Images of modular Galois representations mod $\ell$

Samuele Anni

Universiteit Leiden - Université Bordeaux 1

Leiden, ALGANT meeting;
23rd February 2013
1 Residual modular Galois representations
- Modular curves and Modular Forms
- Residual modular Galois representations
- Image of Residual modular Galois representations
- Algorithm
- Example: projective image $S_4$ in characteristic 3

2 A local-global principle for isogenies of prime degree over number fields
Let us fix a positive integer $n \in \mathbb{Z}_{>0}$.

**Definition**

The congruence subgroup $\Gamma_1(n)$ of $\text{SL}_2(\mathbb{Z})$ is the subgroup given by

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1, \ c \equiv 0 \mod n \right\}.$$

The integer $n$ is called **level** of the congruence subgroup.
Over the upper half plane:

\[ \mathbb{H} = \{ z \in \mathbb{C} | \text{Im}(z) > 0 \} \]

we can define an action of \( \Gamma_1(n) \) via

**fractional transformations:**

\[ \Gamma_1(n) \times \mathbb{H} \rightarrow \mathbb{H} \]

\[ (\gamma, z) \mapsto \gamma(z) = \frac{az + b}{cz + d} \]

where \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \).

Moreover, if \( n \geq 4 \) then \( \Gamma_1(n) \) acts freely on \( \mathbb{H} \).
**Definition**

*We define the **modular curve** $Y_1(n)_\mathbb{C}$ to be the non-compact Riemann surface obtained giving on $\Gamma_1(n) \backslash \mathbb{H}$ the complex structure induced by the quotient map.*

*Let $X_1(n)_{\mathbb{C}}$ be the compactification of $Y_1(n)_{\mathbb{C}}$.***
**Definition**

*We define the modular curve $Y_1(n)_{\mathbb{C}}$ to be the non-compact Riemann surface obtained giving on $\Gamma_1(n) \backslash \mathbb{H}$ the complex structure induced by the quotient map.*

*Let $X_1(n)_{\mathbb{C}}$ be the compactification of $Y_1(n)_{\mathbb{C}}$.***

**Fact:** $Y_1(n)_{\mathbb{C}}$ can be defined algebraically over $\mathbb{Q}$ (in fact over $\mathbb{Z}[1/n]$).
The group $GL_2^+(\mathbb{Q})$ acts on $\mathbb{H}$ via fractional transformation, and its action has a particular behaviour with respect to $\Gamma_1(n)$.
The group $GL_2^+ (\mathbb{Q})$ acts on $\mathbb{H}$ via fractional transformation, and its action has a particular behaviour with respect to $\Gamma_1(n)$.

**Proposition**

$\forall g \in GL_2^+ (\mathbb{Q})$ the discrete groups $g\Gamma_1(n)g^{-1}$ and $\Gamma_1(n)$ are commensurable, i.e. $g\Gamma_1(n)g^{-1} \cap \Gamma_1(n)$ is a subgroup of finite index in $g\Gamma_1(n)g^{-1}$ and $\Gamma_1(n)$. 

![Diagram of modular curves and modular forms](image)
We can define operators on $Y_1(n)$ through the correspondences given before:
We can define operators on $Y_1(n)$ through the correspondences given before:

- the **Hecke operators** $T_p$ for every prime $p$, using

  $$g = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in GL_2^+(\mathbb{Q})$$
We can define operators on $Y_1(n)$ through the correspondences given before:

- **the Hecke operators** $T_p$ for every prime $p$, using
  $$g = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in GL_2^+(\mathbb{Q})$$

- **the diamond operators** $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$, using
  $$g = \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \in GL_2^+(\mathbb{Q}).$$
For $n \geq 5$, $\ell$ prime not dividing $n$, and $k$ integer we define, à la Katz:
For \( n \geq 5 \), \( \ell \) prime not dividing \( n \), and \( k \) integer we define, à la Katz:

\[
S(n, k)_{\mathbb{F}_\ell} = H^0(X_1(n)_{\mathbb{F}_\ell}, \omega^k(-\text{Cusps})).
\]
For $n \geq 5$, $\ell$ prime not dividing $n$, and $k$ integer we define, à la Katz:

$S(n, k)_{\overline{\mathbb{F}}_\ell} = H^0(X_1(n)_{\overline{\mathbb{F}}_\ell}, \omega^k(-\text{Cusps})).$

$S(n, k)_{\overline{\mathbb{F}}_\ell}$ is a finite dimensional $\overline{\mathbb{F}}_\ell$-vector space, equipped with Hecke operators $T_n$ ($n \geq 1$) and diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z} / n\mathbb{Z})^*$. 
For $n \geq 5$, $\ell$ prime not dividing $n$, and $k$ integer we define, à la Katz:

\[
S(n, k)_{\mathbb{F}_\ell} = H^0(X_1(n)_{\mathbb{F}_\ell}, \omega \otimes^k (\text{Cusps})).
\]

$S(n, k)_{\mathbb{F}_\ell}$ is a finite dimensional $\mathbb{F}_\ell$-vector space, equipped with Hecke operators $T_n$ ($n \geq 1$) and diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z} / n\mathbb{Z})^*$. Analogous definition in characteristic zero and over any ring where $n$ is invertible.
One may think that mod $\ell$ modular forms come from reduction of characteristic zero modular forms mod $\ell$:

$$S(n, k)_{\mathbb{Z}[1/n]} \rightarrow S(n, k)_{\mathbb{F}_\ell}.$$
One may think that mod $\ell$ modular forms come from reduction of characteristic zero modular forms mod $\ell$:

$$S(n, k)_{\mathbb{Z}[1/n]} \rightarrow S(n, k)_{\mathbb{F}_\ell}.$$

Unfortunately, this map is not surjective for $k = 1$. 
One may think that mod $\ell$ modular forms come from reduction of characteristic zero modular forms mod $\ell$:

$$S(n, k)_{\mathbb{Z}[1/n]} \to S(n, k)_{\mathbb{F}_{\ell}}.$$ 

Unfortunately, this map is not surjective for $k = 1$. Even worse: given a character $\epsilon: (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ the map

$$S(n, k, \epsilon)_{\mathcal{O}_K} \to S(n, k, \bar{\epsilon})_{\mathbb{F}}$$

is not always surjective even if $k > 1$, where $\mathcal{O}_K$ is the ring of integers of the number field where $\epsilon$ is defined, $\mathbb{F}_{\ell} \subseteq \mathbb{F}$ and

$$S(n, k, \epsilon)_{\mathcal{O}_K} = \{ f \in S(n, k)_{\mathcal{O}_K} \mid \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d \rangle f = \epsilon(d)f \}.$$
**Definition**

