Deformation rings and Hecke rings.

Notes available from http://www.math.mcgill.ca/goren

The Modularity Theorem: Let $E/\mathbb{Q}$ be an elliptic curve then $E$ is modular: there exists a non constant morphism over $\mathbb{Q}$

$$X_0(N_E) \to E.$$ 

Here $N_E$ is the conductor of $E$. Recall that:

- $p \mid N_E$ iff $E$ has bad reduction at $p$;
- $p \parallel N_E$ iff $E$ has multiplicative reduction at $p$;
- for $p > 3$ we have $p^3 \nmid N_E$;
- For $p = 2$ (resp. 3) the multiplicity of $p$ in $N_E$ is at most 8 (resp. 5).

Example: The conductor of the curve

$$E_n : y^2 + nxy + 2ny = x^3 + nx + 3$$

is divisible by $2^4 \cdot 3^5$ if $n \equiv 0 \pmod{18}$ (usually, for all twists).
History of the Proof

**A. Wiles**: For \( E/\mathbb{Q} \) semistable.
(I.e. \( p^2 \nmid N_E \) for every prime \( p \)).

**F. Diamond**: For \( E/\mathbb{Q} \) semistable at 3 and 5.
(I.e. \( 9 \nmid N_E \) and \( 25 \nmid N_E \)).

**B. Conrad, F. Diamond, R. Taylor**: For \( E/\mathbb{Q} \) acquiring a semistable reduction at 3 over a tamely ramified extension of \( \mathbb{Q}_3 \).
(I.e. \( 3^3 \nmid N_E \)).

**C. Breuil, B. Conrad, F. Diamond, R. Taylor**: For any \( E/\mathbb{Q} \).

The goal of this talk:

Explain Wiles’ strategy in the semistable case and how it is modified in the general case.

---

\(^1\)With the collaboration of **R. Taylor**.
Notions and Notations

The Galois group of a field $F$ is denoted $G_F$. In particular $G_Q$, $G_{Q_p}$. Often an embedding $\mathbb{Q}^{alg} \hookrightarrow \mathbb{Q}_p^{alg}$ is chosen and $G_{Q_p}$ is identified with the corresponding decomposition group $G_p$.

Let $K$ be a finite extension $\mathbb{Q}_\ell$ with maximal order $\mathcal{O}$, prime ideal $\lambda$ and residue field $k$. Let $\widehat{\mathcal{C}}_\mathcal{O}$ be the category of complete local Noetherian $\mathcal{O}$-algebras with residue field $k$. Let

$$\rho : G_Q \longrightarrow \text{GL}_2(R), \quad R \in \text{Ob}(\widehat{\mathcal{C}}_\mathcal{O}),$$

be a continuous representation with underlying module $M$. We say that:

- $\rho$ is **semistable at** $p \neq \ell$ if $\rho|_{I_p} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

- $\rho$ is **Barsotti-Tate at** $\ell$ (BT) if for every finite quotient $N$ of $M$ there exists a finite flat group scheme $\mathcal{F}$ over $\mathbb{Z}_\ell$ with $\mathcal{F}(\mathbb{Q}_\ell^{alg})$ isomorphic to $N$ as $\mathbb{Z}_\ell[G_\ell]$ module.

- $\rho$ is **ordinary at** $\ell$ if $\rho|_{I_\ell} \sim \begin{pmatrix} \epsilon & * \\ 0 & 1 \end{pmatrix}$, where $\epsilon$ is the character giving the action on $\ell$-power roots of $1$.

- $\rho$ is **semistable at** $\ell$ if it is either BT and $\text{det}\rho|_{I_\ell} = \epsilon$ or ordinary.

**Example:** If $\rho_{E,\ell}$ is the $\ell$-adic representation

$$\rho_{E,\ell} : G_Q \longrightarrow \text{GL}_2(\mathbb{Z}_\ell)$$

of a semistable elliptic curve $E/\mathbb{Q}$, then $\rho$ is semistable at all primes (use Tate’s uniformization for $p|N_E$).
Strategy of the proof in the semistable case

**Step 0.** Prove that the $\ell$-adic representation

$$\rho_{E,\ell} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_\ell)$$

is modular for some prime $\ell$.

That is: there exists a newform $f = \sum_{n=1}^{\infty} a_n q^n$ of weight 2, level $\Gamma_1(N_f)$ and character $\psi_f$, with field of definition $K_f = \mathbb{Q}[\{a_n(f)\}_n]$, such that the $\ell$-adic representation

$$\rho_{f,\ell} : G_{\mathbb{Q}} \rightarrow GL_2(K_{f,\lambda})$$

($\lambda$ a prime of $K_f$ dividing $\ell$), is similar to $\rho_{E,\ell}$ over $K_{f,\lambda}$.

