# "Wiles' proof of Fermat's Last Theorem for beginners"

15 / Feb / 2012

at 7th Kagoshima AAG Seminar,

Go Yamashita,

Toyota CRDL, Inc.

## §1. Statement

Th (Fermat-Wiles, 1995)

For $n \in \mathbb{Z}$, $n \geqq 3$,

there is no $x, y, z \in \mathbb{Z}$ satisfying

$$x^n + y^n = z^n, \quad xyz \neq 0.$$

## Plan

§1. Statement,

§2. Reduce to Shimura - Taniyama Conjecture
for semistable elliptic curves,
— Ribet

§3. Galois representations,
— Eichler - Shimura

§4. Reduce to the modularity lifting,
— Langlands - Tunnell

§5. Small digress — Wiles' (3, 5) - trick,
— Wiles

§6. Formalism of $R = \mathbb{T}$,
— Mazur, Wiles

§7. Reduce to the minimal case
— Wiles

§8. The minimal case — Taylor - Wiles system
— Taylor - Wiles

deep

(We will explain simplifications of
Wiles' original proof as well.
However, the fundamental ideas of the proof
are same.)

Roughly

FLT §1

$\Uparrow$ Ribet

Shimura-Taniyama Conjecture §2

(for semistable elliptic curves)

$\Uparrow$ Langlands-Tunnell §3, §4
& Wiles' (3,5)-trick §5

Modularity Lifting §6

- Non-Minimal case §7

- Minimal case §8
(= first step of the induction)

# Picture

$$
\begin{tikzcd}
\left(\text{elliptic curves}/\mathbb{Q}\right) \arrow[r, squiggly, shift right, "\text{Wiles et al.}"'] & \left(\begin{array}{c}\text{modular forms}\\ \text{of weight 2}\\ (\text{Hecke eigen, cusp})\end{array}\right) \arrow[l, shift right, "\text{Eichler-Shimura}"']
\end{tikzcd}
$$

$$
\begin{tikzcd}
E \arrow[d, mapsto] & & f \arrow[d, mapsto] \\
\rho_E \arrow[d, squiggly, "\text{``incarnation''}"'] & (\text{Galois representations}) & \rho_f \arrow[d, squiggly, "\text{``incarnation''}"] \\
\color{red}{R} \arrow[rr, "\sim"] & & \color{red}{\mathbb{T}}
\end{tikzcd}
$$

universal deformation rings

Hecke algebras

this isomorphism is the most crucial point of the proof.

# Generalizations of Taylor-Wiles technique

(Clozel-Harris-Taylor et al.)
GL(n)

→ Sato-Tate Conjecture
BLGHT (2011)

↑ generalization

(Taylor-Wiles et al.) $\xrightarrow{\text{generalization}}$ (Kisin)

GL(2)

→ Fermat's Last Theorem
(1995)

→ Shimura-Taniyama Conjecture
BCDT (2001)

GL(2) with integral p-adic Hodge theory

→ Serre's Conjecture
KW (2009)

(All years in this notes are the <u>publication years</u>, not the years of preprints.)

## §2. Reduce to Shimura-Taniyama Conjecture for semistable elliptic curves

The case $n=4 \Rightarrow$ proved by Fermat (1640)

So, may assume $n$ is a prime number $p>2$.

Assume $\exists\, a^p + b^p = c^p$, $abc \neq 0$

$a, b, c \in \mathbb{Z}$

may assume $a, b, c$ have no common divisors.

Then we have

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

(called Frey curve)

- $abc \neq 0 \Rightarrow E$ is nonsingular

  $\Rightarrow E$ is an elliptic curve $/\mathbb{Q}$

- $a, b, c$ have no common divisors

  $\Rightarrow E$ is semistable

# Shimura-Taniyama Conjecture

(proved by Wiles, Taylor, ⋯,
Breuil-Conrad-Diamond-Taylor 2001)

For all elliptic curve $E$ over $\mathbb{Q}$,

there exists a (unique)

Hecke eigen cusp form $f$

such that

$$L(E,s) = L(f,s).$$

L-function of $E$ L-function of $f$

(We say that
"$E$ comes from $f$".)

