Ribet’s Level-Lowering Theorem for Modular Representations

Ricky Magner

November 8, 2017
Overview

1. Galois Representations
2. Level-Lowering Theorems
3. Character Groups
4. Shimura Curves and Modular Curves
Outline for section 1

1. Galois Representations
2. Level-Lowering Theorems
3. Character Groups
4. Shimura Curves and Modular Curves
Let $\ell$ be an odd prime and let $\mathbb{F}$ be a finite field of characteristic $\ell$. Let $\mathbb{T} = \mathbb{T}_N$ be the Hecke algebra associated to $S(N) := S_2(\Gamma_0(N))$, the space of weight 2 cuspforms of level $\Gamma_0(N)$. 
Let $\ell$ be an odd prime and let $\mathbb{F}$ be a finite field of characteristic $\ell$. Let $\mathbb{T} = \mathbb{T}_N$ be the Hecke algebra associated to $S(N) := S_2(\Gamma_0(N))$, the space of weight 2 cuspforms of level $\Gamma_0(N)$.

We say that a (continuous) Galois representation $\rho : G_\mathbb{Q} \to GL_2(\mathbb{F})$ is modular of level $N$ if $\text{det} \circ \rho$ is the mod $\ell$ cyclotomic character, and there is a homomorphism $\omega : \mathbb{T} \to \overline{\mathbb{F}}$ such that

$$\text{tr}(\rho(\text{Frob}_p)) = \omega(T_p)$$

for almost all primes $p$. 

Ribet’s Level-Lowering Theorem for Modular Representations
Theorem (Deligne)

Let $f \in S(N)$ be a Hecke eigenform and let $E$ be the number field generated by its Hecke eigenvalues. Let $\ell$ be prime and pick $\lambda | \ell$ a place of $E$. Then there exists a representation $\rho_f : G_{\mathbb{Q}} \rightarrow GL_2(E_\lambda)$, unramified away from $\ell N$, such that

$$\text{tr}(\rho_f(Frob_p)) = a_p, \text{ and } \det(\rho_f(Frob_p)) = p$$

for all $p \nmid \ell N$. 

For example, if $f \in S(N)$ is a Hecke eigenform, then define $\omega : T \rightarrow F$ by $\omega(T_p f) = a_p \pmod{\ell}$ where $T_p f = a_p f$. Then the "reduction" of the representation $\rho_f$ constructed above is modular of level $N$ by our definition.
Theorem (Deligne)

Let \( f \in S(N) \) be a Hecke eigenform and let \( E \) be the number field generated by its Hecke eigenvalues. Let \( \ell \) be prime and pick \( \lambda \mid \ell \) a place of \( E \). Then there exists a representation \( \rho_f : G_\mathbb{Q} \rightarrow GL_2(E_\lambda) \), unramified away from \( \ell N \), such that

\[
\text{tr}(\rho_f(Frob_p)) = a_p, \quad \text{and } \det(\rho_f(Frob_p)) = p
\]

for all \( p \nmid \ell N \).

For example, if \( f \in S(N) \) is a Hecke eigenform, then define \( \omega : \mathbb{T} \rightarrow \overline{\mathbb{F}} \) by \( \omega(T_p) = a_p \) (“mod \( \ell \” \) ) where \( T_p f = a_p f \). Then the “reduction” of the representation \( \rho_f \) constructed above is modular of level \( N \) by our definition.
Outline for section 2

1. Galois Representations
2. Level-Lowering Theorems
3. Character Groups
4. Shimura Curves and Modular Curves
A condition on representations

Definition

Suppose $\rho : G_\mathbb{Q} \to GL_2(\mathbb{F})$ is a Galois representation. We say $\rho$ is finite at $p$ if there exists a finite flat $\mathbb{F}$-vector space scheme $H$ over $\mathbb{Z}_p$ such that the representation of $G_{\mathbb{Q}_p}$ arising from $H(\overline{\mathbb{Q}_p})$ is the restriction of $\rho$ to the decomposition group at $p$. For example, if $E/\mathbb{Q}$ is an elliptic curve, then $E[\ell]$ is finite at all primes $p \neq \ell$ such that $E$ has good reduction at $p$. 

