In presenting this thesis as a partial fulfillment of the requirements for an advanced degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis in whole or in part in all forms of media, now or hereafter known, including display on the world wide web. I understand that I may select some access restrictions as part of the online submission of this thesis. I retain all ownership rights to the copyright of the thesis. I also retain the right to use in future works (such as articles or books) all or part of this thesis.

Signature:

Jackson Salvatore Morrow	Date

Topics in Elliptic Curves

By

Jackson Salvatore Morrow
Master of Science

Mathematics

David Zureick-Brown
Advisor

Ken Ono
Committee Member

Raman Parimala
Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.
Dean of the James T. Laney School of Graduate Studies

Date

Topics in Elliptic Curves

By

Jackson Salvatore Morrow

Advisor: David Zureick-Brown, Ph.D.

An abstract of
A thesis submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of Science
in Mathematics
2016

Abstract

Topics in Elliptic Curves
By Jackson Salvatore Morrow

In this thesis, the author proves theorems relating to three different areas in the study of elliptic curves: torsion subgroups over number fields, Selmer groups of elliptic curves, and images of Galois. In particular, the thesis contains theorems completing the classification of possible torsion subgroups for elliptic curves defined over cubic number fields; bounding the order of ℓ-Selmer groups for twists of elliptic curves defined over number fields of small degree; and determining the possibilities, indicies, and occurrences of composite level images of Galois for elliptic curves defined over $\mathbf{Q}$.

Topics in Elliptic Curves

By

Jackson Salvatore Morrow

Advisor: David Zureick-Brown, Ph.D.

A thesis submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of Science
in Mathematics
2016

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this thesis, the author proves theorems relating to three different areas in the study of elliptic curves: classification of torsion subgroups over number fields, Selmer groups of elliptic curves, and images of Galois.

First, the author, Anastassia Etropolski, and David Zureick-Brown, in combination with work of Maarten Derickx, complete the classification of isomorphism classes of torsion subgroups for elliptic curves defined over cubic number fields. If the modular curves $X_1(N)$ or $X_1(2, M)$ have rank 0 and gonality at least 4, the authors provably classify the cubic points on these modular curves using a variation of the Mordell-Weil sieve in addition to the moduli property of $X_1(N)$ or $X_1(2, M)$.

Second, the author proves theorems on bounding the order of ℓ-Selmer groups for twists of elliptic curves defined over number fields, where $\ell > 3$ is prime. In [Fre88], Frey provided explicit examples of quadratic twist of elliptic curves over $\mathbf{Q}$ with $\mathbf{Q}$-rational points of odd, prime order ℓ whose ℓ-Selmer groups are non-trivial. The author generalizes Frey's result to elliptic curves defined over number fields of small degree using class field theory and also provides explicit examples of elliptic curves over $\mathbf{Q}$, which satisfy a generalized Frey condition.

Finally, the author proves theorems concerning composite level images of Galois for elliptic curves defined over $\mathbf{Q}$. Building on recent work of Rouse and Zureick-Brown [RZB14] and Zywina [Zyw15], the author finds models for composite level modular curves whose rational points classify elliptic curves over $\mathbf{Q}$ with simultaneously non-surjective composite image of Galois. Also, the author classifies the rational points for all of these curves using a variety of different techniques. Furthermore, the author gives an application of these results to the study of entanglement fields, which play a role in the study of correction factors of various conjectural constants for elliptic curves.

1.1 Organization

In Chapter 2, we recall necessary background information concerning elliptic curves and algebraic number theory. In Chapter 3, we discuss joint work with Anastassia Etropolski, Maarten Derickx, and David Zureick-Brown where the authors complete the the classification of torsion subgroups for elliptic curves defined over cubic number fields. In Chapter 4, we state theorems bounding the order of ℓ-Selmer groups for twists of elliptic curves defined over number fields K and provide examples of elliptic curves over $\mathbf{Q}$, whose base change to K satisfying our theorem.

In Chapter 5, we prove theorems concerning the possibilities, indicies, and occurrences of composite-(m_1, m_2) level image of Galois for elliptic curves defined over $\mathbf{Q}$ for the tuples $(2, \ell)$ where $\ell = 5, 7, 11, 13$ and $(N, 3)$ for $N = 2, 4, 8$. In Chapter 6, we state applications of our results to the study of entanglement fields and, building off previous work of [BJ16], complete the classification of families of elliptic curves over $\mathbf{Q}$ with non-abelian $(2, 3)$-entanglement. In Chapter 7, we discuss future work related to the study of torsion subgroups of elliptic curves defined over quartic number fields, composite level images of Galois, and entanglement fields. Finally, in Ap-

pendix A.3, we present subgroup lattices corresponding to the subgroups from [Zyw15].

1.2 Acknowledgements

It is my pleasure to thank the people that have helped me along this journey.

First and foremost, to my parents Dr. Tika Benveniste and Dr. Casey Morrow. I know the road to this point has been quite bumpy, and yet through all of it, you both never stopped supporting me. I have learned so much from both of you about humility, patience, hard work, and compassion, and I would not be the person I am today without you both. To my chagrin, I don't possess the appropriate vocabulary to properly express my gratitude to you both; all I can say is thank you for keeping me afloat and for all of the love.

To my advisor Dr. David Zureick-Brown: we first met when I was a lowly sophomore at Emory trying to find my way. I was in attendance for the first class you ever taught at Emory, and to this day, I remember us proving that the sum of two even integers is even. It was at that time when I knew I found my passion. It amazes me that that day was nearly four years ago, and just yesterday we had a discussion about derived categories, de Rham cohomology, and the Gauss-Manin connection. I have learned so much from you over these past few years, not only about mathematics, coffee, and beer, but also about how to professionally conduct oneself, how to be open to new ideas, and most importantly how to be an amazing advisor. I am beyond thrilled to have the opportunity to spend the next few years with you trying to learn everything about everything.

To my committee member Prof. Ken Ono: during my junior year at Emory, I attended both of your courses on elementary number theory and abstract algebra. Your enthusiasm and passion for the subject infected me

and inspired me to pursue a graduate career in mathematics. It was a wonderful experience to work with you on a project this past year, and I hope that we will have the opportunity to work on numerous others in the coming years.

To my committee member: Prof. Parimala: during my junior year at Emory, I attended your abstract algebra course, where you introduced me to the rigor and beauty of algebra. It has been a joy to attend your courses and student seminars and to hear your countless, insightful comments on étale cohomology and algebraic groups. To Prof Suresh: thank you for your wonderful course on topology and for always making me think about counterexamples. It has been a pleasure to see you and Prof. Parimala's banter during the étale cohomology and to witness how mathematics is done.

To my friends at Emory: there have been many of you who have supported me through ups and down, such as CJ Ferraro and April Yang. A special shout-out to Henry Yelin who first showed me that mathematics was awesome and introduced me to David Zureick-Brown and to amazing coffee; I know I would not be here without Henry's friendship. Over these past three years, I have made some wonderful friends in the mathematics department at Emory. To Vicman: thank you for your company on the 7 a.m. car rides to the department and for showing me the beautiful symmetry of modular forms. To Bastian: thank you for your patience in explaining algebraic geometry to me. You have shown me how the subtlest details impact a proof, and I look forward to annoying you in the future with more algebraic geometry questions. To Mckenzie: thank you for your friendship, delicious baked goods, and discussion on Brauer groups and CSAs. To Anastassia: thank you for including me in your project concerning cubic torsion and for awesome discussions about Chabauty and elliptic curves. I know there are must be people I have forgotten, however, I hope it does not take away from the gratitude I feel for them; their names will not fit into the margin of the page.

Chapter 2

Background

An elliptic curve E is a smooth, projective, algebraic curve of genus one, with a distinguished point $\mathcal{O}$. For a characteristic $\neq 2, 3$ field K, an elliptic curve defined over K can be written in Weierstrass form as, $y^2 = x^3 + Ax + B$ where $A, B \in K$ and $4A^3 + 27B^2 \neq 0$. The set of K-rational points of E, $E(K)$, forms abelian group with operation defined by setting $P_1 + P_2 + P_3 = \mathcal{O}$ if and only if P_1, P_2, and P_3 are co-linear; so E is an abelian variety of dimension one. The epochal theorem of Mordell-Weil describes the structure of the group $E(K)$.

Theorem 2.0.1 (Mordell-Weil, 1928)**.** *For an elliptic curve* E *defined over a number field* K*, the group* $E(K)$ *is a finitely generated abelian group:*

$$E(K) \cong \mathbf{Z}^r \oplus E[\text{tors}].$$

We call the rank r of the free part of $E(K)$, the rank of E and the finite group $E[\text{tors}]$, the torsion subgroup of E/K. In this thesis, we will prove results relating to the study of both the rank and torsion subgroup of E/K. This chapter is devoted to background information concerning the classification of torsion subgroups over number fields, the algebraic approach to studying

the rank, and class field theory.

2.1 Torsion subgroups

Let E be an elliptic curve over a number field K. For any positive integer n, we denote the n-torsion subgroup of $E(\overline{K})$, where $\overline{K}$ is a fixed algebraic closure of K, by $E[n]$. For a prime ℓ, let

$$E[\ell^\infty] := \bigcup_{n \geq 1} E[\ell^n] \cong \varinjlim_n E[\ell^n]$$

and

$$E[\mathrm{tors}] := \bigcup_{n \geq 1} E[n] \cong \varinjlim_n E[n].$$

By fixing a $\widehat{\mathbf{Z}}$-basis for $E[\mathrm{tors}]$, there is an induced $\mathbf{Z}_\ell$-basis on $E[\ell^\infty]$ for any prime ℓ, and for any positive integer n, there is an induced $\mathbf{Z}/n\mathbf{Z}$-basis on $E[n]$. The absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ has a natural action on each torsion subgroup, which respects each group structure. In particular, we have the following continuous representations:

$$\begin{aligned}
\rho_{E,n} &\colon G_K \longrightarrow \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \cong \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) && (\mathrm{mod}\ n),\\
\rho_{E,\ell^\infty} &\colon G_K \longrightarrow \mathrm{Aut}(E[\ell^\infty]) \cong \mathrm{GL}_2(\mathbf{Z}_\ell) && (\ell\text{-adic}),\\
\rho_E &\colon G_K \longrightarrow \mathrm{Aut}(E[\mathrm{tors}]) \cong \mathrm{GL}_2(\widehat{\mathbf{Z}}) && (\text{adélic}),
\end{aligned}$$

where the image under ρ is uniquely determined up to conjugacy in its respective general linear group. The n-division field $K(E[n])$ is the fixed field of $\overline{K}$ by the kernel of the mod n representation. Moreover, the Galois group of this number field is the image of the mod n representation.

A celebrated theorem of Serre [Ser72] says that for an elliptic curve over K without complex multiplication, the adélic representation ρ_E has open image

in $\mathrm{GL}_2(\widehat{\mathbf{Z}})$. Serre's theorem raised many questions concerning the possible images of the adélic representation. Observe that the group $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ is both a product group and a profinite group via the following isomorphisms

$$\prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbf{Z}_\ell) \cong \mathrm{GL}_2(\widehat{\mathbf{Z}}) \cong \varprojlim_n \mathrm{GL}_2(\mathbf{Z}/\ell^n\mathbf{Z}).$$

Serge Lang [Lan87] refered to these two characterizations as the "vertical" and "horizontal" natures of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$. This binal nature of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ provides two flavors of questions stemming from Serre's work.

Horizontally speaking, for any non-CM elliptic curve over K, there exists a smallest integer $r_{E/K} > 0$ such that for all $\ell \geq r_{E/K}$, the ℓ-adic representation is surjective. Indeed, since the image of ρ_E is open in the topological space $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ endowed with the product topology. Serre asked whether $r_{E/K}$ depends only on K, and he conjectured that $r_{E/\mathbf{Q}} = 37$. In [Zyw11], Zwyina gives a refined conjecture concerning the surjectivity of the mod ℓ and provides a practical algorithm (implemented in Sage) to compute the finite set of primes ℓ for which $\rho_{E,\ell}$ is not surjective; a prime ℓ is called exceptional if it belongs to this finite set.

Vertically speaking, one question that has garnered attention is determining when the adélic image is surjective. Serre showed that the adélic image is always contained in some index 2 subgroup of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$, hence $\rho_E \neq \mathrm{GL}_2(\widehat{\mathbf{Z}})$ for E defined over $\mathbf{Q}$. In his Ph.D. thesis, Greicius [Gre10] found necessary and sufficient conditions on a number field L, namely $\mathbf{Q}^{\mathrm{cyc.}} \cap L = \mathbf{Q}$, for which ρ_E could be surjective, and building on previous work of Duke and Jones in [Duk97, Jon10], Zywina proved that almost all elliptic curves (in the sense of density) have surjective, adélic image of Galois ([Zyw10a, Zyw10b]).

The vertical variant also leads us to determine the possible values for the index of the adélic image for a given non-CM elliptic curve, which is the focus of Mazur's Program B [Maz77, Program B]. This program initiated

with Mazur's work [Maz77] in which he proved for which prime values ℓ does an elliptic curve $E/\mathbf{Q}$ have a $\mathbf{Q}$-rational isogeny; in doing so, he positively answered a conjecture of Ogg on the possible torsion structures of $E(\mathbf{Q})[\mathrm{tors}]$.

Theorem 2.1.1 (Theorem 2 [Maz77]). *Let E be an elliptic curve defined over $\mathbf{Q}$. The torsion subgroup $E[\mathrm{tors}]$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} &\mathbf{Z}/N_1\mathbf{Z} && 1 \leq N_1 \leq 12, N_1 \neq 11, \\ &\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/N_2\mathbf{Z} && 1 \leq N_2 \leq 4. \end{aligned}$$

Furthermore, each of these torsion subgroups occurs infinitely often.

As a consequence of [Maz77, Theorem 2] and Serre's open image theorem, Mazur [Maz77, Theorem 3] showed that for an elliptic curve $E/\mathbf{Q}$ and a prime ℓ, there are three possibilities for the mod ℓ image:

1. $\rho_\ell \colon G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ is surjective,
2. the image ρ_ℓ is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$,
3. $N \leq 19$ or $N = 37, 43, 67,$ or 163.[1]

At its core, Mazur's Program B studies the following question: given an open subgroup $H \subset \mathrm{GL}_2(\widehat{\mathbf{Z}})$, classify all elliptic curves E/k such that the image of ρ_E is contained in H. The work of this program suggests that there exists a constant $B(k)$ such that for every elliptic curve E/k without complex multiplication, the index of $\rho_E(G_k)$ in $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ is bounded by $B(k)$.

[1] In this case, the image of ρ_ℓ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$.

To determine $\rho_E(G_k)$, one begins by computing the ℓ-adic image ρ_{E,ℓ^∞} for each prime ℓ, which leads to the following inclusions

$$\rho_E(G_k) \hookrightarrow \prod_{\ell \text{ prime}} \rho_{E,\ell^\infty}(G_k) \subseteq \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbf{Z}_\ell) \cong \mathrm{GL}_2(\widehat{\mathbf{Z}}).$$

The image of $\rho_E(G_k)$ under the above inclusion will project onto each ℓ-adic factor. To determine the ℓ-adic image, we need to understand the mod ℓ^n image for sufficiently large n.

In recent works, Zywina [Zyw15] describes all known, and conjecturally all, pairs (E, ℓ) such that $\rho_{E,\ell}(G_{\mathbf{Q}})$ is non-surjective, and Rouse and Zureick-Brown [RZB14] give a complete classification of the 1208 possible 2-adic images of Galois representations associated to non-CM elliptic curves over $\mathbf{Q}$. In both of these works, the authors first determine which subgroups G can occur as $\pm\rho_{E,\ell}(G_{\mathbf{Q}})$ and $\pm\rho_{E,2^n}(G_{\mathbf{Q}})$, then proceed by finding equations for the modular curves X_G. If the modular curve X_G has genus equal to 0 and $X_G(\mathbf{Q}) \neq \emptyset$, the authors give rational functions whose values map $X_G \to X(1)$ via the j-line; the computations of these equations occupies the majority of [RZB14] and [Zyw15]. These values correspond to j-invariants of non-CM elliptic curves over $\mathbf{Q}$ with image of Galois conjugate to a subgroup of G. In this thesis, we shall advantageously use these equations to study the composite-(m_1, m_2) level image $(\rho_{E,m_1} \times \rho_{E,m_2})(G_{\mathbf{Q}})$ where m_1, m_2 are relatively prime. Moreover, we determine the possible indicies and the frequencies with which they occur of the composite-(m_1, m_2) level image for the tuples $(2, \ell)$ for $\ell = 5, 7, 11, 13$ and the tuples $(N, 3)$ for $N = 2, 4, 8, 16$.

Mazur's work also inspired the study of possible torsion structures over number fields of small degree. We provide a terse summary of these results and refer the reader to [Sut12b] for a full exposition. We define the set $S(d)$ as the set of primes p for which there exists a number field K of degree $\leq d$ and an elliptic curve E/K such that $p|\#E(K)[\text{tors}]$. We also define $\Phi(d)$

as the set of possible isomorphism types for $E(K)[\mathrm{tors}]$ over all K and E as above. From the work of Faltings and Frey, if $S(d)$ is finite, then $\Phi(d)$ is finite. In [Mer96], Merel proved that for all $d \geq 1$, the set $S(d)$ is bounded by a constant dependent on d; we will denote this by $B(d)$. From the previous works, we have that $\Phi(d)$ is also finite. Moreover, there exist bounds for the value of $p \in S(d)$ that are exponential in d, in particular $p \leq (3^{d/2}+1)^2$ i.e.,

$$S(d) \subset \mathrm{Primes}(3^{d/2}+1)^2.$$

In [Par99], Parent proved an explicit upper bound on the largest prime power that can divide $\#E(K)[\mathrm{tors}]$, yielding an explicit value for $B(d)$ in this case.

The exact value of the set $S(n)$ is currently known for $n \leq 5$, but reasonable good bounds on $S(6)$ and $S(7)$ are given in [Der12]. The exact values of $\Phi(d)$ were previously only known for $n \leq 2$. In this thesis, we compute the exact value for $\Phi(3)$ in joint work with Anastassia Etropolski, Maarten Derickx, and David Zureick-Brown.

n	$S(n)$	Reference	$\#\Phi(n)$	Reference
1	$\mathrm{Primes}(7)$	[Maz77]	15	[Maz77]
2	$\mathrm{Primes}(13)$	[Kam92]	26	[KM+88, Kam92]
3	$\mathrm{Primes}(13)$	[Par03]	26	Theorem 3.1.3
4	$\mathrm{Primes}(17)$	[KSS]	$38 \geq$	
5	$\mathrm{Primes}(19)$	[DKSS]	?	
6	$\subseteq \mathrm{Primes}(19) \cup \{37, 73\}$	[Der12]	?	

Figure 2.1: Summary of $S(n)$ and $\Phi(n)$ for $n \leq 6$

Remark 2.1.2. One can also consider the subset $S_{\mathbf{Q}}(n) \subseteq S(n)$ corresponding to primes that can arise as the order of a rational point on an elliptic curve $E_K = E \times_{\mathbf{Q}} K$ where E is defined over $\mathbf{Q}$ and K is a number field of degree n, and similarly the value $\Phi_{\mathbf{Q}}(n) \leq \Phi(n)$ corresponding to the set of possible isomorphism types for $E(K)[\mathrm{tors}]$ over all K and E_K as above. From [LR13],

it is known that

$$S_{\mathbf{Q}}(n) \subseteq \mathsf{Primes}(13) \cup \{37\} \cup \mathsf{Primes}(2n+1),$$

and [LR13, Corollary 1.1] gives precise values of $S_{\mathbf{Q}}(n)$ for $1 \leq n \leq 21$.

2.2 Algebraic study of rank

We now turn our attention to the algebraic study of rank r of E/K. Loosely speaking, the proof of the Mordell-Weil theorem relies on a combination of the weak Mordell-Weil theorem and height arguments. The weak Mordell--Weil theorem asserts that for $m \geq 2$ the quotient $E(K)/m := E(k)/mE(K)$ is finite. Using Kummer theory and Galois cohomology, this statement is equivalent to the finiteness of the Galois extension $K([m]^{-1}E(K))$, which is the compositum of all fields fields $K(Q)$ as Q ranges over all of the points in $E(\overline{K})$ for which $[m]Q \in E(K)$. Moreover, the weak Mordell-Weil theorem is not apparently effective in the sense that the proof does not explicitly produce the rank or the torsion subgroup of $E(K)$. If the Sharfarevich-Tate group $Ш(E)$ is finite, then the weak Mordell-Weil theorem is effective (see [Sil09, Chapter X.5]). To exhibit a detailed description of $E(K)$, one needs to better understand the quotient $E(K)/m$.

Let $E[m]$ denote the kernel of the multiplication by $[m]\colon E(\overline{K}) \to E(\overline{K})$. The multiplication by m induces the short exact sequence of G_K-modules

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \longrightarrow E(\overline{K}) \longrightarrow 0.$$

If we take Galois cohomology of this sequence and make appropriate reductions, we find that

$$E(K)/m \hookrightarrow H^1(K, E[m]).$$

The weak Mordell-Weil theorem tells us that $E(K)/m$ is finite; however, we know that $H^1(K, E[m])$ is infinite. Hence, we need to find a finite subgroup of $H^1(K, E[m])$ that the quotient $E(K)/m$ injects into. We accomplish this by local approximations.

More specifically, consider the following diagram

$$\begin{array}{ccc} E(K)/m & \xhookrightarrow{\delta} & H^1(K, E[m]) \\ \downarrow & & \downarrow \mathrm{Res}_v \\ \prod_v E(K_v)/m & \xrightarrow{\delta_v} & \prod_v H^1(K_v, E(\overline{K}_v)[m]) \end{array}$$

where δ is the connecting homomorphism from Galois cohomology, v is a place of K, and $E(K_v)/m := E(K_v)/mE(K_v)$. We define the m-Selmer group of E/K to be

$$\mathrm{Sel}_m(E, K) := \left\{ \xi \in H^1(K, E[m]) : \mathrm{Res}_v(\xi) \subset \mathrm{Im}(\delta_v) \text{ for all } v \right\} \subset H^1(K, E[m]). \tag{2.2.1}$$

The m-Selmer group of E/K is finite (see [Sil09, Theorem X.4.2(b)]), and hence the above injection becomes

$$E(K)/m \hookrightarrow \mathrm{Sel}_m(E, K) \hookrightarrow H^1(K, E[m]).$$

Therefore, we can understand the quotient $E(K)/m$ by determining the size of the m-Selmer group. In [Fre88, Theorem 1], Frey exhibits examples of quadratic twists of elliptic curves over $\mathbf{Q}$ with $\mathbf{Q}$-rational points of odd, prime order ℓ whose ℓ-Selmer groups are non-trivial, where $\ell \geq 3$ is prime. In this thesis, we generalize Frey's result to elliptic curves defined over number fields K of small degree using class field theory. We also provide explicit examples of elliptic curves over $\mathbf{Q}$ whose base change to a number K satisfy the generalized Frey condition.

2.3 Class field theory

To prove our results in Chapter 4, we will need to recall some definitions and results from algebraic number theory and class field theory. Let L/K be a Galois extension of K, with ring of integers $\mathcal{O}_L$ and $\mathcal{O}_K$. For any finite prime $\mathfrak{P} \in \mathcal{O}_L$ lying over a prime $\mathfrak{p} \in \mathcal{O}_K$, let $D(\mathfrak{P})$ denote the decomposition group of $\mathfrak{P}$, let $I(\mathfrak{P})$ denote the inertia group of $\mathfrak{P}$ and let $\kappa' := \mathcal{O}_L/\mathfrak{P}$ and $\kappa = \mathcal{O}_K/\mathfrak{p}$ be the residue fields of characteristic $q = p^n$. The Galois theory of the extension encodes the splitting and ramification of $\mathfrak{P}$ over $\mathfrak{p}$, in particular, we have the below correspondence.

$$\begin{array}{ccc}
L & & 1 \\
{\scriptstyle e=|I(\mathfrak{P})|}\big| & & \big|{\scriptstyle e=|I(\mathfrak{P})|} \\
K^{I(\mathfrak{P})} & & I(\mathfrak{P}) \\
{\scriptstyle f=|D(\mathfrak{P})|/e}\big| & & \big|{\scriptstyle f=|D(\mathfrak{P})|/e} \\
K^{D(\mathfrak{P})} & & D(\mathfrak{P}) \\
{\scriptstyle g=n/ef}\big| & & \big|{\scriptstyle g=n/ef} \\
K & & \mathrm{Gal}(L/K)
\end{array}$$

The exact sequence

$$1 \longrightarrow I(\mathfrak{P}) \longrightarrow D(\mathfrak{P}) \longrightarrow \mathrm{Gal}(\kappa'/\kappa) \longrightarrow 1$$

induces an isomorphism $D(\mathfrak{P})/I(\mathfrak{P}) \cong \mathrm{Gal}(\kappa'/\kappa)$. In particular, there is a unique element in $D(\mathfrak{P})/I(\mathfrak{P})$, denote by $\left[\frac{L/K}{\mathfrak{P}}\right]$, which maps to the q^{th} power Frobenius map $\mathrm{Frob}_q \in \mathrm{Gal}(\kappa'/\kappa)$ under the isomorphism, where q is the number of elements in κ. The notation $\left[\frac{L/K}{\mathfrak{P}}\right]$ is referred to as the Artin symbol of the extension L/K at $\mathfrak{P}$. If L/K is an abelian extension, then the Frobenius automorphism $\left[\frac{L/K}{\mathfrak{P}}\right]$ is denoted $\left(\frac{L/K}{\mathfrak{p}}\right)$; this change in notation

reflects the fact that the automorphism is determined by $\mathfrak{p} \in \mathcal{O}_K$ independent of the primes $\mathfrak{P}$ of $\mathcal{O}_L$ above it.