- $L(f,s) := \sum_{n \geq 1} \frac{a_n}{n^s}$ for $f = \sum_{n \geq 1} a_n q^n$

$$= \prod_{\substack{\text{good } p \\ \text{for } f}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \times \prod_{\substack{\text{bad } p \\ \text{for } f}} (\text{omit the details})$$

$\left( q = e^{2\pi i z},\ z \in \mathfrak{h} := \{ z \in \mathbb{C} \mid \mathrm{Im}\, z > 0 \} \right.$ upper half plane

- $$L(E,s) := \prod_{\substack{\text{good } p \\ \text{for } E}} \frac{1}{1 - (1 + p - \# \tilde{E}(\mathbb{F}_p)) p^{-s} + p^{1-2s}}$$

$$\times \prod_{\substack{\text{bad } p \\ \text{for } E}} (\text{omit the details})$$

$\tilde{E}$ : the reduction of $E$ modulo $p$ at a good prime $p$ for $E$.

i.e.

$\forall E$, $\exists f = \sum a_n q^n$ Hecke eigen cusp form such that

$a_p = 1 + p - \# \tilde{E}(\mathbb{F}_p)$ for good $p$

Remark D

BCDT's proof of the remaining cases of
the Shimura-Taniyama Conjecture was
a kind of "case-by-case calculations"
of the deformation rings
of the conductors $= 27, 81, 243$

Kisin gave a conceptual proof of it
by the modified Taylor-Wiles system
by using the integral $p$-adic Hodge theory
(2009)

## Remark 2

Shimura-Taniyama Conjecture is a part of

Langlands correspondence.

$$\left\{\begin{array}{l}\text{n-dimensional} \\ \text{Galois representations} \\ \text{with some conditions} \cdots\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{automorphic} \\ \text{representations} \\ \text{of } GL(n) \\ \text{with some conditions}\end{array}\right\}$$

merit

- weight yoga by Weil conjecture (if it comes from a motive)

merit

- good analytic property
- easy to calculate

examples of the strength of the correspondence

(Galois side) $\longleftrightarrow$ (automorphic side)

① Ramanujan-Petersson Conjecture (Deligne, 1974)

• weight yoga $\xleftarrow{\text{proved by}}$

② Fermat's Last Theorem (Wiles, Taylor-Wiles 1995)

$\xmapsto{\text{proved by}}$ • easy to calculate $S_2(\Gamma_0(2)) = 0$

③ Sato-Tate Conjecture (Taylor et al, 2011)

$\xmapsto{\text{proved by}}$ • good analytic property

## Ribet (level lowering)

Given $E$ : elliptic curve $/\mathbb{Q}$

If $E$ comes from a modular form (necessarily of weight 2) of some level

$\Longrightarrow$ $E[p]$ comes from a modular form

($p$-torsion points)

of weight 2,

and of level = the conductor of $E[p]$

(

" $E[p]$ comes from $f$ " :

$$1 + \ell - \#\tilde{E}(\mathbb{F}_\ell) \equiv a_\ell \mod p$$

for almost all prime $\ell$,

$$f = \sum_{n \geq 1} a_n q^n$$

)

Frey curve

$$E: \quad y^2 = x(x-a^p)(x+b^p)$$

has the discriminant

the differences of the roots

$$\Delta := 16\left((a^p-0)(b^p-0)(a^p-(-b^p))\right)^2$$
$$= 16\,(abc)^{2p}$$

$\rightsquigarrow$ the conductor of $E[p]$

$$= 2 \prod_{\substack{l \mid \Delta \\ l \neq 2}} l$$

the exponent of $l$ in $\Delta$ is not divisible by $p$

$$= 2$$

So, the corresponding modular form

is of weight $= 2$, level $= 2$

However,

$$\underset{\text{weight}=2}{S_2}(\Gamma_0\underset{\text{level}=2}{(2)}) = 0$$

contradiction!

In short,

need to show

- Shimura - Taniyama Conjecture
  for semistable elliptic curves

- Ribet's level lowering
  (already proved)

Fermat's
Last Theorem.

Remark ①

Ribet's level lowering uses
$p$-adic uniformizations of
Shimura curves
and a little bit difficult.

