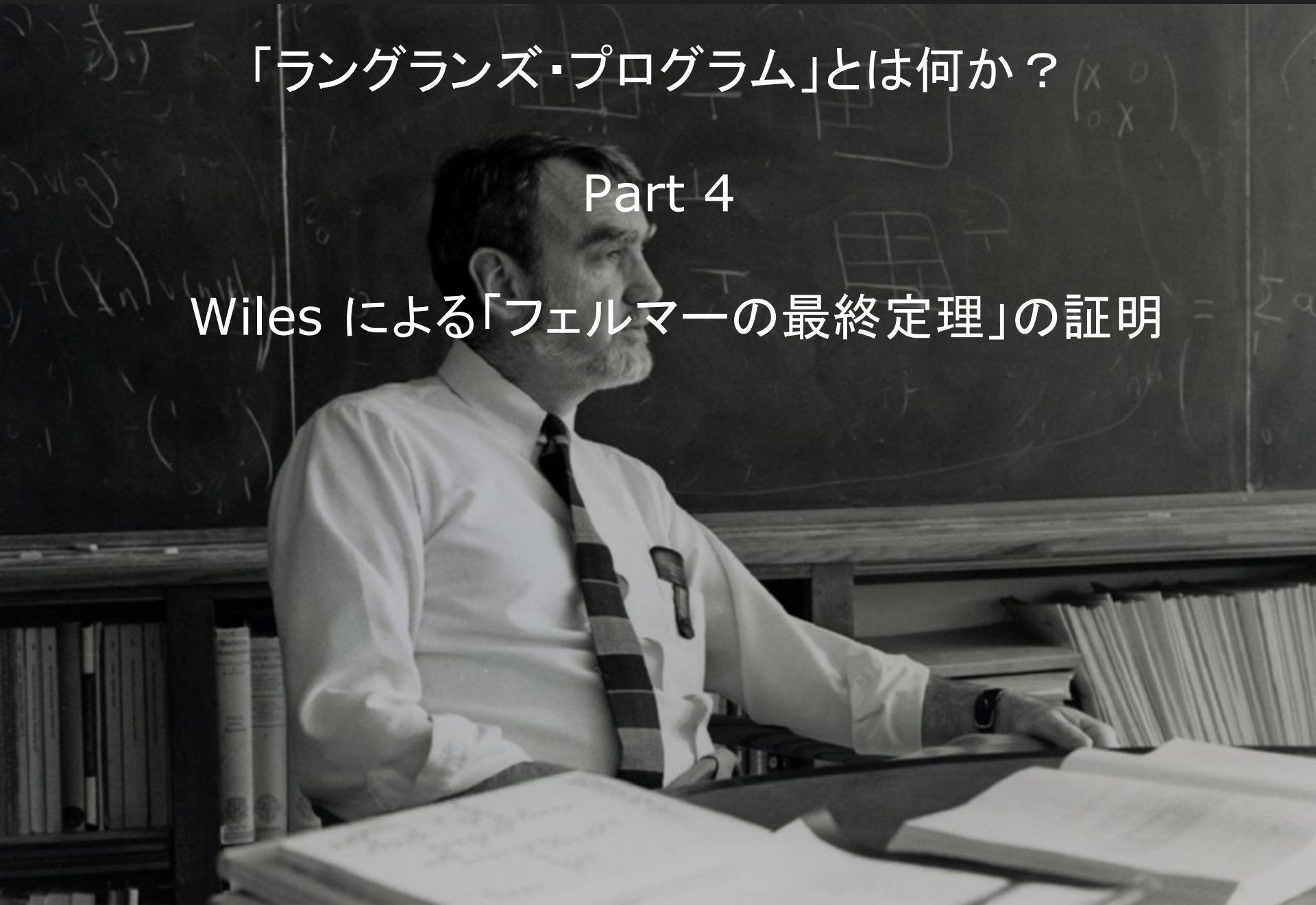


L'œuvre d'Alexandre Grothendieck

Pierre Deligne (French with English subtitles)

https://youtu.be/PeMAyPGjL68


HITACHI
危い!



「ラングランズ・プログラム」とは何か？

Part 4

Wiles による「フェルマーの最終定理」の証明

Part 4

Wiles による「フェルマーの最終定理」の証明

Part 4では、Wilesの「フェルマーの定理」の証明の取り組みを紹介します。

1995年、Wilesは、「谷山・志村予想」をある条件のもとで解いて、それを利用して「フェルマーの最終定理」を解くことに成功します。

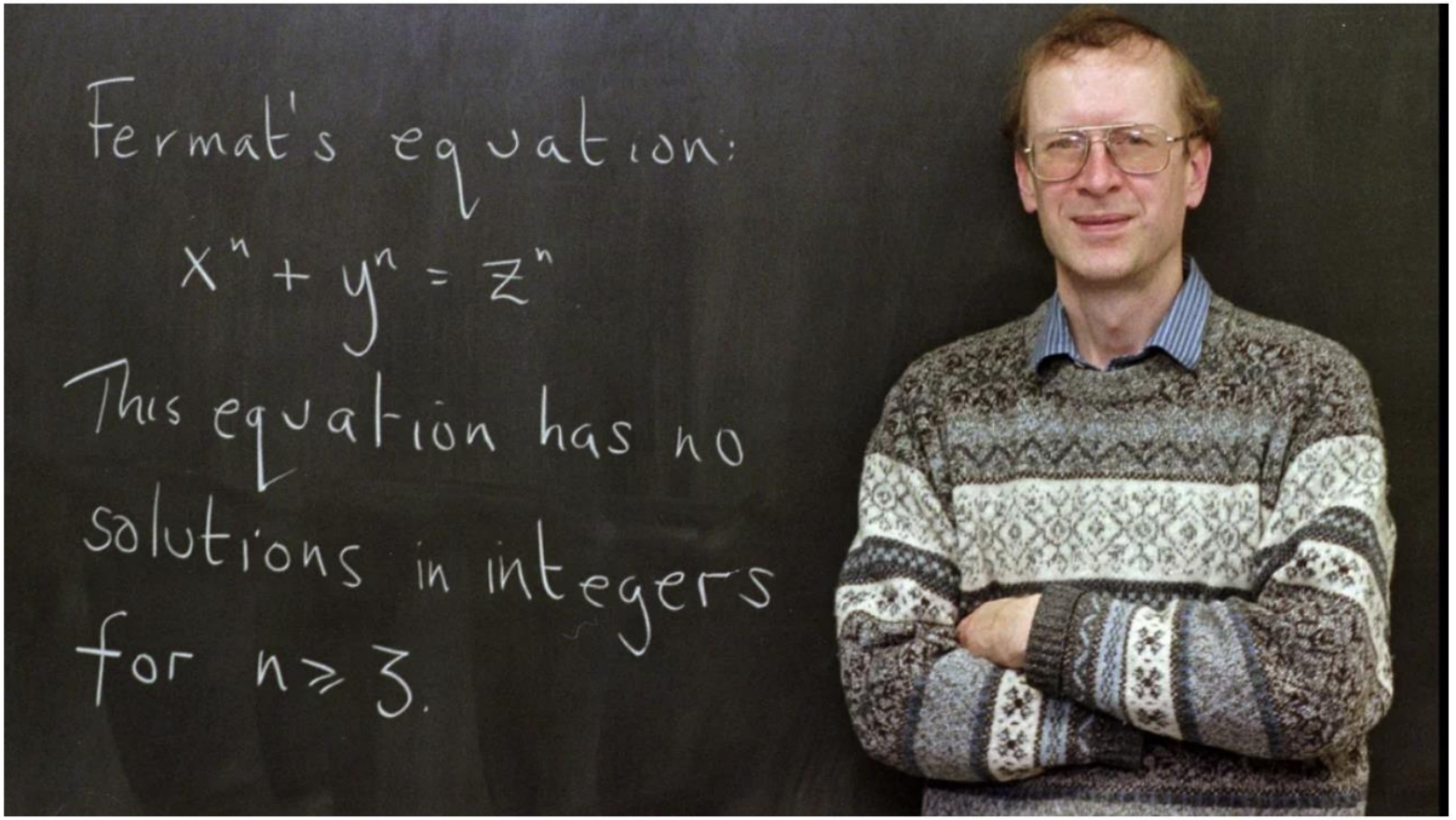
「谷山・志村予想」に対するWilesの貢献は画期的なもので、先に述べたように、2001年には、Wilesの弟子たちによって、「谷山・志村予想」は完全に解かれることになります。

