Galois Representations Attached to Elliptic Curves with Complex Multiplication

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

June 28^{th}
BU/Keio Workshop
Boston University

WORKSHOP 2019

Galois Representations Attached to Elliptic Curves with Complex Multiplication

Álvaro Lozano-Robledo
University of Connecticut

§1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve, and let $T_2(E) = \varprojlim E[2^n]$ be the Tate module. The Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_2(E)$ induces

$$\rho_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_2(E)) \cong \mathrm{GL}(2, \mathbb{Z}_2).$$

Let $E/\mathbb{Q}$ be an elliptic curve, and let $T_2(E) = \varprojlim E[2^n]$ be the Tate module. The Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_2(E)$ induces

$$\rho_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_2(E)) \cong \mathrm{GL}(2, \mathbb{Z}_2).$$

Theorem (Rouse and Zureick-Brown, 2014)

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely 1208 possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further, the representation $\rho_{E,2}$ is defined (at most) modulo 32.

Zagreb (Croatia), June 25-29, 2018.

Zagreb (Croatia), June 25-29, 2018.

Example

For instance, let

$$E : y^2 + xy = x^3 + 210x + 900.$$

Then, the 2-adic image is `X235l` in the notation of the RZB database, which is defined modulo 16, and is generated in $\mathrm{GL}(2, \mathbb{Z}/16\mathbb{Z})$ by

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 12 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 14 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 15 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 8 & 9 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}$$

Note: their matrices act on vectors on the right, so this curve has a rational 16-isogeny.

Example

For instance, let

$$E : y^2 + xy = x^3 + 210x + 900.$$

Then, the 2-adic image is `X235l` in the notation of the RZB database, which is defined modulo 16, and is generated in $\mathrm{GL}(2, \mathbb{Z}/16\mathbb{Z})$ by

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 12 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 14 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 15 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 8 & 9 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}$$

Note: their matrices act on vectors on the right, so this curve has a rational 16-isogeny.

The Rouse–Zureick-Brown classification of 2-adic Galois representations has many interesting arithmetic applications.

Torsion points defined over abelian extensions

Theorem (Ribet, 1981)

Let $A/\mathbb{Q}$ be an abelian variety and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $A(\mathbb{Q}^{ab})_{tors}$ is finite.

Torsion points defined over abelian extensions

Theorem (Ribet, 1981)

Let $A/\mathbb{Q}$ be an abelian variety and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $A(\mathbb{Q}^{ab})_{tors}$ is finite.

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve.

1. *If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4,$ or 5.*

Torsion points defined over abelian extensions

Theorem (Ribet, 1981)

Let $A/\mathbb{Q}$ be an abelian variety and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $A(\mathbb{Q}^{ab})_{tors}$ is finite.

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve.

1. *If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4$, or 5.*
2. *More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6$, or 8.*

Torsion points defined over abelian extensions

Theorem (Ribet, 1981)

Let $A/\mathbb{Q}$ be an abelian variety and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $A(\mathbb{Q}^{ab})_{tors}$ is finite.

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve.

1. *If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4,$ or 5.*
2. *More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6,$ or 8.*
3. *Moreover, $G_n = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to one of 11 abelian groups.*

Torsion points defined over abelian extensions

Theorem (Ribet, 1981)

Let $A/\mathbb{Q}$ be an abelian variety and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $A(\mathbb{Q}^{ab})_{tors}$ is finite.

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve.

1. *If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4,$ or 5.*
2. *More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6,$ or 8.*
3. *Moreover, $G_n = \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to one of 11 abelian groups.*
4. *If $E/\mathbb{Q}$ has CM, and $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2,$ or 3. If $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3,$ or 4.*


We're inseparable

Torsion points defined over abelian extensions

Theorem (Chou, 2018)

Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Then, $\#E(\mathbb{Q}^{ab})_{tors} \leq 163$. This bound is sharp, as the CM curve `26569a1` has a point of order 163 over $\mathbb{Q}^{ab}$. Moreover, a full classification of the possible torsion subgroups is given.


$F_p(t)$
$F_p(t^p)$
We're inseparable

Minimal field of definition of 2^n-torsion points

Let $E/\mathbb{Q}$ be an elliptic curve. By Mazur's theorem, there might be an 8-torsion point over $\mathbb{Q}$, but no 16-torsion points over $\mathbb{Q}$.

Minimal field of definition of 2^n-torsion points

Let $E/\mathbb{Q}$ be an elliptic curve. By Mazur's theorem, there might be an 8-torsion point over $\mathbb{Q}$, but no 16-torsion points over $\mathbb{Q}$.

Question

What is the smallest degree $d_n \geq 2$ such that there is an elliptic curve $E/\mathbb{Q}$ and a field F_n of degree $d_n = [F_n : \mathbb{Q}]$, such that $E(F_n)[2^n]$ contains a point of exact order 2^n?

Minimal field of definition of 2^n-torsion points

Let $E/\mathbb{Q}$ be an elliptic curve. By Mazur's theorem, there might be an 8-torsion point over $\mathbb{Q}$, but no 16-torsion points over $\mathbb{Q}$.

Question

What is the smallest degree $d_n \geq 2$ such that there is an elliptic curve $E/\mathbb{Q}$ and a field F_n of degree $d_n = [F_n : \mathbb{Q}]$, such that $E(F_n)[2^n]$ contains a point of exact order 2^n?

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let $P \in E[2^n]$ be a point of exact order 2^n, with $n \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2n-7}. Moreover, this bound is best possible.

