

学術俯瞰講義 ～数学を創る～ 第2回

Mathematics “On Campus”

ことばを創り、世界を創る

2009. 10. 15

※:このマークが付してある著作物は、第三者が有する著作物ですので、同著作物の再使用、同著作物の二次的著作物の創作等については、著作権者より直接使用許諾を得る必要があります。

中

On Campus

東京大学教養学部英語部会 編

Department of English, The University of Tokyo, Komaba



スタンダード

大学で学ぶ英語の新たな標準!

東大発のベストセラー教科書「ユニヴァース」シリーズのエッセンスを受け継ぎながら、新しいコンセプトでおくる

● 文・理最先端のテキスト、より詳細なノート、読みやすい二色刷

東京大学出版会

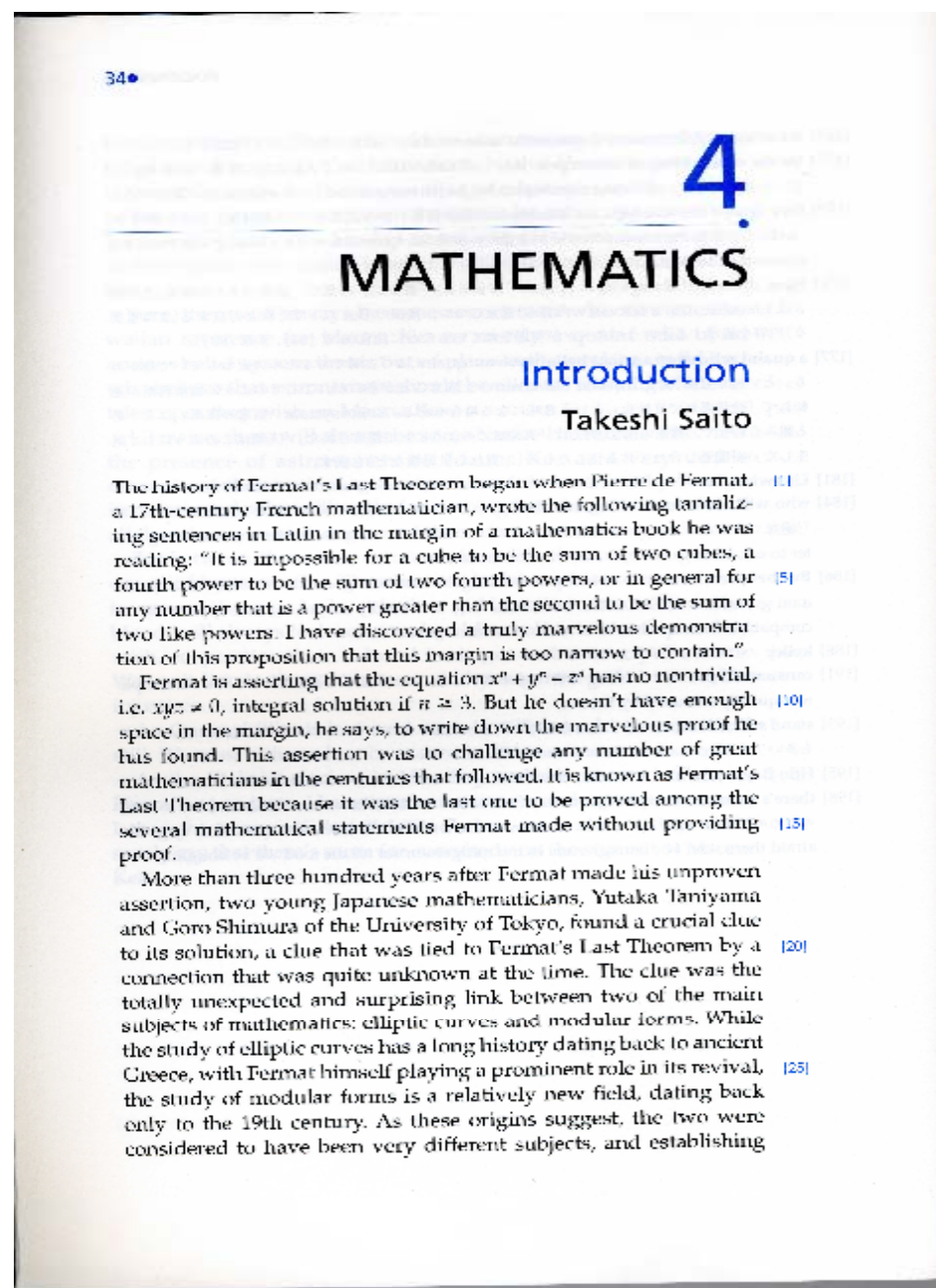
東京大学教養学部英語部会 (編集)
『On Campus』
東京大学出版会 (2006/03)

Mathematics

On Campus

東京大学教養学部英語部会 (編集)
『On Campus』
東京大学出版会 (2006/03)

+



Fermat's Last Theorem

東京大学教養学部英語部会 (編集)
『On Campus』
東京大学出版会 (2006/03)

+

34 ● MATHEMATICS

4.

MATHEMATICS

Introduction

Takeshi Saito

The history of Fermat's Last Theorem began when Pierre de Fermat, a 17th-century French mathematician, wrote the following tantalizing

sentences in Latin in the margin of a mathematical book while reading: "It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers. I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain."

Fermat is asserting that the equation $x^n + y^n = z^n$ has no nontrivial, i.e. $xyz \neq 0$, integral solution if $n \geq 3$. But he doesn't have enough space in the margin, he says, to write down the marvelous proof he has found. This assertion was to challenge any number of great mathematicians in the centuries that followed. It is known as Fermat's Last Theorem because it was the last one to be proved among the several mathematical statements Fermat made without providing proof.

assertion, two young Japanese mathematicians, Yutaka Taniyama and Goro Shimura of the University of Tokyo, found a crucial clue to its solution, a clue that was tied to Fermat's Last Theorem by a connection that was quite unknown at the time. The clue was the totally unexpected and surprising link between two of the main subjects of mathematics: elliptic curves and modular forms. While the study of elliptic curves has a long history dating back to ancient Greece, with Fermat himself playing a prominent role in its revival, the study of modular forms is a relatively new field, dating back only to the 19th century. As these origins suggest, the two were considered to have been very different subjects, and establishing

Fermatの書きこみ (1640年頃?)

It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number greater than the second to be the some of two like powers. I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain.

Fermatの書きこみ(原語バージョン)

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:
cujui rei demonstrationem mirabilem sane
detexi. Hanc, marginis exiguitas non
caperet.

Fermat's last theorem

Fermat is asserting that the equation

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

has no nontrivial, i.e. $xyz \neq 0$, integral solution if $n \geq 3$.

But he doesn't have enough space in the margin, he says, to write down the truly marvelous proof he has found.

フェルマーの最終定理(予想)

フェルマーは、方程式

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

の整数解は、 $n \geq 3$ とすると、自明なもの、つまり $xyz = 0$ をみたすものしかないことを主張した。しかし、この余白には、彼がみつけた素晴らしい証明を書くだけの広さが無い、と書きのこした。

Pierre de Fermat

(1601.8.20-
1665.1.12)

フランスの
トゥールーズの人
「数論の父」



http://en.wikipedia.org/wiki/File:Pierre_de_Fermat.png

Pierre de Fermat

(1601.8.20-
1665.1.12)

フランスの
トゥールーズの人
「数論の父」



http://en.wikipedia.org/wiki/File:Pierre_de_Fermat.jpg

フェルマーが
書きこんだ本
と同じ本

アレキサンドリアの
ディオファントス
(3世紀)の数論の本
のバシェによる復刊
(1621年)





ディオファントス(～300)

フェルマーが 書きこんだ ページ と同じページ



フェルマーの最終定理

$n \geq 3$.