(Recall that by Eichler-Shimura theory $f$ “cuts out” of $J_1(N_f)$ an abelian variety $A_f/\mathbb{Q}$ of $GL_2$ type with endomorphism algebra $K_f$, yielding $\rho_{f,\lambda}$ with

$$\text{Tr}(\rho_{f,\lambda}(\text{Fr}_p)) = a_p(f), \quad \det(\rho_{f,\lambda}(\text{Fr}_p)) = p\psi_f(p), \quad (p, N_f) = 1$$)

- **If $E$ is modular**, then by Eichler-Shimura theory there is such a newform $f$ with the same $\ell$-adic representation as associated to $E$.
- **If there exists such a newform $f$** it implies that the $\ell$-adic Tate modules of $A_f$ and $E$ are isomorphic as Galois modules and, by a theorem of Faltings, that $A_f$ and $E$ are isogenous. Thus $E$ is a quotient of $J_1(N_f)$. (Carayol: One needs not worry about getting the precise conductor).

From now on $\ell$ stands for an odd prime
The main result used to prove the modularity of $\rho_{E,\ell}$ is

**Theorem 1.** (Wiles, Taylor-Wiles) Let

$$\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathcal{O})$$

be an odd continuous representation such that:

1. $\bar{\rho}$ is modular and $\bar{\rho}|_{G_{\mathbb{Q}(\ell^{\square})}}$ is absolutely irreducible.
2. $\rho$ is semistable at $\ell$.
3. $\rho$ is ramified at only finitely many primes.
4. For $p \equiv -1 \pmod{\ell}$, $\bar{\rho}|_{I_p}$ reducible $\Rightarrow \bar{\rho}|_{G_p}$ reducible

Then $\rho$ is modular.

**Notation:** $\mathbb{Q}(\ell^{\square}) \overset{\text{def}}{=} \mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell}) \subset \mathbb{Q}(\zeta_{\ell})$.

Given a semistable elliptic curve $E/\mathbb{Q}$ the assumptions of the theorem are easily verified for $\rho = \rho_{E,\ell}$, except for the modularity of $\bar{\rho}$. For that we have to put ourselves in “favorable conditions” (Step 4).

In fact for a representation coming from a semistable $E/\mathbb{Q}$ we have stronger information. Namely, it is semistable at all primes. We shall discuss the strategy of the proof of Theorem 1 replacing (4) by

(4') $\rho$ is semistable at all primes
**Step 1.** Consider all \( \ell \)-adic representations lifting \( \bar{\rho} \) that are "likely to come" from modular forms.

Start with the mod \( \ell \) representation

\[
\bar{\rho} : G_{\mathbb{Q}} \longrightarrow \operatorname{GL}_2(k).
\]

Given a set of primes \( \Sigma \), one lets \( \text{Cond}(\Sigma) \) be a set of local conditions imposed on the restrictions of Galois representations

\[
\rho : G_{\mathbb{Q}} \longrightarrow \operatorname{GL}_2(R), \quad R \in \text{Ob}(\widehat{\mathcal{C}_O})
\]
lifting \( \bar{\rho} \), to decomposition groups of primes outside \( \Sigma \). The larger is \( \Sigma \) the smaller is \( \text{Cond}(\Sigma) \). Such representations are called of type \( \Sigma \).

Under "favorable conditions" there exists a universal representation of type \( \Sigma \)

\[
\rho_{\Sigma}^U : G_{\mathbb{Q}} \longrightarrow \operatorname{GL}_2(R_\Sigma).
\]

(\( R_\Sigma \) is an object of \( \widehat{\mathcal{C}_O} \) and is known to be generated by traces).

*When \( \Sigma \) is large enough, \( \rho_{E,\ell} \) is of type \( \Sigma \).*
More precisely:
In our situation (assuming “favorable conditions”) $\bar{\rho} = \bar{\rho}_{E,\ell}$ is a continuous, absolutely irreducible representation with determinant $\epsilon$ which is semistable at every prime.

Let $\Sigma$ be a set of unramified primes for $\bar{\rho}$, where $\ell$ may be contained in $\Sigma$ if $\bar{\rho}|_{G_\ell}$ is both BT and ordinary.

A continuous representation lifting $\bar{\rho}$

$$\rho : G_Q \longrightarrow \text{GL}_2(R), \quad R \in \text{Ob}(\widehat{\mathcal{C}_O})$$

is called of type $\Sigma$ if

1. $\rho$ is semistable at $\ell$, and BT at $\ell$ if $\ell \notin \Sigma$ and $\bar{\rho}$ is BT at $\ell$;
2. $\rho$ is minimally ramified at every prime $p \neq \ell$ outside $\Sigma$, meaning: $\rho$ is semistable at $p$ and unramified if at $p$ if $\bar{\rho}$ is.
3. $\det(\rho) = \epsilon$.

Under these conditions we have a lift

$$\rho^U_\Sigma : G_Q \longrightarrow \text{GL}_2(R_\Sigma),$$

which is universal in the following sense:

For every $\rho : G_Q \longrightarrow \text{GL}_2(R)$ of type $\Sigma$, there exists a unique homomorphism $\phi : R_\Sigma \longrightarrow R$ such that $\phi_*\rho^U_\Sigma \sim \rho$, where similarity is by matrices in $M_2(R)$ congruent to 1 modulo $m_R$. 
Furthermore, let $m_\Sigma$ be the maximal ideal of $R_\Sigma$. Then

$$(m_\Sigma/(\lambda, m_\Sigma^2))^* \cong H^1_\Sigma(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho}),$$

where $\text{ad}^0 \bar{\rho}$ is the adjoint representation on trace zero $2 \times 2$ matrices (given by conjugation), and where $H^1_\Sigma(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho})$ is the Selmer group defined by the local conditions:

- $H^1(G_{\mathbb{Q}}/I_p, (\text{ad}^0 \bar{\rho})_{I_p})$ for $p \notin \Sigma \cup \ell$.
- $H^1_\ell(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho})$ (resp. $H^1_{ss}(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho})$) for $\ell \notin \Sigma$ (resp. for $\ell \in \Sigma$). The local condition is built to keep the property of BT (resp. semistable).

