Local-global principle for 11-isogenies of elliptic curves is true over quadratic fields

Stevan Gajović (MPIM Bonn)
Joint work with Jeroen Hanselman (TU Kaiserslautern) and Angelos Koutsianas (Aristotle University of Thessaloniki)

LUCANT 2025,
July 10, 2025

Local global priniple for ℓ-isogenies of elliptic curves

- Let K be a number field and E/K an elliptic curve with $j(E) \neq 0, 1728$ and ℓ a prime number.
- If E admits a K-rational ℓ-isogeny then for almost all primes $\mathfrak{p}$ in K its reduction $\widetilde{E}/\mathbb{F}_{\mathfrak{p}}$ also admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny.

Question

When $\widetilde{E}/\mathbb{F}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny for almost all primes $\mathfrak{p}$ in K, does E admit a K-rational ℓ-isogeny?

Local global priniple for ℓ-isogenies of elliptic curves

- Let K be a number field and E/K an elliptic curve with $j(E) \neq 0, 1728$ and ℓ a prime number.
- If E admits a K-rational ℓ-isogeny then for almost all primes $\mathfrak{p}$ in K its reduction $\widetilde{E}/\mathbb{F}_{\mathfrak{p}}$ also admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny.

Question

When $\widetilde{E}/\mathbb{F}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny for almost all primes $\mathfrak{p}$ in K, does E admit a K-rational ℓ-isogeny?

- Based on the work of Sutherland, Anni, and Banwait-Cremona, we prove that for $\ell = 11$ and $[K : \mathbb{Q}] = 2$, the answer is YES.

Local global priniple for ℓ-isogenies of elliptic curves

- Let K be a number field and E/K an elliptic curve with $j(E) \neq 0, 1728$ and ℓ a prime number.
- If E admits a K-rational ℓ-isogeny then for almost all primes $\mathfrak{p}$ in K its reduction $\widetilde{E}/\mathbb{F}_{\mathfrak{p}}$ also admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny.

Question

When $\widetilde{E}/\mathbb{F}_{\mathfrak{p}}$ admits an $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny for almost all primes $\mathfrak{p}$ in K, does E admit a K-rational ℓ-isogeny?

- Based on the work of Sutherland, Anni, and Banwait-Cremona, we prove that for $\ell = 11$ and $[K : \mathbb{Q}] = 2$, the answer is YES.
- Whether or not E admits an ℓ-isogeny over K depends only on $j(E)$.

Definition

A pair (j_0, ℓ) with $j_0 \in K$ is called *exceptional for K* if there exists E/K with $j(E) = j_0$ and the answer is NO; then ℓ is an *exceptional prime for K*.

Galois representations and modular curves

Theorem (Sutherland, 2012)

The only exceptional pair when $K = \mathbb{Q}$ is $(\frac{2268945}{128}, 7)$.

- Strategy: group theory and rational points on modular curves.

Galois representations and modular curves

Theorem (Sutherland, 2012)

The only exceptional pair when $K = \mathbb{Q}$ is $(\frac{2268945}{128}, 7)$.

- Strategy: group theory and rational points on modular curves.
- For the residual ℓ-torsion representation $\overline{\rho}_{E,\ell} : \mathrm{Gal}_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$, denote $H_{E,\ell}$ the image of $\mathrm{Im}(\overline{\rho}_{E,\ell})$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Let $\ell^* = \left(\frac{-1}{\ell}\right)\ell$.

Theorem (Sutherland, 2012)

Assume $\sqrt{\ell^*} \notin K$. If (j_0, ℓ) is exceptional pair for K, then $\ell \equiv 3 \pmod 4$. For an elliptic curve E/K with $j(E) = j_0$ holds that $H_{E,\ell} \simeq D_{2n}$ (of order $2n$), where $n > 1$ is an odd divisor of $(\ell - 1)/2$.

Galois representations and modular curves

Theorem (Sutherland, 2012)

The only exceptional pair when $K = \mathbb{Q}$ is $(\frac{2268945}{128}, 7)$.

- Strategy: group theory and rational points on modular curves.
- For the residual ℓ-torsion representation $\overline{\rho}_{E,\ell} : \ \mathrm{Gal}_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$, denote $H_{E,\ell}$ the image of $\mathrm{Im}(\overline{\rho}_{E,\ell})$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Let $\ell^* = \left(\frac{-1}{\ell}\right)\ell$.