方程式

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

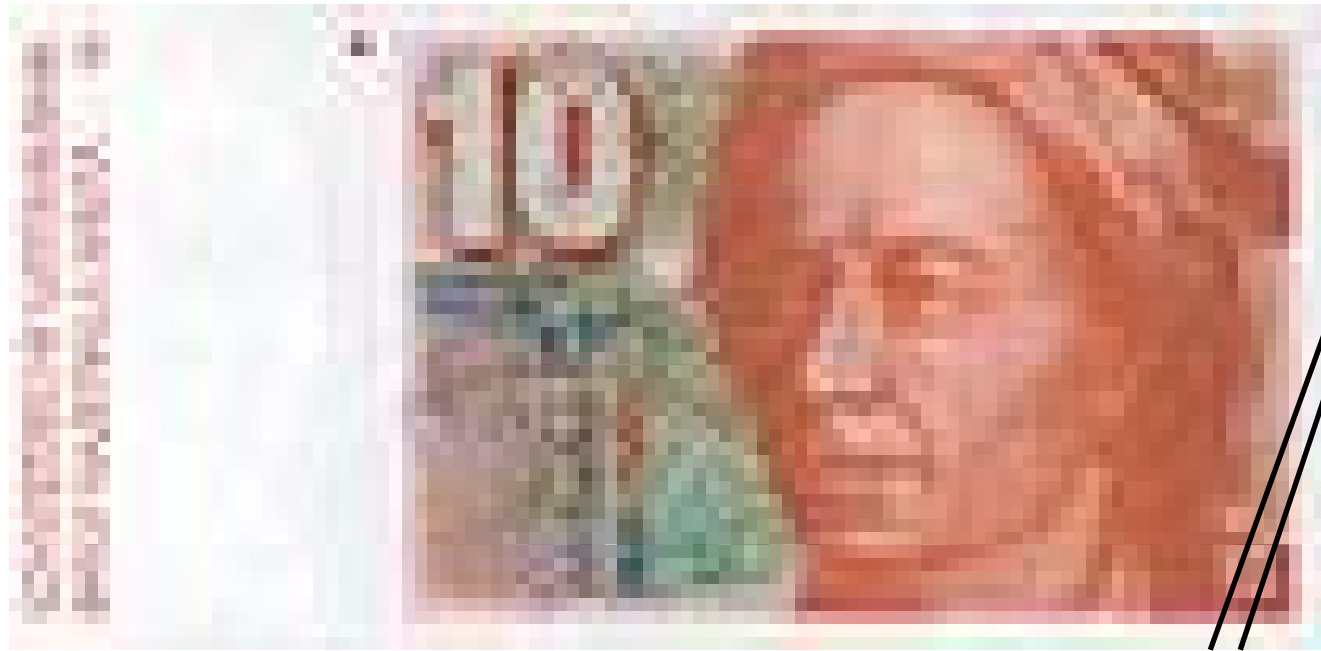
整数解

$$(x, y, z) = (a, b, c)$$

a, b, c のうち 1つは 0

フェルマーの最終定理の解決まで

- ~1640 フェルマー 余白に書き込み
- ~1659 フェルマー $n=4$ の場合
- 1753 オイラー $n=3$ の場合



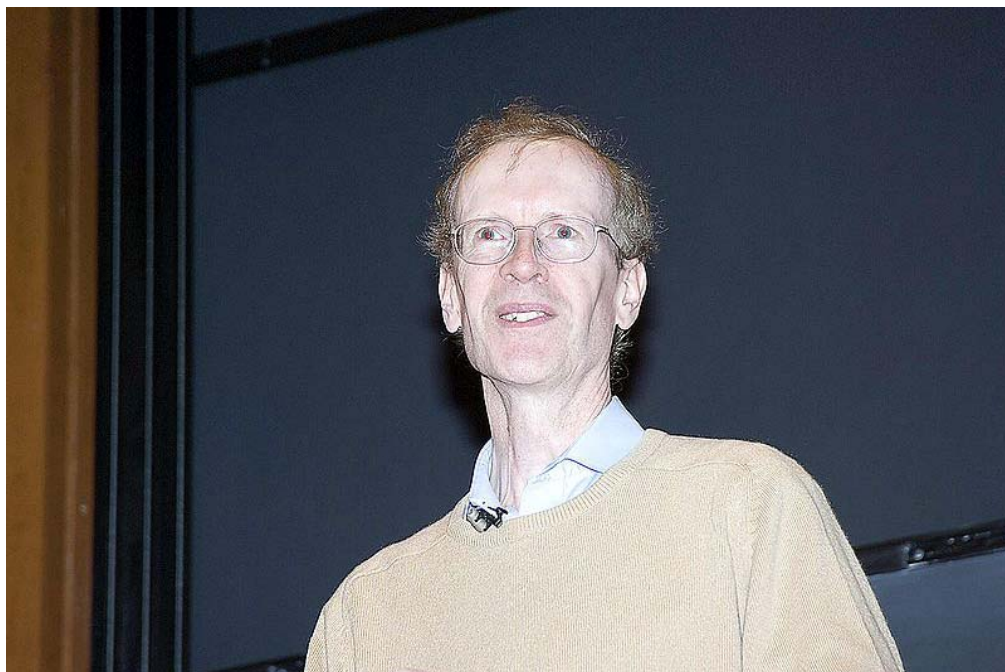
オイラー(1707.4.15 – 1783.9.18)

フェルマーの最終定理の解決まで

- ~1640 フェルマー 余白に書き込み
- ~1659 フェルマー $n=4$ の場合
- 1753 オイラー $n=3$ の場合

.....

- 1994 ワイルズ・テイラー 証明



"copyright C. J. Mozzochi, Princeton N.J"

http://www.mozzochi.org/deligne60/Deligne1/_DSC0024.jpg

著作権処理の都合で

この場所に挿入されていた

Modular elliptic curves and
Fermat's Last Theorem

を省略させていただきます。

ワイルズ(1953.4.11-)と 証明が発表された論文

フェルマーの最終定理の難しさ

- 問題の意味 わかりやすい
表面的には中学生でもわかる!?
- 手がかりが見えない

フェルマーの最終定理の難しさ

なぜ3世紀半かかったのか？

解ける世界を創っていたから

フェルマーの最終定理の解決まで

- ~1640 フェルマー 余白に書き込み
- ~1659 フェルマー $n=4$ の場合
- 1753 オイラー $n=3$ の場合
- 1800~ ガウスほか 楕円曲線
- 1850~ アイゼンシュタインほか 保型形式
- 1960~ 谷山・志村 楕円曲線と保型形式
- 1986 フライ 最終定理と楕円曲線
- 1994 ワイルズ・テイラー 証明

$$n=lm.$$

a, b, c が $x^n + y^n = z^n$ の解なら

a^m, b^m, c^m は $x^l + y^l = z^l$ の解



$n = l$ が 3以上の素数の場合と、

$n = l$ が 4の場合 に帰着

素数 (prime number)

- 自然数 $p \geq 2$ で、
1 と p 以外の自然数では
わりきれないもの.
- 1 は素数ではない.
(素因数分解の一意性)

素数

- 素数は無限個ある.
(古代ギリシャで証明)
- 2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 87,
89, 97, 101, 103, 107, 109, 113, 127, 131,
137, 143, 149,
- 未解決問題多数

素数は無限個ある.

$$2, 2 + 1 = 3,$$

$$2 \cdot 3 + 1 = 7,$$

$$2 \cdot 3 \cdot 7 + 1 = 43,$$

$$2 \cdot 3 \cdot 7 \cdot 43 + 1 = 13 \cdot 139$$

$$2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 + 1 = 53 \cdot 443$$

.....

