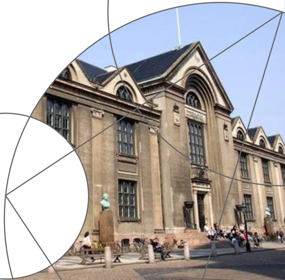
Department of Mathematical Sciences

Elliptic Curves and Galois Representations

Bachelor Defense

Rasmus Juhl Christensen
stud.scient.



Program

9.00-9.20: A presentation on the following topics:

1. Central definitions: Elliptic curves and Galois representations
2. Galois representations attached to elliptic curves
3. Elliptic curves with complex multiplication
4. Serre's open image theorem
5. Elliptic curves defined over $\mathbb{Q}$
6. A criterion for surjectivity of adelic Galois representations attached to elliptic curves
7. An example:
   A method to prove surjectivity of some ℓ-adic Galois representations attached to elliptic curves

9.20: Questions.

Elliptic curves

Let K be a perfect field. We define an elliptic curve in the following way:

Definition (Elliptic curve)

Let $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in K[x,y]$ satisfy that there exists no $P \in \bar{K}^2$, such that $f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$. Then we say f defines the affine elliptic curve E/K by

$$E(\bar{K}) = \{P \in \bar{K}^2 \mid f(P) = 0\}$$

Let $F(X,Y,Z) = Z^3 \cdot f(X/Z, Y/Z) \in K[X,Y,Z]$. Then the set

$$\begin{aligned} &\{P \in \mathbb{P}^2(\bar{K}) \mid F(P) = 0\} \\ =&\{[x_0 : y_0 : 1] \in \mathbb{P}^2(\bar{K}) \mid (x_0, y_0) \in E(\bar{K})\} \cup \{[0:1:0]\} \end{aligned}$$

is the projective elliptic curve E/K. We define $\mathcal{O} := [0:1:0]$

The group law

Then we define the group law on elliptic curves:

Theorem

Let E/K be an elliptic curve, $P = (x_1, y_1), Q = (x_2, y_2) \in E(K)$. If $x_1 \neq x_2$, define $\lambda := \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu := \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$. If $P = Q$ and $\frac{\partial f}{\partial y}(P) \neq 0$, define

$$\lambda := -\frac{\frac{\partial f}{\partial x}(P)}{\frac{\partial f}{\partial y}(P)}, \quad \nu := y_1 - \lambda x_1$$

Then we let:

$$\begin{aligned} P + Q := \big(&\lambda^2 + a_1\lambda - a_2 - 2x_1, \\ &-(\lambda + a_1)(\lambda^2 + a_1\lambda - a_2 - 2x_1) - \nu - a_3\big) \end{aligned}$$

Else let $P + Q = \mathcal{O}$. Then $(E(K) \cup \{\mathcal{O}\}, +)$ is an abelian group with $\mathcal{O}$ as the identity.

Torsion points

Definition

Let E/K be an elliptic curve, and let $n \in \mathbb{N}$. Then for $P \in E(\bar{K})$, we define

$$nP := \underbrace{P + \cdots + P}_{n \text{ times}}$$

and we define

$$E[n] := \{P \in E(\bar{K}) \mid nP = \mathcal{O}\}$$

Torsion points

Definition

Let E/K be an elliptic curve, and let $n \in \mathbb{N}$. Then for $P \in E(\bar{K})$, we define

$$nP := \underbrace{P + \cdots + P}_{n \text{ times}}$$

and we define

$$E[n] := \{P \in E(\bar{K}) \mid nP = \mathcal{O}\}$$

Theorem

Let E/K be an elliptic curve, $n \in \mathbb{N}$ coprime with char K *if* char $K \neq 0$. *Then*

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Galois representations

Definition

Let E/F be Galois with Galois group $\mathrm{Gal}(E/F)$, let R be a topological ring and let $n \in \mathbb{N}$. Then a Galois representation is a continuous homomorphism

$$\rho : \mathrm{Gal}(E/F) \to \mathrm{GL}_n(R)$$

Galois representations

Definition

Let E/F be Galois with Galois group $\mathrm{Gal}(E/F)$, let R be a topological ring and let $n \in \mathbb{N}$. Then a Galois representation is a continuous homomorphism

$$\rho : \mathrm{Gal}(E/F) \to \mathrm{GL}_n(R)$$

Definition (Serre, McGill: Abelian ℓ-adic Representations and Elliptic curves)

Let ℓ be a prime. If V is a vector space over $\mathbb{Q}_\ell$ of degree n, and K is a field with separable algebraic closure K_s, then an ℓ-adic representation of $G := \mathrm{Gal}(K_s/K)$ is a continuous homomorphism

$$\rho : G \to \mathrm{Aut}(V)\,(\cong \mathrm{GL}_n(\mathbb{Q}_\ell))$$

Galois representations attached to elliptic curves

Let K be a perfect field, let $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic extension. Let E/K be an elliptic curve and let $n \in \mathbb{N}$ be coprime with char K if char $K \neq 0$.