Ricky Magner
Ribet’s Level-Lowering Theorem for Modular Representations
A condition on representations

**Definition**

Suppose \( \rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}) \) is a Galois representation. We say \( \rho \) is finite at \( p \) if there exists a finite flat \( \mathbb{F} \)-vector space scheme \( H \) over \( \mathbb{Z}_p \) such that the representation of \( G_{\mathbb{Q}_p} \) arising from \( H(\overline{\mathbb{Q}_p}) \) is the restriction of \( \rho \) to the decomposition group at \( p \).

- For example, if \( E/\mathbb{Q} \) is an elliptic curve, then \( E[\ell] \) is finite at all primes \( p \neq \ell \) such that \( E \) has good reduction at \( p \).
The Main Theorem

**Theorem (Ribet)**

Let $\rho : G_\mathbb{Q} \to GL_2(\mathbb{F})$ be an irreducible modular representation of level $M_p$, with $p \nmid M$ and $\ell = \text{char}(\mathbb{F})$. Assume $\rho$ is finite at $p$. Then $\rho$ is modular of level $M$ if at least one of the following hold:

(i) $\ell \nmid M$,

(ii) $p \not\equiv 1 \mod \ell$. 
To prove Ribet’s theorem, we need to define $\rho_m$ for $m \subset \mathbb{T} = \mathbb{T}_N$ a maximal ideal.

**Theorem**

Let $m \subset \mathbb{T}$ be a maximal ideal. Then there is a unique semisimple representation $\rho_m : G_{\mathbb{Q}} \to GL_2(\mathbb{T}/m)$ unramified away from $mN$ such that

$$tr(\rho_m(Frob_p)) = T_p \mod m,$$

and

$$det(\rho_m(Frob_p)) = p \mod m$$

for all primes $p$ away from $mN$. 
Sketch of the proof

Let $k = \mathbb{T}/m$, and $L$ be the space of weight 2 cuspforms whose $q$-expansions at the usual cusp at $\infty$ lie in $\mathbb{Z}[[q]]$. By carefully lifting $f$, we can apply Deligne's theorem to the corresponding eigenform to get $\rho_f =: \rho_m$, which satisfies the desired properties.
Let $k = \mathbb{T}/m$, and $\mathcal{L}$ be the space of weight 2 cuspforms whose $q$-expansions at the usual cusp at $\infty$ lie in $\mathbb{Z}[[q]]$.

The map $(\mathcal{L} \otimes k) \times (\mathbb{T} \otimes k) \to k$ by $(f, T) \mapsto (\text{the coefficient of } q \text{ in } f|_T)$ induces a map $\mathcal{L} \otimes k \to \text{hom}_\mathbb{Z}(\mathbb{T}, k)$. 

By carefully lifting $f$, we can apply Deligne’s theorem to the corresponding eigenform to get $\rho_f =: \rho_m$, which satisfies the desired properties.
Let $k = \mathbb{T}/\mathfrak{m}$, and $\mathcal{L}$ be the space of weight 2 cuspforms whose $q$-expansions at the usual cusp at $\infty$ lie in $\mathbb{Z}[[q]]$.

The map $(\mathcal{L} \otimes k) \times (\mathbb{T} \otimes k) \to k$ by $(f, T) \mapsto (\text{the coefficient of } q \text{ in } f|_T)$ induces a map $\mathcal{L} \otimes k \to \text{hom}_\mathbb{Z}(\mathbb{T}, k)$.

By a dimension argument, one can show this map is an isomorphism. Taking the canonical element on the right $\mathbb{T} \to \mathbb{T}/\mathfrak{m}$, we get $f \in \mathcal{L} \otimes k$ whose $q$-coefficients are $t_n = T_n \mod \mathfrak{m}$.

By carefully lifting $f$, we can apply Deligne's theorem to the corresponding eigenform to get $\rho_f =: \rho_m$, which satisfies the desired properties.
Sketch of the proof

- Let $k = \mathbb{T}/m$, and $\mathcal{L}$ be the space of weight 2 cuspforms whose $q$-expansions at the usual cusp at $\infty$ lie in $\mathbb{Z}[[q]]$.