Definition 2.3.1. Now let $\mathfrak{m}$ be a modulus divisible by all (finite or infinite) ramified primes of an abelian extension L/K. There is therefore a canonically defined Frobenius element in $\mathrm{Gal}(L/K)$ denoted $\mathrm{Frob}_{\mathfrak{p}}$. The Artin symbol of L/K is defined on the group of prime-to-$\mathfrak{m}$ fractional ideals, $I_K(\mathfrak{m})$, by linearity:

$$\begin{aligned} \left(\frac{L/K}{\bullet}\right) : I_K(\mathfrak{m}) &\longrightarrow \mathrm{Gal}(L/K) \\ \prod_{i=1}^{m} \mathfrak{p}_i^{n_i} &\longmapsto \prod_{i=1}^{m} \mathrm{Frob}_{\mathfrak{p}_i}^{n_i}. \end{aligned}$$

Therefore, we can extend the Artin symbol to give us a group homomorphism

$$\Phi_{\mathfrak{m}} \colon I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

called the global Artin map.

Just as Legendre symbols encode splitting data for rational primes $\mathfrak{p}$ in quadratic fields, Artin symbols capture this information for primes $\mathfrak{p} \subset \mathcal{O}_K$ in quadratic extensions L/K.

Lemma 2.3.2. *Let L/K be a quadratic extension, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, let $\mathfrak{m} = \Delta_{L/K}$ in the definition of the global Artin map, and let $\mathfrak{P}$ denote some prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$, and let $\langle\delta\rangle = \mathrm{Gal}(L/K)$. Then:*

1. *$\mathfrak{p}$ is unramified and splits completely in $L \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{id}$,*
2. *$\mathfrak{p}$ is unramified and non-split in $L \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \delta$,*
3. *$\mathfrak{p}$ is ramified in $L \iff \mathfrak{p} | \Delta_{L/K}$ where $\Delta_{L/K}$ denotes the relative discriminant of L/K.*

Proof. Part (3) follows from Definition 5.1.12. Since $\mathfrak{p}$ is unramified, we know that $|D(\mathfrak{P})| = f$ where f is the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$. A prime $\mathfrak{p}$ splits completely in L if and only if the ramification index e of $\mathfrak{P}$ above $\mathfrak{p}$ and the inertia degree f of $\mathfrak{P}$ above $\mathfrak{p}$ are equal to 1. Hence,

$$|D(\mathfrak{P})| = [\kappa' : \kappa] = 1 \iff \operatorname{ord}\left(\frac{L/K}{\mathfrak{p}}\right) = 1 \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{id},$$

which proves (1). For (2), our assumptions and the fundamental identity tell us that $e = 1$ and $g = 1$ if and only if $f = 2$. Thus,

$$|D(\mathfrak{P})| = [\kappa' : \kappa] = 2 \iff \operatorname{ord}\left(\frac{L/K}{\mathfrak{p}}\right) = 2 \iff \left(\frac{L/K}{\mathfrak{p}}\right) = \delta.$$

□

In Theorem 4.2.1, we use Hecke characters to describe a subset of primes $\mathfrak{p}|N(E)$. We recall the definition of these characters and discuss how their values can encode information about ramification.

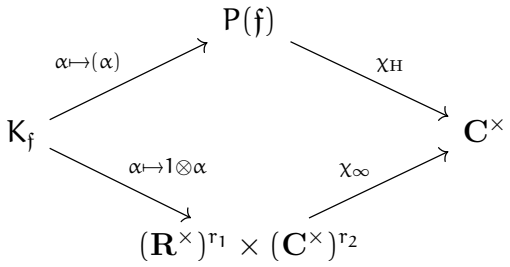
Definition 2.3.3. Let $\mathfrak{f}$ be a non-zero ideal of $\mathcal{O}_K$, and let

$$\chi_\infty \colon (\mathbf{R}^\times)^{r_1} \times (\mathbf{C}^\times)^{r_2} \longrightarrow \mathbf{C}^\times$$

be a continuous character where $[K : \mathbf{Q}] = r_1 + 2r_2$. Then the character

$$\chi_H \colon I(\mathfrak{f}) \longrightarrow \mathbf{C}^\times$$

is a Hecke character with conductor $\mathfrak{f}$ and infinity-type χ_∞ if the following diagram below commutes, where $I(\mathfrak{f})$ is the group of fractional ideals corprime to $\mathfrak{f}$ and $P(\mathfrak{f})$ is the group of principal ideals of $\mathcal{O}_K$ relatively prime to $\mathfrak{f}$. A Hecke character is primitive if it is not induced from another classical Hecke character with conductor $\mathfrak{f}'|\mathfrak{f}$.



Remark 2.3.4. Recall that there is a conductor-preserving correspondence between primitive Dirichlet characters of order ℓ and cyclic, degree ℓ number fields $k/\mathbf{Q}$. From [Was12, Theorem 3.7], the Dirichlet character χ corresponds to the fixed field k of $\ker\chi \subseteq (\mathbf{Z}/f_\chi\mathbf{Z})^\times = \mathrm{Gal}(\mathbf{Q}(\zeta_{f_\chi})/\mathbf{Q})$. For any prime q,

$$\chi(q) = 0 \iff q \text{ ramifies in } k, \quad \text{and} \quad \chi(q) = 1 \iff q \text{ splits in } k.$$

By class field theory, any Hecke character χ_H of K of order ℓ determines a cyclic extension N/K of degree ℓ. Moreover, the set of Hecke characters determining this cyclic extension equals $\{\chi_H, \chi_H^2, \ldots, \chi_H^{\ell-1}\}$. These $\ell-1$ Hecke characters have the same conductor $\mathfrak{f}$, and the determinant of L/K equals their product $\mathfrak{f}^{\ell-1}$ by the Hasse conductor-discriminant theorem. Thus for any prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$, we have that

$$\chi_H(\mathfrak{q}) = 0 \iff \mathfrak{q} \text{ ramifies in } N, \quad \text{and} \quad \chi_H(\mathfrak{q}) = 1 \iff \mathfrak{q} \text{ splits in } N.$$

Chapter 3

Torsion in cubic number fields

3.1 Introduction

In Section 2.1, we briefly discussed the torsion behavior of elliptic curves over number fields K. In this chapter, we provide a detailed account of the case where K is a degree 3 number field. For the remainder of this chapter, let K be a cubic number field. The first step in the cubic classification was to determine, which torsion subgroups can occur infinitely often.

Theorem 3.1.1 (Theorem 3.4 [JKS04])**.** *As K varies over all cubic number fields and E varies over all elliptic curves defined over K, the abelian groups which appear infinitely often as $E(K)[\mathrm{tors}]$ are exactly the following:*

$$\begin{aligned} &\mathbf{Z}/N_1\mathbf{Z} && N_1 = 1, \ldots, 16, 18, 20, \\ &\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/N_2\mathbf{Z} && N_2 = 1, \ldots, 7. \end{aligned}$$

As alluded to in Remark 2.1.2, one may consider the question of determining the possible torsion subgroups of elliptic curves with $\mathbf{Q}$ coefficients defined over a cubic number field K. Najman [Naj12] classified all of theses structures and found a sporadic cubic point on $X_1(21)$.

Theorem 3.1.2 (Theorem 1 [Naj12]). *Let* $E/\mathbf{Q}$ *be an elliptic curve with rational coefficients, and let* $K/\mathbf{Q}$ *be a cubic number field. Then* $E(K)[\mathrm{tors}]$ *is one of the following:*

$$\begin{aligned} &\mathbf{Z}/N_1\mathbf{Z} && N_1 = 1,\dots,10,12,13,14,18,21, \\ &\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/N_2\mathbf{Z} && N_2 = 1,2,3,4,7. \end{aligned}$$

The elliptic curve `162b1` *over* $\mathbf{Q}(\zeta_9)^+$ *is the unique rational elliptic curve over a cubic field with* $\mathbf{Z}/21\mathbf{Z}$ *torsion. For all of the other groups* G*, there exists infinitely many rational elliptic curves with torsion subgroup* G*.*

Since degree 3 is the lowest possible degree of a sporadic point on a modular curve $X_1(N)$, it was formally conjectured in [Wan15, Conjecture 1.1.2] that only possible torsion structures for elliptic curves over K are listed above in Theorems 3.1.1, 3.1.2. In combination with work of Maarten Derickx, Anastassia Etropolski, the author, and David Zureick-Brown provide a positive answer to this conjecture.

Theorem 3.1.3. *Let* E *be an elliptic curve defined over* K*. The torsion subgroup* $E[\mathrm{tors}]$ *is isomorphic to one of the following* 26 *groups:*

$$\begin{aligned} &\mathbf{Z}/N_1\mathbf{Z} && N_1 = 1,\dots,16,18,20,21, \\ &\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/N_2\mathbf{Z} && N_2 = 1,\dots,7. \end{aligned}$$

The elliptic curve `162b1` *defined over* $\mathbf{Q}(\zeta_9)^+$ *is the unique elliptic curve over a cubic field with* $\mathbf{Z}/21\mathbf{Z}$ *torsion.*

To prove of Theorem 3.1.3, we need to find the cubic points on the modular curves $X_1(N)$ and $X_1(2,M)$ where N, M are specific composite integers. In this thesis, we discuss our method to provably compute the cubic points on the modular curves $X_1(N)$ or $X_1(2,M)$ with rank 0 and gonality at least

4. Given a modular curve $X_1(N)$ or $X_1(2, M)$, our rank and gonality assumptions suggest that there are no $\mathbf{Q}$-rational points on the symmetric cube $\mathrm{Sym}^3 X$, and hence we need a technique to verify that our curve does not have any rational points outside of the rational cusps.

3.2 Proof technique of Theorem 3.1.3

Let X be a smooth projective geometrically irreducible curve of genus ≥ 3 defined over a number field K. The gonality, denoted by γ, is defined to be the least possible degree of any non-constant morphism $X \to \mathbf{P}^1$. Let J denote the Jacobian of X.

Definition 3.2.1. For a positive integer d, the d^{th}-symmetric power of X, is defined by $\mathrm{Sym}^d X := X^d/S_d$ where S_d is the symmetric group on d letters.

Remark 3.2.2. The points on $\mathrm{Sym}^d X$ corresponds to effective K-rational divisors on X of degree d.

Suppose that $\mathrm{Sym}^d X(\mathbf{Q})$ is non-empty and let E be a fixed divisor of degree d. We consider the corresponding Abel-Jacobi map $D \mapsto D - E$. If X has a K rational point P, we typically take E to be dP. In our situation, we have $d = 3$ and $\gamma \geq 4$, which implies that $\mathrm{Sym}^d X(K)$ is isomorphic to its image in J. Moreover, it follows from Faltings' theorem [Fal94] that $\mathrm{Sym}^d X(K)$ is finite.

3.2.3 Mordell-Weil sieve

This technique is used to verify that a given curve $X/\mathbf{Q}$ does not have any $\mathbf{Q}$-rational points. The idea is to derive a contradiction from various bits of local information, using the global constraint that a $\mathbf{Q}$-rational point on the curve maps into the Mordell-Weil group. Given a curve $X/\mathbf{Q}$ consider the

commutative diagram where ν runs through the (finite and infinite) place of $\mathbf{Q}$,

$$\begin{array}{ccc} X(\mathbf{Q}) & \xhookrightarrow{\iota} & \mathrm{Jac}_X(\mathbf{Q}) \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} \\ \prod_\nu X(\mathbf{Q}_\nu) & \xhookrightarrow{\prod \iota_\nu} & \prod_\nu \mathrm{Jac}_X(\mathbf{Q}_\nu). \end{array}$$

We assume that we know an embedding $\iota\colon X \to \mathrm{Jac}_X$ defined over $\mathbf{Q}$ (e.g. we know a $\mathbf{Q}$-rational divisor class of degree 1 on X) and that we know generators of the Mordell-Weil group $\mathrm{Jac}_X(\mathbf{Q})$. If the images of α and ι_ν are disjoint, then $X(\mathbf{Q}) = \emptyset$.

As a further simplification, we can just use a set S of primes of good reduction and replace the above diagram by the following one:

$$\begin{array}{ccc} X(\mathbf{Q}) & \xhookrightarrow{\iota} & \mathrm{Jac}_X(\mathbf{Q}) \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} \\ \prod_{p\in S} X(\mathbf{F}_p) & \xhookrightarrow{\iota_S} & \prod_{p\in S} \mathrm{Jac}_X(\mathbf{F}_p). \end{array}$$

Furthermore, the Mordell-Weil sieve asserts that

$$\alpha(\mathrm{Jac}_X(\mathbf{Q})) \cap \iota_S(\beta(X(\mathbf{Q}))) = \emptyset \iff X(\mathbf{Q}) = \emptyset.$$

See [BS10] for a further discussion of the Mordell-Weil sieve.

3.2.4 A four-fold Mordell-Weil sieve

Let N, M be composite integers. We now outline the general technique of proof to compute cubic points on the modular curves $X_1(N)$ or $X_1(2, M)$ with rank 0 and gonality at least 4.

Remark 3.2.5. To compute the rank of $J_1(N)$, we utilize theorems of Kolyvagin and Logach [KL89] relating non-zero values of L-series of modular abelian

varieties at $s = 1$ and finiteness of the Mordell-Weil group. Using MAGMA, we can decompose the modular abelian varieties $J_1(N)$ into abelian factors B_i and compute the non-vanishing of the L-series at $s = 1$ via the command `IsZeroAt(LSeries(B),1)`. For the Jacobians $J_1(2, M)$, we cannot use the above MAGMA instrinsics. Instead, we decompose $J_1(2, M)$ into lower dimensional abelian varieties and compute their ranks using different methods. The lower bound results for gonality of $X_1(N)$ and $X_1(2, M)$ are compiled from three different resources: for $X_1(N)$ where $N \leq 40$ come from [DVH14], for $X_1(N)$ where $N \geq 41$ come from [Abr96], and for $X_1(2, M)$ come from [JKP06].

Remark 3.2.6. The rank constraints imply that the Jacobian of our modular curve X is torsion, so in theory, one can exhibit generators for $J(X)$. In practice, this decomposition is difficult to achieve for curves of high genus, which introduces a complication in the Mordell-Weil sieve setup. The Mordell-Weil sieve relies on a sufficient understanding of the Jacobian of a curve X; more specifically, one ideally needs to know generators for $J(X)$ or at least a finite index subgroup of $J(X)$.

For the sake of notation, we will discuss the computations for the modular curves $X_1(N)$; the below construction will follow mutatis mutandis for the modular curves $X_1(2, M)$.

Suppose there exist a $\mathbf{Q}$-rational point $P \in \mathrm{Sym}^3 X_1(N)(\mathbf{Q})$. Our proofs consist of constructing a contradiction to the existence of a $\mathbf{Q}$-rational point on $\mathrm{Sym}^3 X_1(N)$ using local and moduli data. The following diagram will serve as a road map for our four-fold Mordell-Weil sieve. At each step of the four-fold Mordell-Weil sieve, we present a technique that constitutes a proof by contradiction.

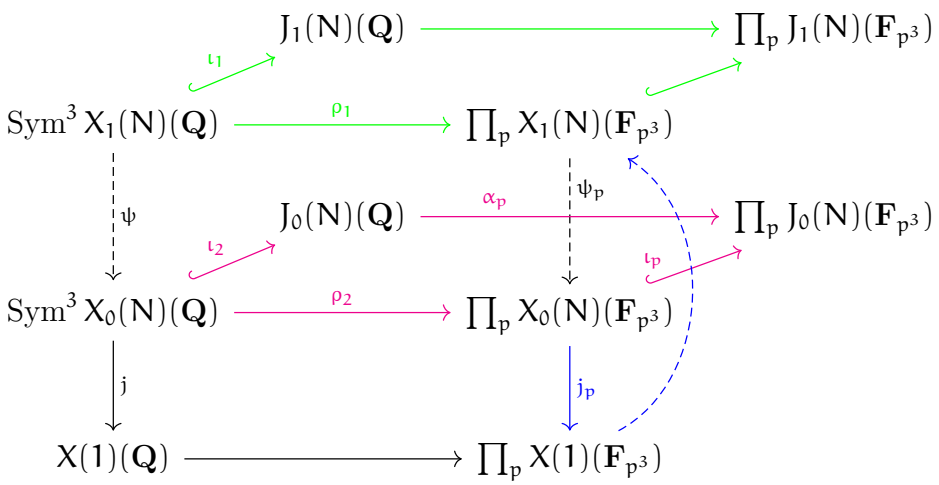


Figure 3.1: Road map for four-fold Mordell-Weil sieving

First sift

The first sifting corresponds to using the Mordell-Weil sieve on the green diagram. We encounter an immediate issue with this approach; local approximations tell us that the torsion on $J_1(N)$ is unwieldy, for example $\#J_1(45)|83608347651268608$. Although this sift is the logical first step, it is also the most computationally inefficient in our case. We only need to apply this sift to one case, and we do successfully Mordell-Weil sieve on $J_1(2,18)$ to prove that $\mathrm{Sym}^3 X_1(2,18)(\mathbf{Q}) = \emptyset$.

Remark 3.2.7. We remark that the approach taken by Maarten Derickx focuses on taming the torsion via improved techniques to compute the torsion of $J_1(N)(\mathbf{Q})$ coming from the differences of cusps.

Second sift

The second level of the sieve utilizes the existence of numerous sub-covers of the modular curves $X_1(N)$. We know that there exist morphisms $X_1(N) \to$

$X_0(N)$ and $X_1(N) \to X_1(p)$ where $p|N$. In some cases, these maps are given by quotients, but in most cases, we do not have equations for this map; hence we denote these maps by dashed arrows. By [Sut12a], we have optimized equations for $X_1(N)$ for $N \leq 100$ and for the j-map $j\colon X_1(N) \to X(1)$. MAGMA's intrinsic `SmallModularCurve(N)` computes the defining equation for the modular curve $X_0(N)$ and the instrinsic `jInvariant(SmallModularCurve(N),N)` produces the j-map from $X_0(N) \to X(1)$. We will use the explicit equations for these sub-covers and their j-maps to construct our second sift.

We can consider the image of the point $\psi(P) \in \mathrm{Sym}^3 X_0(N)$. The lower genus of $X_0(N)$ assists us in the determination of the generators for $J_0(N)$; in Section 3.3.1, we discuss an interesting case of this analysis. The second sift is an application of the Mordell-Weil sieve to the magenta diagram. We may also use the data at numerous primes p of good reduction to construct this contradiction; one must be careful when comparing local data. Furthermore, one may conduct the above procedure for any morphism from $X_1(N)$ to any algebraic group A, where A admits a reduction mod p; this follows from [PSS07, Remark 12.1].

Third trick

The third iteration of the sieve exploits the moduli property of $\mathrm{Sym}^3 X_1(N)(\mathbf{Q})$. First, suppose that we have equations for the map ψ. If the second sift fails, then we have local conditions on $X_0(N)(\mathbf{F}_{p^3})$ that determine when the point $Q \in X_0(N)(\mathbf{F}_{p^3})$ is in the image $\rho_2(\psi(P))$. Using the equation for ψ and reducing mod p, we can compute pre-images of the points $X_0(N)(\mathbf{F}_{p^3})$ in $X_1(N)(\mathbf{F}_{p^3})$, and ideally we find that these pre-images are the reductions of cuspidal points.

Now suppose that we do not know the equations for ψ. Recall that a point $P \in \mathrm{Sym}^3 X_1(N)(\mathbf{Q})$ corresponds to an isomorphism class of elliptic curves defined over some cubic number field with $\mathbf{Z}/N\mathbf{Z}$ torsion subgroup.

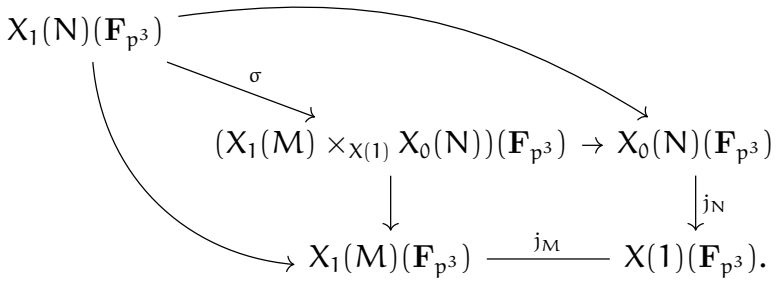
For a prime of good reduction $\mathfrak{p}$, we compute the points on $X_0(N)(\mathbf{F}_{\mathfrak{p}^3})$ satisfying the local datum determined by $\rho_2(\psi(P))$, equivalently by $\psi_{\mathfrak{p}}(\rho_1(P))$, and then take the image of each such point under $j_{\mathfrak{p}}$. Using the moduli property of $\mathrm{Sym}^3 X_1(N)(\mathbf{Q})$, we know that the image of such points under $j_{\mathfrak{p}}$ corresponds to elliptic curves over $\mathbf{F}_{\mathfrak{p}^3}$ with $\mathbf{Z}/N\mathbf{Z}$ torsion. MAGMA's intrinsics can quickly compute whether such elliptic curves over $\mathbf{F}_{\mathfrak{p}^3}$, and their quadratic twists, satisfy our prescribed torsion condition. If we find no such curve or twist, then we have contradicted the existence of the $\mathbf{Q}$-rational point P.

If we do find such an elliptic curve, then we can repeat the above process for a different prime $\mathfrak{p}'$ of good reduction and compare the local data to achieve a contradiction. Succinctly, this trick consists of applying the Mordell-Weil sieve to the magenta diagram, considering the image of the points in $X_0(\mathbf{F}_{\mathfrak{p}^3})$ under the blue arrows, and then use the moduli property of $\mathrm{Sym}^3 X_1(N)$ to construct a contradiction. As above, one may conduct this procedure for any morphism from $X_1(N)$ to any algebraic group A, which admits a reduction mod $\mathfrak{p}$ map.

Fourth sift

The fourth sift encompasses the other three steps, and it involves sieving using j-maps and simultaneously comparing local data at different primes $\mathfrak{p}$ of good reduction. We present a general framework of the fourth sift for the modular curves $X_1(N)$ where $N = 2M$ for some composite integer M and $X_1(M)$, $X_0(N)$ have finitely many $\mathbf{Q}$-rational points. Using the morphisms $X_1(N) \to X_1(M)$, $X_1(N) \to X_0(N)$ and $X_1(N) \to X_0(M)$, we can compute local datum on the points $X_1(R)(\mathbf{F}_{\mathfrak{p}^3})$ and $X_0(N)(\mathbf{F}_{\mathfrak{p}^3})$, and by varying over primes $\mathfrak{p}$ of good reduction, we can refine these constraints. Now consider

the following diagram



The existence of the map σ follows from the universal property of fibered products, but note that we are fibering over a $\mathbf{P}^1$, so a priori, we do not have an explicit description of the set $(X_1(M) \times_{X(1)} X_0(N))(\mathbf{F}_{p^3})$.

The lack of a nice description implies that we can only sieve using the maps j_M, j_N. For a fixed prime p of good reduction, consider the image of the points $X_1(M)(\mathbf{F}_{p^3})$ (resp. $X_0(N)(\mathbf{F}_{p^3})$) that satisfy our local constraints induced by the maps j_M (resp. j_N). If the intersection of these two sets is empty, then we have achieved a contradiction to the existence of a $\mathbf{Q}$-rational point on $\mathrm{Sym}^3 X_1(\mathbf{Q})$. If the intersection is non-empty, then we can check using MAGMA that this j-invariant corresponds to an elliptic curve $E/\mathbf{F}_{p^3}$ with $\mathbf{Z}/N\mathbf{Z}$; if not, then we have reached our desired contradiction. We can repeat the above procedure for different primes p of good reduction and for any morphism $X_1(N) \to X$ where X is a curve with finitely many points that admits a reduction mod p.

