On the modularity of reducible Galois representations

Joint work (in progress) with Ricardo Menares

Nicolas Billerey

Laboratoire de mathématiques Blaise Pascal
Université Clermont Auvergne

Representation theory XVIII – Dubrovnik
June 2023

Table of contents

First example

- Let $E = X_1(11)$ be the elliptic curve of conductor 11 defined by $y^2 + y = x^3 - x^2$.
- The curve E has a rational point of order 5. For every prime number $p \neq 11$, we have

$$a_p(E) = 1 + p - \left|\widetilde{E}(\mathbf{F}_p)\right| \equiv 1 + p \pmod{5}.$$

- The curve E is modular (Eichler) : there exists a newform

$$f_E(z) = \sum_{n \geq 1} a_n q^n = q - 2q^2 + 2q^3 + \cdots \in \mathbf{Z}[\![q]\!] \quad (z \in \mathfrak{H},\ q = e^{2\pi i z})$$

of weight 2 and level $\Gamma_0(11)$ such that $a_n(E) = a_n$ for every $n \geq 1$.
- Therefore, for every prime number $p \neq 11$, we have

$$a_p \equiv 1 + p \pmod{5}.$$

Second example

- Let

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n \in \mathbf{Z}[\![q]\!] \quad (z \in \mathfrak{H},\ q = e^{2\pi i z})$$

  be the unique newform of weight 12 and level 1.
- For every prime number p, we have the Ramanujan's congruence

$$\tau(p) \equiv 1 + p^{11} \pmod{691}.$$

Eisenstein primes

Definition

Let M, k be positive integers. A prime number l is an **Eisenstein prime** of weight k and level M if there exist a **newform**

$$f = \sum_{n \geq 1} a_n q^n \in \mathcal{S}_k^{\text{new}}(\Gamma_0(M))$$

and a prime ideal λ above l in $\overline{\mathbf{Q}}$ such for all but finitely many prime numbers p, we have

$$a_p \equiv 1 + p^{k-1} \pmod{\lambda}.$$

- $l = 5$ is an **Eisenstein prime** of weight 2 and level 11.
- $l = 691$ is an **Eisenstein prime** of weight 12 and level 1.

What are the Eisenstein primes ? What are they good for ?

Definition

- Let $\overline{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$.
- For a prime number l, let $\overline{\mathbf{F}}_l$ be an algebraic closure of $\mathbf{F}_l = \mathbf{Z}/l\mathbf{Z}$.
- We equip $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ with the profinite topology and $\mathrm{GL}_2(\overline{\mathbf{F}}_l)$ with the discrete topology.

Definition

A (mod l) **Galois representation** is a continuous group homomorphism
$$\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l).$$

- With this definition, Galois representations always factors through Galois groups of finite extensions of $\mathbf{Q}$ and hence they have **finite** image.

Examples of Galois representations

- $\nu_i \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ $(i = 1, 2)$ Galois characters $\rightsquigarrow \rho = \nu_1 \oplus \nu_2$
- (Deligne) Let $f = \sum_{n \geq 1} a_n q^n$ be a **newform** of weight $k \geq 2$, level $N \geq 1$ and Nebentypus character ϵ. Fix a place over l in $\overline{\mathbf{Q}}$ (viewed as a subfield of $\mathbf{C}$). Up to isomorphism, there is a unique **semisimple** mod l Galois representation

$$\rho_{f,l} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$$

satisfying the following property : It is unramified outside Nl and for every prime $p \nmid Nl$, the characteristic polynomial of $\rho_{f,l}(\mathrm{Frob}_p)$ is the reduction of

$$X^2 - a_p X + \epsilon(p) p^{k-1}.$$

Here Frob_p denotes a Frobenius element at p in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Serre's weight, level and character

Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ be a Galois representation.