We define the **Hecke algebra** $\mathcal{T}(n, k)$ of $S(n, k)_C$ as the $\mathbb{Z}$-subalgebra of $\text{End}_C(S(\Gamma_1(n), k)_C)$ generated by the Hecke operators $T_p$ for every prime $p$ and the diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z} / n\mathbb{Z})^*$. 
**Definition**

We define the Hecke algebra $\mathcal{T}(n, k)$ of $S(n, k)_\mathbb{C}$ as the $\mathbb{Z}$-subalgebra of $\text{End}_{\mathbb{C}}(S(\Gamma_1(n), k)_\mathbb{C})$ generated by the Hecke operators $T_p$ for every prime $p$ and the diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^\ast$.

Fact: $\mathcal{T}(n, k)$ is finitely generated as $\mathbb{Z}$-module.

We can associate a Hecke algebra $\mathcal{T}(n, k, \epsilon)$ to each $S(n, k, \epsilon)_\mathbb{C}$.
Theorem (Shimura, Deligne)

Let $n$ and $k$ be positive integers. Let $F$ be a finite field of characteristic $\ell$, $\ell \nmid n$, and $f : \mathbb{Z}(n, k) \to F$ a surjective morphism of rings. Then there is a continuous semi-simple representation: $\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(F)$ that is unramified outside $n\ell$ such that for all $p$ not dividing $n\ell$ we have, in $F$:

$$\text{Tr}(\rho_f(\text{Frob}_p)) = f(T_p) \quad \text{and} \quad \text{det}(\rho_f(\text{Frob}_p)) = f(\langle p \rangle)p^{k-1}.$$ 

Such a $\rho_f$ is unique up to isomorphism.
Theorem (Shimura, Deligne)

Let $n$ and $k$ be positive integers. Let $\mathbb{F}$ be a finite field of characteristic $\ell$, $\ell \nmid n$, and $f : T(n, k) \to \mathbb{F}$ a surjective morphism of rings. Then there is a continuous semi-simple representation: $\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F})$ that is unramified outside $n\ell$ such that for all $p$ not dividing $n\ell$ we have, in $\mathbb{F}$:

$$\text{Tr}(\rho_f(\text{Frob}_p)) = f(T_p) \quad \text{and} \quad \det(\rho_f(\text{Frob}_p)) = f(\langle p \rangle)p^{k-1}.$$

Such a $\rho_f$ is unique up to isomorphism.
**Theorem (Shimura, Deligne)**

Let \( n \) and \( k \) be positive integers. Let \( \mathbb{F} \) be a finite field of characteristic \( \ell \), \( \ell \nmid n \), and \( f : \mathbb{T}(n, k) \rightarrow \mathbb{F} \) a surjective morphism of rings. Then there is a continuous semi-simple representation: 
\[
\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F})
\]
that is unramified outside \( n \ell \) such that for all \( p \) not dividing \( n \ell \) we have, in \( \mathbb{F} \):

\[
\text{Tr}(\rho_f(\text{Frob}_p)) = f(T_p) \quad \text{and} \quad \det(\rho_f(\text{Frob}_p)) = f(\langle p \rangle)p^{k-1}.
\]

Such a \( \rho_f \) is unique up to isomorphism.

Computing \( \rho_f \) is “difficult”,

**Theorem (Shimura, Deligne)**

Let $n$ and $k$ be positive integers. Let $\mathbb{F}$ be a finite field of characteristic $\ell$, $\ell \nmid n$, and $f : \mathbb{T}(n, k) \to \mathbb{F}$ a surjective morphism of rings. Then there is a continuous semi-simple representation: $\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F})$ that is unramified outside $n\ell$ such that for all $p$ not dividing $n\ell$ we have, in $\mathbb{F}$:

$$\text{Tr}(\rho_f(\text{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\text{Frob}_p)) = f(\langle p \rangle)p^{k-1}.$$ 

Such a $\rho_f$ is unique up to isomorphism.

Computing $\rho_f$ is “difficult”, but theoretically it can be done in polynomial time in $n, k, \#\mathbb{F}$. 

---

**Image of Residual modular Galois representations**

**Algorithm**

**Example: projective image $S_4$ in characteristic 3**
**QUESTION**

Can we compute the image of a residual modular Galois representation without computing the representation?
Main ingredients:

**Theorem (Dickson)**

Let $\ell$ be an odd prime and $H$ a finite subgroup of $\text{PGL}_2(\overline{\mathbb{F}_\ell})$. Then a conjugate of $H$ is one of the following groups:

- a finite subgroups of the upper triangular matrices;
- $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ or $\text{PGL}_2(\mathbb{F}_\ell)$ for $r \in \mathbb{Z}_{>0}$;
- a dihedral group $D_{2n}$ with $n \in \mathbb{Z}_{>1}$, $(\ell, n) = 1$;
- or it is isomorphic to $A_4$, $S_4$ or $A_5$. 
Theorem (Khare, Wintenberger, Dieulefait) - Serre’s Conjecture

Let $\ell$ be a prime number and let $\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, absolutely irreducible, continuous representation. Then $\rho$ is modular of level $N(\rho)$, weight $k(\rho)$ and character $\epsilon(\rho)$.
Theorem (Khare, Wintenberger, Dieulefait) - Serre’s Conjecture

Let $\ell$ be a prime number and let $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, absolutely irreducible, continuous representation. Then $\rho$ is modular of level $N(\rho)$, weight $k(\rho)$ and character $\epsilon(\rho)$.