Remark 3.2.8. If the second, third, and fourth sift do not prove that $\mathrm{Sym}^3 X_1(N)(\mathbf{Q})$ is all cuspidal, the one should revisit the first sift and proceed with a Mordell-Weil sieve on a finite index subgroup of $J_1(N)$.

3.3 Analysis of $X_1(45)$

In this section, we prove that the symmetric cube $\mathrm{Sym}^3 X_1(45)$ does not have any $\mathbf{Q}$-rational points using the second sift of our four-fold Mordell-Weil sieve. Consider the map $\psi\colon X_1(45) \to X_0(45)$ where $X_0(45)$ is a genus 3 non-hyperelliptic curve defined over $\mathbf{Q}$. For the remainder of this section, let $X := X_0(45)$.

Using similar methods to Remark 3.2.5, we compute that $\mathrm{rk}\, J_0(45) = 0$. Local computations suggest that $J_0(45) \subset \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. However, our computations produce divisors generating a $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ subgroup of $J_0(45)$, so we need different methods to determine the 2-torsion on the Jacobian of our genus 3 non-hyperelliptic curve X.

3.3.1 Theta divisors, bitangents, and 2-torsion on Jacobians

Let $\overline{\mathbf{Q}}/\mathbf{Q}$ be an algebraic closure of $\mathbf{Q}$ and let $\overline{X} := X \times_{\mathbf{Q}} \overline{\mathbf{Q}}$ be the base change of X to $\overline{\mathbf{Q}}$. We have a correspondence between divisors $D \in \mathrm{Div}\,\overline{X}$ and line bundles $\mathcal{F}$ via their global sections. In particular for each divisor D, we can find a line bundle $\mathcal{F}$ such that $H^0(\overline{X}, \mathcal{F}) \cong \mathcal{O}_{\overline{X}}(D)$. Recall that the Picard group of $\overline{X}$, denoted by $\mathrm{Pic}\,\overline{X}$, is the group of isomorphism classes of line bundles on the scheme $\overline{X}$ with operation given by tensor products and that the Jacobian of $\overline{X}$ is the subgroup of $\mathrm{Pic}\,\overline{X}$ of degree 0 line bundles.

Definition 3.3.2. Let $D \in \mathrm{Pic}\,\overline{X}$. If $2D \backsim K$, where K is the canonical divisor of of $\overline{X}$, then D is a theta divisor. We say that D is even or odd according to parity of $h^0(\mathcal{O}_{\overline{X}}(D))$.

Let $\mathrm{TD}(\overline{X})$ denote the set of theta divisors of $\overline{X}$. Then $\mathrm{TD}(\overline{X})$ forms a torsor under $J_{\overline{X}}[2]$. Fix a $D \in \mathrm{TD}(\overline{X})$. We define the action of $J_{\overline{X}}[2]$ for

$D' \in J(\overline{X})[2]$ by setting

$$(\mathcal{O}(D) \otimes \mathcal{O}(D')^{-1})^{\otimes 2} \cong \mathcal{O}_{\overline{X}} \otimes \omega_{\overline{X}} \cong \omega_{\overline{X}}.$$

Recall that X is a non-hyperelliptic smooth projective, geometrically irreducible curve of genus 3. It is a well-known fact that canonical image of X is a smooth plane quartic; this fact may be deduce from basic principles or from Petri's theorem [Pet23]. We define a bitangent of $\overline{X}$ to be a line such that $(L \cdot \overline{X}) = 2[P] + 2[Q]$ for some $P, Q \in \operatorname{Div} \overline{X}$. We now sketch the relationship between bitangents on a genus 3 non-hyperelliptic curve and odd theta divisors on X.

Let $\operatorname{Bit}(\overline{X})$ denote the set of bitangents of $\overline{X}$. Notice that if L is a bitangent of $\overline{X}$, then

$$\frac{1}{2}(L \cdot \overline{X}) = [P] + [Q]$$

is an odd theta divisor. Furthermore, there exists a bijection between bitangents $\psi\colon \operatorname{Bit}(\overline{X}) \to \Theta\mathrm{D}_{\mathrm{odd}}(\overline{X})$ defined by sending $L \mapsto 1/2(L \cdot \overline{X})$. The map ψ is injective since the linear equivalence $[P] + [Q] \backsim [R] + [S]$ implies that $[P] + [Q] = [R] + [S]$; this follows from $\overline{X}$ not being hyperelliptic and the linear equivalence witnessing this gonality. To show surjectivity, suppose that $D \in \Theta\mathrm{D}_{\mathrm{odd}}(\overline{X})$. The assumptions imply that $2D = K$ and $D = [P] + [Q]$, and thus the line joining P and Q is a bitangent. Therefore, we have established the following bijections for nice genus 3 non-hyperelliptic curves $\overline{X}$:

$$\operatorname{Bit}(\overline{X}) \longleftrightarrow \Theta\mathrm{D}_{\mathrm{odd}}(\overline{X}).$$

For a fixed bitangent D, we see that the difference $D - D'$ generates $J_{\overline{X}}[2]$ for some $D' \in \operatorname{Bit}(\overline{X})$; succinctly, we have that the difference between the bitangents of $\overline{X}$ will generate the 2-torsion on the Jacobian of $\overline{X}$.

Returning to our original problem, we want to show that the 2-torsion

of $J(X)$ has rank 2, which would imply that $J(X) \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. By the above discussion, we need to compute the bitangents of the curve $\overline{X}$ and the action of $G_{\mathbf{Q}}$ on these lines. We accomplish this by computing the number field over which the bitangents are defined. Roughly speaking, this reduces to computing a Gröbner basis for a system of equations, so we omit the full details of this computations.[1] We find that these bitangents of $\overline{X}$ are defined over a quartic number field with Galois group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

We find a transitive subgroup H of $\mathrm{GSp}_6(\mathbf{F}_2)$ such that $H \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and hence the action of $G_{\mathbf{Q}}$ on the bitangents is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Moreover, the 2-rank of $J(X)$ is 2, and hence we have proved that $J(X) \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. Since we have explicitly determined the torsion on $J_0(45)$, we can use our four-fold Morell-Weil sieve. At the second sift, we derive a contradiction at $p = 7$ to our assumption on the existence of a $\mathbf{Q}$-rational point $\mathrm{Sym}^3 X_1(45)$, and therefore we have proved that $\mathrm{Sym}^3 X_1(45)(\mathbf{Q})$ is cuspidal.

N.B. We conclude by remarking that the above analysis demonstrates a failure of the local-global principle on the torsion of the Jacobian of X.

[1] MAGMA code for these computations is available upon request.

Chapter 4

Selmer groups of twists of elliptic curves over K with K-rational torsion points

4.1 Definitions and Notation

Let ℓ be an odd, rational prime and let E/K be an elliptic curve defined over a number field K. The K-rational points $\mathsf{E}(\mathsf{K})$ form a finitely generated group by the Mordell-Weil theorem. Recall from [Sil09, Section X.4] that we have the following exact sequence

$$0 \to \mathsf{E}(\mathsf{K})/\ell\mathsf{E}(\mathsf{K}) \to \mathrm{Sel}_\ell(\mathsf{E},\mathsf{K}) \to Ш(\mathsf{E},\mathsf{K})[\ell] \to 0,$$

where $\mathrm{Sel}_\ell(\mathsf{E},\mathsf{K})$ denotes the ℓ-Selmer group and $Ш(\mathsf{E},\mathsf{K})[\ell]$ is ℓ-Shafarevich-Tate group. If $\mathsf{K} = \mathbf{Q}$, then Frey [Fre88] provides explicit examples of quadratic twist of elliptic curves over $\mathbf{Q}$ with $\mathbf{Q}$-rational points of odd, prime order ℓ whose ℓ-Selmer groups are non-trivial; a theorem of Mazur [Maz77] implies that $\ell \in \{3, 5, 7\}$.

Theorem 4.1.1 ([Fre88]). *Suppose that* $E/\mathbf{Q}$ *is an elliptic curve with a* $\mathbf{Q}$*-rational torsion point* P *of odd prime order* ℓ*, and suppose that* P *is not contained in the kernel of reduction modulo* ℓ*; in particular, this means that* E *is not supersingular modulo* ℓ *if* $\mathrm{ord}_\ell(j_E) \geq 0$*. Let* $\widetilde{S}_E$ *be the subsets of primes dividing the conductor* $N(E)$ *of* E *defined by*

$$\widetilde{S}_E := \{p | N(E) : 2 < p \equiv -1 \pmod{\ell},\ \ell \nmid \mathrm{ord}_p(\Delta_E)\},$$

where j_E *is the* j*-invariant of* E *and* Δ_E *is the discriminant of* E*. Suppose that* $\widetilde{S}_E = \emptyset$*. Then, whenever* $d \equiv 3 \pmod 4$ *is a negative, square-free integer coprime to* $\ell N(E)$ *satisfying:*

1. *if* $\mathrm{ord}_\ell(j_E) < 0$*, then* $\left(\frac{d}{\ell}\right) = -1$*;*
2. *if* $p | N(E)$ *is an odd prime, then*

$$\left(\frac{d}{p}\right) = \begin{cases} -1 & \text{if } \mathrm{ord}_p(j_E) \geq 0; \\ -1 & \text{if } \mathrm{ord}_p(j_E) < 0 \text{ and } E/\mathbf{Q}_p \text{ is a Tate curve}; \\ 1 & \text{otherwise}; \end{cases}$$

we have that $\mathrm{Sel}_\ell(E^d, \mathbf{Q})$ *is non-trivial if and only if the* ℓ*-part of the class group of* $\mathbf{Q}(\sqrt{d})$ *is non-trivial.*

Remark 4.1.2. Frey actually proved a more general, double divisibility statement concerning the ℓ-Selmer group of E^d and the order of Galois groups of particular number fields unramified outside of $\widetilde{S}_E$, when $\widetilde{S}_E \neq \emptyset$; we generalize [Fre88, Theorem] in Theorem 4.2.2 and [Fre88, Corollary] in Corollary 4.2.6.

Frey's idea was to obtain information about $\mathrm{Sel}_\ell(E^d, \mathbf{Q})$ when $E(\mathbf{Q})$ contains an element of order ℓ. In particular, he studied the behavior of E over local fields $\mathbf{Q}_\ell$ and their algebraic closures $\overline{\mathbf{Q}}_\ell$. In this paper, we investigate the ℓ-Selmer rank in families of quadratic twist of elliptic curves E/K with

K-rational points of odd prime order ℓ. We use Frey's proof as a blueprint for our own, but the techniques we utilize come from class field theory. That being said, many of his arguments go through undisturbed.

The problem of constructing elements in the Selmer group is a classical question with many avenues of approach. Frey's condition that the elliptic curve E/K have a K-rational point of odd prime power order $\ell > 3$ has two immediate consequences. First, the image of Galois under the mod ℓ representation is conjugate to

$$\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbf{F}_\ell),$$

which will assist in our explicitly description the Galois structure of splitting fields of ℓ-covers of E/K and the splitting fields of elements in $\mathrm{Sel}_\ell(E^d, K)$. The second is that we can immediately identify a quotient of $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})[\ell])$, namely $H^1(\mathrm{Gal}(\overline{K}/K), \zeta_\ell)$. Frey's (and our) proof relies on an analysis of cocyles in $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K})[\ell])$ and this fact will allow us to deduce local triviality in certain cases using Hilbert's Theorem 90. A laborious aspect of our proofs is the case by case analysis of how primes $\mathfrak{p}$ dividing $N(E)$ behave in the field $K(\sqrt{d}) \cdot K(E[\ell])$ where $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ yields the quadratic twist E^d of E and $K(E[\ell])$ is the ℓ-division field of E/K.

Notation

We set the following notation.

$$
\begin{aligned}
K &:= \text{Galois number field,}\\
\ell &:= \text{odd, rational prime in } S(\mathfrak{n}) \setminus \{2,3\} \text{ such that } \ell \nmid \mathrm{cl}(K) \text{ and } \zeta_\ell \notin K,\\
L/K &:= \text{algebraic extension of } K,\\
\mathfrak{p} &:= \text{prime divisor of the rational prime } \mathfrak{p} \text{ in } \mathcal{O}_K,\\
\mathfrak{P} &:= \text{prime divisor of } \mathfrak{p} \text{ in } \mathcal{O}_L,\\
K_\mathfrak{p} &:= \text{completion of } K \text{ with respect to } \mathfrak{p},\\
L_\mathfrak{P} &:= \text{completion of } L \text{ with respect to } \mathfrak{P},\\
S &:= \text{finite set of primes of } \mathcal{O}_K,\\
M/L &:= \text{Galois extension with abelian Galois group of exponent } \ell.
\end{aligned}
$$

More generally, lower case gothic font will denote a divisor of a rational prime of $\mathbf{Q}$, and similarly, upper case gothic font will denote a divisor of a prime of K.

Definition 4.1.3. M/L is said to be little ramified outside S if for primes $\mathfrak{p} \notin S$ and all $\mathfrak{P}_L|\mathfrak{p}$ one has

$$M \cdot L_\mathfrak{P}(\zeta_\ell) = L_\mathfrak{P}(\zeta_\ell)(\sqrt[\ell]{u_1}, \ldots, \sqrt[\ell]{u_k})$$

with $k \in \mathbf{N}$ and $\mathrm{ord}_{\mathfrak{P}_L}(u_i) = 0$. Here ζ_ℓ is a ℓ^{th} root of unity, $u_1, \ldots, u_k$ are elements in $L_\mathfrak{P}(\zeta_\ell)$, and $\mathrm{ord}_{\mathfrak{P}_L}$ is the normed valuation belonging to $\mathfrak{P}_L$.

If M/L little ramified outside S, then M/L is unramified at all divisors of primes $\mathfrak{p} \notin S \cup \{\ell\}$.

Notation

We set the following notation, which comes directly from [Fre88]:

$$\begin{aligned}
L_S &:= \text{maximal abelian extension of exponent } \ell \text{ of } L \text{ which is} \\
&\quad \text{little ramified outside } S, \\
L_{S,u} &:= \text{maximal subfield of } L_S \text{ which is unramified outside of } S, \\
H_S(L) &:= \text{Galois group of } L_S/L, \\
H_{S,u}(L) &:= \text{Galois group of } L_{S,u}/L, \\
\mathrm{cl}_S(L)\,[\ell] &:= \text{order of } H_S(L), \\
\mathrm{cl}_{S,u}(L)\,[\ell] &:= \text{order of } H_{S,u}(L).
\end{aligned}$$

Remark 4.1.4. If $S = \emptyset$, we see that $\mathrm{cl}_{\emptyset,u}(L)$ is equal to the order of the subgroup of the divisor class group of L consisting of elements of order ℓ which we denote by $\mathrm{cl}(L)[\ell]$.

Now assume that L/K is normal with cyclic Galois group generated by an element γ of order $\ell - 1$. Take an extension $\widetilde{\gamma}$ to $L(\zeta_\ell)$. Let χ_ℓ be the cyclotomic character induced by the action of $\mathrm{Gal}(L(\zeta_\ell)/K)$ on $\langle \zeta_\ell \rangle$. Then $\chi_\ell(\widetilde{\gamma})$ is determined by

$$\widetilde{\gamma}(\zeta_\ell) = \zeta_\ell^{\chi_\ell(\widetilde{\gamma})}.$$

Let M be normal over K containing L such that $\mathrm{Gal}(M/L)$ is abelian of exponent ℓ. Then $\widetilde{\gamma}$ operates by conjugation on

$$\mathrm{Gal}(M(\zeta_\ell)/L(\zeta_\ell)) \cong \mathrm{Gal}(M/L),$$

and this operation does not depend on choice of $\widetilde{\gamma}$. Hence the subgroup

$$H(\chi_\ell) := \left\{ \alpha \in \mathrm{Gal}(M/L) : \widetilde{\gamma}\alpha\widetilde{\gamma}^{-1} = \alpha^{\chi_\ell(\widetilde{\gamma})} \right\} \subseteq \mathrm{Gal}(M/L)$$

is well-defined. In the special case that $M = L_S$, we denote the order of $H_S(L)(\chi_\ell)$ by $\mathrm{cl}_S(L)_\ell(\chi_\ell)$.

Now we shall consider an elliptic curve E/K given by a Weierstrass equation $F(x, y) = 0$ with coefficients in $\mathcal{O}_K$ and minimal discriminant Δ_E. For any extension L/K, we denote the L-rational points of E (including ∞) by $E(L)$. Let χ_H be a primitive Hecke character of order ℓ and let

$$\widetilde{S}_E := \{\mathfrak{p} | N(E) : \chi_H(\mathfrak{p}) \neq 0, \mathrm{ord}_\mathfrak{p}(\Delta_E) \not\equiv 0 \pmod{\ell}\}$$
$$S_E := \{\mathfrak{p} \in \widetilde{S}_E : \mathrm{ord}_\mathfrak{p}(j_E) < 0\}.$$

Let $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ and denote the twist of E/K by E^d/K. Via the general theory of twists [Sil09, Section X.2], we know that E^d is isomorphic to E over $K(\sqrt{d})$ but not over K. Let $G_K := \mathrm{Gal}(\overline{K}, K)$ denote the absolute Galois group. Let $\mathfrak{W}(E^d, K)[\ell]$ be the set of elements of order ℓ in the kernel of

$$\rho\colon H^1(G_K, E^d(\overline{K})) \longrightarrow \bigoplus_{\mathfrak{p} \text{ prime}} H^1(\mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p}), E^d(\overline{K_\mathfrak{p}})).$$

The group of elements of order ℓ in the Selmer group of E^d, denoted by $\mathrm{Sel}_\ell(E^d, K)$ is given as the pre-image of $\mathfrak{W}(E^d, K)[\ell]$ by the map

$$\alpha\colon H^1(G_K, E^d(\overline{K})[\ell]) \longrightarrow H^1(G_K, E^d(\overline{K})).$$

There are two main cases we need to consider:

Case 1:

Assume that $\mathrm{ord}_\mathfrak{p}(j_E) \geq 0$. Then there is a finite extension N/K such that E has good reduction modulo all $\mathfrak{P}_N|\mathfrak{p}$ i.e., we find an elliptic curve $\widetilde{E}$ such that $\tilde{E}$ modulo $\mathfrak{P}_N$ is an elliptic curve over the residue field of $\mathfrak{P}_N$. $\widetilde{E}(\overline{N_\mathfrak{P}})$ contains a subgroup $\widetilde{E}_-(N_\mathfrak{P})$ consisting of points $(\widetilde{x}, \widetilde{y})$ with $\mathrm{ord}_{\mathfrak{P}_N}(\widetilde{x}) < 0$.

$\widetilde{E}_-$ is the kernel of reduction modulo $\mathfrak{P}_N$, and $\mathrm{ord}_{\mathfrak{P}_N}(\widetilde{x}/\widetilde{y})$ is the level of $(\widetilde{x},\widetilde{y})$. For ease of notation, we say that a point $(x,y) \in E(\overline{N_{\mathfrak{P}}})$ is in the kernel of the reduction modulo $\mathfrak{P}_N$ if its image $(\widetilde{x},\widetilde{y}) \in \widetilde{E}_-(\overline{N_{\mathfrak{P}}})$.

Case 2:

Assume that $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$. Then after an extension $L/K_{\mathfrak{p}}$ of degree ≤ 2, E becomes a Tate curve (via a theorem of Tate [Sil09, Theorem C.14.1]); in particular, one has a Tate parametrization

$$\tau\colon \overline{L}^{\times}/\langle q\rangle \longrightarrow E(\overline{L})$$

where q is the $\mathfrak{p}$-adic period of E. One also has that

$$j_E = \frac{1}{q} + \sum_{i=0}^{\infty} a_i q^i \quad \text{with } a_i \in \mathbf{Z}$$

and the points of order ℓ in $E(\overline{L})$ are of the form $\tau(\zeta_\ell^{\alpha}(q^{\beta/\ell}))$ where $\alpha,\beta \in \{1,\dots,\ell-1\}$.

Definition 4.1.5. If F/K is a number field and $\mathfrak{P}_F|\mathfrak{p}$ we say that a point $(x,y) \in E(F_{\mathfrak{P}})$ is in the connected component of the unity modulo $\mathfrak{P}_F$ if it is of the form $\tau(u)$ with u a $\mathfrak{P}_F$-adic unit, and (x,y) is in the kernel of the reduction modulo $\mathfrak{P}_F$ if $u-1 \in \mathfrak{P}_F$.

Remark 4.1.6. One should notice that if E is not a Tate curve over $K_{\mathfrak{p}}$ but over an extension of degree 2 of $K_{\mathfrak{p}}$, then for all points $P \in E(K_{\mathfrak{p}})$, $2P$ is in the connected component of unity modulo $\mathfrak{p}$.

4.2 Statement of Results

As mentioned above, [Fre88, Theorem] gives a double divsibility statement involving the ℓ-torsion of the Selmer group. First, we generalize his single divisibility to elliptic curves E/K defined over number fields K of finite degree with K-rational points of odd, prime order ℓ. Recall that $S(n)$ is the set of primes that can arise as the order of a rational point on an elliptic curve defined over a number field of degree n.

Theorem 4.2.1. *Let K be a Galois number field and choose $\ell \in S(n) \setminus \{2,3\}$ such that $\ell \nmid \mathrm{cl}(K)$ and $\zeta_\ell \notin K$. Let E/K be an elliptic curve over K with a K-rational point P of order ℓ; let χ_H denote a primitive Hecke character of K with order ℓ; let $\mathfrak{q}$ denote a prime of $\mathcal{O}_K$ that lies above 2; and let $\mathfrak{l}$ denote a prime of $\mathcal{O}_K$ that lies above ℓ. Suppose that P is not contained in the kernel of reduction modulo $\mathfrak{l}$; in particular, this means that E is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$. Let S_E be the set of primes*

$$S_E := \{\mathfrak{p} | N(E) : \mathrm{ord}_{\mathfrak{p}}(\Delta_E) \not\equiv 0 \pmod{\ell}, \chi_H(\mathfrak{p}) \neq 0, \text{ and } \mathrm{ord}_{\mathfrak{p}}(j_E) < 0\}.$$

Suppose that $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ is negative[1], coprime to $\mathfrak{l} \cdot N(E)$, and satisfies the following divisibility and Artin symbol conditions where $\langle \delta \rangle = \mathrm{Gal}(K(\sqrt{d})/K)$:

1. *if $\mathfrak{q} | N(E)$, then $\mathfrak{q} | \Delta_{K(\sqrt{d})/K}$;*
2. *if $\mathrm{ord}_{\mathfrak{l}}(j_E) < 0$, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{l}}\right) = \delta$;*
3. *if $\mathfrak{p} | N(E)$ is a prime of K with $\mathfrak{p} \notin S_E$, then*
   - *if $\mathrm{ord}_{\mathfrak{p}}(j_E) \geq 0$, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;*
   - *if $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$ and $E/K_{\mathfrak{p}}$ is a Tate curve, then $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;*

[1] We say that $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ is negative if the image of d under each real embedding is negative

- *otherwise,* $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \mathrm{id}$.

Then we have that the order of the ℓ*-torsion of the* S_E*-ray class group of* $K(\sqrt{d})$ *divides the order of* $\mathrm{Sel}_\ell(E^d, K)$*. More precisely, the single divisibility statement holds:*

$$\mathrm{cl}_{S_E,u}(K(\sqrt{d}))[\ell] \Big| \#\,\mathrm{Sel}_\ell(E^d, K). \tag{4.2.1}$$

We also prove a stronger, more explicit version of Theorem 4.2.1 in the form of a double divisibility statement, which completely generalizes [Fre88, Theorem].

