Global Focus on Knowledge -Creating Mathematics-

Lecture two

Mathematics “On Campus”

Creating words, Originating worlds

2009.10.15

‡

This is the textbook of English class for freshmen in the university of Tokyo.

Mathematics

On Campus

4. MATHEMATICS

Introduction

Takeshi Saito

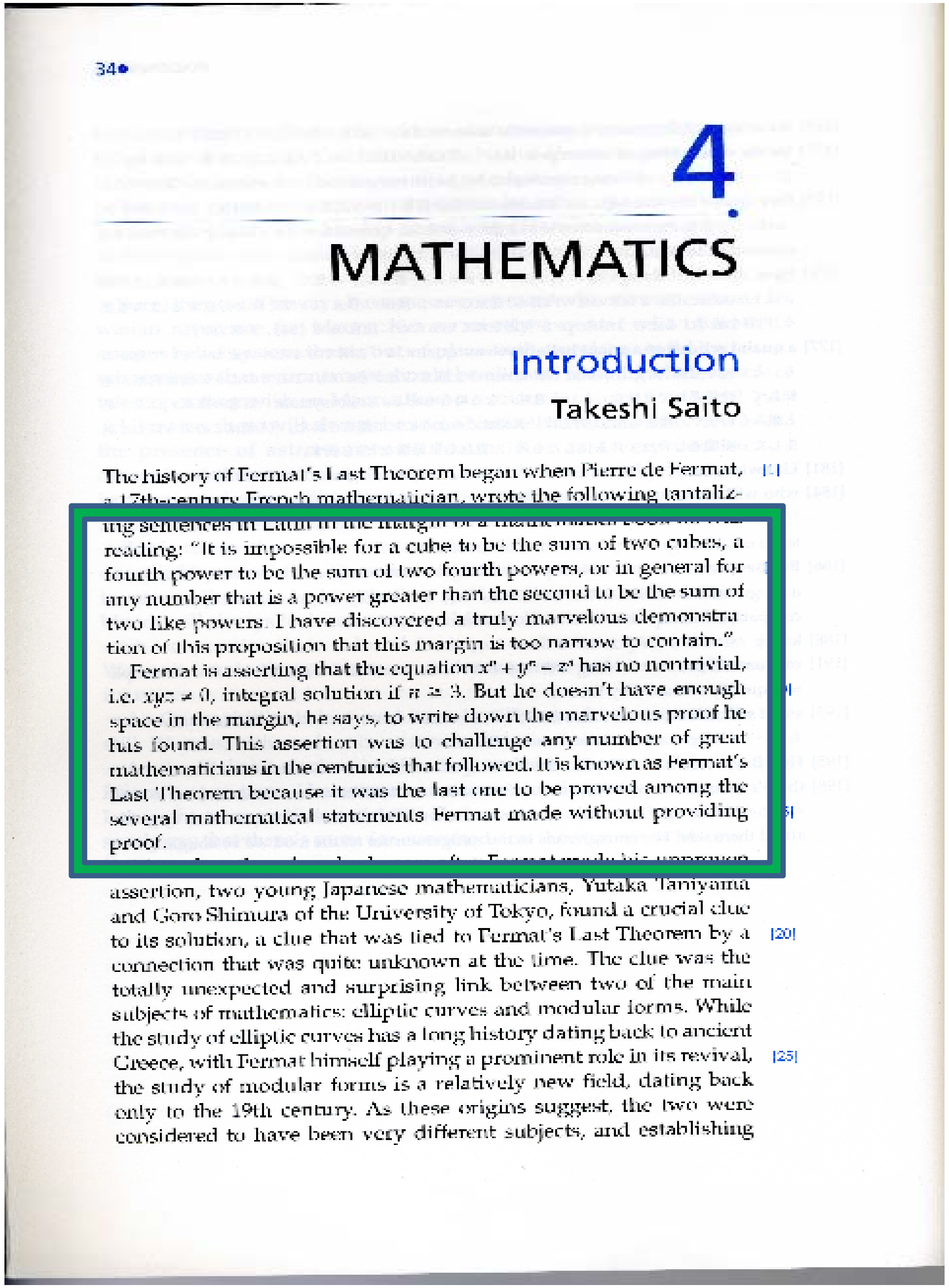
The history of Fermat's Last Theorem began when Pierre de Fermat, a 17th-century French mathematician, wrote the following tantalizing sentences in Latin in the margin of a mathematics book he was reading: "It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth 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.

More than three hundred years after Fermat made his unproven 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's Last Theorem



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 mathematics book he was 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." [1]

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.

Some three hundred years after Fermat made his unproven 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 [20] 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, [25] 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’s note (around 1640?)

