Number theory via Representation theory

Eknath Ghate

November 9, 2014

Eightieth Annual Meeting, Chennai
Indian Academy of Sciences[1]

[1] This is a non-technical 20 minute talk intended for a general Academy audience.

Galois group of $\mathbb{Q}$ and its Representations

The Galois group of $\mathbb{Q}$ is the group of all automorphisms σ of $\bar{\mathbb{Q}}$ which fix $\mathbb{Q}$.

Galois group of $\mathbb{Q}$ and its Representations

The Galois group of $\mathbb{Q}$ is the group of all automorphisms σ of $\bar{\mathbb{Q}}$ which fix $\mathbb{Q}$. Denote it by:

$$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

Galois group of $\mathbb{Q}$ and its Representations

The Galois group of $\mathbb{Q}$ is the group of all automorphisms σ of $\bar{\mathbb{Q}}$ which fix $\mathbb{Q}$. Denote it by:

$$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

N.B. If α is a root of a polynomial with coefficients in $\mathbb{Q}$ and $\sigma \in G$, then $\sigma(\alpha)$ must also be a root of this polynomial.

E.g., $\sigma(\sqrt{2}) = \sqrt{2}$ or -$\sqrt{2}$, since these are the roots of $x^2 = 2$.

Galois group of $\mathbb{Q}$ and its Representations

The Galois group of $\mathbb{Q}$ is the group of all automorphisms σ of $\bar{\mathbb{Q}}$ which fix $\mathbb{Q}$. Denote it by:

$$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

N.B. If α is a root of a polynomial with coefficients in $\mathbb{Q}$ and $\sigma \in G$, then $\sigma(\alpha)$ must also be a root of this polynomial.

E.g., $\sigma(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$, since these are the roots of $x^2 = 2$.

The group G is huge and is understood via its representations:

$$\rho : G \to \mathrm{GL}_n(A),$$

where $n \geq 1$ and A is a (topological) ring.

The maps ρ are called **Galois representations.**

Modular forms

A large class of Galois representations arises from **modular forms**. These are complex valued functions f with many symmetries.

Modular forms

A large class of Galois representations arises from **modular forms**. These are complex valued functions f with many symmetries. Each f has a q-expansion

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

where $q = e^{2\pi i z}$, with z in the complex upper half plane.

Modular forms have a **weight** $k \geq 2$ and a **level** $N \geq 1$.

Modular forms

A large class of Galois representations arises from **modular forms**. These are complex valued functions f with many symmetries. Each f has a q-expansion

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

where $q = e^{2\pi iz}$, with z in the complex upper half plane.

Modular forms have a **weight** $k \geq 2$ and a **level** $N \geq 1$.

For each (nice) modular form f of weight $k \geq 2$ and each prime p there is a (2-dimensional) Galois representation:

$$\rho_f : G \to \mathrm{GL}_2(A)$$

where A is a p-adic ring (like $\mathbb{Z}_p$).

Delta function

The first example of a modular form f is Ramanujan's **Delta function** of weight $k = 12$ and level $N = 1$.

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

Delta function

The first example of a modular form f is Ramanujan's **Delta function** of weight $k = 12$ and level $N = 1$.

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

The numbers $\tau(n) \in \mathbb{Z}$ were studied by Ramanujan.

Delta function

The first example of a modular form f is Ramanujan's **Delta function** of weight $k = 12$ and level $N = 1$.

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

The numbers $\tau(n) \in \mathbb{Z}$ were studied by Ramanujan.

Question: Does $p|\tau(p)$, if p is a prime number?

Delta function

The first example of a modular form f is Ramanujan's **Delta function** of weight $k = 12$ and level $N = 1$.

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

The numbers $\tau(n) \in \mathbb{Z}$ were studied by Ramanujan.

Question: Does $p|\tau(p)$, if p is a prime number?

Answer: Not very often, but probably infinitely often:

- $2^3|\tau(2) = -24, \quad 3^2|\tau(3) = 252, \quad 5|\tau(5) \quad$ and $7|\tau(7)$.
- $p \nmid \tau(p)$, for $11 \leq p < 10^6$, except for $p = 2,411$.
- $p|\tau(p)$ again, for $p = 7,758,337,633$ (found in 2010).

Reduction of ρ_f

Given ρ_f, one can talk about its **reduction**:

$$\bar{\rho}_f : G \to \mathrm{GL}_2(\mathbb{F})$$

where $\mathbb{F}$ is a finite field (like $\mathbb{F}_p$), the residue field of A.