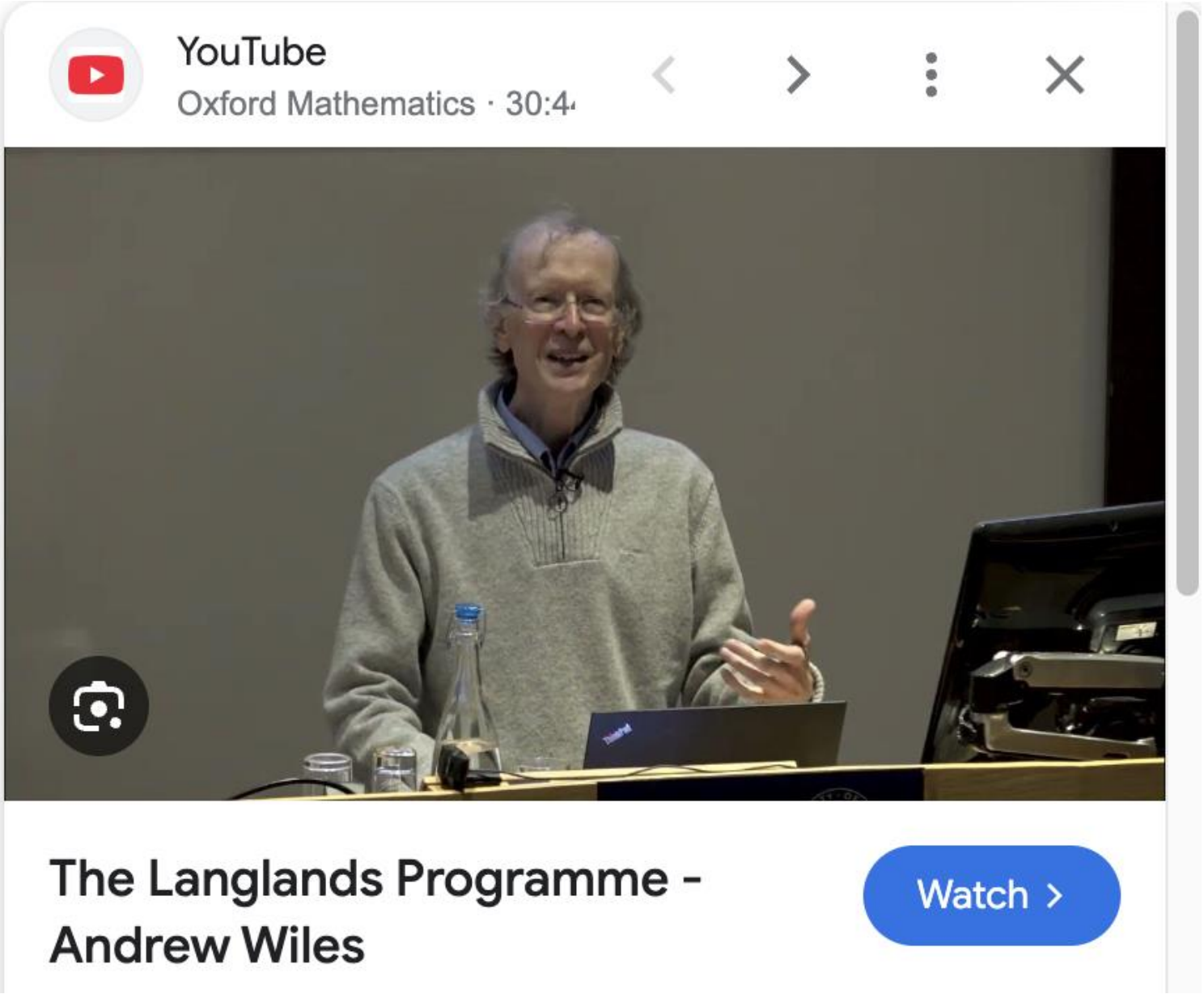
Wilesによる「フェルマーの定理」の証明は、20世紀の数学の大きな達成とみなされているのですが、その導きの糸となったのは、Langlands programであったという話ができたらと思っています。