Remark ②

easier technique

Skinner-Wiles' base change arguments (2001)

$\Rightarrow$ can avoid Ribet's level lowering
(and hard algebraic geometry)

## §3. Galois representations



$p$ : prime

◦ elliptic curve $E$ over $\mathbb{Q}$

$p^n$-torsion points

$$\rightsquigarrow \quad T_p E := \varprojlim_n E[p^n](\overline{\mathbb{Q}})$$

$\circlearrowleft$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

free of rank $= 2$

Tate module of $E$

$$\rightsquigarrow \quad \rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}_p)$$

- $f$ : modular form

$$\xrightarrow{\text{(omit)}} \rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_p)$$

Galois representation associated to a modular form

Constructions

$$\begin{cases} \text{weight} = 2 & : \text{Eichler-Shimura} \\ \text{weight} > 2 & : \text{Deligne (1971)} \\ \text{weight} = 1 & : \text{Deligne-Serre (1974)} \end{cases}$$

( For simplicity, we used $GL_2(\mathbb{Z}_p)$ here.

In general, we need to use

the ring of integers of $\mathbb{Q}_p(a_n | n \geq 1)$

for $f = \sum a_n q^n$

instead of $\mathbb{Z}_p$. )

elliptic curves $E$ $\longleftrightarrow$ modular forms $f$

very far

$\rho_{E,p}$ $\qquad\qquad$ $\rho_{f,p}$

Galois representations

compare them by the Galois representations!

N.P. Given $E$,

<u>Find</u> $f$ such that

$$\rho_{E,p} \cong \rho_{f,p}$$

for some $p$!

( $\Longleftarrow$ [easy] $\rho_{E,p} \cong \rho_{f,p}$ for all $p$ )

## §4. Reduce to the modularity lifting

Given $E$, Want to find $f$

such that $\rho_{E,p} \cong \rho_{f,p}$

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "\rho_{E,p}"] \arrow[dr, "\overline{\rho}_{E,p}"'] & GL_2(\mathbb{Z}_p) \arrow[d, "\bmod p"] \\ & GL_2(\mathbb{F}_p) \end{tikzcd}$$

Strategy

① Show $\overline{\rho}_{E,p}$ is modular.

(i.e. comes from a modular form)

② Next, show $\rho_{E,p}$ is modular.

( For simplicity, we used $GL_2(\mathbb{Z}_p)$ from now on.

In general, we need to use

the ring of integers of

a finite extension of $\mathbb{Q}_p$

instead of $\mathbb{Z}_p$. )

As for ①,

for $p = 3$ $\quad GL_2(\mathbb{F}_3)$ is <u>solvable</u>

$\Longrightarrow$ <u>Langlands - Tunnell</u> (base change theorems)

$\bar{\rho}_{E,3}$ is modular

Step ① is OK !

Remark

Khare - Wintenberger's

strictly compatible system

$\Rightarrow$ can avoid Langlands - Tunnell (2005)

this is also based on Wiles'

$R = \mathbb{T}$ techniques.

# §5. Small digress – Wiles' (3,5)-trick

<u>Want</u> $\overline{\rho}_p$ : modular $\Longrightarrow$ $\rho_p$ : modular

called modularity lifting

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "\rho_p"] \arrow[dr, "\overline{\rho}_p"'] & GL_2(\mathbb{Z}_p) \arrow[d] \\ & GL_2(\mathbb{F}_p) \end{tikzcd}$$

Wiles' techniques work

only when $\overline{\rho}_p$ is <u>absolutely irreducible</u>

Unfortunately $\overline{\rho}_{E,3}$ may <u>not</u>

be absolutely irreducible.

By using <u>Mazur's theorem</u>

If $\overline{\rho}_{E,3}$ is not absolutely irreducible

$\Longrightarrow$ $\overline{\rho}_{E,5}$ <u>is</u> absolutely irreducible

But, we don't know

$\overline{\rho}_{E,5}$ is modular.

( $GL_2(\mathbb{F}_5)$ is <u>not</u> solvable. )

In short

$\bar{\rho}_{E,3}$

- modular
- may not be absolutely irreducible.

$\bar{\rho}_{E,5}$

- don't know to be modular
- absolutely irreducible if $\bar{\rho}_{E,3}$ is not.