$\Rightarrow$ $R_\Sigma$ is topologically generated over $\mathcal{O}$ by $\dim_k H^1_\Sigma(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho})$ elements. We also note that if $f : \text{Spec}(k) \longrightarrow \text{Spec}(R_\Sigma)$ is $\bar{\rho}$ then

$$m_\Sigma/(\lambda, m_\Sigma^2) = f^*\Omega_{R_\Sigma/\mathcal{O}}.$$

The representation $\text{ad}^0 \bar{\rho}(1)$ is Cartier dual to $\text{ad}^0 \bar{\rho}$. Say $\ell \notin \Sigma$. Using Poitou-Tate duality and the dual Selmer group $H^1_\Sigma(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho}(1))$ one obtains in the situation $\bar{\rho} = \bar{\rho}_{E,\ell}$ that $R_\Sigma$ is topologically generated over $\mathcal{O}$ by

$$\dim_k H^1_\Sigma(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho}(1)) + \sum_{p \in \Sigma} \dim_k H^0(G_{\mathbb{Q}}/I_p, \text{ad}^0 \bar{\rho}(1)).$$

Given $\phi : R_\Sigma \rightarrow \mathcal{O}$, let $\rho = \phi_*\rho_{\Sigma}^U$ and let $\varphi = \text{Ker}(\phi)$ then

$${\text{Hom}}(\varphi/\varphi^2, K/\mathcal{O}) \cong H^1_{\Sigma}(G_{\mathbb{Q}}, \text{ad}^0 \rho \otimes K/\mathcal{O}).$$

Let $f : \text{Spec}(\mathcal{O}) \longrightarrow \text{Spec}(R_\Sigma)$ the corresponding morphism then

$$\varphi/\varphi^2 \cong f^*\Omega_{R_{\Sigma}/\mathcal{O}} \cong \Omega_{R_{\Sigma}/\mathcal{O}} \otimes_{R_{\Sigma}} \mathcal{O}.$$

\footnote{If $\ell = 3$ one needs to assume that $\bar{\rho}|_{G_{\mathbb{Q}(\ell)}}$ is absolutely irreducible.}
Step 2. Consider all “correct” modular lifts.

Under “favorable conditions” one constructs out of Hecke algebras a ring $\mathbb{T}_\Sigma$ and a representation

$$\rho^M_\Sigma : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{T}_\Sigma)$$

whose specializations via $\mathbb{T}_\Sigma \rightarrow \mathcal{O}$ are all modular of a “correct” level. One obtains easily from the definition that $R_\Sigma \rightarrow \mathbb{T}_\Sigma$.

The main and crucial point is to prove that $R_\Sigma \rightarrow \mathbb{T}_\Sigma$ is an isomorphism.

This is a very delicate point, especially when working under relaxed hypotheses (even in Diamond’s case): We are asserting that the local conditions of semistability and minimal ramification that modular lifts of bounded conductor have characterize them among all Galois lifts.

Moral support: Langlands and Fontaine-Mazur conjectures: “all lifts are modular”.

Then (having proved $R_\Sigma \cong \mathbb{T}_\Sigma$), for a suitable $\Sigma$ the original representation $\rho_{E,\ell}$ is of type $\Sigma$ and hence obtained by pushing forward the universal representation $\rho^U_\Sigma$ via a homomorphism $R_\Sigma \rightarrow \mathcal{O}$, or what is the same (!), by pushing forward the representation $\rho^M_\Sigma$ via a homomorphism $\mathbb{T}_\Sigma \rightarrow \mathcal{O}$. It follows that $\rho_{E,\ell}$ is modular.
More precisely:

Let $\mathcal{N}_\Sigma$ denote the set of newforms $f$ such that

$$\rho_f : G_Q \longrightarrow \text{GL}_2(\mathcal{O}_f) \longrightarrow \text{GL}_2(\mathcal{O})$$

is a lifting of $\bar{\rho}$ of type $\Sigma$ and such that $\ell^2 \not| N_f$.

Equivalently, $\mathcal{N}_\Sigma$ is the set of newforms $f$ such that $\bar{\rho}_f \cong \bar{\rho}$, $\psi_f$ is trivial (i.e. $f$ is of level $\Gamma_0(N_f)$), and

$$N_f| N(\Sigma) \overset{\text{def}}{=} \ell^\delta N(\bar{\rho}) \prod_{p \in \Sigma \setminus \{\ell\}} p^2,$$

where $\delta = 0$ of $\bar{\rho}$ is BT and $\ell \not\in \Sigma$ and $\delta = 1$ otherwise. Thus, $\mathcal{N}_\Sigma$ is finite. By a fundamental theorem (Ribet+...), $\mathcal{N}_\Sigma \neq \emptyset$.

