

"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  $n \in \mathbb{Z}, n \geq 3,$

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  $R = T$ ,  
- 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

③  
bis

FLT §1

⇕ Ribet

Shimura-Taniyama Conjecture §2

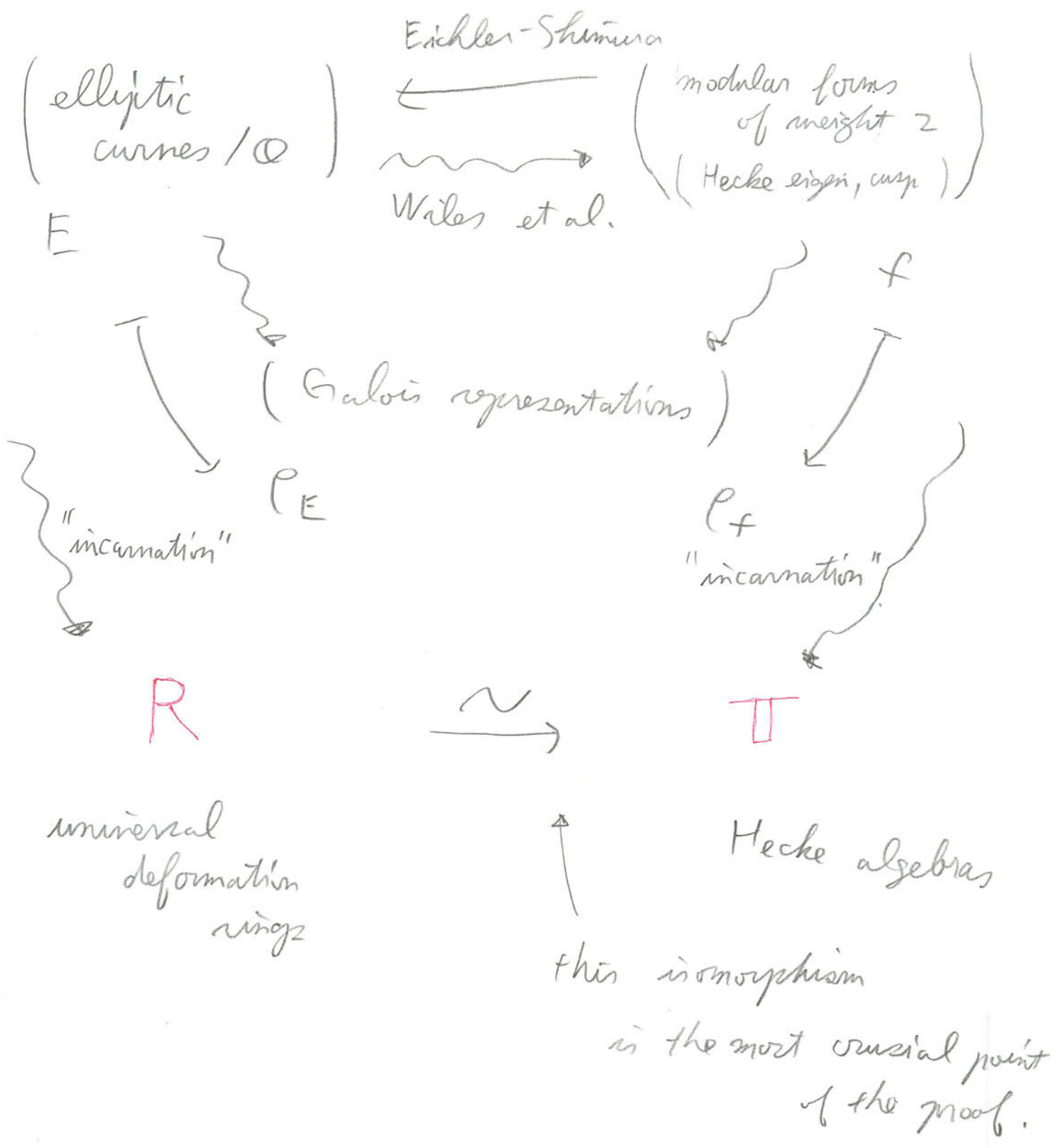
(for semistable elliptic curves)

⇕ 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



# Generalizations of Taylor-Wiles

(4) bis

technique

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

→ Sato-Tate Conjecture  
BLGHT (2011)

↑  
generalization

(Taylor-Wiles)  
et al.  
 $GL(2)$

generalization

→ (Kisin)

$GL(2)$  with  
integral  $p$ -adic  
Hodge theory

→ Fermat's Last Theorem  
(1995)

→ Shimura-Taniyama Conjecture  
BCDT (2001)

→ Serre's Conjecture  
KW (2009)

( All years in this notes are  
the publication years,  
not the years of preprints. )

§2. Reduce to Shimura-Taniyama Conjecture

(5)

for semistable elliptic curves

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

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

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

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

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

Then we have

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

(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

(17)

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

$= \prod_{\substack{\text{good } p \\ \text{inf}}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$   $\left( \begin{array}{l} q = e^{2\pi i z}, \\ z \in \mathcal{Y} := \{z \in \mathbb{C} \mid \text{Im } z > 0\} \\ \text{upper half plane} \end{array} \right.$

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

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

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

$\tilde{E}$ : the reduction of  $E$  modulo  $p$

i.e. at a good prime  $p$  for  $E$ .