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's note (original version)

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 was 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 didn't have enough space in the margin, he said, to write down the truly marvelous proof he had found.

Pierre de Fermat

(1601.8.20-1665.1.12)

a man of Toulouse, France

"Father of number theory"

Reprinted from
http://en.wikipedia.org/wiki/File:Pierre_de_Fermat.png(2010/09/03)

Pierre
de Fermat

(1601.8.20-
1665.1.12)

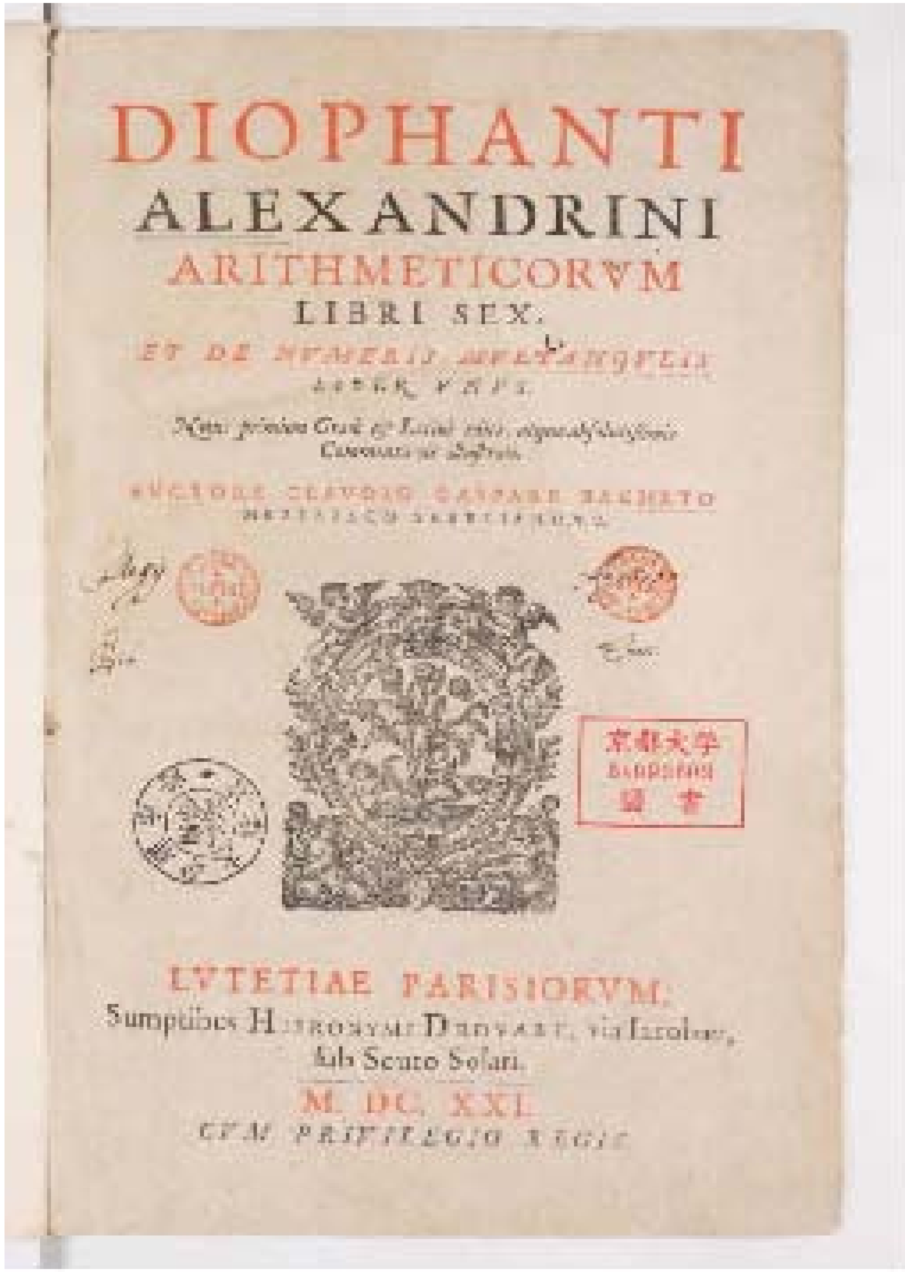
a man of Toulouse,
France

“Father of number
theory”

Reprinted from
http://en.wikipedia.org/wiki/File:Pierre_de_Fermat.jpg(2010/09/03)

A copy of the book Fermat left a note on

A book on number theory written by Diophantus of Alexandria in 3rd century, and revived by Bachet on 1621



Reprinted from
http://en.wikipedia.org/wiki/File:Diophantus-cover.jpg(2010/09/03)

Diophantus of Alexandria (-300)

Fermat’s annotation was written on a copy of this page


Arithmeticorum Lib. II. 85

QVAESTIO VIII.