Reduction of ρ_f

Given ρ_f, one can talk about its **reduction**:

$$\bar{\rho}_f : G \to \mathrm{GL}_2(\mathbb{F})$$

where $\mathbb{F}$ is a finite field (like $\mathbb{F}_p$), the residue field of A.

The image of the reduction $\bar{\rho}_f$ is reasonably well understood. In general, the image of $\bar{\rho}_f$ is of **four types**.

Reduction of ρ_f

Given ρ_f, one can talk about its **reduction**:

$$\bar{\rho}_f : G \to \mathrm{GL}_2(\mathbb{F})$$

where $\mathbb{F}$ is a finite field (like $\mathbb{F}_p$), the residue field of A.

The image of the reduction $\bar{\rho}_f$ is reasonably well understood. In general, the image of $\bar{\rho}_f$ is of **four types**.

E.g., These days Ramanujan's congruence

$$\tau(\ell) \equiv 1 + \ell^{11} \mod 691,$$

for all primes $\ell \neq 691$, is explained by saying that the image of $\bar{\rho}_\Delta$ lies in the upper triangular matrices, for $p = 691$.

Local Galois representations

Let $I_p \subset G$ be the **inertia subgroup** of G at p.

Local Galois representations

Let $I_p \subset G$ be the **inertia subgroup** of G at p.

One may restrict ρ_f to I_p to obtain a **local Galois representation**

$$\rho : I_p \to \mathrm{GL}_2(A).$$

Local Galois representations

Let $I_p \subset G$ be the **inertia subgroup** of G at p.

One may restrict ρ_f to I_p to obtain a **local Galois representation**

$$\rho : I_p \to \mathrm{GL}_2(A).$$

N.B. One can also restrict to the bigger **decomposition subgroup** at p.

Local Galois representations

Let $I_p \subset G$ be the **inertia subgroup** of G at p.

One may restrict ρ_f to I_p to obtain a **local Galois representation**

$$\rho : I_p \to \mathrm{GL}_2(A).$$

N.B. One can also restrict to the bigger **decomposition subgroup** at p.

Goal: Describe the (semisimplifications of the) reductions

$$\bar{\rho} : I_p \to \mathrm{GL}_2(\mathbb{F})$$

of the local Galois representations ρ, for **good** primes p.

Here 'good' means that $p \nmid N$.

Fundamental characters

Let $\omega = \omega_1$ and ω_2 be the **fundamental characters** of I_p of level 1 and 2.

Fundamental characters

Let $\omega = \omega_1$ and ω_2 be the **fundamental characters** of I_p of level 1 and 2. These are homomorphisms

$$I_p \to \mathbb{F}^*$$

of order $p-1$ and p^2-1 respectively.

Fundamental characters

Let $\omega = \omega_1$ and ω_2 be the **fundamental characters** of I_p of level 1 and 2. These are homomorphisms

$$I_p \to \mathbb{F}^*$$

of order $p-1$ and p^2-1 respectively.

It turns that there are only **two possibilities** for the reduction $\bar{\rho}$, up to a twist.

Fundamental characters

Let $\omega = \omega_1$ and ω_2 be the **fundamental characters** of I_p of level 1 and 2. These are homomorphisms

$$I_p \to \mathbb{F}^*$$

of order $p-1$ and p^2-1 respectively.

It turns that there are only **two possibilities** for the reduction $\bar{\rho}$, up to a twist. We have:

1. $$\bar{\rho} = \begin{pmatrix} \omega^a & * \\ 0 & 1 \end{pmatrix},$$

Fundamental characters

Let $\omega = \omega_1$ and ω_2 be the **fundamental characters** of I_p of level 1 and 2. These are homomorphisms

$$I_p \to \mathbb{F}^*$$

of order $p-1$ and p^2-1 respectively.

It turns that there are only **two possibilities** for the reduction $\bar{\rho}$, up to a twist. We have:

1. $$\bar{\rho} = \begin{pmatrix} \omega^a & * \\ 0 & 1 \end{pmatrix},$$

2. $$\bar{\rho} = \begin{pmatrix} \omega_2^b & 0 \\ 0 & \omega_2^{bp} \end{pmatrix},$$

for some integers $0 \leq a \leq p-2$, $0 \leq b \leq p^2-2$ ($p+1 \nmid b$).