Consider the ring $\widetilde{T}_\Sigma = \prod_{f \in \mathcal{N}_\Sigma} \mathcal{O}$. For every $f \in \mathcal{N}_\Sigma$ we have a representation of type $\Sigma$

$$\rho_f : G_Q \longrightarrow \text{GL}_2(\mathcal{O}_f) \longrightarrow \text{GL}_2(\mathcal{O})$$

deduced from $f$, and hence a morphism $\phi_f : R_\Sigma \longrightarrow \mathcal{O}$ such that $\phi_f^* \rho_\Sigma^U = \rho_f$. In particular, for $p \nmid \ell \cdot N_f$ we have

$$\phi_f(\text{Tr} \rho_\Sigma^U(\text{Fr}_p)) = \text{Tr} \rho_f(\text{Fr}_p) = a_p(f).$$

We let $T_\Sigma$ be the subalgebra of $\widetilde{T}_\Sigma$ given by the image of the diagonal map $\prod_{f \in \mathcal{N}_\Sigma} \phi_f : R_\Sigma \longrightarrow \widetilde{T}_\Sigma$. It is generated as an $\mathcal{O}$-algebra by the elements $(a_p(f))_{f \in \mathcal{N}_\Sigma}$ for $p \nmid \ell \cdot N(\Sigma)$. Moreover, the resulting map $\phi_\Sigma : R_\Sigma \rightarrow T_\Sigma$ induces a representation

$$\rho_\Sigma^M : G_Q \longrightarrow \text{GL}_2(T_\Sigma)$$

with the property $\pi_f^* \rho_\Sigma^M = \rho_f$, where $\pi_f$ is the homomorphism induced from the projection $\widetilde{T}_\Sigma \longrightarrow \mathcal{O}$ on the ”$f$-component”.
Step 3. Proving that $R_\Sigma \longrightarrow T_\Sigma$ is an isomorphism.

The argument is divided into two parts:

(i) **Show that $R_\emptyset \longrightarrow T_\emptyset$ is an isomorphism**, using appropriate auxiliary sets of primes $Q$ and the relation

\[
\begin{array}{c}
R_Q \\ \downarrow \\
R_\emptyset \\
\end{array} \quad \begin{array}{c}
\rightarrow \\
\downarrow \\
\rightarrow \\
\end{array} \quad \begin{array}{c}
T_Q \\ \downarrow \\
T_\emptyset \\
\end{array}
\]

The vertical arrows are surjections and are easy to understand. One uses the $R_Q \rightarrow T_Q$ only as approximations. A key step in the original argument of T-W was to prove (after de Shalit) that for suitable sets $Q$, $T_Q$ is free over $\mathcal{O}[\Delta_Q]$, where $\Delta_Q = \prod_{q \in Q} \Delta_q$ and $\Delta_q$ is the $\ell$-part of $\mathbb{Z}/q\mathbb{Z}^\times$ (the action is coming from the diamond operators). This provided a sort of Iwasawa theory approach. A later simplification (Diamond) was that it is enough to find a non-zero $T_Q$ module, which is free over $\mathcal{O}[\Delta_Q]$.

(ii) Show the general case by using

\[
\begin{array}{c}
R_\Sigma \\ \downarrow \\
R_\emptyset \\
\end{array} \quad \begin{array}{c}
\rightarrow \\
\equiv \\
\rightarrow \\
\end{array} \quad \begin{array}{c}
T_\Sigma \\ \downarrow \\
T_\emptyset \\
\end{array}
\]

The vertical arrows are surjections and studied via Galois cohomology techniques. The numerical data:

- $\dim(m_\Sigma/(\lambda, m^2_\Sigma))^* = \dim H^1_\Sigma(G_\mathbb{Q}, \text{ad}^0 \bar{\rho})$
  \[= \dim_k H^1_\Sigma(G_\mathbb{Q}, \text{ad}^0 \bar{\rho}(1)) + \sum_{p \in \Sigma} \dim_k H^0(G_{\mathbb{Q}_p}, \text{ad}^0 \bar{\rho}(1)),\]
- $\text{Hom}(\mathcal{O}/\mathcal{O}^2, K/\mathcal{O}) \cong H^1_\Sigma(G_\mathbb{Q}, \text{ad}^0 \rho \otimes K/\mathcal{O})$,

together with its variation under increasing $\Sigma$ are the main tool. (One uses that length$_{\mathcal{O}}(\mathcal{O}/\mathcal{O}^2)$ is related to congruences between the newforms in $N_\Sigma$).
**Step 4.** Favorable conditions: show that we may get to a situation where for some odd prime \( \ell \) the residual representation \( \bar{\rho}_{E,\ell} \) is modular, semistable at all primes and absolutely irreducible when restricted to \( G_{Q(\ell)} \).

First one shows that under modularity and semistability at all primes, “irreducible” is equivalent to “absolutely irreducible when restricted to \( Q(\ell) \)”.

