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

Stevan Gajović, Jeroen Hanselman, and Angelos Koutsianas

Abstract. In this paper, we prove that the local-global principle for 11-isogenies for elliptic curves over quadratic fields holds. This gives a positive answer to a conjecture by Banwait and Cremona [5, Conjecture 1.14]. The proof is based on the determination of the set of quadratic points on the modular curve $X_{D_{10}}(11)$.

1. Introduction

Let K be a number field and let E be an elliptic curve over K. If ℓ is a prime and E admits a K-rational ℓ-isogeny, then it is easy to show that the reduction $\tilde{E}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$ of E at a prime $\mathfrak{p}$ of good reduction of E also has a $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny, where $\mathbb{F}_{\mathfrak{p}}$ is the residue field of $\mathfrak{p}$. It is natural to ask the converse question:

Question 1.1. If $\tilde{E}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}$ admits a $\mathbb{F}_{\mathfrak{p}}$-rational ℓ-isogeny for a density 1 set of primes $\mathfrak{p}$, then does E/K admit a K-rational ℓ-isogeny?

In [20] Sutherland studied the above question and explained that in most cases, we can expect the answer to be "yes". However, the most interesting case is when the answer is "no" and this local-global property is violated.

The existence of a K-rational ℓ-isogeny for E depends only on the j-invariant $j(E)$ of E when $j(E) \neq 0, 1728$; in other words, if E'/K is an elliptic curve with $j(E) = j(E')$ then the answer is "no" for E/K if and only if it is "no" for E'/K. Following Sutherland, a pair (ℓ, j_0) with $j_0 \neq 0, 1728$ and $j_0 \in K$ is called *exceptional for* K if there exists an elliptic curve E/K with $j(E) = j_0$ such that the answer to Question 1.1 is "no". The prime ℓ of an exceptional pair is called an *exceptional prime for* K.

We denote by $\rho_{E,\ell}$ the residual Galois representation that arises from the action of G_K on $E(\bar{K})[\ell]$. We denote by $G_{E,\ell} := \mathrm{Im}(\rho_{E,\ell}) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ and $H_{E,\ell}$ is the image of $G_{E,\ell}$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. For $j(E) \neq 0, 1728$ the conjugacy class of $H_{E,\ell}$ in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ depends only on $j(E)$.

For any number field K, it is known that the prime $\ell = 2$ is never an exceptional prime by [1, Remark 2.5]. Therefore, we assume that ℓ is odd and set $\ell^* = (-1)^{(\ell-1)/2}\ell$. We denote by D_{2n} the dihedral group of order $2n$.

2020 *Mathematics Subject Classification.* Primary 14G05, 11G18, Secondary 11G05.

Key words and phrases. Local-global principle, isogenies of elliptic curves, exceptional primes, modular curves, symmetric Chabauty.

THEOREM 1.2 ([20, Theorem 1, Lemma 1]). *Suppose $\sqrt{\ell^*} \notin K$ and (ℓ, j_0) is an exceptional pair for K. Let E/K be an elliptic curve with $j(E) = j_0$. Then, the following statements hold:*

(1) The group $H_{E,\ell}$ is isomorphic to D_{2n}, where $n > 1$ is an odd divisor of $(\ell-1)/2$.
(2) $\ell \equiv 3 \pmod 4$.
(3) The group $G_{E,\ell}$ is contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.
(4) E obtains a rational ℓ-isogeny over $K(\sqrt{\ell^*})$.

REMARK 1.3. As a consequence of Theorem 1.2, when $\sqrt{\ell^*} \notin K$, then any exceptional pair gives rise to a non-cuspidal K-rational point on the modular curve $X_{D_{2n}}(\ell)$ (see the definition in Section 3) for some odd divisor $n > 1$ of $\frac{\ell-1}{2}$.

Using Theorem 1.2 Sutherland proves that the only exceptional pair for $\mathbb{Q}$ is $\left(7, \frac{2268945}{128}\right)$ [20, Theorem 2]. In [5, Proposition 1.3] the authors prove an analogous result to Theorem 1.2 for the case $\sqrt{\ell^*} \in K$.

THEOREM 1.4 ([5, Proposition 1.3]). *Suppose $\sqrt{\ell^*} \in K$. Then (ℓ, j_0) is exceptional for K if and only if one of the following holds for elliptic curves E/K with $j(E) = j_0$:*

- *$H_{E,\ell} \simeq A_4$ and $\ell \equiv 1 \pmod{12}$.*
- *$H_{E,\ell} \simeq S_4$ and $\ell \equiv 1 \pmod{24}$.*
- *$H_{E,\ell} \simeq A_5$ and $\ell \equiv 1 \pmod{60}$.*
- *$H_{E,\ell} \simeq D_{2n}$ and $\ell \equiv 1 \pmod 4$, $n > 1$ is a divisor of $(\ell-1)/2$, and $G_{E,\ell}$ lies in a normaliser of a split Cartan subgroup.*

At the same time, Anni [1] focuses only on exceptional primes and proves that for a given K there are only finitely many.

THEOREM 1.5 ([1, Main Theorem]). *Let K be a number field of degree d over $\mathbb{Q}$ and discriminant Δ, and let $\ell_K := \max\{|\Delta|, 6d+1\}$. The following holds:*

- *If (ℓ, j_0) is an exceptional pair for K then $\ell \leq \ell_K$.*
- *There are only finitely many exceptional pairs for K with $7 < \ell \leq \ell_K$.*

REMARK 1.6. The cases $\ell = 2, 3, 5, 7$ are also covered in [1]. In particular, the primes $\ell = 2, 3$ are not exceptional for any K, the prime $\ell = 5$ is exceptional if and only if $\sqrt{5} \in K$ and the prime $\ell = 7$ appears in infinitely many exceptional pairs for K if and only if the rank over K of the elliptic curve

$$y^2 = x^3 - 1715x + 33614,$$

is positive.