Theorem 4.2.2. *Let* K *be a Galois number field of degree* $n \leq 5$ *such that* $N_{K/\mathbf{Q}}(\mathfrak{q}) = 2$ *for all* $\mathfrak{q}|2$*. Choose* $\ell \in S(n) \setminus \{2,3\}$ *such that* $\ell \nmid \mathrm{cl}(K)$ *and* $\zeta_\ell \notin K$*. Let* E/K *be an elliptic curve over* K *with a* K*-rational point* P *of order* ℓ*; let* χ_H *denote a primitive Hecke character of* K *with order* ℓ*; let* $\mathfrak{q}$ *denote a prime ideal of* $\mathcal{O}_K$ *that lies above 2; and let* $\mathfrak{l}$ *denote a prime ideal of* $\mathcal{O}_K$ *that lies above* ℓ*. If* $[K : \mathbf{Q}] = 5$ *and* $\ell = 5$*, then we must make the added assumption that* $(\ell)\mathcal{O}_K$ *is not totally ramified. Suppose that* P *is not contained in the kernel of reduction modulo* $\mathfrak{l}$*; in particular, this means that* E *is not supersingular modulo* $\mathfrak{l}$ *if* $\mathrm{ord}_\mathfrak{l}(j_E) \geq 0$*. Let* $\widetilde{S}_E$ *and* S_E *be the sets of primes*

$$\begin{aligned}\widetilde{S}_E &:= \{\mathfrak{p}|N(E) : \chi_H(\mathfrak{p}) \neq 0,\, \mathrm{ord}_\mathfrak{p}(\Delta_E) \not\equiv 0 \pmod{\ell}\},\\ S_E &:= \{\mathfrak{p} \in \widetilde{S}_E : \mathrm{ord}_\mathfrak{p}(j_E) < 0\}.\end{aligned}$$

Suppose that $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ *is negative, coprime to* $\mathfrak{l}\cdot N(E)$*, and satisfies the following divisibility and Artin symbol conditions where* $\langle\delta\rangle = \mathrm{Gal}(K(\sqrt{d})/K)$*:*

1. *if* $\mathfrak{q}|N(E)$*, then* $\mathfrak{q}|\Delta_{K(\sqrt{d})/K}$*;*
2. *if* $\mathrm{ord}_\mathfrak{l}(j_E) < 0$*, then* $\left(\frac{K(\sqrt{d})/K}{\mathfrak{l}}\right) = \delta$*;*
3. *if* $\mathfrak{p}|N(E)$ *is a prime of* K *with* $\mathfrak{p} \notin S_E$*, then*

- *if* $\mathrm{ord}_{\mathfrak{p}}(j_E) \geq 0$, *then* $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;
- *if* $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$ *and* $E/K_{\mathfrak{p}}$ *is a Tate curve, then* $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$;
- *otherwise,* $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \mathrm{id}$.

Then we have the following double divisibility

$$\mathrm{cl}_{S_E,u}(K(\sqrt{d}))[\ell] \Big| \#\,\mathrm{Sel}_\ell(E^d, K) \Big| \mathrm{cl}_{\widetilde{S}_E,u}(K(\sqrt{d}))[\ell] \cdot \mathrm{cl}_{S_E}(K')[\ell](\chi_\ell), \qquad (4.2.2)$$

where K' *is the subfield of* $K(\sqrt{d}, \zeta_\ell)$ *of index 2 containing neither* ζ_ℓ *nor* $\sqrt{d}$.

Remark 4.2.3. In words, (4.2.2) states that the order of the ℓ-torsion of the S_E-ray class group of $K(\sqrt{d})$ divides the order of $\mathrm{Sel}_\ell(E^d, K)$, and the order of $\mathrm{Sel}_\ell(E^d, K)$ divides the order of the ℓ-torsion of the $\widetilde{S}_E$-ray class group of $K(\sqrt{d})$ times the degree of the maximal abelian extension K'' of K' of exponent ℓ unramified outside of $S_E \cup \{\mathfrak{l}\}$ such that the Galois group $\mathrm{Gal}(K'/K)$ acts on $\mathrm{Gal}(K''/K)$ by $\chi_\ell \varepsilon_d$, where ε_d is the character prescribing the Galois action on $\sqrt{d}$.

Once we have proved Theorems 4.2.1, 4.2.2, we can immediately extend the divisibility statements (4.2.1), (4.2.2) to elliptic curves E defined over $\mathbf{Q}$ by considering the values of $S_{\mathbf{Q}}(n)$.

Corollary 4.2.4. *C Let* $E/\mathbf{Q}$ *be an elliptic curve defined over* $\mathbf{Q}$. *For some Galois number field* K, *suppose that* E_K *attains a* K*-rational point* P *of order* ℓ *where* $\ell \in S_{\mathbf{Q}}(n) \setminus \{2, 3\}$ *such that* $\ell \nmid \mathrm{cl}(K)$ *and* $\zeta_\ell \notin K$. *In keeping with the notation and assumptions of Theorem 4.2.1, we can produce examples of quadratic twists* E_K^d *that satisfy the divisibility statement* (4.2.1).

Corollary 4.2.5. *D Let* $E/\mathbf{Q}$ *be an elliptic curve defined over* $\mathbf{Q}$; *let* E_K *denote the base change of this curve to a Galois number field of degree* $n \leq 20$ *such that* $N_{K/\mathbf{Q}}(\mathfrak{q}) = 2$ *for all* $\mathfrak{q}|2$. *Choose* $\ell \in S_{\mathbf{Q}}(n) \setminus \{2, 3\}$ *such that* $\ell \nmid$

$\mathrm{cl}(K)$, $\zeta_\ell \notin K$, *and the ramification index* $e_\mathfrak{l}(K/\mathbf{Q})$ *satisfies* $1 > e_\mathfrak{l}(K/\mathbf{Q})/(\ell - 1) - 1$. *Suppose that* E_K *attains a* K*-rational point* P *of order* ℓ, *then in keeping with the notation and assumptions of Theorem 4.2.2, we can produce examples of quadratic twists* E_K^d *that satisfy the double divisibility statement* (4.2.2).

We can also generalize [Fre88, Corollary], which we stated as Theorem 4.1.1.

Corollary 4.2.6. *E Let* (E, ℓ, K, d) *be as in Theorem 4.2.2 or in Corollary 4.2.5. If* $\widetilde{S}_E = \emptyset$, *then* $\mathrm{Sel}_\ell(E^d, K)$ *is non-trivial if and only if the* ℓ*-torsion of the class group of* $K(\sqrt{d})$ *is non-trivial, in particular*

$$\mathrm{cl}(K(\sqrt{d}))[\ell] \Big| \#\,\mathrm{Sel}_\ell(E^d, K) \Big| (\mathrm{cl}(K(\sqrt{d}))[\ell])^2.$$

Remark 4.2.7. In his Ph.D. thesis [Mai03], Mailhot was able to recover and sharpen [Fre88, Theorem] for elliptic curves defined over $\mathbf{Q}$ using purely cohomological methods. His refinement comes from prescribing a splitting behavior of primes above K' instead of just a non-ramified condition. We remark that our methods and results are disjoint, however, we believe that [Mai03, Corollary 2.17] can be generalized to elliptic curves defined over number fields K, using Theorem 4.2.2.

4.3 Proof of Theorem 4.2.1

In this section, we prove the divisibility statement (4.2.1). Before we proceed, we make a remark about some of the prime assumptions of Theorem 4.2.1.

Remark 4.3.1 (Prime assumptions). If $\mathrm{ord}_\mathfrak{p}(j_E) < 0$, then we have that $E/K_\mathfrak{p}$ has a Tate parametrization. The second condition $\mathrm{ord}_\mathfrak{p}(\Delta_E) \not\equiv 0 \pmod{\ell}$ assists us in Lemma 4.3.2. In short, it allows us to understand ramification

in the ℓ-division field of $E_{K_\mathfrak{p}}$. The final condition $\chi_H(\mathfrak{p}) \neq 0$ is used in Lemma 4.3.3 and is an analogue of Frey's condition that $\mathfrak{p} \equiv -1 \pmod{\ell}$. Moreover, this condition allows us to deduce, using Remark 2.3.4, that for a cyclic extension M_2/K of degree ℓ, $\mathfrak{p}$ is unramified in M_2.

The first step in the proof is to exhibit an element in $\mathrm{Sel}_\ell(E^d, K)$.

Lemma 4.3.2. *Let $\ell > 3$ be a rational prime; let M/K be a non-abelian Galois extension of degree 2ℓ containing $K(\sqrt{d})$ that is unramified over this field outside of S_E; let α be a generator of $\mathrm{Gal}(M/K(\sqrt{d}))$; and let ϕ the element in $H^1(\mathrm{Gal}(M/K), E^d(M)[\ell])$ determined by $\phi(\alpha) = P$, where P is a K-rational point of order ℓ. Then ϕ is an element of $\mathrm{Sel}_\ell(E^d, K)$.*

Proof. First, we need to show that there exists some element

$$\phi \in H^1(\mathrm{Gal}(M/K), E^d(M)[\ell])$$

whose restriction $\overline{\phi}$ to $\mathrm{Gal}(M/K(\sqrt{d})) = \langle\alpha\rangle$ is given by $\overline{\phi}(\alpha) = P$. We identify $E^d(M)[\ell]$ with $E(M)[\ell] = \langle P\rangle$. Since $E^d(K(\sqrt{d}))[\ell] = \langle P\rangle$ and $\delta(P) = -P$ where $\langle\delta\rangle = \mathrm{Gal}(K(\sqrt{d})/K)$, we have invariance of ϕ under δ from the fact that $\delta\alpha\delta = \alpha^{-1}$. Since

$$H^1(\mathrm{Gal}(M/K), E^d(M)[\ell]) = H^1(\mathrm{Gal}(M/K(\sqrt{d})), E^d(M)[\ell])^\delta,$$

our assertions follows.

Hence it remains to show that $\overline{\phi}$ is locally trivial when regarded as an element of

$$H^1(\mathrm{Gal}(M/K(\sqrt{d})), E^d(M)).$$

We may restrict ourselves to primes $\mathfrak{P}_M | \mathfrak{l}\cdot N(E)$. By condition (1) of Theorem 4.2.1, the divisors of $\mathfrak{q}$ are unramified in $M/K(\sqrt{d})$ if $\mathfrak{q}|N(E)$, and hence we may assume that $\mathfrak{P}_M \nmid \mathfrak{q}$.

Assume that $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \delta$. In this case, $\mathfrak{P}_M$ is either fully ramified or decomposed (since M/K is non-abelian). So assume that $\mathfrak{P}_M$ is fully ramified and divides $\mathfrak{p}$. Then $\mathfrak{p} \in S_E$ and in particular $\mathfrak{p} \neq \mathfrak{l}$ and $\mathrm{ord}_{\mathfrak{p}}(\Delta_{E_K}) \neq 0 \pmod{\ell}$. We claim that $E^d/K_{\mathfrak{p}}(\sqrt{d})$ is a Tate curve and that P is contained in the connected component of the unity over $K_{\mathfrak{p}}(\sqrt{d})$ corresponding to an ℓ^{th} root of unity ζ_ℓ.

The fact that $E^d/K_{\mathfrak{p}}(\sqrt{d})$ is a Tate curve follows since $\mathfrak{p} \in S_E$ and so $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$. Since $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) \neq 0 \pmod{\ell}$, we know that adjoining $q^{1/\ell}$ to $K_{\mathfrak{p}}(\sqrt{d})$, where q is the $\mathfrak{p}$-adic period of E, is a non-trivial extension. Under the Tate parametrization τ, we have that torsion points of order ℓ in $E^d(\overline{K_{\mathfrak{p}}(\sqrt{d})})[\ell]$ are of the form $\tau(\zeta_\ell^\alpha q^{\beta/\ell})$ where $\alpha, \beta \in \{1, \ldots, \ell-1\}$. Since P is a point of order ℓ defined over $K_{\mathfrak{p}}(\sqrt{d})$, we know that $\zeta_\ell^\alpha \in K_{\mathfrak{p}}(\sqrt{d})$ for some $\alpha \in \{1, \ldots, \ell-1\}$ and that

$$\tau^{-1}(P) = \zeta_\ell^\alpha q^{\beta/\ell} \in K_{\mathfrak{p}}(\sqrt{d}).$$

In order for $\zeta_\ell^\alpha q^{\beta/\ell} \in K_{\mathfrak{p}}(\sqrt{d})$, we must have that $\beta = 0$ since q is not an $1/\ell^{\text{th}}$ power. Thus, $\tau^{-1}(P) = \zeta_\ell^\alpha$, and hence P is contained in the connected component of the unity over $K_{\mathfrak{p}}(\sqrt{d})$ corresponding to an ℓ^{th} root of unity ζ_ℓ. Since $M_{\mathfrak{P}}/K_{\mathfrak{p}}(\sqrt{d})$ is cyclic of degree ℓ, we have that $\zeta_\ell = \alpha x/x$ for some $x \in M_{\mathfrak{P}}$ by Hilbert' Theorem 90, and therefore, $\overline{\phi}$ is trivial when considered in $H^1(\mathrm{Gal}(M_{\mathfrak{P}}/K_{\mathfrak{p}}), E^d(M_{\mathfrak{P}}))$.

Next assume that $\left(\frac{K(\sqrt{d})/K}{\mathfrak{p}}\right) = \mathrm{id}$ and $\mathfrak{p} \neq \mathfrak{l}$. Then $\mathrm{ord}_{\mathfrak{p}}(j_E) < 0$ and E is a Tate curve over $K_{\mathfrak{p}}$, and so again P corresponds to some ℓ^{th} root of unity ζ_ℓ under the Tate parametrization of $E = E^d$ over $K_{\mathfrak{p}}(\zeta_\ell)$ and hence $\overline{\phi}$ is split by $K_{\mathfrak{p}}(\zeta_\ell)$ as seen above. But since the degree of $K_{\mathfrak{p}}(\zeta_\ell)$ over $K_{\mathfrak{p}}$ is prime to ℓ, $\overline{\phi}$ is split over $K_{\mathfrak{p}}$ already, and thus $\overline{\phi}$ is locally trivial.

There is one remaining case: $\mathfrak{p} = \mathfrak{l}$ and $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$. Let $\mathfrak{L}_M | \mathfrak{l}$. By the assumption, M/K is unramified at $\mathfrak{L}_M$, and we can find a normal extension

N/K of degree prime to ℓ such that E has good reduction modulo all primes $\mathfrak{L}_N|\mathfrak{l}$. In particular, we may take $N = K(\zeta_{12}, \sqrt[12]{\mathfrak{l}})$. Now

$$H^1(\mathrm{Gal}(M_{\mathfrak{L}} \cdot N/K_{\mathfrak{l}} \cdot N), E^d(M_{\mathfrak{L}} \cdot N)) = 0$$

since the reduction of E^d modulo $\mathfrak{L}$ is good and $M_{\mathfrak{L}}N/K_{\mathfrak{l}}N$ is unramified, and hence it follows that

$$H^1(\mathrm{Gal}(M_{\mathfrak{L}}/K_{\mathfrak{l}}), E^d(M_{\mathfrak{L}})) = 0.$$

□

Next, we look at the action of δ on $H_{S_E,u}(K(\sqrt{d}))$.

Lemma 4.3.3. *The generator* $\langle\delta\rangle = \mathrm{Gal}(K(\sqrt{d})/K)$ *acts as* $-\mathrm{id}$ *on the Galois group* $H_{S_E,u}(K(\sqrt{d}))$.

Proof. We may write

$$H_{S_E,u}(K(\sqrt{d})) = H^- \oplus H^+$$

where H^- is the part where δ acts as $-\mathrm{id}$, and H^+ the part with $\delta = \mathrm{id}$. Let $\widetilde{M} := M_{S_E,u}^{H^-}$, which is the fixed field of $M_{S_E,u}$ by H^-. Assume that M_1 is a subfield of $\widetilde{M}$ that is cyclic over $K(\sqrt{d})$. Hence M_1/K is cyclic of degree $2 \cdot [M_1 : K(\sqrt{d})]$. Let M_2 be the cyclic extension of K with degree $[M_1 : K(\sqrt{d})]$ contained in M_1. Then M_2 is unramifed outside of S_E. For $\mathfrak{p} \in S_E$, we have that $\chi_H(\mathfrak{p}) \neq 0$. Since $[M_2 : K]|\ell$ and $\ell \nmid \mathrm{cl}(K)$, it follows that M_2 is not contained in the Hilbert class field of K and is unramified at all primes K. Thus, we have that $M_2 = K$, $M_1 = K(\sqrt{d})$ and hence $\widetilde{M} = K(\sqrt{d})$. □

Proof of Theorem 4.2.1. The divisibility of $\#\,\mathrm{Sel}_\ell(E^d, K)$ by $\mathrm{cl}_{S_E,u}(K(\sqrt{d}))[\ell]$ follows from Lemmas 4.3.2, 4.3.3 since our element $\phi \in \mathrm{Sel}_\ell(E^d, K)$ is induced

by $\alpha \in \mathrm{Gal}(M/K(\sqrt{d}))$ and the action of $\langle\delta\rangle$ on $H_{S_E,u}(K(\sqrt{d}))$ does not affect the order of α when considered as an element of $H_{S_E,u}(K(\sqrt{d}))$. □

4.4 Proof of Theorem 4.2.2

Before we proceed with a proof of Theorem 4.2.2, we wish to shed some light onto our assumptions. In general, our hypotheses allow us to control the ramification in cyclic extensions of $K(\sqrt{d})$.

Remark 4.4.1 (Field assumptions). We assume that our field K is a number field of degree $n \leq 5$ such that $N_{K/\mathbf{Q}}(\mathfrak{q}) = 2$ for all $\mathfrak{q}|2$ and that for some $\ell \in S(n)\setminus\{2,3\}$, $\ell \nmid \mathrm{cl}(K)$ and $\zeta_\ell \notin K$. The degree and norm condition appear in Lemma 5.1.1 and allow us to deduce ramification conditions on prime divisors $\mathfrak{Q}_M|\mathfrak{q}$ where M_1/K is cyclic. The condition that $\ell \nmid \mathrm{cl}(K)$ implies that there does not exist an extension M_2/K of degree ℓ contained in the Hilbert class field of K; once again this gives us a ramification consequence. The assumption that $\zeta_\ell \notin K$ is subtle, but it allows for more ramification possibilities since Kummer theory does not restrict cyclic extensions. The final condition that $e_\mathfrak{l}(K/\mathbf{Q}) \neq 5$ when $[K:\mathbf{Q}] = 5$ and $\ell = 5$ is due to a deep result of Katz [Kat80] concerning the injectivity of ℓ-torsion under the reduction map; the assumption $1 > e_\mathfrak{l}(K/\mathbf{Q})/(\ell-1) - 1$ from Theorem 4.2.5 is the general condition. This assumption allows us to use the fact that prime to 2 torsion will inject under the reduction map.

To prove Theorem 4.2.2, it suffices to prove the divisibility statement

$$\#\,\mathrm{Sel}_\ell(E^d, K)\Big|\, \mathrm{cl}_{\widetilde{S}_E,u}(K(\sqrt{d}))[\ell]\cdot \mathrm{cl}_{S_E}(K')[\ell](\chi_\ell).$$

To begin, we discuss the Galois structure of the ℓ-division field of elliptic curves E/K from Theorem 4.2.2.

4.4.2 Galois structure of splitting fields of ℓ-covers of E

We want to determine the Galois group structure of splitting fields of elements in $H^1(G_K, E(\overline{K})[\ell])$ for elliptic curves having a K-rational point P of order ℓ. Recall that $\zeta_\ell \notin K$. Denote the ℓ-division field by $K(E[\ell])$; this is the field obtained by adjoining the x, y coordinates of all points of order ℓ of E to K. Then $K(E[\ell])$ is a Galois extension of K containing $K(\zeta_\ell)$, and it is cyclic over $K(\zeta_\ell)$ of degree dividing ℓ. From this point on, we shall abbreviate $E(\overline{K})[\ell]$ with $E[\ell]$, and similarly for $E^d[\ell]$.

Lemma 4.4.3. *The Galois group $K(E[\ell])/K$ is generated by two elements $\overline{\gamma}, \overline{\varepsilon}$ with $\overline{\gamma}^{\ell-1} = \mathrm{id}$, $\overline{\varepsilon}^{\ell} = \mathrm{id}$, $\overline{\gamma}|K(\zeta_\ell)$ generates $K(\zeta_\ell)/K$, and $\overline{\gamma\varepsilon\gamma}^{-1} = \overline{\varepsilon}^{\chi_\ell(\overline{\gamma})^{-1}}$.*

Proof. Choose a base of the form $\{P, Q\}$ of $E[\ell]$ such that for $\sigma \in \mathrm{Gal}(K(E[\ell])/K)$ the action of σ on $E[\ell]$ induces the matrix

$$\rho_\sigma = \left(\begin{smallmatrix} 1 & b \\ 0 & a \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_\ell),$$

with $a = \det(\rho_\sigma) \equiv \chi_\ell(\sigma) \mod \ell$. Now we choose $\overline{\gamma}$ such that

$$\rho_{\overline{\gamma}} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_\ell).$$

with w a generator of $(\mathbf{Z}/\ell\mathbf{Z})^\times$. Also, we pick $\overline{\varepsilon} = \mathrm{id}$ if $K(E[\ell]) = K(\zeta_\ell)$. If $K(E[\ell]) \neq K(\zeta_\ell)$, we choose $\overline{\varepsilon}$ such that

$$\rho_{\overline{\varepsilon}} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_\ell).$$

Then $\overline{\gamma}$ and $\overline{\varepsilon}$ generate $\mathrm{Gal}(K(E[\ell])/K)$ and since

$$\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & w^{-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & w^{-1} \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^{w^{-1}}$$

we have the relation $\overline{\gamma\varepsilon\gamma}^{-1} = \overline{\varepsilon}^{\chi_\ell(\overline{\gamma})^{-1}}$. □

Remark 4.4.4. The choice of $\overline{\gamma}$ and $\overline{\varepsilon}$ is closely related to the choice of base $\{P, Q\}$. In particular, we have $\overline{\varepsilon}(Q) = P + Q$ if $\overline{\varepsilon} \neq \mathrm{id}$ and $\overline{\gamma}(Q) = \chi_\ell(\overline{\gamma})Q$.

Let $d \in \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ be negative and relatively prime to $\mathfrak{l} \cdot N(E)$. We define L_d to be the quadratic extension of $K(E[\ell])$ given by the compositum $K(\sqrt{d}) \cdot K(E[\ell])$. The Galois group $\mathrm{Gal}(L_d/K)$ is generated by three elements $\delta, \gamma, \varepsilon$ with δ commuting with ε and γ and

$$\begin{aligned} \delta^2 &= \mathrm{id}, & \delta(\sqrt{d}) &= -\sqrt{d}, \\ \gamma^{\ell-1} &= \mathrm{id}, & \gamma|K(E[\ell]) &= \overline{\gamma}, \\ \varepsilon^\ell &= \mathrm{id}, & \varepsilon|K(E[\ell]) &= \overline{\varepsilon}, \\ \gamma^i\varepsilon^j|K(\sqrt{d}) &= \mathrm{id}, & \gamma\varepsilon\gamma^{-1} &= \varepsilon^{\chi_\ell(\gamma)^{-1}}. \end{aligned}$$

In particular, we have that δ operates as $-\mathrm{id}$ on $E^d[\ell]$, the points of order ℓ of E^d. The fixed field of ε is $K(\sqrt{d}, \zeta_\ell)$ and the fixed field of $\langle \varepsilon, \delta\gamma^{(\ell-1)/2} \rangle$ is K' as defined in Theorem 4.2.2. Thus, we have the following field diagram: We now describe the elements in $H^1(G_K, E^d[\ell])$. We have the exact inflation-restriction sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) \xrightarrow{\text{inf.}} H^1(G_K, E^d[\ell]) \xrightarrow{\text{res.}} H^1(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell]),$$

where $H^1(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell]) = \mathrm{Hom}_{\mathrm{Gal}(L_d/K)}(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell])$.

Lemma 4.4.5. *The group* $H^1(G_K, E^d[\ell])$ *injects into* $\mathrm{Hom}_{\mathrm{Gal}(L_d/K)}(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell])$.

Proof. We need to show that $H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) = 0$. If $\varepsilon = \mathrm{id}$, the degree of L_d/K is prime to ℓ, and the assertion follows. Now let ε be of order ℓ. Using the inflation-restriction sequence, one has that

$$H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) = H^1(\langle \varepsilon \rangle, E^d[\ell])^{\langle \delta, \gamma \rangle}.$$

Let P_d, Q_d be the points of order ℓ of $E^d[\ell]$ corresponding to $P, Q \in E[\ell]$.

Then $P_d = \varepsilon Q_d - Q_d$, and hence $H^1(\langle\varepsilon\rangle, E^d[\ell])$ is generated by the class of cocycle ψ which sends ε to Q_d. Since $\delta\varepsilon\delta = \varepsilon$ and $\delta Q_d = -Q_d$, we have that $\psi \notin H^1(\langle\varepsilon\rangle, E^d[\ell])^{\langle\delta\rangle}$, and thus $H^1(\mathrm{Gal}(L_d/K), E^d[\ell]) = H^1(\langle\varepsilon\rangle, E^d[\ell])^{\langle\delta,\gamma\rangle} = 0$. □

Take an element $\widetilde{\Phi} \in H^1(G_K, E^d[\ell])$ with

$$\mathrm{res}\,\widetilde{\Phi} = \phi \in \mathrm{Hom}_{\mathrm{Gal}(L_d/K)}(\mathrm{Gal}(\overline{K}/L_d), E^d[\ell])$$

and denote by M the fixed field of the kernel of ϕ. M/K is normal and $\mathrm{Gal}(M/L_d)$ is possibly generated by two elements α_1, α_2 with $\alpha_i^\ell = \mathrm{id}$, which we may choose in such a way that

$$\phi(\alpha_1) = \mu_1 P \quad \text{and} \quad \phi(\alpha_2) = \mu_2 Q.$$

We may also assume that $\mu_i = 1$ if $\alpha_i \neq \mathrm{id}$.