Galois representations attached to elliptic curves

Let K be a perfect field, let $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic extension. Let E/K be an elliptic curve and let $n \in \mathbb{N}$ be coprime with char K if char $K \neq 0$.

Now let $g \in G_K$ act on $P = (x_0, y_0)$ by $gP = (gx_0, gy_0)$, $g\mathcal{O} = \mathcal{O}$. From the group law, we get $g(mP) = mg(P)$, and so we get

$$\rho'_{E,n} : G_K \to \mathrm{Aut}(E[n])$$

Galois representations attached to elliptic curves

Let K be a perfect field, let $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic extension. Let E/K be an elliptic curve and let $n \in \mathbb{N}$ be coprime with char K if char $K \neq 0$.

Now let $g \in G_K$ act on $P = (x_0, y_0)$ by $gP = (gx_0, gy_0)$, $g\mathcal{O} = \mathcal{O}$. From the group law, we get $g(mP) = mg(P)$, and so we get

$$\rho'_{E,n} : G_K \to \mathrm{Aut}(E[n])$$

Recall $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. Hence, we can pick a basis (P, Q) of $E[n]$ and get a mod n Galois representation:

$$\rho_{E,n} : G_K \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

Now fix a prime $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$. Picking a compatible system of bases, we can then draw the commutative diagram

Now fix a prime $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$. Picking a compatible system of bases, we can then draw the commutative diagram

$$
\begin{tikzcd}
 & \mathrm{Gal}(\bar{K}/K) \arrow[dl, "\rho'_{E,\ell}"'] \arrow[d, "\rho'_{E,\ell^2}"] \arrow[dr] & \\
\mathrm{Aut}(E[\ell]) \arrow[d, "\wr"] & \mathrm{Aut}(E[\ell^2]) \arrow[l, "\mathrm{res}"] \arrow[d, "\wr"] & \cdots \arrow[l] \arrow[d, "\wr"] \\
\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) & \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z}) \arrow[l, "(\mathrm{mod}\ \ell)"] & \cdots \arrow[l]
\end{tikzcd}
$$

Now fix a prime $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$. Picking a compatible system of bases, we can then draw the commutative diagram

$$\begin{tikzcd}
 & \mathrm{Gal}(\bar{K}/K) \arrow[dl, "\rho'_{E,\ell}"'] \arrow[d, "\rho'_{E,\ell^2}"] \arrow[dr] & \\
\mathrm{Aut}(E[\ell]) \arrow[d, "\wr"] & \mathrm{Aut}(E[\ell^2]) \arrow[l, "\mathrm{res}"] \arrow[d, "\wr"] & \cdots \arrow[l] \arrow[d, "\wr"] \\
\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) & \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z}) \arrow[l, "(\mathrm{mod}\ \ell)"] & \cdots \arrow[l]
\end{tikzcd}$$

Taking inverse limits and defining $T_\ell[E] = \varprojlim_{n\in\mathbb{N}} E[\ell^n]$, we get a ℓ-adic Galois representation.

Now fix a prime $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$. Picking a compatible system of bases, we can then draw the commutative diagram

$$\begin{tikzcd}
& \mathrm{Gal}(\bar{K}/K) \arrow[dl, "\rho'_{E,\ell}"] \arrow[d, "\rho'_{E,\ell^2}"] \arrow[dr] \arrow[drr, "\rho'_{E,\ell^\infty}"] & & \\
\mathrm{Aut}(E[\ell]) \arrow[d, "\wr"] & \mathrm{Aut}(E[\ell^2]) \arrow[l, "\mathrm{res}"'] \arrow[d, "\wr"] & \cdots \arrow[l] \arrow[d, "\wr"] & \mathrm{Aut}(T_\ell[E]) \arrow[d, "\wr"] \\
\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) & \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z}) \arrow[l, "(\mathrm{mod}\ \ell)"'] & \cdots \arrow[l] & \mathrm{GL}_2(\mathbb{Z}_\ell)
\end{tikzcd}$$

Taking inverse limits and defining $T_\ell[E] = \varprojlim_{n \in \mathbb{N}} E[\ell^n]$, we get a ℓ-adic Galois representation.