From Theorem 1.5 we understand that there are two important directions in which we can look for exceptional primes.

- Either we fix K and determine all the exceptional primes with $\ell \leq \ell_K$,
- or, we fix ℓ and a "suitable" family S of number fields, and determine all the number fields in S for which ℓ is an exceptional prime.

REMARK 1.7. According to Theorem 1.5 a natural choice of the family S is the set of all number fields of a fixed degree d. This choice becomes even more natural because, for odd degree extensions K, the bound $\ell_K = 6d+1$ is a uniform bound with respect to d [1, Theorem 4.3].

Name	Coordinates
P_1	$(-3/4, 1/4, 0, \frac{\sqrt{77}}{2}, 0, 1)$
P_2	$(3/4, -5/4, 0, \frac{\sqrt{77}}{2}, 0, 1)$
P_3	$(1, 1, 1, \sqrt{-11}, \sqrt{-11}, 1)$
P_4	$(-1/3, 0, -1/3, \frac{\sqrt{22}}{3}, \frac{\sqrt{22}}{3}, 1)$
P_5	$(-2/5, 2/5, 1/5, \frac{\sqrt{209}}{5}, -\frac{\sqrt{209}}{5}, 1)$
P_6	$(-1, 7, 5, \sqrt{473}, -\sqrt{473}, 1)$

TABLE 1. The quadratic points of $X_{D_{10}}(11)$ up to conjugation.

Having all the above results in mind, in particular the fact that 11 is always in the range of potential exceptional primes when K is a quadratic field, Banwait and Cremona conjectured that the prime 11 is not an exceptional prime for any quadratic field K [5, Conjecture 1.14]. In this paper, we give a positive answer to the conjecture.

THEOREM 1.8. *The prime* 11 *is not an exceptional prime for any quadratic field.*

Theorem 1.8 is a consequence of Theorem 1.9 and [5, Proposition 10.1].

THEOREM 1.9. *The quadratic points of the modular curve* $X_{D_{10}}(11)$ *with respect to the model* (3.2) *are listed in Table 1 (up to conjugation).*

The key ingredients in the proof of Theorem 1.9 are the development of the (relative) symmetric Chabauty method and the Mordell-Weil sieve [17, 9, 10], the existence of Assaf's implementations of the space of modular forms for an arbitrary congruence subgroup Γ [2], the LMFDB modular curves database [16] and the fact that its quotient curve $X^+_{D_{10}}(11)$ is a genus 2 curve such that $\mathrm{rank}(J_{X_{D_{10}}}(K)) = \mathrm{rank}(J_{X^+_{D_{10}}}(K))$ for $K = \mathbb{Q}, \mathbb{Q}(\sqrt{-11})$.

A number of steps in the proofs were verified computationally using the Magma computer algebra system [7]. In our computations we used Magma V2.28-23. We rely on the Modular forms package by Eran Assaf [2] https://github.com/assaferan/ModFrmGL2 and code by Samir Siksek [18] which is available on https://github.com/samirsiksek/siksek.github.io/tree/main/progs/chabnf. All of our computations were done on a machine running Ubuntu 22.04.1 with an 2 Intel Xeon E5-2660, 8 core CPUs at 2.2/3.0 GHz, 64 GB RAM. Most computations finish relatively quickly. Only computing the isomorphism between the model computed by Assaf's code and our own simplified equation might take more than an hour. The code used in this paper is available on https://github.com/akoutsianas/local_global_isogenies. In the paper we will clearly indicate whenever we rely on Magma. Instructions on how to reproduce the steps can be found in the repository.

2. Acknowledgments

The second and third authors would like to thank the first author and Charles University for their hospitality when this collaboration took place in Prague. The

first and the third author want to thank the University of Groningen for their hospitality when they collaborated in Groningen. The first author was supported by the Czech Science Foundation GAČR, grant 21-00420M, Junior Fund grant for postdoctoral positions at Charles University and by the MPIM guest postdoctoral fellowship program during various stages of this project. The second author is supported by MaRDI, funded by the Deutsche Forschungsgemeinschaft (DFG), project number 460135501, NFDI 29/1. The third author is supported by the Special Account for Research Funds, AUTH research grant *"Solving Diophantine Equations-10349"*. Moreover, the third author wants to thank Professor Imin Chen for providing access to the servers of the Mathematics Department of Simon Fraser University, where the code was written and tested. We are especially grateful to the anonymous referees for their careful reports and many suggestions and improvements to this paper. We want to thank Imin Chen, Diana Mocanu, Steffen Müller and Lazar Radičević for useful conversations about the project.

3. The modular curve $X_{D_{10}}(11)$

Let N be a positive integer. Suppose G is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\Gamma_G = \{A \in \mathrm{SL}_2(\mathbb{Z}) : A \pmod N \in G_0\}$. Because $\Gamma_G \supset \Gamma(N)$ we have that Γ_G is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We denote by X_G the modular curve that parametrizes elliptic curves over $\mathbb{C}$ whose residual representation modulo N lies in G up to conjugation. The curve X_G has a model defined over $\mathbb{Q}(\zeta_N)^{\det(G)}$ where $\det : G \to (\mathbb{Z}/N\mathbb{Z})^*$ is the determinant map. Over $\mathbb{C}$ the curve X_G is a compact Riemann surface and it holds $X_G(\mathbb{C}) \simeq \Gamma_G \setminus \mathbb{H}^*$.