フェルマー素数

$2^n + 1$ が素数 $\longrightarrow n = 2^m$

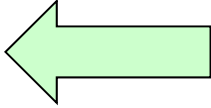
$$2^3 + 1 = 3^2, \quad 2^5 + 1 = 3 \cdot 11,$$

$$2^6 + 1 = 5 \cdot 13,$$

$$2^{10} + 1 = 5^2 \cdot 401,$$

.....

フェルマー素数

逆 $2^n + 1$ が素数  $n = 2^m$
も正しい? (フェルマー)

$$2^1 + 1 = 3, \quad 2^2 + 1 = 5,$$

$$2^4 + 1 = 17, \quad 2^8 + 1 = 257,$$

$$2^{16} + 1 = 65537,$$

.....

フェルマー素数

$$2^{16} + 1 = 65537,$$

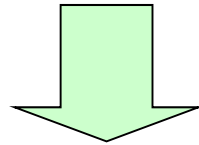
$$2^{32} + 1 = 641 \cdot 6700417,$$

(オイラー)

.....

フェルマー素数

$$p = 2^{2^n} + 1 \text{ が素数}$$



正 p 角形は

定規とコンパスで作図できる

(ガウス 1796.3.30)



http://en.wikipedia.org/wiki/File:Carl_Friedrich_Gauss.jpg

ガウス (1777.4.30 - 1855.2.23)

フェルマー素数

セーラー予想の証明

(カレ 2005)

- 素数に関する帰納法
- フェルマー素数でない素数が無限個ある

✦



<http://www.math.ucla.edu/~shekhar/>

カレ (1967 -)

フェルマーの業績

- 接線、最大最小
(微積分のさきがけ)
- 座標の考え
(デカルトと同時代)

フェルマーの業績 「数論の父」

- フェルマーの小定理
- 素数 p が 2乗数 2つの和
となる条件
- 楕円曲線の有理点

.....

フェルマーの小定理

p が素数なら、 $a^p - a$ は p でわりきれる
(RSA暗号の基礎)

$$2^7 - 2 = 128 - 2 = 126 = 7 \times 18,$$

$$2^{11} - 2 = 2048 - 2 = 2046 = 11 \times 186,$$

$$3^5 - 3 = 243 - 3 = 240 = 5 \times 48,$$

.....

素数 $p \neq 2$ が2乗数2つの和

$$p = a^2 + b^2$$

になるための条件:

p を 4 でわるとあまりが 1.

4 でわるとあまりが 1 の素数

2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, ...

$$\begin{aligned} 5 &= 1+4, & 13 &= 4+9, & 17 &= 1+16, & 29 &= 4+25, \\ 37 &= 1+36, & 41 &= 16+25, & 53 &= 4+49, & 61 &= 25+36, \\ 73 &= 9+64, & & & & & & \dots\dots \end{aligned}$$

方程式 $y^2 = x^3 - x$ の有理数解 (楕円曲線)

は

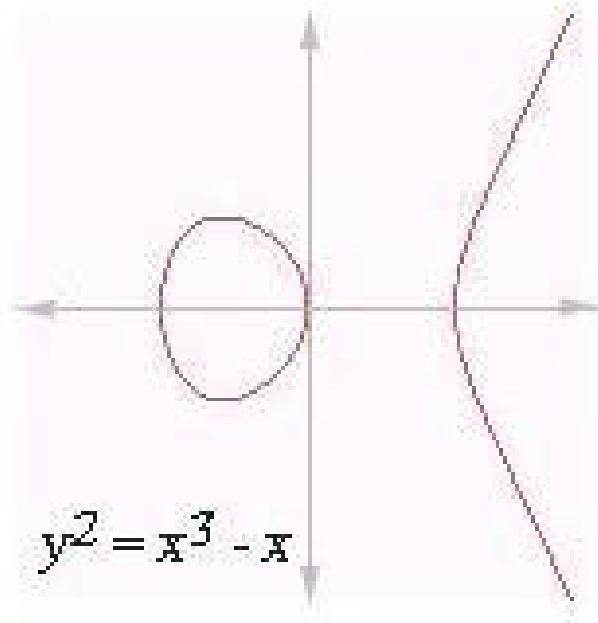
$$(x, y) = (0, 0), (1, 0), (-1, 0)$$

の3つしかない. (無限降下法)

- フェルマーの最終定理の $n = 4$ の場合
- 3 辺の長さがすべて有理数の直角 3 角形で面積が 1 のものは存在しない.

楕円曲線

- $y^2 = x^3 - x$ のように,
方程式 $y^2 = x$ の3次式 で定義される曲線



出典: <http://ja.wikipedia.org/wiki/ファイル:ECexamples01.png>

楕円曲線

- 楕円 $ax^2 + by^2 = 1$ ではない.
(楕円の長さを求める積分と関係)
- 「楕円曲線についてなら、
いくらでも書くことができる。
これは脅しではない」 (S. ラング)

楕円曲線とフェルマーの最終定理

- $n = 3, 4$ の場合

楕円曲線を定める方程式

$$y^2 = x^3 - x \quad (\text{フェルマー}),$$

$$y^3 = x^3 - 1 \quad (\text{オイラー})$$

の有理数解を調べて証明

- n が5以上の素数の場合

楕円曲線を定める方程式 $y^2 = x(x-a^n)(x-c^n)$

そのものの非存在を示して証明



4 テニス(試合の申し込

み受け付けます)

●斎藤毅(数理)

1 数学・整数論

2 わたしは活字中毒で

・説す。本を読んでいるとし

いあわせです。みなさんも本

・・を読みましょう

3 駒場図書館

4 水泳とジョギング

●坪井俊(数理)

1 位相幾何

2 物事を深く勉強できる

時間は無限にあるわけでは



●時

●中

1

物理

方程

トル

2

読書案内

(一般向け)