For example, the curve $E : y^2 + xy = x^3 + 210x + 900$, with the 2-adic image `X235l`, has a point P_n, for every $n \geq 4$, that achieves the bound.

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let $P \in E[2^n]$ be a point of exact order 2^n, with $n \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2n-7}. Moreover, this bound is best possible.

Theorem (González-Jiménez, L-R., 2015)

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let $P \in E[2^n]$ be a point of exact order 2^n, with $n \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2n-7}. Moreover, this bound is best possible.

What about elliptic curves with CM?

The CM case

Let

- K be an imaginary quadratic field, discriminant Δ_K, integers $\mathcal{O}_K$,
- $f \geq 1$, and $\mathcal{O}_{K,f}$ the order of K of conductor f,
- $j_{K,f} = j(\mathcal{O}_{K,f})$ its j-invariant.
- $E/\mathbb{Q}(j_{K,f})$ an elliptic curve with CM by $\mathcal{O}_{K,f}$.

The CM case

Let

- K be an imaginary quadratic field, discriminant Δ_K, integers $\mathcal{O}_K$,
- $f \geq 1$, and $\mathcal{O}_{K,f}$ the order of K of conductor f,
- $j_{K,f} = j(\mathcal{O}_{K,f})$ its j-invariant.
- $E/\mathbb{Q}(j_{K,f})$ an elliptic curve with CM by $\mathcal{O}_{K,f}$.

Theorem (Bourdon and Clark, 2016)

Let $N \geq 2$. There is an explicit integer $T(\mathcal{O}_{K,f}, N)$ such that if P is a point on E of exact order N, then $[K(j_f, P) : K(j_f)]$ is divisible by $T(\mathcal{O}_{K,f}, N)$.

$F_p(t)$
$F_p(t^p)$
We're inseparable


We're inseparable

Example

When $N = 2^n$, and $E/\mathbb{Q}$, the explicit formulas say that the smallest value of $T(\mathcal{O}_{K,f}, 2^n)$ occurs when $2 \mid \Delta_K$ and $2 \mid f$.

Example

When $N = 2^n$, and $E/\mathbb{Q}$, the explicit formulas say that the smallest value of $T(\mathcal{O}_{K,f}, 2^n)$ occurs when $2 \mid \Delta_K$ and $2 \mid f$. Thus, $\Delta_K = -4$ or -8, and $f \geq 2$, and $T(\mathcal{O}_{K,f}, 2^n) = 2^{2n-5}$ for $n > 3$.

For example, $E/\mathbb{Q} : y^2 = x^3 - 11x + 14$ has CM by $\mathbb{Z}[2i]$, and if $P \in E$ has exact order 2^n, for $n \geq 2$, then $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2n-4} (and equality holds for some such P).

Example

When $N = 2^n$, and E/K, we can achieve $[K(P) : K] = T(\mathcal{O}_{K,f}, 2^n) = 2^{2n-5}$.

Example

When $N = 2^n$, and E/K, we can achieve $[K(P) : K] = T(\mathcal{O}_{K,f}, 2^n) = 2^{2n-5}$.

For example, let $K = \mathbb{Q}(\sqrt{-2})$, let $f = 2$, and let $\mathcal{O}_{K,f} = \mathbb{Z}[2\sqrt{-2}]$. In this case $j_f = 26125000 + 18473000\sqrt{2}$. Let

$$E/K : y^2 + \sqrt{2}xy = x^3 - \sqrt{2}x^2 + (2 - 2\sqrt{2})x + 5 - 3\sqrt{2}$$

that has CM by $\mathbb{Z}[2\sqrt{-2}]$. This is the curve `64.1-a6` over $\mathbb{Q}(\sqrt{-2})$ in the LMFDB.

For this curve, if $P \in E$ has exact order 2^n, for $n \geq 2$, then $[K(P) : K]$ is divisible by 2^{2n-5} (and equality holds for some such P).

Example

When $N = 2^n$, and E/K, we can achieve $[K(P) : K] = T(\mathcal{O}_{K,f}, 2^n) = 2^{2n-5}$.

For example, let $K = \mathbb{Q}(\sqrt{-2})$, let $f = 2$, and let $\mathcal{O}_{K,f} = \mathbb{Z}[2\sqrt{-2}]$. In this case $j_f = 26125000 + 18473000\sqrt{2}$. Let

$$E/K : y^2 + \sqrt{2}xy = x^3 - \sqrt{2}x^2 + (2 - 2\sqrt{2})x + 5 - 3\sqrt{2}$$

that has CM by $\mathbb{Z}[2\sqrt{-2}]$. This is the curve `64.1-a6` over $\mathbb{Q}(\sqrt{-2})$ in the LMFDB.

For this curve, if $P \in E$ has exact order 2^n, for $n \geq 2$, then $[K(P) : K]$ is divisible by 2^{2n-5} (and equality holds for some such P).

The same problem can be solved if we classify all 2-adic representations for elliptic curves $E/\mathbb{Q}(j_f)$ with CM by $\mathcal{O}_{K,f}$.

Back to 2-adic representations

Theorem (Rouse and Zureick-Brown, 2014)

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely **1208** *possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further, the representation $\rho_{E,2}$ is defined (at most) modulo 32.*

Back to 2-adic representations

Theorem (Rouse and Zureick-Brown, 2014)

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely **1208** *possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further, the representation $\rho_{E,2}$ is defined (at most) modulo 32.*

What about representations coming from elliptic curves with CM?