Now fix a prime $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$. Picking a compatible system of bases, we can then draw the commutative diagram

$$
\begin{tikzcd}
 & \mathrm{Gal}(\bar{K}/K) \arrow[dl, "\rho'_{E,\ell}"'] \arrow[d, "\rho'_{E,\ell^2}"] \arrow[dr] \arrow[drr, "\rho'_{E,\ell^\infty}"] & & \\
\mathrm{Aut}(E[\ell]) \arrow[d, "\wr"] & \mathrm{Aut}(E[\ell^2]) \arrow[l, "\mathrm{res}"] \arrow[d, "\wr"] & \cdots \arrow[l] \arrow[d, "\wr"] & \mathrm{Aut}(T_\ell[E]) \arrow[d, "\wr"] \\
\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) & \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z}) \arrow[l, "(\mathrm{mod}\ \ell)"] & \cdots \arrow[l] & \mathrm{GL}_2(\mathbb{Z}_\ell)
\end{tikzcd}
$$

Taking inverse limits and defining $T_\ell[E] = \varprojlim_{n\in\mathbb{N}} E[\ell^n]$, we get a ℓ-adic Galois representation. If $\operatorname{char} K = 0$, then for a compatible system of bases, we may pack the ℓ-adic Galois representations for all primes ℓ into a single adelic Galois representation via $\mathrm{Aut}(\prod_p T_p[E])$:

$$\rho_E : G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}})$$

Now fix a prime $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$. Picking a compatible system of bases, we can then draw the commutative diagram

$$
\begin{tikzcd}
 & & \mathrm{Gal}(\bar{K}/K) \arrow[dll] \arrow[d, "\rho'_{E,\ell^2}"] \arrow[dl, phantom, "\rho'_{E,\ell}"] \arrow[dr] \arrow[drr, "\rho'_{E,\ell^\infty}"] & & \\
\mathrm{Aut}(E[\ell]) \arrow[d, "\wr"] & & \mathrm{Aut}(E[\ell^2]) \arrow[ll, "\mathrm{res}"'] \arrow[d, "\wr"] & \cdots \arrow[l] \arrow[d, "\wr"] & \mathrm{Aut}(T_\ell[E]) \arrow[d, "\wr"] \\
\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) & & \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z}) \arrow[ll, "(\mathrm{mod}\ \ell)"'] & \cdots \arrow[l] & \mathrm{GL}_2(\mathbb{Z}_\ell)
\end{tikzcd}
$$

Taking inverse limits and defining $T_\ell[E] = \varprojlim_{n\in\mathbb{N}} E[\ell^n]$, we get a ℓ-adic Galois representation. If $\operatorname{char} K = 0$, then for a compatible system of bases, we may pack the ℓ-adic Galois representations for all primes ℓ into a single adelic Galois representation via $\mathrm{Aut}(\prod_p T_p[E])$:

$$\rho_E : G_K \to \mathrm{GL}_2(\hat{\mathbb{Z}})$$

These representations are only defined up to conjugation. Also, we can recover the mod m and the ℓ-adic Galois representation via projections $r_m : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, $\pi_\ell : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$.

Complex multiplication

Let K be a perfect field, let ℓ be a prime such that $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$.

Complex multiplication

Let K be a perfect field, let ℓ be a prime such that $\ell \neq \text{char}\, K$ if $\text{char}\, K \neq 0$.

Definition

Let E/K be an elliptic curve. Then $\psi : E(\bar{K}) \to E(\bar{K})$ is an endomorphism over K if $\psi = [g_0 : g_1 : g_2]$ with $g_0, g_1, g_2 \in K(E)$ regular (defined at each $P \in E(\bar{K})$) and $\psi(\mathcal{O}) = \mathcal{O}$.

Complex multiplication

Let K be a perfect field, let ℓ be a prime such that $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$.

Definition

Let E/K be an elliptic curve. Then $\psi : E(\bar{K}) \to E(\bar{K})$ is an endomorphism over K if $\psi = [g_0 : g_1 : g_2]$ with $g_0, g_1, g_2 \in K(E)$ regular (defined at each $P \in E(\bar{K})$) and $\psi(\mathcal{O}) = \mathcal{O}$.