Theorem (Sutherland, 2012)

Assume $\sqrt{\ell^*} \notin K$. If (j_0, ℓ) is exceptional pair for K, then $\ell \equiv 3 \pmod 4$. For an elliptic curve E/K with $j(E) = j_0$ holds that $H_{E,\ell} \simeq D_{2n}$ (of order $2n$), where $n > 1$ is an odd divisor of $(\ell - 1)/2$.

Conclusion

When $\sqrt{\ell^*} \notin K$, exceptional pairs lead to non-cuspidal K-rational points on the modular curve $X_{D_{2n}}(\ell)$ for some odd divisor $n > 1$ of $\frac{\ell-1}{2}$.

Exceptional primes for quadratic fields and bounds

Question

1. *Fix K and try to find all exceptional primes ℓ for K - not today!*

Exceptional primes for quadratic fields and bounds

Question

1. *Fix K and try to find all exceptional primes ℓ for K - not today!*
2. *Fix ℓ and search if ℓ is exceptional in a family of number fields K.*
3. *Which are exceptional primes for quadratic fields?*

Exceptional primes for quadratic fields and bounds

Question

1. *Fix K and try to find all exceptional primes ℓ for K - not today!*
2. *Fix ℓ and search if ℓ is exceptional in a family of number fields K.*
3. *Which are exceptional primes for quadratic fields?*

Theorem (Anni, 2014)

Let K a number field of degree d with an exceptional pair (j_0, ℓ).

1. *Then $\ell \geq 5$ and characterisation of exceptional pairs when $\ell = 5, 7$.*
2. *If $\sqrt{\ell^*} \notin K$, then $\ell \leq 6d + 1$.*
3. *There are finitely many exceptional pairs (j_0, ℓ) with $\ell > 7$.*

Exceptional primes for quadratic fields and bounds

Question

1. *Fix K and try to find all exceptional primes ℓ for K - not today!*
2. *Fix ℓ and search if ℓ is exceptional in a family of number fields K.*
3. *Which are exceptional primes for quadratic fields?*

Theorem (Anni, 2014)

Let K a number field of degree d with an exceptional pair (j_0, ℓ).

1. *Then $\ell \geq 5$ and characterisation of exceptional pairs when $\ell = 5, 7$.*
2. *If $\sqrt{\ell^*} \notin K$, then $\ell \leq 6d + 1$.*
3. *There are finitely many exceptional pairs (j_0, ℓ) with $\ell > 7$.*

Conclusion

If $K = \mathbb{Q}(\sqrt{m})$, then an exceptional prime $\ell > 7$ for K can be 11 or $|m| = \ell$ if $m = \ell^*$ for some prime $\ell > 7$.

What if $\sqrt{\ell^*} \in K$ and conclusion

Theorem (Banwait-Cremona, 2014)

Let $\sqrt{\ell^*} \in K$. If (j_0, ℓ) is exceptional pair for K, then $\ell \equiv 1 \pmod 4$.
More precise description of $H_{E,\ell}$ for an elliptic curve E/K with $j(E) = j_0$.

What if $\sqrt{\ell^*} \in K$ and conclusion

Theorem (Banwait-Cremona, 2014)

Let $\sqrt{\ell^*} \in K$. If (j_0, ℓ) is exceptional pair for K, then $\ell \equiv 1 \pmod 4$.
More precise description of $H_{E,\ell}$ for an elliptic curve E/K with $j(E) = j_0$.

Conclusion

If $\ell > 11$, $\ell \equiv 3 \pmod 4$, then ℓ is not exceptional for any quadratic number field.
Also, $\ell = 11$ is not exceptional for $K = \mathbb{Q}(\sqrt{-11})$.

What if $\sqrt{\ell^*} \in K$ and conclusion

Theorem (Banwait-Cremona, 2014)

Let $\sqrt{\ell^*} \in K$. If (j_0, ℓ) is exceptional pair for K, then $\ell \equiv 1 \pmod 4$. More precise description of $H_{E,\ell}$ for an elliptic curve E/K with $j(E) = j_0$.

Conclusion

If $\ell > 11$, $\ell \equiv 3 \pmod 4$, then ℓ is not exceptional for any quadratic number field.
Also, $\ell = 11$ is not exceptional for $K = \mathbb{Q}(\sqrt{-11})$.