$\forall E, \exists f = \sum a_n q^n$  Hecke eigen cusp form such that  $a_p = 1 + p - \#\tilde{E}(\mathbb{F}_p)$  for good  $p$

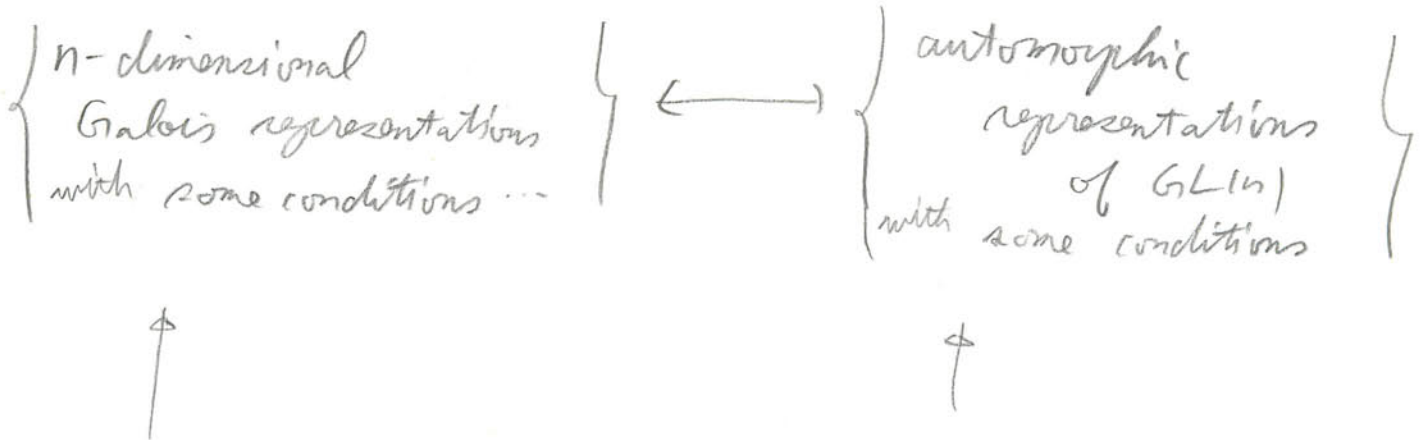
Remark D

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.



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

(15)

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

① Ramanujan-Petersson Conjecture (Deligne, 1974)

proved by

• weight yoga  $\longleftarrow$

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

proved by

$\longrightarrow$  • easy to calculate

$$S_2(\Gamma_0(2)) = 0$$

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

proved by

$\longrightarrow$  • good analytic property

# Ribet (level lowering)

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

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

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

( $\mu$ -torsion points) of weight 2,

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

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

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

for almost all primes  $\ell$ ,

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

Frey curve

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

has the discriminant

the differences of the roots

↙ ↓ ↓

$$\begin{aligned} \Delta &:= 16 (a^p - 0)(b^p - 0)(a^p - (-b^p))^2 \\ &= 16 (abc)^{2p} \end{aligned}$$