Fundamental characters

Let $\omega = \omega_1$ and ω_2 be the **fundamental characters** of I_p of level 1 and 2. These are homomorphisms

$$I_p \to \mathbb{F}^*$$

of order $p-1$ and p^2-1 respectively.

It turns that there are only **two possibilities** for the reduction $\bar{\rho}$, up to a twist. We have:

1. $$\bar{\rho} = \begin{pmatrix} \omega^a & * \\ 0 & 1 \end{pmatrix},$$

2. $$\bar{\rho} = \begin{pmatrix} \omega_2^b & 0 \\ 0 & \omega_2^{bp} \end{pmatrix},$$

for some integers $0 \leq a \leq p-2$, $0 \leq b \leq p^2-2$ ($p+1 \nmid b$).

Question: Which case occurs, and for what values of a, b?

What is known?

The answer depends on **two** quantities:

What is known?

The answer depends on **two** quantities:

1. The **weight** k of f, which is a positive integer ≥ 2.
2. The **slope** v of f, a positive (rational) number which (roughly) measures how divisible a_p is by p.

What is known?

The answer depends on **two** quantities:

1. The **weight** k of f, which is a positive integer ≥ 2.
2. The **slope** v of f, a positive (rational) number which (roughly) measures how divisible a_p is by p.

The answer is **known** if $v = 0$, or roughly if $p \nmid a_p$ (Deligne):

$$\bar{\rho} = \begin{pmatrix} \omega^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

What is known?

The answer depends on **two** quantities:

1. The **weight** k of f, which is a positive integer ≥ 2.
2. The **slope** v of f, a positive (rational) number which (roughly) measures how divisible a_p is by p.

The answer is **known** if $v = 0$, or roughly if $p \nmid a_p$ (Deligne):

$$\bar{\rho} = \begin{pmatrix} \omega^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

But if $v > 0$ (roughly $p | a_p$), then this question is notoriously difficult.

What is known?

The answer depends on **two** quantities:

1. The **weight** k of f, which is a positive integer ≥ 2.
2. The **slope** v of f, a positive (rational) number which (roughly) measures how divisible a_p is by p.

The answer is **known** if $v = 0$, or roughly if $p \nmid a_p$ (Deligne):

$$\bar{\rho} = \begin{pmatrix} \omega^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

But if $v > 0$ (roughly $p | a_p$), then this question is notoriously difficult. It is **known only** for

- **Small weights** $k \leq 2p + 1$ (Fontaine-Edixhoven, Breuil)

What is known?

The answer depends on **two** quantities:

1. The **weight** k of f, which is a positive integer ≥ 2.
2. The **slope** v of f, a positive (rational) number which (roughly) measures how divisible a_p is by p.

The answer is **known** if $v = 0$, or roughly if $p \nmid a_p$ (Deligne):

$$\bar{\rho} = \begin{pmatrix} \omega^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

But if $v > 0$ (roughly $p | a_p$), then this question is notoriously difficult. It is **known only** for

- **Small weights** $k \leq 2p + 1$ (Fontaine-Edixhoven, Breuil)
- **Small slopes** $0 < v < 1$ (Buzzard-Gee)

What is known?

The answer depends on **two** quantities:

1. The **weight** k of f, which is a positive integer ≥ 2.
2. The **slope** v of f, a positive (rational) number which (roughly) measures how divisible a_p is by p.

The answer is **known** if $v = 0$, or roughly if $p \nmid a_p$ (Deligne):

$$\bar{\rho} = \begin{pmatrix} \omega^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

But if $v > 0$ (roughly $p|a_p$), then this question is notoriously difficult. It is **known only** for

- **Small weights** $k \leq 2p + 1$ (Fontaine-Edixhoven, Breuil)
- **Small slopes** $0 < v < 1$ (Buzzard-Gee)
- **Large slopes** $v > \lfloor \frac{k-2}{p-1} \rfloor$ (Berger-Li-Zhu).