Any endomorphism ψ of E/K satisfies

$$\psi(P + Q) = \psi(P) + \psi(Q)$$

for all $P, Q \in E(\bar{K})$.

Complex multiplication

Let K be a perfect field, let ℓ be a prime such that $\ell \neq \operatorname{char} K$ if $\operatorname{char} K \neq 0$.

Definition

Let E/K be an elliptic curve. Then $\psi : E(\bar{K}) \to E(\bar{K})$ is an endomorphism over K if $\psi = [g_0 : g_1 : g_2]$ with $g_0, g_1, g_2 \in K(E)$ regular (defined at each $P \in E(\bar{K})$) and $\psi(\mathcal{O}) = \mathcal{O}$.

Any endomorphism ψ of E/K satisfies

$$\psi(P + Q) = \psi(P) + \psi(Q)$$

for all $P, Q \in E(\bar{K})$.

An endomorphism over K of an elliptic curve E/K induces an endomorphism of $T_\ell[E]$ commuting with the endomorphisms induced by G_K. We have $\operatorname{End}(T_\ell[E]) \cong M_2(\mathbb{Z}_\ell)$, and so multiplication by m maps for $m \in \mathbb{N}$ are endomorphisms with action on $T_\ell[E]$ represented by

$$\begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}$$

Definition

Let E/K be an elliptic curve. If there exists an endomorphism of E over K that is not a multiplication by m map, then we shall say E has complex multiplication.

Definition

Let E/K be an elliptic curve. If there exists an endomorphism of E over K that is not a multiplication by m map, then we shall say E has complex multiplication.

The following statements are then true:

Definition

Let E/K be an elliptic curve. If there exists an endomorphism of E over K that is not a multiplication by m map, then we shall say E has complex multiplication.

The following statements are then true:

Theorem

If E/K has complex multiplication, there exists a non-scalar matrix that commutes with $\rho_{E,\ell^\infty}(G_K)$ and $\rho_{E,\ell^\infty}(G_K)$ is abelian. Hence $\rho_{E,\ell^\infty}(G_K)$ is of infinite index in $GL_2(\mathbb{Z}_\ell)$ and in particular ρ_{E,ℓ^∞} is not surjective.

Definition

Let E/K be an elliptic curve. If there exists an endomorphism of E over K that is not a multiplication by m map, then we shall say E has complex multiplication.

The following statements are then true:

Theorem

If E/K has complex multiplication, there exists a non-scalar matrix that commutes with $\rho_{E,\ell^\infty}(G_K)$ and $\rho_{E,\ell^\infty}(G_K)$ is abelian. Hence $\rho_{E,\ell^\infty}(G_K)$ is of infinite index in $GL_2(\mathbb{Z}_\ell)$ and in particular ρ_{E,ℓ^∞} is not surjective.

If E/K has complex multiplication over any field L with L/K a finite extension, then ρ_{E,ℓ^∞} is then not surjective.

Definition

Let E/K be an elliptic curve. If there exists an endomorphism of E over K that is not a multiplication by m map, then we shall say E has complex multiplication.

The following statements are then true:

Theorem

If E/K has complex multiplication, there exists a non-scalar matrix that commutes with $\rho_{E,\ell^\infty}(G_K)$ and $\rho_{E,\ell^\infty}(G_K)$ is abelian. Hence $\rho_{E,\ell^\infty}(G_K)$ is of infinite index in $GL_2(\mathbb{Z}_\ell)$ and in particular ρ_{E,ℓ^∞} is not surjective.

If E/K has complex multiplication over any field L with L/K a finite extension, then ρ_{E,ℓ^∞} is then not surjective.

If $\operatorname{char} K = 0$, and E/K has complex multiplication over any field L with L/K an algebraic extension, then ρ_E is not surjective. Also, $\rho_E(G_K)$ is not open in $GL_2(\hat{\mathbb{Z}})$

Serre's open image theorem

Let K be a number field, $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic field extension.

Theorem (Serre's open image theorem)

Let E/K be an elliptic curve without complex multiplication. Then the image of ρ_E in $GL_2(\hat{\mathbb{Z}})$ is open.

Serre's open image theorem

Let K be a number field, $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic field extension.