- サイモン・シン

『フェルマーの最終定理』

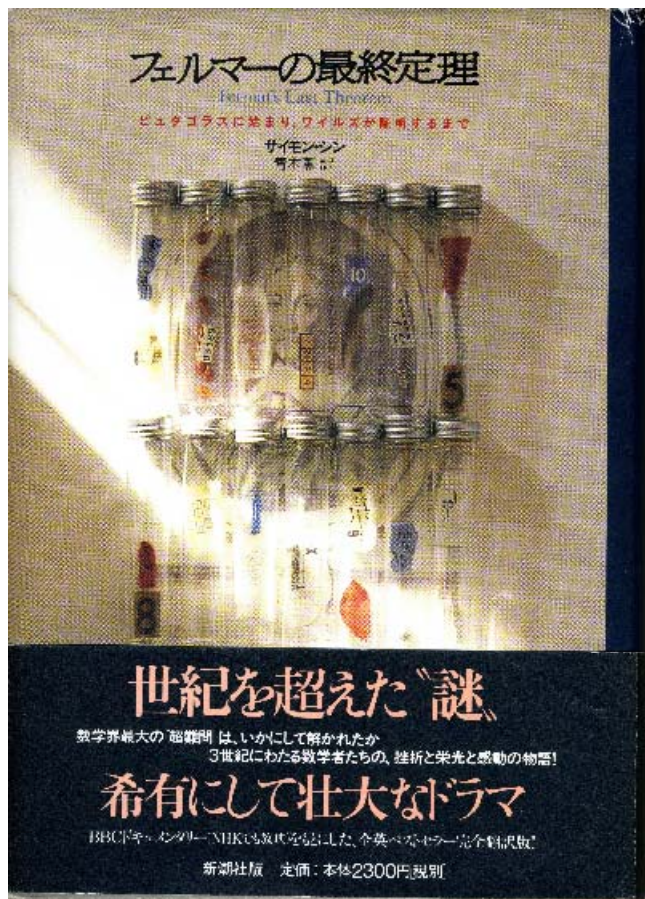
新潮文庫

- 加藤和也

『解決！フェルマーの最終定理』

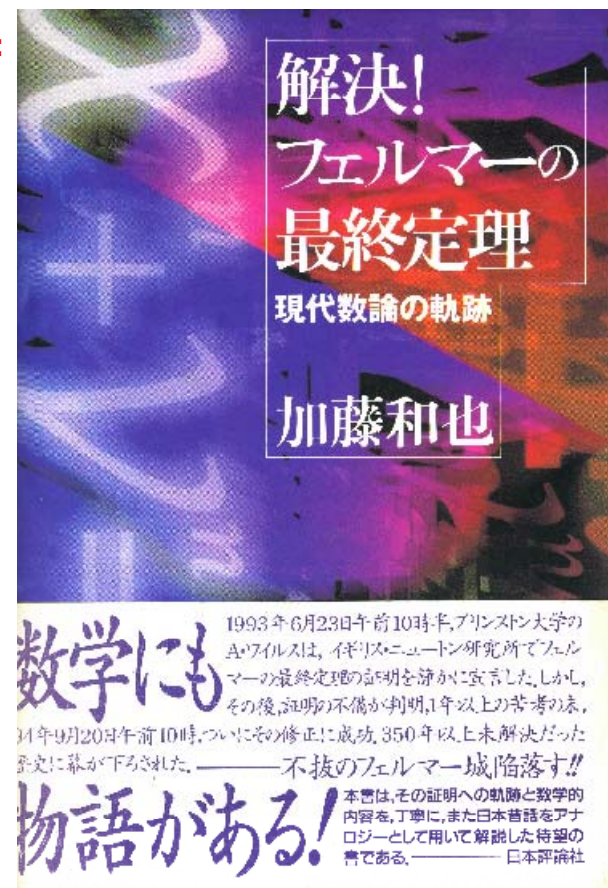
日本評論社

+



サイモン シン (著), Simon Singh (原著), 青木 薫 (翻訳)
『フェルマーの最終定理—ピュタゴラスに始まり、ワイルズ
が証明するまで』
新潮社 (2000/01)

+



加藤和也(著)
『解決！フェルマーの最終定理 現代数論の軌跡』
日本評論社 (1995/10)

読書案内
(入門編)

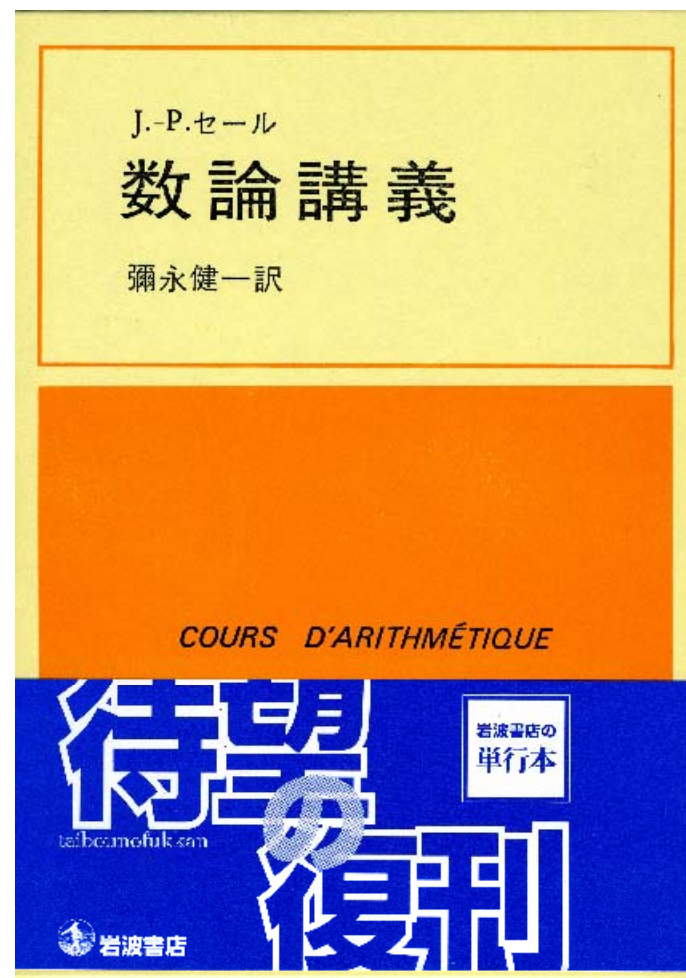
- 藤崎源二郎、森田康夫、山本芳彦
『数論への出発』 日本評論社
- セール
『数論講義』 岩波書店

中



藤崎 源二郎(著), 森田 康夫(著), 山本 芳彦(著)
『数論への出発 増補版』
日本評論社(2004/06)

中



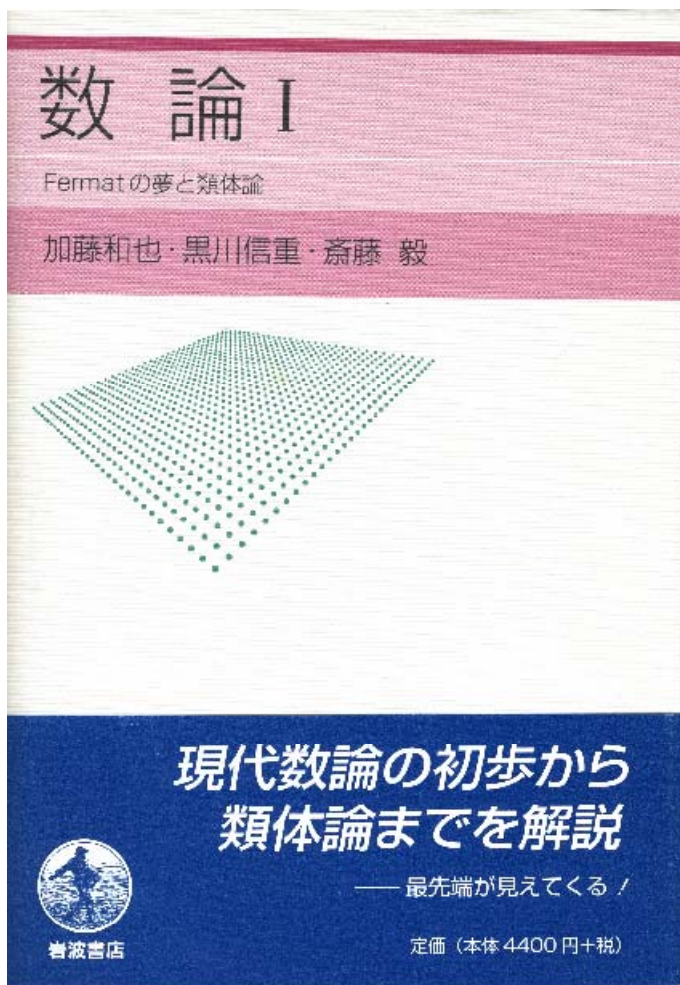
J. - P. セール(著), 彌永 健一(翻訳)
『数論講義』
岩波書店(1979/01)