Back to 2-adic representations

Theorem (Rouse and Zureick-Brown, 2014)

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely **1208** *possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further, the representation $\rho_{E,2}$ is defined (at most) modulo 32.*

What about representations coming from elliptic curves with CM?

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve. Then, there are precisely **1235** *possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further, the representation $\rho_{E,2}$ is defined (at most) modulo 32.*

In the rest of the talk, we discuss the proof that there are **27** additional types of 2-adic representations coming from elliptic curves over $\mathbb{Q}$ with CM.

§2. Results

Cartan subgroups:

For $N \geq 3$, we define groups of GL$(2, \mathbb{Z}/N\mathbb{Z})$ as follows:

- If $\Delta_K f^2 \equiv 0 \bmod 4$, or N is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.
- If $\Delta_K f^2 \equiv 1 \bmod 4$, and N is even, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.

Then, the Cartan subgroup $\mathcal{C}_{\delta,\phi}(N)$ of GL$(2, \mathbb{Z}/N\mathbb{Z})$ is

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z},\ a^2 + ab\phi - \delta b^2 \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$$

and $\mathcal{N}_{\delta,\phi}(N) = \left\langle \mathcal{C}_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle$.

The Cartan subgroup $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \left(\begin{array}{cc} a+b\phi & b \\ \delta b & a \end{array} \right) : a, b \in \mathbb{Z}/N\mathbb{Z},\ a^2 + ab\phi - \delta b^2 \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$$

and $\mathcal{N}_{\delta,\phi}(N) = \left\langle \mathcal{C}_{\delta,\phi}(N), \left(\begin{array}{cc} -1 & 0 \\ \phi & 1 \end{array} \right) \right\rangle$.

Theorem (The image in coordinates)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the representation $\mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

The Cartan subgroup $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ is

$$\mathcal{C}_{\delta,\phi}(N)=\left\{\begin{pmatrix} a+b\phi & b \\ \delta b & a \end{pmatrix} : a,b\in\mathbb{Z}/N\mathbb{Z},\ a^2+ab\phi-\delta b^2\in(\mathbb{Z}/N\mathbb{Z})^\times\right\}$$

and $\mathcal{N}_{\delta,\phi}(N)=\left\langle \mathcal{C}_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix}\right\rangle$.

Theorem (The image in coordinates)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N\geq 3$, and let $\rho_{E,N}$ be the representation $\mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f}))\to\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$. Then,

1. *There is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$ such that the image of $\rho_{E,N}$ is contained in $\mathcal{N}_{\delta,\phi}(N)$.*

The Cartan subgroup $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ is

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z},\ a^2 + ab\phi - \delta b^2 \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$$

and $\mathcal{N}_{\delta,\phi}(N) = \left\langle \mathcal{C}_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle$.

Theorem (The image in coordinates)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$, let $N \geq 3$, and let $\rho_{E,N}$ be the representation $\mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$*. Then,*

1. *There is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$ such that the image of $\rho_{E,N}$ is contained in $\mathcal{N}_{\delta,\phi}(N)$.*
2. *Moreover, the index of the image of $\rho_{E,N}$ in $\mathcal{N}_{\delta,f}(N)$ coincides with the order of the Galois group* $\mathrm{Gal}(K(j_{K,f}, E[N])/K(j_{K,f}, h(E[N]))$*, for a Weber function h, and it is a divisor of the order of $\mathcal{O}_{K,f}^\times$.*

Theorem (The adelic image)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$.

- *If $\Delta_K f^2 \equiv 0 \bmod 4$, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.*
- *If $\Delta_K f^2 \equiv 1 \bmod 4$, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.*

Let ρ_E be the adelic Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \varprojlim \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \widehat{\mathbb{Z}}),$$

and let $\mathcal{N}_{\delta,\phi} = \varprojlim \mathcal{N}_{\delta,\phi}(N)$.

Theorem (The adelic image)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$.

- *If $\Delta_K f^2 \equiv 0 \bmod 4$, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.*
- *If $\Delta_K f^2 \equiv 1 \bmod 4$, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.*

Let ρ_E be the adelic Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \varprojlim \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \widehat{\mathbb{Z}}),$$

and let $\mathcal{N}_{\delta,\phi} = \varprojlim \mathcal{N}_{\delta,\phi}(N)$. Then:

1. *there is a compatible system of bases of $E[N]$ such that the image of ρ_E is contained in $\mathcal{N}_{\delta,\phi}$,*

Theorem (The adelic image)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$.

- *If $\Delta_K f^2 \equiv 0 \bmod 4$, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.*
- *If $\Delta_K f^2 \equiv 1 \bmod 4$, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.*

Let ρ_E be the adelic Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \varprojlim \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \widehat{\mathbb{Z}}),$$

and let $\mathcal{N}_{\delta,\phi} = \varprojlim \mathcal{N}_{\delta,\phi}(N)$. Then:

1. *there is a compatible system of bases of $E[N]$ such that the image of ρ_E is contained in $\mathcal{N}_{\delta,\phi}$,*
2. *the index of the image of ρ_E in $\mathcal{N}_{\delta,\phi}$ is a divisor of the order $\mathcal{O}_{K,f}^\times$, and the index is a divisor of 4 or 6. [Lombardo, Bourdon–Clark]*

Theorem (The adelic image)

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by $\mathcal{O}_{K,f}$.