QVAESTIO IX.

Reprinted from
http://en.wikipedia.org/wiki/File:Diophantus-II-8-Fermat.jpg(2010/09/03)

Fermat's last theorem

$n \geqq 3$.

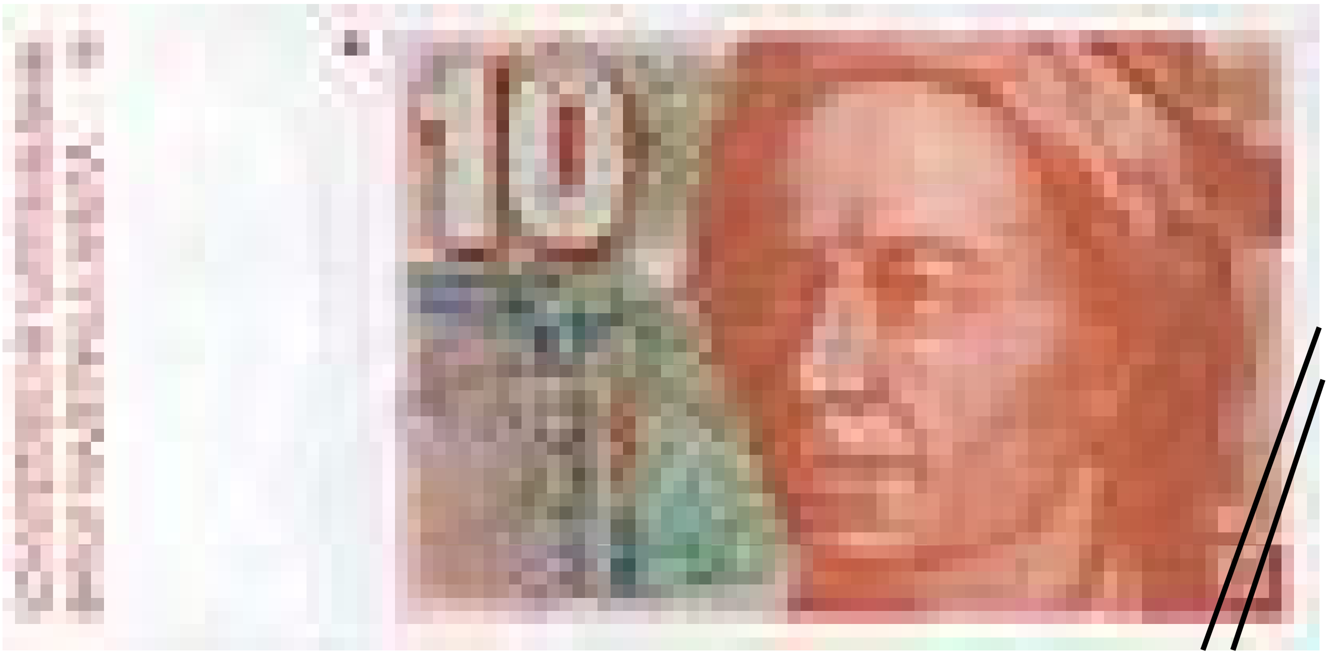
Equation $$x^n + y^n = z^n$$

Integer solution $(x,\ y,\ z) = (a,\ b,\ c)$

at least one of $a,\ b,\ c$ should be zero

Towards the resolution of Fermat's last theorem

- -1640 Fermat's note
- -1659 Fermat in case of n=4
- 1753 Euler in case of n=3



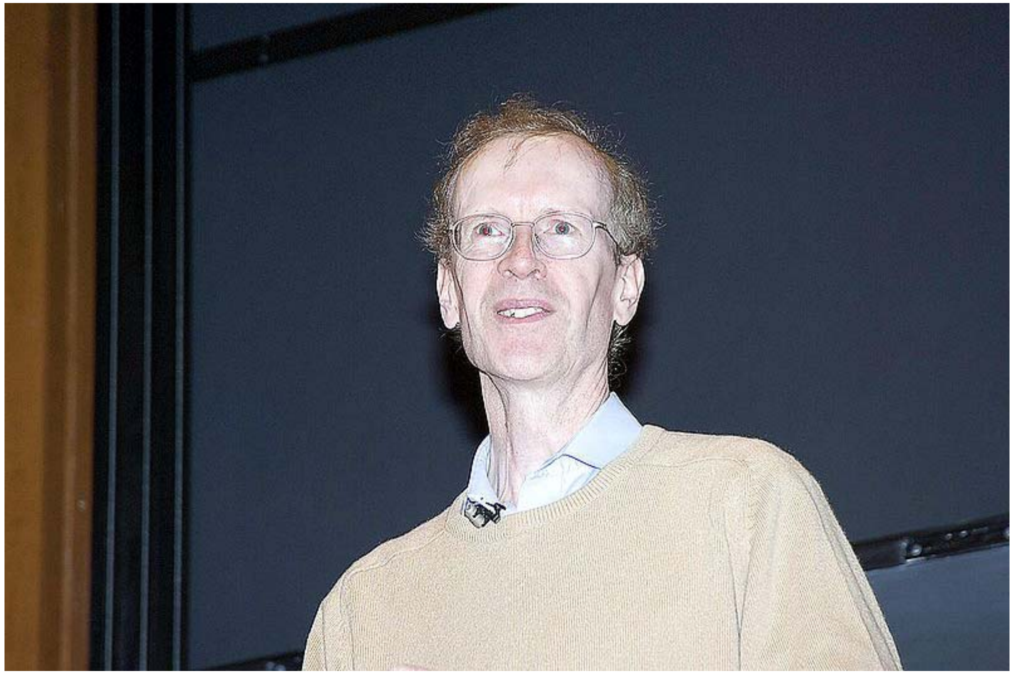
Euler(1707.4.15 - 1783.9.18)

Towards the resolution of Fermat’s last theorem

- -1640 Fermat’s note
- -1659 Fermat in case of n=4
- 1753 Euler in case of n=3

. . . .

- 1994 Wiles, Taylor a complete proof



"copyright C. J. Mozzochi, Princeton N.J"
http://www.mozzochi.org/deligne60/Deligne1/_DSC0024.jpg

Figure removed due to copyright restrictions

Wiles (1953.4.11-) and his article on the proof of Fermat's last theorem

the Difficulty in proving Fermat's last theorem

- the statement is easy to understand.

superficially even for a junior high school student

- But the solution is elusive

the Difficulty in proving Fermat's last theorem

Why did it took as long as 360 years?

Because it was necessary to create a mathematical world before getting to the heart of Fermat's last theorem.

Before the general proof of Fermat's last theorem

- -1640 Fermat's note
- -1659 Fermat in case of n=4
- 1753 Euler in case of n=3
- 1800- Gauss et al. elliptic curves
- 1850- Eisenstein et al. automorphic forms
- 1960- Taniyama and Shimura

  elliptic curves and automorphic forms
- 1986 Frey

  Fermat's Last theorem and elliptic curves
- 1994 Wiles and Taylor complete proof

$n=lm$

if a, b, c are the solution of

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

a^m, b^m, c^m are the solution of

$x^l + y^l = z^l$

$$\Downarrow$$

the problem reduces to

either $n = l$ is a prime number larger than 3

or $n = l$ equals to 4

A Prime number

- a natural number p with $p \geq 2$

and cannot be divided by any natural numbers other than 1 and p itself.

- 1 is not a prime number.

(uniqueness of prime factor decomposition)

A prime number