Let $D_{10} \subset \mathrm{PGL}_2(\mathbb{F}_{11})$, $G_{D_{10}}$ the pullback of D_{10} to $\mathrm{GL}_2(\mathbb{F}_{11})$ and $\Gamma_{D_{10}} := \Gamma_{G_{D_{10}}}$. We define the modular curve[1] $X_{D_{10}}(11) := X_{\Gamma_{D_{10}}}$ which is, from the above, defined over $\mathbb{Q}$ because $\det(G) = \mathbb{F}_{11}^*$ [20, Proposition 3].

In [14] Galbraith described a method to compute a model of a modular curve $X(\Gamma)$ for a congruence subgroup Γ as long as we are able to compute a basis of $S_2(\Gamma)$. Galbraith's ideas have been used and extended by Banwait and Cremona[2] [5, 4], Zywina [21] and Box [8]. Moreover, in [2] Assaf describes a general method of computing $S_2(\Gamma)$ and the algorithm has been implemented in Magma [7].

In our case we use Assaf's algorithm and his implementation to compute $S_2(\Gamma_{D_{10}})$. We pick an explicit subgroup H of $\mathrm{PGL}_2(\mathbb{F}_{11})$ isomorphic to D_{10}; in particular, the one that is generated by the following matrices

$$A = \begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

With the terminology of [2, Definition 1.2.1] the group $\Gamma_{D_{10}}$ is of *real type*. Assaf's implementation computes the space $S_2(\Gamma_{D_{10}})$ which has dimension 6. This implies that the genus of $X_{D_{10}}(11)$ is 6. We note that one can compute the genus of $X_{D_{10}}(11)$ using known formulas, for example, in [13, Theorem 3.1.1].

Remark 3.1. A different choice of the generators of D_{10} gives an isomorphic space of newforms which will not affect our computations of a model of $X_{D_{10}}(11)$.

The model we get for $X_{D_{10}}(11)$ by Assaf's implementation is given by equations with big coefficients. However, we know that $X_{D_{10}}(11)$ is isomorphic to $X_0(121)$

[1] The curve $X_{D_{10}}(11)$ has label 11.132.6.b.1 in LMFDB beta version [16].
[2] The authors determine a model for the modular curve $X_{S_4}(13)$.

over $L := \mathbb{Q}(\sqrt{-11})$ [4, Lemma 3.3.7]. A model of $X_0(121)$ is given in Galbraith's thesis [14, p. 36] which we recall below.

(3.1)
$$X_0(121): \begin{cases} uw - 2vw + 2ux - 6vx + 2uy + 2vy + uz = 0, \\ uw + vw + 2ux - 2vx + 2uy - 10vy - 5uz + 11vz = 0, \\ -6u^2 + 6uv - 3v^2 - w^2 + 6wx - x^2 - 8wy + 10xy \\ -9y^2 - 4wz + 10xz = 0, \\ 6u^2 + 12uv + 12v^2 - 17wx - 2x^2 - 5wy + 4xy + 14y^2 \\ -6wz - 7xz - 11yz = 0, \\ -9v^2 - 8w^2 + wx + 9x^2 + 7wy - 10xy + y^2 - 7wz + 27xz - 11yz = 0, \\ -6u^2 - 12uv - 12v^2 - 3w^2 + 7wx - 6x^2 + 11wy + 12xy + 10y^2 + 4wz \\ +17xz - 11yz - 11z^2 = 0. \end{cases}$$

We search for a model of $X_{D_{10}}(11)$ so that it is isomorphic to $X_0(121)$ over L but not over $\mathbb{Q}$. Simultaneously, we test if it is isomorphic to the model obtained by Assaf's implementation using *IsIsomorphic* in Magma [7]. So, at the end we obtain the following model:

(3.2)
$$X_{D_{10}}(11): \begin{cases} uw - 2vw + 2ux - 6vx + 2uy + 2vy + uz = 0, \\ uw + vw + 2ux - 2vx + 2uy - 10vy - 5uz + 11vz = 0, \\ -6u^2 + 6uv - 3v^2 + 11w^2 - 66wx + 11x^2 + 88wy - 110xy + 99y^2 \\ +44wz - 110xz = 0, \\ 6u^2 + 12uv + 12v^2 + 187wx + 22x^2 + 55wy - 44xy - 154y^2 + 66wz \\ +77xz + 121yz = 0, \\ -9v^2 + 88w^2 - 11wx - 99x^2 - 77wy + 110xy - 11y^2 + 77wz - 297xz \\ +121yz = 0, \\ -6u^2 - 12uv - 12v^2 + 33w^2 - 77wx + 66x^2 - 121wy - 132xy - 110y^2 \\ -44wz - 187xz + 121yz + 121z^2 = 0 \end{cases}$$

The isomorphism ϕ over L between the two models of $X_{D_{10}}(11)$ and $X_0(121)$ is given explicitly,

(3.3)
$$\begin{aligned} \phi: \ & X_0(121) \to X_{D_{10}}(11), \\ & [x:y:z:u:v:w] \mapsto [x:y:z:\sqrt{-11}u:\sqrt{-11}v:w]. \end{aligned}$$

Let w_{121} be the Atkin-Lehner involution of $X_0(121)$. We define

(3.4)
$$w_{11} := \phi \circ w_{121} \circ \phi^{-1}.$$

We define $X_0^+(121) := X_0(121)/w_{121}$ and $X_{D_{10}}^+(11) := X_{D_{10}}(11)/w_{11}$.