Delta revisited

For the Delta function $f = \Delta$ of weight $k = 12$ we have the following results (due to Serre & Swinnerton-Dyer for $p \leq 7$):

1. If $p \nmid \tau(p)$, then $v = 0$ and

$$\bar{\rho} = \begin{pmatrix} \omega^{11} & * \\ 0 & 1 \end{pmatrix}.$$

Delta revisited

For the Delta function $f = \Delta$ of weight $k = 12$ we have the following results (due to Serre & Swinnerton-Dyer for $p \leq 7$):

1. If $p \nmid \tau(p)$, then $v = 0$ and
$$\bar{\rho} = \begin{pmatrix} \omega^{11} & * \\ 0 & 1 \end{pmatrix}.$$

2. If $p = 2$, then $v = 3$ and $\bar{\rho}^{\mathrm{ss}}$ is trivial.

Delta revisited

For the Delta function $f = \Delta$ of weight $k = 12$ we have the following results (due to Serre & Swinnerton-Dyer for $p \leq 7$):

1. If $p \nmid \tau(p)$, then $v = 0$ and
$$\bar{\rho} = \begin{pmatrix} \omega^{11} & * \\ 0 & 1 \end{pmatrix}.$$
2. If $p = 2$, then $v = 3$ and $\bar{\rho}^{\mathrm{ss}}$ is trivial.
3. If $p = 3$, then $v = 2$, and
$$\bar{\rho}^{\mathrm{ss}} = \begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix}.$$

Delta revisited continued

4. If $p = 5$, then $v = 1$ and

$$\overline{\rho}^{\mathrm{SS}} = \begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix} \otimes \omega.$$

Delta revisited continued

4. If $p = 5$, then $v = 1$ and

$$\overline{\rho}^{\mathrm{ss}} = \begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix} \otimes \omega.$$

5. If $p = 7$, then $v = 1$ and

$$\overline{\rho}^{\mathrm{ss}} = \begin{pmatrix} \omega^3 & 0 \\ 0 & 1 \end{pmatrix} \otimes \omega.$$

Delta revisited continued

4. If $p = 5$, then $v = 1$ and

$$\overline{\rho}^{\mathrm{ss}} = \begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix} \otimes \omega.$$

5. If $p = 7$, then $v = 1$ and

$$\overline{\rho}^{\mathrm{ss}} = \begin{pmatrix} \omega^3 & 0 \\ 0 & 1 \end{pmatrix} \otimes \omega.$$

6. If $p \geq 11$, $v > 0$ (e.g., $p = 2,411$ or $7,758,337,633$), then

$$\overline{\rho} = \begin{pmatrix} \omega_2^{11} & 0 \\ 0 & \omega_2^{11p} \end{pmatrix}.$$

Delta revisited continued

4. If $p = 5$, then $v = 1$ and

$$\overline{\rho}^{\mathrm{ss}} = \begin{pmatrix} \omega & 0 \\ 0 & 1 \end{pmatrix} \otimes \omega.$$

5. If $p = 7$, then $v = 1$ and

$$\overline{\rho}^{\mathrm{ss}} = \begin{pmatrix} \omega^3 & 0 \\ 0 & 1 \end{pmatrix} \otimes \omega.$$

6. If $p \geq 11$, $v > 0$ (e.g., $p = 2,411$ or $7,758,337,633$), then

$$\bar{\rho} = \begin{pmatrix} \omega_2^{11} & 0 \\ 0 & \omega_2^{11p} \end{pmatrix}.$$

Thus, the local reduction $\bar{\rho}$ is known for all primes p.

What we do

Recall: $\bar{\rho}^{\mathrm{SS}}$ is known in general for $0 \leq v < 1$ and $k \geq 2$.

What we do

Recall: $\bar{\rho}^{\mathrm{SS}}$ is known in general for $0 \leq v < 1$ and $k \geq 2$.

In **two forthcoming papers**:

1. A. Ganguli and E. Ghate, *JNT* **147** (2015) 250–286.
2. S. Bhattacharya and E. Ghate, *Preprint* (2015), 42 pages.

What we do

Recall: $\bar{\rho}^{\mathrm{SS}}$ is known in general for $0 \leq v < 1$ and $k \geq 2$.

In **two forthcoming papers**:

1. A. Ganguli and E. Ghate, *JNT* **147** (2015) 250–286.
2. S. Bhattacharya and E. Ghate, *Preprint* (2015), 42 pages.

we tackle the **next range of slopes**

$$1 < v < 2$$

What we do

Recall: $\bar{\rho}^{\mathrm{ss}}$ is known in general for $0 \leq v < 1$ and $k \geq 2$.