- The **weight** $k(\rho)$ of ρ
  - is an integer in the range $2, \ldots, l^2 - 1$;
  - only depends on the restriction of ρ to an inertia subgroup at l.
- The **level** $N(\rho)$ of ρ
  - is the prime-to-l part of the Artin conductor of ρ ;
  - controls the ramification of ρ away from l.
- The **character** $\epsilon(\rho) : (\mathbf{Z}/N(\rho)\mathbf{Z})^\times \to \overline{\mathbf{F}}_l^\times$ of ρ
  - satisfies $\det(\rho) = \epsilon(\rho)\chi_l^{k(\rho)-1}$, where χ_l denotes the mod l cyclotomic character ;
  - is identified with its unique lift $(\mathbf{Z}/N(\rho)\mathbf{Z})^\times \to \mathbf{C}^\times$ (w.r.t. a given place above l in $\overline{\mathbf{Q}} \subset \mathbf{C}$) with values in the roots of unity of prime-to-l order.

Modular Galois representations

Definition

A mod l Galois representation $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ is **modular** if there exist a newform f and a place of $\overline{\mathbf{Q}}$ above l such that

$$\rho \simeq \rho_{f,l}.$$

In that case, we also say that ρ **arises** from f.

Every modular Galois representation ρ is **semisimple** and **odd** (i.e. $\det \rho(c.c.) = -1$).

Serre's modularity conjecture (Khare–Wintenberger, 2005)

Let $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ be **odd** and **irreducible**.

- (Weak form) The representation ρ is modular.
- (Strong form) If $l \geq 5$, then ρ arises from f of the 'optimal' type $(N(\rho), k(\rho), \epsilon(\rho))$.

Non-optimal levels

Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ be a Galois representation.

- (Carayol, 1986) If ρ arises from a weight-$k(\rho)$ newform of level M, then $N(\rho) \mid M$.

Definition

A **non-optimal level** of ρ is an integer $M > N(\rho)$ such that ρ arises from a weight-$k(\rho)$ **newform** of level M.

- (Diamond–Taylor, 1994) Under the assumption $l > k(\rho) + 1$, **complete characterization** of the non-optimal levels for each **irreducible** ρ.

Reducible modular Galois representations

- It may happen that the mod l representation $\rho_{f,l}$ attached to a newform f is **reducible**.

Example

Let $f = f_E$ be the unique newform of weight 2 and level 11. Then the mod 5 representation of f is reducible and $\rho_{f,5} \simeq \mathbf{1} \oplus \chi_5$.

Example (Ramanujan, Serre–Swinnerton-Dyer)

The representation $\rho_{\Delta,l}$ is reducible if (and only if) $l \in \{2, 3, 5, 7, 691\}$. Moreover, $\rho_{\Delta,691} \simeq \mathbf{1} \oplus \chi_{691}^{11}$ thanks to the Ramanujan's congruence

$$\tau(p) \equiv 1 + p^{11} \pmod{691}, \quad \text{for } p \text{ prime.}$$

Modular reducible Galois representations

Ce sont des représentations irréductibles (sinon ce n'est pas très intéressant)...

J-P. Serre, letter to A. Grothendieck (december 31, 1986)

Let $\rho = \nu_1 \oplus \nu_2 \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ be an **odd (semisimple reducible)** Galois representation.

- (Weak modularity) Is ρ modular ?
- (Strong modularity) Is ρ modular of 'optimal' type ?
- (Non-optimal levels) What are the non-optimal levels of ρ ?

Weak modularity

Theorem 1 (B.–Menares, 2016)

Every odd mod l Galois representation $\rho = \nu_1 \oplus \nu_2$ is modular.

- First proof by Ghitza (2006) with completely different tools.

Example

The representation $\mathbf{1} \oplus \chi_5^3$ arises in weight 24 and level 1 (Ghitza) and in weight 4 and level $\Gamma_0(7)$ (B.–Menares).