→ the conductor of  $E[p]$

$$= 2 \prod l$$

$$\frac{l|\Delta}{l \neq 2}$$

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

$$= 2$$

So, the corresponding modular form  
is of weight = 2, level = 2

However,

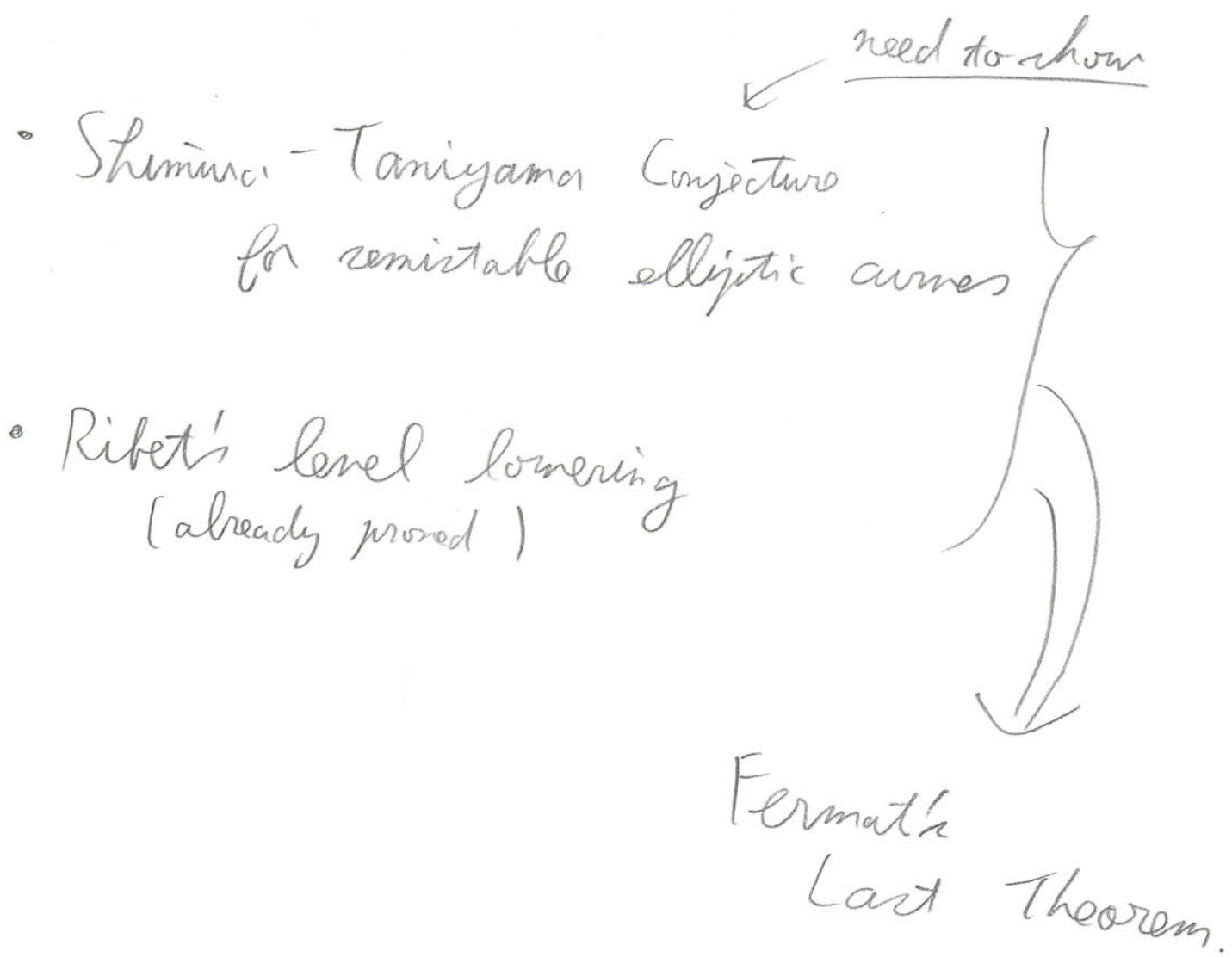
$$S_2(\Gamma_0(2)) = 0$$

↑	↑
weight = 2	level = 2

contradiction!



In short,



Remark ①

(16)

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)

⇒ can avoid Ribet's level lowering  
(and hard algebraic geometry)

### § 3. Galois representations

(17)

$\mu$ : prime

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

$\mu^n$ -torsion points

$$\rightsquigarrow T_\mu E := \varprojlim_n E[\mu^n](\overline{\mathbb{Q}})$$

$$\curvearrowright \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

free of rank = 2

Tate module of  $E$

$$\rightsquigarrow \rho_{E,\mu} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_\mu)$$

$f$  : modular form

$$\text{(omit)} \rightarrow \rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_p)$$

Galois representation associated to a modular form

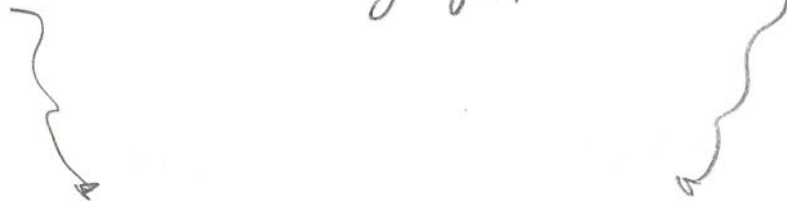
Constructions

- weight = 2 : Eichler - Shimura
- weight > 2 : Deligne (1971)
- weight = 1 : Deligne - Serre (1974)

For simplicity, we used  $\text{GL}_2(\mathbb{Z}_p)$  here.  
 In general, we need to use  
 the ring of integers of  $\mathbb{Q}(a_n/nz_1)$   
 for  $f = \sum a_n q^n$   
 instead of  $\mathbb{Z}_p$ .

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

very far



$\rho_{E,p}$

$\rho_{f,p}$

Galois representations

compare them by the Galois representations!

d.r.p. Given  $E,$

Find  $f$  such that

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

for some  $p$ !

$$\left( \begin{array}{l} \text{easy} \\ \implies \end{array} \rho_{E,p} \cong \rho_{f,p} \text{ for all } p \right)$$

## §4. Reduce to the modularity lifting

(20)

Given  $E$ , want to find  $f$   
such that  $\rho_{E, \mu} \cong \rho_{f, \mu}$

$$\begin{array}{ccc} \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_{E, \mu}} & \text{GL}_2(\mathbb{Z}_\mu) \\ & \searrow \bar{\rho}_{E, \mu} & \downarrow \text{mod } \mu \\ & & \text{GL}_2(\mathbb{F}_\mu) \end{array}$$

### Strategy

- ① Show  $\bar{\rho}_{E, \mu}$  is modular.  
(i.e. comes from a modular form)
- ② Next, show  $\rho_{E, \mu}$  is modular.

For simplicity, we used  $\text{GL}_2(\mathbb{Z}_\mu)$  from now on.