$N(\rho)$ (the level) is the Artin conductor away from $\ell$. 
Theorem (Khare, Wintenberger, Dieulefait) - Serre’s Conjecture

Let $\ell$ be a prime number and let $\rho : \text{Gal}(\overbar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overbar{\mathbb{F}}_\ell)$ be an odd, absolutely irreducible, continuous representation. Then $\rho$ is modular of level $N(\rho)$, weight $k(\rho)$ and character $\epsilon(\rho)$.

$N(\rho)$ (the level) is the Artin conductor away from $\ell$.

$k(\rho)$ (the weight) is given by a recipe in terms of $\rho|_{I_\ell}$.
Let $\ell$ be a prime number and let $\rho: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_{\ell})$ be an odd, absolutely irreducible, continuous representation. Then $\rho$ is modular of level $N(\rho)$, weight $k(\rho)$ and character $\epsilon(\rho)$.

$N(\rho)$ (the level) is the Artin conductor away from $\ell$.

$k(\rho)$ (the weight) is given by a recipe in terms of $\rho|_{I_{\ell}}$.

$\epsilon(\rho): (\mathbb{Z}/N(\rho)\mathbb{Z})^* \rightarrow \overline{\mathbb{F}}_{\ell}^*$ is given by:

$$\det \circ \rho = \epsilon(\rho)\chi^{k(\rho)-1}.$$
Residual modular Galois representations

A local-global principle for isogenies over number fields

Modular curves and Modular Forms
Residual modular Galois representations
Image of Residual modular Galois representations
Algorithm
Example: projective image $S_4$ in characteristic 3

Algorithm

Input:
- $n$ positive integer;
- $\ell$ prime such that $(n, \ell) = 1$;
- $k$ positive integer such that $2 \leq k \leq \ell + 1$;
- a character $\epsilon: (\mathbb{Z}/n\mathbb{Z})^\ast \rightarrow \mathbb{C}^\ast$;
- a morphism of ring $f: T(n, k, \epsilon) \rightarrow F_\ell$;

Output:
- Image of the associated Galois representation $\rho_f$, up to conjugacy as subgroup of $GL_2(F_\ell)$. 

Samuele Anni

Images of modular Galois representations mod $\ell$
Algorithm

Input: \( n \) positive integer; \( \ell \) prime such that \((n,\ell) = 1\); \( k \) positive integer such that \(2 \leq k \leq \ell + 1\); a character \( \epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^* \); a morphism of ring \( f : T(n,k,\epsilon) \to F_\ell \);

Output: Image of the associated Galois representation \( \rho_f \), up to conjugacy as subgroup of \( GL_2(F_\ell) \).
Residual modular Galois representations
A local-global principle for isogenies over number fields

Modular curves and Modular Forms
Residual modular Galois representations
Image of Residual modular Galois representations
Algorithm
Example: projective image $S_4$ in characteristic 3

Algorithm

Input:
- $n$ positive integer;
- $\ell$ prime such that $(n, \ell) = 1$;
- $k$ positive integer such that $2 \leq k \leq \ell + 1$;
- a character $\epsilon: (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^*$;
- a morphism of ring $f: T(n, k, \epsilon) \rightarrow F_\ell$;

Output:
- Image of the associated Galois representation $\rho_f$, up to conjugacy as subgroup of $\text{GL}_2(F_\ell)$. 

Samuele Anni
Images of modular Galois representations mod $\ell$
Algorithm

Input:
**Algorithm**

**Input:**
- $n$ positive integer;
- $\ell$ prime such that $(n, \ell) = 1$;
- $k$ positive integer such that $2 \leq k \leq \ell + 1$;
- a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;
- a morphism of ring $f : \mathcal{T}(n, k, \epsilon) \to \overline{\mathbb{F}_\ell}$;
Algorithm

Input:
- $n$ positive integer;
- $\ell$ prime such that $(n, \ell) = 1$;
- $k$ positive integer such that $2 \leq k \leq \ell + 1$;
- a character $\epsilon: (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^*$;
- a morphism of ring $f: \mathbb{T}(n, k, \epsilon) \rightarrow \overline{\mathbb{F}}_\ell$;

Output:
Algorithm

Input:
- $n$ positive integer;
- $\ell$ prime such that $(n, \ell) = 1$;
- $k$ positive integer such that $2 \leq k \leq \ell + 1$;
- a character $\epsilon: (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;
- a morphism of ring $f: \mathbb{T}(n, k, \epsilon) \to \overline{\mathbb{F}}_\ell$;

Output:
Image of the associated Galois representation $\rho_f$, up to conjugacy as subgroup of $\text{GL}_2(\overline{\mathbb{F}}_\ell)$. 
How do we want to construct this algorithm?
How do we want to construct this algorithm?

Iteration “down to top”, i.e. considering all divisors of \( n \) (and all twists).

Determination of the projective image. Determination of the image.
How do we want to construct this algorithm?

Iteration “down to top”, i.e. considering all divisors of \( n \) (and all twists).

Determination of the projective image. Determination of the image.

How many \( T_p \)?
How do we want to construct this algorithm?

Iteration “down to top”, i.e. considering all divisors of $n$ (and all twists).

Determination of the projective image. Determination of the image.

How many $T_p$?

Bound linear in $n$ (and $k$): Sturm Bound at level $n$, which we will denote as $SB(n, k)$ (at the moment the known bound is $\sim \ell^5 n^3$).
Results

We have studied the field of definition of the representation, and of the projective representation: in both cases we can determine such fields computing operators up to $SB(n,k)$.

We have a result about twists of representation: this will speed up the computation of the projective image.

We are studying methods for switching characteristic in the case of "exceptional" projective image, i.e. projective image isomorphic to $A_4$, $S_4$, or $A_5$.

Idea: construct a database in characteristic 2, 3 and 5 to have information in larger characteristic.
Results

We have studied the field of definition of the representation, and of the projective representation:
Results

- We have studied the field of definition of the representation, and of the projective representation: in both cases we can determine such fields computing operators up $SB(n, k)$. 