LEMMA 3.2. *The Atkin-Lehner involution w_{121} on $X_0(121)$ and the involution w_{11} on $X_{D_{10}}(11)$ are both defined over $\mathbb{Q}$ and are given by $[x:y:z:u:v:w] \mapsto [x:y:z:-u:-v:w]$ with respect to the models defined by the equations given above.*

PROOF. We know that w_{121} is defined over $\mathbb{Q}$. From [15, Theorem 0.1], [3, Theorem 8] and [6, Proposition] we get that $\mathrm{Aut}_{\mathbb{Q}}(X_0(121)) = \langle w_{121} \rangle \simeq C_2$. Finally, the statement for w_{11} is clear from its definition. □

Then[3] $C := X_0^+(121)$ has genus $g(C) = 2$, hence it is a hyperelliptic curve given by the equation

$$C: \ y^2 = x^6 - 6x^5 + 11x^4 - 8x^3 + 11x^2 - 6x + 1. \tag{3.5}$$

We also have explicitly computed the quotient maps $\phi_{X_0}: X_0(121) \to X_0^+(121)$ and $\phi_{X_{D_{10}}}: X_{D_{10}}(11) \to X_{D_{10}}^+(11)$ which can be found in our GitHub repository.

REMARK 3.3. In the computations in Section 4 we use the fact that both $\phi_{X_{D_{10}}}$ and $X_{D_{10}}^+(11)$ are defined over $\mathbb{Q}$.

LEMMA 3.4. *The curves $X_0^+(121)$ and $X_{D_{10}}^+(11)$ are isomorphic over $\mathbb{Q}$.*

PROOF. We know that $X_0(121)$ and $X_{D_{10}}(11)$ are isomorphic over L under the isomorphism ϕ above. From (3.3) and (3.4) we observe that

$$\phi^\sigma = \begin{cases} \phi, & \sigma|_L = id, \\ \phi \circ w_{121} = w_{11} \circ \phi, & \sigma|_L \neq id, \end{cases}$$

where $\phi^\sigma := \sigma^{-1} \circ \phi \circ \sigma$ and $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Together with the fact that ϕ_{X_0} and $\phi_{X_{D_{10}}}$ are defined over $\mathbb{Q}$ this implies that, when we take quotients by w_{121}, and w_{11}, the curves $X_0^+(121)$ and $X_{D_{10}}^+(11)$ become isomorphic over $\mathbb{Q}$. □

By abusing notation, let $\phi_{X_{D_{10}}}$ denote the composition of $\phi_{X_{D_{10}}}$ and the isomorphism between $X_{D_{10}}^+(11) \simeq C$ then we have the commutative diagram

$$\begin{array}{ccc} X_0(121) & \xrightarrow{\quad\phi\quad} & X_{D_{10}}(11) \\ & {\scriptstyle \phi_{X_0}} \searrow \quad \swarrow {\scriptstyle \phi_{X_{D_{10}}}} & \\ & C & \end{array} \tag{3.6}$$

where every map has been computed explicitly.

4. The Mordell-Weil group of $J_{D_{10}}$

We denote by J_0, $J_{D_{10}}$ and J_C the Jacobians of $X_0(121)$, $X_{D_{10}}(11)$ and C, respectively. It holds that

$$J_0 \sim E_{f_1} \oplus E_{f_2} \oplus E_{f_3} \oplus E_{f_4} \oplus E_{f_5}^2, \tag{4.1}$$

where f_i for $i = 1, 2, 3, 4$ are the four rational newforms of level 121, the ordering is according to the LMFDB, and f_5 is the unique rational newform of level 11. By modularity, f_i corresponds to the elliptic curve E_{f_i} over $\mathbb{Q}$ for each i. It holds that $\mathrm{rank}_{\mathbb{Q}}(E_{f_2}) = 1$ and $\mathrm{rank}_{\mathbb{Q}}(E_{f_i}) = 0$ for $i \neq 2$. Therefore, $\mathrm{rank}_{\mathbb{Q}}(J_0) = 1$.

Moreover, over L we have $\mathrm{rank}_L(E_{f_i}) = 0$ for $i \neq 2$ and $\mathrm{rank}_L(E_{f_2}) = 2$. Because the isogeny in (4.1) is defined over $\mathbb{Q}$, we get $\mathrm{rank}_L(J_0) = \mathrm{rank}_L(J_{D_{10}}) = 2$.

[3] We recall that $X_0^+(121) \simeq X_{sp}^+(11)$.

The curve C has two points at infinity with $\infty = (1,1,0)$ and $(-\infty) = (1,-1,0)$ in the weighted projective plane $\mathbb{P}^2(1,3,1)$. Using the implementation of the method [19] in Magma, we prove that $J_C(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$ with generators $G_1 = [(0,-1) - (-\infty)]$ and $G_2 = [\infty - (-\infty)]$ of order 5 and infinite, respectively. Since Chabauty's rank condition is satisfied for C ($\mathrm{rank}(J_C(\mathbb{Q})) = 1 < 2 = g(C)$), we use the implementation of the method of Chabauty and Coleman in Magma to compute $C(\mathbb{Q})$.

PROPOSITION 4.1. We have that $C(\mathbb{Q}) = \{(1,\pm 2),(0,\pm 1),\pm\infty\}$.

For the computations and the proofs that follow it is important to explicitly compute $\phi^{-1}_{X_{D_{10}}}(C(\mathbb{Q}))$. Using Magma we get

$$\begin{aligned} \phi^{-1}_{X_{D_{10}}}((1,-2)) &= \{P_1,\bar{P}_1\}, \quad \phi^{-1}_{X_{D_{10}}}((1,2)) = \{P_2,\bar{P}_2\},\\ \phi^{-1}_{X_{D_{10}}}(-\infty) &= \{P_3,\bar{P}_3\}, \quad \phi^{-1}_{X_{D_{10}}}(\infty) = \{P_4,\bar{P}_4\},\\ \phi^{-1}_{X_{D_{10}}}((0,-1)) &= \{P_5,\bar{P}_5\}, \quad \phi^{-1}_{X_{D_{10}}}((0,1)) = \{P_6,\bar{P}_6\}, \end{aligned}$$

where $\bar{P}_i$ is the conjugate of P_i.