Theorem (Serre's open image theorem)

Let E/K be an elliptic curve without complex multiplication. Then the image of ρ_E in $GL_2(\hat{\mathbb{Z}})$ is open.

This has the following equivalent formulations:

Serre's open image theorem

Let K be a number field, $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic field extension.

Theorem (Serre's open image theorem)

Let E/K be an elliptic curve without complex multiplication. Then the image of ρ_E in $GL_2(\hat{\mathbb{Z}})$ is open.

This has the following equivalent formulations:

- For all but finitely many primes ℓ, ρ_{E,ℓ^∞} is surjective.

Serre's open image theorem

Let K be a number field, $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic field extension.

Theorem (Serre's open image theorem)

Let E/K be an elliptic curve without complex multiplication. Then the image of ρ_E in $GL_2(\hat{\mathbb{Z}})$ is open.

This has the following equivalent formulations:

- For all but finitely many primes ℓ, ρ_{E,ℓ^∞} is surjective.
- For all but finitely many primes ℓ, $\rho_{E,\ell}$ is surjective.

Serre's open image theorem

Let K be a number field, $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic field extension.

Theorem (Serre's open image theorem)

Let E/K be an elliptic curve without complex multiplication. Then the image of ρ_E in $GL_2(\hat{\mathbb{Z}})$ is open.

This has the following equivalent formulations:

- For all but finitely many primes ℓ, ρ_{E,ℓ^∞} is surjective.
- For all but finitely many primes ℓ, $\rho_{E,\ell}$ is surjective.
- There exists $m \in \mathbb{N}$, such that

$$\{A \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \mid r_m(A) = I\} \subseteq \rho_E(G_K)$$

Serre's open image theorem

Let K be a number field, $G_L = \mathrm{Gal}(\bar{K}/L)$ for L/K an algebraic field extension.

Theorem (Serre's open image theorem)

Let E/K be an elliptic curve without complex multiplication. Then the image of ρ_E in $GL_2(\hat{\mathbb{Z}})$ is open.

This has the following equivalent formulations:

- For all but finitely many primes ℓ, ρ_{E,ℓ^∞} is surjective.
- For all but finitely many primes ℓ, $\rho_{E,\ell}$ is surjective.
- There exists $m \in \mathbb{N}$, such that

$$\{A \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \mid r_m(A) = I\} \subseteq \rho_E(G_K)$$

- There exists $m \in \mathbb{N}$, such that

$$\rho_E(G_K) = r_m^{-1}(\rho_{E,m}(G_K))$$

Surjectivity of adelic Galois representations attached to elliptic cruves

We can prove the following statements:

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. Then ρ_E is not surjective.

And the more general version:

Theorem (Greicius 2010)

Let E/K be an elliptic curve over a number field K. Let $\Delta \in K^\times$ be the discriminant of any Weierstrass model of E/K. Then ρ_E is surjective if and only if

1. *the ℓ-adic Galois representation $\rho_{\ell^\infty} : G_K \to GL_2(\mathbb{Z}_\ell)$ is surjective for all ℓ,*
2. $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ *and*
3. $\sqrt{\Delta} \notin K(\zeta_\infty)$

Determining if adelic Galois representations attached to elliptic curves are surjective

We will be pursuing the following steps to find an elliptic curve with surjective adelic Galois representation:

Determining if adelic Galois representations attached to elliptic curves are surjective

We will be pursuing the following steps to find an elliptic curve with surjective adelic Galois representation:

1. Determining if $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ and if $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.

Determining if adelic Galois representations attached to elliptic curves are surjective

We will be pursuing the following steps to find an elliptic curve with surjective adelic Galois representation:

1. Determining if $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ and if $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.
2. Reducing the set of primes, that could be *exceptional*, to a finite set.

Determining if adelic Galois representations attached to elliptic curves are surjective

We will be pursuing the following steps to find an elliptic curve with surjective adelic Galois representation:

1. Determining if $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ and if $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.
2. Reducing the set of primes, that could be *exceptional*, to a finite set.
3. Determining whether the ℓ-adic Galois representations for each prime in the finite set is surjective.

Determining if adelic Galois representations attached to elliptic curves are surjective

We will be pursuing the following steps to find an elliptic curve with surjective adelic Galois representation:

1. Determining if $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ and if $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.
2. Reducing the set of primes, that could be *exceptional*, to a finite set.
3. Determining whether the ℓ-adic Galois representations for each prime in the finite set is surjective.