Idea: construct a database in characteristic 2, 3 and 5 to have information in larger characteristic.
**Results**

- We have studied the field of definition of the representation, and of the projective representation: in both cases we can determine such fields computing operators up $SB(n, k)$.
- We have a result about twists of representation: this will speed up the computation of the projective image.
**Results**

- We have studied the field of definition of the representation, and of the projective representation: in both cases we can determine such fields computing operators up $SB(n, k)$.

- We have a result about twists of representation: this will speed up the computation of the projective image.

- We are studying methods for switching characteristic in the case of “exceptional” projective image, i.e. projective image isomorphic to $A_4$, $S_4$ or $A_5$. Idea: construct a database in characteristic 2, 3 and 5 to have information in larger characteristic.
Example: projective image $S_4$ in characteristic 3.

Idea:

A modular representation which has $S_4$ as projective image in characteristic 3 has "big" projective image, i.e., $\text{PGL}_2(F_3) \simeq S_4$; from mod 3 modular forms with projective image $S_4$, we want to construct characteristic 0 forms; use these forms to decide about projective image $S_4$ in characteristic larger than 3.
Example: projective image $S_4$ in characteristic 3.

**Ideas:**

- A modular representation which has $S_4$ as projective image in characteristic 3 has “big” projective image i.e. $PGL_2(\mathbb{F}_3) \cong S_4$.
Example: projective image $S_4$ in characteristic 3.

**Ideas:**

- A modular representation which has $S_4$ as projective image in characteristic 3 has “big” projective image i.e. $\text{PGL}_2(\mathbb{F}_3) \cong S_4$;
- From mod 3 modular forms with projective image $S_4$, we want to construct characteristic 0 forms;
Example: projective image $S_4$ in characteristic 3.

**Ideas:**

- a modular representation which has $S_4$ as projective image in characteristic 3 has “big” projective image i.e. $\text{PGL}_2(\mathbb{F}_3) \cong S_4$;
- from mod 3 modular forms with projective image $S_4$, we want to construct characteristic 0 forms;
- use these forms to decide about projective image $S_4$ in characteristic larger than 3.
**Input:**

- A positive integer, \( (n, 3) = 1 \);
- An integer \( k \in \{2, 3, 4\} \);
- A character \( \epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^* \);
- A morphism of rings \( f : T(n, k, \epsilon) \to F_3 \).
Input:

\begin{itemize}
\item \textbf{Input:} \\
\end{itemize}
Input:

- $n$ positive integer, $(n, 3) = 1$;
- $k \in \{2, 3, 4\}$;
- a character $\epsilon: (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;
- a morphism of rings $f: \mathbb{T}(n, k, \epsilon) \to \overline{\mathbb{F}}_3$. 

Samuele Anni
Suppose the algorithm has certified that $\rho_f$ is absolutely irreducible and that $\mathbb{P}\rho_f \cong S_4$. Suppose also that $f$ is “minimal” with respect to weight, level and twisting.
Suppose the algorithm has certified that $\rho_f$ is absolutely irreducible and that $\mathbb{P}\rho_f \cong S_4$. Suppose also that $f$ is “minimal” with respect to weight, level and twisting. What else do we know?

- Field of definition of the representation: $\mathbb{F}$;
- Field of definition of the projective representation: $\mathbb{F}_3$;
- Data on the local components;
- Image of the representation: $\rho_f(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \mathbb{F}^* \cdot \text{GL}_2(\mathbb{F}_3)$. 
Suppose the algorithm has certified that $\rho_f$ is absolutely irreducible and that $\mathbb{P}\rho_f \cong S_4$. Suppose also that $f$ is “minimal” with respect to weight, level and twisting. What else do we know?

- Field of definition of the representation: $\mathbb{F}$;
- Field of definition of the projective representation: $\mathbb{F}_3$;
- Data on the local components;
- Image of the representation: $\rho_f(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \mathbb{F}^* \cdot \text{GL}_2(\mathbb{F}_3)$.

Let $\beta : \mathbb{F}^* \cdot \text{GL}_2(\mathbb{F}_3) \to \text{GL}_2(\mathcal{O}_K)$ be a faithful irreducible 2-dimensional representation, where $\mathcal{O}_K$ is the ring of integers of a number field.
Residual modular Galois representations
A local-global principle for isogenies over number fields

Modular curves and Modular Forms
Residual modular Galois representations
Image of Residual modular Galois representations
Algorithm
Example: projective image $S_4$ in characteristic 3

By Serre’s conjecture there exists $f_{\beta}$ of weight 1 such that
$\rho_f \sim \beta \circ \rho_f$.

Can we determine the level of $f_{\beta}$?
Yes, we can bound it.
Can we determine $f_{\beta}(T_p)$, $f_{\beta}(\langle p \rangle)$ for all $p$?
Yes for the primes dividing the level and 3
No for the unramified primes! Problem: distinguish elements in $GL_2(F_3)$ using only traces and determinants is not possible.
Solution: check in characteristic 2 and 5.

Images of modular Galois representations mod $\ell$

Samuele Anni
Residual modular Galois representations

A local-global principle for isogenies over number fields

Modular curves and Modular Forms

Image of Residual modular Galois representations

Algorithm

Example: projective image $S_4$ in characteristic 3

\[
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_f} \mathbb{F}^* \xrightarrow{\beta} \text{GL}_2(\mathbb{F}_3) \xrightarrow{\beta} \text{GL}_2(\mathcal{O}_K)
\]

By Serre’s conjecture there exists $f_{\beta}$ of weight 1 such that $\rho_{f_{\beta}} \sim \beta \circ \rho_f$.

Can we determine the level of $f_{\beta}$?

Yes, we can bound it.

Can we determine $f_{\beta}(T_p)$, $f_{\beta}(\langle p \rangle)$ for all $p$?

Yes for the primes dividing the level and 3.

No for the unramified primes! Problem: distinguish elements in $\text{GL}_2(\mathbb{F}_3)$ using only traces and determinants is not possible.