## Wiles' (3, 5)-trick

$\exists E'/\mathbb{Q}$ such that

① $E'$: semistable

② $E'[5] \cong E[5]$

as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representations

③ $E'[3]$ is absolutely irreducible.

modular curves

( We use (the genus of $X(5) = 0$ and)

the genus of $X(\Gamma(5) \cap \Gamma_0(3)) = 9 > 1$

& a theorem of Faltings (Mordell Conjecture)

( In the original paper,

Wiles' used Hilbert irreducibility theorem ) )

Then

$T_3E'$ (…) $T_5E'$ $T_5E$

absolutely irreducible

$E'[3]$

modularity lifting for $p=3$

$E'[5] \cong E[5]$

absolutely irreducible if $E[3]$ is not

modularity lifting for $p=5$

modular by Langlands-Tunnell

So we reduced Fermat's Last Theorem to the modularity lifting (for $p=3,5$)

Remark ① We used for $p=3$, $q=5$

① $\bar{\rho}_{E,3}$ is not absolutely irreducible
$\Rightarrow$ $\bar{\rho}_{E,q}$ is absolutely irreducible
(by Mazur's theorem)

② $g(X(\Gamma(q)\cap\Gamma_0(p)))>1$

③ $GL_2(\mathbb{F}_p)$ is solvable

④ $g(X(q))=0$

① holds for $\forall q>3$

② holds for $(p,q)\neq(3,2),(5,2),(2,3)$

③ holds only for $p=2,3$

④ holds only for $q=2,3,5$

$\Rightarrow$ For odd primes $p\neq q$,
only $(3,5)$ can be available!

(we want to avoid $p=2$
since the case $p=2$ has some exceptional matters
(related with $\#\mathrm{Gal}(\mathbb{C}/\mathbb{R})=2$))

Remark 2

This (3,5)-trick is a prototype of the following techniques

1. Taylor's variant by Hilbert-Blumenthal varieties

    ⇝ potential modularity (2002, 2006) for $GL_2$

2. Harris-Shepherd-Barron-Taylor's variant by Calabi-Yau family

    ⇝ potential automorphy for unitary groups

    ⇝ a large part of Sato-Tate Conjecture (2010)

3. Khare-Wintenberger's strict compatible systems

    ⇝ Serre's Conjecture (2006, 2006, 2009, 2009)

# §6. Formalism of $R = \mathbb{T}$

## Mazur's idea

Fix $\bar{\rho}_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_p)$,

and $\Sigma$ : a finite set of primes

$\Rightarrow$ Consider <u>all</u> lifts

$$\rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}_p)$$

with the restriction on the ramification of $\rho_p$.

i.e. $\rho_p$ should have the "same" ramification outside $\Sigma$,

and no ramification condition in $\Sigma$.

( If $\Sigma \ni p$, we put a semistability at $p$, instead of no condition at $p$. )

If $\bar{\rho}_p$ is absolutely irreducible

$\Longrightarrow$ $\exists!$ universal representation among such lifts.

i.e. $\exists!$ $R_\Sigma$ : noetherian local ring / $\mathbb{Z}_p$

$\exists!$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_p^{\mathrm{univ}}} GL_2(R_\Sigma)$

such that

$\forall \rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}_p)$ a lift of $\bar{\rho}_p$ satisfying the ramification condition,

$\exists!$ $R_\Sigma \twoheadrightarrow \mathbb{Z}_p$ such that

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "\rho_p^{\mathrm{univ}}"] \arrow[dr, "\rho_p"'] & GL_2(R_\Sigma) \arrow[d] \arrow[dl, phantom, "\circlearrowright"] \\ & GL_2(\mathbb{Z}_p) \end{tikzcd}$$

$R_\Sigma$ is called the universal deformation ring.

(Without the ramification condition, we cannot show the existence of such a $R$.)