- There are infinite number of prime numbers.

  (demonstrated by ancient Greeks)

- 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,……
- A lot of unresolved problems

Infinite number of Prime numbers

$2, 2 + 1 = 3,$

$2 \cdot 3 + 1 = 7,$

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

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

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

…………………

Fermat prime number

$2^n + 1$ is a prime $\Longrightarrow$ $n=2^m$

$2^3 + 1 = 3^2$, $2^5 + 1 = 33 \cdot 11$,

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

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

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

Fermat prime number

inverse

$2^n + 1$ is a prime $\Leftarrow$ $n=2^m$

true or not true?(Fermat)

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

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

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

……………

Fermat prime number

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

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

(Euler)

…………………

Fermat prime number

$p=2^{2^n}+1$ is a prime

$$\Downarrow$$

regular p-gon can be

It is possible to construct regular using compass and ruler only

(Gauss 1796.3.30)

Reprinted from
http://en.wikipedia.org/wiki/File:Carl_Friedrich_Gauss.jpg(2010/09/03)

Gauss (1777.4.30 - 1855.2.23)

Fermat prime number

Serre's conjecture was settled

(Khare 2005)

- inductive reasoning concerned with prime number
- there are infinite number of prime numbers that are not Fermat prime number

‡

Reprinted from
http://www.math.ucla.edu/~shekhar/(2010/09/03)

Khare (1967 -)

Fermat’s contribution

- Tangent lines, maximum/minimum

(pioneer work in differentiation and integration)

- The concept of coordinates

(contemporary with Decartes)

Fermat’s contribution
“Father of number theory”

- Fermat’s little theorem
- On the condition for a prime p to be written as the sum of two square numbers
- Rational point on elliptic curves

……………

Fermat's little theorem

let p be a prime then $a^p - a$ can be divided by p.