We will use the commutative diagram (3.6) and the fact that $X_{D_{10}}(11)$ is isomorphic to $X_0(121)$ over L in order to determine a finite index subgroup of $J_{D_{10}}(\mathbb{Q})$.

The first step is to determine $J_C(L)$. Using the information of $J_C(L)$ and the fact that $\phi_{X_{D_{10}}}$ is defined over $\mathbb{Q}$ we are able to determine a finite index supgroup of $J_{D_{10}}(\mathbb{Q})$.

PROPOSITION 4.2. It holds that $J_C(L)_{\mathrm{Tor}} = \langle G_1\rangle$ and $\mathrm{rank}(J_C(L)) = 2$. In particular, the group generated by $\langle G_1, G_2, G_3\rangle$ is a finite index subgroup of $J_C(L)$ with

$$G_3 = \left[\left(\frac{-1+\sqrt{-3}}{2}, -\sqrt{-11}\right) + \left(\frac{-1-\sqrt{-3}}{2}, -\sqrt{-11}\right) - \infty - (-\infty)\right].$$

PROOF. By computing the order of the reduction of J_C modulo good primes and using the fact that the torsion subgroup injects into these groups (in Magma) we get that $\#J_C(L)_{\mathrm{Tor}} \leq 5$. Because $\#J_C(\mathbb{Q})_{\mathrm{Tor}} = 5$ and $J_C(\mathbb{Q})_{\mathrm{Tor}} \subset J_C(L)_{\mathrm{Tor}}$ we understand that $J_C(L)_{\mathrm{Tor}} = J_C(\mathbb{Q})_{\mathrm{Tor}} = \langle G_1\rangle$.

Using the implementation of 2-descent [19] in Magma, we also get that $\mathrm{rank}(J_C(L)) \leq 2$. The point G_3 is a point of infinite order with $G_3 \notin J_C(\mathbb{Q})$. We prove that G_2 and G_3 are linearly independent elements in $J_C(L)$ by using Siksek's code. The idea is the following; if G_2, G_3 are linear dependent then the pairs $(\lambda,\mu) \in \mathbb{Z}^2$ such that $\lambda G_1 + \mu G_2 = 0$ is a subgroup Λ of $\mathbb{Z}^2$. We can also assume that there exists a pair (λ,μ) such that λ,μ are coprime away $\#J_C(L)_{\mathrm{Tor}}$. Using the reduction of $J_C(L)$ modulo small primes we prove that exist a prime $p \nmid \#J_C(L)_{\mathrm{Tor}}$ such that $\Lambda \subseteq p\mathbb{Z}^2$. □

PROPOSITION 4.3. It holds that $\mathrm{rank}(J_{D_{10}}(\mathbb{Q})) = 1$ and $J_{D_{10}}(\mathbb{Q})_{\mathrm{Tor}}$ is isomorphic to C_5 or $C_5 \times C_5$. In particular, the group $G = \langle D_1, D_2\rangle$ where

$$\begin{aligned} D_1 &= \left[P_6 + \bar{P}_6 - P_4 - \bar{P}_4\right],\\ D_2 &= \left[P_3 + \bar{P}_3 - P_4 - \bar{P}_4\right], \end{aligned}$$

with $5D_1 = 0$ and D_2 has infinite order, is a finite index subgroup of $J_{D_{10}}(\mathbb{Q})$ such that $10J_{D_{10}}(\mathbb{Q}) \subseteq G$.

20 Jun 2025 01:07:04 PDT
250129-Koutsianas Version 4 - Submitted to LuCaNT

PROOF. As in Proposition 4.2 we prove that $\#J_{D_{10}}(\mathbb{Q})_{\mathrm{Tor}} \mid 25$. At the same time we also prove that $J_{D_{10}}(\mathbb{Q})_{\mathrm{Tor}} \not\simeq C_{25}$, therefore the torsion part of $J_{D_{10}}(\mathbb{Q})$ is isomorphic to a subgroup of $C_5 \times C_5$. We have that $\phi^*_{X_{D_{10}}}$ injects $J_C(\mathbb{Q})_{\mathrm{Tor}}$ into $J_{D_{10}}(\mathbb{Q})_{\mathrm{Tor}}$ because $(\deg(\phi_{X_{D_{10}}}), \#J_{D_{10}}(\mathbb{Q})_{\mathrm{Tor}}) = 1$. Since, $J_C(\mathbb{Q})_{\mathrm{Tor}} \simeq C_5$ we understand that $J_{D_{10}}(\mathbb{Q})_{\mathrm{Tor}} \simeq C_5$ or $C_5 \times C_5$. Let $D_1 = \phi^*_{X_{D_{10}}}(G_1)$ then it holds $5D_1 = 0$.

The quotient map $\phi_{X_{D_{10}}} : X_{D_{10}}(11) \longrightarrow C$ induces an isogeny $J_{D_{10}} \sim J_C \times A$ where $A/\mathbb{Q}$ is some abelian variety and the isogeny is defined over $\mathbb{Q}$. Since $\mathrm{rank}(J_{D_{10}}(L)) = \mathrm{rank}(J_C(L)) = 2$, we have $\mathrm{rank}(A(L)) = 0$, so $\mathrm{rank}(A(\mathbb{Q})) = 0$. Hence, $\mathrm{rank}(J_{D_{10}}(\mathbb{Q})) = \mathrm{rank}(J_C(\mathbb{Q})) = 1$.