読書案内

(中級編)

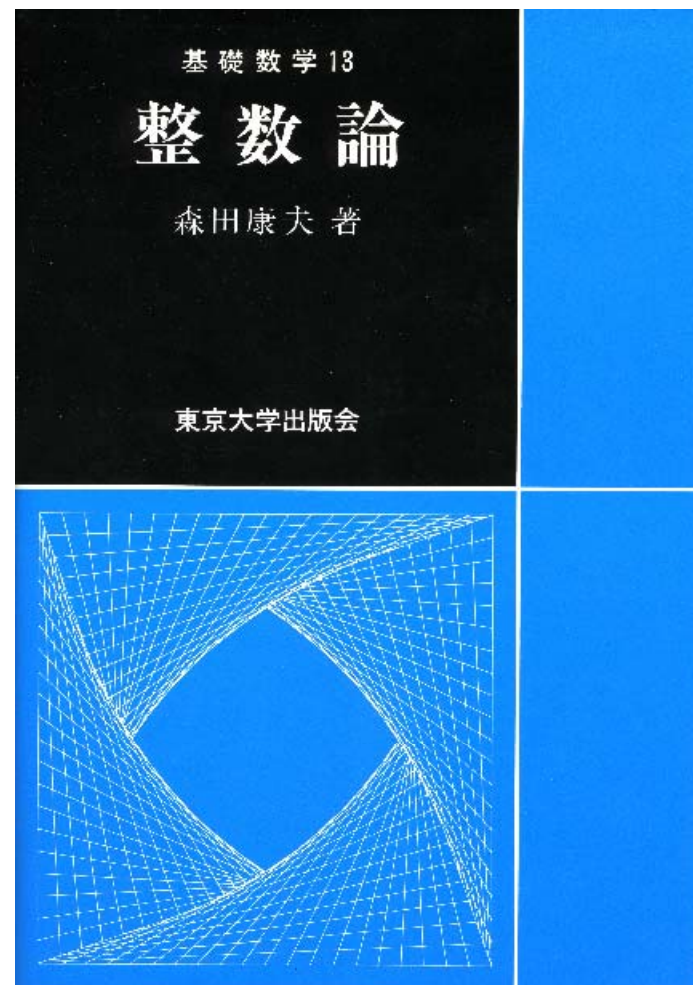
- 加藤和也、栗原将人、黒川信重、
斎藤 毅
『数論I, II』 岩波書店
- 森田康夫
『整数論』 東京大学出版会

中



加藤 和也(著), 黒川 信重(著), 斎藤 毅(著)
『数論(1) Fermatの夢と類体論』
岩波書店(2005/01)

中



森田 康夫(著)
『基礎数学13 整数論』
東京大学出版会(1999/03)

読
書
案
内

- ・ 足立恒雄

『フェルマーの大定理—整数論の源流』

日本評論社

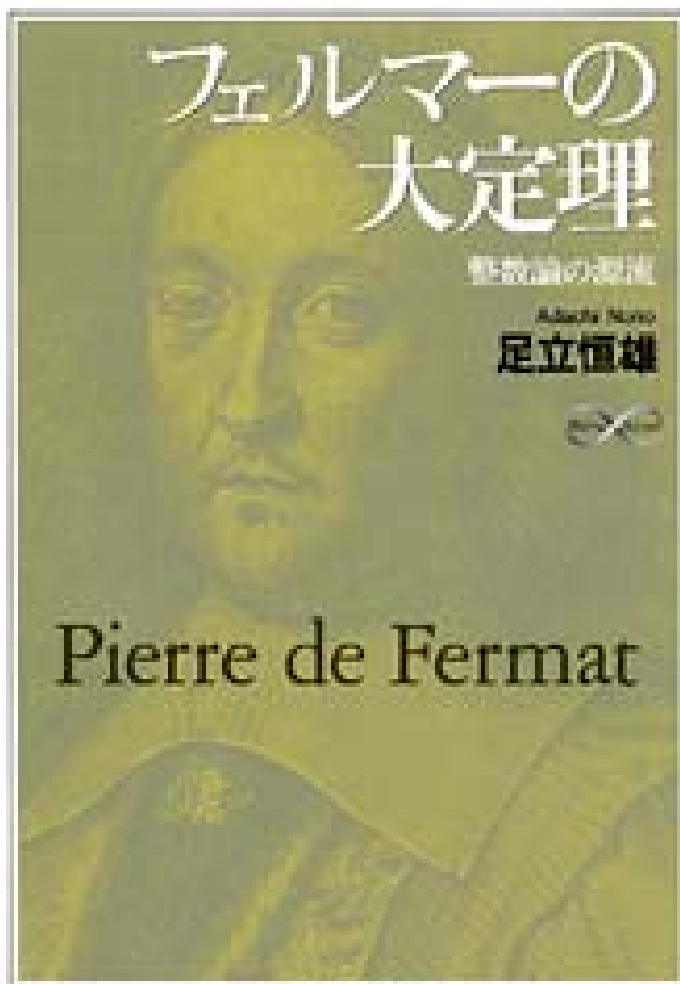
(歴
史
編)

- ・ アンドレ・ヴェイユ

『数論—歴史からのアプローチ』

日本評論社

+



足立 恒雄(著)
『フェルマーの大定理—整数論の源流』
筑摩書房(2006/09)

+



アンドレ ヴェイユ(著), 足立 恒雄(翻訳), 三宅 克哉(翻訳)
『数論—歴史からのアプローチ』
日本評論社(1987/12)

読書案内

(上級編)