We extend $\delta, \gamma, \varepsilon \in \mathrm{Gal}(L_d/K)$ to elements $\widetilde{\delta}, \widetilde{\gamma}, \widetilde{\varepsilon} \in \mathrm{Gal}(M/K)$ and compute that the actions of these elements on α_i. We assume that $\widetilde{\delta}^2 = \widetilde{\gamma}^{\ell-1} = \mathrm{id}$. Since

$$\phi(\beta\alpha_i\beta^{-1}) = \beta\phi(\alpha_i) \quad \forall\,\beta \in \mathrm{Gal}(M/K)$$

via the fact that ϕ is a group homomorphism and the cocycle condition we

get:

$$\begin{aligned}
\widetilde{\delta}\alpha_i\widetilde{\delta} &= \alpha_i^{-1} && (\because\ \widetilde{\delta}|E^d[\ell] = -\mathrm{id})\\
\widetilde{\gamma}\alpha_1\widetilde{\gamma}^{-1} &= \alpha_1 && (\because\ \widetilde{\gamma}P = P),\\
\widetilde{\gamma}\alpha_2\widetilde{\gamma}^{-1} &= \alpha_2^{\chi_\ell(\widetilde{\gamma})} && (\because\ \widetilde{\gamma}Q = \chi_\ell(\widetilde{\gamma})Q),\\
\widetilde{\varepsilon}\alpha_1\widetilde{\varepsilon}^{-1} &= \alpha_1 && (\because\ \widetilde{\varepsilon}P = P),\\
\widetilde{\varepsilon}\alpha_2\widetilde{\varepsilon}^{-1} &= \alpha_1\alpha_2 && \text{if } \varepsilon \neq \mathrm{id} \text{ and } \alpha_2 \neq \mathrm{id}(\because\ \text{then } \varepsilon\phi(\alpha) =\\
& && \varepsilon P = P + Q = \phi(\alpha_1\alpha_2);\ \text{necessarily } \alpha_1 \neq \mathrm{id}\\
& && \text{in this case}).
\end{aligned}$$

In particular, it follows that $\langle\alpha_1\rangle$ is a normal subgroup of $\mathrm{Gal}(M/K)$ and that $\langle\alpha_2\rangle$ is normal if either $\alpha_2 = \mathrm{id}$ or $\widetilde{\varepsilon} = \mathrm{id}$.

Now we distinguish between two cases:

Case 1. $\widetilde{\varepsilon} = \mathrm{id}$. In this case $\langle\alpha_1\rangle$ and $\langle\alpha_2\rangle$ are both normal in $\mathrm{Gal}(M/K)$ and hence

$$M_i := M^{\langle\alpha_i\rangle}$$

are normal extensions of K. The Galois group of $M_2/K(\sqrt{d})$ is abelian and generated by the restriction of $\langle\widetilde{\gamma}, \alpha_1\rangle$ to M_2. Hence

$$\overline{M}_2 := M^{\langle\alpha_2,\widetilde{\gamma}\rangle}$$

is Galois over K containing $K(\sqrt{d})$ and if $\alpha_1 \neq \mathrm{id}$, then $\mathrm{Gal}(\overline{M}_2/K)$ is non-abelian of order 2ℓ. Since

$$\widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}\alpha_2(\widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2})^{-1} = \alpha_2,$$

it follows that M_1 is abelian over K' and hence

$$\overline{M}_1 := M^{\langle \alpha_1, \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2} \rangle}$$

is normal over K. Its Galois group is generated by

$$\overline{\alpha}_2 = \alpha_2 | \overline{M}_1 \quad \text{and} \quad \overline{\gamma} = \widetilde{\gamma} | \overline{M}_1,$$

and its order is equal to $|\alpha_2| \cdot (\ell - 1)$. Also one has the relation $\overline{\gamma \alpha_2 \gamma}^{-1} = \overline{\alpha}_2^{\chi_\ell(\overline{\gamma})}$. To summarize, we have that

$$\begin{aligned} \overline{M}_1(\phi) &:= M^{\langle \alpha_1, \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2} \rangle}, \\ \overline{M}_2(\phi) &:= M^{\langle \alpha_2, \widetilde{\gamma} \rangle}. \end{aligned}$$

Case 2. $|\widetilde{\varepsilon}| = \ell$. In this case, we may assume that $\alpha_1 \neq \mathrm{id}$ for $\alpha_1 = \mathrm{id}$ implies that $\alpha_2 = \mathrm{id}$, as well.

Subcase (i). $\alpha_2 = \mathrm{id}$. We assert that $\mathrm{Gal}(M/K(\zeta_\ell, \sqrt{d}))$ is not cyclic. Otherwise $\widetilde{\varepsilon}$ would be an element of order ℓ^2 with $\widetilde{\varepsilon}^\ell = \alpha_1$ (without lose of generality). So $\widetilde{\delta}\widetilde{\varepsilon}^\ell\widetilde{\delta} = \widetilde{\varepsilon}^{-\ell}$ and hence

$$\widetilde{\delta}\widetilde{\varepsilon}\widetilde{\delta} = \widetilde{\varepsilon}^k \quad \text{with } k \equiv -1 \mod \ell.$$

But since $\delta\varepsilon\delta = \varepsilon$, we would get $\delta\widetilde{\varepsilon}\delta = \widetilde{\varepsilon} \cdot (\widetilde{\varepsilon}^\ell)^n = \widetilde{\varepsilon}^{1+\ell n}$ which gives a contradiction. Hence, we can choose $\widetilde{\varepsilon}$ so that

$$\widetilde{\varepsilon}^\ell = \widetilde{\alpha}_1^\ell = \mathrm{id} \quad \text{and} \quad \widetilde{\delta}\widetilde{\varepsilon}\widetilde{\delta} = \widetilde{\varepsilon},$$

which determines $\widetilde{\varepsilon}$ uniquely. Thus, $\overline{M}_2 := M^{\langle \widetilde{\varepsilon}, \widetilde{\gamma} \rangle}$ is normal over K and contains $K(\sqrt{d})$ and its Galois group is dihedral of order 2ℓ and generated

by $\langle \alpha_1, \widetilde{\delta} \rangle$. To summarize, we say that

$$\overline{M}_1(\phi) := M^{\langle \alpha_1, \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2} \rangle},$$
$$\overline{M}_2(\phi) := M^{\langle \widetilde{\varepsilon}, \widetilde{\gamma} \rangle}.$$

Subcase (ii). $\alpha_2 \neq \mathrm{id}$. We have that $M_1 := M^{\langle \alpha_1 \rangle}$ is normal over K and of degree ℓ over L_d. Since $\widetilde{\delta}\alpha_2\widetilde{\delta} = \alpha_2^{-1}$, we conclude as above that ε has an extension $\widetilde{\varepsilon}$ to M_1 of order ℓ with $\widetilde{\delta}\widetilde{\varepsilon}\widetilde{\delta} = \widetilde{\varepsilon}$. Since $\widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}$ acts trivially on α_2 and $\widetilde{\varepsilon}$ acts trivially on $\alpha_2|M_1$, we have that $\langle \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}, \widetilde{\varepsilon} \rangle$ is a normal subgroup of $\mathrm{Gal}(M_1/K)$. Hence

$$\overline{M}_1 := M_1^{\langle \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}, \widetilde{\varepsilon} \rangle}$$

is normal over K containing K', and its Galois group over K' is generated by $\overline{\alpha}_2 = \alpha_2|\overline{M}_1$, which is of order ℓ and satisfies the relation

$$\overline{\gamma}\overline{\alpha}_2\overline{\gamma}^{-1} = \overline{\alpha}_2^{\chi_\ell(\overline{\gamma})} \quad \text{with } \overline{\gamma} = \widetilde{\gamma}|K'.$$

In order to simplify notation, we define $\overline{M}_2(\phi) := K(\sqrt{d})$ if either $\varepsilon \neq \mathrm{id}$ or $\alpha_2 \neq \mathrm{id}$. To summarize, we say that

$$\overline{M}_1(\phi) := M_1^{\langle \widetilde{\delta}\widetilde{\gamma}^{(\ell-1)/2}, \widetilde{\varepsilon} \rangle},$$
$$\overline{M}_2(\phi) := K(\sqrt{d}).$$

Hence for a given

$$\widetilde{\Phi} \in H^1(G_K, E^d[\ell])$$

we have a field $M = M(\phi)$ which determines $\langle \phi \rangle$ completely where $\phi = \mathrm{res}(\widetilde{\Phi})$. We want to study the information we attain from the pair $(\overline{M}_1(\phi), \overline{M}_2(\phi))$. If $\varepsilon = \mathrm{id}$ or $\alpha_2 = \mathrm{id}$, then we get back $M(\phi) = M$ from $(\overline{M}_1(\phi), \overline{M}_2(\phi))$. In

these cases, we shall say that ϕ is of first type. What happens if $\varepsilon \neq \mathrm{id}$ and $\alpha_2 \neq \mathrm{id}$? Assume that

$$\phi \neq \psi \in H^1(G_K, E^d[\ell])$$

have fields $M(\phi)$ and $M(\psi)$ with Galois groups $\langle \alpha_1, \alpha_2 \rangle$ and $\langle \beta_1, \beta_2 \rangle$ as above such that

$$M(\phi)^{\alpha_1} = M(\psi)^{\beta_1}.$$

Let N be the composite of $M(\phi)$ and $M(\psi)$. Then the Galois group $\mathrm{Gal}(N/L_d)$ is generated by three elements $\langle \sigma_1, \sigma_2, \sigma_3 \rangle$, which we can choose in such a way that

$$\sigma_1|M(\phi) = \alpha_1, \;\; \sigma_1|M(\psi) = \beta_1^\lambda$$

$$\sigma_2|M(\phi) = \alpha_2, \;\; \sigma_2|M(\psi) = \beta_2^\lambda$$

where $\lambda \in \{1, \ldots, \ell - 1\}$. N is a splitting field of ϕ and ψ, and

$$(\phi - \lambda^{\ell-1}\psi)(\sigma_1) = (\phi - \lambda^{\ell-1}\psi)(\sigma_2) = 0.$$

Hence the fixed field of the kernel of $\phi - \lambda\psi$ is a cyclic extension of L_d which is normal over K, and $\phi - \lambda^{-1}\psi$ is of first type.

Thus, $\overline{M}_1(\phi)$ determines $\langle \phi \rangle$ up to elements of first type, and in order to determine all elements in $H^1(G_K, E^d[\ell])$, it is enough to determine all dihedral extensions of K of degree 2ℓ containing $K(\sqrt{d})$ and all extensions M_1 of degree ℓ over K' which are normal over K such that conjugation by $\overline{\gamma}$ on $\mathrm{Gal}(\overline{M}_1, K')$ is equal to $\chi_\ell(\overline{\gamma})$.

Therefore to prove the double divisibility, one has to show that for $\phi \in \mathrm{Sel}_\ell(E^d, K)$, the field $\overline{M}_2(\phi)$ is unramified over $K(\sqrt{d})$ outside $\widetilde{S}_E$, and $\overline{M}_1(\phi)$ is unramifed over K' outside S_E and little ramified at divisors of $\mathfrak{l}$.

4.4.6 Splitting fields of elements in $\mathrm{Sel}_\ell(E^d, K)$

We shall continue to use the assumptions and the notations of the Theorem 4.2.2 and Section 4.4.2.

Lemma 4.4.7. *Let ϕ be an element in $\mathrm{Sel}_\ell(E^d, K)$. Then $\overline{M}_1(\phi) =: \overline{M}_1$ is unramified at $\mathfrak{q}$ over K' and $\overline{M}_2(\phi) =: \overline{M}_2$ is unramified at $\mathfrak{q}$ over $K(\sqrt{d})$.*

Proof. We first prove the latter statement. Since $\mathfrak{q}|\Delta_{K(\sqrt{d})/K}$, we have that $K(\sqrt{d})$ and K' are ramified at $\mathfrak{q}$ over K. Hence the norm of $\mathfrak{Q}|\mathfrak{q}$ in $K(\sqrt{d})$ is equal to $\mathfrak{q}$, and by assumption the norm of $\mathfrak{Q}|2$ is equal to 2. Suppose that $K(\sqrt{d})$ had a cyclic extension of degree ℓ in which $\mathfrak{Q}$ is ramified. Then the completion $K(\sqrt{d})_{\mathfrak{Q}}$ admits a cyclic extension of degree ℓ ramified at $\mathfrak{Q}$. Since ℓ is odd and $\mathfrak{Q}$ has residue characteristic two, this extension is tamely ramified. By local class field theory, the tamely ramified cyclic extensions of a local field $K(\sqrt{d})_{\mathfrak{Q}}$ all have degree dividing $|\kappa^\times|$, where κ is the residue field. Since $\kappa = \mathbf{F}_2$, we have that there are no tamely ramified and ramified extensions of $K(\sqrt{d})_{\mathfrak{Q}}$. Thus, $K(\sqrt{d})$ has no cyclic extension of degree ℓ in which $\mathfrak{Q}$ ramifies, and hence $\overline{M}_2$ is unramified at $\mathfrak{q}$ over $K(\sqrt{d})$.

To prove the former statement, we shall utilize the proof of [Fre88, Lemma 3] and look prime by prime. For $\ell = 5$, the same argument as above can be applied to $\mathfrak{Q}_{K'}|\mathfrak{q}$. For $\ell = 7$, there is only one extension $\mathfrak{Q}|\mathfrak{q}$ to K' which is ramified of order 2 and has norm 8. Assume that $\mathfrak{Q}_{K'}$ is ramified in $\overline{M}_1/K'$ and let $\mathfrak{Q}_{\overline{M}_1}$ be the unique extension of $\mathfrak{Q}_{K'}$ to $\overline{M}_1$. Let M_t be the subfield of $\overline{M}_1$ in which $\mathfrak{Q}_{\overline{M}_1}$ is tamely ramified. Then M_t is a cyclic extension of degree 7 over $K(\zeta_7 + \zeta_7^{-1})$, and $\overline{M}_1$ is the compositum of M_t with K' over $K(\zeta_7 + \zeta_7^{-1})$. Thus, $\mathrm{Gal}(\overline{M}_1/K(\zeta_7 + \zeta_7^{-1}))$ is abelian. But this contradicts the fact that

$$\overline{\gamma}^3\overline{\alpha}\overline{\gamma}^3 = \overline{\alpha}^{\chi_7(\overline{\gamma}^3)} = \overline{\alpha}^{-1},$$

where $\langle\overline{\alpha}\rangle = \mathrm{Gal}(\overline{M}_1/K')$ and $\langle\overline{\gamma}\rangle = \mathrm{Gal}(K'/K)$.

For $\ell = 11, 13, 19, 37$, we can use the same proof as the first statement since

$$\begin{array}{llll} 11 \nmid (2^5 - 1) & 13 \nmid (2^2 - 1) & 37 \nmid (2^3 - 1) & 37 \nmid (2^{18} - 1) \\ 13 \nmid (2^6 - 1) & 19 \nmid (2^9 - 1) & 37 \nmid (2^9 - 1) & 37 \nmid (2^2 - 1). \\ 13 \nmid (2^3 - 1) & 19 \nmid (2^3 - 1) & 37 \nmid (2^6 - 1) & \end{array}$$

For $\ell = 17$, there there is only one extension $\mathfrak{Q}|\mathfrak{q}$ to K' which is ramified of order 2 and has norm 2^8 (note that $17|(2^8 - 1)$). If we assume that $\mathfrak{Q}_{K'}$ is ramified in $\overline{M}_1/K'$, then we can use the above argument to construct the same contradiction. □

Remark 4.4.8. Since $73|(2^{36} - 1)$, $73|(2^9 - 1)$, and $73|(2^{18} - 1)$, we may not assume that there is a unique cyclic extension of K' with degree 73 in which $\mathfrak{Q}$ is ramified, and hence the above argument does work for $\ell = 73$. This precludes us from extending Theorem 4.2.2 to number fields K of degree 6.

Therefore, we can assume that $\mathfrak{p} \nmid \mathfrak{q} \cdot \mathfrak{l}$, but $\mathfrak{p}|N(E)$.

Lemma 4.4.9. *Let ϕ be an element in $\mathrm{Sel}_\ell(E^d, K)$. Then $\overline{M}_1/K'$ is unramified outside of $S_E \cup \{\mathfrak{l}\}$ and $\overline{M}_2/K(\sqrt{d})$ is unramified outside $\widetilde{S}_E \cup \{\mathfrak{l}\}$.*

Proof. We have to test prime numbers $\mathfrak{p} \neq \mathfrak{l}$ that divide $N(E)$.

1. If $\mathrm{ord}_\mathfrak{p}(j_E) \geq 0$, then it follows from Néron's list of minimal models of elliptic curves with potentially good reduction that ℓ must be equal to 3 ([Nér64, p.124]). Since we only consider primes $\ell > 3$, we can exclude this case from consideration.

2. Now assume that $\mathrm{ord}_\mathfrak{p}(j_E) < 0$. We have two subcases:

   (a) If $\mathrm{ord}_\mathfrak{p}(j_E) \equiv 0 \mod \ell$, we have that $\mathfrak{p} \notin S_E$ and so E^d is not a Tate curve over $K_\mathfrak{p}$. Moreover, $K_\mathfrak{p}(E[\ell])$ is unramified over $K_\mathfrak{p}$ and hence

$\overline{M_1}/K'$ and $\overline{M_2}/K(\sqrt{d})$ are unramified at all divisors of $\mathfrak{p}$ if and only if M_1/L_d (resp. M_2/L_d) are unramified at all divisors of $\mathfrak{p}$. We now use the triviality of the $\phi \in \mathrm{Sel}_\ell(E^d, K)$ over $K_\mathfrak{p}$ from Lemma 4.3.2. Also recall that M is the fixed field of the kernel of ϕ. We shall show that $\mathfrak{Q}_M$ is unramified over L_d.

There is a $\widetilde{P} \in E^d(M_\mathfrak{P})$ where $\mathfrak{P}_M|\mathfrak{p}$ such that for all $\sigma \in D(\mathfrak{P}_M)$, we have $\sigma\widetilde{P} - \widetilde{P} = \phi(\sigma)$. Hence

$$P' := \ell \cdot \widetilde{P} \in E^d(K_\mathfrak{p})$$

and so $2P'$ is in the connected component of unity modulo $\mathfrak{p}$ via Remark 4.1.6. Hence $\widetilde{P} = \widetilde{P}_1 + P_2$ with $P_2 \in E^d[\ell]$ and $2\widetilde{P}_1$ in the component of the unity of $E \mod \mathfrak{P}_M$, so $\widetilde{P}_1$ corresponds to a $\mathfrak{P}_M$-adic unity u under the Tate parametrization. Now take

$$\alpha \in \langle \alpha_1, \alpha_2 \rangle \cap I(\mathfrak{P}_M)$$

where $I(\mathfrak{P}_M)$ is the interia group of $\mathfrak{P}_M$. Then $2(\alpha\widetilde{P} - \widetilde{P})$ corresponds to $\alpha u/u$ and is an ℓ^{th} root of unity. By Hilbert's Theorem 90, we have that $\alpha = \mathrm{id}$, and thus, $\mathfrak{P}_M$ is unramified over L_d.

(b) If $\mathrm{ord}_\mathfrak{p}(j_E) \not\equiv 0 \mod \ell$, then the values at the Hecke characters χ of order ℓ tell us that either E is a Tate curve over $K_\mathfrak{p}$ or that $\mathfrak{p} \in S_E$. Consider the former situation. Our assumptions from Theorem 4.2.2 tell us that $\mathfrak{q}$ is not completely decomposed in $K(\sqrt{d})$ and K'. Since

$$K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^\ell \cong K_\mathfrak{p}(\sqrt{d})^\times/(K_\mathfrak{p}(\sqrt{d})^\times)^\ell \cong K_\mathfrak{P}'^\times/(K_\mathfrak{P}'^\times)^\ell$$

for all $\mathfrak{P}_{K'}|\mathfrak{p}$, we see that for all cyclic extensions $\overline{M}_1$ of K' and $\overline{M}_2/K(\sqrt{d})$ of degree ℓ and divisors $\mathfrak{P}_{M_i}|\mathfrak{p}$, one has that $\mathrm{Gal}(\overline{M}_{i,\mathfrak{P}_{M_i}}/K_\mathfrak{q})$ is abelian

of even order. But this implies that

$$\overline{M}_{1,\mathfrak{P}} = K'_{\mathfrak{p}} \quad \text{and} \quad \overline{M}_{2,\mathfrak{P}} = K_{\mathfrak{P}}(\sqrt{d}),$$

which is absurd. Thus $\mathfrak{p} \in S_E$ and our lemma follows.

□

The next step is to describe the behavior of $\overline{M}_i$ at divisors of $\mathfrak{l}$.

Lemma 4.4.10. *Assume that* $\mathrm{ord}_{\mathfrak{l}}(j_E) < 0$ *and* $\phi \in \mathrm{Sel}_\ell(E^d, K)$. *Then* $\overline{M}_2/K(\sqrt{d})$ *is unramified at* $\mathfrak{l}$ *and* $\overline{M}_1/K'$ *is little ramified at divisors of* $\mathfrak{l}$.

Proof. The assumptions tells us that $E/K_{\mathfrak{l}}$ is a Tate curve but that $E^d/K_{\mathfrak{l}}$ is not a Tate curve. Since $K_{\mathfrak{l}}(E[\ell]) = K_{\mathfrak{l}}(\zeta_\ell)$, the behavior of $\overline{M}_i$ at $\mathfrak{l}$ is determined by the behavior of M at $\mathfrak{l}$. Let $\mathfrak{L}_M|\mathfrak{l}$, let $I(\mathfrak{L}_M)$ be the inertia group of $\mathfrak{L}_M$, and let

$$\alpha \in \langle \alpha_1, \alpha_2 \rangle \cap I(\mathfrak{L}_M).$$

As in the proof of Lemma 4.4.9, we can use the fact that $E^d/K_{\mathfrak{l}}$ is not a Tate curve to show that there is a $\widetilde{Q} \in E^d(M_{\mathfrak{L}})$ where $\mathfrak{L}_M|\mathfrak{l}$ and $\alpha\widetilde{Q} - \widetilde{Q} = \phi(\alpha)$. Hence $2\widetilde{Q}$ is in the connected component of unity modulo $\mathfrak{L}_M$ via Remark 4.1.6. This implies that

$$M_{\mathfrak{L}_M} = M_{\mathfrak{L}_M}^{\langle\alpha\rangle}(\sqrt[\ell]{u})$$

where u is a $\mathfrak{L}_M$-adic unit corresponding to $2\widetilde{Q}$ under the Tate parametrization. Moreover, M_1/L_d is little ramified at $\mathfrak{l}$.

Now assume that $\alpha_2 = \mathrm{id}$ or $\varepsilon = \mathrm{id}$. Then $\overline{M}_2/K(\sqrt{d})$ is of degree ℓ, and we have to show that $\overline{M}_2/K(\sqrt{d})$ is unramified at $\mathfrak{L}_{\overline{M}_2}|\mathfrak{l}$. We recall the choice of point Q. Since $\gamma Q = \chi_\ell(\gamma)Q$ where $\langle\gamma\rangle = \mathrm{Gal}(K(\zeta_\ell)/K)$, it follows that Q is in the kernel of the reduction of E modulo all divisors of $\mathfrak{l}$, and hence $P + \lambda Q$ is not in this kernel where $\lambda \in \mathbf{N}$. For $\alpha \in I(\mathfrak{L}_M)$, we saw that

$\sigma\widetilde{Q} - \widetilde{Q} = \phi(\sigma)$ is in the kernel of the reduction modulo $\mathfrak{L}_M$, and hence

$$\alpha_1\alpha_2^\lambda \notin I(\mathfrak{L}_M) \quad \forall \lambda \in \mathbf{N} \text{ and } \mathfrak{L}_M|\mathfrak{l}.$$

Thus, it follows that $M^{\langle\alpha_2\rangle}/L_d$ is unramified at $\mathfrak{L}_M$ and $\overline{M}_2/K(\sqrt{d})$ is unramified at $\mathfrak{l}$. □

Finally, we look at the case where $\mathrm{ord}_\mathfrak{l}(j_E) \geq 0$.