We will deal with the first two steps ad hoc. Reflecting the difficulty of the second step, we have the following unsolved problem:

Determining if adelic Galois representations attached to elliptic curves are surjective

We will be pursuing the following steps to find an elliptic curve with surjective adelic Galois representation:

1. Determining if $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ and if $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.
2. Reducing the set of primes, that could be *exceptional*, to a finite set.
3. Determining whether the ℓ-adic Galois representations for each prime in the finite set is surjective.

We will deal with the first two steps ad hoc. Reflecting the difficulty of the second step, we have the following unsolved problem:

Uniformity conjecture (Serre): *For every number field K, there exists some prime p, such that for every elliptic curve E/K and prime $\ell > p$, ρ_{E,ℓ^∞} is surjective.*

For $K = \mathbb{Q}$, $p = 37$ is conjectured to be such a number.

Surjectivity of ℓ-adic Galois representations attached to elliptic curves

Once again, let K be a number field.

We can reduce the final step to a manageable problem by the following theorem:

Surjectivity of ℓ-adic Galois representations attached to elliptic curves

Once again, let K be a number field.

We can reduce the final step to a manageable problem by the following theorem:

Theorem

Assume $\ell \geq 5$ is a prime, E/K an elliptic curve and $\det : \rho_{E,\ell^\infty}(G_K) \to \mathbb{Z}_\ell^\times$ is surjective. Then $\rho_{E,\ell}$ is surjective if and only if ρ_{E,ℓ^∞} is surjective.
Further, $\rho_{E,8}$ surjective if and only if $\rho_{E,2^\infty}$ is surjective and $\rho_{E,9}$ is surjective if and only if $\rho_{E,3^\infty}$ is surjective.

Surjectivity of ℓ-adic Galois representations attached to elliptic curves

Once again, let K be a number field.

We can reduce the final step to a manageable problem by the following theorem:

Theorem

Assume $\ell \geq 5$ is a prime, E/K an elliptic curve and $\det : \rho_{E,\ell^\infty}(G_K) \to \mathbb{Z}_\ell^\times$ is surjective. Then $\rho_{E,\ell}$ is surjective if and only if ρ_{E,ℓ^∞} is surjective.
Further, $\rho_{E,8}$ surjective if and only if $\rho_{E,2^\infty}$ is surjective and $\rho_{E,9}$ is surjective if and only if $\rho_{E,3^\infty}$ is surjective.

Since the subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ are classified stemming back to a book by Dickson from 1901, we may actually derive a sufficient condition for primes $p \geq 5$:

Theorem

Let $\ell \geq 5$ and suppose $H \leq GL_2(\mathbb{F}_\ell)$ contains

1. *s such that $\mathrm{Tr}(s)^2 - 4\det s$ is a non-zero square in $\mathbb{F}_\ell$ and so that $\mathrm{Tr}(s) \neq 0$*
2. *s' such that $\mathrm{Tr}(s')^2 - 4\det s'$ is not a square in $\mathbb{F}_\ell$ and so that $\mathrm{Tr}(s') \neq 0$*
3. *s'' such that $u = \mathrm{Tr}(s'')^2/\det(s'') \neq 0, 1, 2, 4$ and such that $u^2 - 3u + 1 \neq 0$*

Then H contains $SL_2(\mathbb{F}_\ell)$. If further $\det : H \to \mathbb{F}_\ell^\times$ is surjective, $H = GL_2(\mathbb{F}_\ell)$.

Choose a model of E with coefficients in $\mathcal{O}_K$.

Theorem

Let $\mathfrak{p} \nmid \ell$ be a prime ideal in $\mathcal{O}_K$ with $\Delta_E \not\equiv 0 \pmod{\mathfrak{p}}$. Let $t_\mathfrak{p}$ be the trace of the Frobenius map of $\tilde{E}_\mathfrak{p}$ (the reduction of E modulo $\mathfrak{p}$) and $q_\mathfrak{p}$ the determinant. There exists $g \in G_K$ such that
$$t_\mathfrak{p} \equiv \mathrm{Tr}\,\rho_{E,\ell}(g) \pmod{\ell}, \quad q_\mathfrak{p} \equiv \det \rho_{E,\ell}(g) \pmod{\ell}$$

An example

We will now consider an elliptic curve with surjective adelic Galois representation.