Solution: check in characteristic 2 and 5.
Residual modular Galois representations

A local-global principle for isogenies over number fields

Modular curves and Modular Forms

Residual modular Galois representations

Image of Residual modular Galois representations

Algorithm

Example: projective image $S_4$ in characteristic 3

\[
\begin{array}{ccc}
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_f} & \mathbb{F}^* \text{GL}_2(\mathbb{F}_3) & \xrightarrow{\beta} & \text{GL}_2(\mathcal{O}_K) \\
\end{array}
\]

By Serre’s conjecture there exists $f_\beta$ of weight 1 such that $\rho_{f_\beta} \cong \beta \circ \rho_f$. 

Images of modular Galois representations mod $\ell$
By Serre’s conjecture there exists $f_{\beta}$ of weight 1 such that $\rho_{f_{\beta}} \cong \beta \circ \rho_f$.

Can we determine the level of $f_{\beta}$?
Residual modular Galois representations

A local-global principle for isogenies over number fields

Modular curves and Modular Forms
Residual modular Galois representations
Image of Residual modular Galois representations
Algorithm
Example: projective image $S_4$ in characteristic 3

Can we determine the level of $f_{\beta}$?

Yes, we can bound it.

By Serre’s conjecture there exists $f_{\beta}$ of weight 1 such that $\rho_{f_{\beta}} \cong \beta \circ \rho_f$. 
By Serre’s conjecture there exists \( f_\beta \) of weight 1 such that \( \rho_{f_\beta} \cong \beta \circ \rho_f \).

**Can we determine the level of \( f_\beta \)?**

Yes, we can bound it.

**Can we determine \( f_\beta(T_p), f_\beta(\langle p \rangle) \) for all \( p \)?**

Yes for the primes dividing the level and 3. No for the unramified primes! Problem: distinguish elements in \( \text{GL}_2(F_3) \) using only traces and determinants is not possible. Solution: check in characteristic 2 and 5.
Residual modular Galois representations
A local-global principle for isogenies over number fields

Gal(\overline{\mathbb{Q}} / \mathbb{Q}) \overset{\rho_f}{\longrightarrow} \mathbb{F}^* \text{GL}_2(\mathbb{F}_3) \overset{\beta}{\longrightarrow} \text{GL}_2(\mathcal{O}_K)

By Serre’s conjecture there exists \( f_\beta \) of weight 1 such that \( \rho_{f_\beta} \cong \beta \circ \rho_f \).

**Can we determine the level of \( f_\beta \)?**
Yes, we can bound it.

**Can we determine \( f_\beta(T_p), f_\beta(\langle p \rangle) \) for all \( p \)?**
Yes for the primes dividing the level and 3.
By Serre’s conjecture there exists $f_{\beta}$ of weight 1 such that $\rho_{f_{\beta}} \cong \beta \circ \rho_f$.

**Can we determine the level of $f_{\beta}$?**

Yes, we can bound it.

**Can we determine $f_{\beta}(T_p)$, $f_{\beta}(\langle p \rangle)$ for all $p$?**

Yes for the primes dividing the level and 3.

No for the unramified primes! Problem: distinguish elements in $GL_2(\mathbb{F}_3)$ using only traces and determinants is not possible.
Residual modular Galois representations

A local-global principle for isogenies over number fields

Modular curves and Modular Forms

Image of Residual modular Galois representations

Algorithm

Example: projective image $S_4$ in characteristic 3

\[ \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_f} \mathbb{F}^* \text{GL}_2(\mathbb{F}_3) \xrightarrow{\beta} \text{GL}_2(\mathcal{O}_K) \]

By Serre’s conjecture there exists $f_\beta$ of weight 1 such that $\rho_{f_\beta} \cong \beta \circ \rho_f$.

**Can we determine the level of $f_\beta$?**

Yes, we can bound it.

**Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ for all $p$?**

Yes for the primes dividing the level and 3

No for the unramified primes! Problem: distinguish elements in $\text{GL}_2(\mathbb{F}_3)$ using only traces and determinants is not possible.

**Solution:**

check in characteristic 2 and 5.
Residual modular Galois representations

A local-global principle for isogenies over number fields

Example: projective image $S_4$ in characteristic 3

$\mathbb{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_f} \mathbb{F}^* \xrightarrow{\beta} \mathbb{GL}_2(\mathbb{F}_3) \xrightarrow{\beta} \mathbb{GL}_2(\mathcal{O}_K) \xrightarrow{\pi} \mathbb{GL}_2(\overline{\mathbb{F}}_2)$
Residual modular Galois representations
A local-global principle for isogenies over number fields

Image of Residual modular Galois representations
Algorithm

Example: projective image $S_4$ in characteristic 3

\[
\begin{align*}
\rho_f \pi \beta & \quad \rho_f & \quad \rho_f \pi \beta & \quad \rho_f \pi \beta \rho_f (\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \mathbb{F}^* \times \text{GL}_2(\mathbb{F}_2) \\
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \rightarrow & \mathbb{F}^* \times \text{GL}_2(\mathbb{F}_3) & \rightarrow & \text{GL}_2(\mathcal{O}_K) & \rightarrow & \text{GL}_2(\overline{\mathbb{F}}_2) \\
& & & \downarrow & \downarrow & \uparrow \\
& & & & \pi & & \\
& & & & \rho_f \pi \beta & & \\
& & & & \rho_f & & \\
& & & & \rho_f \pi \beta & & \\
& & & & \rho_f & & \\
& & & & \rho_f \pi \beta \rho_f (\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) & \sim & S_3
\end{align*}
\]
There exists a mod 2 modular form $f_{\pi \beta}$ such that $\rho_{f_{\pi \beta}} \cong \pi \circ \beta \circ \rho_f$. 
There exists a mod 2 modular form $f_{\pi \beta}$ such that $\rho f_{\pi \beta} \cong \pi \circ \beta \circ \rho_f$. 

Can we determine the level of $f_{\pi \beta}$? 

Yes, we can bound it. 

Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ using $f_{\pi \beta}(T_p)$, $f_{\pi \beta}(\langle p \rangle)$ for all $p$? 