For the given $\Sigma$ & $\bar{\rho}_p$,

we also have a (localized) Hecke algebra

$$\mathbb{T}_\Sigma$$

(which acts on a space of cusp forms)

- Eichler–Shimura construction,
- Carayol's local-global compatibility (1986)

+ some arguments

$$\rightsquigarrow \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\exists !} GL_2(\mathbb{T}_\Sigma)$$

universal among lifts of $\bar{\rho}_p$

— satisfying the given ramification condition

— and <u>modular</u>

$\rightsquigarrow$ By the universality of $R_\Sigma$,

$$\exists! \; R_\Sigma \longrightarrow \mathbb{T}_\Sigma$$

universal w.r.t.
- lifts of $\bar{\rho}_p$
- ramification condition $\Sigma$

universal w.r.t.
- lifts of $\bar{\rho}_p$
- ramification condition $\Sigma$
- <u>modular</u>

<u>Want</u> to show

$$R_\Sigma \xrightarrow{\sim} \mathbb{T}_\Sigma \;!$$

Picture

(elliptic curves)

(modular forms)

(Galois representations)

"incarnation"

"incarnation"

$$R_\Sigma \longrightarrow\!\!\!\!\rightarrow \mathbb{T}_\Sigma$$

deformation ring

Hecke algebra

<u>Want</u> to show

$$R_\Sigma \twoheadrightarrow \Pi_\Sigma$$

is an isom. for $^\forall \Sigma$.

<u>Strategy</u>

① Show $R_\Sigma \xrightarrow{\sim} \Pi_\Sigma$

for $\Sigma = \phi$ (empty set)

② Induction on $\Sigma$ i.e.

Assume $R_\Sigma \xrightarrow{\sim} \Pi_\Sigma$

$\Rightarrow$ Show $R_{\Sigma \cup \{\ell\}} \xrightarrow{\sim} \Pi_{\Sigma \cup \{\ell\}}$

for $^\forall \ell \notin \Sigma$

To show $R_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$

is an isom.

<u>Want</u>

to show

- $R_\Sigma$ is <u>small</u> enough

  i.e. bound it from the above,

- $\mathbb{T}_\Sigma$ is <u>large</u> enough

  i.e. bound it from the below,

Fix $f$ : a modular form satisfying the given ramification condition.

(If $\bar{\rho}_p$ is modular, such $f$ exists)

$$\rightsquigarrow R_\Sigma \to \mathbb{T}_\Sigma \xrightarrow[\pi_{\mathbb{T}_\Sigma}]{} \mathbb{Z}_p$$

by $\rho_{f,p}$

$\pi_{R_\Sigma}$

- To calculate a "size" of $R_\Sigma$, we use the cotangent space
$$\mathfrak{p}_\Sigma / \mathfrak{p}_\Sigma^2$$

- To calculate a "size" of $\mathbb{T}_\Sigma$ we use the congruence ideal
$$\eta_\Sigma \ (\subset \mathbb{Z}_p)$$

$$\left( \begin{array}{l} \mathfrak{p}_\Sigma := \ker(\pi_{R_\Sigma} : R_\Sigma \twoheadrightarrow \mathbb{Z}_p), \quad \mathfrak{p}_\Sigma \subset R_\Sigma \\ \\ \eta_\Sigma := \pi_{\mathbb{T}_\Sigma}\left( \operatorname{Ann}_{\mathbb{T}_\Sigma} (\ker \pi_{\mathbb{T}_\Sigma}) \right), \quad \eta_\Sigma \subset \mathbb{Z}_p \end{array} \right)$$

We have

$$\#(\mathfrak{p}_\Sigma/\mathfrak{p}_\Sigma^2) \geq \#(\mathbb{Z}_p/\eta_\Sigma)$$

Wiles' numerical criterion (purely commutative algebra)

$R_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$ is an isom.

& they are locally of complete intersection

$$\Longleftrightarrow \#(\mathfrak{p}_\Sigma/\mathfrak{p}_\Sigma^2) = \#(\mathbb{Z}_p/\eta_\Sigma)$$

Remark In Wiles' original paper,

he assumed the Gorenstein-ness of $\mathbb{T}_\Sigma$.

Lenstra showed the numerical criterion

without Gorenstein-ness.