(fundamentals for RSA cryptography)

2^7-2 = 12-2 = 126 = 7 × 18,

2^{11}-2 = 2048-2 = 2046 = 11 × 186,

3^5-3 = 243-3 = 240 = 5 × 48,

....

The condition for a prime $p \neq 2$ to be the sum of two square numbers:

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

p leaves a remainder of 1 when divided by 4.

Prime numbers that leave a remainder of 1 when divided by 4

2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41,

43, 47, 53, 59, 61, 67, 71, 73, 79, 83, …

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 , ……..

Rational solution of
Eq. $y^2 = x^3 - x$
(elliptic curves)

There are only three solutions

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

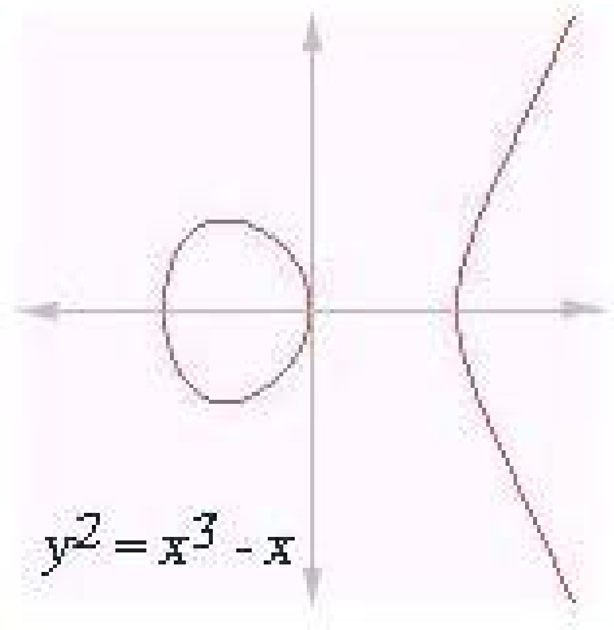
(infinite descent)

- n = 4 version of Fermat's last theorem
- There exist no right triangles of unit area with three sides whose lengths are all rational number

Elliptic curves

- example: $y^2 = x^3 - x$

Curves that are defined by y^2 =(cubic function of x)



http://upload.wikimedia.org/wikipedia/commons/5/5b/ECexamples01.png

Elliptic curves

- are different from ellipses $ax^2 + by^2 = 1$

  (concerned with integrals used to calculate the length of ellipses)

- "There are unlimited things to write about elliptic curves. I am not exaggerating"(S. Lang)

Elliptic curves and Fermat's last theorem

- In case of $n = 3, 4$

equations that define certain elliptic curves

$y^2 = x^3 - x$ (Fermat)

$y^3 = x^3 - 1$ (Euler)

Demonstrated by studying the properties of their rational number solution

- In case a prime number n is larger than 5

Demonstrated by showing that the equation that defines an elliptic curve $y^2 = x (x-a^n) (x-c^n)$ does not exist

りで
おせ
符に
数学
・説
さい
ト：
ご
イナ
いた
ムげ

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す。本を読んでいると、しあわせです。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
1
●中
1 物理
方程
トル
2

Fermat's last theorem

n is a prime number larger than 5

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

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

at least one of a, b, c should be zero

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 particulary 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.

Cited from "On Campus" p36

Yutaka Taniyama

(1927.11.12-1958.11.17)

and

Goro Shimura

(1930-   )

Figure removed due to copyright restrictions

‡

Reprinted from
http://www.s.u-tokyo.ac.jp/imagebank/?mode=show&id=sc0028(2010/09/03)

ex. Faculty of Science Bldg.1

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.