Yes for the primes dividing the level and 3. 

For the unramified primes there is still a problem but we have candidates, i.e. a finite list of mod 2 modular forms with prescribed properties. 

How can we solve this problem? 

For each candidate we have a power series in characteristic 0. All power series are defined over the same ring of integers so we can reduce them modulo 5 and check if the list we obtain does occur as eigenvalue system or not. Claim: only one power series is a modular form.
There exists a mod 2 modular form $f_{\pi\beta}$ such that $\rho_{f_{\pi\beta}} \cong \pi \circ \beta \circ \rho_f$.

Can we determine the level of $f_{\pi\beta}$?

Yes, we can bound it.
There exists a mod 2 modular form $f_{\pi\beta}$ such that $\rho_{f_{\pi\beta}} \cong \pi \circ \beta \circ \rho_f$.

**Can we determine the level of $f_{\pi\beta}$?**

Yes, we can bound it.

**Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ using $f_{\pi\beta}(T_p)$, $f_{\pi\beta}(\langle p \rangle)$ for all $p$?**

Yes for the primes dividing the level and 3. For the unramified primes there is still a problem but we have candidates, i.e. a finite list of mod 2 modular forms with prescribed properties. How can we solve this problem? For each candidate we have a power series in characteristic 0. All power series are defined over the same ring of integers so we can reduce them modulo 5 and check if the list we obtain does occur as eigenvalue system or not. Claim: only one power series is a modular form.
There exists a mod 2 modular form $f_{\pi \beta}$ such that $\rho_{f_{\pi \beta}} \cong \pi \circ \beta \circ \rho_f$.

**Can we determine the level of $f_{\pi \beta}$?**

Yes, we can bound it.

**Can we determine $f_{\beta}(T_p)$, $f_{\beta}(\langle p \rangle)$ using $f_{\pi \beta}(T_p)$, $f_{\pi \beta}(\langle p \rangle)$ for all $p$?**

Yes for the primes dividing the level and 3.
There exists a mod 2 modular form $f_{\pi \beta}$ such that $\rho_{f_{\pi \beta}} \cong \pi \circ \beta \circ \rho_f$.

**Can we determine the level of $f_{\pi \beta}$?**

Yes, we can bound it.

**Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ using $f_{\pi \beta}(T_p)$, $f_{\pi \beta}(\langle p \rangle)$ for all $p$?**

Yes for the primes dividing the level and 3. For the unramified primes there is still a problem but we have candidates i.e. a finite list of mod 2 modular forms with prescribed properties.
There exists a mod 2 modular form $f_{\pi \beta}$ such that $\rho_{f_{\pi \beta}} \cong \pi \circ \beta \circ \rho_f$.

**Can we determine the level of $f_{\pi \beta}$?**
Yes, we can bound it.

**Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ using $f_{\pi \beta}(T_p)$, $f_{\pi \beta}(\langle p \rangle)$ for all $p$?**
Yes for the primes dividing the level and 3. For the unramified primes there is still a problem but we have candidates i.e. a finite list of mod 2 modular forms with prescribed properties.

**How can we solve this problem?**
For each candidate we have a power series in characteristic 0. All power series are defined over the same ring of integers so we can reduce them modulo 5 and check if the list we obtain does occur as eigenvalue system or not. Claim: only one power series is a modular form.
Residual modular Galois representations

A local-global principle for isogenies over number fields

Preliminaries and introduction to the problem
New results
Finiteness result

Residual modular Galois representations

A local-global principle for isogenies of prime degree over number fields

Preliminaries and introduction to the problem
New results
Finiteness result

Samuele Anni
Definition

Let \( E \) be an elliptic curve defined on a number field \( K \), and let \( \ell \) be a prime number. If \( \mathfrak{p} \) is a prime of \( K \) where \( E \) has good reduction, \( \mathfrak{p} \) not dividing \( \ell \), we say that \( E \) admits an \( \ell \)-isogeny \textbf{locally at} \( \mathfrak{p} \) if the Néron model of \( E \) over the ring of integer of \( K_{\mathfrak{p}} \) admits an \( \ell \)-isogeny.
**Definition**

Let $E$ be an elliptic curve defined on a number field $K$, and let $\ell$ be a prime number. If $\mathfrak{p}$ is a prime of $K$ where $E$ has good reduction, $\mathfrak{p}$ not dividing $\ell$, we say that $E$ admits an $\ell$-isogeny **locally at** $\mathfrak{p}$ if the Néron model of $E$ over the ring of integer of $K_{\mathfrak{p}}$ admits an $\ell$-isogeny.

**Question**

Let $E$ be an elliptic curve defined over a number field $K$, and let $\ell$ be a prime number, if $E$ admits an $\ell$-isogeny locally at a set of primes with density one then does $E$ admit an $\ell$-isogeny over $K$?
Theorem (Sutherland)

Let $E$ be an elliptic curve defined over a number field $K$ and let $\ell$ be a prime number. Assume $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \notin K$, and suppose $E/K$ admits an $\ell$-isogeny locally at a set of primes with density one. Then $E$ admits an $\ell$-isogeny over a quadratic extension of $K$. Moreover, if $\ell \equiv 1 \mod 4$ or $\ell < 7$, $E$ admits an $\ell$-isogeny defined over $K$. 
**Definition**

Let $K$ be a number field, let $E$ be an elliptic curve over $K$ and $\ell$ a prime number, a pair $(\ell, j(E))$ is said to be **exceptional** for $K$ if $E/K$ admits an $\ell$-isogeny locally everywhere but not over $K$.
**Definition**

Let $K$ be a number field, let $E$ be an elliptic curve over $K$ and $\ell$ a prime number, a pair $(\ell, j(E))$ is said to be **exceptional** for $K$ if $E/K$ admits an $\ell$-isogeny locally everywhere but not over $K$.

Sutherland proved the following result:
**Definition**

Let $K$ be a number field, let $E$ be an elliptic curve over $K$ and $\ell$ a prime number, a pair $(\ell, j(E))$ is said to be **exceptional** for $K$ if $E/K$ admits an $\ell$-isogeny locally everywhere but not over $K$.