Professor Who Solved Fermat's Last Theorem Wins Math's Abel Prize

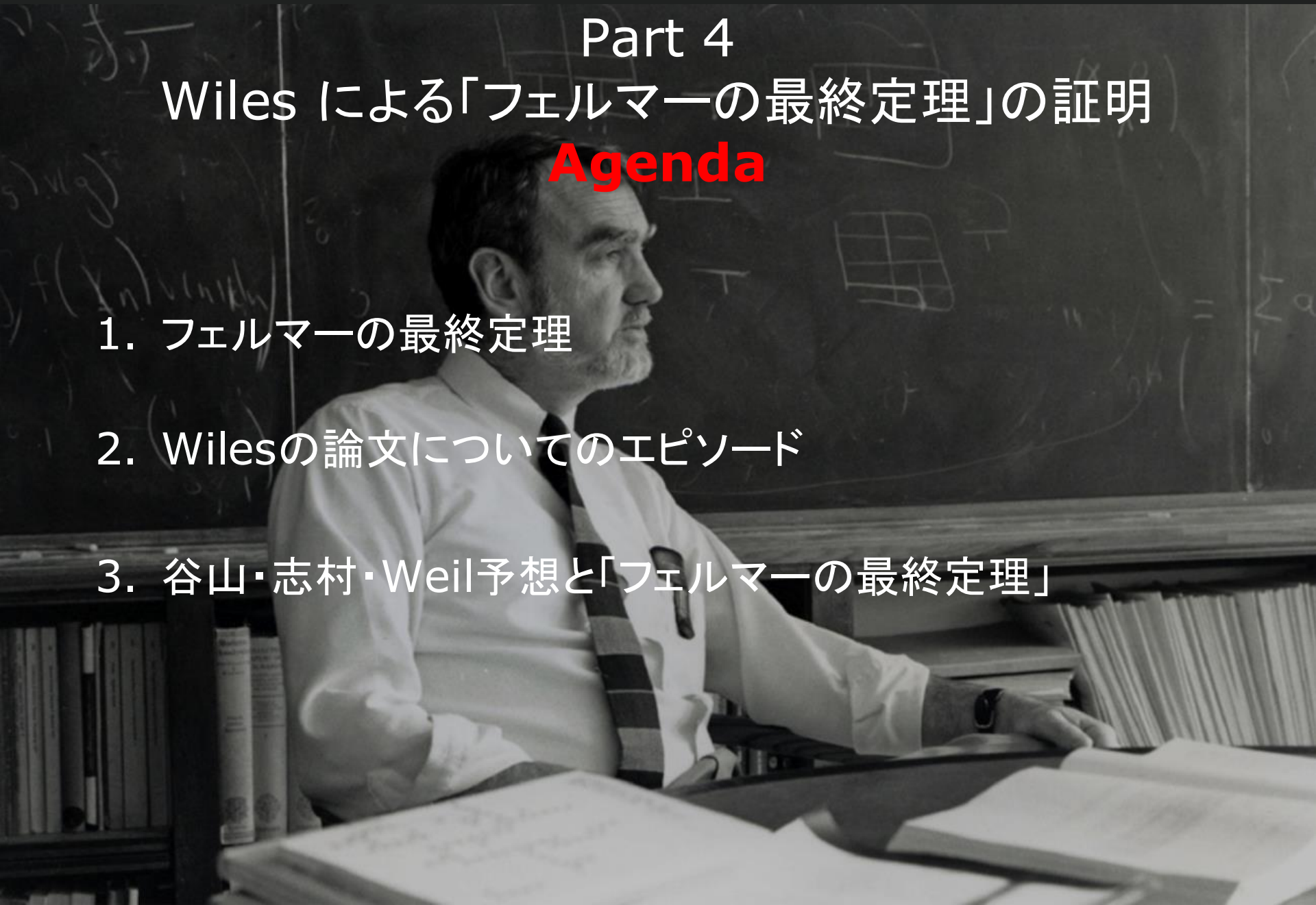
MARCH 17, 2016 · 8:19 AM ET

By Bill Chappell





https://youtu.be/ZFOPxZtlkig



Part 4
Wiles による「フェルマーの最終定理」の証明
Agenda

1. フェルマーの最終定理
2. Wilesの論文についてのエピソード
3. 谷山･志村･Weil予想と「フェルマーの最終定理」

フェルマーの最終定理

Pierre de Fermat
1607−1665

Langlands program Seminar Part 4-1

「フェルマーの最終定理」

1637年にフェルマーが提出した定理は、「フェルマーの最終定理」あるいは、「フェルマーの大定理」とも呼ばれる。

3 以上の自然数 n について、

$$x^n + y^n = z^n$$

となる自然数の組 (x, y, z) は存在しない、

という定理である。（ただし $xyz \neq 0$ とする）

nが2の場合の

$$x^2 + y^2 = z^2$$

は、ピタゴラスの三平方の定理で、無限に多くの整数の組(x, y, z) が存在する。

フェルマーの「小定理」

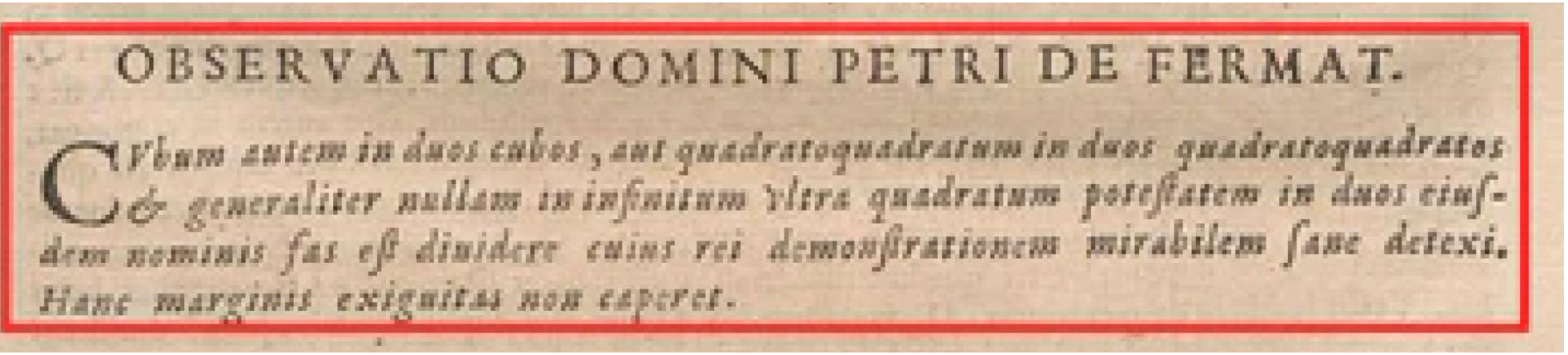
pを素数とし、aを整数とすると、

$$a^p \equiv a \ (mod\ p)$$

あるいは、pを素数とし、aを pの倍数でない整数とすると、

$$a^{p-1} \equiv 1 \ (mod\ p)$$

「最終定理」についての有名なエピソード



OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat ~ 1637

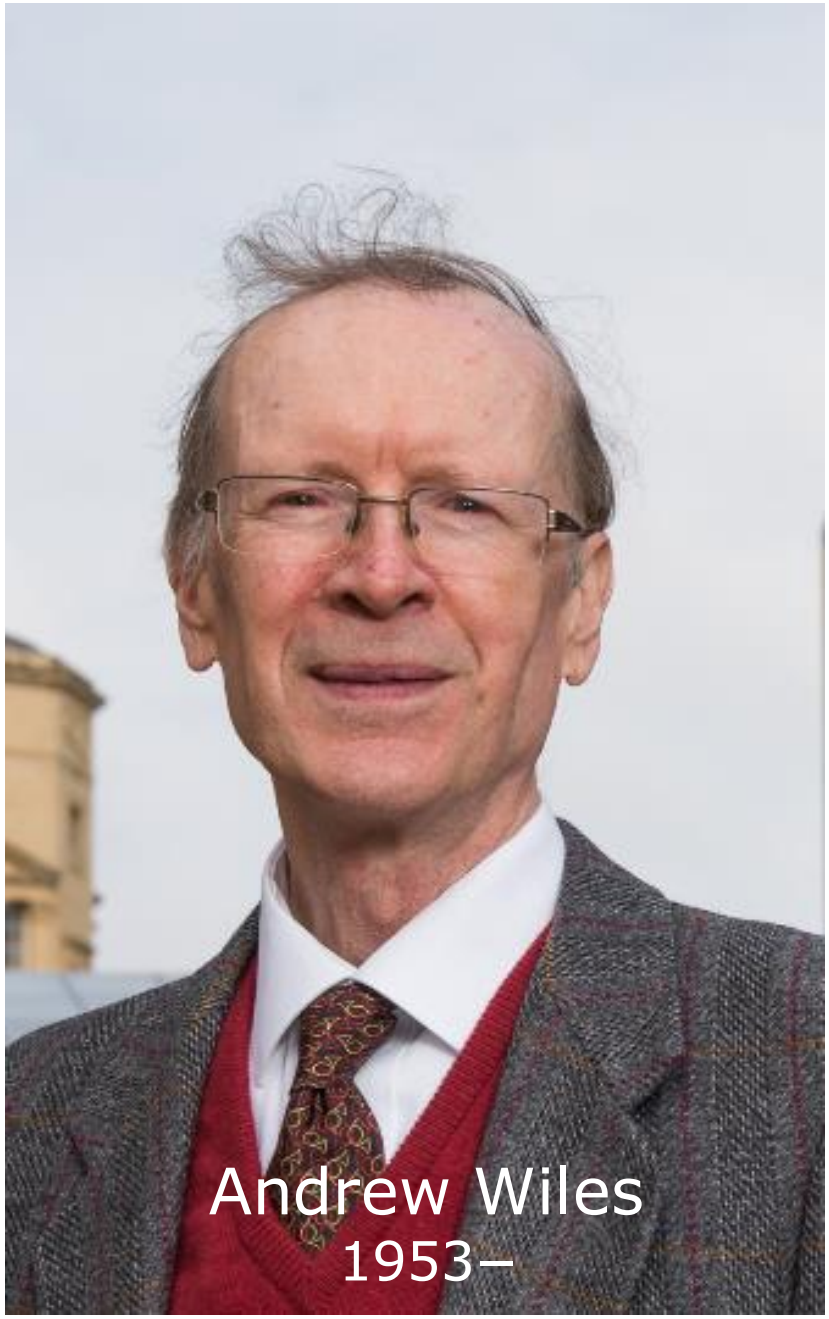
「立方数を2つの立方数の和に分けることはできない。4乗数を2つの4乗数の和に分けることはできない。一般に、冪が2より大きいとき、その冪乗数を2つの冪乗数の和に分けることはできない。

この定理に関して、私は真に驚くべき証明を見つけたが、この余白はそれを書くには狭すぎる。」

Andrew Wiles

1995年、Andrew Wiles は、300年以上未解決だった、「フェルマーの定理」を証明した。

証明の成功だけでなく、彼が証明のために開発した多くの新しい手法は、現代の数学に、深い影響を与えた。



Annals of Mathematics, **142** (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By ANDREW WILES*