Conjecture (Banwait-Cremona, 2014)

11 *is not an exceptional prime for any quadratic field.*

What if $\sqrt{\ell^*} \in K$ and conclusion

Theorem (Banwait-Cremona, 2014)

Let $\sqrt{\ell^*} \in K$. If (j_0, ℓ) is exceptional pair for K, then $\ell \equiv 1 \pmod 4$.
More precise description of $H_{E,\ell}$ for an elliptic curve E/K with $j(E) = j_0$.

Conclusion

If $\ell > 11$, $\ell \equiv 3 \pmod 4$, then ℓ is not exceptional for any quadratic number field.
Also, $\ell = 11$ is not exceptional for $K = \mathbb{Q}(\sqrt{-11})$.

Conjecture (Banwait-Cremona, 2014)

11 *is not an exceptional prime for any quadratic field.*

Task

Compute $X_{D_{10}}^{(2)}(\mathbb{Q})$ and check if quadratic points lead to exceptional pairs.

The modular curve $X_{D_{10}}$

- Use the work of Galbraith, Box, Assaf $\rightsquigarrow$ compute a model of $X_{D_{10}}$.
- The genus of $X_{D_{10}}$ is $g = 6$ and the rank of its Jacobian $J/\mathbb{Q}$ is $r = 1$.
- The rank condition $r + 2 \leq g$ to apply symmetric Chabauty for quadratic points on $X_{D_{10}}$ is satisfied!

The modular curve $X_{D_{10}}$

- Use the work of Galbraith, Box, Assaf $\rightsquigarrow$ compute a model of $X_{D_{10}}$.
- The genus of $X_{D_{10}}$ is $g = 6$ and the rank of its Jacobian $J/\mathbb{Q}$ is $r = 1$.
- The rank condition $r + 2 \leq g$ to apply symmetric Chabauty for quadratic points on $X_{D_{10}}$ is satisfied!
- There is a degree 2 cover $\phi : X_{D_{10}} \to X_0^+(121)$.
- $g(X_0^+(121)) = 2 > r(X_0^+(121)) = 1$: rank condition for the method of Chabauty and Coleman is satisfied $\rightsquigarrow$ compute $X_0^+(121)(\mathbb{Q})$.

The modular curve $X_{D_{10}}$

- Use the work of Galbraith, Box, Assaf $\rightsquigarrow$ compute a model of $X_{D_{10}}$.
- The genus of $X_{D_{10}}$ is $g = 6$ and the rank of its Jacobian $J/\mathbb{Q}$ is $r = 1$.
- The rank condition $r + 2 \leq g$ to apply symmetric Chabauty for quadratic points on $X_{D_{10}}$ is satisfied!
- There is a degree 2 cover $\phi : X_{D_{10}} \to X_0^+(121)$.
- $g(X_0^+(121)) = 2 > r(X_0^+(121)) = 1$: rank condition for the method of Chabauty and Coleman is satisfied $\rightsquigarrow$ compute $X_0^+(121)(\mathbb{Q})$.
- We have $\phi^*(X_0^+(121)(\mathbb{Q})) \subseteq X_{D_{10}}^{(2)}(\mathbb{Q})$ and our search does not find any other quadratic points.

Goal

Use symmetric Chabauty and Mordell-Weil sieve to prove $X_{D_{10}}^{(2)}(\mathbb{Q}) = \phi^*(X_0^+(121)(\mathbb{Q}))$.

Idea of symmetric Chabauty

- Let p be a prime of good reduction for $X_{D_{10}}$.
- As in the method of Chabauty and Coleman, construct enough p-adic locally analytic functions which vanish on $J(\mathbb{Q})$.
- In this step, we use p-adic (Coleman) integration of appropriate holomorphic differentials.

Idea of symmetric Chabauty

- Let p be a prime of good reduction for $X_{D_{10}}$.
- As in the method of Chabauty and Coleman, construct enough p-adic locally analytic functions which vanish on $J(\mathbb{Q})$.
- In this step, we use p-adic (Coleman) integration of appropriate holomorphic differentials.
- In principle, these differentials depend on the choice of p, but in this case, they can be determined globally, due to a rank zero quotient.