The rest has become a standard technique. One first tries \( \ell = 3 \). In case \( \bar{\rho}_{E,3} \) is irreducible, one uses Langlands-Tunnell to prove it is modular (\( \text{GL}_2(\mathbb{F}_3) \) is solvable). Else, discarding finitely many cases (corresponding to rational points of the genus 1 curve \( X_0(15) \), one concludes that for \( \ell = 5 \) the representation \( \bar{\rho}_{E,5} \) is irreducible. Next, one argues that there exists an auxiliary elliptic curve \( J/Q \) that is semistable, \( \bar{\rho}_{E,5} \cong \bar{\rho}_{J,5} \) and \( \bar{\rho}_{J,3} \) is irreducible.

Then:

\[
\begin{align*}
\rho_{J,3} \text{ is modular} & \quad \Rightarrow \quad \rho_{J,5} \text{ is modular} \\
& \quad \Rightarrow \quad \bar{\rho}_{J,5} \text{ is modular} \\
& \quad \Rightarrow \quad \bar{\rho}_{E,5} \text{ is modular} \\
& \quad \Rightarrow \quad \rho_{E,5} \text{ is modular!}
\end{align*}
\]
Summary of Strategy

**Step 0.** Prove the $\ell$-adic representation $\rho_{E,\ell} : G_\mathbb{Q} \to \text{GL}_2(\mathbb{Z}_\ell)$ is modular for some prime $\ell$.

**Step 1.** Consider all $\ell$-adic representations lifting the residual representation $\bar{\rho}_{E,\ell} : G_\mathbb{Q} \to \text{GL}_2(k)$ and satisfying some local conditions $\text{Cond}(\Sigma)$ (det, semi-stability) inspired by modularity. Get a universal lifting $\rho_{\Sigma}^U : G_\mathbb{Q} \to \text{GL}_2(R_\Sigma)$.

**Step 2.** Consider all newforms of suitably bounded level and character that lift $\bar{\rho}_{E,\ell}$ and patch the modular representations into one modular representation $\rho_{\Sigma}^M : G_\mathbb{Q} \to \text{GL}_2(T_\Sigma)$.

**Step 3.** Show that the surjection $R_\Sigma \to T_\Sigma$ is an isomorphism by first showing that for $\Sigma = \emptyset$ using suitable sets of primes $Q$, and conclude the general case studying the vertical variation in

$$
\begin{array}{ccc}
R_\Sigma & \to & T_\Sigma \\
\downarrow & & \downarrow \\
R_\emptyset & \cong & T_\emptyset
\end{array}
$$

using numerical invariants coming from congruences and Galois cohomology calculations.

**Step 4.** Using 3–5 tricks and Langlands-Tunnell (*Oh! How lucky we are!*) show that one may assume “favorable conditions”.
A Motivating Comment

Theorem 2. (Diamond) Let

\[ \rho : G_\mathbb{Q} \rightarrow \text{GL}_2(\mathcal{O}) \]

be an odd continuous representation such that:

1. \( \bar{\rho} \) is modular and \( \bar{\rho}|_{G_{\mathbb{Q}(\mathbb{C})}} \) is absolutely irreducible.
2. \( \rho \) is semistable at \( \ell \).
3. \( \rho \) is ramified at finitely many primes.

Then \( \rho \) is modular.

This is Theorem 1 without the assumption

\[
\text{For } p \equiv -1 \pmod{\ell}, \quad \bar{\rho}|_{I_p} \text{ reducible} \Rightarrow \bar{\rho}|_{G_p} \text{ reducible}
\]

I.e., “vexing primes” congruent to \(-1 \pmod{\ell}\) are now allowed.

The problem is to find the right notion of *minimally ramified* and to match it on the Hecke side. If one “ignores” the problem then the identification

\[ (m_\Sigma/(\lambda, m_\Sigma^2))^* \cong H^1_{\Sigma}(G_{\mathbb{Q}}, \text{ad}^0 \bar{\rho}), \]

is no longer true. One needs to impose local conditions at the vexing primes. The problem is this: At a vexing prime

\[ \bar{\rho} = \text{Ind}_{G_{p^2}}^{G_\mathbb{Q}} \psi \]

for \( \psi : G_{Q_{p^2}} \rightarrow k^\times \) such that \( \psi^{\text{Fr}} \neq \psi \). It has conductor \( N(\psi)^2 \).

Let \( \hat{\psi} : G_{Q_{p^2}} \rightarrow \mathcal{O}^\times \) the composition with the Teichmüller lift.

The representations \[ \rho = \text{Ind}_{G_{p^2}}^{G_\mathbb{Q}} \mu \hat{\psi}, \] with \( \mu : G_{Q_{p^2}} \rightarrow \mathcal{O}^\times \) a character of order \( \ell \) (they exist!), are lifts of conductor \( N(\psi)^2 \) that cannot be detected by “change in the level”. Diamond requires that if \( \rho \) lifts \( \bar{\rho} \) then \( \rho|_{I_\ell} \) is the Teichmüller lift of \( \bar{\rho}|_{I_\ell} \).