In general, we need to use  
the ring of integers of  
a finite extension of  $\mathbb{Q}$   
instead of  $\mathbb{Z}_\mu$ .

As for  $\mathbb{D}$ ,

(21)

for  $p=3$   $GL_2(\mathbb{F}_3)$  is solvable

$\Rightarrow$  Langlands-Tunnell (base change theorems)

$\overline{\rho}_{F,3}$  is modular

Step  $\mathbb{D}$  is OK!

Remark

Khare - Winterberger's

strictly compatible system

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

this is also based on Wiles'

$R = T$  techniques.



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

(23)

Want  $\bar{\rho}_n$  : modular  $\Rightarrow \rho_n$  : modular

called *modularity lifting*

$$\begin{array}{ccc} \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_n} & \text{GL}_2(\mathbb{Z}_n) \\ & \searrow \bar{\rho}_n & \downarrow \\ & & \text{GL}_2(\mathbb{F}_n) \end{array}$$

Wiles' techniques work

only when  $\bar{\rho}_n$  is absolutely irreducible

Unfortunately  $\bar{\rho}_{E,3}$  may not

be absolutely irreducible.




By using Mazur's theorem

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

$\implies \bar{\rho}_{E,5}$  is absolutely irreducible

But, we don't know

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

(  $GL_2(\mathbb{F}_5)$  is not solvable. ) 

In short

$\overline{\rho}_{E,3}$  } • modular  
 • may not be absolutely irreducible.

$\overline{\rho}_{E,5}$  } • don't know to be modular  
 • absolutely irreducible  
 if  $\overline{\rho}_{E,3}$  is not.

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

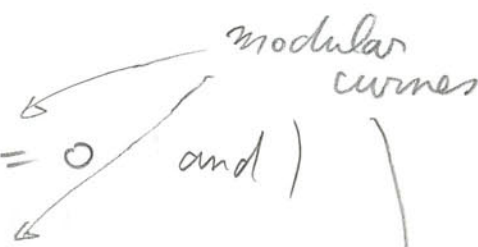
①  $E'$ : semistable

②  $E'[5] \cong E[5]$

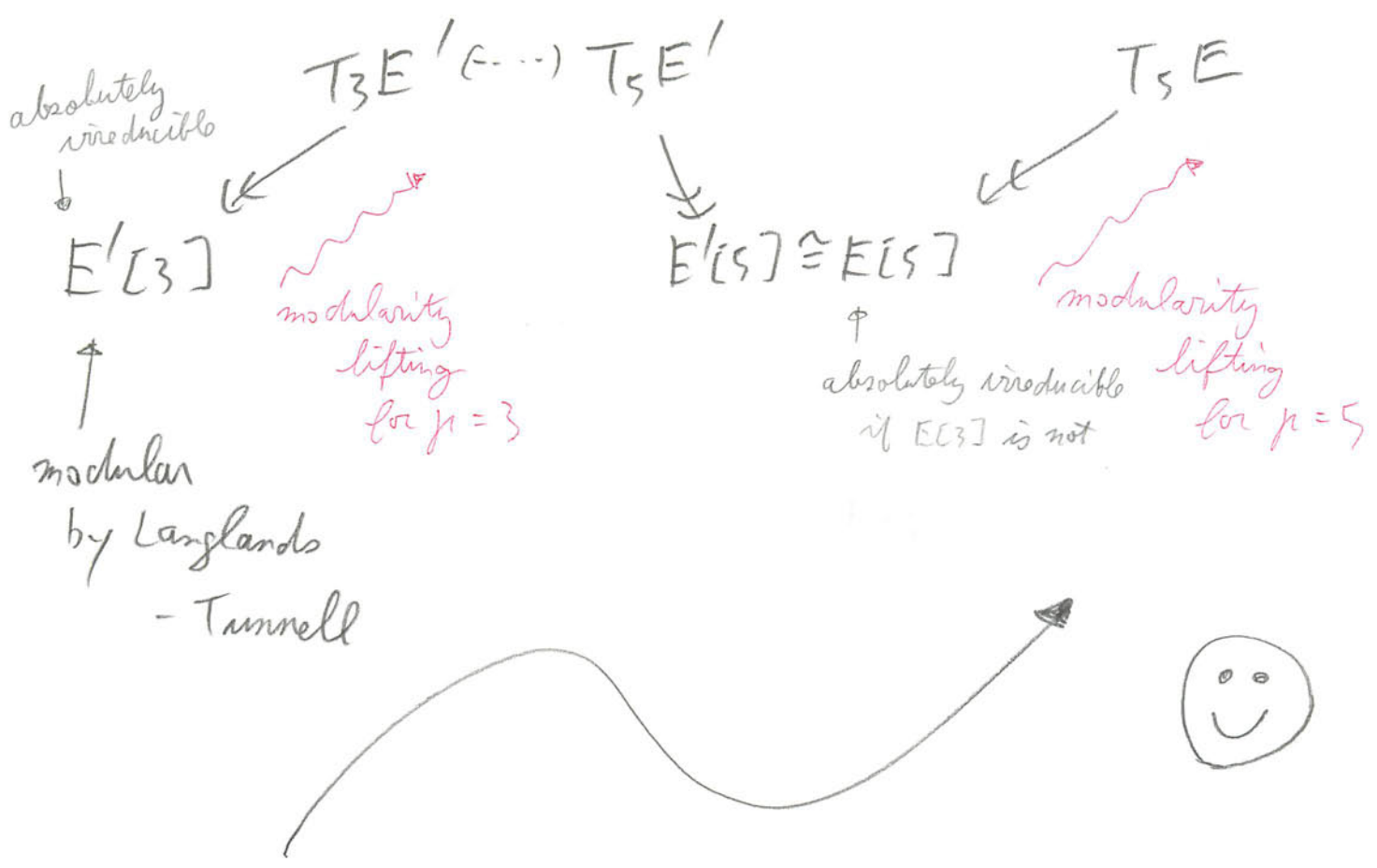
as  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -representations