- The map $(\mathcal{L} \otimes k) \times (\mathbb{T} \otimes k) \to k$ by $(f, T) \mapsto (\text{the coefficient of } q \text{ in } f|_T)$ induces a map $\mathcal{L} \otimes k \to \text{hom}_{\mathbb{Z}}(\mathbb{T}, k)$.

- By a dimension argument, one can show this map is an isomorphism. Taking the canonical element on the right $\mathbb{T} \to \mathbb{T}/m$, we get $f \in \mathcal{L} \otimes k$ whose $q$-coefficients are $t_n = T_n \mod m$.

- By carefully lifting $f$, we can apply Deligne’s theorem to the corresponding eigenform to get $\rho_f =: \rho_m$, which satisfies the desired properties.
Fix $M$ and $p \nmid M$ an odd prime. Let $T = T_{Mp}$, and $m \subset T$ a maximal ideal.

Mazur’s Level-Lowering Theorem

Theorem (Mazur)

Suppose $\rho_m$ is irreducible, $\ell = \text{char}(T/m)$ is odd, and $\rho_m$ is finite at $p$. If also $p \not\equiv 1 \pmod{\ell}$, then $\rho_m$ is modular of level $M$. 
Fix $M$ and $p \nmid M$ an odd prime. Let $T = T_{Mp}$, and $m \subset T$ a maximal ideal.

**Theorem (Mazur)**

Suppose $\rho_m$ is irreducible, $\ell = \text{char}(T/m)$ is odd, and $\rho_m$ is finite at $p$. If also $p \not\equiv 1 \mod \ell$, then $\rho_m$ is modular of level $M$. 
Strategy for the Proof of Main Theorem

- Start with \( \rho_m \) of level \( Mp, p \nmid M \) with the assumptions in Ribet’s theorem. To show it is of level \( M \), we use three steps:
Strategy for the Proof of Main Theorem

- Start with $\rho_m$ of level $Mp$, $p \nmid M$ with the assumptions in Ribet’s theorem. To show it is of level $M$, we use three steps:
  1. **Raise the level** from $Mp$ to $Mpq$ for a convenient choice of odd prime $q \nmid Mp$.

\[ \begin{align*}
  &Mp 
  \quad \text{Raise Level} \quad \longrightarrow \\
  &\quad \text{Ribet} \quad \longrightarrow \\
  &Mq 
  \quad \text{Mazur} \quad \longrightarrow \\
  &M
\end{align*} \]
Strategy for the Proof of Main Theorem

- Start with \( \rho_m \) of level \( M_p \), \( p \nmid M \) with the assumptions in Ribet’s theorem. To show it is of level \( M \), we use three steps:
  
  1. **Raise the level** from \( M_p \) to \( M_{pq} \) for a convenient choice of odd prime \( q \nmid M_p \).
  2. **Lower the level** using Ribet’s main work to go from \( M_{pq} \) to \( M_q \).
Strategy for the Proof of Main Theorem

- Start with $\rho_m$ of level $Mp$, $p \nmid M$ with the assumptions in Ribet’s theorem. To show it is of level $M$, we use three steps:
  1. **Raise the level** from $Mp$ to $Mpq$ for a convenient choice of odd prime $q \nmid Mp$.
  2. **Lower the level** using Ribet’s main work to go from $Mpq$ to $Mq$.
  3. **Use Mazur’s theorem** to get rid of $q$ in the level to get level $M$.

![](image)
Strategy for the Proof of Main Theorem

- Start with $\rho_m$ of level $Mp$, $p \nmid M$ with the assumptions in Ribet’s theorem. To show it is of level $M$, we use three steps:
  1. **Raise the level** from $Mp$ to $Mpq$ for a convenient choice of odd prime $q \nmid Mp$.
  2. **Lower the level** using Ribet’s main work to go from $Mpq$ to $Mq$.
  3. **Use Mazur’s theorem** to get rid of $q$ in the level to get level $M$.