(1995)

$\rightsquigarrow$ Reduced showing a ring isomorphism

to a numerical equality

① To calculate $\wp_\Sigma/\wp_\Sigma^2$, we have

$\mathrm{ad}^0(-) = \mathrm{End}(-)^{\mathrm{tr}=0}$ ← dim = 3

$\circlearrowleft \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

$$H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho_{f,p} \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

$$\simeq \mathrm{Hom}_{\mathbb{Z}_p}(\wp_\Sigma/\wp_\Sigma^2, \mathbb{Q}_p/\mathbb{Z}_p)$$

Selmer group

(Galois cohomology with local conditions)

② We can calculate $\eta_\Sigma$

via the pairing on Hecke modules

$H_\Sigma$

$\mathbb{T}_\Sigma \circlearrowright$

a (localized) space of cusp forms

Remark

In the original paper,

Wiles needed to show that

$$H_\Sigma \text{ is } \underline{\text{free}} \text{ over } \mathbb{T}_\Sigma$$

need mod $p$ multiplicity one

(Mazur's technique)

Diamond (improvement of Taylor-Wiles system, and Wiles' numerical criterion 1997)

Use

$$\Omega_\Sigma := H_\Sigma / \left( H_\Sigma[\mathfrak{p}_{\mathbb{T}_\Sigma}] + H_\Sigma[\mathrm{Ann}_{\mathbb{T}_\Sigma} \mathfrak{p}_{\mathbb{T}_\Sigma}] \right)$$

where $\mathfrak{p}_{\mathbb{T}_\Sigma} := \ker(\pi_{\mathbb{T}_\Sigma} : \mathbb{T}_\Sigma \longrightarrow \mathbb{Z}_p)$

<u>instead of $\eta_\Sigma$</u>

$\Longrightarrow$ No need to show $H_\Sigma$ is free over $\mathbb{T}_\Sigma$

Moreover can show the freeness <u>as an output</u>.

(the criterion is replaced by

$$\mathrm{length}_{\mathbb{Z}_p} \mathfrak{p}_\Sigma / \mathfrak{p}_\Sigma^2 = \mathrm{length}_{\mathbb{Z}_p} \Omega_\Sigma$$
)

# §7. Reduce to the minimal case

Want to show

If $R_\Sigma \xrightarrow{\sim} \mathbb{T}_\Sigma$ $\left( \iff \# \wp_\Sigma / \wp_\Sigma^2 = \# \mathbb{Z}_p / \eta_\Sigma \right)$

& they are locally of complete intersection

$\implies R_{\Sigma \cup \{\ell\}} \xrightarrow{\sim} \mathbb{T}_{\Sigma \cup \{\ell\}}$

for $\ell \notin \Sigma$ $\left( \iff \# \wp_{\Sigma \cup \{\ell\}} / \wp_{\Sigma \cup \{\ell\}}^2 = \# \mathbb{Z}_p / \eta_{\Sigma \cup \{\ell\}} \right)$

& they are locally of complete intersection

By the numerical criterion,

it suffices to show that

$$\#\left(\left(\mathfrak{p}_\Sigma u_{\{e_4\}} / \mathfrak{p}_\Sigma^2 u_{\{e_4\}}\right) / \left(\mathfrak{p}_\Sigma / \mathfrak{p}_\Sigma^2\right)\right)$$

$$\leqq \#\left(\eta_\Sigma / \eta_\Sigma u_{\{e_4\}}\right)$$

(In Diamond's method

$$\mathrm{length}_{\mathbb{Z}_p}\left(\left(\mathfrak{p}_\Sigma u_{\{e_4\}} / \mathfrak{p}_\Sigma^2 u_{\{e_4\}}\right) / \left(\mathfrak{p}_\Sigma / \mathfrak{p}_\Sigma^2\right)\right)$$

$$\leqq \mathrm{length}_{\mathbb{Z}_p} \Omega_\Sigma u_{\{e_4\}} / \Omega_\Sigma$$ )

① <u>Want</u> to calculate

$$\left(\mathfrak{p}_{\Sigma\cup\{\ell\}}/\mathfrak{p}^2_{\Sigma\cup\{\ell\}}\right)\Big/\left(\mathfrak{p}_{\Sigma}/\mathfrak{p}^2_{\Sigma}\right)$$

$$\begin{array}{ccc} \updownarrow & & \updownarrow \\ \text{Selmer gp} \quad H^1_{\Sigma\cup\{\ell\}} & \longleftrightarrow & H^1_{\Sigma} \end{array}$$

<u>difference</u>

can calculate by

local Galois cohomology

② Want to calculate

$$\eta_\Sigma / \eta_{\Sigma \cup \{\ell\}} \quad \left( \text{or} \quad \Omega_{\Sigma \cup \{\ell\}} / \Omega_\Sigma \right)$$

$$\begin{array}{ccc} \wr & & \wr \\ H_\Sigma & \longleftrightarrow & H_{\Sigma \cup \{\ell\}} \\ & \underline{\text{difference}} & \end{array}$$

can calculate by

Ihara's lemma

and its generalization

by Wiles.