③  $E'[3]$  is absolutely irreducible.

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



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

Remark ① We used for  $\mu=3, q=5$

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

②  $g(X(\Gamma(q) \cap \Gamma_0(\mu))) > 1$

③  $GL_2(\mathbb{F}_\mu)$  is solvable

④  $g(X(q)) = 0$

① holds for  $\forall q > 3$

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

③ holds only for  $\mu = 2, 3$

④ holds only for  $q = 2, 3, 5$

For odd primes  $\mu \neq q$ ,

only  $(3, 5)$  can be available!

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

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 $R = T$

(30)

### Mazur's idea

$$\text{Fix } \bar{\rho}_\mu : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\mathbb{F}_\mu),$$

and  $\Sigma$  : a finite set of primes

$\Rightarrow$  Consider all lifts

$$\rho_\mu : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\mathbb{Z}_\mu)$$

with the restriction on the ramification  
of  $\rho_\mu$ .

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

and no ramification condition in  $\Sigma$ .

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



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

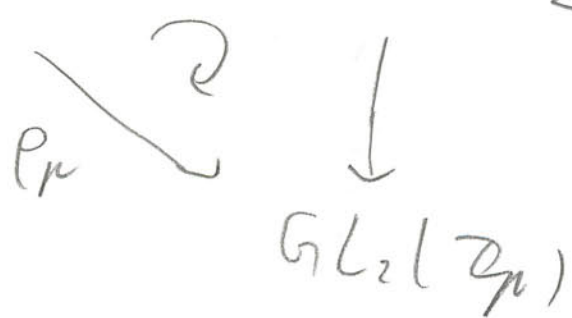
$\Rightarrow \exists!$  universal representation among such lifts.

i.e.  $\exists!$   $R_\Sigma$  : noetherian local ring /  $\mathbb{Z}_p$   
 $\exists!$   $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_p^{\text{univ}}} \text{GL}_2(R_\Sigma)$   
such that

$\forall \rho_p : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_p)$   
a lift of  $\bar{\rho}_p$  satisfying the ramification condition,

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

$$\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_p^{\text{univ}}} \text{GL}_2(R_\Sigma)$$



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

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

For the given  $\Sigma$  &  $\bar{P}_\mu$ ,

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)

$$\rightsquigarrow \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\exists!} \text{GL}_2(\mathbb{T}_\Sigma)$$

some arguments

universal among lifts of  $\bar{P}_\mu$

- satisfying the given ramification condition
- and modular

By the universality of  $R_\Sigma$ ,

$$\exists! R_\Sigma \longrightarrow T_\Sigma$$

universal  
w.r.t.

- lifts of  $\bar{P}_n$
- ramification conditions  $\Sigma$

universal  
w.r.t.

- lifts of  $\bar{P}_n$
- ramification conditions  $\Sigma$
- modular

Want to show

$$R_\Sigma \xrightarrow{\sim} T_\Sigma !$$

Picture

(elliptic curves)

(modular forms)

(Galois representations)

"incarnation"

"incarnation"