For Nada, Clare, Kate and Olivia

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat

Introduction

An elliptic curve over $\mathbf{Q}$ is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a

https://staff.fnwi.uva.nl/a.l.kret/Galoistheorie/wiles.pdf

「最終定理」についてフェルマーが証明したこと
n=4の場合

フェルマー自身は、n=4の場合 すなわち

$$x^4 + y^4 = z^4$$

を満たす自然数の組(x, y, z) は存在しないことを証明している。

まず、$x^4 + y^4 = z^2$ となる自然数の組(x, y, z) は存在しないことを証明する。$(xyz \neq 0)$

それから、

$$x^4 + y^4 = z^4$$

を満たす自然数の組(x, y, z) は存在しないことは導かれる。

ピタゴラス数

ここではまず、$x^4 + y^4 = z^2$ となる自然数の組(x, y, z) は存在しないことを証明する。

$x^4 + y^4 = (x^2)^2 + (y^2)^2 = z^2$ だから、
$A = x^2, B = y^2, C = z$ とすると、

$$A^2 + B^2 = C^2$$

これは(A, B, C)がピタゴラスの定理を満たす直角三角形の辺であることを意味する。こうした組をピタゴラス数と呼ぶ。

ピタゴラス数の別表示

ピタゴラス数 (A, B, C)には、次のようなm, nが存在する。

$$(A, B, C) = (2mn, m^2 - n^2, m^2 + n^2)$$

(1) $A = x^2 = 2mn$
(2) $B = y^2 = m^2 - n^2$
(3) $C = z = m^2 + n^2$

この時、$m^2 + n^2 = z$である。

(2)から $n^2 + y^2 = m^2$

(n, y, m)は、ピタゴラス数である。

(n, y, m)には、次のようなn_1, m_1が存在する。

$$(n, y, m) = (2n_1m_1,\ n_1^2 - m_1^2,\ n_1^2 + m_1^2)$$

(4) $\mathrm{n} = 2n_1m_1$

(5) $\mathrm{y} = n_1^2 - m_1^2$

(6) $\mathrm{m} = n_1^2 + m_1^2$

(1)と(4), (6) から

$$x^2 = 2mn = 2(n_1^2 + m_1^2)(2n_1m_1) = 4n_1m_1(n_1^2 + m_1^2)$$

無限降下法

$$x^2 = 4n_1m_1(n_1^2+m_1^2)$$

$n_1m_1, n_1^2+m_1^2$ は互いに素だから、n_1m_1も $n_1^2+m_1^2$ も平方数である。
よって、$P_1^2 = n_1^2+m_1^2 = m$ となるP_1が存在する。
ただし、

$$m_1^2+n_1^2 = m < m^2 < m^2+n^2 = z < \mathrm{z}^2$$

$n_1^2+m_1^2 = P_1^2$ だから、(n_1, m_1, P_1)ははピタゴラス数である。

同じ手順を繰り返すと $n_2^2+m_2^2 = P_2^2$ なるn_2, m_2, P_2が存在することになる。

$x^4 + y^4 = z^2$ となる
自然数の組(x, y, z) は存在しない

まとめると

$(x^2)^2 + (y^2)^2 = z^2$ なら
$m^2 + n^2 = z$ なるm, nが存在し、その時
$m_1^2 + n_1^2 = m = P_1^2$ なるm_1, n_1が存在し、その時
$m_2^2 + n_2^2 = P_2^2$ なるm_2, n_2が存在し、その時
$m_3^2 + n_3^2 = P_3^2$ なるm_3, n_3が存在し、その時
……
……

ただし、こうした無限下降列は存在し得ない

ので、前提の
$(x^2)^2 + (y^2)^2 = z^2$
が、正しくないことが分かる。

$x^4 + y^4 = z^4$ となる自然数の組(x, y, z) は存在しない

先に、$x^4 + y^4 = z^2$ となる自然数の組(x, y, z) は存在しないことを見てきた。

これから、$x^4 + y^4 = z^4 = (z^2)^2$ となる自然数の組(x, y, z) は存在しないことは直ちに導かれる。

$x^n + y^n \neq z^n$の $n = 4$以外の場合の個別のnについての証明

n = 3	1770	Euler
n = 5	1825	Legendre
		Dirichlet
n = 7	1839	Lamé
	1840	Lebesgue

これらの証明は、基本的に「無限降下法」を利用している。

Kummerの仕事

「nの値が増大するにつれて生じる困難を克服する他の方法が必要であることは、すぐに明らかになった。

ここで紹介するこれらの方法は、クンマー（1810-1893）によって導入された。彼の成果は、彼以前にも以後にも、このテーマに関して数学者が成し遂げたものの中で最も重要な貢献であった。

それらは最も一般的であっただけでなく、いくつかのクラスに含まれるnの値の多数に対してフェルマーの最終定理を証明することに成功した。数学の発展における重要な段階となった。」

Mordell, LJ (1921). "Three Lectures on Fermat's Last Theorem" https://archive.org/details/cu31924001075880

「Ideal の理論は、現在では数論の基礎の一部となっているが、クンマーがこのテーマと一般的な相互法則について研究したことが起源となっている。

彼の方法と結果は、彼が亡くなった後、何年も経ってから開始された数多くの研究の出発点となり、過去12年以内でも非常に驚くべき結果につながっている。

彼の業績は、数学と数学者が、1つか2つの孤立した問題の考察に負うところが大きいことを、見事に示している。」

Mordell 同上書より

「それゆえ、Lame, Cauchy そしてKummerといった数学者たちが、当初は、上の代数的整数はユニークに因数分解できると信じていたとしても、驚くにはあたらない。

Lameは、Liouville と Kummerが指摘したように、フェルマーの最終定理の証明を提示する際に、この誤った仮定を立てた。

Kummerもまた、Dirichletが指摘したように、以前に証明を試みた際に同じ間違いを犯しており、Dirichletは、代数的数は一般には、一意的に因数分解できないという見解を示した。」

Mordell 同上書より

Mordell 予想とその解決

「Gerd FaltingsによるMordell予想の解決（1983年）により、3以上のnに対するフェルマー方程式 $x^n + y^n = z^n$ が整数解をもつならば（つまりフェルマー予想が誤りならば）その解の個数は本質的に（自明な場合を除いて）有限個しかないことが証明される

この「有限個」が「実は 0 個」であることが示されればフェルマー予想は証明できたことになるが、この方向からの絞り込みには行き詰まりが指摘されていた。

ともあれ、この時点でフェルマー予想が「ほとんど全ての場合について正しい（各nに対して非自明な解は高々有限個である）」ことが判明したと言うことはできた。」

https://ja.wikipedia.org/フェルマーの最終定理/

Computational studies

20世紀後半には、コンピュータによる手法が用いられ、クンマーの手法が非正規素数にも拡張された。

1954年には、Harry VandiverがSWACコンピュータを使用して、2521までの素数すべてについてフェルマーの最終定理を証明した。

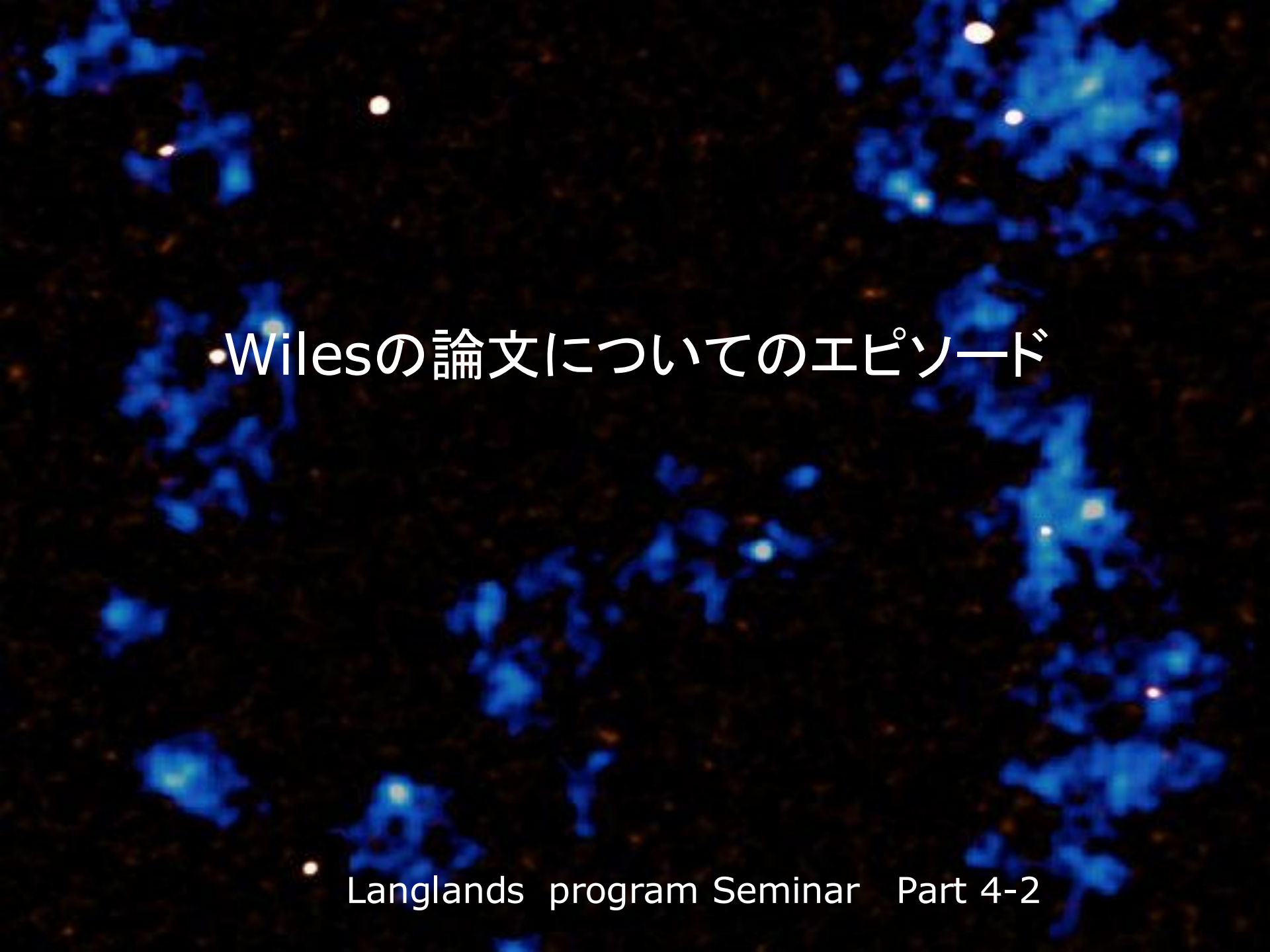
1978年までに、Samuel Wagstaffはこれを125,000未満の素数すべてに拡張した。