Cited from "On Campus" p42

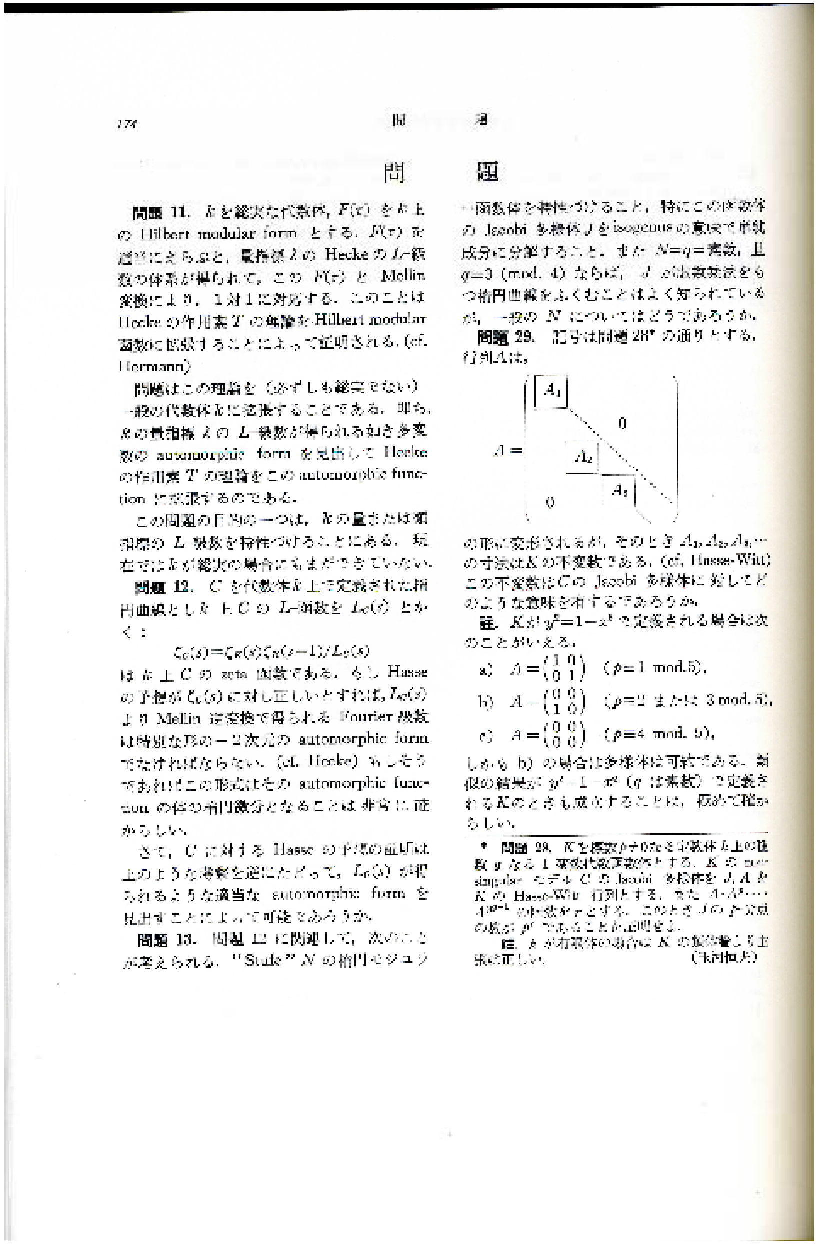
International conference on number theory held in Nikko

(1955)

‡

By courtesy of Nikkokanaya hotel

‡



問 題

問題 11. k を総実な代数体, $F(\tau)$ を k 上の Hilbert modular form とする. $F(\tau)$ を適当にえらぶと, 量指標 λ の Hecke の L-級数の体系が得られて, この $F(\tau)$ 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 函数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 (必ずしも総実でない) 一般の代数体 k に拡張することである. 即ち, k の量指標 λ の L-級数が得られる如き多変数の 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 の量または類指標の L-級数を特性づけることにある. 現在では k が総実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 C の L-函数を $L_C(s)$ とかく:

$$\zeta_C(s)=\zeta_k(s)\zeta_k(s-1)/L_C(s)$$

は k 上 C の zeta 函数である. もし Hasse の予想が $\zeta_C(s)$ に対し正しいとすれば, $L_C(s)$ より Mellin 逆変換で得られる 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 の体の楕円微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逆にたどって, $L_C(s)$ 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. "Stufe" N の楕円モジュラー函数体を特性づけること, 特にこの函数体の Jacobi 多様体 J を isogenous の意味で単純成分に分解すること. また $N=q=$素数, 且 $q\equiv3$ (mod. 4) ならば, J が虚数乗法をもつ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,

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

の形に変形されるが, そのとき $A_1, A_2, A_3, \cdots$ の寸法は K の不変数である. (cf. Hasse-Witt) この不変数は C 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 $y^2=1-x^5$ で定義される場合には次のことがいえる.

a) $A=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ ($p\equiv1$ mod. 5),

b) $A=\begin{pmatrix}0&0\\1&0\end{pmatrix}$ ($p\equiv2$ または 3 mod. 5),

c) $A=\begin{pmatrix}0&0\\0&0\end{pmatrix}$ ($p\equiv4$ mod. 5).

しかも b) の場合は多様体は可約である. 類似の結果が $y^2=1-x^q$ (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 $p\neq0$ なる定数体 k 上の種数 g なる 1 変数代数函数体とする. K の non-singular モデル C の Jacobi 多様体を J, A を K の Hasse-Witt 行列とする. また $A\cdot A^p\cdots A^{p^{g-1}}$ の階数を r とする. このとき J の p 位点の数が p^r であることを証明せよ.