As a diagram:

$$
\begin{align*}
   \text{Mp} & \xrightarrow{\text{Raise Level}} \text{Mpq} & \xrightarrow{\text{Ribet}} \text{Mq} & \xrightarrow{\text{Mazur}} \text{M}
\end{align*}
$$
So what we need to show now is

**Theorem (Ribet)**

\[
\text{Suppose } \ell \nmid qM \text{ and } \rho_m \text{ (of level } Mpq) \text{ is finite at } p. \text{ Assume } q \not\equiv 1 \mod \ell. \text{ Then } \rho_m \text{ is modular of level } Mq.
\]

Note that by Mazur’s theorem, we can assume \( p \equiv 1 \mod \ell \), so in particular, \( \ell \nmid Mpq \).
Outline for section 3

1. Galois Representations
2. Level-Lowering Theorems
3. Character Groups
4. Shimura Curves and Modular Curves
Let $C$ be a curve over a $p$-adic field $K$. Let $C$ be the regular minimal model over $\mathcal{O}_K$. Write $C_k$ for the special fiber.
Let $C$ be a curve over a $p$-adic field $K$. Let $C$ be the regular minimal model over $\mathcal{O}_K$. Write $C_k$ for the special fiber.

Suppose the gcd of the multiplicity of the irreducible components of $C_k$ is 1 and all singular points of $C_k$ are ordinary double points (i.e. look like $xy = 0$ locally).

(These conditions will be satisfied in our applications.)
The normalization of $\mathcal{C}_k$ is the disjoint union of some nonsingular curves $D_j$ inducing a surjection

$$\text{Pic}^0(\mathcal{C}_k) \to \prod_j \text{Pic}^0(D_j)$$

whose kernel is a torus $T$. 

Define $X = X(T)$ to be the character group of $T$. We call this the character group associated to the reduction of $\mathcal{C}_k$. 

Ricky Magner  
Ribet’s Level-Lowering Theorem for Modular Representations
Character Groups Associated to Reductions

- The normalization of $\mathcal{C}_k$ is the disjoint union of some nonsingular curves $D_j$ inducing a surjection

$$\text{Pic}^0(\mathcal{C}_k) \to \prod_j \text{Pic}^0(D_j)$$

whose kernel is a torus $T$.

- Define $X = X(T)$ to be the character group of $T$. We call this the character group associated to the reduction of $C$. 
Outline for section 4

1. Galois Representations

2. Level-Lowering Theorems

3. Character Groups

4. Shimura Curves and Modular Curves
Let $M, p, q, \ell$ be as before.
Let $M, p, q, \ell$ be as before.

Let $C$ be the Shimura curve associated to the norm 1 units in a level $M$ Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant $pq$. 
From $\rho_m$ to Shimura Curves

- Let $M, p, q, \ell$ be as before.
- Let $C$ be the Shimura curve associated to the norm 1 units in a level $M$ Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant $pq$.
- Set $J = \text{Pic}^0(C)$ and let $W = J(\mathbb{Q})[m]$ be the group of elements of $J(\mathbb{Q})$ annihilated by $m \subset T$. In particular, if $\ell = \text{char}(T/m)$, then $W \subseteq J(\mathbb{Q})[\ell]$ as $G_{\mathbb{Q}}$-modules.
Let $M, p, q, \ell$ be as before.

Let $C$ be the Shimura curve associated to the norm 1 units in a level $M$ Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant $pq$.

Set $J = \text{Pic}^0(C)$ and let $W = J(\overline{\mathbb{Q}})[m]$ be the group of elements of $J(\overline{\mathbb{Q}})$ annihilated by $m \subset \mathbb{T}$. In particular, if $\ell = \text{char}(\mathbb{T}/m)$, then $W \subseteq J(\overline{\mathbb{Q}})[\ell]$ as $G_{\mathbb{Q}}$-modules.

If $V$ is the underlying vector space of $\rho_m$, one can show $V \hookrightarrow W$ as $\mathbb{T}/m[G_{\mathbb{Q}}]$-modules.
Let $M, p, q, \ell$ be as before.

Let $C$ be the Shimura curve associated to the norm 1 units in a level $M$ Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant $pq$.

Set $J = \text{Pic}^0(C)$ and let $W = J(\overline{\mathbb{Q}})[m]$ be the group of elements of $J(\overline{\mathbb{Q}})$ annihilated by $m \subset T$. In particular, if $\ell = \text{char}(T/m)$, then $W \subseteq J(\overline{\mathbb{Q}})[\ell]$ as $G_{\mathbb{Q}}$-modules.