In **two forthcoming papers**:

1. A. Ganguli and E. Ghate, *JNT* **147** (2015) 250–286.
2. S. Bhattacharya and E. Ghate, *Preprint* (2015), 42 pages.

we tackle the **next range of slopes**

$$1 < v < 2$$

for

1. weights $k \leq p^2 - p$

What we do

Recall: $\bar{\rho}^{\mathrm{ss}}$ is known in general for $0 \leq v < 1$ and $k \geq 2$.

In **two forthcoming papers**:

1. A. Ganguli and E. Ghate, *JNT* **147** (2015) 250–286.
2. S. Bhattacharya and E. Ghate, *Preprint* (2015), 42 pages.

we tackle the **next range of slopes**

$$1 < v < 2$$

for

1. weights $k \leq p^2 - p$
2. **all** weights $k \geq 2$, respectively (under a mild hypothesis).

What we do

Recall: $\bar{\rho}^{\mathrm{ss}}$ is known in general for $0 \leq v < 1$ and $k \geq 2$.

In **two forthcoming papers**:

1. A. Ganguli and E. Ghate, *JNT* **147** (2015) 250–286.
2. S. Bhattacharya and E. Ghate, *Preprint* (2015), 42 pages.

we tackle the **next range of slopes**

$$1 < v < 2$$

for

1. weights $k \leq p^2 - p$
2. **all** weights $k \geq 2$, respectively (under a mild hypothesis).

N.B. In a separate work we plan to treat the important case

$$v = 1$$

for **all** weights, generalizing for instance the result for $p = 5$ and $f = \Delta$ above to all forms f and all good primes $p \geq 5$.

How we do it

We use **Representation theory**.

How we do it

We use **Representation theory**. We make heavy use of the following result due to Breuil (and a p-adic analog due to Breuil, Berger, Colmez, Paškūnas).

How we do it

We use **Representation theory**. We make heavy use of the following result due to Breuil (and a p-adic analog due to Breuil, Berger, Colmez, Paškūnas).

Local Langlands Correspondence: To each local mod p Galois representations the LLC associates a smooth admissible mod p representations of $\mathrm{GL}_2(\mathbb{Q}_p)$.

How we do it

We use **Representation theory**. We make heavy use of the following result due to Breuil (and a p-adic analog due to Breuil, Berger, Colmez, Paškūnas).

Local Langlands Correspondence: To each local mod p Galois representations the LLC associates a smooth admissible mod p representations of $\mathrm{GL}_2(\mathbb{Q}_p)$.

It is known that the image of $\bar{\rho}$ under the LLC is the reduction $\bar{\Theta}_{k,a_p}$ of a **lattice** Θ_{k,a_p} in the $\mathrm{GL}_2(\mathbb{Q}_p)$-representation

$$\Pi_{k,a_p} = \frac{\mathrm{ind}_{\mathbb{Q}_p^\times \mathrm{GL}_2(\mathbb{Z}_p)}^{\mathrm{GL}_2(\mathbb{Q}_p)} \mathrm{Sym}^{k-2}\mathbb{Q}_p^2}{T - a_p}$$

where T is the **Hecke operator** at p.

How we do it

We use **Representation theory**. We make heavy use of the following result due to Breuil (and a p-adic analog due to Breuil, Berger, Colmez, Paškūnas).

Local Langlands Correspondence: To each local mod p Galois representations the LLC associates a smooth admissible mod p representations of $\mathrm{GL}_2(\mathbb{Q}_p)$.

It is known that the image of $\bar{\rho}$ under the LLC is the reduction $\bar{\Theta}_{k,a_p}$ of a **lattice** Θ_{k,a_p} in the $\mathrm{GL}_2(\mathbb{Q}_p)$-representation

$$\Pi_{k,a_p} = \frac{\mathrm{ind}_{\mathbb{Q}_p^\times \mathrm{GL}_2(\mathbb{Z}_p)}^{\mathrm{GL}_2(\mathbb{Q}_p)} \mathrm{Sym}^{k-2}\mathbb{Q}_p^2}{T - a_p}$$

where T is the **Hecke operator** at p.

It is also known that the LLC is 1 to 1 (but not onto).

How we do it

We use **Representation theory**. We make heavy use of the following result due to Breuil (and a p-adic analog due to Breuil, Berger, Colmez, Paškūnas).

Local Langlands Correspondence: To each local mod p Galois representations the LLC associates a smooth admissible mod p representations of $\mathrm{GL}_2(\mathbb{Q}_p)$.