Let $D_2 = \phi^*_{X_{D_{10}}}(G_2) \in J_{D_{10}}(\mathbb{Q})$, then D_2 has an infinite order in $J_{D_{10}}(\mathbb{Q})$ because G_2 has an infinite order in $J_C(\mathbb{Q})$. Finally, from the above and [9, Proposition 3.1] we have that $10J_{D_{10}}(\mathbb{Q}) \subseteq G$. □

5. Symmetric Chabauty

In this section we apply the relative symmetric Chabauty as it is described in [17, 9, 10]. We also give a brief exposition of the idea of symmetric Chabauty following [9, Section 2.2].

5.1. Introduction. Let $X/\mathbb{Q}$ be a smooth projective curve of genus g that has good reduction at a prime $p > 2$. Let J be the Jacobian of X and r the rank of $J(\mathbb{Q})$. We also assume that $r \leq g - 2$, i.e., the Chabauty condition holds for quadratic points. We denote by $\mathcal{X}$ the proper minimal regular model of X. In the space of global differential forms $\Omega_{X/\mathbb{Q}_p}(X)$, we have the $\mathbb{Z}_p$-submodule $\Omega_{\mathcal{X}/\mathbb{Z}_p}(\mathcal{X})$. In [12] Coleman defines the pairing

$$\Omega_{X/\mathbb{Q}_p}(X) \times J(\mathbb{Q}_p) \to \mathbb{Q}_p, \quad \left(\omega, \left[\sum_i P_i - Q_i\right]\right) \mapsto \sum_i \int_{Q_i}^{P_i} \omega.$$

We denote by V the annihilator of $J(\mathbb{Q})$ under the above pairing, write $\mathcal{V} = V \cap \Omega_{\mathcal{X}/\mathbb{Z}_p}(\mathcal{X})$ and let $\tilde{V}$ be the image of $\mathcal{V}$ under the reduction map.

Let $\mathcal{Q} = \{Q_1, Q_2\} \in X^{(2)}(\mathbb{Q})$, where $X^{(2)}$ is the symmetric square of X. Suppose $\omega_1, \cdots, \omega_k$ is a basis of $\tilde{V}$. We fix a place v of $\mathbb{Q}(Q_1, Q_2)$ above p and denote by $\tilde{Q}_i$ the reduction of Q_i with respect to v. Let $t_{\tilde{Q}_i}$ be a uniformiser of $\tilde{Q}_i$. Then, we can expand ω_j around $\tilde{Q}_i$ with respect to $t_{\tilde{Q}_i}$ as a formal power series. In particular, it holds that

$$\omega_j = (a_0(\omega_j, t_{\tilde{Q}_i}) + a_1(\omega_j, t_{\tilde{Q}_i})t_{\tilde{Q}_i} + a_2(\omega_j, t_{\tilde{Q}_i})t^2_{\tilde{Q}_i} + \cdots)dt_{\tilde{Q}_i} \tag{5.1}$$

If $Q_1 \neq Q_2$, we define

$$\mathcal{A} = \begin{pmatrix} a_0(\omega_1, t_{\tilde{Q}_1}) & a_0(\omega_1, t_{\tilde{Q}_2}) \\ \vdots & \vdots \\ a_0(\omega_k, t_{\tilde{Q}_1}) & a_0(\omega_k, t_{\tilde{Q}_2}) \end{pmatrix},$$

and when $Q_1 = Q_2$, we define

$$\mathcal{A} = \begin{pmatrix} a_0(\omega_1, t_{\tilde{Q}_1}) & a_1(\omega_1, t_{\tilde{Q}_1})/2 \\ \vdots & \vdots \\ a_0(\omega_k, t_{\tilde{Q}_1}) & a_1(\omega_k, t_{\tilde{Q}_1})/2 \end{pmatrix}.$$

THEOREM 5.1 ([17, Theorem 3.2]). *Suppose $p \geq 5$. If $\mathrm{rank}(\mathcal{A}) = 2$, then $\mathcal{Q}$ is the only point on $X^{(2)}(\mathbb{Q})$ in its residue class modulo p, i.e. for any $\mathcal{R} \in X^{(2)}(\mathbb{Q})$ such that $\mathcal{Q} \equiv \mathcal{R} \pmod{v}$, we have $\mathcal{R} = \mathcal{Q}$.*

Suppose $\rho : X \to C$ is a degree 2 map to a smooth non-singular curve C and $\mathcal{C}$ its proper minimal regular model. We also assume that C has good reduction at p. Suppose that ρ extends to a morphism $\mathcal{X} \to \mathcal{C}$ which corresponds to a degree 2 map $\tilde{X} = \tilde{\mathcal{X}} \to \mathcal{C}_{\mathbb{F}_p}$. The map $\rho : X \to C$ induces the trace map on the holomorphic differentials $\mathrm{Tr}\colon \Omega_{X/\mathbb{Q}_p}(X) \to \Omega_{C/\mathbb{Q}_p}(C)$, for more details, see [10, §2.6].

Let $\mathcal{V}_0 = \mathcal{V} \cap \ker\left(\Omega_{X/\mathbb{Q}_p}(X) \xrightarrow{\mathrm{Tr}} \Omega_{C/\mathbb{Q}_p}(C)\right)$ and $\tilde{V}_0$ the image of $\mathcal{V}_0$ under the reduction map. Let $\mathcal{Q} = \{Q_1, Q_2\} \in \rho^* C(\mathbb{Q})$, $\omega_1, \cdots, \omega_{k'}$ be a basis of $\tilde{V}_0$ and p, v, $\tilde{Q}_1$, $t_{\tilde{Q}_1}$ be as above.

THEOREM 5.2 ([17, Theorem 4.3]). *Suppose $p \geq 5$. If there exist ω_i for some $i \in \{1, \cdots, k'\}$ such that*

$$\frac{\omega_i}{dt_{\tilde{Q}_1}} \mid_{t_{\tilde{Q}_1}=0} \neq 0,$$

then every point in $X^{(2)}(\mathbb{Q})$ in the residue class of $\mathcal{Q}$ belongs to $\rho^*(C(\mathbb{Q}))$.