If $V$ is the underlying vector space of $\rho_m$, one can show $V \hookrightarrow W$ as $T/m[G_{\mathbb{Q}}]$-modules.

As $V$ is finite at $p \neq \ell$, $V$ is unramified at $p$. Hence we can identify it with a subgroup of $J(\overline{\mathbb{F}}_p)$. 
Let $X$ be the character group associated to the reduction of $X_0(Mq) \mod q$, and $L$ the character group associated to the reduction of $X_0(Mpq) \mod q$. 
Let $X$ be the character group associated to the reduction of $X_0(Mq) \mod q$, and $L$ the character group associated to the reduction of $X_0(Mpq) \mod q$.

The natural degeneracy maps $X_0(Mpq) \to X_0(Mq)$ yield a map $L \to X \oplus X$, which is surjective. Let $Y$ be the kernel.
Let $Z$ be the character group associated to the reduction of the Shimura curve $C$ defined earlier mod $p$. Let $\Psi$ be the component group of $J$ mod $p$. 

Theorem

There is a Hecke-equivariant isomorphism $Z \cong \Psi$.

Combining this with some facts about the group $X$ associated to $X_0(Mq) \mod q$, we get

Theorem

There is an exact sequence of Hecke modules

$$0 \to K \to (X \oplus X)/\gamma(X \oplus X) \to \Psi \to C \to 0$$

for some groups $K$ and $C$, and $\gamma = (T_p)^{2-1} \in T_p$. 

Ricky Magner

Ribet’s Level-Lowering Theorem for Modular Representations
From Modular to Shimura Curves

Let $Z$ be the character group associated to the reduction of the Shimura curve $C$ defined earlier mod $p$. Let $\Psi$ be the component group of $J$ mod $p$.

**Theorem**

*There is a Hecke-equivariant isomorphism $Z \cong Y$.***
Let $Z$ be the character group associated to the reduction of the Shimura curve $C$ defined earlier mod $p$. Let $\Psi$ be the component group of $J$ mod $p$.

**Theorem**

There is a Hecke-equivariant isomorphism $Z \cong Y$.

Combining this with some facts about the group $X$ associated to $X_0(Mq)$ mod $q$, we get
From Modular to Shimura Curves

- Let $Z$ be the character group associated to the reduction of the Shimura curve $C$ defined earlier mod $p$. Let $\Psi$ be the component group of $J$ mod $p$.

**Theorem**

There is a Hecke-equivariant isomorphism $Z \cong Y$.

- Combining this with some facts about the group $X$ associated to $X_0(Mq)$ mod $q$, we get

**Theorem**

There is an exact sequence of Hecke modules

$$0 \to K \to (X \oplus X)/\gamma(X \oplus X) \to \Psi \to C \to 0$$

for some groups $K$ and $C$, and $\gamma = (T_p)^2 - 1 \in \mathbb{T}$.
The Proof in One Case

- If $V \subset J(\overline{\mathbb{F}_p})$ is not zero in $\Psi$, the component group of the reduction, then $\mathfrak{m}$ is in the support of $\Psi$. 
The Proof in One Case

- If $V \subset J(\overline{F}_p)$ is not zero in $\Psi$, the component group of the reduction, then $m$ is in the support of $\Psi$.
- By the earlier exact sequence, this implies $m$ lies in the support of $X \oplus X$ as a Hecke module.
If $V \subset J(\overline{\mathbb{F}_p})$ is not zero in $\Psi$, the component group of the reduction, then $\mathfrak{m}$ is in the support of $\Psi$.

By the earlier exact sequence, this implies $\mathfrak{m}$ lies in the support of $X \oplus X$ as a Hecke module.

But one can show that the action of $T$ on $X \oplus X$ is through the $p$-old quotient! Thus there exists a $\lambda \subset T_{Mq}$ such that $\rho_{\mathfrak{m}} \cong \rho_{\lambda}$, i.e. $\rho_{\mathfrak{m}}$ is of level $Mq$. 
If $V \subset J(\overline{\mathbb{F}_p})$ is not zero in $\Psi$, the component group of the reduction, then $m$ is in the support of $\Psi$.