1993年までに、フェルマーの最終定理は400万未満の素数すべてについて証明された。

しかし、これらの努力と成果にもかかわらず、フェルマの最終定理の証明は存在しなかった。

個々の指数の証明は、その性質上、一般的な場合を証明することは決してできない。たとえすべての指数が非常に大きな数 X まで検証されたとしても、X を超えるより高い指数が存在し、その主張が真実ではない可能性がある。

https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem


Wilesの論文についてのエピソード
Langlands program Seminar Part 4-2

Wilesの歴史的な論文についてのエピソード

このセッションでは、「フェルマーの最終定理」を解決したWilesの歴史的な論文についてのエピソードを紹介しようと思います。

その論文は、“Modular elliptic curve and Fermat’s Last Theorem” というタイトルで、1995年に、Annals of Mathematics 142巻の443-551ページに公開されています。

以前にも紹介しました。

Annals of Mathematics, **142** (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By Andrew Wiles*

For Nada, Clare, Kate and Olivia

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat

Introduction

An elliptic curve over **Q** is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a

https://staff.fnwi.uva.nl/a.l.kret/Galoistheorie/wiles.pdf

ところが、この論文には、1995年に、Annals of Mathematics 141巻の443-551ページに公開されてiる、別のバージョンがあります。

著者の写真が入っているのと、Introductionの前に、Abstractが入っているところが違っています。

こんな感じです。

Annals of Mathematics, **141** (1995), 443-551

Pierre de Fermat

Modular elliptic curves and Fermat's Last Theorem

By Andrew John Wiles*

For Nada, Claire, Kate and Olivia

Andrew John Wiles

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatum in duos ejusdem nominis fas est dividere: cujes rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

- Pierre de Fermat ~ 1637

Abstract. When Andrew John Wiles was 10 years old, he read Eric Temple Bell's *The Last Problem* and was so impressed by it that he decided that he would be the first person to prove Fermat's Last Theorem. This theorem states that there are no nonzero integers a, b, c, n with $n > 2$ such that $a^n + b^n = c^n$. The object of this paper is to prove that all semistable elliptic curves over the set of rational numbers are modular. Fermat's Last Theorem follows as a corollary by virtue of previous work by Frey, Serre and Ribet.

http://www.scienzamedia.uniroma2.it/~eal/Wiles-Fermat.pdf

Abstract はずいぶん長いもので、研究の経緯を示す論文の貴重なまとめになっています。多分、Wilesにしか書けないものだと思います。

でも、長いAbstractを含んでいるのに、両者のページ数が同じなのは奇妙です。実際のAnnals of Mathematics誌をチェックすれば分かることなのですが、僕にはできませんでした。