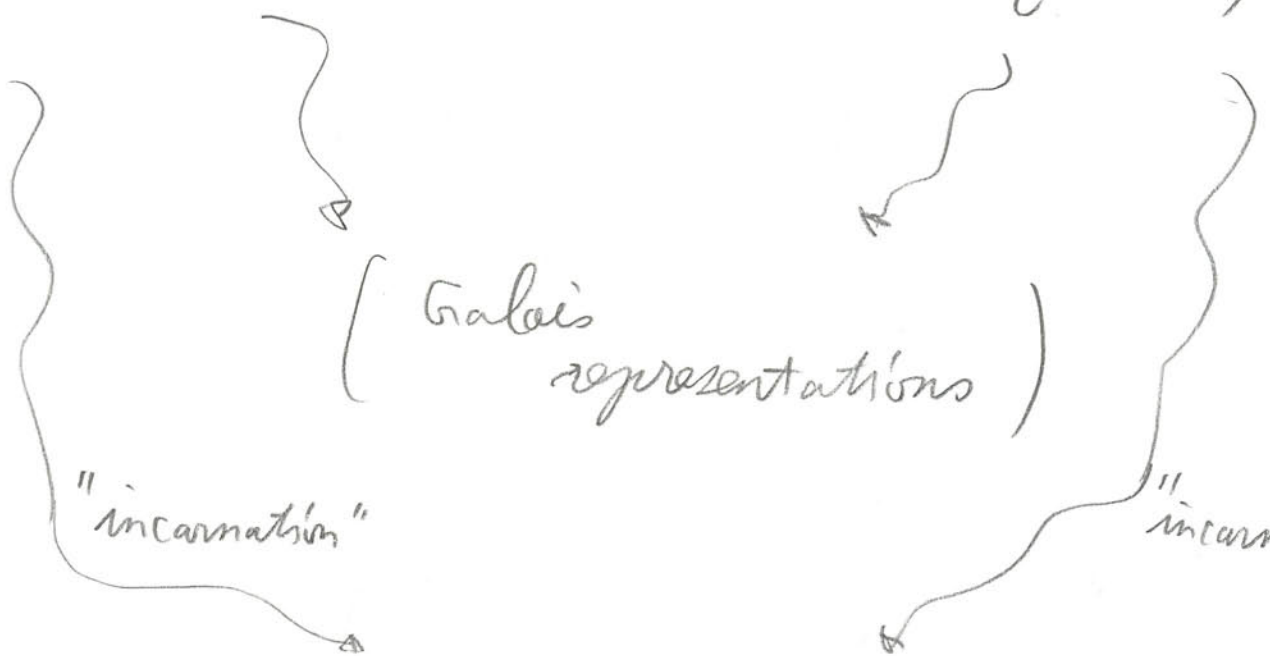
$R_\Sigma$

$\longrightarrow$

$H_\Sigma$

deformation ring

Hecke algebra



Want to show

(35)

$$R_{\Sigma} \twoheadrightarrow T_{\Sigma}$$

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

Strategy

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

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

② Induction on  $\Sigma$  i.e.

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

$\Rightarrow$  Show  $R_{\Sigma \cup \{a\}} \xrightarrow{\sim} T_{\Sigma \cup \{a\}}$   
for  $\forall a \in \Sigma$

To show  $R_\Sigma \xrightarrow{\cong} \mathbb{T}_\Sigma$   
is an isom.

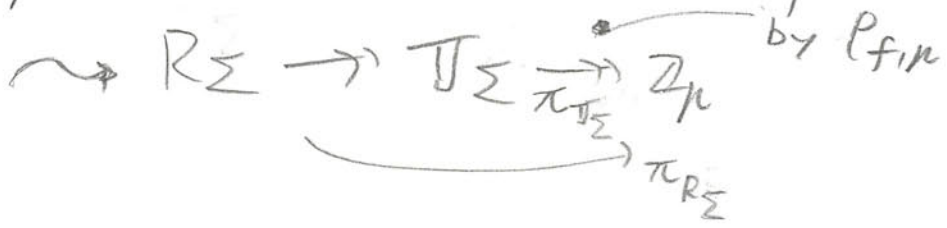
Want

to show

- $R_\Sigma$  is small enough  
i.e. bound it from the above,
- $\mathbb{T}_\Sigma$  is large 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)



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

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

$$\left( \begin{array}{l}
 \mathfrak{p}_\Sigma := \ker(\pi_{R_\Sigma} : R_\Sigma \rightarrow \mathbb{Z}_p) \\
 \eta_\Sigma := \pi_{T_\Sigma} \left( \text{Ann}_{T_\Sigma}(\ker \pi_{T_\Sigma}) \right) \\
 \cap \\
 \mathbb{Z}_p
 \end{array} \right)$$

We have

$$\#(R_{\Sigma}/R_{\Sigma}^2) \geq \#(Z_{\mu}/\eta_{\Sigma})$$

Wiles' numerical criterion (purely commutative algebra)

$R_{\Sigma} \rightarrow T_{\Sigma}$  is an isom.

& they are locally of complete intersection

$$\Leftrightarrow \#(R_{\Sigma}/R_{\Sigma}^2) = \#(Z_{\mu}/\eta_{\Sigma})$$

Remark In Wiles' original paper,

he assumed the Gorenstein-ness of  $T_{\Sigma}$ .

Lenstra showed the numerical criterion without Gorenstein-ness.

(1995)

→ Reduced showing a ring isomorphism  
to a numerical equality



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

$\swarrow \dim = 3$   
 $ad^0(-) = \text{End}(-)^{tr=0}$   
 $\mathbb{Q} \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

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

$$\uparrow \cong \text{Hom}_{\mathbb{Z}_p}(\beta_\Sigma / \beta_\Sigma^2, \Phi/\mathbb{Z}_p)$$

Selmer group

(Galois cohomology with local conditions)

② We can calculate  $\eta_\Sigma$

via the pairing on Hecke modules

$$H_\Sigma$$

$$\mathbb{H}_\Sigma \overset{\mathbb{Q}}{\uparrow}$$

a (localized) space of cusp forms

## Remark

(40)

In the original paper,

Wiles needed to show that

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

need mod  $\mu$  multiplicity one  
(Mazur's technique)

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

Use

$$\Omega_\Sigma := H_\Sigma / (H_\Sigma[\rho_{\mathbb{T}_\Sigma}] + H_\Sigma[\text{Ann}_{\mathbb{T}_\Sigma} \rho_{\mathbb{T}_\Sigma}])$$

where  $\rho_{\mathbb{T}_\Sigma} := \ker(\pi_{\mathbb{T}_\Sigma}: \mathbb{T}_\Sigma \rightarrow \mathbb{Z}_\mu)$

instead of  $\eta_\Sigma$

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

Moreover can show the freeness as an output.