Running assumptions and notation

- Let $\rho = \nu_1 \oplus \nu_2$ be a (reducible semisimple) mod l Galois representation. If $l > k(\rho) + 1$, then $\rho \simeq \epsilon_1 \oplus \epsilon_2 \chi_l^{k(\rho)-1}$ with ϵ_1, ϵ_2 characters unramified at l.
- Conversely, let k be an integer ≥ 2 such that $l > k + 1$ and let ϵ_1, ϵ_2 be characters unramified at l, then $\rho = \epsilon_1 \oplus \epsilon_2 \chi_l^{k-1}$ has weight $k(\rho) = k$.
- **From now on**, assume $\rho = \epsilon_1 \oplus \epsilon_2 \chi_l^{k-1}$ with
  - $k \geq 2$;
  - $l > k + 1$;
  - ϵ_1, ϵ_2 unramified at l, of conductors of ϵ_1, ϵ_2 respectively.
- We have $(N(\rho), k(\rho), \epsilon(\rho)) = (\mathfrak{c}_1\mathfrak{c}_2, k, \epsilon_1\epsilon_2)$. Set

$$\eta = \epsilon_1^{-1}\epsilon_2 \quad \text{and} \quad N = \mathfrak{c}_1\mathfrak{c}_2,$$

- Moreover, ρ is odd if and only if $(\epsilon_1\epsilon_2)(-1) = (-1)^k$.

Strong modularity

Definition

We say that a representation ρ is **strongly modular** if it arises from a newform of its optimal type $(N(\rho), k(\rho), \epsilon(\rho))$.

- A reducible ρ need not be strongly modular ! Counterex. : $\mathbf{1} \oplus \chi_l$.

Theorem 2 (B.–Menares, 2018)

Let $\rho = \epsilon_1 \oplus \epsilon_2 \chi_l^{k-1}$ be an odd mod l Galois representation as before. Then ρ is **strongly modular** if and only if $\frac{B_{k,\eta}}{2k} \prod_{p|N} (\eta(p)p^k - 1) = 0$,

where p runs through the prime divisors of N.
[Here $B_{k,\eta}$ is the k-th generalized mod l Bernoulli number associated with η.]

- Generalization to $N > 1$ of a result by Ribet (1975).

Refined non-optimal levels

- Restrict further to the **special case** $\rho = \mathbf{1} \oplus \chi_l^{k-1}$ with $k \geq 2$ even and $l > k+1$. Recall that $(N(\rho), k(\rho), \epsilon(\rho)) = (1, k, \mathbf{1})$.

Definition

A **refined non-optimal level** of $\rho = \mathbf{1} \oplus \chi_l^{k-1}$ is an integer $M > 1$ such that ρ arises in $\mathcal{S}_k^{\text{new}}(M, \mathbf{1}) = \mathcal{S}_k^{\text{new}}(\Gamma_0(M))$.

- Note that l is an **Eisenstein prime** of weight k and level $M > 1$ if and only if M is a **refined non-optimal level** of $\rho = \mathbf{1} \oplus \chi_l^{k-1}$.

$k \backslash M$	1 (optimal)	M prime
2	$\times\times\times\times\times\times\times\times\times\times\times\times\times\times$	$M \equiv 1 \pmod{l}$ (Mazur, 1977)
≥ 4	$l \mid \text{Num}\,(B_k)$ (Ribet, 1975) (or Theorem 2)	See next slide

Table – NSC for having a refined non-optimal level of $\mathbf{1} \oplus \chi_l^{k-1}$

Eisenstein primes in prime levels

Theorem 3 (B.–Menares, 2016)

Let $k \geq 4$ be an even integer and let l be a prime number such that $l > k+1$. Then, l is an Eisenstein prime of weight k and **prime** level $M \neq l$ if and only if the following assertions hold :

(1) l divides $(M^k - 1)(M^{k-2} - 1)$ and

(2) l divides $\frac{B_k}{2k}(M^k - 1)$.