Sutherland proved the following result:

**Theorem (Sutherland)**

The pair $(7, 2268945/128)$ is the only exceptional pair for $\mathbb{Q}$.
Theorem (Sutherland)

Let $E$ be an elliptic curve defined over a number field $K$ and let $\ell$ be a prime number. Assume $\sqrt{\left(\frac{-1}{\ell}\right)} \not\in K$, and suppose $E/K$ admits an $\ell$-isogeny locally at a set of primes with density one. Then $E$ admits an $\ell$-isogeny over a quadratic extension of $K$. Moreover, if $\ell \equiv 1 \mod 4$ or $\ell < 7$, $E$ admits an $\ell$-isogeny defined over $K$. 
Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) and let 
\(G = \rho_{E, \ell}(\text{Gal}(\overline{\mathbb{Q}}/K))\). Then \(G\) is a subgroup of \(\text{GL}_2(\mathbb{F}_\ell)\) such that 
\(|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0\) for all \(g \in G\) but 
\(|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0\).
Remark

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) and let \(G = \rho_{E, \ell}(\text{Gal}(\overline{Q}/K))\). Then \(G\) is a subgroup of \(\text{GL}_2(\mathbb{F}_\ell)\) such that \(|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0\) for all \(g \in G\) but \(|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0\).

Given an elliptic curve \(E\), defined over a number field \(K\), the compatibility between \(\rho_{E, \ell}\) and the Weil pairing on \(E[\ell]\) implies that:
Remark

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) and let 
\[ G = \rho_{E,\ell}(\text{Gal}(\overline{\mathbb{Q}}/K)) . \]
Then \(G\) is a subgroup of \(\text{GL}_2(\mathbb{F}_\ell)\) such that 
\[ |\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0 \text{ for all } g \in G \text{ but } |\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0. \]

Given an elliptic curve \(E\), defined over a number field \(K\), the compatibility between \(\rho_{E,\ell}\) and the Weil pairing on \(E[\ell]\) implies that:
Remark

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) and let \(G = \rho_{E,\ell}(\text{Gal}(\overline{Q}/K))\). Then \(G\) is a subgroup of \(\text{GL}_2(\mathbb{F}_\ell)\) such that \(|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0\) for all \(g \in G\) but \(|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0\).

Given an elliptic curve \(E\), defined over a number field \(K\), the compatibility between \(\rho_{E,\ell}\) and the Weil pairing on \(E[\ell]\) implies that:

- \(\zeta_\ell\) is in \(K\) if and only if \(G\) is contained in \(\text{SL}_2(\mathbb{F}_\ell)\);
Remark

Let $(\ell, j(E))$ be an exceptional pair for the number field $K$ and let $G = \rho_{E,\ell}(\text{Gal}(\overline{\mathbb{Q}}/K))$. Then $G$ is a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ such that $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$.

Given an elliptic curve $E$, defined over a number field $K$, the compatibility between $\rho_{E,\ell}$ and the Weil pairing on $E[\ell]$ implies that:

- $\zeta_\ell$ is in $K$ if and only if $G$ is contained in $\text{SL}_2(\mathbb{F}_\ell)$;
- $H$, the projective image of $G$, is contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$ if and only if $\sqrt{(-1)^{\ell}} \ell$ is in $K$.

Hence, the study of the local-global principle about $\ell$-isogenies over an arbitrary number field $K$ depends on $\sqrt{(-1)^{\ell}} \ell$ belonging to $K$ or not.
**Lemma (Sutherland)**

Let $G$ be a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ whose image $H$ in $\text{PGL}_2(\mathbb{F}_\ell)$ is not contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. Then $\ell \equiv 3 \text{ mod } 4$ and the following holds:

1. $H$ is dihedral of order $2n$, where $n > 1$ is an odd divisor of $(\ell-1)/2$;
2. $G$ is properly contained in the normalizer of a split Cartan subgroup;
3. $\mathbb{P}^1(\mathbb{F}_\ell)/G$ contains an orbit of size 2.
Proposition (A.)

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\), and assume that \(\sqrt{(-1)/\ell} \notin K\). Let \(G = \rho_{E,\ell}(\text{Gal}(\overline{\mathbb{Q}}/K))\) and let \(H\) be its image in \(\text{PGL}_2(\mathbb{F}_\ell)\). Let \(C \subset G\) be the preimage of the maximal cyclic subgroup of \(H\). Then

\[
\det(C) \in (\mathbb{F}_\ell^*)^2.
\]

where \((\mathbb{F}_\ell^*)^2\) denotes the group of squares in \(\mathbb{F}_\ell^*\).
Proposition (A.)

Let $(\ell,j(E))$ be an exceptional pair for the number field $K$, and assume that $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \notin K$. Let $G$ be $\rho_{E,\ell}(\text{Gal}(\overline{\mathbb{Q}}/K))$ and let $H$ be its image in $\text{PGL}_2(\mathbb{F}_\ell)$. Let $\mathcal{C} \subset G$ be the preimage of the maximal cyclic subgroup of $H$. Then

$$\det(\mathcal{C}) \in (\mathbb{F}_\ell^*)^2.$$ 

where $(\mathbb{F}_\ell^*)^2$ denotes the group of squares in $\mathbb{F}_\ell^*$.

Proposition (A.)

Let $(\ell,j(E))$ be an exceptional pair for the number field $K$ with $\sqrt{\left(\frac{-1}{\ell}\right)} \ell$ not belonging to $K$. Then $E$ admits an $\ell$-isogeny over $K(\sqrt{-\ell})$ (and actually, two such isogenies).
Main Theorem (A.)

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) of degree \(d\) over \(\mathbb{Q}\), such that \(\sqrt{\left(-\frac{1}{\ell}\right)} \ell \not\in K\). Then \(\ell \equiv 3 \text{ mod } 4\) and

\[
7 \leq \ell \leq 6d + 1.
\]
Main Theorem (A.)