It is known that the image of $\bar{\rho}$ under the LLC is the reduction $\bar{\Theta}_{k,a_p}$ of a **lattice** Θ_{k,a_p} in the $\mathrm{GL}_2(\mathbb{Q}_p)$-representation

$$\Pi_{k,a_p} = \frac{\mathrm{ind}_{\mathbb{Q}_p^\times \mathrm{GL}_2(\mathbb{Z}_p)}^{\mathrm{GL}_2(\mathbb{Q}_p)} \mathrm{Sym}^{k-2}\mathbb{Q}_p^2}{T - a_p}$$

where T is the **Hecke operator** at p.

It is also known that the LLC is 1 to 1 (but not onto).
So if one can compute $\bar{\Theta}_{k,a_p}^{\mathrm{ss}}$, then one can compute $\bar{\rho}^{\mathrm{ss}}$!

How we do it continued

One can compute $\bar{\Theta}^{\mathrm{SS}}_{k,a_p}$ when $1 < v < 2$, as follows:

How we do it continued

One can compute $\bar{\Theta}^{\mathrm{SS}}_{k,a_p}$ when $1 < v < 2$, as follows:

Let $r = k - 2 \geq 0$.

How we do it continued

One can compute $\bar{\Theta}^{\mathrm{ss}}_{k,a_p}$ when $1 < v < 2$, as follows:

Let $r = k - 2 \geq 0$.

Let V_r be the space of homogeneous polynomials of degree r in two variables X and Y over $\mathbb{F}_p$.

Let $\Gamma = \mathrm{GL}_2(\mathbb{F}_p)$.

Then V_r is a Γ-module in the usual way: if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, then

$$\gamma : (X, Y) \mapsto (aX + cY, bX + dY).$$

How we do it continued

One can compute $\bar{\Theta}^{\mathrm{ss}}_{k,a_p}$ when $1 < v < 2$, as follows:

Let $r = k - 2 \geq 0$.

Let V_r be the space of homogeneous polynomials of degree r in two variables X and Y over $\mathbb{F}_p$.

Let $\Gamma = \mathrm{GL}_2(\mathbb{F}_p)$.

Then V_r is a Γ-module in the usual way: if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, then

$$\gamma : (X, Y) \mapsto (aX + cY, bX + dY).$$

V_r is then also a $\mathbb{Q}_p^\times \mathrm{GL}_2(\mathbb{Z}_p)$-module via the projection $\mathrm{GL}_2(\mathbb{Z}_p) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_p)$ (and letting $p \in \mathbb{Q}_p^\times$ act trivially).

Two important submodules of V_r

Consider the two submodules of V_r defined by

1. $U =$ the submodule generated by $X^{r-1}Y$,

Two important submodules of V_r

Consider the two submodules of V_r defined by

1. $U =$ the submodule generated by $X^{r-1}Y$,
2. $W =$ the submodule consisting of all multiples of the polynomial $(X^pY - XY^p)^2$.

Two important submodules of V_r

Consider the two submodules of V_r defined by

1. $U =$ the submodule generated by $X^{r-1}Y$,
2. $W =$ the submodule consisting of all multiples of the polynomial $(X^pY - XY^p)^2$.

Let

$$Q = \frac{V_r}{U + W}$$

be the quotient.

Two important submodules of V_r

Consider the two submodules of V_r defined by

1. $U =$ the submodule generated by $X^{r-1}Y$,
2. $W =$ the submodule consisting of all multiples of the polynomial $(X^pY - XY^p)^2$.

Let

$$Q = \frac{V_r}{U + W}$$

be the quotient.

Buzzard-Gee: When $1 < v < 2$ and $r \geq 2p + 1$, there is a natural onto map

$$\mathrm{ind}_{\mathbb{Q}_p^\times \mathrm{GL}_2(\mathbb{Z}_p)}^{\mathrm{GL}_2(\mathbb{Q}_p)} Q \twoheadrightarrow \bar{\Theta}_{k,a_p}.$$

Computing the quotient Q

We show that **three** possibilities occur, with the second possibility being the most frequent:

Computing the quotient Q

We show that **three** possibilities occur, with the second possibility being the most frequent:

1. Q **is irreducible**, in which case we know $\bar{\Theta}^{\mathrm{SS}}_{k,a_p}$, up to separating out some reducible cases.

Computing the quotient Q

We show that **three** possibilities occur, with the second possibility being the most frequent:

1. Q **is irreducible**, in which case we know $\bar{\Theta}^{\mathrm{SS}}_{k,a_p}$, up to separating out some reducible cases.
2. Q **has 2 JH-factors**, in which case we do some delicate computations with the Hecke operator T to **eliminate one of them**, and reduce to the previous case.