- *If $\Delta_K f^2 \equiv 0 \bmod 4$, let $\delta = \Delta_K f^2/4$, and $\phi = 0$.*
- *If $\Delta_K f^2 \equiv 1 \bmod 4$, let $\delta = \frac{(\Delta_K - 1)}{4} f^2$, let $\phi = f$.*

Let ρ_E be the adelic Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}(j_{K,f})}/\mathbb{Q}(j_{K,f})) \to \varprojlim \mathrm{Aut}(E[N]) \cong \mathrm{GL}(2, \widehat{\mathbb{Z}}),$$

and let $\mathcal{N}_{\delta,\phi} = \varprojlim \mathcal{N}_{\delta,\phi}(N)$. Then:

1. *there is a compatible system of bases of $E[N]$ such that the image of ρ_E is contained in $\mathcal{N}_{\delta,\phi}$,*
2. *the index of the image of ρ_E in $\mathcal{N}_{\delta,\phi}$ is a divisor of the order $\mathcal{O}_{K,f}^\times$, and the index is a divisor of 4 or 6. [Lombardo, Bourdon–Clark]*
3. *Moreover, for every K and $f \geq 1$, and a fixed $N \geq 3$, there is an elliptic curve $E/\mathbb{Q}(j_{K,f})$ such that the index of the image of $\rho_{E,N}$ in $\mathcal{N}_{\delta,\phi}(N)$ is 1. [Bourdon–Clark]*

Moreover, for every K and $f \geq 1$, and a fixed $N \geq 3$, there is an elliptic curve $E/\mathbb{Q}(j_{K,f})$ such that the index of the image of $\rho_{E,N}$ in $\mathcal{N}_{\delta,\phi}(N)$ is 1.

However, the adelic representation may not have index 1 in $\mathcal{N}_{\delta,\phi}$ in certain cases.

Theorem (L.-R., 2018)

Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = 1728$, and choose compatible bases of $E[N]$, for each $N \geq 2$, such that the image of ρ_E is contained in $\mathcal{N}_{\delta,\phi}$. Then, the index of the image of ρ_E in $\mathcal{N}_{\delta,\phi}$ is 2 or 4.

Moreover, for every K and $f \geq 1$, and a fixed $N \geq 3$, there is an elliptic curve $E/\mathbb{Q}(j_{K,f})$ such that the index of the image of $\rho_{E,N}$ in $\mathcal{N}_{\delta,\phi}(N)$ is 1.

However, the adelic representation may not have index 1 in $\mathcal{N}_{\delta,\phi}$ in certain cases.

Theorem (L.-R., 2018)

Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = 1728$, and choose compatible bases of $E[N]$, for each $N \geq 2$, such that the image of ρ_E is contained in $\mathcal{N}_{\delta,\phi}$. Then, the index of the image of ρ_E in $\mathcal{N}_{\delta,\phi}$ is 2 or 4.

Theorem (L.-R., 2018)

Let $E/\mathbb{Q}$ be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ in an imaginary quadratic field K with $\Delta_K \neq -4, -8$ and $j_{K,f} \neq 0$, and choose compatible bases of $E[N]$, for each $N \geq 2$, such that the image of ρ_E is contained in $\mathcal{N}_{\delta,\phi}$. Then, the index of the image of ρ_E in $\mathcal{N}_{\delta,\phi}$ is 2.

Using our work, we can classify all the p-adic Galois representations that arise from elliptic curves over $\mathbb{Q}(j_{K,f})$, up to conjugation

Using our work, we can classify all the p-adic Galois representations that arise from elliptic curves over $\mathbb{Q}(j_{K,f})$, up to conjugation... including $p = 2$ and $p = 3$!

Using our work, we can classify all the p-adic Galois representations that arise from elliptic curves over $\mathbb{Q}(j_{K,f})$, up to conjugation... including $p = 2$ and $p = 3$!

Here is the complete list of 2-adic images coming from CM over $\mathbb{Q}$:

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,\phi}(2^\infty)$	E
0	-3	1	1	$y^2 = x^3 + 2$
0	-3	1	3	$y^2 = x^3 + 1$
$2^4 \cdot 3^3 \cdot 5^3$	-3	2	1	$y^2 = x^3 - 15x + 22$
$-2^{15} \cdot 3 \cdot 5^3$	-3	3	1	$y^2 + y = x^3 - 30x + 63$
$-3^3 \cdot 5^3$	-7	1	1	$y^2 + xy = x^3 - x^2 - 2x - 1$
$3^3 \cdot 5^3 \cdot 17^3$	-7	2	1	$y^2 = x^3 - 595x + 5586$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Using our work, we can classify all the p-adic Galois representations that arise from elliptic curves over $\mathbb{Q}(j_{K,f})$, up to conjugation... including $p = 2$ and $p = 3$!

Here is the complete list of 2-adic images coming from CM over $\mathbb{Q}$:

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,\phi}(2^\infty)$	E
0	-3	1	1	$y^2 = x^3 + 2$
0	-3	1	3	$y^2 = x^3 + 1$
$2^4 \cdot 3^3 \cdot 5^3$	-3	2	1	$y^2 = x^3 - 15x + 22$
$-2^{15} \cdot 3 \cdot 5^3$	-3	3	1	$y^2 + y = x^3 - 30x + 63$
$-3^3 \cdot 5^3$	-7	1	1	$y^2 + xy = x^3 - x^2 - 2x - 1$
$3^3 \cdot 5^3 \cdot 17^3$	-7	2	1	$y^2 = x^3 - 595x + 5586$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Note: the images for $(\Delta_K, f) = (-3, 2)$ and $(-7, 2)$ are conjugates modulo 16, but not modulo 32.