- 加藤和也

『フェルマーの最終定理・

佐藤-テイト予想解決への道』

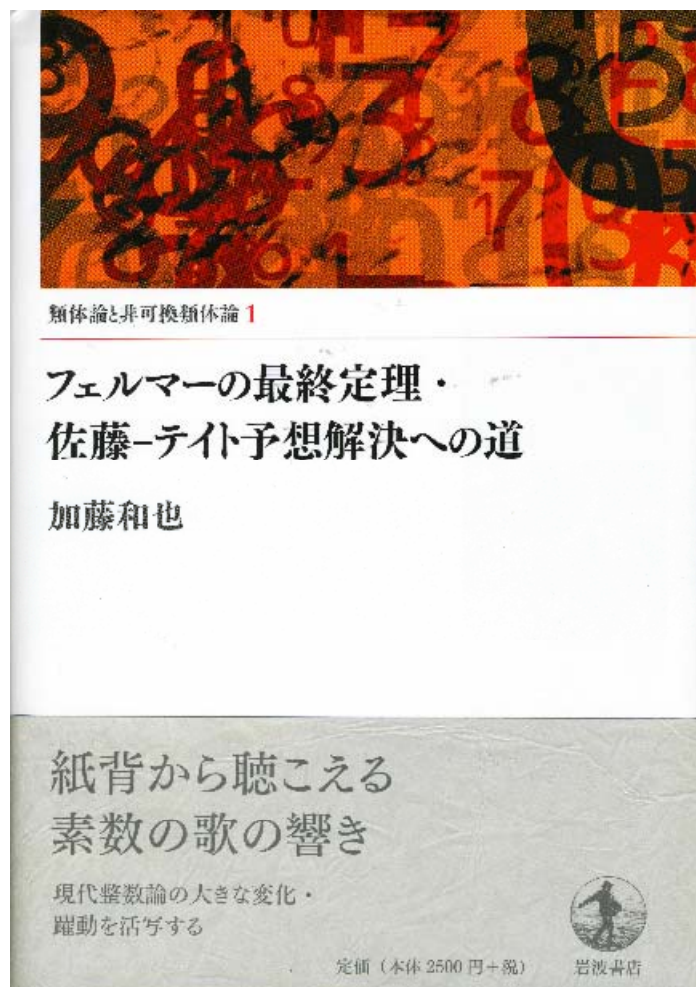
岩波書店

- 斎藤 毅

『フェルマー予想』

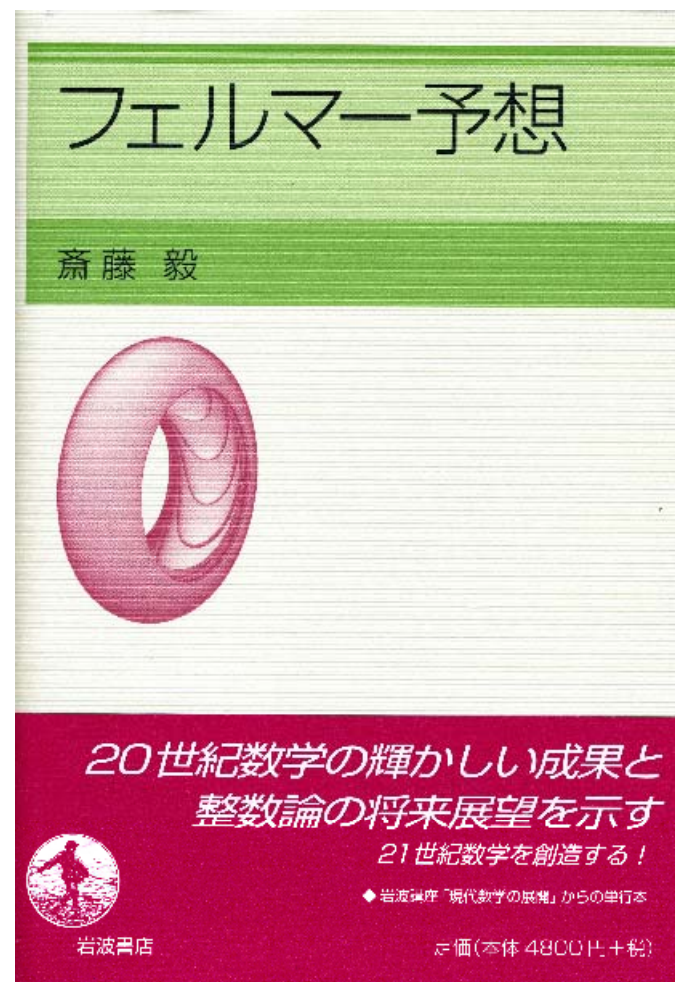
岩波書店

✦



加藤 和也(著)
『フェルマーの最終定理・佐藤 - テイト予想
解決への道』
岩波書店(2009/01)

✦



斎藤 毅(著)
『フェルマー予想』
岩波書店(2009/02)

読書案内 (番外編)



斎藤 毅(著)
『線形代数の世界—抽象数学の入り口』
東京大学出版会(2007/10)



斎藤 毅(著)
『集合と位相』
東京大学出版会(2009/09)

フェルマーの最終定理

n は5以上の素数

方程式
$$X^n + y^n = Z^n$$

整数解
$$(X, y, Z) = (a, b, c)$$

a, b, c のうち 1つは 0

Taniyama and Shimura

In January of 1954 a talented young mathematician at the University of Tokyo paid a routine visit to his departmental library. Goro Shimura was in search of a copy of *Mathematische Annalen*, Vol. 24. In particular he was after by Deuring on his algebraic theory of complex multiplication, which he needed in order to help him with a particularly awkward and esoteric calculation.

To his surprise and dismay, the volume was already out. The borrower was Yutaka Taniyama, a vague acquaintance of Shimura who lived on the other side of the campus. Shimura wrote to Taniyama explaining that he urgently needed the journal to complete the nasty calculation, and politely asked when it would be returned. A few days later, a postcard landed on Shimura's desk. Taniyama had replied, saying that he too was working on the exact same calculation and was stuck at the same point in the logic. He suggested that they share their ideas and perhaps collaborate on the problem.

谷山豊

(1927.11.12-
1958.11.17)

と

志村五郎

(1930-)

著作権処理の都合で
この場所に挿入されていた
谷山豊と志村五郎の写真
を省略させていただきます。

中



<http://www.s.u-tokyo.ac.jp/imagebank/?mode=show&id=sc0028>

理学部旧1号館

In September 1955 an international symposium was held in Tokyo. It was a unique opportunity for the many young Japanese researchers to show off to the rest of the world what they had learned. They handed around a collection of thirty-six problems related to their work, accompanied by a humble introduction — *Some unsolved problems in mathematics: no mature preparation has been made, so there may be some trivial or already solved ones among these. The participants are requested to give comments on any of these problems.*

Four of the questions were from Taniyama, and these hinted at a curious relationship between modular forms and elliptic equations. These innocent questions would ultimately lead to a revolution in number theory. All of the questions handed out by Taniyama at the symposium were related to his hypothesis that each modular form is really an elliptic equation in disguise. The idea that every elliptic equation was related to a modular form was so extraordinary that those who glanced at Taniyama's questions treated them as nothing more than curious observation. Taniyama's only ally was Shimura, who believed in the power and depth of his friend's idea. Following the symposium, he worked with Taniyama in an attempt to develop the hypothesis to a level where the rest of the world could no longer ignore their work. Shimura wanted to find more evidence to back up the relationship between the modular and elliptic worlds.

東京日光整数論国際研究集会 (1955)

✚



写真提供: 日光金谷ホテル

問 題

問題 11. K を実数体でない、 $F(x)$ を K 上の Hilbert modular form とする、 $F(x)$ を K の L -級数 $L(F, s)$ の Hecke の L -級数の体系が得られて、この $L(F, s)$ と Mellin 変換により、1対1に対応する。このことは Hecke の作用素 T の理論を Hilbert modular 形式に拡張することによって証明される。(cf. Hermann)

問題はこの理論を (必ずしも実数でない) 一般の代数体 K に拡張することである。即ち、 K の素数 p の L -級数が得られるべき多変数の automorphic form を見出して Hecke の作用素 T の理論をこの automorphic function に拡張するのである。

この問題の目的の一つは、 K の量または類体標の L -級数を持つことにある。現在では K が実数の場合にもまだできていない。

問題 12. C を代数体 K 上で定義された楕円曲線とし、 K 上の L -級数を $L_C(s)$ とかく：

$$L_C(s) = \zeta_K(s) \zeta_K(s-1) / L_E(s)$$

は K 上の L -級数である。もし Hasse の予想が K に対して正しいとすれば、 $L_C(s)$ より Mellin 変換で得られる Fourier 級数は特別な形の 2 次元の automorphic form でなければならない。(cf. Hecke) もしそうであればこの形式はその automorphic function の体の付随積分となることは非常に確からしい。

さて、 C に対する Hasse の予想の証明は上のような考察を定めた上で、 $L_C(s)$ が得られるような適当な automorphic form を見出すことによって可能であろうか。

問題 13. 問題 12 に関連して、次のことが考えられる。“State” N の楕円モジュリ

形式を特性づけること、特にこの楕円体の Jacobi 多様体 J を isogenous の意味で単純成分に分解すること。また $N=q$ は素数、且 $q \equiv 3 \pmod{4}$ ならば、 J が法数 q の素数の楕円曲線をふくむことはよく知られているが、一般の N についてはどうであろうか。