Computing the quotient Q

We show that **three** possibilities occur, with the second possibility being the most frequent:

1. Q **is irreducible**, in which case we know $\bar{\Theta}^{\mathrm{ss}}_{k,a_p}$, up to separating out some reducible cases.
2. Q **has 2 JH-factors**, in which case we do some delicate computations with the Hecke operator T to **eliminate one of them**, and reduce to the previous case.
3. Q **has 3 JH-factors**, in which case one can usually use the Hecke operator T to **eliminate 2 JH-factors** (not the one we eliminated in the previous case!) and again reduce to the first case.

Computing the quotient Q

We show that **three** possibilities occur, with the second possibility being the most frequent:

1. Q **is irreducible**, in which case we know $\bar{\Theta}^{\mathrm{SS}}_{k,a_p}$, up to separating out some reducible cases.
2. Q **has 2 JH-factors**, in which case we do some delicate computations with the Hecke operator T to **eliminate one of them**, and reduce to the previous case.
3. Q **has 3 JH-factors**, in which case one can usually use the Hecke operator T to **eliminate 2 JH-factors** (not the one we eliminated in the previous case!) and again reduce to the first case.

Finally, we separate out the reducible cases, under a mild hypothesis. Thus, in most cases, we can compute $\bar{\Theta}^{\mathrm{SS}}_{k,a_p}$ and hence $\bar{\rho}^{\mathrm{SS}}$ by the LLC.

Main Theorem

Let $p \geq 5$ and $r \geq 2p + 1$.

Main Theorem

Let $p \geq 5$ and $r \geq 2p + 1$.

Say $1 < v < 2$.

Main Theorem

Let $p \geq 5$ and $r \geq 2p + 1$.

Say $1 < v < 2$.

Say that $r \equiv b \mod p - 1$ with $b = 2, 3 \ldots, p$.

Main Theorem

Let $p \geq 5$ and $r \geq 2p + 1$.

Say $1 < v < 2$.

Say that $r \equiv b \mod p - 1$ with $b = 2, 3 \ldots, p$.

Then $\bar{\rho}$ is generically **irreducible** on decomposition and on I_p

$$\bar{\rho} = \begin{pmatrix} \omega_2^{b+p} & 0 \\ 0 & \omega_2^{(b+p)p} \end{pmatrix},$$

Main Theorem

Let $p \geq 5$ and $r \geq 2p+1$.

Say $1 < v < 2$.

Say that $r \equiv b \mod p-1$ with $b = 2, 3 \ldots, p$.

Then $\bar{\rho}$ is generically **irreducible** on decomposition and on I_p

$$\bar{\rho} = \begin{pmatrix} \omega_2^{b+p} & 0 \\ 0 & \omega_2^{(b+p)p} \end{pmatrix},$$

except if

1. $b = 2,\ p \nmid r(r-1)$
2. $b = 3,\ p | r-b$ and either $v \neq \frac{3}{2}$ or $v = \frac{3}{2}$ & $v(a_p^2 - p^3) = 3$
3. $4 \leq b \leq p-1,\ p | r-b$,

in which case

$$\bar{\rho} = \begin{pmatrix} \omega_2^{b+1} & 0 \\ 0 & \omega_2^{(b+1)p} \end{pmatrix}.$$

Main Theorem

Let $p \geq 5$ and $r \geq 2p+1$.

Say $1 < v < 2$.

Say that $r \equiv b \mod p-1$ with $b = 2, 3 \ldots, p$.

Then $\bar{\rho}$ is generically **irreducible** on decomposition and on I_p

$$\bar{\rho} = \begin{pmatrix} \omega_2^{b+p} & 0 \\ 0 & \omega_2^{(b+p)p} \end{pmatrix},$$

except if

1. $b = 2,\ p \nmid r(r-1)$
2. $b = 3,\ p | r-b$ and either $v \neq \frac{3}{2}$ or $v = \frac{3}{2}$ & $v(a_p^2 - p^3) = 3$
3. $4 \leq b \leq p-1,\ p | r-b$,

in which case

$$\bar{\rho} = \begin{pmatrix} \omega_2^{b+1} & 0 \\ 0 & \omega_2^{(b+1)p} \end{pmatrix}.$$

Main Theorem (continued)