The list of 2-adic images coming from CM over $\mathbb{Q}$: (continued)

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,\phi}(2^\infty)$	E
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$1728 = 2^6 \cdot 3^3$	-4	1	1	$y^2 = x^3 + 3x$
1728	-4	1	2	$y^2 = x^3 + 9x$
1728	-4	1	2	$y^2 = x^3 - 9x$
1728	-4	1	2	$y^2 = x^3 + 18x$
1728	-4	1	2	$y^2 = x^3 - 18x$
1728	-4	1	4	$y^2 = x^3 + x$
1728	-4	1	4	$y^2 = x^3 - x$
1728	-4	1	4	$y^2 = x^3 + 2x$
1728	-4	1	4	$y^2 = x^3 - 2x$
1728	-4	1	4	$y^2 = x^3 + 4x$
1728	-4	1	4	$y^2 = x^3 - 4x$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

The list of 2-adic images coming from CM over $\mathbb{Q}$: (continued)

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,\phi}(2^\infty)$	E
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^3 \cdot 3^3 \cdot 11^3$	-4	2	1	$y^2 = x^3 - 99x + 378$
$2^3 \cdot 3^3 \cdot 11^3$	-4	2	2	$y^2 = x^3 - 11x + 14$
$2^3 \cdot 3^3 \cdot 11^3$	-4	2	2	$y^2 = x^3 - 11x - 14$
$2^3 \cdot 3^3 \cdot 11^3$	-4	2	2	$y^2 = x^3 - 44x + 112$
$2^3 \cdot 3^3 \cdot 11^3$	-4	2	2	$y^2 = x^3 - 44x + 112$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

The list of 2-adic images coming from CM over $\mathbb{Q}$: (continued)

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,\phi}(2^\infty)$	E
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^6 \cdot 5^3$	-8	1	1	$y^2 = x^3 - 38880x + 2612736$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 4320x + 96768$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 4320x - 96768$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 17280x + 774144$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 17280x - 774144$

The list of 2-adic images coming from CM over $\mathbb{Q}$: (continued)

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,\phi}(2^\infty)$	E
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^6 \cdot 5^3$	-8	1	1	$y^2 = x^3 - 38880x + 2612736$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 4320x + 96768$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 4320x - 96768$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 17280x + 774144$
$2^6 \cdot 5^3$	-8	1	2	$y^2 = x^3 - 17280x - 774144$

Note: The last four examples are particularly interesting: the index of the image in $\mathcal{N}_{\delta,\phi}(4)$ is 1, but the index in $\mathcal{N}_{\delta,\phi}(8)$ and the 2-adic index is 2.

Example

The elliptic curve $E : y^2 = x^3 - 4320x + 96768$ has CM by the maximal order of $K = \mathbb{Q}(\sqrt{-2})$, $f = 1$, and $j_{K,f} = 2^6 \cdot 5^3$. Its 2-adic image is conjugate to the group:

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -\delta & -1 \end{pmatrix} \right\rangle \subseteq \mathcal{N}_{\delta,0}(2^\infty) \subseteq \mathrm{GL}(2, \mathbb{Z}_2),$$

where $\delta = \Delta_K f^2/4 = -2$.

These examples are the CM analog of those non-CM images described by Dokchitser and Dokchitser that are surjective mod 4 (onto $\mathrm{GL}(2, \mathbb{Z}/4\mathbb{Z})$) but not mod 8.


$F_p(t)$
$F_p(t^p)$
We're inseparable

A similar effect happens for $p = 3$ when $j_{K,f} = 0$. Here is the list of 3-adic images coming from CM over $\mathbb{Q}$:

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,0}(3^\infty)$	E
$1728 = 2^3 \cdot 3^3$	-4	1	1	$y^2 = x^3 + x$
-2^{15}	-11	1	1	$y^2 + y = x^3 - x^2 - 7x + 10$
0	-3	1	1	$y^2 = x^3 - 1$
0	-3	1	2	$y^2 = x^3 + 1$
0	-3	1	2	$y^2 = x^3 - 3$
0	-3	1	3	$y^2 = x^3 + 2$
0	-3	1	3	$y^2 = x^3 + 6$
0	-3	1	3	$y^2 = x^3 + 18$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Note: the last two groups are conjugates mod 9 but not mod 27.

The list of 3-adic images coming from CM: (continued)

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,0}(3^\infty)$	E
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	-3	1	6	$y^2 = x^3 + 16$
0	-3	1	6	$y^2 = x^3 - 432$
0	-3	1	6	$y^2 = x^3 + 1296$
0	-3	1	6	$y^2 = x^3 - 48$
0	-3	1	6	$y^2 = x^3 + 144$
0	-3	1	6	$y^2 = x^3 - 3888$

The list of 3-adic images coming from CM: (continued)

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,0}(3^\infty)$	E
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	-3	1	6	$y^2 = x^3 + 16$
0	-3	1	6	$y^2 = x^3 - 432$
0	-3	1	6	$y^2 = x^3 + 1296$
0	-3	1	6	$y^2 = x^3 - 48$
0	-3	1	6	$y^2 = x^3 + 144$
0	-3	1	6	$y^2 = x^3 - 3888$

Note: The last four examples are particularly interesting: the index of the image in $\mathcal{N}_{\delta,\phi}(3)$ is 2, but the index in $\mathcal{N}_{\delta,\phi}(9)$ and the 3-adic index is 6. These examples are CM analogs of those non-CM images described by Elkies that are surjective mod 3 (onto $\mathrm{GL}(2, \mathbb{Z}/3\mathbb{Z})$) but not mod 9.