Lemma 4.4.11. *Assume that E/K has a K-rational point P of order $\ell > 3$, that $\mathrm{ord}_\mathfrak{l}(j_E) \geq 0$, and that P is not contained in the kernel of reduction modulo $\mathfrak{l}$, in particular, this means that E is not supersingular modulo $\mathfrak{l}$. Let ϕ be an element in $\mathrm{Sel}_\ell(E^d, K)$ with corresponding fields $\overline{M}_1$ and $\overline{M}_2$. Then $\overline{M}_1/K'$ is little ramified at $\mathfrak{l}$, and $\overline{M}_2/K(\sqrt{d})$ is unramified at $\mathfrak{l}$.*

Proof. Suppose that $\mathrm{ord}_\mathfrak{l}(j_E) \geq 0$, which implies that E has potentially good reduction at $\mathfrak{l}$. Since E/K has a K-rational point P of order $\ell > 3$, we know that $\mathrm{Gal}(K(E[\ell])/K(\zeta_\ell))$ is a subgroup of the additive group $\mathbf{F}_\ell^+$. We want to show that all divisors of $\mathfrak{l}$ are not ramified in $K(E[\ell])/K(\zeta_\ell)$. If E has good reduction over $K(\zeta_\ell)$, then we are immediately done. If E does not have good reduction over $K(\zeta_\ell)$, then there must exist some extension $N/K(\zeta_\ell)$ such that $[N : K(\zeta_\ell)]|6$ and that E has good reduction at all divisors $\mathfrak{L}_N|\mathfrak{l}$; this divisibility condition is similar to the proof of [Sil09, Proposition VII.5.4.c]. From our assumptions, it follows that $N_\mathfrak{L}$ contains $K(E[\ell])$ and that $\langle Q\rangle$ is the subgroup of order ℓ of the kernel of reduction modulo $\mathfrak{L}_N$. Hence all divisors of $\mathfrak{l}$ are not ramified in $K(E[\ell])/K(\zeta_\ell)$, and we can prove the lemma by looking at the behavior of $\mathfrak{l}$ in M/L_d.

Assume that $\mathfrak{L}_M|\mathfrak{l}$ and let $I(\mathfrak{L}_M)$ be the inertia group of $\mathfrak{L}_M$. Suppose that $\alpha_1^\mu\alpha_2^\lambda \in I(\mathfrak{L}_M)$. There there is a $\widetilde{P} \in E(M_\mathfrak{L})$ with

$$(\alpha_1^\mu\alpha_2^\lambda)\widetilde{P} - \widetilde{P} = \mu P + \lambda Q.$$

But we know that for $\mu \neq 0$, the point $\mu P + \lambda Q$ is not in the kernel of reduction modulo $\mathfrak{L}_M$. Let $\widetilde{E}$ be a model of E over N having good reduction modulo $\mathfrak{L}_N|\mathfrak{l}$. Since $(I(\mathfrak{L}_M) - \mathrm{id})\widetilde{E}(N \cdot M_{\mathfrak{L}})$ is contained in this kernel, we must have that $\mu = 0$, and hence

$$I(\mathfrak{L}_M) \cap \mathrm{Gal}(M/L_d) \subseteq \langle \alpha_2 \rangle.$$

Thus, $M^{\langle \alpha_2 \rangle}/L_d$ is unramified at $\mathfrak{L}_M$; moreover, $\overline{M}_2/K(\sqrt{d})$ is unramified above $\mathfrak{l}$.

Now assume that $I(\mathfrak{L}_M) = \langle \alpha_2 \rangle$. Then $Q = \alpha_2 \widetilde{Q} - \widetilde{Q}$ and since $\langle \alpha_2 \rangle$ acts trivially on $\widetilde{E}(N \cdot M_{\mathfrak{L}})/\widetilde{E}_-(N \cdot M_{\mathfrak{L}})$, we may assume that $\widetilde{Q} \in \widetilde{E}_-(N \cdot M_{\mathfrak{L}})$ and hence $\ell \cdot \widetilde{Q} \in \widetilde{E}_-(N \cdot K_{\mathfrak{l}})$. Since $\widetilde{E}$ has ordinary reduction modulo $\mathfrak{L}_M$, we have that $N \cdot K_{\mathfrak{l}}(\widetilde{Q})$ is little ramified at divisors of $\mathfrak{l}$. Thus, our lemma follows. □

Lemmas 5.1.1, 4.4.9, 5.1.2, 5.1.3 prove that for $\phi \in \mathrm{Sel}_\ell(E^d, K)$, the field $\overline{M}_2(\phi)$ is unramified over $K(\sqrt{d})$ outside $\widetilde{S}_E \cup \{\mathfrak{l}\}$, and $\overline{M}_1(\phi)$ is unramifed over K' outside S_E and little ramified at divisors of $\mathfrak{l}$. Moreover, we have proved that

$$\#\,\mathrm{Sel}_\ell(E^d, K) \Big| \, \mathrm{cl}_{\widetilde{S}_E, u}(K(\sqrt{d}))[\ell] \cdot \mathrm{cl}_{S_E}(K')[\ell](\chi_\ell),$$

which completes the proof of Theorem 4.2.2.

Proof of Corollary 4.2.6

Since we have established our double divisibility statement (4.2.2), we can proceed with a proof of Corollary 4.2.6. By the definitions established in Section 4.1, we have that

$$\mathrm{cl}_{\widetilde{S}_E, u}(K(\sqrt{d}))[\ell] \cdot \mathrm{cl}_{S_E}(K')[\ell](\chi_\ell) \Big| \, \mathrm{cl}_{\emptyset, u}(K(\sqrt{d}))[\ell] \cdot \mathrm{cl}_{\emptyset}(K')[\ell](\chi_\ell) \cdot \varepsilon_S$$

where ε_S is a number depending only on $\widetilde{S}_E$. Note that when $\widetilde{S}_E = \emptyset$, we have that $\varepsilon_S = 1$ and that $\mathrm{cl}_{\emptyset,u}(K(\sqrt{d}))[\ell] = \mathrm{cl}(K(\sqrt{d}))[\ell]$ by Remark 4.1.4. Corollary 4.2.6 follows immediately from the following lemma.

Lemma 4.4.12. $\mathrm{cl}_\emptyset(K')[\ell](\chi_\ell) \mid \mathrm{cl}(K(\sqrt{d}))[\ell]$.

Proof. Let M/K be a Galois extension containing K' with $\langle\alpha\rangle = \mathrm{Gal}(M/K)$, with the relations

$$\alpha^\ell = \mathrm{id} \quad \text{and} \quad \overline{\gamma}\alpha\overline{\gamma}^{-1} = \alpha^{\chi_\ell(\overline{\gamma})} \text{ where } \langle\overline{\gamma}\rangle = \mathrm{Gal}(K'/K).$$

We assume that M is unramified outside $\mathfrak{l}$ and little ramified at $\mathfrak{l}$; hence

$$M(\zeta_\ell) = K'(\sqrt{d})(\sqrt[\ell]{c}),$$

with $c \in M(\sqrt{d})$ and the principal divisor of c is a ℓ^{th} power. We want to extend c to an element of order ℓ in the divisor class group of $K(\sqrt{d})$.

Let $\widetilde{\gamma}$ be an extension of $\overline{\gamma}$ to $\mathrm{Gal}(M(\sqrt{d})/K)$ such that $\widetilde{\gamma}^{\ell-1} = \mathrm{id}$, $\widetilde{\gamma}|K(\zeta_\ell)$ generates $\mathrm{Gal}(K(\zeta_\ell)/K)$, and $\widetilde{\gamma}|K(\sqrt{d}) = \mathrm{id}$. Since $M(\sqrt{d})/K$ is normal, we have $\widetilde{\gamma}(c) = c^i \cdot e^\ell$ with $1 \le i \le \ell - 1$ and $e \in K'(\sqrt{d})$. Hence,

$$\widetilde{\gamma}(\sqrt[\ell]{c}) = (\sqrt[\ell]{c})^i \cdot e \cdot \xi_{\widetilde{\gamma}}$$

with $\xi_{\widetilde{\gamma}}^\ell = 1$. Let $\widetilde{\alpha}$ be an extension of α to $M(\sqrt{d})$ of order ℓ. We can see that $i = 1$ since

$$\widetilde{\gamma}\widetilde{\alpha}(\sqrt[\ell]{c}) = \xi_{\widetilde{\alpha}}^{\chi_\ell(\overline{\gamma})}\widetilde{\gamma}(\sqrt[\ell]{c})$$

and

$$\widetilde{\alpha}^{\chi_\ell(\gamma)}\widetilde{\gamma}(\sqrt[\ell]{c}) = \widetilde{\alpha}^{\chi_\ell(\gamma)}(\xi_{\widetilde{\gamma}}(\sqrt[\ell]{c})^i \cdot e) = \xi_{\widetilde{\alpha}}^{i\cdot\chi_\ell(\overline{\gamma})} \cdot \widetilde{\gamma}(\sqrt[\ell]{c}),$$

and hence

$$M(\sqrt{d}) = K(\sqrt{d}, \sqrt[\ell]{c}, \zeta_\ell).$$

There exists an element $\widetilde{c} = c^{\ell-1} \cdot e'^{\ell} \in M(\sqrt{d})$ with $e' \in K'(\sqrt{d})$ such that the divisor of $\widetilde{c}$ is a ℓ^{th} power. However, since $\pm\widetilde{c}$ is not an ℓ^{th} power in $K(\sqrt{d})$, it is an element of order ℓ in the divisor class group of $K(\sqrt{d})$. □

4.5 Elliptic curves satisfying Corollary 4.2.5

Let E be an elliptic curve over a number field K. In a recent work [Zyw15], Zywina has described all known, and conjecturally all, pairs $(E/\mathbf{Q}, \ell)$ such that mod ℓ image of Galois, $\rho_{E,\ell}(G_{\mathbf{Q}})$, is non-surjective. Using Zywina's classification, we can find elliptic curves $E/\mathbf{Q}$ that will satisfy the conditions of Corollary 4.2.5. First, we present an example of this technique for the case when $\ell = 3$. We remark that this case does not apply to Corollary 4.2.5; however, it best illustrates the technique.

Let $E/\mathbf{Q}$ be a non-CM elliptic curve over $\mathbf{Q}$ such that $\rho_{E,3}(G_{\mathbf{Q}})$ conjugate to

$$B(3) := \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \subset GL_2(\mathbf{F}_3).$$

We can use Galois theory to prove the following result:

Proposition 4.5.1. *Let $E/\mathbf{Q}$ have mod 3 image of Galois conjugate to $B(3)$. Then $\mathbf{Q}(E[3]) = \mathbf{Q}(x(E[3])) \cdot K$ where K is an explicitly computable quadratic extension.*

Before we prove Proposition 4.5.1, we prove the following lemma which tells us over which extension E obtains a 3-torsion point.

Lemma 4.5.2. *For $E/\mathbf{Q}$ from Proposition 4.5.1, there exists some quadratic extension K such that E has a K-rational 3-torsion point. In particular, $E(K)[3] = \langle P \rangle$.*

Proof. Let $E\colon y^2 = x^3 - Ax - B$ for $A, B \in \mathbf{Q}$. Via the Weil-pairing, we know that $\mathbf{Q}(\zeta_3) \subseteq \mathbf{Q}(E[3])$. It is also a well known fact that $B(3) \cong S_3 \times \mathbf{Z}/2\mathbf{Z}$.

Combining these results with our assumptions, we have the following diagram of Galois sub-fields of $\mathbf{Q}(E[3])$: where the extension $\mathbf{Q}(x(E[3]))$ is the index 2 sub-field of $\mathbf{Q}(E[3])$ generated by the x-coordinates of points in $E(\overline{\mathbf{Q}})[3]$. Recall that the roots of the 3-division polynomial

$$\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

correspond to x-coordinates of $E(\overline{\mathbf{Q}})[3]$. In particular, $\psi_3(x)$ is the minimal polynomial of the degree 6, Galois extension $\mathbf{Q}(x(E[3]))$.

Since S_4 does not contain any transitive subgroups of order 6, we know that $\psi_3(x)$ must have a linear factor, so we write $\psi_3(x) = (x-\alpha)g(x)$ where $\alpha \in \mathbf{Q}$ and $g(x)$ is an irreducible cubic. This implies that there exists some $P \in E(\overline{\mathbf{Q}})[3]$ with $\mathbf{Q}$-rational x-coordinate given by α. Moreover, we see that there is a 3-torsion point

$$P = (\alpha, \sqrt{f(\alpha)}).$$

that is defined over the quadratic extension $\mathbf{Q}(\sqrt{f(\alpha)})$. □

Remark 4.5.3. From the above proof, one can easily see that $\mathrm{Gal}(\mathbf{Q}(x(E[3]))/\mathbf{Q}) \cong S_3$. Indeed, since $\mathbf{Q}(x(E[3]))$ is Galois, we showed that the Galois group of $\psi_3(x)$ is actually the Galois group of the cubic $g(x)$. Since $[\mathbf{Q}(x(E[3])) : \mathbf{Q}] = 6$, we know $g(x)$ must be an irreducible cubic with non-square discriminant, which immediately implies our claim.

Proof of Proposition 4.5.1. Let K denote the quadratic extension from Lemma 4.5.2. It is clear that $K \subset \mathbf{Q}(E[3])$ and that $K \nsubseteq \mathbf{Q}(x(E[3]))$, so we have $\mathbf{Q}(E(3))$ is the compositum of $\mathbf{Q}(x(E[3]))$ and K. □

The idea behind finding elliptic curves over $\mathbf{Q}$ such that $E(\mathbf{Q})[\ell] = \{\mathcal{O}\}$ and $E(K)[\ell] = \langle P \rangle$ is to consider $E/\mathbf{Q}$ with $\rho_{E,\ell}(G_{\mathbf{Q}})$ conjugate to a subgroup H such that

$$\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \subsetneq H \subseteq \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) =: B(\ell).$$

We can see that E will attain an ℓ torsion point over an extension K where the degree of $K/\mathbf{Q}$ is determined the cardinality of the upper left entry. For $\ell = 3$, we saw that $H = B(3)$ and thus the upper left entry has order 2, which gives a less explicit proof of Proposition 4.5.1.

Let $\ell \in \{5, 13\}$. Below, we provide examples of elliptic curves $E/\mathbf{Q}$ that do not have a $\mathbf{Q}$-rational point of order ℓ but attain a K-rational point P of order ℓ over some extension of small degree K that satisfies the conditions of Corollary 4.2.5. The final step in our verification is showing P is not contained in the kernel of reduction modulo $\mathfrak{l}$; in particular, this means that E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$. This condition is computable via the MAGMA command `IsSupersingular`.

In order to conduct a thorough search, we consider all subgroups H which can occur as an image of Galois for a non-CM $E/\mathbf{Q}$ and satisfy the above containment. In particular, we run through a large list elliptic curves $E/\mathbf{Q}$ with prescribed non-surjective mod ℓ image of Galois coming from the modular curves X_H of Zywina [Zyw15]. Since this list is comprehensive, we also give examples of elliptic curves over $\mathbf{Q}$ that do not satisfy and potentially satisfy Corollary 4.2.5, modulo some computations.

For $\ell = 5$, we only have one example.

Example 4.5.3.1 ($\ell = 5$). Let $E/\mathbf{Q}$ be the elliptic curve

$$E\colon y^2 = f(x) = x^3 - \frac{185193}{185193}x + \frac{185193}{149}.$$

E has mod 5 image of Galois conjugate to $B(5) \subset \mathrm{GL}_2(\mathbf{F}_5)$, and hence E attains a K-rational point of order 5 over a bi-quadratic extension K of $\mathbf{Q}$. The first quadratic extension $L/\mathbf{Q}$ is given by adjoining the quadratic root α of the 5-division polynomial ψ_5, and then the second quadratic is given by adjoining the square root of the $f(\alpha)$. For E defined above, we compute that $\mathrm{cl}(K) = 8$, $\zeta_5 \notin K$, 2 is ramified in $\mathcal{O}_K$, and that E/K is not supersingular

modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|5$. Therefore, the elliptic curve E and the number field K satisfy the conditions of Corollary 4.2.5.

For $\ell = 7$, we have two possibilities.

Potential example 4.5.3.2 ($\ell = 7$). Let $E/\mathbf{Q}$ be the elliptic curve

$$E\colon y^2 = f(x) = x^3 - \frac{81469949623875}{3017401762489}x + \frac{162939899247750}{3017401762489},$$

which has mod 7 image conjugate to $B(7)$. E attains a K-rational point of order 7 over an extension K of degree 6. The extension K is given by first adjoining the root α of the cubic factor of ψ_7 and then adjoining the square root of $f(\alpha)$. We verify almost all of the conditions from Corollary 4.2.5 for E and K; however, we are not able to verify that $7 \nmid \mathrm{cl}(K)$.

Non-example 4.5.3.3 ($\ell = 7$). Suppose that $E/\mathbf{Q}$ has $\rho_{E,7}(G_{\mathbf{Q}})$ conjugate to

$$H := \begin{pmatrix} a^2 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_7.$$

Since $\#(\mathbf{F}_7^{\times})^2 = 3$, we have that E attains a K-rational point of order 7 over a cubic extension K. Moreover, this extension is given adjoining the root of the cubic factor of the 7-division polynomial ψ_7. In our search, we find that all E/K are supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|7$.

For $\ell = 11$, there do not exist any subgroups coming from [Zyw15] that have our desired condition. For $\ell = 13$, we find a few examples of curves satisfying Corollary 4.2.5.

Example 4.5.3.4 ($\ell = 13$). Suppose that $E/\mathbf{Q}$ has $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to

$$H = \begin{pmatrix} a^3 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_{13},$$

then E attains a K-rational point of order 13 over a bi-quadratic extension

$K/\mathbf{Q}$ since $\#(\mathbf{F}_{13}^{\times})^3 = 4$. As an example, consider the elliptic curve

$$E\colon y^2 = x^3 - \frac{2248091}{180353}x + \frac{4496182}{180353},$$

which has mod 13 image conjugate to H. E attains a K-rational point of order 13 over a bi-quadratic extension K of $\mathbf{Q}$. The first quadratic extension $L/\mathbf{Q}$ is given by adjoining a quadratic root α of the 13-division polynomial ψ_{13}, and then the second quadratic is given by adjoining the square root of the $f(\alpha)$. We compute that $\mathrm{cl}(K) = 2$, $\zeta_{13} \notin K$, (2) splits in $\mathcal{O}_K$, and E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|13$. Therefore, the elliptic curve E and the number field K satisfy the conditions of Corollary 4.2.5.

Example 4.5.3.5 ($\ell = 13$). Suppose that $E/\mathbf{Q}$ has $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to

$$H := \left(\begin{smallmatrix} a^4 & * \\ 0 & * \end{smallmatrix}\right) \quad \text{where } a \in \mathbf{F}_{13}.$$

Since $\#(\mathbf{F}_{13}^{\times})^4 = 3$, E attains a K-rational point of order 13 over cubic extension $K/\mathbf{Q}$. For example, consider the elliptic curve

$$E\colon y^2 = x^3 + 13674069x + 324405221670.$$

Using [Zyw15], E has mod 13 image conjugate to H. Now let $K/\mathbf{Q}$ denote the number field defined by the cubic factor of ψ_{13}. For notational purposes, we shall write $K = \mathbf{Q}(\alpha)$ where α is the primitive element of K. By base changing to K, we find that $E_K = E \times_{\mathbf{Q}} K$ has K-rational 13-torsion point. We also compute that $\mathrm{cl}(F) = 1$, 2 splits in $\mathcal{O}_K$, $\zeta_{13} \notin K$, and that E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|13$. Therefore, the elliptic curve E and the number field K satisfy the conditions of Corollary 4.2.5.

Example 4.5.3.6 ($\ell = 13$). Suppose that elliptic curve with $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to

$$\left(\begin{smallmatrix} a^2 & * \\ 0 & * \end{smallmatrix}\right) \quad \text{where } a \in \mathbf{F}_{13}.$$

Since $\#(\mathbf{F}_{13}^{\times})^2 = 6$, E will attain a K-rational point of order 13 over an extension of degree 6. As an example, consider the elliptic curve

$$E\colon y^2 = x^3 - \frac{12096}{529}x + \frac{24192}{529},$$

which satisfies the above property. E attains a K-rational point of order 13 over a sextic extension K of $\mathbf{Q}$. The first cubic extension $L/\mathbf{Q}$ is given by adjoining a cubic root α of the 13-division polynomial ψ_{13}, and then the second quadratic is given by adjoining the square root of the $f(\alpha)$. We also compute that $\mathrm{cl}(F) = 4$, 2 splits in $\mathcal{O}_K$, $\zeta_{13} \notin K$, and that E/K is not supersingular modulo $\mathfrak{l}$ if $\mathrm{ord}_{\mathfrak{l}}(j_E) \geq 0$ where $\mathfrak{l}|13$. Therefore, the elliptic curve E and number field K satisfy the conditions of Corollary 4.2.5.

Potential example 4.5.3.7 ($\ell = 13$). Suppose that elliptic curve $E/\mathbf{Q}$ with mod 13 image conjugate to $B(13)$ will attain a K-rational point of order 13 over an extension of degree 12. The difficultly in verifying the conditions of Corollary 4.2.5 is computing the class number and ramification indicies for the duodecic extension K.

Finally for $\ell = 37$, there is only one $E/\overline{\mathbf{Q}}$ that we need to consider.

Potential example 4.5.3.8 ($\ell = 37$). Suppose that $E/\mathbf{Q}$ is the elliptic curve with j-invariant $-7 \cdot 11^3$, which has affine equation

$$E\colon y^2 = x^3 - \frac{251559}{11045}x + \frac{503118}{11045}.$$

From [Zyw15, Theorem 1.10.(ii)], we know that the mod 37 image of E is conjugate to

$$H := \begin{pmatrix} a^3 & * \\ 0 & * \end{pmatrix} \quad \text{where } a \in \mathbf{F}_{37}.$$

Since $\#(\mathbf{F}_{37}^{\times})^3 = 12$, E attains a K-rational point of order 37 over a duodecic extension $K/\mathbf{Q}$. As before, the difficultly in verifying the conditions of Corollary 4.2.5 is computing the class number and ramification indicies for

the duodecic extension K.

Chapter 5

Composite level images of Galois

5.1 Background

Let ℓ be an exceptional prime. In [Zyw15], Zywina studies the mod ℓ images of Galois by constructing modular curves of prime level and computing their $\mathbf{Q}$-rational points. Zywina first determines which proper subgroups of $\mathrm{GL}_2(\mathbf{F}_\ell)$ can occur as the mod ℓ image of Galois. For a subgroup $G \subset \mathrm{GL}_2(\mathbf{F}_\ell)$ with $\det(G) = \mathbf{F}_\ell^\times$ and $-I \in G$, we can associate a modular curve X_G, which is a smooth, projective, and geometrically irreducible curve over $\mathbf{Q}$. It comes with a natural morphism

$$\pi_G \colon X_G \longrightarrow \operatorname{Spec} \mathbf{Q}[j] \cup \{\infty\} =: \mathbf{P}^1_{\mathbf{Q}},$$

such that for an elliptic curve $E/\mathbf{Q}$ with $j_E \notin \{0, 1728\}$, the group $\rho_{E,\ell}(G_{\mathbf{Q}})$ is conjugate to a subgroup of G if and only if the $j_E = \pi_G(P)$ for some rational point $P \in X_G(\mathbf{Q})$. The modular curves X_G of genus 0 with $X_G(\mathbf{Q}) \neq \emptyset$ are isomorphic to the projective line, and their function field is of form $\mathbf{Q}(h)$ for some modular function h of level ℓ. Giving the morphism π_G is then equivalent to expressing the modular j-invariant in the form $J(h)$ for a unique

rational function $J(t) \in \mathbf{Q}(t)$. We now describe the complete set of necessary conditions on the possible non-surjective images of $\rho_{E,n}(G_{\mathbf{Q}})$, where $n > 1$ is some positive integer.

Definition 5.1.1. A subgroup G of $GL_2(\mathbf{Z}/n\mathbf{Z})$ is applicable if it satisfies the following conditions:

- $G \neq GL_2(\mathbf{Z}/n\mathbf{Z})$,
- $-I \in G$ and $\det(G) = (\mathbf{Z}/n\mathbf{Z})^{\times}$,
- G contains an element with trace 0 and determinant -1 that fixes a point in $(\mathbf{Z}/n\mathbf{Z})^2$ of order n.

Proposition 5.1.2 (Proposition 2.2 [Zyw15])**.** *Let E be an elliptic curve over $\mathbf{Q}$ for which $\rho_{E,n}$ is not surjective. Then $\pm\rho_{E,n}(G_{\mathbf{Q}})$ is an applicable subgroup of $GL_2(\mathbf{Z}/n\mathbf{Z})$.*

Proposition 5.1.2 gives necessary conditions for when a proper subgroup of $GL_2(\mathbf{Z}/n\mathbf{Z})$ can occur as the image of Galois, and hence reduces a part of the problem to a group theoretic computation. From here, Zywina constructs the modular curves corresponding to these subgroups and classifies the rational points on them. This result gives a conjecturally complete description of the "horizontal" flavored question concerning the mod ℓ representations.