① + ②

$\leadsto$ can show

$$\# \left( (\wp_{\Sigma \cup \{\ell\}} / \wp^2_{\Sigma \cup \{\ell\}}) / (\wp_\Sigma / \wp_\Sigma^2) \right) \leq \# (\eta_\Sigma / \eta_{\Sigma \cup \{\ell\}})$$

$$\left( \text{or } \operatorname{length}_{\mathbb{Z}_p} \left( (\wp_{\Sigma \cup \{\ell\}} / \wp^2_{\Sigma \cup \{\ell\}}) / (\wp_\Sigma / \wp^2_\Sigma) \right) \leq \operatorname{length}_{\mathbb{Z}_p} \Omega_{\Sigma \cup \{\ell\}} / \Omega_\Sigma \right)$$

Remark ①

Kisin's modified Taylor-Wiles system

by using the integral $p$-adic
Hodge theory
(2009)

$\Longrightarrow$ No need of the induction.

In particular, no need of
Ihara's lemma

(In the unitary group case ($\rightsquigarrow$ Sato-Tate conjecture),
Ihara's lemma is still open, and
this improvement was essential
for the proof of Sato-Tate conjecture!)

Remark ②

For the fixed $f$ $\left(\rightsquigarrow \pi_\Sigma \xrightarrow{\pi\text{-}\theta_\Sigma} \mathbb{Z}_p\right)$

Shimura

$$\frac{L(\mathrm{Sym}^2 f, 2)}{\sqrt{-1}\,\pi\,\Omega_f} \sim N^{-1} \#(\mathbb{Z}_p/\eta_\Sigma)$$

up to $\mathbb{Z}_p^\times$

$N :=$ level of $f$

$\Omega_f$ : the period of $f$.

by Rankin-Selberg method.

Therefore,

$$\#(\mathfrak{P}_\Sigma/\mathfrak{P}_\Sigma^2) = \#(\mathbb{Z}_p/\eta_\Sigma)$$

says

the special value of the L-function for $\mathrm{Sym}^2$ of $f$

can be expressed by

- the period $\Omega_f$ and
- the order of the Selmer group

→ a generalization of the analytic class number formula

(Beilinson Conjecture, and Bloch-Kato's Tamagawa number Conjecture.)

# §8. The minimal case

## — Taylor-Wiles system

Want to show

$$R_\phi \xrightarrow{\sim} \mathbb{T}_\phi$$

In the original paper,

Wiles showed that

$\mathbb{T}_\phi$ is locally of complete intersection

by Taylor-Wiles system

$\underset{\text{some arguments}}{\Longrightarrow}$ $R_\phi \xrightarrow{\sim} \mathbb{T}_\phi$ by using the numerical criterion once again.

## Remark

**Taylor - Wiles (1995)**

$\left\{\begin{array}{l}\cdot \text{ the existence of Taylor-Wiles system} \\ \cdot \text{ the freeness of } H_\Sigma \text{ over } \mathbb{T}_\Sigma\end{array}\right.$

$\Longrightarrow$ $\mathbb{T}_\phi$ is locally of complete intersection

$\left( \underset{+\text{ some arguments + numerical criterion}}{\Longrightarrow} \quad R_\phi \xrightarrow{\sim} \mathbb{T}_\phi \right)$

**Faltings (1995)**

$\left\{\begin{array}{l}\cdot \text{ the existence of Taylor-Wiles system} \\ \cdot \text{ the freeness of } H_\Sigma \text{ over } \mathbb{T}_\Sigma\end{array}\right.$

$\underset{\text{directly}}{\Longrightarrow} \left\{\begin{array}{l}\cdot\ R_\phi \xrightarrow{\sim} \mathbb{T}_\phi \\ \cdot\ \mathbb{T}_\phi \text{ is locally of complete intersection}\end{array}\right.$