Idea of symmetric Chabauty

- Let p be a prime of good reduction for $X_{D_{10}}$.
- As in the method of Chabauty and Coleman, construct enough p-adic locally analytic functions which vanish on $J(\mathbb{Q})$.
- In this step, we use p-adic (Coleman) integration of appropriate holomorphic differentials.
- In principle, these differentials depend on the choice of p, but in this case, they can be determined globally, due to a rank zero quotient.
- Use explicit computational criteria (Siksek+Box) to check

(1) whether a quadratic point is alone in its residue polydisc;

(2) if a quadratic point appears as a pull-back of a rational point of $X_0^+(121)$ by ϕ, to check if all quadratic points in its residue polydisc are also pull-back or a rational point of $X_0^+(121)$.

Mordell-Weil sieve and conclusion

- Ideal outcome would be to successfully apply critertion (2) is all residue polydiscs to conclude $X_{D_{10}}^{(2)}(\mathbb{Q}) = \phi^*(X_0^+(121)(\mathbb{Q}))$, but in reality it does not work that easily.

Mordell-Weil sieve and conclusion

- Ideal outcome would be to successfully apply critertion (2) is all residue polydiscs to conclude $X_{D_{10}}^{(2)}(\mathbb{Q}) = \phi^*(X_0^+(121)(\mathbb{Q}))$, but in reality it does not work that easily.
- In practice, we try to apply such criteria for different primes (in this case $p = 5, 7, 13, 17$), and collect the information where we failed.
- Using finite groups $J(\mathbb{F}_p)$, we obtain conditions on their coordinates in $J(\mathbb{Q})$. If such conditions have empty intersection, which happens here, then the points we have found and described the total set $X_{D_{10}}^{(2)}(\mathbb{Q})$.

Mordell-Weil sieve and conclusion

- Ideal outcome would be to successfully apply critertion (2) is all residue polydiscs to conclude $X_{D_{10}}^{(2)}(\mathbb{Q}) = \phi^*(X_0^+(121)(\mathbb{Q}))$, but in reality it does not work that easily.
- In practice, we try to apply such criteria for different primes (in this case $p = 5, 7, 13, 17$), and collect the information where we failed.
- Using finite groups $J(\mathbb{F}_p)$, we obtain conditions on their coordinates in $J(\mathbb{Q})$. If such conditions have empty intersection, which happens here, then the points we have found and described the total set $X_{D_{10}}^{(2)}(\mathbb{Q})$.
- The images of $X_{D_{10}}^{(2)}(\mathbb{Q})$ under the j-map correspond to CM elliptic curves which cannot give exceptional pairs over quadratic fields.

Mordell-Weil sieve and conclusion

- Ideal outcome would be to successfully apply critertion (2) is all residue polydiscs to conclude $X_{D_{10}}^{(2)}(\mathbb{Q}) = \phi^*(X_0^+(121)(\mathbb{Q}))$, but in reality it does not work that easily.
- In practice, we try to apply such criteria for different primes (in this case $p = 5, 7, 13, 17$), and collect the information where we failed.
- Using finite groups $J(\mathbb{F}_p)$, we obtain conditions on their coordinates in $J(\mathbb{Q})$. If such conditions have empty intersection, which happens here, then the points we have found and described the total set $X_{D_{10}}^{(2)}(\mathbb{Q})$.
- The images of $X_{D_{10}}^{(2)}(\mathbb{Q})$ under the j-map correspond to CM elliptic curves which cannot give exceptional pairs over quadratic fields.

Theorem (G.-Hanselman-Koutsianas)

11 *is not an exceptional prime for any quadratic field.*

Future Work - Cubic Case

Question

What can we say about exceptional primes $\ell > 7$ for cubic number fields?

- It amounts to consider $\ell = 11, 19$.

Future Work - Cubic Case

Question

What can we say about exceptional primes $\ell > 7$ for cubic number fields?

- It amounts to consider $\ell = 11, 19$.

$\ell = 11$

Cubic points on $X_{D_{10}}$: $r = 1$, $g = 6$ - seems possible to compute $X_{D_{10}}^{(3)}(\mathbb{Q})$. Preliminary search does not find any truly cubic points, so the goal might be to prove there are none.

Future Work - Cubic Case

Question

What can we say about exceptional primes $\ell > 7$ for cubic number fields?

- It amounts to consider $\ell = 11, 19$.