5.2. Relative Symmetric Chabauty for $X_{D_{10}}(11)$. Let W be the image of $1 - w_{11}^* : \Omega_{X_{D_{10}}(11)/\mathbb{Q}} \to \Omega_{X_{D_{10}}(11)/\mathbb{Q}}$.

PROPOSITION 5.3. The space W annihilates $J_{D_{10}}(\mathbb{Q})$ under the integration pairing, hence

$$\int_0^D \omega = 0,$$

for all $\omega \in W$ and $D \in J_{D_{10}}(\mathbb{Q})$. In addition, W lies in the kernel of the $\mathrm{Tr}_{\phi_{X_{D_{10}}}} : \Omega_{X_{D_{10}}(11)/\mathbb{Q}} \to \Omega_{C/\mathbb{Q}}$.

PROOF. The proof is similar to [9, Lemma 3.4] because $\mathrm{rank}(J_{D_{10}}(\mathbb{Q})) = \mathrm{rank}(J_C(\mathbb{Q}))$ and $1 + w_{11}^*$ is the trace map with respect to $\phi_{X_{D_{10}}}$. We also use [10, Lemma 2.2]. □

Let $\tilde{W}$ be the image of $W \cap \Omega_{\mathcal{X}_{D_{10}}/\mathbb{Z}_p}$ under the reduction map.

PROPOSITION 5.4. The space $\tilde{W}$ is the image of $1 - \tilde{w}_{11}^* : \Omega_{\tilde{\mathcal{X}}_{D_{10}}/\mathbb{F}_p} \to \Omega_{\tilde{\mathcal{X}}_{D_{10}}/\mathbb{F}_p}$.

PROOF. We use [9, Lemma 3.6] and the proof follows in the same way as the proof of [9, Proposition 3.5]. □

6. Mordell-Weil sieve

In this section, we briefly recall the Mordell-Weil sieve as discussed in [17, 9, 10] and which has its origin in [11]. Again we follow [9, Section 2.4].

Suppose $X/\mathbb{Q}$ be smooth projective curve with Jacobian J and $\rho : X \to C$ a degree 2 map (defined over $\mathbb{Q}$) where $C/\mathbb{Q}$ is another curve. We assume that we have the following data:

(1) $D_1, \cdots, D_r$ are divisors of $J(\mathbb{Q})$ that generate a finite index subgroup G of $J(\mathbb{Q})$,
(2) A number N such that $NJ(\mathbb{Q}) \subset G$,
(3) A rational degree 2 divisor which we denote by ∞,

(4) $\mathcal{L}'$ is a known finite subset of $X^{(2)}(\mathbb{Q})$. The set $\mathcal{L}'$ may also include points from $\rho^*(C(\mathbb{Q}))$,
(5) $p_1, \cdots, p_n$ are primes of good reduction for X.

We define $\mathcal{L} = \mathcal{L}' \cup \rho^* C(\mathbb{Q})$.

Let p be one of the primes $p_1, \cdots, p_r$. We define the maps $\phi : \mathbb{Z}^n \to G$ where $\phi(a_1, \cdots, a_n) = \sum_{i=1}^n a_i D_i$, $\iota : X^{(2)}(\mathbb{Q}) \to G$ where $\iota(\mathcal{Q}) = N[\mathcal{Q} - \infty]$ and $\iota_p : \tilde{X}^{(2)}(\mathbb{F}_p) \to J(\mathbb{F}_p)$ where $\iota_p(\mathcal{R}) = N[\mathcal{R} - \tilde{\infty}]$. In particular, we have the following diagram

$$\begin{array}{ccccccc} \mathcal{L} & \xrightarrow{i} & X^{(2)}(\mathbb{Q}) & \xrightarrow{\iota} & G & \xleftarrow{\phi} & \mathbb{Z}^r \\ & \searrow & \downarrow \text{red} & & \downarrow \text{red} & \swarrow_{\phi_p} & \\ & & \tilde{X}^{(2)}(\mathbb{F}_p) & \xrightarrow{\iota_p} & J(\mathbb{F}_p) & & \end{array}$$

where red is the reduction map and $\phi_p := \text{red} \circ \phi$.

Let $\mathcal{M}_p \subset \tilde{X}^{(2)}(\mathbb{F}_p)$ be the subset of points $\mathcal{R} \in \iota_p^{-1}(\text{Im}(\phi_p))$ which satisfy one of the following:

- $\mathcal{R} \notin \text{red}(\mathcal{L}')$,
- $\mathcal{R} = \tilde{\mathcal{Q}}$ for some point $\mathcal{Q} \in \mathcal{L}' \setminus \rho^* C(\mathbb{Q})$ not satisfying the conditions of Theorem 5.1,
- $\mathcal{R} = \tilde{\mathcal{Q}}$ for some $\rho^* C(\mathbb{Q})$ not satisfying the conditions of Theorem 5.2.

THEOREM 6.1 (Mordell-Weil sieve [17, Theorem 5.1], [9, Theorem 2.6]). *Suppose*

$$\bigcap_{j=1}^{r} \phi_{p_j}^{-1}\left(\iota_{p_j}\left(\mathcal{M}_{p_j}\right)\right) = \emptyset,$$

then $X^{(2)}(\mathbb{Q}) = \mathcal{L}$.

7. Proof of Theorem 1.9

In this section we give the proof of Theorem 1.9. With the notation of Section 6 we set $\mathcal{L}' = \emptyset$ and $\mathcal{L} = \phi^*_{X_{D_{10}}} C(\mathbb{Q}) \subset X_{D_{10}}(11)^{(2)}(\mathbb{Q})$.