(the criterion is replaced by  
 $\text{length}_{\mathbb{T}_\Sigma} \rho_\Sigma / \mathfrak{p}_\Sigma^2 = \text{length}_{\mathbb{T}_\Sigma} \Omega_\Sigma$ )

# § 7. Reduce to the minimal case

(41)

Want to show

$$\text{If } R_\Sigma \xrightarrow{\sim} T_\Sigma \quad (\Leftrightarrow) \# \beta_\Sigma / \beta_\Sigma^2 = \# \mathbb{Z}_p / \eta_\Sigma$$

& they are locally of complete intersection

$$\Rightarrow R_{\Sigma^{\vee_{l \in L}}} \xrightarrow{\sim} T_{\Sigma^{\vee_{l \in L}}}$$

$$\text{for } l \in \Sigma \quad \left( \begin{array}{l} (\Leftrightarrow) \# \beta_{\Sigma^{\vee_{l \in L}}} / \beta_{\Sigma^{\vee_{l \in L}}}^2 \\ = \# \mathbb{Z}_p / \eta_{\Sigma^{\vee_{l \in L}}} \end{array} \right)$$

& they are locally of complete intersection

By the numerical criterion,

it suffices to show that

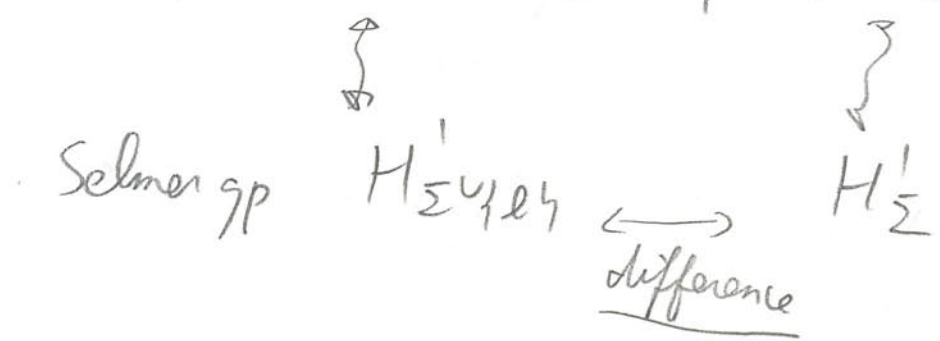
$$\begin{aligned} \# \left( (\rho_{\Sigma}^{\nu_{124}} / \rho_{\Sigma}^2) / (\rho_{\Sigma} / \rho_{\Sigma}^2) \right) \\ \leq \# \left( \eta_{\Sigma} / \eta_{\Sigma}^{\nu_{124}} \right) \end{aligned}$$

( In Diamond's method )

$$\begin{aligned} \text{length}_{\mathbb{Z}_p} \left( (\rho_{\Sigma}^{\nu_{124}} / \rho_{\Sigma}^2) / (\rho_{\Sigma} / \rho_{\Sigma}^2) \right) \\ \leq \text{length}_{\mathbb{Z}_p} \Omega_{\Sigma}^{\nu_{124}} / \Omega_{\Sigma} \end{aligned}$$

① Want to calculate

$$(\rho_{\Sigma^4 \ell^4} / \rho_{\Sigma^4 \ell^4}^2) / (\rho_{\Sigma} / \rho_{\Sigma}^2)$$



can calculate by  
*local Galois cohomology*

② Want to calculate

$$\eta_\Sigma / \eta_{\Sigma^4} \quad (\text{or} \quad \Omega_{\Sigma^4} / \Omega_\Sigma)$$

$$\begin{matrix} \uparrow & & \uparrow \\ H_\Sigma & \xrightarrow{\text{difference}} & H_{\Sigma^4} \end{matrix}$$

can calculate by

Ihara's lemma

and its generalization

by Wiles.

①+②

can show

$$\# \left( \frac{|\mathcal{P}_{\Sigma^4} / \mathcal{P}_{\Sigma^4}^2|}{|\mathcal{P}_\Sigma / \mathcal{P}_\Sigma^2|} \right) \leq \# \left( \eta_\Sigma / \eta_{\Sigma^4} \right)$$

$$\left( \text{or } \text{length}_m \left( \frac{|\mathcal{P}_{\Sigma^4} / \mathcal{P}_{\Sigma^4}^2|}{|\mathcal{P}_\Sigma / \mathcal{P}_\Sigma^2|} \right) \leq \text{length}_m \Omega_{\Sigma^4} / \Omega_\Sigma \right)$$

Remark ①

Kisinn's modified Taylor-Wiles system

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

$\Rightarrow$  No need of the induction.