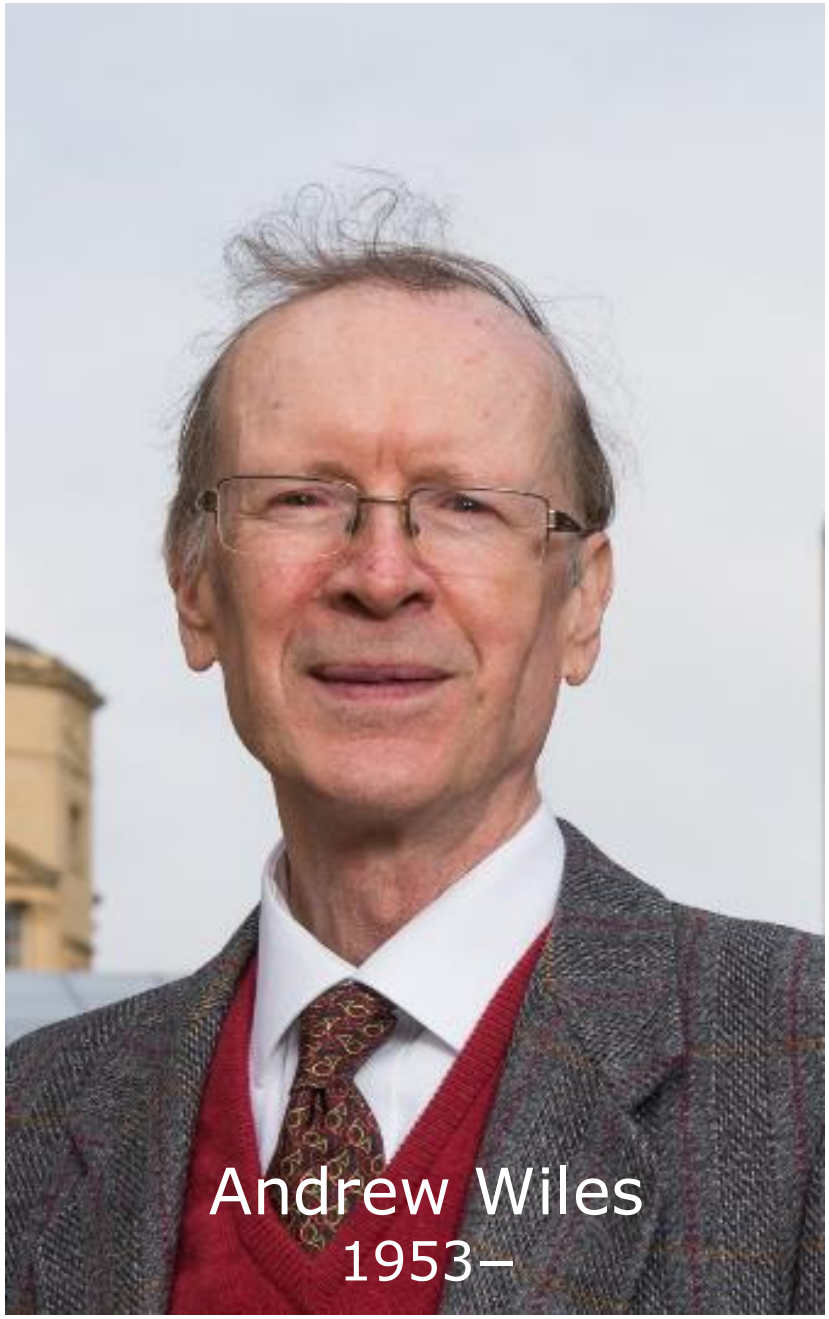
多分、Wilesのジョークなのだろうとも思います。

写真は、フェルマーの定理に興味を覚えた、Wilesが10歳の時のものだと思います。

Andrew Wiles

1995年、Andrew Wiles は、300年以上未解決だった、「フェルマーの定理」を証明した。

証明の成功だけでなく、彼が証明のために開発した多くの新しい手法は、現代の数学に、深い影響を与えた。



Andrew Wiles

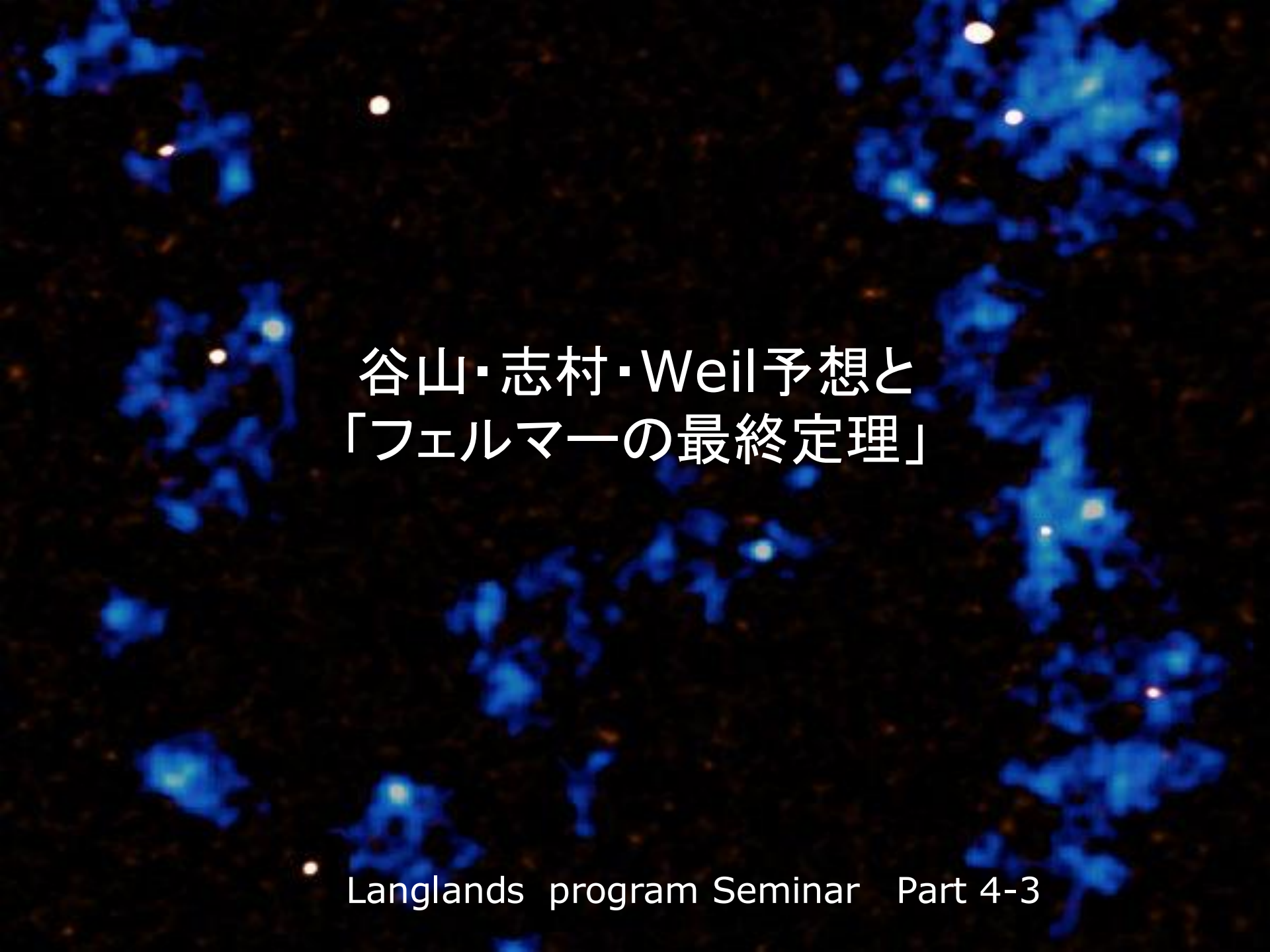
1995年、Andrew Wiles は、300年以上未解決だった、「フェルマーの定理」を証明した。

証明の成功だけでなく、彼が証明のために開発した多くの新しい手法は、現代の数学に、深い影響を与えた。

Wilesには、他にも面白いエピソードがあります。

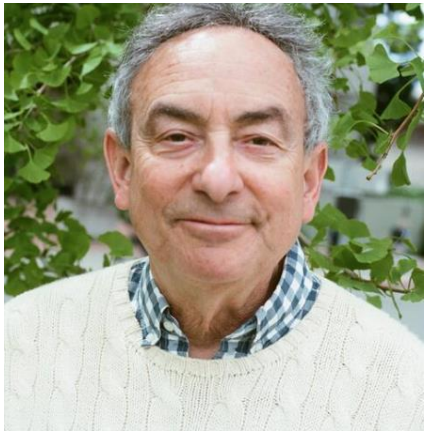
フェルマーの最終定理に取り組んでいることを、ずっと皆に隠していたとか、完全な証明が完成する1994年以前の1993年に、「証明ができた！」と大々的な発表会をしたのに、撤回したとか。