The list of 3-adic images coming from CM: (continued)

$j_{K,f}$	Δ_K	f	index in $\mathcal{N}_{\delta,0}(3^\infty)$	E
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	-3	1	6	$y^2 = x^3 + 16$
0	-3	1	6	$y^2 = x^3 - 432$
0	-3	1	6	$y^2 = x^3 + 1296$
0	-3	1	6	$y^2 = x^3 - 48$
0	-3	1	6	$y^2 = x^3 + 144$
0	-3	1	6	$y^2 = x^3 - 3888$

Note: The last four examples are particularly interesting: the index of the image in $\mathcal{N}_{\delta,\phi}(3)$ is 2, but the index in $\mathcal{N}_{\delta,\phi}(9)$ and the 3-adic index is 6. These examples are CM analogs of those non-CM images described by Elkies that are surjective mod 3 (onto $\mathrm{GL}(2,\mathbb{Z}/3\mathbb{Z})$) but not mod 9.

Special thanks to Drew Sutherland for helping me in computing these examples.


$F_p(t)$
$F_p(t^p)$
We're inseparable

Example

The elliptic curve $E : y^2 = x^3 + 144$ has CM by the maximal order of $K = \mathbb{Q}(\sqrt{-3})$, $f = 1$, and $j_{K,f} = 0$. Its 3-adic image is conjugate to the group:

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} -5/4 & 1/2 \\ -3/8 & -5/4 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}(2, \mathbb{Z}_3).$$

§3. Proofs

First step: understand the image in coordinates.

If we define the Cartan subgroup $\mathcal{C}_{\delta,\phi}(N)$ of $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ by

$$\mathcal{C}_{\delta,\phi}(N) = \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} : a, b \in \mathbb{Z}/N\mathbb{Z},\ a^2 + ab\phi - \delta b^2 \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$$

and

$$\mathcal{N}_{\delta,\phi}(N) = \left\langle \mathcal{C}_{\delta,\phi}(N), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle,$$

then there is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N]$ such that the image of $\rho_{E,N}$ is contained in $\mathcal{N}_{\delta,\phi}(N)$.

Q

$$
\begin{tikzcd}
\mathbb{Q}(j_{k,\rho}, E[N]) \arrow[d, dash] \\
\mathbb{Q}(j_{k,\rho}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}
$$

$$\begin{array}{l}
\mathbb{Q}(j_{k,g}, E[N]) = H_g(E[N]) \quad \text{if } N \geq 3 \\
\quad | \\
H_g = K(j_{k,g}) \\
\quad | \\
\mathbb{Q}(j_{k,g}) \\
\quad | \\
\mathbb{Q}
\end{array}$$

$$
\begin{tikzcd}[column sep=small]
\mathbb{Q}(j_{K,\mathfrak{f}}, E[N]) = H_{\mathfrak{f}}(E[N]) \arrow[d, dash] \\
H_{\mathfrak{f}}(h(E[N])) \arrow[d, dash] \\
H_{\mathfrak{f}} = K(j_{K,\mathfrak{f}}) \arrow[d, dash] \\
\mathbb{Q}(j_{K,\mathfrak{f}}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}
$$

if $N \geqslant 3$

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{Q}(j_{K,f}, E[N]) = H_f(E[N]) \\
 & H_f(h(E[N])) \arrow[u] \\
H_f = K(j_{K,f}) \arrow[uur, bend left=40, "\left(\mathcal{O}_{K,f}/N\mathcal{O}_{K,f}\right)^{\times} \supseteq \text{ by CM thy.}"] \arrow[ur] & \\
\mathbb{Q}(j_{K,f}) \arrow[u] & \\
\mathbb{Q} \arrow[u] &
\end{tikzcd}$$

if $N \geq 3$

$$
\begin{tikzcd}
\mathbb{Q}(j_{K,\mathfrak{f}}, E[N]) = H_{\mathfrak{f}}(E[N]) \text{ if } N \geqslant 3 \arrow[dd, dash, bend right=60, "\left(\mathcal{O}_{K,\mathfrak{f}}/N\mathcal{O}_{K,\mathfrak{f}}\right)^{\times} \cong \text{ by CM thy.}"'] \arrow[d, dash] \\
H_{\mathfrak{f}}(h(E[N])) \arrow[d, dash] \arrow[d, dash, bend left=60, "\cong \left(\mathcal{O}_{K,\mathfrak{f}}/N\mathcal{O}_{K,\mathfrak{f}}\right)^{\times} \big/ \mathcal{O}_{K,\mathfrak{f}}^{\times} \big/ \mathcal{O}_{K,\mathfrak{f},N}^{\times} \text{ by CFT}"] \\
H_{\mathfrak{f}} = K(j_{K,\mathfrak{f}}) \arrow[d, dash] \\
\mathbb{Q}(j_{K,\mathfrak{f}}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}
$$