**Lesson:** In the non semistable case, finer conditions must be imposed both at the modular and the Galois deformation side such that the strategy we’ve discussed go through. Namely, the matching of \( R_\Sigma \) and \( T_\Sigma \).
Theorem 3. (C. Breuil, B. Conrad, F. Diamond, R. Taylor) Let
\[ \rho : G_{\mathbb{Q}} \rightarrow \text{GL}_2(K) \]
be an odd continuous representation, ramified at only finitely many primes. Assume that its reduction
\[ \bar{\rho} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(k) \]
is modular and \( \bar{\rho}|_{G_{\mathbb{Q}(\zeta_\ell)}} \) is absolutely irreducible. Furthermore, suppose that:

1. \( \bar{\rho}|_{G_\ell} \) has centralizer consisting of scalars.
2. \( \rho|_{G_\ell} \) is potentially BT with \( \ell \)-type \( \tau \) (resp. with extended \( \ell \)-type \( \tau' \)).
3. \( \tau \) (resp. \( \tau' \)) admits \( \bar{\rho} \).
4. \( \tau \) (resp. \( \tau' \)) is weakly acceptable for \( \bar{\rho} \).

Then \( \rho \) is modular.

Theorem 4. (BCDT) Let \( \bar{\rho} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{F}_5) \) be an irreducible continuous representation with cyclotomic determinant, then \( \bar{\rho} \) is modular.

Goal:

1. Explain hypotheses (2)-(4) (they all relate to \( \rho|_{G_\ell} \));
2. Explain modified definition of deformation rings and Hecke rings appearing in the proof of Theorem 3;
3. Explain deduction of the Modularity Theorem.
Deduction of the Modularity Theorem.

Let $\rho_{E,\ell}$ be the $\ell$-adic representation arising from $E$, and $\bar{\rho}_{E,\ell}$ the mod $\ell$ representation. BCDT consider three cases:

1. $\bar{\rho}_{E,5}|_{G_{\mathbb{Q}(5 \mid \mathbb{Q})}}$ is irreducible.
2. $\bar{\rho}_{E,5}|_{G_{\mathbb{Q}(5 \mid \mathbb{Q})}}$ is reducible, but $\bar{\rho}_{E,3}|_{G_{\mathbb{Q}(3 \mid \mathbb{Q})}}$ is absolutely irreducible.
3. The remaining cases.

- The remaining cases occur for finitely many $j$-invariants and are shown to be modular by direct arguments. The argument consists of calculating the rational points on certain twisted modular curves (luckily, all posses an elliptic quotient).

- In cases (1), (2) one first shows that $\bar{\rho}_{E,\ell}$ is modular. In case (2) this is the Langlands-Tunnell Theorem. In case (1) this is Theorem 4. In both cases one gets that $\bar{\rho}_{E,\ell}$ is modular and, in fact, $E$ acquires a semistable reduction over a tamely ramified extension of $\mathbb{Q}_\ell$ ($\ell = 3$ or $5$). Then already by CDT one concludes that $\rho_{E,\ell}$ is modular.

---

3Collaboration with N. Elkies.
• It remains then to prove Theorem 4.
  
  First one twists the original mod 5 representation such that its behaviour at 3 is classified (6 cases: conductors $3^i$ for $0 \leq i \leq 5$). Next, according to each case, one shows the existence of an auxiliary elliptic curve $J/\mathbb{Q}$ whose mod 5 representation is $\bar{\rho}$ and having a mod 3 representation which is surjective and whose restriction to inertia at 3 is of a specific nature depending on the case. Then a vexing case-by-case study shows that one can apply Theorem 3 and conclude that $\rho_{J,3}$ is modular. Hence $\rho_{J,5}$ is modular and so is $\bar{\rho}_{J,5} \sim \bar{\rho}$.

• Regarding the conditions of Theorem 3: Note that the modularity of $\bar{\rho}_{J,3}$ is given by Langlands-Tunnell. What remains is a very difficult verification that indeed the assumptions (2)-(4) of Theorem 3 hold! Namely, that the type chosen for $\bar{\rho}_{J,3}$ in each of the cases above works. The conditions involving $\ell$-type are murderous!

  It is here that the results of Breuil (classification of $\ell$-torsion commutative finite flat group schemes over an $\ell$-adic base, with no restriction on ramification) are used.

---

4This extends a lemma of Manoharmayum.
The Notions of Theorem 3

Let $\rho : G_\ell \longrightarrow \text{GL}_2(K)$.

- We say $\rho$ is **potentially BT** if for some finite extension $F/\mathbb{Q}_\ell$ we have $\rho|_{G_F}$ is BT. I.e., $\rho|_{G_F}$ comes from an $\ell$-divisible group (this only depends on $\rho|_{I_\ell}$). Then $\rho$ is **potentially semistable** in the sense of Fontaine. There is therefore an associated representation

$$\text{WD}(\rho) : W_\ell \longrightarrow \text{GL}(D)$$

where $D$ is a certain two dimensional vector space over $\mathbb{Q}_\ell^{\text{alg}}$.

- An **extended $\ell$-type** $\tau'$ is an isomorphism class of two dimensional representations of the Weil group $W_\ell$ over $\mathbb{Q}_\ell^{\text{alg}}$. An **$\ell$-type** $\tau$ is a restriction of such $\tau'$ to $I_\ell$.

  Therefore, saying that a potentially BT representation $\rho$ is of a certain (extended) $\ell$-type makes sense.