In [RZB14], Rouse and Zureick-Brown consider the "vertical" flavored question through their study of the 2-adic images. The authors determine the possible 2-adic images of Galois by finding all the rational points on the "tower" of 2-power level modular curves. For a subgroup H of $GL_2(\widehat{\mathbf{Z}})$ and an integer n such that H contains the kernel of the reduction map $GL_2(\widehat{\mathbf{Z}}) \to GL_2(\mathbf{Z}/n\mathbf{Z})$, the authors define X_H to be the quotient of the modular curve $X(n)$ by the image $H(n)$ of H in $GL_2(\mathbf{Z}/n\mathbf{Z})$. This quotient roughly classifies elliptic curves whose adélic image of Galois is contained in H. Furthermore,

the authors describe a necessary condition on the p-adic image, where p is any prime.

Definition 5.1.3. A subgroup $H \subset \mathrm{GL}_2(\mathbf{Z}_p)$ is arithmetically maximal if

- $\det\colon H \to \mathbf{Z}_p^\times$ is surjective,
- there is an $M \in H$ with determinant -1 and trace zero, and
- there is no subgroup K with $H \subseteq K$ so that X_K has genus ≥ 2.

Rouse and Zureick-Brown give an equivalent statement to that in Proposition 5.1.2. In particular if $E/\mathbf{Q}$ is an elliptic curve and $H = \rho_{E,2^\infty}(G_{\mathbf{Q}})$, then H is arithmetically maximal. The authors determine that there exist 727 arithmetically maximal subgroups of $\mathrm{GL}_2(\mathbf{Z}_2)$ and give a beautifully detailed diagram of these subgroups (see [RZB14, Figure 1]). We shall let H_n denote the n^{th} subgroup in their list (as given in [RZB, `gl2data.txt`]).

Below, we reproduce the list of applicable subgroups from [Zyw15] and give the rational function expressing the modular j-invariant for certain exceptional primes ℓ. In Appendix A.3, we present these subgroups as lattices in $\mathrm{GL}_2(\mathbf{F}_\ell)$.

Notation

We set some notation for specific subgroups of $\mathrm{GL}_2(\mathbf{F}_\ell)$. Let $C_{\mathrm{sp}}(\ell)$ be the subgroup of diagonal matrices. Let $\epsilon = -1$ if $\ell \equiv 3 \pmod 4$ and otherwise let $\epsilon \geq 2$ be the smallest integer which is not a quadratic residue modulo ℓ. Let $C_{\mathrm{nsp}}(\ell)$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a & b\epsilon \\ b & a \end{smallmatrix}\right)$ with $(a, b) \in \mathbf{F}_\ell^2 \setminus \{(0,0)\}$. Let $N_{\mathrm{sp}}(\ell)$ and $N_{\mathrm{nsp}}(\ell)$ be the normalizers of $C_{\mathrm{sp}}(\ell)$ and $C_{\mathrm{nsp}}(\ell)$, respectively, in $\mathrm{GL}_2(\mathbf{F}_\ell)$. We have $[N_{\mathrm{sp}}(\ell) : C_{\mathrm{sp}}(\ell)] = 2$ and the non-identity coset of $C_{\mathrm{sp}}(\ell)$ in $N_{\mathrm{sp}}(\ell)$ is represented by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. We have $[N_{\mathrm{nsp}}(\ell) : C_{\mathrm{nsp}}(\ell)] = 2$ and the non-identity coset of $C_{\mathrm{nsp}}(\ell)$ in $N_{\mathrm{nsp}}(\ell)$ is represented by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Let $B(\ell)$ be the subgroup of upper triangular matrices

in $\mathrm{GL}_2(\mathbf{F}_\ell)$.

5.1.4 $\underline{\text{List}}(\ell = 2)$

Up to conjugacy there are three proper subgroups of $\mathrm{GL}_2(\mathbf{F}_2)$, all of which are arithmetically maximal:

$$G_1 = \{I\}, \qquad G_2 = \{I, \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\}, \qquad G_3 = \{I, \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)\}.$$

From [Zyw15, Theorem 1.1], $\rho_{E,2}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{F}_2)$ to a subgroup of G_i if and only if j_E is of the form:

$$J_1(t) = 256\frac{(t^2+t+1)^3}{t^2(t+1)}, \qquad J_2(t) = 256\frac{(t+1)^3}{t}, \qquad J_3(t) = t^2 + 1728$$

for some $t \in \mathbf{Q}$ and each respective i.

5.1.5 $\underline{\text{List}}(\ell = 3)$

Define the following subgroups of $\mathrm{GL}_2(\mathbf{F}_3)$:

- let G_1 be the group $C_{sp}(3)$,
- let G_2 be the group $N_{sp}(3)$,
- let G_3 be the group $B(3)$,
- let G_4 be the group $N_{nsp}(3)$,
- let $H_{1,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}1&0\\0&*\end{smallmatrix}\right)$,
- let $H_{3,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}1&*\\0&*\end{smallmatrix}\right)$,
- let $H_{3,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}*&*\\0&1\end{smallmatrix}\right)$.

Each of the groups G_i contain $-I$, and the groups $H_{i,j}$ do not contain $-I$. Moreover, we have $G_i = \pm H_{i,j}$. From [Zyw15, Theorem 1.2(ii)], $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{F}_3)$ to a subgroup of G_i if and only if j_E is of the form:

$$J_1(t) = 27\frac{(t+1)^3(t+3)^3(t^2+3)^3}{t^3(t^2+3t+3)^3}, \qquad J_2(t) = 27\frac{(t+1)^3(t-3)^3}{t^3},$$
$$J_3(t) = 27\frac{(t+1)(t+9)^3}{t^3}, \qquad J_4(t) = t^3$$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zyw15, Theorem 1.2(iii,iv)] provides explicit conditions (isomorphisms) when $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate to $H_{i,j}$ for $i = 1, 3$ and $j = 1, 2$.

5.1.6 List($\ell = 5$)

Define the following subgroups of $\mathrm{GL}_2(\mathbf{F}_5)$:

- let G_1 be the subgroup consisting of the matrices of the form $\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$,
- let G_2 be the group $C_{\mathrm{sp}}(5)$,
- let G_3 be the unique subgroup of $N_{\mathrm{nsp}}(5)$ of index 3; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 0 & 1 \\ 3 & 0 \end{smallmatrix}\right)$,
- let G_4 be the group $N_{\mathrm{sp}}(5)$,
- let G_5 be the subgroup consisting of the matrices of the form $\pm \left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$,
- let G_6 be the subgroup consisting of the matrices of the form $\pm \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$,
- let G_7 be the group $N_{\mathrm{nsp}}(5)$,
- let G_8 be the group $B(5)$,
- let G_9 be the unique maximal subgroup of $\mathrm{GL}_2(\mathbf{F}_5)$ which contains $N_{\mathrm{sp}}(5)$; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$,

- let $H_{1,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}1 & 0\\ 0 & *\end{smallmatrix}\right)$,
- let $H_{1,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}a^2 & 0\\ 0 & a\end{smallmatrix}\right)$,
- let $H_{5,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}* & *\\ 0 & 1\end{smallmatrix}\right)$,
- let $H_{5,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}a & *\\ 0 & a^2\end{smallmatrix}\right)$,
- let$H_{6,1}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}1 & *\\ 0 & *\end{smallmatrix}\right)$,
- let $H_{6,2}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}a^2 & *\\ 0 & a\end{smallmatrix}\right)$.

Each of the groups G_i contain $-I$, and the groups $H_{i,j}$ do not contain $-I$. Moreover, we have $G_i = \pm H_{i,j}$. From [Zyw15, Theorem 1.4(ii)], $\rho_{E,5}(G_{\mathbf{Q}})$ is conjugate in $GL_2(\mathbf{F}_5)$ to a subgroup of G_i if and only if j_E is of the form:

$$
\begin{aligned}
J_1(t) &= \frac{(t^{20}+228t^{15}+494t^{10}-228t^5+1)^3}{t^5(t^{10}-11t^5-1)^5},\\
J_2(t) &= \frac{(t^2+5t+5)^3(t^4+5t^2+25)^3(t^4+5t^3+20t^2+25t+25)^3}{t^5(t^4+5t^3+15t^2+25t+25)^5},\\
J_3(t) &= \frac{5^4t^3(t^2+5t+10)^3(2t^2+5t+5)^3(4t^4+30t^3+95t^2+150t+100)^3}{(t^2+5t+5)^5(t^4+5t^3+15t^2+25t+25)^5},\\
J_4(t) &= \frac{(t+5)^3(t^2-5)^3(t^2+5t+10)^3}{(t^2+5t+10)^3},\\
J_5(t) &= \frac{(t^4+228t^3+494t^2-228t+1)^3}{t(t^2-11t-1)^5},\\
J_6(t) &= \frac{(t^4-12t^3+14t^2+12t+1)^3}{t^5(t^2-11t-1)},\\
J_7(t) &= \frac{5^3(t+1)(2t+1)^3(2t^3-3t+3)^3}{(t^2+t-1)^5},\\
J_8(t) &= \frac{5^2(t^2+10t+5)^3}{t^5},\\
J_9(t) &= t^3(t^2+5t+40)
\end{aligned}
$$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zyw15, Theorem 1.4(iii)] provides explicit conditions when $\rho_{E,5}(G_{\mathbf{Q}})$ is conjugate to $H_{i,j}$ for $i = 1, 5, 6$ and $j = 1, 2$.

5.1.7 List($\ell = 7$)

Define the following subgroups of $\mathrm{GL}_2(\mathbf{F}_7)$:

- let G_1 be the subgroup of $N_{sp}(7)$ consisting of elements of $C_{sp}(7)$ with square determinant and elements of $N_{sp}(7) \setminus C_{sp}(7)$ with non-square determinant; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 9 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$,
- let G_2 be the group $N_{sp}(7)$,
- let G_3 be the subgroup consisting of matrices of the form $\pm\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$,
- let G_4 be the subgroup consisting of matrices of the form $\pm\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$,
- let G_5 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a & * \\ 0 & \pm a \end{smallmatrix}\right)$,
- let G_6 be the group $N_{nsp}(7)$,
- let G_7 be the group $B(7)$,
- let $H_{1,1}$ be the subgroup generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$,
- let $H_{3,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $H_{3,2}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} \pm 1 & * \\ 0 & a^2 \end{smallmatrix}\right)$,
- let $H_{4,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$,
- let $H_{4,2}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & \pm 1 \end{smallmatrix}\right)$,
- let $H_{5,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} \pm a^2 & * \\ 0 & a^2 \end{smallmatrix}\right)$,

- let $H_{5,2}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & \pm a^2 \end{smallmatrix}\right)$,
- let $H_{7,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & a^2 \end{smallmatrix}\right)$,
- let $H_{7,2}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & * \end{smallmatrix}\right)$.

Each of the groups G_i contain $-I$, and the groups $H_{i,j}$ do not contain $-I$. Moreover, we have $G_i = \pm H_{i,j}$. From [Zyw15, Theorem 1.5(ii)], $\rho_{E,7}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{F}_7)$ to a subgroup of G_i if and only if j_E is of the form:

$$
\begin{aligned}
J_1(t) &= 3^3 \cdot 5 \cdot 7^5/2^7, \\
J_2(t) &= \frac{t(t+1)^3(t^2-5t-1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7}, \\
J_3(t) &= \frac{(t^2-t+1)^3(t^6-11t^5+30t^4-15t^3-10t^2+t+1)^3}{(t-1)^7t^7(t^3-8t^2+5t+1)}, \\
J_4(t) &= \frac{(t^2-t+1)^3(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)^3}{(t-1)t(t^3-8t^2+5t+1)^7}, \\
J_5(t) &= -\frac{(t^2-3t-3)^3(t^2-t+1)^3(3t^2-9t+5)^3(5t^2-t-1)^3}{(t^3-2t^2-t+1)(t^3-t^2-2t+1)^7}, \\
J_6(t) &= \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14y-7)^3}{(t^3-7t^2+7t+7)^7}, \\
J_7(t) &= \frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7}
\end{aligned}
$$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zyw15, Theorem 1.5(iii,iv)] provides us with explicit conditions when $\rho_{E,7}(G_{\mathbf{Q}})$ is conjugate to $H_{i,j}$ for $i = 1, 3, 4, 5, 7$ and $j = 1, 2$.

5.1.8 List($\ell = 11$)

Define the following subgroups of $\mathrm{GL}_2(\mathbf{F}_{11})$:

- let G_1 be the subgroup generated by $\pm\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 6 \end{smallmatrix}\right)$,

- let G_2 be the subgroup generated by $\pm\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right)$,
- let G_3 be the group $N_{\mathrm{nsp}}(11)$,
- let $H_{1,1}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right)$,
- let $H_{1,2}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}7&0\\0&5\end{smallmatrix}\right)$,
- let $H_{2,1}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right)$,
- let $H_{2,2}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}6&0\\0&4\end{smallmatrix}\right)$.

Each of the groups G_i contain $-I$, and the groups $H_{i,j}$ do not contain $-I$. Moreover, we have $G_i = \pm H_{i,j}$. From [Zyw15, Theorem 1.6(ii,iii)], there are unique values for j_E that correspond to $\pm\rho_{E,11}(G_{\mathbf{Q}})$ being conjugate in $\mathrm{GL}_2(\mathbf{F}_{11})$ to a subgroup of G_1 and G_2.

The modular curve $X_{G_3}(11) = X^+_{\mathrm{nsp}}(11)$ is the only one from Zywina's classification that has genus 1 with infinitely many rational points. To explicitly describe this modular curve, let $\mathcal{E}$ be the elliptic curve over $\mathbf{Q}$ defined by the Weierstrass equation $y^2 + y = x^3 - x^2 - 7x + 10$ and let $\mathcal{O}$ be the point at infinity. The Mordell-Weil group $\mathcal{E}(\mathbf{Q})$ is an infinite cyclic group generated by the point $(4, 5)$. Halberstadt [Hal98] showed that $X^+_{\mathrm{nsp}}(11)$ is isomorphic to $\mathcal{E}$ and that the morphism to the j-line corresponds to

$$J(x, y) := \frac{(f_1 f_2 f_3 f_4)^3}{f_5^2 f_6^{11}},$$

where

$$f_1 = x^2 + 3x - 6, \qquad f_2 = 11(x^2 - 5y) + (2x^4 + 23x^3 - 72x^2 - 28x + 127),$$
$$f_3 = 6y + 11x - 19, \qquad f_4 = 22(x - 2)y + (5x^3 + 17x^2 - 112x - 120),$$
$$f_5 = 11y + (2x^2 + 17x - 34), \qquad f_6 = (x - 4)y - (5x - 9).$$

From [Zyw15, Theorem 1.6(iv)], $\rho_{E,11}(G_{\mathbf{Q}})$ is conjugate to G_3 if and only if $j_E = J(P)$ for some point $P \in \mathcal{E}(\mathbf{Q}) \setminus \{\mathcal{O}\}$.

Remark 5.1.9. In [Zyw15, Section 4.5.5], Zywina gives explicit polynomials $A, B, C \in \mathbf{Q}[x]$ of degree 55 such that for a non-CM elliptic curve $E/\mathbf{Q}$, we have $j_E = J(P)$ for some $P \in \mathcal{E}(\mathbf{Q}) \setminus \{\mathcal{O}\}$ if and only if the polynomial $A(x)j_E^2 + B(x)j_E + C(x) \in \mathbf{Q}[x]$ has a rational root. Hence given a numerical j_E, this gives a straightforward way to check the criterion that $\rho_{E,11}(G_{\mathbf{Q}})$ is conjugate to a subgroup of G_3.

5.1.10 List($\ell = 13$)

Define the following subgroups of $\mathrm{GL}_2(\mathbf{F}_{13})$:

- let G_1 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & b^3 \end{smallmatrix}\right)$,
- let G_2 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^3 & * \\ 0 & * \end{smallmatrix}\right)$,
- let G_3 be the subgroup consisting of matrices $\left(\begin{smallmatrix} a & * \\ 0 & b \end{smallmatrix}\right)$ for which $(a/b)^4 = 1$,
- let G_4 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & b^2 \end{smallmatrix}\right)$,
- let G_5 be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & * \end{smallmatrix}\right)$,
- let G_6 be the group $B(13)$,
- let G_7 be the subgroup generated by the matrices $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$; it contains the scalar matrices and its image in $\mathrm{PGL}_2(\mathbf{F}_{13})$ is isomorphic to $\mathfrak{S}_4$,
- let $H_{4,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & a^4 \end{smallmatrix}\right)$,
- let $H_{4,2}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} b^2 & * \\ 0 & a^4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$,

- let $H_{5,1}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^4 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $H_{5,2}$be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^4 & * \\ 0 & b^2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 2 \end{smallmatrix}\right)$.

Each of the groups G_i contain $-I$, and the groups $H_{i,j}$ do not contain $-I$. Moreover, we have $G_i = \pm H_{i,j}$. Define the polynomials

$$P_1(t) = \begin{array}{c} t^{12} + 231t^{11} + 269t^{10} - 3160t^9 + 6022t^8 - 9616t^7 + 21880t^6 \\ -34102t^5 + 28297t^4 - 12455t^3 + 2876t^2 - 243t + 1 \end{array},$$

$$P_2(t) = t^{12} - 9t^{11} + 29t^{10} - 40t^9 + 22t^8 - 16t^7 + 40t^6 - 22t^5 - 23t^4 + 25t^3 - 4t^2 - 3t + 1,$$

$$P_3(t) = (t^4 - t^3 + 2t^2 - 9t + 3)(3t^4 - 3t^3 - 7t^2 + 12t - 4)(4t^4 - 4t^3 - 5t^2 + 3t - 1),$$

$$P_4(t) = t^8 + 235t^7 + 1207t^6 + 955t^5 + 3840t^4 - 955t^3 + 1207t^2 - 235t + 1,$$

$$P_5(t) = t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1,$$

$$P_6(t) = t^4 + 7t^3 + 20t^2 + 19t + 1.$$

From [Zyw15, Theorem 1.8(ii)], $\rho_{E,13}(G_{\mathbf{Q}})$ is conjugate in $GL_2(\mathbf{F}_{13})$ to a subgroup of G_i if and only if j_E is of the form:

$$J_1(t) = \frac{(t^2 - t + 1)^3 P_1(t)^3}{(t-1)t(t^3 - 4t^2 + t + 1)^{13}} \qquad J_2(t) = \frac{(t^2 - t + 1)^3 P_2(t)^3}{(t-1)^{13}t^{13}(t^3 - 4t^2 + t + 1)}$$

$$J_3(t) = -\frac{13^4(t^2 - t + 1)^3 P_3(t)^3}{((t^3 - 4t^2 + t + 1)^{13}(5t^3 - 7t^2 - 8t + 5))} \qquad J_4(t) = \frac{(t^4 - t^3 + 5t^2 + t + 1)P_4(t)^3}{t(t^2 - 3t - 1)^{13}}$$

$$J_5(t) = \frac{(t^4 - t^3 + 5t^2 + t + 1)P_5(t)^3}{t^{13}(t^2 - 3t - 1)} \qquad J_6(t) = \frac{(t^2 + 5t + 13)P_6(t)^3}{t}$$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zyw15, Theorem 1.8(iii)] gives explicit conditions on when $\rho_{E,13}(G_{\mathbf{Q}})$ is conjugate to $H_{i,j}$ for $i = 4, 5$ and $j = 1, 2$, and [Zyw15, Theorem 1.8(iv)] gives necessary numerical conditions for when $\rho_{E,13}(G_{\mathbf{Q}})$ is conjugate to G_7. The case $\ell = 13$ is the first case for which Zywina does not give a complete description, which is due to three

outstanding cases (see Section 5.6).

For the remainder of this chapter, we will only consider elliptic curves $E/\mathbf{Q}$. Let $3 \leq \ell 13$ be a prime; let $G \subset GL_2(\mathbf{F}_\ell)$ be a subgroup from [Zyw15]; and let $H \subset GL_2(\mathbf{F}_{2^n})$ be a subgroup from [RZB14]. Using the rational functions corresponding to the j-maps of the modular curves $X_H(2^n)$ and $X_G(\ell)$, we construct the following fibered diagram

$$\begin{array}{ccc} X' & \longrightarrow & X_G(\ell) \\ \downarrow & & \downarrow{\scriptstyle j(G)} \\ X_H(2^n) & \xrightarrow[j(H)]{} & \mathbf{P}^1_{\mathbf{Q}} \end{array}$$

We define composite-$(2^n, \ell)$ level modular curve $X_{H,G}(2^n \cdot \ell)$ to be the normalization of the fibered product X'; the aforementioned j-map equations allow us to easily find equations for these curves. The $\mathbf{Q}$-rational points on $X_{H,G}(2^n \cdot \ell)$ correspond to j-invariants of over $\mathbf{Q}$ with composite-$(2^n, \ell)$ image conjugate to some subgroup of $H \times G \subset GL_2(\mathbf{F}_{2^n}) \times GL_2(\mathbf{F}_\ell) \cong GL_2(\mathbf{Z}/2^n \cdot \ell\mathbf{Z})$ via the Chinese Remainder Theorem. Succinctly, these $\mathbf{Q}$-rational points classify elliptic curves over $\mathbf{Q}$ with simultaneously non-surjective, composite-$(2^n, \ell)$ image of Galois.

5.1.11 Statement of Results

In this paper, we will find equations for composite-$(2^n, \ell)$ level modular curves and determine their rational points for the tuples $(2, \ell)$ where $\ell = 5, 7, 11, 13$ and $(N, 3)$ where $N = 2, 4, 8$.

Theorem 5.1.12. *Let E be a non-CM elliptic curve over $\mathbf{Q}$ such that the discriminant of E is a rational square. Then there:*

1. *is 1 possibility for simultaneously non-surjective, composite-$(2, 5)$ image*

of Galois;

2. *is 1 possibility for simultaneously non-surjective, composite-*$(2, 7)$ *image of Galois;*

3. *is at most 1 possibility for simultaneously non-surjective, composite-*$(2, 11)$ *image of Galois;*

4. *are at most 3 possiblilties for simultaneously non-surjective, composite-*$(2, 13)$ *image of Galois.*

Corollary 5.1.13. *Let* E *be a non-CM elliptic curve over* $\mathbf{Q}$ *such that the discriminant of* E *is a rational square. Then the index of* $(\rho_{\mathsf{E},2} \times \rho_{\mathsf{E},\ell})(\mathsf{G}_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/2 \cdot \ell\mathbf{Z})$ *dividing*

1. *10 for* $\ell = 5$ *occurs infinitely often;*

2. *16 for* $\ell = 7$ *occurs infinitely often;*

3. *110 for* $\ell = 11$ *occurs finitely often;*

4. *156 or 182 for* $\ell = 13$ *occurs finitely often.*

Remark 5.1.14. The assumption on the discriminant of E plays a vital role in the construction of the composite level modular curves (see Section 5.1.17). In particular, this condition allows us to quickly find nice models for these curves.

Theorem 5.1.15. *Let* E *be a non-CM elliptic curve over* $\mathbf{Q}$*. Then there are:*

1. *6 possibilities for simultaneously non-surjective, composite-*$(2, 3)$ *image of Galois;*

2. *5 possibilities for simultaneously non-surjective, composite-*$(4, 3)$ *image of Galois;*

3. *6 possibilities for simultaneously non-surjective, composite-*$(8, 3)$ *image of Galois;*

Corollary 5.1.16. *Let* E *be a non-CM elliptic curve over* $\mathbf{Q}$*. Then the index of* $(\rho_{E,2^n} \times \rho_{E,3})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/2^n \cdot 3\mathbf{Z})$

1. *being either 4, 8, 9, 12, 18, or 36 for the tuple* $(2, 3)$ *occurs infinitely often;*

2. *dividing 18 or 24 for the tuple* $(4, 3)$ *occurs infinitely often;*

3. *dividing 36 the tuple* $(8, 3)$ *occurs infinitely often;*

The idea behind the proofs of Theorem 5.1.12 and Theorem 5.1.15 is to first find models for the composite level modular curves corresponding to the subgroups from [RZB14, Zyw15]. Once we have the models for these modular curves, we determine the rational points on these models. The analysis of rational points on this collection of modular curves involves a variety of techniques, including local methods, Chabauty, étale descent, and the Mordell-Weil sieve, which we discuss in Section 5.3.

In the proof of Theorem 5.1.12, we first consider maximal subgroups. If $H, H' \subseteq \mathrm{GL}_2(\mathbf{F}_\ell)$ from [Zyw15] such that H is maximal and $H' \subset H$, then we have a map between the composite level modular curves $X_{G,H'} \to X_{G,H}$. Hence, the points on $X_{G,H'}$ must map to points on $X_{G,H}$. In particular, if $X_{G,H}(\mathbf{Q})$ is finite, then so is $X_{G,H'}(\mathbf{Q})$. Moreover, if $X_{G,H}(\mathbf{Q})$ only contains CM or cuspidal points, then so will $X_{G,H'}(\mathbf{Q})$, which reduces the number of modular curves we need to analyze; we note when this occurs our Tables below.