$$\begin{tikzcd}
\mathbb{Q}(j_{K,\mathfrak{f}}, E[N]) = H_{\mathfrak{f}}(E[N]) \text{ if } N \geq 3 \arrow[d, dash] \arrow[d, dash, bend left=60, "\subseteq \mathcal{O}_{K,\mathfrak{f}}^\times / \mathcal{O}_{K,\mathfrak{f},N}^\times"] \arrow[dd, dash, bend right=70, "\left(\mathcal{O}_{K,\mathfrak{f}}/N\mathcal{O}_{K,\mathfrak{f}}\right)^\times \supseteq \text{ by CM thy.}"'] \\
H_{\mathfrak{f}}(h(E[N])) \arrow[d, dash] \arrow[d, dash, bend left=60, "\cong \left(\left(\mathcal{O}_{K,\mathfrak{f}}/N\mathcal{O}_{K,\mathfrak{f}}\right)^\times \big/ \mathcal{O}_{K,\mathfrak{f}}^\times / \mathcal{O}_{K,\mathfrak{f},N}^\times\right) \text{ by CFT}"] \\
H_{\mathfrak{f}} = K(j_{K,\mathfrak{f}}) \arrow[d, dash] \\
\mathbb{Q}(j_{K,\mathfrak{f}}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

$$
\begin{tikzcd}[row sep=large]
\mathbb{Q}(j_{k,f}, E[N]) = H_f(E[N]) \text{ if } N \geq 3 \\
H_f(h(E[N])) \arrow[u, dash] \arrow[u, bend right=60, dash, "\subseteq \mathcal{O}_{k,f}^\times / \mathcal{O}_{k,f,N}^\times"'] \\
H_f = K(j_{k,f}) \arrow[u, dash] \arrow[u, bend right=60, dash, "\cong \left(\mathcal{O}_{k,f}/N\mathcal{O}_{k,f}\right)^\times \Big/ \left(\mathcal{O}_{k,f}^\times / \mathcal{O}_{k,f,N}^\times\right) \text{ by CFT}"'] \arrow[uu, bend left=60, dash, "\left(\mathcal{O}_{k,f}/N\mathcal{O}_{k,f}\right)^\times \supseteq \text{ by CM thy.}"] \\
\mathbb{Q}(j_{k,f}) \arrow[u, dash] \arrow[uuu, bend left=80, dash, "\left(\mathcal{O}_{k,f}/N\mathcal{O}_{k,f}\right)^\times \rtimes \langle c \rangle \cong"] \\
\mathbb{Q} \arrow[u, dash]
\end{tikzcd}
$$

complex conjugation

Key step: understand $\mathrm{Gal}(H_f(h(E[N]))/H_f)$

Theorem

Let $E/\mathbb{Q}(j_{K,f})$ be an elliptic curve with CM by an order $\mathcal{O}_{K,f}$ of conductor $f \geq 1$ in an imaginary quadratic field K, and let $N \geq 2$. Let $H_f = K(j_{K,f})$. Then,

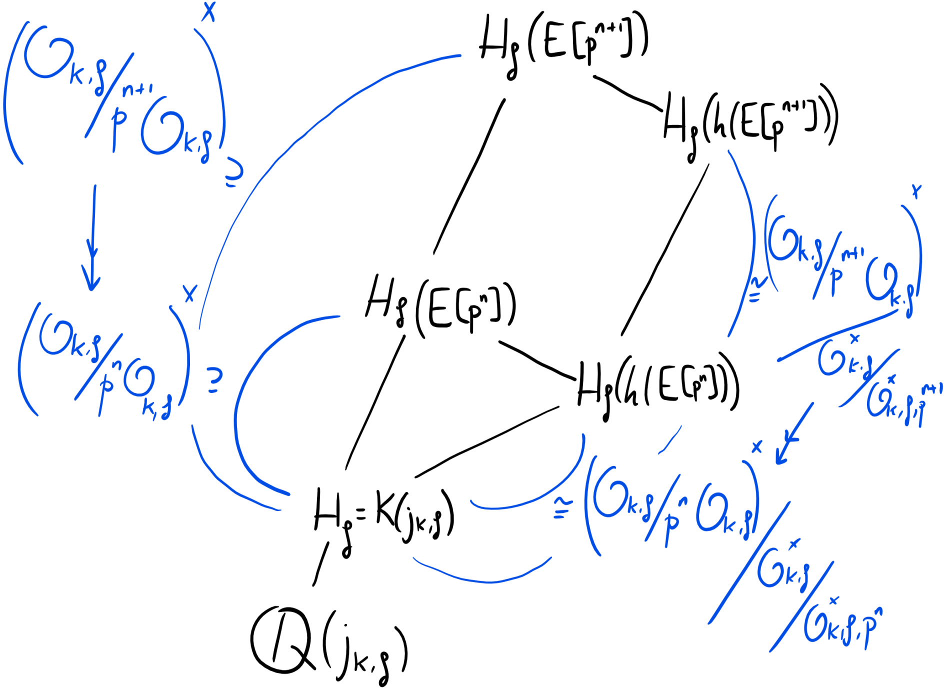
$$\mathrm{Gal}(H_f(h(E[N]))/H_f) \cong \left(\frac{\mathcal{O}_{K,f}}{N\mathcal{O}_{K,f}}\right)^\times \Big/ \frac{\mathcal{O}_{K,f}^\times}{\mathcal{O}_{K,f,N}^\times}.$$

Note:

- Stevenhagen gives a description of the extension and the Galois group using an adelic approach and Shimura reciprocity.
- Bourdon and Clark deduce an explicit description of the field $K(j_{K,f}, h(E[N]))$ as the compositum of a ray class field and a ring class field.
- We use a classical class field theory approach to describe it in terms of quotients of groups of proper $\mathcal{O}_{K,f}$-ideals


$\mathbb{F}_p(t)$
|
$\mathbb{F}_p(t^p)$
We're inseparable

Next step: for a fixed prime p, understand the tower $H_f(E[p^n])$ as n grows, and its Galois group over H_f.