- Different proofs of (refined versions of) this theorem by Gaba–Popa (2018) and by Kumar–Kumari–Moree–Singh (2021).

Example

- We have $691 \mid \mathrm{Num}(B_{12})$ and $691 \mid 89^{10} - 1$.
- Let $f = \sum_{n \geq 1} a_n q^n$ be a newform generating the 37-dimensional conjugacy class in $\mathcal{S}_{12}^{\mathrm{new}}(\Gamma_0(89))$.
- Its coefficient field is $\mathbf{Q}_f = \mathbf{Q}(a_2)$.
- Let λ be a place of $\overline{\mathbf{Q}}$ over the prime ideal in $\mathbf{Q}_f$ generated by 691 and $a_2 + 24$.
- We check that

$$a_p \equiv 1 + p^{11} \pmod{\lambda}, \quad \text{for every prime } p < 90.$$

- This **proves** that $\rho_{f,691} \simeq \mathbf{1} \oplus \chi_{691}^{11}$.
- It is possible to determine and certify such isomorphisms for higher weights/levels using Peaucelle's work and his PARI/GP code.

Application (statement)

For integers $k \geq 2$ and $M \geq 1$, set

$$d_k(M) = \max\left\{[\mathbf{Q}_f : \mathbf{Q}];\ f \text{ newform of weight } k \text{ and level } \Gamma_0(M)\right\}.$$

- Serre : $d_k(M) \to +\infty$ when $k + M \to +\infty$.

For $M \to \infty$ **prime** :

- Royer (2000), Murty–Sinha (2009) : $d_k(M) \gg_k \sqrt{\log\log M}$.
- Lipnowski–Schaeffer (2018, $k = 2$)
Bettin–Perret-Gentil–Radziwiłł (2019) $\Big\}$ $d_k(M) \gg_k \log\log(M)$.

Theorem 4 (B.–Menares, 2016)

Let $k \geq 2$ be a fixed even integer. There is an **explicit** set of primes $\mathcal{P}$ of natural lower density $\geq 3/4$ such that for every $M \in \mathcal{P}$ with $M \geq (k+1)^4$, we have

$$d_k(M) \geq c_k \log(M), \quad \text{with } c_k = \left(8\log\left(1 + 2^{(k-1)/2}\right)\right)^{-1}.$$

Application (proof)

- Let M be a (large enough) prime and let l be a prime divisor of $M-1$ such that $l > k+1$ (if it exists).
- Since $M-1 \mid M^k - 1$, there exist a newform $f = \sum_{n\geq 1} a_n q^n$ of weight k and level $\Gamma_0(M)$ and a prime ideal λ above l in its coefficient field $\mathbf{Q}_f$ such that

$$a_p \equiv 1 + p^{k-1} \pmod{\lambda}, \quad \text{for every prime } p \neq l, M.$$

- Taking $p = 2$, by Deligne's bounds, we have $a_2 \neq 1 + 2^{k-1}$ and

$$l \mid \mathrm{Norm}_{\mathbf{Q}_f/\mathbf{Q}} \left(a_2 - \left(1 + 2^{k-1}\right)\right) \leq \left(1 + 2^{(k-1)/2}\right)^{2[\mathbf{Q}_f:\mathbf{Q}]}.$$

  Hence $[\mathbf{Q}_f : \mathbf{Q}] \geq 4c_k \log l$.
- If $P(n)$ denotes the largest prime divisor of $n \geq 2$, apply this with

$$M \in \mathcal{P} = \left\{ N \text{ prime s.t. } P(N-1) > N^{1/4} \right\} \quad \text{and} \quad l = P(M-1).$$

Two primes in the level

- Here p, q, l are distinct primes with $l > k + 1$.