An example

We will now consider an elliptic curve with surjective adelic Galois representation.So let α be the real root of $x^3 + x + 1$, let $K = \mathbb{Q}(\alpha)$ and let E/K be the elliptic curve defined by $y^2 + 2xy + \alpha y = x^3 - x^2$.

An example

We will now consider an elliptic curve with surjective adelic Galois representation.So let α be the real root of $x^3 + x + 1$, let $K = \mathbb{Q}(\alpha)$ and let E/K be the elliptic curve defined by $y^2 + 2xy + \alpha y = x^3 - x^2$.

1. A check shows that $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ and $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.

An example

We will now consider an elliptic curve with surjective adelic Galois representation.So let α be the real root of x^3+x+1, let $K=\mathbb{Q}(\alpha)$ and let E/K be the elliptic curve defined by $y^2+2xy+\alpha y=x^3-x^2$.

1. A check shows that $K\cap\mathbb{Q}(\zeta_\infty)=\mathbb{Q}$ and $\sqrt{\Delta_E}\notin K(\zeta_\infty)$.
2. It is possible to prove that for any prime ℓ unramified in K, and prime ideal $\mathfrak{p}$ for which $\Delta_E\not\equiv 0 \pmod{\mathfrak{p}}$ (and further $\ell\nmid v_{\mathfrak{p}}(j_E)$ if $\ell=2,3,5$) , then $\ell\mid\#\tilde{E}_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p})$ if $\rho_{E,\ell}(G_K)\neq\mathrm{GL}_2(\mathbb{F}_\ell)$. Using primes (2) and $(\alpha^2+\alpha+2)$, we get $\ell\mid 9,10$ if $\ell\neq 2,3,31$ and $\rho_{E,\ell}(G_K)\neq\mathrm{GL}_2(\mathbb{F}_\ell)$.

An example

We will now consider an elliptic curve with surjective adelic Galois representation.So let α be the real root of x^3+x+1, let $K=\mathbb{Q}(\alpha)$ and let E/K be the elliptic curve defined by $y^2+2xy+\alpha y=x^3-x^2$.

1. A check shows that $K \cap \mathbb{Q}(\zeta_\infty)=\mathbb{Q}$ and $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.
2. It is possible to prove that for any prime ℓ unramified in K, and prime ideal $\mathfrak{p}$ for which $\Delta_E \not\equiv 0 \pmod{\mathfrak{p}}$ (and further $\ell \nmid v_{\mathfrak{p}}(j_E)$ if $\ell=2,3,5$) , then $\ell \mid \#\tilde{E}_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p})$ if $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$. Using primes (2) and $(\alpha^2+\alpha+2)$, we get $\ell \mid 9, 10$ if $\ell \neq 2,3,31$ and $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$.
3. In the case $\ell=31$, we can find elements with traces and determinants satisfying the conditions listed needed to prove $\rho_{E,31}=\mathrm{GL}_2(\mathbb{F}_31)$ as outlined in the previous slide. This can be done by using the method involving Frobenius maps at the primes (7) and $(\alpha-2)$.

An example

We will now consider an elliptic curve with surjective adelic Galois representation.So let α be the real root of $x^3 + x + 1$, let $K = \mathbb{Q}(\alpha)$ and let E/K be the elliptic curve defined by $y^2 + 2xy + \alpha y = x^3 - x^2$.

1. A check shows that $K \cap \mathbb{Q}(\zeta_\infty) = \mathbb{Q}$ and $\sqrt{\Delta_E} \notin K(\zeta_\infty)$.
2. It is possible to prove that for any prime ℓ unramified in K, and prime ideal $\mathfrak{p}$ for which $\Delta_E \not\equiv 0 \pmod{\mathfrak{p}}$ (and further $\ell \nmid v_{\mathfrak{p}}(j_E)$ if $\ell = 2, 3, 5$) , then $\ell \mid \#\tilde{E}_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p})$ if $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$. Using primes (2) and $(\alpha^2 + \alpha + 2)$, we get $\ell \mid 9, 10$ if $\ell \neq 2, 3, 31$ and $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$.
3. In the case $\ell = 31$, we can find elements with traces and determinants satisfying the conditions listed needed to prove $\rho_{E,31} = \mathrm{GL}_2(\mathbb{F}_31)$ as outlined in the previous slide. This can be done by using the method involving Frobenius maps at the primes (7) and $(\alpha - 2)$.
   Similar but more technical arguments can be used to deal with the cases $\ell = 2, 3$.

Questions

Questions

Questions