PROOF OF THEOREM 1.9. We apply relative symmetric Chabauty for $p = 5, 7, 13, 17, 19, 23$ and we prove that the elements in $\mathcal{L}$ are the only elements in their residue disks modulo p. Because $\mathcal{L}' = \emptyset$ we only had to apply Theorem 5.2. Finally, it is enough to apply the Mordell-Weil sieve, Theorem 6.1, where G is the finite-index subgroup of $J_{D_{10}}(\mathbb{Q})$ from Proposition 4.3, and $N = 10$, for the above choice of primes and get $\mathcal{L} = X_{D_{10}}(11)^{(2)}(\mathbb{Q})$. □

PROOF OF THEOREM 1.8. We may assume that $K \neq \mathbb{Q}(\sqrt{-11})$ by Theorem 1.4. For the other quadratic fields, we may apply Theorem 1.2 and Remark 1.3, which explains that it is enough to compute the quadratic points on $X_{D_{10}}(11)$.

From Theorem 1.9 we have determined the quadratic points of $X_{D_{10}}(11)$. All the quadratic points of $X_{D_{10}}(11)$ are pullbacks of the rational points of C. The image of the set of rational points of C under the j-map has been computed in the LMFDB modular curves database[4] and is equal to

$$J = [\infty, -3375, 8000, -884736, 16581375, -884736000].$$

[4]Since $C \simeq X_{sp}^+(11)$ the j-map of C can be found in https://beta.lmfdb.org/ModularCurve/Q/11.66.2.a.1/.

20 Jun 2025 01:07:04 PDT
250129-Koutsianas Version 4 - Submitted to LuCaNT

Let $\Phi_{11}(x, y)$ be the class modular polynomial. With a short script we show that $\Phi_{11}(x, j_0)$ has a linear factor over $\mathbb{Q}[x]$, hence it also has a linear factor over any quadratic extension $K/\mathbb{Q}$, for all possible $j_0 \in J$ with $j_0 \neq \infty$, which by [5, Proposition 10.1] is enough to conclude the proof. □

References

[1] Samuele Anni. A local-global principle for isogenies of prime degree over number fields. *J. Lond. Math. Soc., II. Ser.*, 89(3):745–761, 2014. 1, 1, 1.5, 1.6, 1.7

[2] Eran Assaf. Computing classical modular forms for arbitrary congruence subgroups. In Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, editors, *Arithmetic Geometry, Number Theory, and Computation*, pages 43–104, Cham, 2021. Springer International Publishing. 1, 1, 3

[3] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970. 3

[4] Barinder S. Banwait. *On some local to global phenomena for abelian varieties*. ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–University of Warwick (United Kingdom). 3, 3

[5] Barinder S. Banwait and John E. Cremona. Tetrahedral elliptic curves and the local-global principle for isogenies. *Algebra Number Theory*, 8(5):1201–1229, 2014. (document), 1, 1.4, 1, 1, 3, 7

[6] Francesc Bars. The group structure of the normalizer of $\Gamma_0(N)$ after Atkin-Lehner. *Comm. Algebra*, 36(6):2160–2170, 2008. 3

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 1, 3, 3

[8] Josha Box. Computing models for quotients of modular curves. *Res. Number Theory*, 7(3):Paper No. 51, 34, 2021. 3

[9] Josha Box. Quadratic points on modular curves with infinite Mordell-Weil group. *Math. Comp.*, 90(327):321–343, 2021. 1, 4, 5, 5.2, 5.2, 6, 6.1

[10] Josha Box, Stevan Gajović, and Pip Goodman. Cubic and Quartic Points on Modular Curves Using Generalised Symmetric Chabauty. *Int. Math. Res. Not. IMRN*, 02 2022. 1, 5, 5.1, 5.2, 6

[11] Nils Bruin and Michael Stoll. Deciding existence of rational points on curves: an experiment. *Experiment. Math.*, 17(2):181–189, 2008. 6

[12] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985. 5.1

[13] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Grad. Texts Math.* Berlin: Springer, 2005. 3

[14] Steven Galbraith. *Equations for modular curves*. PhD thesis, University of Oxford, 1996. https://www.math.auckland.ac.nz/~sgal018/thesis.pdf. 3, 3

[15] M. A. Kenku and Fumiyuki Momose. Automorphism groups of the modular curves $X_0(N)$. *Compositio Math.*, 65(1):51–80, 1988. 3

[16] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024. [Online; accessed 18 October 2024]. 1, 1

[17] Samir Siksek. Chabauty for symmetric powers of curves. *Algebra Number Theory*, 3(2):209–236, 2009. 1, 5, 5.1, 5.2, 6, 6.1

[18] Samir Siksek. Explicit Chabauty over number fields. *Algebra & Number Theory*, 7(4):765 – 793, 2013. 1

[19] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001. 4, 4

[20] Andrew V. Sutherland. A local-global principle for rational isogenies of prime degree. *J. Théor. Nombres Bordeaux*, 24(2):475–485, 2012. 1, 1.2, 1, 3

[21] David Zywina. Computing actions on cusp forms. 2021. https://arxiv.org/abs/2001.07270. 3

Max Planck Institute for Mathematics in Bonn, Charles University Prague

Faculty of Mathematics and Physics, Charles University, Ke Karlovu 3, 121 16 Praha 2, Czech Republic
Email address: stevangajovic@gmail.com

AG Algebra, Geometrie und Computeralgebra, RPTU Kaiserslautern-Landau
Email address: hanselm@rptu.de

Department of Mathematics, Aristotle University of Thessaloniki, 54124, Thessaloniki, Greece.
Email address: akoutsianas@math.auth.gr