問題 29. 記号は問題 28* の通りとする、行列 A は、

$$A = \begin{pmatrix} A_1 & & \\ & A_2 & \\ 0 & & A_3 \end{pmatrix}$$

の形に変形されるが、そのとき $A_1, A_2, A_3, \dots$ の寸法は K の不変数である。(cf. Hasse-Witt) この不変数は G の Jacobi 多様体に対してどのような意味を有するであろうか。

註. K が $q^2=1-x^2$ で定義される場合は次のことがいえる。

- a) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ($p \equiv 1 \pmod{5}$),
- b) $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ ($p \equiv 2$ または $3 \pmod{5}$),
- c) $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ($p \equiv 4 \pmod{5}$),

しかも b) の場合は多様体は可約である。類似の結果が $q^2=1-x^2$ (q は素数) で定義される K のときも成立することは、極めて確からしい。

* 問題 28. K を標数 $p \neq 0$ の代数体 K 上の法数 q なる 1 次元代数体とする。 K の nonsingular な G の Jacobi 多様体 J, A, B を K の Hasse-Witt 行列とする。また $A, A^2, \dots, A^{p-1}$ の中から A を取る。このとき J の付随積分が q であることが証明される。

註. K が有理体の場合 K の代数体 K 上の法数 q なる 1 次元代数体とする。 (cf. Hasse-Witt)

谷山が提出した問題

フェルマーの最終定理

n は5以上の素数

方程式
$$X^n + y^n = Z^n$$

整数解
$$(X, y, Z) = (a, b, c)$$

a, b, c のうち 1つは 0

フェルマーの最終定理

方程式 $x^n + y^n = z^n$

整数解 $(x, y, z) = (a, b, c)$

a, b, c のどれも 0 でないもの



(自明でない解)

矛盾

証明のあらすじ

① 自明でない **解** (a, b, c)

② **楕円曲線** $E: y^2 = x(x-a^n)(x-c^n)$

③ 対応する **保型形式**

矛盾

フェルマーの最終定理の解決まで

- ~1640 フェルマー 余白に書き込み
.....
- 1960~ 谷山・志村 楕円曲線と保型形式②
- 1986 フライ 最終定理と楕円曲線①
- 1987 メイザー・リベット 保型形式の性質③
- 1994 ワイルズ・テイラー 証明 ②

谷山志村予想

②

あるいは

楕円曲線の保型性予想

- 有理数係数の方程式

$$y^2 = x \text{ の 3 次式}$$

で定義された **楕円曲線** は、

すべて **保型形式** と **結び** ついている

1986～1987

- ①, ③ により,

フェルマーの最終定理が、
谷山・志村予想の帰結である
ことがわかった。

(フライ、セール、メイザー、リベット)

≠



http://www.math.uoc.gr/~antoniad/frey_crete_2003/



http://en.wikipedia.org/wiki/File:Jean-Pierre_Serre.jpg

フライ(1944-) と セール(1926.9.15-)



(c)1992 George M. Bergman

http://en.wikipedia.org/wiki/File:Barry_Mazur_1992.jpg



<http://en.wikipedia.org/wiki/File:Ribet.JPG>

メイザー(1937.12.19-)とリベット(1948.6.28-)

フェルマーの最終定理before 1986

- 超有名で、
- 歴史的に重要

代数的整数論の確立(クンマー)

フェルマーの最終定理before 1986

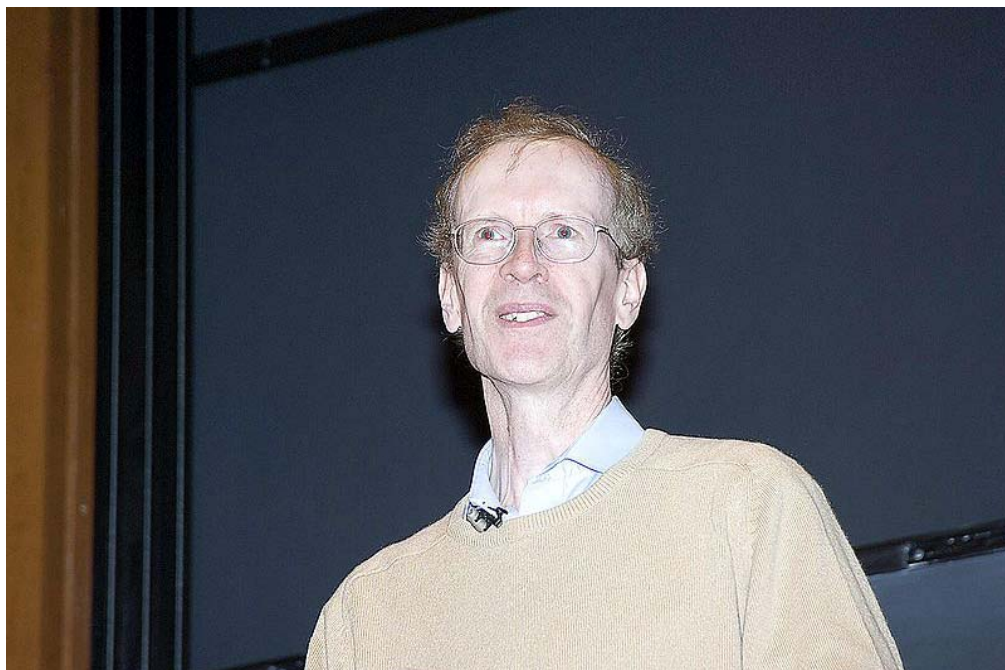
- 超有名で、
- 歴史的に重要
代数的整数論の確立（クンマー）
なのは間違いないが、
- 正しいかどうかは、よくわからない

フェルマーの最終定理 after 1987

- 数論の**中心的未解決問題**と
結びついた
- 正しいことは**間違いない**
- 証明できるのは、まだ**だいぶん先**？

フェルマーの最終定理 after 1987

- 数論の**中心的未解決問題**と
結びついた
- 正しいことは**間違いない**
- 証明できるのは、まだ**だいぶん先**？
- そう思わない人が**一人**いた



著作権処理の都合で

この場所に挿入されていた

Modular elliptic curves and
Fermat's Last Theorem

を省略させていただきます。

Andrew Wiles(1953.4.11-)

証明 1994

フェルマーの最終定理の解決まで

- ~1640 フェルマー 余白に書き込み
.....
- 1832 ガロワ ガロワ理論
- 1920 高木貞治 類体論
- 1960~ 谷山・志村 楕円曲線と保型形式
- 1986 フライ 最終定理と楕円曲線
- 1987 メイザー・リベット 保型形式の性質
- 1994 ワイルズ・テイラー 証明

類体論 (1920～)

- 「4 でわると 1 あまる素数は
2つの2乗数の和」(フェルマー)
を拡張する大理論
- 高木貞治
日本人最初の世界的数学者

井



<http://kyokan.ms.u-tokyo.ac.jp/~gakubu/takagi.html>

高木貞治 (1875.4.21-1960.2.28)

類体論 (1920～)

- 類体論

有理数体の絶対ガロワ群

(有理数係数の方程式の解を
統制する群)の

1次元表現の理論



<http://en.wikipedia.org/wiki/File:Galois.jpg>

ガロワ (1811.10.25-1832.5.31)

類体論と谷山・志村予想

- 類体論

有理数体の絶対ガロワ群 の

1次元表現の理論

- 谷山・志村予想

有理数体の絶対ガロワ群 の

2次元表現の理論の帰結

理想的な解かれ方？

- フェルマーの最終定理は、
ただ解かれたのではなく、
- 数論の中心的な問題に
突破口が開かれた。
- そして今、有理数体の絶対ガロワ群
の2次元表現の理論が、
完成に近づきつつある