By the earlier exact sequence, this implies $m$ lies in the support of $X \oplus X$ as a Hecke module.

But one can show that the action of $\mathbb{T}$ on $X \oplus X$ is through the $p$-old quotient! Thus there exists a $\lambda \subset \mathbb{T}_{Mq}$ such that $\rho_m \cong \rho_\lambda$, i.e. $\rho_m$ is of level $Mq$.

The case when $V$ is zero in $\Psi$ requires a few more facts....
If $V$ is zero in $\Psi$, then one shows that it must be contained in $\text{hom}(\mathbb{Z}/m\mathbb{Z}, \mu_\ell)$, so that $\dim \mathbb{Z}/m\mathbb{Z} \geq 2$ (as a $k = \mathbb{T}/m$ vector space).
The Second Case

- If $V$ is zero in $\Psi$, then one shows that it must be contained in $\text{hom}(\mathbb{Z}/m\mathbb{Z}, \mu_{\ell})$, so that $\dim \mathbb{Z}/m\mathbb{Z} \geq 2$ (as a $k = \mathbb{T}/m$ vector space).
- Using $Z \cong Y$, we get $\dim_k Y/mY \geq 2$. 

Ricky Magner
Ribet’s Level-Lowering Theorem for Modular Representations
The Second Case

- If $V$ is zero in $\Psi$, then one shows that it must be contained in $\text{hom}(Z/mZ, \mu_\ell)$, so that $\dim Z/mZ \geq 2$ (as a $k = \mathbb{T}/m$ vector space).
- Using $Z \cong Y$, we get $\dim_k Y/mY \geq 2$.
- Assume $m$ does not belong to the support of $X \oplus X$ (otherwise the previous argument finishes the proof). But then using

$$0 \to Y \to L \to X \to 0$$

we get $Y/mY \cong L/mL$, i.e. $\dim_k L/mL \geq 2$. 
The Second Case

- If $V$ is zero in $\Psi$, then one shows that it must be contained in $\text{hom}(\mathbb{Z}/m\mathbb{Z}, \mu_\ell)$, so that $\dim \mathbb{Z}/m\mathbb{Z} \geq 2$ (as a $k = \mathbb{T}/m$ vector space).

- Using $\mathbb{Z} \cong \mathbb{Y}$, we get $\dim_k \mathbb{Y}/m\mathbb{Y} \geq 2$.

- Assume $m$ does not belong to the support of $X \oplus X$ (otherwise the previous argument finishes the proof). But then using

$$0 \rightarrow \mathbb{Y} \rightarrow \mathbb{L} \rightarrow X \rightarrow 0$$

we get $\mathbb{Y}/m\mathbb{Y} \cong \mathbb{L}/m\mathbb{L}$, i.e. $\dim_k \mathbb{L}/m\mathbb{L} \geq 2$.

- But one can show that $\dim_k \mathbb{L}/m\mathbb{L} \leq 1$, so we have a contradiction and $m$ belongs to the support of $X \oplus X$. 

This finishes the proof of Ribet's theorem used in the step $M_{pq} \rightarrow M_{q}$. 

Ricky Magner

Ribet's Level-Lowering Theorem for Modular Representations
The Second Case

- If $V$ is zero in $\Psi$, then one shows that it must be contained in $\text{hom}(\mathbb{Z}/m\mathbb{Z}, \mu_\ell)$, so that $\dim \mathbb{Z}/m\mathbb{Z} \geq 2$ (as a $k = \mathbb{T}/m$ vector space).
- Using $Z \cong Y$, we get $\dim_k Y/mY \geq 2$.
- Assume $m$ does not belong to the support of $X \oplus X$ (otherwise the previous argument finishes the proof). But then using

$$0 \to Y \to L \to X \to 0$$

we get $Y/mY \cong L/mL$, i.e. $\dim_k L/mL \geq 2$.
- But one can show that $\dim_k L/mL \leq 1$, so we have a contradiction and $m$ belongs to the support of $X \oplus X$.
- This finishes the proof of Ribet’s theorem used in the step $Mpq \to Mq$. 