- Let $\bar{\rho}$ be a residual representation of $G_\ell$ with trivial centralizer. Let $\tau$ be an $\ell$-type. A **lift** $\rho : G_\ell \longrightarrow \text{GL}_2(\mathcal{O})$

  is of **type** $\tau$ if:

  1. $\rho$ is potentially BT;
  2. WD($\rho$) is of type $\tau$;
  3. $\text{det}(\rho)/\epsilon$ is of finite order prime to $\ell$. 
Let $R$ be the universal deformation ring for representations of $G_\ell$ lifting $\bar{\rho}$. Given an $\ell$-type $\tau$ denote by
\[ R^\tau = R/ \bigcap_{p \text{ of type } \tau} p \quad (= 0 \text{ if no such } p). \]

(p of type $\tau$ means that $R/p$ is finite over $\mathcal{O}$ and the deduced representation $\rho$ on $R/p$ is of type $\tau$).

We say that $\tau$ is weakly acceptable for $\bar{\rho}$ if $R^\tau$ is topologically generated over $\mathcal{O}$ by one element lying in its maximal ideal. We say that $\tau$ is acceptable for $\bar{\rho}$ if $R^\tau$ is also non zero.

It remains to explain the notion “$\tau$ admits $\bar{\rho}$”. If $\bar{\rho}$ is modular, it means that there exists some modular lift of $\bar{\rho}$ of type $\tau$. Conjecturally (BCDT) it is the same as saying that $R^\tau \neq 0$. We leave it at that.
On the proof of Theorem 3

**Theorem 3** Let

\[ \rho : G_\mathbb{Q} \rightarrow \text{GL}_2(K) \]

be an odd continuous representation, ramified at only finitely many primes. Assume that its reduction \( \bar{\rho} : G_\mathbb{Q} \rightarrow \text{GL}_2(k) \) is modular and \( \bar{\rho}|_{G_{\mathbb{Q}(\ell)}^{\infty}} \) is absolutely irreducible. Furthermore, suppose that:

1. \( \bar{\rho}|_{G_{\ell}} \) has trivial centralizer,
2. \( \rho|_{G_{\ell}} \) is potentially BT with \( \ell \)-type \( \tau \), and
3. BCDT → stronger assumptions → CDT

\[ \begin{array}{c|c|c}
\tau \text{ admits } \bar{\rho} \text{ and is weakly acceptable for } \bar{\rho} & \tau \text{ is acceptable for } \bar{\rho} & \tau \text{ is strongly acceptable for } \bar{\rho} \\
\end{array} \]

Then \( \rho \) is modular.

**Remark:** The case of extended type is very similar.

**Step 1.** Let

\[ \bar{\rho} : G_\mathbb{Q} \rightarrow \text{GL}_2(k) \]

be an odd continuous representation with \( \bar{\rho}|_{G_{\mathbb{Q}(\ell)}^{\infty}} \) absolutely irreducible and with \( \text{End}_{k[G_\mathbb{Q}]}(\bar{\rho}) \) consisting of scalars. Let \( \tau \) be an \( \ell \)-type such that \( \tau \) admits \( \bar{\rho} \) and is weakly acceptable for \( \bar{\rho} \).

Consider all \( \ell \)-adic representations lifting \( \bar{\rho} \) and satisfying some local conditions Cond(\( \Sigma \)) inspired by modularity and imposed outside \( \Sigma \). Get a universal lifting \( \rho^U_{(\Sigma,\tau)} : G_\mathbb{Q} \rightarrow \text{GL}_2(R_{(\Sigma,\tau)}) \).
More precisely: Let \( \mathcal{C}_O \) be the category of local topological \( O \)-algebra \( A \) such that \( A \cong \varprojlim A/a \) – the limit being over all open ideals \( a \) such that \( A/a \) is Artinian.

Let \( \Sigma \) be a finite set of primes; \( \ell \not\in \Sigma \). Let \( M \) be a free \( A \) module of rank two. A deformation

\[
\rho : G_\mathbb{Q} \longrightarrow \text{GL}(M)
\]

is of type \((\Sigma, \tau)\) if:

- \( \rho|_{G_\ell} \) is weakly of type \( \tau \): meaning that the map \( R \longrightarrow A \) inducing \( \rho|_{G_\ell} \) factors through \( R^\tau \). (Recall that \( R \) is the universal \( G_\ell \)-deformation ring).
- If \( p \not\in \Sigma \cup \{\ell\} \) then:
  1. if the order of \( \bar{\rho}(I_p) \) is not \( \ell \) then \( \rho(I_p) \cong \bar{\rho}(I_p) \);
  2. if the order of \( \bar{\rho}(I_p) \) is \( \ell \), then \( M/M^I_p \) is free of rank 1 over \( A \).
- \( \det(\rho)/\epsilon \) has a finite order prime to \( \ell \).

One shows that there exists a universal deformation

\[
\rho_{U(\Sigma, \tau)}^U : G_\mathbb{Q} \longrightarrow \text{GL}_2(R(\Sigma, \tau))
\]

and moreover, \( R(\Sigma, \tau) \) is a local Noetherian complete \( O \)-algebra with residue field \( k \), and is generated by traces.