註. k が有限体の場合は K の類数論より主張は正しい. ([illegible])

Taniyama proposed some problems

Fermat's last theorem

n is a prime number larger than 5

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

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

at least one of a, b, c should be zero

Fermat's last theorem

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

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

All of a, b, c are not zero

(nontrivial solution)

Contradiction

Sketch of proof

Nontrivial solution (a,b,c)

$\Big\downarrow$ 1

Elliptic curve $y^2 = x\,(x-a^n)\,(x-c^n)$

$\Big\downarrow$ 2

Corresponding automorphic forms

$\Big\downarrow$ 3

Contradiction

Before the general proof of Fermat's last theorem

- -1640 Fermat's notes

  ....

- 1960- Taniyama and Shimura

  elliptic curves and automorphic forms 2

- 1986 Frey

  Fermat's Last theorem and elliptic curves 1

- 1987 Mazur and Ribet

  Characteristics of automorphic forms 3

- 1994 Wiles and Taylor complete proof 2

Taniyama-Shimura conjecture 2

or

conjecture about the automorphicity of elliptic curves

- All elliptic curves defined by an equation with rational number coefficient

$$y^2 = 3^{rd} \text{ order } x$$

are related to automorphic forms

1986-1987

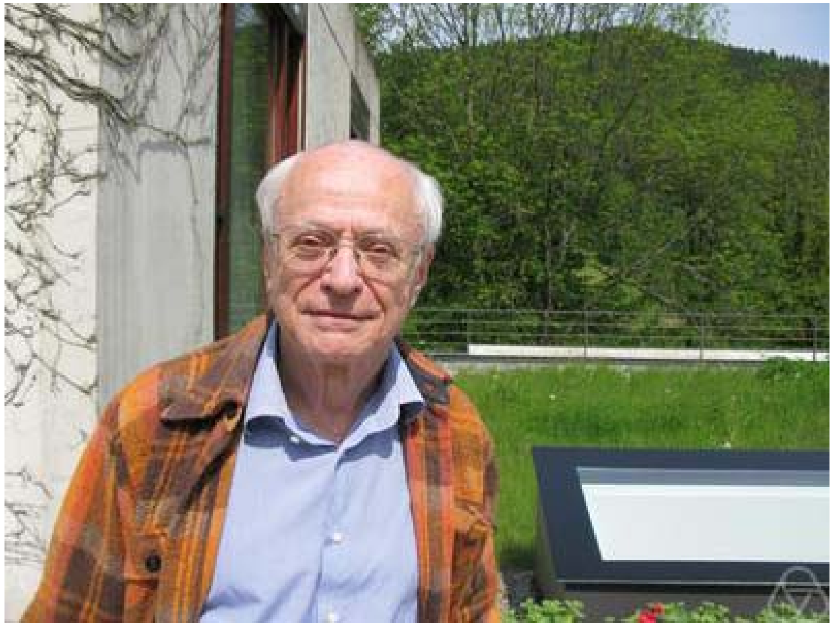
- With 1 and 3,

Fermat’s last theorem was found to be a consequence of Taniyama and Shimura Conjecture.

(Frey, Serre, Mazur, Ribet)

‡ 

Reprinted from
http://www.math.uoc.gr/~antoniad/frey_crete_2003/(2010/09/03)



Reprinted from
http://en.wikipedia.org/wiki/File:Jean-Pierre_Serre.jpg(2010/09/03)

Frey(1944-) and Serre(1926.9.15-)

(c)1992 George M. Bergman

Reprinted from
http://en.wikipedia.org/wiki/File:Barry_Mazur_1992.jpg(2010/09/03)

Reprinted from
http://en.wikipedia.org/wiki/File:Ribet.JPG(2010/09/03)

Mazur(1937.12.19-) and Ribet(1948.6.28-)

Fermat’s last theorem before 1986

- Very popular
- Of historical importance

Algebraic number theory (Kummer)

Fermat's last theorem before 1986

- Very popular
- Of historical importance

    Algebraic number theory (Kummer)

  but

- it is doubtful whether it is true

Fermat's last theorem after 1987

- Linked to the central unresolved problem of number theory
- Fairly certain to be true
- For a proof, it would take fairly long time ?

Fermat's last theorem after 1987

- Linked to the central unresolved problem of number theory
- Fairly certain to be true
- For a proof, it would take fairly long time ?

- A man did not think so.