**Diamond (1997)**

the existence of Taylor-Wiles system

$\Longrightarrow \left\{\begin{array}{l}\cdot\ R_\phi \xrightarrow{\sim} \mathbb{T}_\phi \\ \cdot\ \mathbb{T}_\phi \text{ is locally of complete intersection} \\ \cdot\ H_\phi \text{ is free over } \mathbb{T}_\phi\end{array}\right.$

Taylor-Wiles system

$$\begin{tikzcd} & \mathbb{Z}_p[[X_1, \cdots, X_r]] \arrow[d] & & \\ \mathbb{Z}_p[[S_1, \cdots, S_r]] \arrow[r] & R_{Q_n} \arrow[r, two heads] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & \mathbb{T}_{Q_n} \arrow[d] & \circlearrowright H_{Q_n} \text{ faithful} \arrow[d] \\ & R_\phi \arrow[r, two heads] & \mathbb{T}_\phi & \circlearrowright H_\phi \end{tikzcd}$$

this is not compatible system
with respect to $n$.

( not assuming the existence of
$R_{Q_{n+1}} \to R_{Q_n}$ etc. )

$Q_n \ni {}^\forall q, \quad q \equiv 1 \mod p^n$

① By carefully choosing $Q_n$ (by Čebotarev density),

we can kill the dual Selmer group
for $Q_n$

$\rightsquigarrow$ can bound $R_{Q_n}$ from the above
by the same $r$
independent of $n$

② By de Shalit's method,

can show

$H_{\Omega_n}$ is free over

$$\mathbb{Z}_p[S_1, \cdots, S_r] / ((S_1+1)^{p^n}-1, \cdots, (S_r+1)^{p^n}-1)$$

the same $r$

$\rightsquigarrow$ can bound $\mathcal{T}_{\Omega_n}$ from the below.

Remark

In the original paper,

he needed the Gorenstein-ness of $\mathbb{T}_{Q_n}$

need mod $p$ multiplicity one.

Diamond (improvement of Taylor-Wiles system 1997)

No need of the Gorenstein-ness of $\mathbb{T}_{Q_n}$

By patching arguments

(using "pigeon hole principle")

can take a projective limit

after taking the reduction modulo $p$,

and taking a subsequence of $n$.

$$\Longrightarrow \quad \begin{tikzcd} & \mathbb{F}_p[[X_1, \cdots, X_r]] \arrow[d] & \\ \mathbb{F}_p[[S_1, \cdots, S_r]] \arrow[r] \arrow[drr, hook, bend right] & R_\infty \arrow[r, two heads] & \mathbb{T}_\infty \arrow[d, hook] \\ & & \mathrm{End}(H_\infty) \end{tikzcd}$$

$\uparrow$
freeness of
$H_{Q_n}$ over
$\mathbb{Z}_p[S_1, \cdots, S_r]/((S_1+1)^{p^n}-1, \cdots, (S_r+1)^{p^n}-1)$

$$\Longrightarrow \quad R_\infty \xrightarrow{\sim} \mathbb{T}_\infty$$

$$\Longrightarrow \quad R_\phi \otimes_{\mathbb{Z}_p} \mathbb{F}_p \xrightarrow{\sim} \mathbb{T}_\phi \otimes_{\mathbb{Z}_p} \mathbb{F}_p$$

$$\Longrightarrow \quad R_\phi \xrightarrow{\sim} \mathbb{T}_\phi \quad !$$

Q.E.D.

# My works (partially with S. Yasuda (RIMS, Kyoto))

① Clozel-Harris-Taylor et al. $\rightsquigarrow$ Y.-Yasuda

GL(n) → Sato-Tate Conjecture

this direction

GL(n) with integral p-adic Hodge theory

Taylor-Wiles et al. $\rightsquigarrow$ Kisin

GL(2)
→ Fermat's Conjecture
→ Shimura-Taniyama Conjecture

GL(2) with integral p-adic Hodge theory
→ Serre's Conjecture

② Kisin's modified Taylor-Wiles system

⇝ need to investigate
the universal deformation rings
for a <u>local</u> field

⇝ need to calculate
the reductions modulo $p$
of the crystalline representations

⇝ We (Y.-Yasuda) calculated them
for weight $\leq (p^2-p)/2$

the <u>hypergeometric functions</u>
mysteriously appeared.

Thank you

very much!