In particular, no need of  
Ihara's lemma

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



Remark 2

(46)

For the fixed  $f$  ( $\sim \pi_\Sigma \xrightarrow{\pi_\Sigma} \mathbb{Z}_N$ )

Shimura

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

↑  
up to  $\mathbb{Z}_N^\times$

$N :=$  level of  $f$

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

by Rankin-Selberg method.



Therefore,

$$\#(P_{\Sigma}/P_{\Sigma}^2) = \#(D_{\mu}/\eta_{\Sigma})$$

rays

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

(48)

- 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

$\implies R\phi \xrightarrow{\sim} \mathbb{T}\phi$  by using  
some arguments

the numerical criterion  
once again.

Remark

Taylor-Wiles (1995)

- } the existence of Taylor-Wiles system
  - } the freeness of  $H_\Sigma$  over  $\mathbb{T}_\Sigma$
- $\Rightarrow \mathbb{T}_\phi$  is locally of complete intersection
- ( $\Rightarrow R_\phi \xrightarrow{\sim} \mathbb{T}_\phi$   
+ zeta arguments + numerical criterion)

Faltings (1995)

- } the existence of Taylor-Wiles system
  - } the freeness of  $H_\Sigma$  over  $\mathbb{T}_\Sigma$
- $\Rightarrow$  directly
  - }  $R_\phi \xrightarrow{\sim} \mathbb{T}_\phi$
  - }  $\mathbb{T}_\phi$  is locally of complete intersection

Diamond (1997)

the existence of Taylor-Wiles system

- $\Rightarrow$ 
  - }  $R_\phi \xrightarrow{\sim} \mathbb{T}_\phi$
  - }  $\mathbb{T}_\phi$  is locally of complete intersection
  - }  $H_\phi$  is free over  $\mathbb{T}_\phi$

# Taylor-Wiles system

(49)

$$\begin{array}{ccccccc}
 & & \mathbb{Z}_p[X_1, \dots, X_r] & & & & \\
 & & \downarrow & & & & \\
 \mathbb{Z}_p[S_1, \dots, S_r] & \longrightarrow & R_{Q_n} & \longrightarrow & \Pi_{Q_n} & \supset & \text{faithful} \\
 & & \downarrow & & \downarrow & & H_{Q_n} \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & R_\phi & \longrightarrow & \Pi_\phi & \supset & H_\phi
 \end{array}$$

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

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

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

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

we can kill the dual Selmer group  
for  $Q_n$

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

(2) By de Shalit's method,

(50)

can show

$H_{2n}$  is free over

$$\mathbb{Z}_p[S_1, \dots, S_r] / ((S_1+1)^{n_1}-1, \dots, (S_r+1)^{n_r}-1)$$

the same  $r$

$\leadsto$  can bound  $\mathbb{T}_{2n}$  from the below.

Remark

In the original paper,

he needed the Gorenstein-ness of  $\Pi_{\Theta_n}$

↑  
need mod  $p$  multiplicity one.

Diamond (improvement of Taylor-Wiles system)  
1997

No need of the Gorenstein-ness of  $\Pi_{\Theta_n}$

By patching arguments

(using "noether hole principle")

can take a projective limit

after taking the reduction modulo  $\mu$ ,

and taking a subsequence of  $n$ .

$$\begin{array}{ccc} & \mathbb{F}_\mu[X_1, \dots, X_r] & \\ & \downarrow & \\ \Rightarrow & \mathbb{F}_\mu[S_1, \dots, S_r] \longrightarrow R_\infty & \longrightarrow \Pi_\infty \\ & & \downarrow \\ & & \text{End}(H_\infty) \end{array}$$

$\cdot \neq$   
 freeness of  
 $H_\infty$  over  
 $\mathbb{Z}_\mu[S_1, \dots, S_r][S_{r+1}^{p^h-1}, \dots, S_{r+1}^{p^h-1}]$

$$\Rightarrow R_\infty \xrightarrow{\sim} \Pi_\infty$$

$$\Rightarrow R_\phi \otimes_{\mathbb{Z}_\mu} \mathbb{F}_\mu \xrightarrow{\sim} \Pi_\phi \otimes_{\mathbb{Z}_\mu} \mathbb{F}_\mu$$

$$\Rightarrow R_\phi \xrightarrow{\sim} \Pi_\phi !$$

Q.E.D.



My works <sup>(partially)</sup> (with S. Yasuda)  
(RIMS, Kyoto)

(53)

① Clozel-Harris-Taylor  $\rightsquigarrow$  Y. - Yasuda  
et al.  
 $GL(n)$   $GL(n)$  with  
 $\rightarrow$  Sato-Tate Conjecture this direction integral  $p$ -adic  
Hodge theory

Taylor-Wiles  $\rightsquigarrow$  Kisin  
et al.  
 $GL(2)$   $GL(2)$  with  
 $\rightarrow$  Fermat's Conjecture integral  $p$ -adic  
 $\rightarrow$  Shimura-Taniyama Conjecture Hodge theory  
 $\rightarrow$  Serre's Conjecture



② Kisin's modified Taylor-Wiles system

→ need to investigate  
the universal deformation rings  
for a local field

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

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

the hypergeometric functions  
mysteriously appeared.

Thank you

very much!