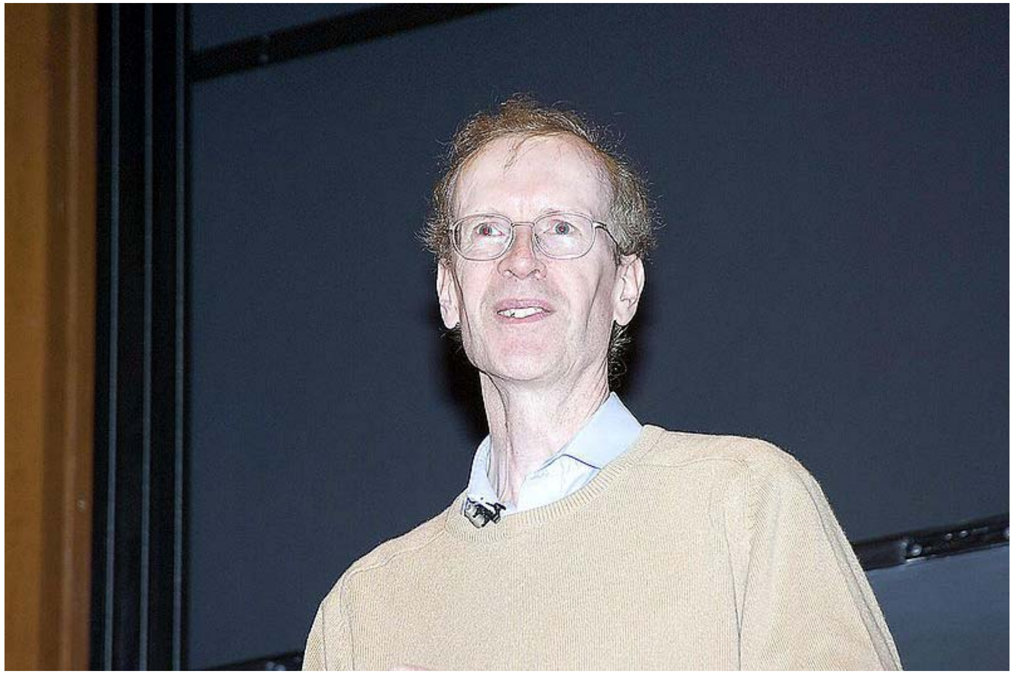


Figure removed due to copyright restrictions

Andrew Wiles(1953.4.11-)

proved in 1994

Before the general proof of Fermat's last theorem

- -1640 Fermat's note

  ....

- 1832 Galois Galois theory
- 1920 Teiji Takagi Class field theory

  ....

- 1960- Taniyama and Shimura

  elliptic curves and automorphic forms

- 1986 Frey

  Fermat's Last theorem and elliptic curves

- 1987 Mazur and Ribet

  Characteristics of automorphic forms

- 1994 Wiles and Taylor complete proof

Class field theory (1920-)

- A great theory that extends the fact “a prime number that leaves a remainder of 1 when divided by 4 is expressed by the sum of two square numbers” (Fermat)
- Teiji Takagi

  the first world-famous mathematician in Japan

‡

Reprinted from
http://kyokan.ms.u-tokyo.ac.jp/~gakubu/takagi.html(2010/09/03)

Teiji Takagi (1875.4.21-1960.2.28)

Class field theory (1920-)

- Class field theory

one dimensional representation theory of

absolute Galois group of the rational number field

(a group that controls the solution of an equation with rational number coefficient)

Reprinted from
http://en.wikipedia.org/wiki/File:Galois.jpg(2010/09/03)

Galois (1811.10.25-1832.5.31)

Class field theory and Taniyama-Shimura Conjecture

- Class field theory

  one dimensional representation theory of the absolute Galois group of the rational number field

- Taniyama-Shimura Conjecture

  Consequences of two dimensional representation theory of the absolute Galois group of the rational number field

an ideal solution?

- Fermat's last theorem was

  not simply solved,

- But solved along with a clue to

  a central problem in number theory.

- And now, the two dimensional representation theory of the absolute Galois group of rational number field is near completion.

The connection of Elliptic curves with automorphic forms

The number of combination$(x, y) = (a, b)$,

$a, b = 0, 1, 2, \ldots, p - 1$ (p is a prime number)

Such that

$y^2-(x^3 - x)$ is divisible by p

Is denoted by $n(p)$

The connection of Elliptic curves with automorphic forms

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

The connection of Elliptic curves with automorphic forms

- $q \times \{(1-q^4)(1-q^8)\}^2$
  $\times \{(1-q^8)(1-q^{16})\}^2$
  $\times \{(1-q^{12})(1-q^{24})\}^2 \times \cdots$

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

The connection of Elliptic curves with automorphic forms

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

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

what is Automorphic forms ?

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

$$= e^{-2\pi y} (\cos 2\pi x + i \ \sin 2\pi x)$$