次回のセッションでは、Wilesの証明の鍵になった、フェルマーの最終定理と谷山・志村・Weil予想の関係の話をします。

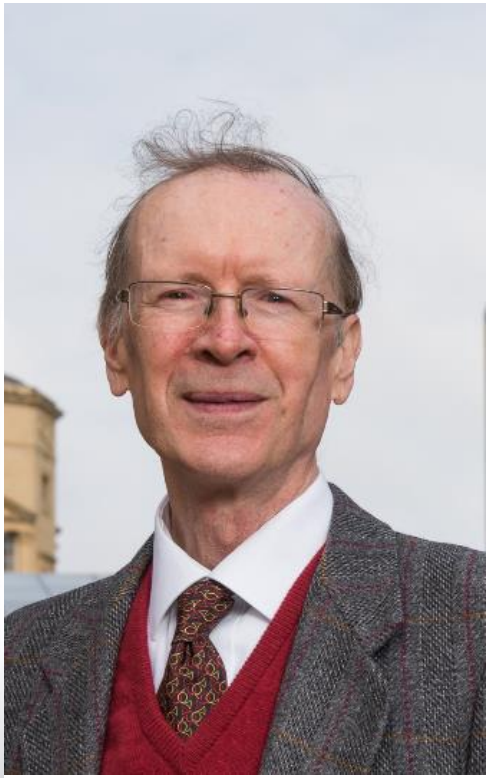

谷山･志村･Weil予想と
「フェルマーの最終定理」
Langlands program Seminar Part 4-3

今回のセッションの主要な登場人物

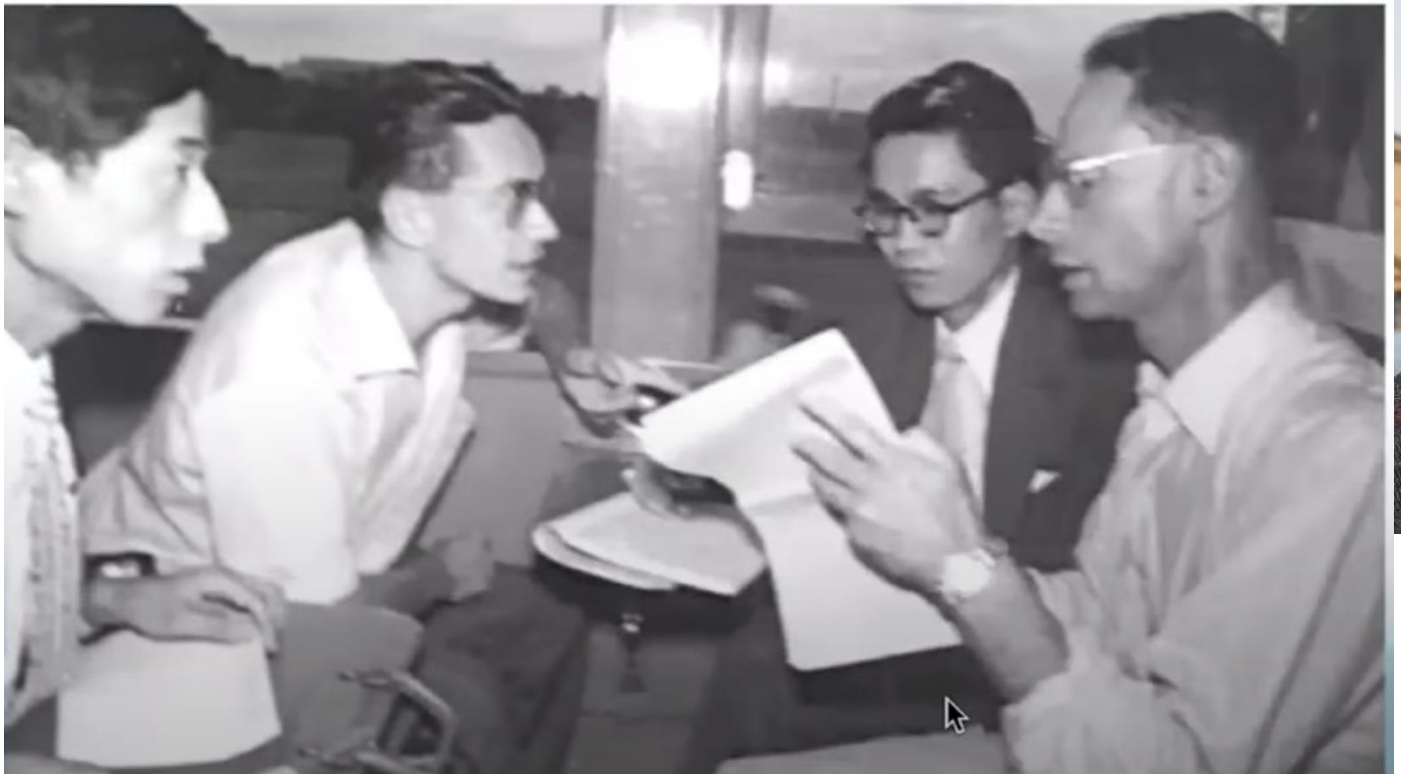
Gerhard Frey



Ken Ribet



Andrew Wiles



志村五郎　**Jean-Pierre Serre**　谷山豊　**André Weil**

Wilesの証明に先行した動き

「フェルマーの最終定理」は、これまで見てきたように、最終的にはWilesによって20世紀末 1995年に解決されるのだが、それに先行した重要な動きがある。

このセッションでは、Wilesの証明を準備した、これらの動きを紹介しようと思う。

「フェルマーの最終定理」と楕円曲線との接点
1985年　Freyの新しいアイデア

Freyは、「フェルマーの最終定理」の反例となるような整数(a, b, c, p)が存在するとすると、何が起きるかを考えた。

すなわち、pは≥ 3の素数で、次の式が成り立っているとする。

$$a^p + b^p = c^p$$

この時、Freyは、次のような楕円曲線を考える。

$$y^2 = x(x - a^p)(x + b^p)$$

この仮想的に構成された曲線をFrey curveと呼ぶ。

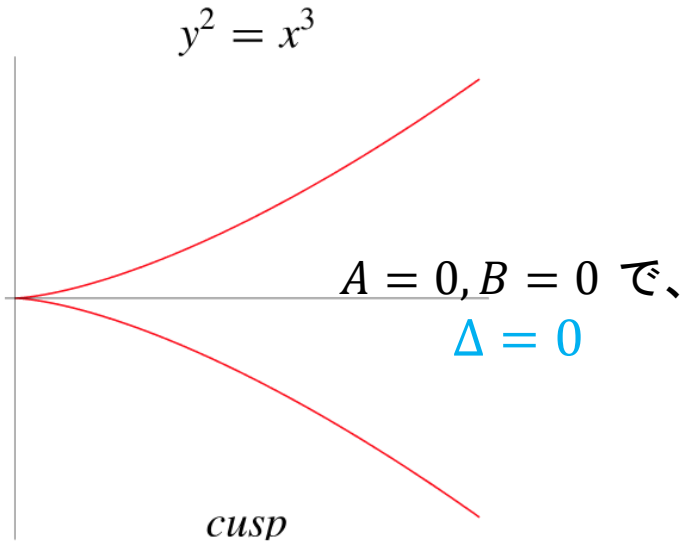
Frey curveの奇妙な性質

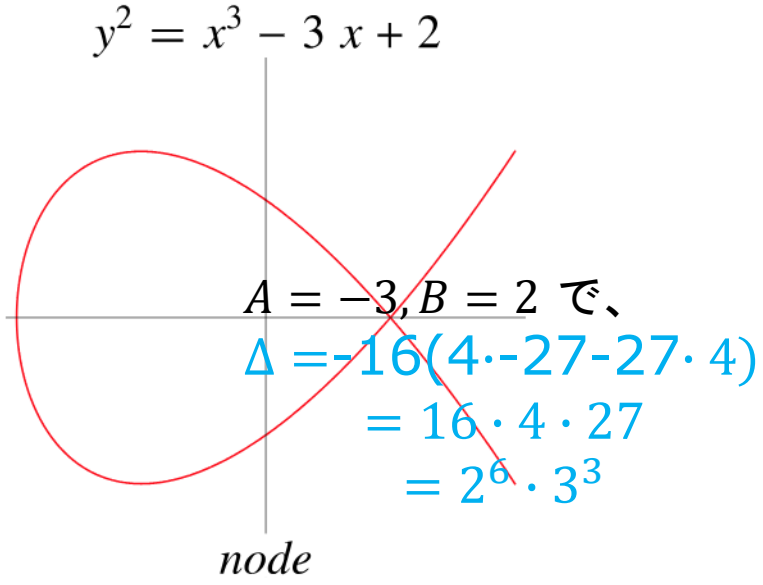
Freyは、この曲線が,奇妙な性質を持っていることに気づく。

楕円曲線 $y^2 = x^3 + Ax + B$の判別式Δは、次の式で定義される。

$$\Delta = -16(4A^3 - 27B^2)$$

例えば、次のように。





Frey curveの判別式を計算してみる。

$$y^3 = x(x - a^p)(x + b^p)$$
$$= x(x^2 - (a^p - b^p) - a^p b^p))$$

この時、Frey curveの最小判別式は、次の 平方数の形を取る。

$$(a^p b^p c^p)^2$$

Freyが考えたこと

Freyは、どうもおかしいと考え始める。

これは、このような楕円曲線は存在しないことを意味しているのではないかと。

彼はさらに考える。

全ての楕円曲線は、モジュラーである」という谷山・志村・Weil予想が正しいとするなら、フェルマー最終定理の反例から構成されたFrey curveが存在しないことは、それがモジュラーでないことを示せばいいと。

Non-abelian approach

Frey (1985): New idea! Suppose $a^p + b^p = c^p$, p prime ≥ 3, $a, b, c \in \mathbb{Z}$.

Consider $y^2 = x(x - a^p)(x + b^p)$.

Discriminant is $(a^p b^p c^p)^2$.

Non-abelian approach

Frey (1985): New idea! Suppose $a^p + b^p = c^p$, p prime ≥ 3, $a, b, c \in \mathbb{Z}$.

Consider $y^2 = x(x - a^p)(x + b^p)$.

Discriminant is $(a^p b^p c^p)^2$.

Such a curve should not exist! Discriminants should not be p^{th} powers.

Non-abelian approach

Frey (1985): New idea! Suppose $a^p + b^p = c^p$, p prime ≥ 3, $a, b, c \in \mathbb{Z}$.

Consider $y^2 = x(x - a^p)(x + b^p)$.

Discriminant is $(a^p b^p c^p)^2$.

Such a curve should not exist! Discriminants should not be p^{th} powers.

New way to prove F.L.T.: show there is no such elliptic curve.