楕円曲線と保型形式の 結びつき

- $y^2 = (x^3 - x)$ が
素数 p でわりきれるような
 $(x, y) = (a, b)$,
 $a, b = 0, 1, 2, \dots, p-1$
の個数 $n(p)$

楕円曲線と保型形式の 結びつき

p	2	3	5	7	11	13	17
$n(p)$	2	3	7	7	11	7	15
$p - n(p)$	0	0	-2	0	0	6	2

楕円曲線と保型形式の 結びつき

$$\begin{aligned} & \bullet q \times \{(1 - q^4)(1 - q^8)\}^2 \\ & \quad \times \{(1 - q^8)(1 - q^{16})\}^2 \\ & \quad \times \{(1 - q^{12})(1 - q^{24})\}^2 \times \dots \\ & = q - 2 q^5 - 3 q^9 + 6 q^{13} + 2 q^{17} \\ & \quad - q^{25} - 10 q^{29} - 2 q^{37} + \dots \end{aligned}$$

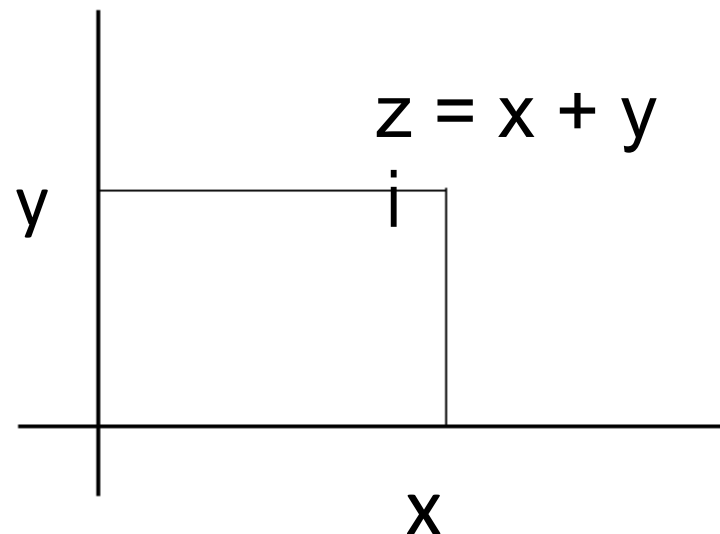
楕円曲線と保型形式の 結びつき

p	2	3	5	7	11	13	17
$p - n(p)$	0	0	-2	0	0	6	2

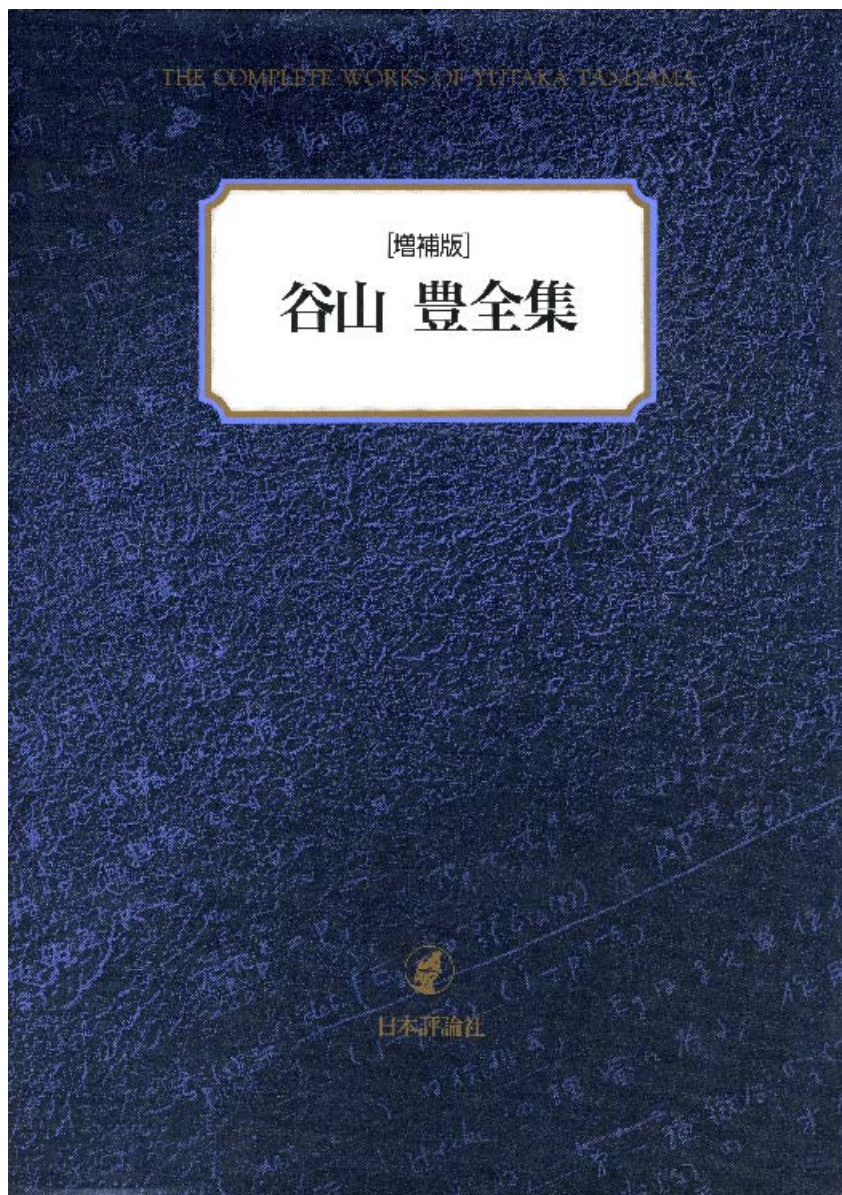
$$\begin{aligned}
 q &- 2 q^5 - 3 q^9 + 6 q^{13} + 2 q^{17} \\
 &- q^{25} - 10 q^{29} - 2 q^{37} + \cdots
 \end{aligned}$$

保型形式とは？

- $q = e^{2\pi i z} \quad (z = x + y i, y > 0)$
 $= e^{-2\pi y} (\cos 2\pi x + i \sin 2\pi x)$

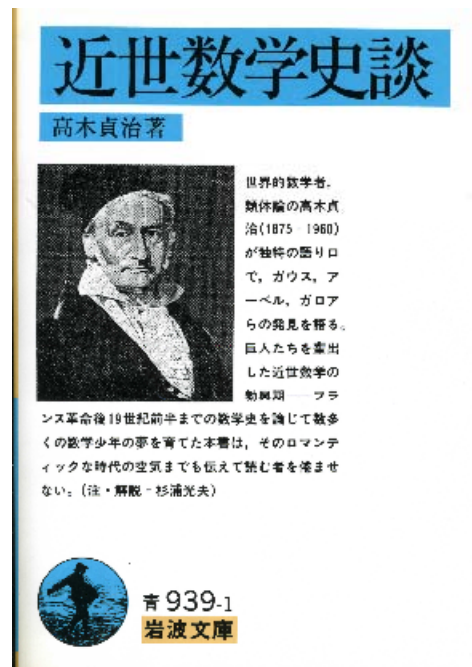


✚



杉浦 光夫(編集代表)
『谷山豊全集 増補版』
日本評論社(1994/10)

✚



高木 貞治(著)
『近世数学史談』
岩波書店(1995/08)