$\left(\mathcal{O}_{k,\wp}/p^{n+1}\mathcal{O}_{k,\wp}\right)^\times \supseteq$
$\left(\mathcal{O}_{k,\wp}/p^{n}\mathcal{O}_{k,\wp}\right)^\times \supseteq$
$H_\wp(E[p^{n+1}])$
$H_\wp(h(E[p^{n+1}]))$
$H_\wp(E[p^n])$
$H_\wp(h(E[p^n]))$
$\simeq \left(\mathcal{O}_{k,\wp}/p^{n+1}\mathcal{O}_{k,\wp}\right)^\times \Big/ \mathcal{O}_{k,\wp}^\times / \mathcal{O}_{k,\wp,p^{n+1}}^\times$
$H_\wp = K(j_{k,\wp})$
$\simeq \left(\mathcal{O}_{k,\wp}/p^{n}\mathcal{O}_{k,\wp}\right)^\times \Big/ \mathcal{O}_{k,\wp}^\times / \mathcal{O}_{k,\wp,p^{n}}^\times$
$\mathbb{Q}(j_{k,\wp})$

Theorem

Let $t = 1$ *if* $p > 2$ *and* $t = 2$ *if* $p = 2$*, and suppose one of the following holds:*

- $[H_f(E[p^n]) : H_f(h(E[p^n]))]$ *is relatively prime to* p*, for some* $n \geq t$*.*
- $j_{K,f} \neq 0$*, and* $p > 2$*.*
- $j_{K,f} = 0$ *and* $p > 3$*.*

Then, the image of the group $\mathrm{Gal}(H_f(E[p^{n+1}])/H_f)$ *in* $(\mathcal{O}_{K,f}/p^{n+1}\mathcal{O}_{K,f})^\times$ *is the full inverse image of the image of* $\mathrm{Gal}(H_f(E[p^n])/H_f)$ *in* $(\mathcal{O}_{K,f}/p^n\mathcal{O}_{K,f})^\times$ *under the natural reduction map modulo* p^n*.*

Next steps: understand the Galois group of $H_f(E[N])$ over $\mathbb{Q}(j_{K,f})$.

- Describe $(\mathcal{O}_{K,f}/N\mathcal{O}_{K,f})^\times$, for N a power of 2 or 3, in terms of generators in $\mathcal{O}_{K,f}$.
- Subgroups of $(\mathcal{O}_{K,f}/N\mathcal{O}_{K,f})^\times$, for N a power of 2 or 3, that are missing a certain root of unity, stable under complex conjugation, and are of a certain index.
- Determine the possible shapes of complex conjugation.

For example, the more interesting 2-adic representations arise like so:

Lemma

1. *Let* $n \geq 2$*, let* H_n *be a subgroup of index* 2 *of* $(\mathcal{O}_{K,f}/2^n\mathcal{O}_{K,f})^\times$*, and let* $H_2 \equiv H_n \bmod 4\mathcal{O}_{K,f}$ *be the reduction of* H_n *modulo* 4*. Suppose that:*

- -1 *is not in* H_2*, and*
- H_2 *is fixed under complex conjugation.*

Then, $\Delta_K f^2 \equiv 0 \bmod 16$ *and there are precisely two such subgroups* H_n*, namely* $\langle 5, 1 + f\tau \rangle / 2^n$ *and* $\langle 5, -1 - f\tau \rangle / 2^n$*.*

For example, the more interesting 2-adic representations arise like so:

Lemma

1. *Let* $n \geq 2$, *let* H_n *be a subgroup of index* 2 *of* $(\mathcal{O}_{K,f}/2^n\mathcal{O}_{K,f})^\times$, *and let* $H_2 \equiv H_n \bmod 4\mathcal{O}_{K,f}$ *be the reduction of* H_n *modulo* 4*. Suppose that:*

- -1 *is not in* H_2, *and*
- H_2 *is fixed under complex conjugation.*

Then, $\Delta_K f^2 \equiv 0 \bmod 16$ *and there are precisely two such subgroups* H_n, *namely* $\langle 5, 1 + f\tau \rangle / 2^n$ *and* $\langle 5, -1 - f\tau \rangle / 2^n$.

2. *Suppose* $n \geq 3$ *and* H_n *is a subgroup of index* 2 *of* $(\mathcal{O}_{K,f}/2^n\mathcal{O}_{K,f})^\times$ *such that:*

- -1 *is not in* H_n,
- H_n *is fixed under complex conjugation,*
- H_n *surjects onto* $(\mathcal{O}_{K,f}/4\mathcal{O}_{K,f})^\times$ *when reduced* $\bmod 4\mathcal{O}_{K,f}$.

Then, $\Delta_K \equiv 0 \bmod 8$ *and there are precisely two such subgroups, namely* $\langle 3, 1 + f\tau \rangle / 2^n$ *and* $\langle 3, -1 - f\tau \rangle / 2^n$.

THANK YOU

alvaro.lozano-robledo@uconn.edu

http://alozano.clas.uconn.edu

"*If by chance I have omitted anything
more or less proper or necessary,
I beg forgiveness,
since there is no one who is without fault
and circumspect in all matters.*"

Leonardo Pisano (Fibonacci), *Liber Abaci*.