Let \((\ell, j(E))\) be an exceptional pair for the number field \(K\) of degree \(d\) over \(\mathbb{Q}\), such that \(\sqrt{\left(-\frac{1}{\ell}\right)} \not\in K\). Then \(\ell \equiv 3 \mod 4\) and

\[ 7 \leq \ell \leq 6d+1. \]

Remark

This theorem implies the result obtained by Sutherland in the case \(K = \mathbb{Q}\).
Let us assume that $\sqrt{\left(\frac{-1}{\ell}\right) \ell}$ belongs to $K$. 
Let us assume that $\sqrt{\left(\frac{-1}{\ell}\right) \ell}$ belongs to $K$.

**Lemma (A.)**

Let $G$ be a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ whose image $H$ in $\text{PGL}_2(\mathbb{F}_\ell)$ is contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. Then $\ell \equiv 1 \mod 4$ and one of the followings holds:

1. $H$ is dihedral of order $2n$, where $n \in \mathbb{Z}_{> 1}$ is a divisor of $\ell - 1$;
2. $H$ is isomorphic to one of the following exceptional groups: $A_4$, $S_4$ or $A_5$. 
**Corollary (A.)**

Let $G$ be a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ whose image $H$ in $\text{PGL}_2(\mathbb{F}_\ell)$ is contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. If $H$ is dihedral of order $2n$, where $n \in \mathbb{Z}_{>1}$ is a divisor of $\ell-1$, then $G$ is properly contained in the normalizer of a split Cartan subgroup and $\mathbb{P}^1(\mathbb{F}_\ell)/G$ contains an orbit of size 2.

**Corollary (A.)**

Let $G$ be a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ whose image $H$ in $\text{PGL}_2(\mathbb{F}_\ell)$ is contained in $\text{SL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Suppose $|\mathbb{P}^1(\mathbb{F}_\ell)^g| > 0$ for all $g \in G$ but $|\mathbb{P}^1(\mathbb{F}_\ell)^G| = 0$. Then:

- if $H$ is isomorphic to $A_4$ then $\ell \equiv 1 \text{ mod } 12$;
- if $H$ is isomorphic to $S_4$ then $\ell \equiv 1 \text{ mod } 24$;
- if $H$ is isomorphic to $A_5$ then $\ell \equiv 1 \text{ mod } 60$. 
Proposition (A.)

Let $E$ be an elliptic curve defined over a number field $K$ of degree $d$ over $\mathbb{Q}$ and let $\ell$ be a prime number. Let us suppose $\sqrt{\left(\frac{-1}{\ell}\right)} \ell \in K$. Suppose $E/K$ admits an $\ell$-isogeny locally at a set of primes with density one. Then:

1. If $\ell \equiv 3 \mod 4$ the elliptic curve $E$ admits a global $\ell$-isogeny over $K$;
2. If $\ell \equiv 1 \mod 4$ the elliptic curve $E$ admits an $\ell$-isogeny over $L$, finite extension of $K$, which can ramify only at primes dividing the conductor of $E$ and $\ell$. Moreover, if $\ell \equiv -1 \mod 3$ or if $\ell \geq 60d+1$, then $E$ admits an $\ell$-isogeny over a quadratic extension $L$ of $K$. 
**Question**

Let $K$ be a number field and let $\ell$ be a prime number, how many exceptional pairs $(\ell, j(E))$ do exist over $K$?
**Question**

Let $K$ be a number field and let $\ell$ be a prime number, how many exceptional pairs $(\ell, j(E))$ do exist over $K$?

**Proposition (A.)**

Let $(\ell, j(E))$ be an exceptional pair for the number field $K$ of degree $d$ over $\mathbb{Q}$ and discriminant $\Delta$. Then

$$\ell \leq \max \{\Delta, 6d+1\}.$$
Proposition (A.)

Given a number field $K$: 

If $\ell = 2, 3$ then there exists no exceptional pair; there exist infinitely many exceptional pairs $(5, j(E))$ for the number field $K$ if and only if $\sqrt{5}$ belongs to $K$; if $\ell > 7$, then the number of exceptional pairs $(\ell, j(E))$ is finite.
PROPOSITION (A.)

Given a number field $K$:

- if $\ell = 2, 3$ then there exists no exceptional pair;
Proposition (A.)

Given a number field $K$:

- if $\ell = 2, 3$ then there exists no exceptional pair;
- there exist infinitely many exceptional pairs $(5, j(E))$ for the number field $K$ if and only if $\sqrt{5}$ belongs to $K$;
Proposition (A.)

Given a number field $K$:

- if $\ell = 2, 3$ then there exists no exceptional pair;
- there exist infinitely many exceptional pairs $(5, j(E))$ for the number field $K$ if and only if $\sqrt{5}$ belongs to $K$;
- if $\ell > 7$, then the number of exceptional pairs $(\ell, j(E))$ is finite.
The local-global principle for 7-isogenies leads us to a dichotomy between a finite and an infinite number of counterexamples according to the rank of a specific elliptic curve that we call the Elkies-Sutherland curve:
The local-global principle for 7-isogenies leads us to a dichotomy between a finite and an infinite number of counterexamples according to the rank of a specific elliptic curve that we call the Elkies-Sutherland curve:

**Proposition (A.)**

If \( \ell = 7 \) then the number of exceptional pairs \((7, j(E))\) for a number field \(K\), is finite or infinite, depending on the rank of the elliptic curve

\[
E' : y^2 = x^3 - 1715x + 33614
\]

being respectively 0 or positive.
Further Directions

- Generalization for simple abelian varieties of dimension $d$ over $\mathbb{Q}$ which are principally polarized i.e. study of the subgroups of $\mathbb{P} \, \text{GSp}_d(\mathbb{F}_\ell)$...
- Generalization for abelian varieties of $\text{GL}_2$-type;
- Generalization for isogenies of prime power degree;
- Generalization for isogenies of degree given by products of primes;
- ...
Images of modular Galois representations mod $\ell$

Samuele Anni

Universiteit Leiden - Université Bordeaux 1

Leiden, ALGANT meeting;
23rd February 2013

Thanks!