$\ell = 11$

Cubic points on $X_{D_{10}}$: $r = 1$, $g = 6$ - seems possible to compute $X_{D_{10}}^{(3)}(\mathbb{Q})$. Preliminary search does not find any truly cubic points, so the goal might be to prove there are none.

$\ell = 19$

The curve $X_{D_{18}}$: $r = 8$, $g = 9$ - symmetric Chabauty cannot be used to compute $X_{D_{18}}^{(3)}(\mathbb{Q})$.
Another strategy: this is a limit case from Anni's theorem. Go through the proof for these concrete values.

The end

Thank you for your attention!

Question

Any questions?

Question for the Audience

If you are working on computing rational points on curves that are in LMFDB, please contact me today or tomorrow to prevent any potential overlaps.

Appendix 1: Modular Curve $X_{D_{10}}$

Let $D_{10} \subseteq \mathrm{PGL}_2(\mathbb{F}_{11})$, $G := G_{D_{10}}$ the pullback of D_{10} to $\mathrm{GL}_2(\mathbb{F}_{11})$. $\Gamma_G = \{A \in \mathrm{SL}_2(\mathbb{Z}), A \pmod{11} \in G\}$. Define $X_{D_{10}} := \Gamma_G \setminus \mathbb{H}^*$ which has label 11.132.6.b.1. $X_{D_{10}}$ parametrizes elliptic curves whose residual representation modulo 11 lies in G up to conjugation. $X_{D_{10}}$ is defined over $\mathbb{Q}$ because $\det(G) = \mathbb{F}_{11}^*$. Model of $X_{D_{10}}$:

$$
\begin{aligned}
&uw - 2vw + 2ux - 6vx + 2uy + 2vy + uz = 0,\\
&uw + vw + 2ux - 2vx + 2uy - 10vy - 5uz + 11vz = 0,\\
&-6u^2 + 6uv - 3v^2 + 11w^2 - 66wx + 11x^2 + 88wy - 110xy + 99y^2 + 44wz - 110xz = 0,\\
&6u^2 + 12uv + 12v^2 + 187wx + 22x^2 + 55wy - 44xy - 154y^2 + 66wz + 77xz + 121yz = 0,\\
&-9v^2 + 88w^2 - 11wx - 99x^2 - 77wy + 110xy - 11y^2 + 77wz - 297xz + 121yz = 0,\\
&-6u^2 - 12uv - 12v^2 + 33w^2 - 77wx + 66x^2 - 121wy - 132xy - 110y^2\\
&-44wz - 187xz + 121yz + 121z^2 = 0.
\end{aligned}
$$

The set of its truly quadratic points is

$$
\begin{aligned}
X_{D_{10}}^{(2)}(\mathbb{Q}) =\{&(-3/4, 1/4, 0, \pm\frac{\sqrt{77}}{2}, 0, 1),\ (3/4, -5/4, 0, \pm\frac{\sqrt{77}}{2}, 0, 1)\\
&(1, 1, 1, \pm\sqrt{-11}, \pm\sqrt{-11}, 1),\ (-2/5, 2/5, 1/5, \pm\frac{\sqrt{209}}{5}, \mp\frac{\sqrt{209}}{5}, 1),\\
&(-1, 7, 5, \pm\sqrt{473}, \mp\sqrt{473}, 1), (-1/3, 0, -1/3, \pm\frac{\sqrt{22}}{3}, \pm\frac{\sqrt{22}}{3}, 1)\},
\end{aligned}
$$

Appendix 2: Modular Curve $X_0^+(121)$

LMFDB: `https://beta.lmfdb.org/ModularCurve/Q/11.66.2.a.1/`.

The curve $X_0^+(121)$ is a hyperelliptic curve given by a model

$$X_0^+(121): \; y^2 + (x^3 + x^2 + x + 1)y = -2x^5 + 2x^4 - 3x^3 + 2x^2 - 2x,$$

We have that $X_0^+(121)(\mathbb{Q}) = \{(1,-3),(1,-1),(0,-1),(0,0),\pm\infty\}$.

The set of the images of the j-map of points in $X_0^+(121)(\mathbb{Q})$ (and whence of $X_{D_{10}}^{(2)}(\mathbb{Q})$) is already computed in LMFDB, and it is:

$$\{\infty, -3375, 8000, -884736, 16581375, -884736000\}.$$