In addition, the following **reducible** case

1. might occur if $b = 3$, $p \nmid r - b$, $v = \frac{3}{2}$ & the inequality $v(a_p^2 - p^3\binom{r-1}{2}(r-2)) > 3$ holds:

$$\bar{\rho} = \begin{pmatrix} \omega^2 & * \\ 0 & \omega^2 \end{pmatrix},$$

Main Theorem (continued)

In addition, the following **reducible** case

1. might occur if $b = 3$, $p \nmid r - b$, $v = \frac{3}{2}$ & the inequality $v(a_p^2 - p^3\binom{r-1}{2}(r-2)) > 3$ holds:

$$\bar{\rho} = \begin{pmatrix} \omega^2 & * \\ 0 & \omega^2 \end{pmatrix},$$

2. always occurs if $b = p$, $p^2 | r - b$:

$$\bar{\rho} = \begin{pmatrix} \omega & * \\ 0 & \omega \end{pmatrix}.$$

Main Theorem (continued)

In addition, the following **reducible** case

1. might occur if $b = 3,\ p \nmid r - b,\ v = \frac{3}{2}$ & the inequality $v(a_p^2 - p^3\binom{r-1}{2}(r-2)) > 3$ holds:

$$\bar{\rho} = \begin{pmatrix} \omega^2 & * \\ 0 & \omega^2 \end{pmatrix},$$

2. always occurs if $b = p,\ p^2 | r - b$:

$$\bar{\rho} = \begin{pmatrix} \omega & * \\ 0 & \omega \end{pmatrix}.$$

Rmk: The following cases are still being investigated:

- $b = 3,\ p | r - b,\ v = \frac{3}{2}$ and $v(a_p^2 - p^3) > 3$
- Separating out the reducible cases in 1. above
- $p = 3$.

Endnote: a by-product of our proof

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Do you see a pattern?

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Do you see a pattern? We can now write down what these numbers are (and specify the structure of U completely; this structure is used to prove the Main Theorem).

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Do you see a pattern? We can now write down what these numbers are (and specify the structure of U completely; this structure is used to prove the Main Theorem).

Write $r = p^{v(r)}s$ with $(s, p) = 1$.

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Do you see a pattern? We can now write down what these numbers are (and specify the structure of U completely; this structure is used to prove the Main Theorem).

Write $r = p^{v(r)}s$ with $(s, p) = 1$.

Let $\Sigma =$ sum of the p-adic digits of $s - 1$;

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Do you see a pattern? We can now write down what these numbers are (and specify the structure of U completely; this structure is used to prove the Main Theorem).

Write $r = p^{v(r)}s$ with $(s, p) = 1$.

Let $\Sigma =$ sum of the p-adic digits of $s - 1$; $\delta = \begin{cases} 0 & \text{if } r = s, \\ 1 & \text{otherwise.} \end{cases}$

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Do you see a pattern? We can now write down what these numbers are (and specify the structure of U completely; this structure is used to prove the Main Theorem).

Write $r = p^{v(r)}s$ with $(s, p) = 1$.

Let $\Sigma =$ sum of the p-adic digits of $s - 1$; $\delta = \begin{cases} 0 & \text{if } r = s, \\ 1 & \text{otherwise.} \end{cases}$

Proposition

Assume $r \geq 2p + 1$. Then U has 2, 3 or 4 JH factors,

Endnote: a by-product of our proof

When we started this project, the module U was mysterious.

E.g., Here is dim U for $p = 5$, for say $15 \leq r \leq 30$:

$$\ldots, 10, 8, 10, 12, 12, 11, 10, 12, 12, 12, 8, 4, 6, 8, 10, 9, \ldots$$

Do you see a pattern? We can now write down what these numbers are (and specify the structure of U completely; this structure is used to prove the Main Theorem).

Write $r = p^{v(r)}s$ with $(s, p) = 1$.

Let $\Sigma =$ sum of the p-adic digits of $s - 1$; $\delta = \begin{cases} 0 & \text{if } r = s, \\ 1 & \text{otherwise.} \end{cases}$

Proposition

Assume $r \geq 2p + 1$. Then U has 2, 3 or 4 JH factors, and

$$\dim U = \begin{cases} 2\Sigma + 2 + \delta(p + 1 - \Sigma) & \text{if } \Sigma \leq p - 1 \\ 2p + 2 & \text{if } \Sigma > p - 1. \end{cases}$$

Thank you!