フェルマーの最終定理証明の新しいアプローチ

フェルマーの最終定理に対する反例は、モジュラーでない楕円曲線が存在することを意味する。

フェルマーの最終定理を反証できる数（a、b、c、n）の集合は、谷山・志村・Weil予想を反証するのにも使えると考える十分な理由がある。

したがって、もし谷山・志村・Weil予想が真であれば、フェルマーを反証できる数の集合は存在し得ないので、フェルマーの最終定理も真でなければならない。

Serreのイプシロン予想

谷村・志村・Weil予想とフェルマーの最終定理には、つながりがあるというFreyの直感は、正しいものだった。

ただ、このつながりを完成させるためには、Frey曲線が存在するとしても、それはモジュラーではありえないことを示す必要があった。

1985年、Jean-Pierre SerreはFrey曲線がモジュラーになり得ないことを部分的に証明した。その完全な証明のために残された必要な部分は、「Serreのイプシロン予想」と呼ばれる。

「Frey curveはモジュラーではない」
Ribetの定理　1986年

1986年夏、Ken Ribetは、現在Ribetの定理として知られているε予想の証明に成功した。彼の論文は1990年に出版された。

その際、Ribetは、Freyが示唆したように、Freyが特定した種類の楕円曲線に対する谷山-志村-Weil予想の証明が、Ribetの定理とともにフェルマーの最終定理をも証明することを確認し、2つの定理の関連性を最終的に証明した。

数学的な言い方をすれば、Ribetの定理は、楕円曲線に関連するガロア表現がある性質（Freyの曲線が持っている）を持っている場合、その曲線は、同じガロア表現を生じさせるモジュラー形式が存在しないという意味で、モジュラーではありえないことを示した。

Wilesの証明直前の到達点

Frey曲線に関連するSerreとRibetによる発展、そしてフェルマの最終定理と谷山・志村・Weil予想との関連に従えば、フェルマーの最終定理の証明は、谷山-志村-Weil予想の証明、あるいは少なくともFreyの方程式を含む種類の楕円曲線（半安定楕円曲線として知られている）についての予想の証明から導かれることになる。

ただ、ほとんどすべての数学者が、谷山-志村-Weil予想そのものを現在の知識では証明することが全く不可能であると見ていたため、フェルマーに対するこのアプローチも広く使えないと考えられていたという。

例えば、ワイルズの元指導教員であるジョン・コーツは、「実際に証明することは不可能」であると述べており、Ken Ribetは、自分自身を「(それが)完全にアクセス不可能であると信じていた大多数の人々の一人」であると考えていたという。

Ribetは後に、「Wilesはおそらく、実際にそれを証明することができると夢見る大胆さを持った、地球上で数少ない人物の一人であった」とコメントしている。

Wilesの証明の成功

「RibetがFreyの関連性を証明したことを知ったAndrew Wilesは、フェルマーの最終定理に幼少の頃から魅了され、楕円曲線や関連分野の研究をしていた経験から、フェルマーの最終定理を証明する手段として、谷山-志村予想を証明しようと決意した。

1993年、6年間にわたって秘密裏にこの問題に取り組んだ後、ワイルズはフェルマーの最終定理を証明するのに十分なこの予想の証明を成功させた。

ワイルズの論文は、その規模と範囲において膨大なものだった。査読の過程で、当初の論文の一部分に誤りが見つかり、その修正にはさらに1年を要し、かつての教え子であるRichard Taylorとの共同作業が必要となった。」

「その結果、1995年に最終的な証明が発表された。その際、修正された手順が有効であることを示す小規模な共同論文も発表された。

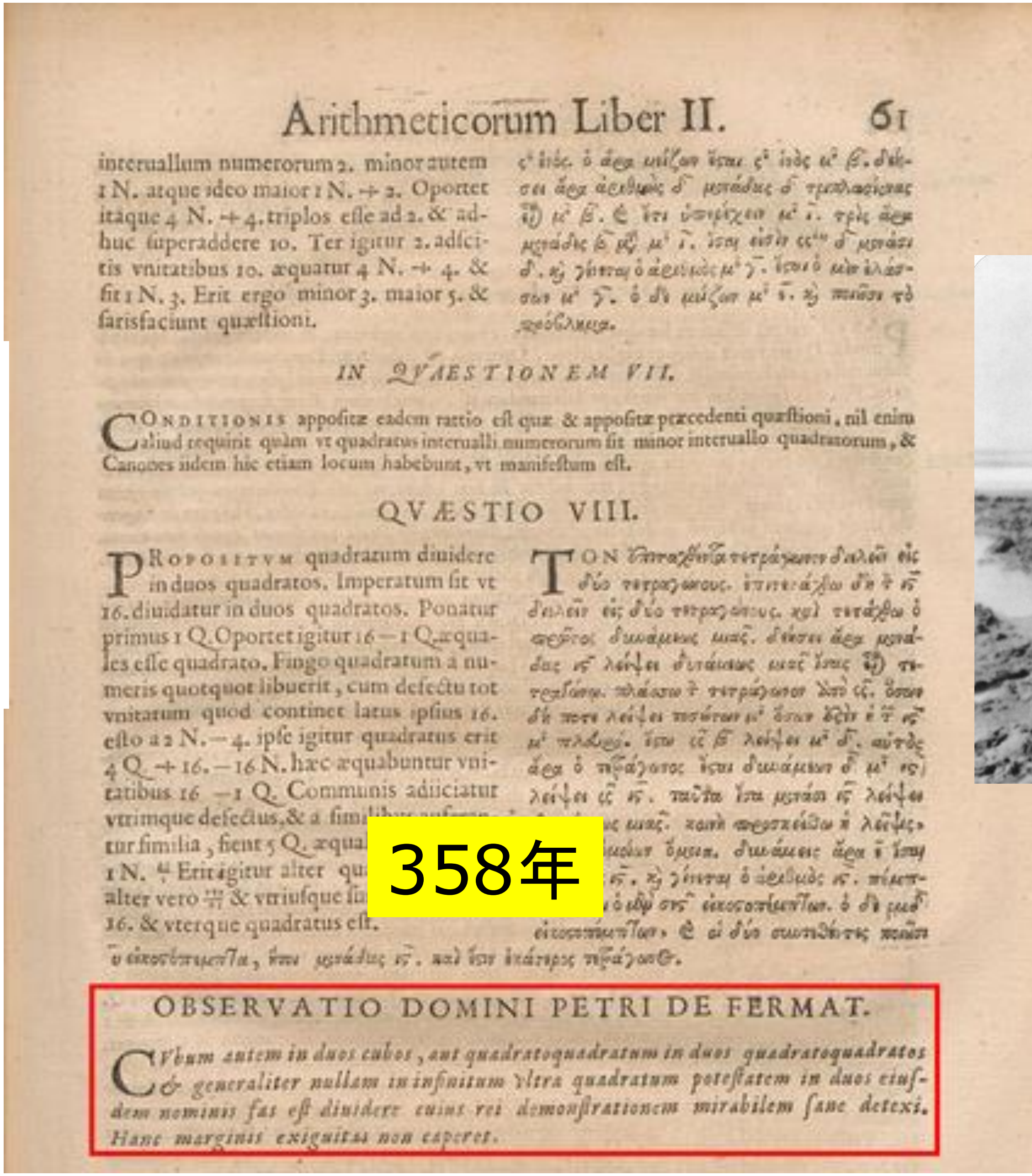
ワイルズの功績は一般紙でも広く報道され、書籍やテレビ番組でも取り上げられた。谷山・志村・Weil予想の残りの部分は、後に証明され、モジュラー性定理として知られるようになった。

これは、1996年から2001年の間にワイルズの研究を基に他の数学者たちによって証明された。 ワイルズは、この証明により、2016年のアーベル賞を含む数々の賞を受賞した。」

https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem

Pierre de Fermat

1637年



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVÆSTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 – 1 Q. æquales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. – 4. ipse igitur quadratus erit 4 Q. + 16. – 16 N. hæc æquabuntur vnitatibus 16 – 1 Q. Communis adiiciatur vtrimque defectus, & a simi[...] tur similia, fient 5 Q. æqua[...] 1 N. $\frac{16}{5}$ Erit igitur alter qu[...] alter vero $\frac{144}{25}$ & vtriusque su[...] 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

358年

1995年

Annals of Mathematics, **141** (1995), 443-551

Pierre de Fermat

Modular elliptic curves and Fermat's Last Theorem

By Andrew John Wiles*

For Nada, Claire, Kate and Olivia

Andrew John Wiles

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatum in duos ejusdem nominis fas est dividere: cujes rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

- Pierre de Fermat ~ 1637

Abstract. When Andrew John Wiles was 10 years old, he read Eric Temple Bell's *The Last Problem* and was so impressed by it that he decided that he would be the first person to prove Fermat's Last Theorem. This theorem states that there are no nonzero integers a, b, c, n with $n > 2$ such that $a^n + b^n = c^n$. The object of this paper is to prove that all semistable elliptic curves over the set of rational numbers are modular. Fermat's Last Theorem follows as a corollary by virtue of previous work by Frey, Serre and Ribet.


HITACHI
危い!