One may define a dual Selmer group \( H^1_{(\Sigma, \tau)}(G_\mathbb{Q}, \text{ad}^0 \bar{\rho}(1)) \) and obtain that \( R(\Sigma, \tau) \) is generated by

\[
\dim_k H^1_{(\Sigma, \tau)}(G_\mathbb{Q}, \text{ad}^0 \bar{\rho}(1)) + \sum_{p \in \Sigma} \dim_k H^0(G_{\mathbb{Q}p}, \text{ad}^0 \bar{\rho}(1)).
\]

5 elements,\(^5\) and similar information about “\( \varphi/\varphi^2 \) ”.

\(^5\)One uses that \( \tau \) is acceptable for \( \bar{\rho}|_{G_\ell} \).
Step 2. Assume that $\bar{\rho}$ is modular. Consider all newforms of suitably restricted local behaviour and character that lift $\bar{\rho}_{E,\ell}$ and patch the modular representations into one modular representation

$$\rho^M_{\Sigma} : G_{\mathbb{Q}} \longrightarrow \text{GL}_2(T_{\Sigma}).$$

One uses adelic language: the equivalence $\pi \leftrightarrow f_{\pi}$ between (i) cuspidal automorphic representations $\pi \cong \otimes_{v \leq \infty} \pi_v$ with $\pi_\infty$ discrete series with lowest weight 2 and (ii) weight 2 newforms; the local Langlands correspondence $\pi_p \leftrightarrow WD(\pi_p)$ between (i) irreducible admissible infinite-dimensional representations of $\text{GL}_2(\mathbb{Q}_p)$ defined over $\mathbb{Q}^{alg}$ (mod $\cong$), and (ii) continuous semisimple representations $W_{\mathbb{Q}_p} \longrightarrow \text{GL}_2(\mathbb{Q}_p^{alg})$ (mod $\cong$).

Recall the operators

$$T_p = \left[ \text{GL}_2(\mathbb{Z}_p) \left( \begin{array}{cc} p & 0 \\ 0 & 1 \end{array} \right) \text{GL}_2(\mathbb{Z}_p) \right], \quad S_p = \left[ \text{GL}_2(\mathbb{Z}_p) \left( \begin{array}{cc} p & 0 \\ 0 & p \end{array} \right) \text{GL}_2(\mathbb{Z}_p) \right].$$

They are the mirror of the operators $T_p$ and the diamond operator on the modular forms side. If $\pi_p$ is unramified then the modular representation $\rho_{f_{\pi}} : G_{\mathbb{Q}} \longrightarrow \text{GL}_2(\mathbb{Q}_p^{alg})$ is unramified at $p$ and

$$\text{Tr}(\rho_{f_{\pi}}(\text{Fr}_p)) = t_p, \quad \det(\rho_{f_{\pi}}(\text{Fr}_p)) = ps_p.$$

Let $\mathcal{N}_\Sigma$ to be the set of such $\pi$ such that $\rho_{f_{\pi}}$ is a deformation of $\bar{\rho}$ of type $(\Sigma, \tau)$. One proves that $\mathcal{N}_\Sigma$ is nonempty and finite

Let $S(\bar{\rho})$ be the set of primes consisting of $\ell$ and the ramified primes for $\bar{\rho}$. Let $T_{(\Sigma,\tau)}$ be the image of the homomorphism

$$\mathcal{O}[T_p, S_p : p \notin \Sigma \cup S(\bar{\rho})] \longrightarrow \prod_{\pi \in \mathcal{N}_\Sigma} \mathbb{Q}_\ell^{alg}, \quad (T_p \mapsto t_p, \ S_p \mapsto s_p).$$

$T_{(\Sigma,\tau)}$ is a finitely generated local complete Noetherian $\mathcal{O}$ algebra.
Step 3. Under the hypotheses:

\[ \bar{\rho} : G_Q \rightarrow \text{GL}_2(k) \]

continuous odd modular representation, \( \bar{\rho}|_{G_{Q(\ell)}} \) absolutely irreducible, \( \text{End}_{k[G_{\ell}]}(\bar{\rho}) \) consisting of scalars, and \( \tau \) an \( \ell \)-type such that \( \tau \) admits \( \bar{\rho} \) and is weakly acceptable for \( \bar{\rho} \), show that the surjection \( R(\Sigma, \tau) \rightarrow T(\Sigma, \tau) \) is an isomorphism.

First show that for \( \Sigma = \emptyset \) using suitable sets of primes \( Q \). The choice of \( Q \) and the algebra involved are as in the semistable case. In particular, one again produces a non-zero \( T_Q \)-module \( L_Q \) (defined for any set \( Q \), in fact), which is a free \( \mathcal{O}[\Delta_Q] \)-module, out of the first cohomology of a suitable modular curve.

Next, one concludes the general case by the same method of studying the vertical variation in

\[
\begin{align*}
R(\Sigma, \tau) & \rightarrow T(\Sigma, \tau) \\
\downarrow & \\
R(\emptyset, \tau) & \cong T(\emptyset, \tau)
\end{align*}
\]

The same module \( L_\Sigma \) intervenes. One uses the same sort of numerical invariants coming from congruences and Galois cohomology calculations.