$k \backslash M$	p^2	pq
2	$p \equiv -1 \pmod{l}$ (Lang–Wake, 2022)	$p \equiv 1 \pmod{l}$ and 1) either $q \equiv 1 \pmod{l}$ 2) or q is an lth power mod p [or same with p, q swapped] (Ribet–Yoo, 2019)
≥ 4	? ? ? ? ? ? ? ? ? ? ? ? ? ? ?	See next slide

Table – Sufficient (and necessary) conditions for having a refined non-optimal level of $\mathbf{1} \oplus \chi_l^{k-1}$.

Lang–Wake's result above is crucial in their proof of the following.

.

Theorem (Lang–Wake, 2022)

Let p, l be prime numbers such that $l \geq 5$ and $p \equiv -1 \pmod{l}$. Then, l divides the class number of $\mathbf{Q}(p^{1/l})$.

Adding squarefree integers to the level

- Let $\rho = \epsilon_1 \oplus \epsilon_2 \chi_l^{k-1}$ be an odd mod l Galois representation as before. Recall : $\eta = \epsilon_1^{-1}\epsilon_2$ and $(N(\rho), k(\rho), \epsilon(\rho)) = (N, k, \epsilon_1\epsilon_2)$.

Conjecture

Let $r \geq 1$ be **squarefree** and **coprime to** Nl.

Assume $r = 1$ or $(N, k) \neq (1, 2)$.

The representation $\rho = \epsilon_1 \oplus \epsilon_2 \chi_l^{k-1}$ arises from a **newform** of weight k, level Nr which is $\Gamma_1(N) \cap \Gamma_0(r)$-invariant if and only if the following conditions hold :

(1) $(\eta(p)p^k - 1)(\eta(p)p^{k-2} - 1) = 0$ for every prime $p \mid r$;

(2) $\displaystyle \frac{B_{k,\eta}}{2k} \prod_{p \mid Nr} (\eta(p)p^k - 1) = 0$, where p runs through the prime divisors of Nr.

Eisenstein primes in squarefree levels

Conjecture (special case $N = 1$, that is $\rho = \mathbf{1} \oplus \chi_l^{k-1}$)

Let $k \geq 4$ be an even integer such that $l > k+1$ and let $r \geq 1$ be a **squarefree** integer such that $l \nmid r$.

Then l is an **Eisenstein prime** of weight k and level r if and only if the following conditions hold :

(1) l divides $(p^k - 1)(p^{k-2} - 1) = 0$ for every prime $p \mid r$;

(2) l divides $\dfrac{B_k}{2k} \prod_{p \mid r} (p^k - 1) = 0$, where p runs through the prime divisors of r.

Known results towards the conjecture

- $r = 1$ (and arbitrary $N \geq 1$) : Theorem 2 (B.–Menares, 2018) ;
- $N = 1$ and r prime : Theorem 3 (B.–Menares, 2016) ;
- $N = 1$ et r squarefree : partial (and/or conditional) results by Deo (2022).

Sample theorem (Deo, 2022)

Let $k \geq 4$ be an even integer and let $p_0, p_1, \ldots, p_k, l$ be distinct prime numbers such that $l > k + 1$. Assume the following assertions hold :

- $l \mid p_0^k - 1$, but $l \nmid p_0^2 - 1$;
- $l \mid p_i^{k-2} - 1$, but $l \nmid p_i - 1$, for all $1 \leq i \leq k$;
- $l \nmid B_k$.

Then, l is an Eisenstein prime of weight k and level $p_0 p_1 \cdots p_k$.

Forthcoming results

Theorem 5 (B.–Menares, 2023 ?)

The conjecture holds :

(a) for r prime (and arbitrary N) ;

(b) for r a product of **two** distinct prime numbers **and** $N > 1$.

- Part (a) is a straightforward generalization of Theorem 3.
- The proof of (b) is much more involved and follows Diamond–Taylor's approach for the irreducible case.
- Unfortunately it misses the determination of Eisenstein primes in levels that are product of two distinct primes...

Thank you for your attention !