5.1.17 Models for Theorem 5.1.12

The discriminant condition in Theorem 5.1.12 allows us to construct models for the composite-$(2,\ell)$ level modular curves as hyperelliptic curves. Indeed, since an elliptic curve $E/\mathbf{Q}$ with such a discriminant has 2-division field $\mathbf{Q}(E[2])$ isomorphic to $\mathbf{Q}(\alpha)$ where α is a root of the defining cubic equation $f(x)$ of E. From[Zyw15, Theorem 1.1], the condition on the discriminant is equivalent to $\rho_{E,2}(G_{\mathbf{Q}})$ being conjugate in $GL_2(\mathbf{F}_2)$ to the index 2 subgroup

$$G_3 := \{I, \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)\}.$$

For subgroups $H \subset GL_2(\mathbf{F}_\ell)$ coming from [Zyw15], the composite-$(2,\ell)$ level modular curve has the form $s^2+1728 = f(t)/g(t)$, where $f, g \in \mathbf{Q}[t]$. Through some simple manipulation, we rewrite our modular curve as

$$X_{G_3,G}(2\cdot\ell)\colon g(t)^2s^2 = h(t)^2w(t)$$

for some $h, w \in \mathbf{Q}[t]$. Then we consider the bi-rational map

$$\begin{aligned}\varphi\colon X_{G_3,G}(2\cdot\ell) &\longrightarrow X\\ (s,t) &\longmapsto (g(t)s/h(t), t).\end{aligned}$$

Hence we have reduced our problem to finding the rational points on the hyperelliptic curve

$$X\colon y^2 = w(t).$$

In the proof of Theorem 5.1.15, we build the "tower" of $(2^n\cdot 3)$-power level modular curves; the idea of this "tower" of $(2^n\cdot 3)$-power level modular curves comes from [RZB14]. First, we compute the rational points on the level 6

modular curves, which acts as the foundation of our tower. If the subgroup $H \times G \subset \mathrm{GL}_2(\mathbf{F}_2) \times \mathrm{GL}_2(\mathbf{F}_3) \cong \mathrm{GL}_2(\mathbf{Z}/6\mathbf{Z})$ occurs as a composite image of Galois, then we find the subgroups of level 4 from [RZB, `gl2data.txt`] that cover H (e.g. that do not contain H in the kernel of reduction). We find such level 4 subgroups for all 6 possible composite-$(2,3)$ images and proceed by computing the rational points on the composite-$(4,3)$ level modular curves. We repeat this procedure for each tier of our tower ending with level 8.

5.1.18 Models for Theorem 5.1.15

For $n = 1$, we find a hyperelliptic model as we did in Section 5.1.17. For $n = 2, 3$, we need different methods to determine the smooth compactification of the modular curves X of genus g. The primary tool to compute these smooth models for X is by taking the image of X under the canonical map. We briefly recall the construction of the canonical map. Choose a basis $\omega_1, \ldots, \omega_g$ of $\Omega^1(X)$. The canonical map φ is the map associated to the linear series of all holomorphic 1-forms ω_i, precisely

$$\begin{aligned} \varphi \colon X &\longrightarrow \mathbf{P}^{g-1} \\ P &\longmapsto (\omega_1(P), \ldots, \omega_g(P)). \end{aligned}$$

For $g = 1$, we cannot utilize the canonical map since the canonical divisor K is trivial, so instead we compute image of the log-canonical map. For any divisor D of the form $K + Q$ where Q is effective, we can construct a map to a (possibly empty) projective space. The log-canonical map generalizes the canonical map (set $Q = 0$), and we define the log-canonical map as we did the canonical map; this definition implicitly uses the adjunction formula which relates smooth divisors to canonical bundles.

For a number of our curves X, we can immediately see that X has a cubic point, equivalently an effective degree 3 divisor D. Once we find this D, we

compute the log-canonical map associated to $K + D$ using some MAGMA's intrinsics and proceed with our usual analysis. We find that the remaining curves have a quartic point, and hence we repeat the above procedure for the corresponding degree 4 divisor. If the genus of X is greater than 2, then MAGMA's instrinsic `IsHyperelliptic(C)` determines if C is hyperelliptic, and if so, it computes a hyperelliptic model H for C and a map from $C \to H$.

5.1.19 Organization

In Section 5.2, we construct our composite level modular curves and give proofs for Theorems 5.1.12 and 5.1.15. We devote a large portion of this chapter to an analysis of the $\mathbf{Q}$-rational points on our modular curves. In Section 5.3, we explain the techniques and theory used to determine these rational points, and the subsequent sections provide further details of this analysis for curves of increasing genera.

5.2 Composite level modular curves

In this section, we present tables containing equations for models, genera, and rational points of the composite level modular curves. We stress that the points in the tables *do not* correspond to points on the given models, but rather on the modular curve $X_{H,G}(N)$ where N is composite. In Section 5.3, we provide a detailed analysis of the rational points on these modular curves.

Tables for Theorem 5.1.12

For simplicity, we shall consider the composite-$(2, \ell)$ level modular curves for $\ell = 5, 7, 11, 13$, separately. We denote the cases when the modular curve $X_{H,G}$ has genus 0 and a rational point by $\mathbf{P}^1_{\mathbf{Q}}$. Furthermore, we provide a

parametrization for these curves in [Mor]. We present these tables in Appendix A.1

Tables for Theorem 5.1.15

The curves found in Table A.5 correspond to the subgroups $H \times G \leq GL_2(\mathbf{Z}/6\mathbf{Z})$ where H comes from List 5.1.4 and G from List 5.1.5. In [Mor], we give tables and diagrams for the composite-$(2^n, 3)$ level modular curves for $n = 1, 2, 3$. In these tables, we provide similar data as above for the modular curves corresponding to subgroups $H_n \times G \leq GL_2(\mathbf{Z}/2^n \cdot 3\mathbf{Z})$ where H_n comes from [RZB, `gl2data.txt`] and G from List 5.1.5 and the rational points on these curves. For $G_{\in}\{G_1, G_2\}$, we find bi-rational maps from the modular curves $X_{H_n,G}$ to the curve X_{H_n,G_4} using similar methods to those in Section 5.1.17. In the case where X_{H_n,G_4} only contains finitely many CM or cuspidal points, it suffices to compute the points on this model, and when this occurs, we simply provide the data for the curve X_{H_n,G_4}; we denote these case in our tables by the tuple $(H_n, \mathfrak{G})$. We present these tables in Appendix A.2.

Equipt with the data from these tables, we prove Theorems 5.1.12 and 5.1.15

Proof of Theorems. The proof of Theorem 5.1.15 follows directly from Table A.5 and the Tables in [Mor, `RZBTables.pdf`]. For Theorem 5.1.12, we need to provide a bit more detail. Parts (1) and (2) follow directly from the Tables A.1, A.2, respectively. Since we are unsuccessful in our attempt to provably find the rational points on the genus 7 non-hyperelliptic modular curve $X_{G_3,G_3}(22)$, there remains at most one possibility of simultaneously non-surjective composite-$(2, 11)$; hence part (3) is clear. As mentioned in List 5.1.10, there are three outstanding cases of the mod 13 image, and these cases correspond to the three cases in part (4). Piecing these results together, we have proved Theorem 5.1.12. □

5.3 Analysis of Rational Points -Theory

The composite level curves whose models we computed have genera either $0, 1, 2, 3, 7$.

For the genus 0 curves, we determine whether the curve has a rational point, and if so we compute an explicit isomorphism with $\mathbf{P}^1_{\mathbf{Q}}$. For the genus 1 curves, we determine whether the curves have a non-singular rational point, and if so compute a model for the resulting elliptic curve and determine its rank and torsion subgroup. This is straightforward: all but one of the covering maps have degree 2, so we end up with a model of the form $y^2 = p(t)$, where $p(t)$ is a polynomial, and the desired technique is implemented in MAGMA. The remaining case is handled via a brute force search for points.

For genus less than 7, we determine the complete set of rational points. Each of the following techniques play a role:

1. local methods,
2. Chabauty for genus 2 curves,
3. quotients,
4. étale descent,
5. Mordell-Weil sieve,

In this section, we describe in detail the theory behind these techniques, except that of the Mordell-Weil sieve (see Section 3.2.3), used to analyze the rational points on the lower genus curves, and the subsequent sections provide a case by case analysis of the rational points on the various composite level modular curves.

Type	Number
$X_{H,G} \cong \mathbf{P}^1$	17
Pointless conics	2
Elliptic curves with positive rank	2
Elliptic curves with rank zero	29
Genus 1 curves without rational points	1
Genus 2 models and points computed	12
Genus 3 hyperelliptic models and points computed	2
Genus 7 curve whose points are not computed	1

Table 5.1: Summary of the 66 composite level models

5.3.1 Chabauty

See [MP07] for a survey. The practical output is that if $\operatorname{rk} \operatorname{Jac}_X(\mathbf{Q}) < \dim \operatorname{Jac}_X = g(X)$, then p-adic integration produces an explicit 1-variable power series $f \in \mathbf{Q}_p[\![t]\!]$ whose set of $\mathbf{Z}_p$-solutions contains all of the rational points. This is all implemented in Magma for genus 2 curves over number fields. In the section below, we discuss the documentation for Magma's implemented Chabauty command on genus 2 curves.

5.3.2 Étale descent

Étale descent is a "going up" style technique, first studied in [CG89] and [Wet97] and developed as a full theory (especially the non-abelian case) in [Sko01]. It is now a standard technique for resolving the rational points on curves (cf. [FW01, Bru03]).

Let $\pi\colon X \to Y$ be a degree n étale cover defined over a number field K such that Y is the quotient of some free action of a group G on X. By Riemann-Hurwitz, the genus of X is $ng(Y) - (n-1)$. Then there exists a

finite collection $\pi_1 \colon X_1 \to Y, \ldots, \pi_n \colon X_n \to Y$ of twist of $X \to Y$ such that

$$\bigcup_{i=1}^{n} \pi_i(X_i(K)) = Y(K).$$

Moreover, if we let S be the union of the sets of primes of bad reduction of X and Y and of the primes of $\mathcal{O}_K$ over the primes dividing $\#G$, then the cocycles corresponding to the twist are unramifeid outside of S.

We shall use this procedure on in the case of étale double covers. In this case, $G = \mathbf{Z}/2\mathbf{Z}$, and since the twists are consequently quadratic, we will instead denote the twist of a double cover $X \to Y$ by $X_d \to Y$, where $d \in K^\times/(K^\times)^2$. The above discussion gives that, for any point of $Y(K)$, there will exist $d \in \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2$ such that P lifts to a point of $X_d(K)$.

5.3.3 Quotients

Taking quotients is a "going down" technique. If C is a curve of genus g, it is very helpful to be able to find maps from C to curves of lower genus. In this context, it is helpful to compute the group G of automoprhisms of C and consider quotients C/H for subgroups $H \leq G$. Magma's algebraic function field machinery is able to compute automorphism groups of curves, however, the performance of these routines varies quite significantly based on the complexity of the base field.

We are interested in constructing automorphisms (define over $\overline{\mathbf{Q}}$) of non-hyperelliptic curves $C/\mathbf{Q}$ with genus ≤ 3, and for our purposes, Magma's rountines are sufficient. For a new, faster procedure for efficiently constructing all "probable" automorphisms of non-hyperelliptic curves of genus ≥ 3 over number fields, see [RZB14, Section 7.7].

5.3.4 Probable computations of rank

It is straightforward to compute the rank of a curve of genus at most 2 using MAGMA's preexisting commands via `RankBound`, an implementation of [Sto01]. Computations of the rank of the Jacobian of a genus 3 plan curve have recently been worked out [BPS12], but it is often impratical [BPS12, Remark 1.1] and moreover has not been implemented in a publicly available way. For the determination of the rational points on each $X_{H,G}$ we shall use a rigorous computation of rank for genus at most 2 and use cyclic descent for genus equal to 3 (see Section 5.1.18).

In the following sections, we provably compute all of the rational points on the modular curves of genus 2, 3, and 7. The MAGMA code verifying the below claims is available at [Mor].

5.4 Analysis of Rational Points - Genus 2

There are 12 composite level modular curves with genus 2. Among these, 6 have Jacobians with rank 0, 4 with rank 1, and 2 with rank 2. We will use étale descent on the rank 2 cases and Chabauty and quotients on the others. In each case, the rank of the Jacobian is computed with MAGMA's `RankBound` command. In the subsections below, the curve X will denote a hyperelliptic curve of genus 2.

5.4.1 Rank 0

If $\mathrm{rk}\ \mathrm{Jac}_X(\mathbf{Q}) = 0$, then $\mathrm{Jac}_X(\mathbf{Q})$ is torsion. To find all of the rational points on X it thus suffices to compute the torsion subgroup of $\mathrm{Jac}_X(\mathbf{Q})$ and compute the preimages under an inclusion $X \hookrightarrow \mathrm{Jac}_X$. This is implemented in MAGMA as the `Chabauty0(J)` command, where `J` is Jac_X.

5.4.2 Rank 1

If rk $\mathrm{Jac}_X(\mathbf{Q}) = 1$, then one can attempt Chabauty's method. This is implemented in MAGMA as the `Chabauty(ptJ,p)` command, where `ptJ` is a point on Jac_X which generates $\mathrm{Jac}_X / \mathrm{Jac}_X[\mathrm{tors}]$ and `p` is a prime of good reduction of X. The output of this command is an indexed set of tuples $\langle (x, z, \nu, k) \rangle$ such that there are at most k pairs of rational points on X whose image in $\mathbf{P}^1_{\mathbf{Q}}$ under the x-coordinate map are congruent to $(x : z)$ modulo p^ν, and such that the only rational points on X outside of these congruence classes are Weierstrass points. Using the command `Support(RamificationDivisor(X))`, we compute the Weierstrass points on our curve which live over $\mathbf{Q}$ and thus the rational points on the curve X.

5.4.3 Rank 2

If rk $\mathrm{Jac}_X(\mathbf{Q}) = 2$, then Chabauty's method does not apply; instead, we proceed with étale descent. In each case, the Jacobian of X has a rational 2-torsion point. Thus, given a model

$$X\colon y^2 = f(x)$$

of X, f factors as $f_1 f_2$ where both polynomials are of positive, even degree, and X admits étale double covers $C_d \to X$, where the curves C_d is given by

$$\begin{aligned} C_d\colon d y_1^2 &= f_1(x) \\ d y_2^2 &= f_2(x). \end{aligned}$$

Let S denote the set of bad places as in Section 5.3.2. By étale descent, every rational point on X lifts to a rational point on $C_d(\mathbf{Q})$ for d in the set of divisors of primes in S, their multiples, and negations. The Jacobian of C_d is isogenous to $\mathrm{Jac}(X) \times E_d$, where E_d is the Jacobian of the (possibly pointless)

genus one curve $dy_2^2 = f_2(x)$ (where we assume that $\deg f_2 \geq \deg f_1$, so that $\deg f_2 \geq 3$).

There is only one isomorphism class of genus 2 curves in our list with Jacobain of rank 2 $(X_{H_{40},G_4}(24), X_{H_{97},G_4}(24))$. The two curves in this class are isomorphic to the hyperelliptic curve

$$H\colon y^2 = 2x^6 + 2 = 2(x^2+1)(x^4 - x^2 + 1).$$

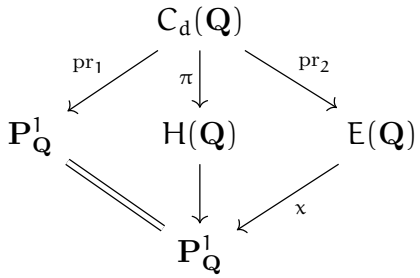
This curve admits étale covers by the genus 3 curves

$$\begin{aligned} C_d\colon dy_1^2 &= (x^2+1) \\ dy_2^2 &= 2(x^4 - x^2 + 1). \end{aligned}$$

for $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. We find that the genus 1 curves $dy_2^2 = 2(x^4 - x^2 + 1)$ only have local points everywhere when $d = 2$. We compute that the curve $2y_1^2 = (x^2+1)$ is isomorphic to $\mathbf{P}^1_{\mathbf{Q}}$ and the curve $2y_2^2 = 2(x^4 - x^2 + 1)$ is isomorphic to the rank 0 elliptic curve

$$E\colon y^2 + 2xy = x^3 - 8x^2 + 12x.$$

Hence the following diagram



tells us that the points on $C_d(\mathbf{Q})$ come from the preimages of the points on $E(\mathbf{Q})$. This allows us to determine the rational points on C_d and thus on H

and on $X_{H_{40},G_4}(24)$ and $X_{H_{97},G_4}(24)$.

5.5 Analysis of Rational Points - Genus 3

There are 22 genus 3 curves (and at most 20 isomorphism classes). Of the isomorphism classes, 12 are hyperelliptic. The curves $X_{G_3,G_2}(14)$, $X_{G_3,G_6}(14)$, and $X_{G_3,G_3}(10)$ are hyperelliptic and have rank equal to 0, and we handle these curves by using a Mordell-Weil sieve argument.

5.5.1 Analysis of $X_{G_3,G_2}(14)$

The modular curve $X_{G_3,G_2}(14)$ has a model given by the genus 3 hyperelliptic curve

$$X_{G_3,G_2}(14)\colon y^2 = -(x^3 - 2x^2 - x + 1)(x^4 + 2x^3 - 9x^2 - 10x - 3).$$

For simplicity, we denote the smooth compactification of the modular curve $X_{G_3,G_2}(14)$ by X. MAGMA computes that $\operatorname{rk} \operatorname{Jac}_X(\mathbf{Q}) = 0$, so $\operatorname{Jac}_X(\mathbf{Q})$ is torsion. We find that there exists a non-singular point $(1 : 0 : 0) \in X(\mathbf{Q})$, and we claim that this is in fact the only point on X. For ease of notation, we shall denote this point as P_0. We provide a proof determining the rational points on $X_{G_3,G_2}(14)$, and we refer the reader to [Mor] for the code verifying this proof and that of $X_{G_3,G_6}(14)$.

Since the rank of our curve is zero, $\operatorname{Jac}_X(\mathbf{Q})$ is torsion. From [HS00, Exercise C.4], we have $\#\operatorname{Jac}_X(\mathbf{F}_p) = P_1(1)$, where $P_1(T)$ is the numerator of the Weil zeta function of $X(\mathbf{F}_p)$ for some prime p. Moreover, by computing this value for a large number of primes and taking greatest common divisor, we find that $\#\operatorname{Jac}_X(\mathbf{Q})$ must divide 6. Since we have a point P_0 on X, we

can embed X into Jac_X via the Abel-Jacobi map

$$\begin{aligned} X &\longrightarrow \mathrm{Jac}_X \\ P &\longmapsto [P - P_0]. \end{aligned}$$

Our above computation tells us the possible torsion in $\mathrm{Jac}_X(\mathbf{Q})$ is of order $1, 2, 3$ or 6. We shall show that no point on $X(\mathbf{Q})$ maps to a non-trivial torsion point in $\mathrm{Jac}_X(\mathbf{Q})$, from which we can conclude that P_0 is the only point in $X(\mathbf{Q})$.

First, we recall the fact that the prime to p torsion of $\mathrm{Jac}_X(\mathbf{Q})$ injects into $\mathrm{Jac}_X(\mathbf{F}_p)$. Using this fact, we apply a Mordell-Weil sieve type argument to prove our desired claim. Let $S = \{5, 11\}$ and consider the following commutative diagram

$$\begin{array}{ccc} X(\mathbf{Q}) & \xhookrightarrow{\iota} & \mathrm{Jac}_X(\mathbf{Q}) \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} \\ \prod_{p \in S} X(\mathbf{F}_p) & \xhookrightarrow{\iota_p} & \prod_{p \in S} \mathrm{Jac}_X(\mathbf{F}_p) \end{array}$$

If the divisor $[P - Q]$ was a torsion point over $\mathbf{Q}$, then it must also be torsion over $\mathbf{F}_p$ for all p. Using MAGMA, we can enumerate $X(\mathbf{F}_p)$ and check individually the orders of $[P - Q]$ in $\mathrm{Jac}_X(\mathbf{F}_p)$. For the primes in S, we compute that the points on $X(\mathbf{F}_5)$ map to points of exact order $\{1, 51\}$ in $\mathrm{Jac}_X(\mathbf{F}_5)$ and the points on $X(\mathbf{F}_{11})$ map to points of exact order $\{1, 8, 20, 40, 60, 120\}$ in $\mathrm{Jac}_X(\mathbf{F}_{11})$. Since none of these values coincide and the prime to p torsion injects, we have that the divisor $[P - Q]$ of $\mathrm{Jac}_X(\mathbf{Q})$ could have order $\{5, 255\}$ or $\{11, 88, 66, 220, 440, 660, 1320\}$, and in particular a 5 or 11 torsion point could map to the identity. However, our initial computation told us that the possible torsion in $\mathrm{Jac}_X(\mathbf{Q})$ must divide 6. Therefore, no point on $X(\mathbf{Q})$ can inject into a non-trivial torsion point on $\mathrm{Jac}_X(\mathbf{Q})$, and so, $\{P_0\} = X(\mathbf{Q})$.

5.5.2 Analysis of $X_{G_3,G_3}(10)$

The modular curve $X_{G_3,G_3}(10)$ has a model as a genus 3 hyperelliptic curve

$$X\colon y^2 = 3x^8 + 8x^7 + 26x^6 + 9x^5 + 10x^4 - 99x^3 - 104x^2 - 148x - 77.$$

MAGMA's `RankBound` command does not give a useful bound. To ameliorate this problem, we use quotients. Let $\mathcal{A}$ denote the automorphism group of X. We find that $\mathcal{A} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and that the quotient curve X/α, where α is a generator of $\mathcal{A}$, is the rank 0 elliptic curve

$$E\colon y^2 = x^3 + x^2 - 33x - 62.$$

By pulling back the points on E, we find that $X(\mathbf{Q}) = \emptyset$.

5.6 Analysis of Rational Points - Higher Genus

We encounter a genus 7 curve coming from the anomalous genus 1 modular curve $X_{G_3}(11)$ with infinitely many points.

5.6.1 Analysis of $X_{G_3,G_3}(22)$

As mentioned in Section 5.1, there is only one modular curve from [Zyw15] of genus 1 with rank 1, namely $X_{G_3}(11)$, which is isomorphic to the elliptic curve $\mathcal{E}\colon y^2 + y = x^3 - x^2 - 7x + 10$. Recall the morhpism $J(x,y)$ corresponding to the map from $\mathcal{E} \to \mathbf{A}^1_{\mathbf{Q}} \cup \{\infty\}$ and that $\mathcal{E}(\mathbf{Q}) \cong \langle (4,5) \rangle$. The composite-$(2,11)$ level modular curve

$$X_{G_3,G_3}(22)\colon \begin{array}{c} y^2 + y = x^3 - x^2 - 7x + 10 \\ s^2 + 12^3 = J(x,y) \end{array}$$

is a genus 7 curve in $\mathbf{A}_3(\mathbf{Q})$. For simplicity, we denote the smooth compactification of this curve by X. By pulling back points from $\mathcal{E}(\mathbf{Q})$, we find a cuspidal point and the CM point $(x : y : s : z) = (2 : 0 : 0 : 1)$ on X. Unfortunately, we are unable to provably compute the rational points on the curve X. Below, we discuss the attempted techniques and facts about said curve.

Let $\mathrm{Jac}_X(\mathbf{Q})$ be the Jacobian of X. Local computations strongly suggest that

$$\mathrm{Jac}_X(\mathbf{Q}) \hookrightarrow \mathcal{E} \times E^2 \times A \times A'$$

where $\mathcal{E}$ is the elliptic curve defined above, $E/\mathbf{Q}$ is an elliptic curve, and A, A' are some 2-dimensional abelian varieties. We cannot prove that $\mathrm{Jac}_X(\mathbf{Q})$ decomposes as above since the computations over the finite fields $\mathbf{F}_{p^4}$ exceeds MAGMA's capabilities.

The geometry of the curve suggests that we use quotients to provably find the rational points on X. Using MAGMA, we compute the the automorphism group of X is $\mathbf{Z}/2\mathbf{Z}$, and the only curve quotient of X is the elliptic curve $\mathcal{E}$ with positive rank; this procedure takes around 13 hours. If the above decomposition does hold, then we want to determine the other elliptic factor E.

As suggested by Jeremy Rouse, it could be possible that there exists some maximal subgroup H of $\mathrm{GL}_2(\mathbf{Z}/22\mathbf{Z})$ such that $G_3 \times G_3 \leq H$, which may correspond to the existence of a modular curve X_H of lower genus for which $X(\mathbf{Q}) \to X_H(\mathbf{Q})$. Since these subgroups do not have any special condition, there is no reason a priori that X_H should have lower genus. Using MAGMA, we find one applicable maximal subgroup H containing $G_3 \times G_3$. To our chagrin, the index of $G_3 \times G_3$ in H is 2, and hence the modular curve X_H is isomorphic to $\mathcal{E}$ by our above curve quotient computation.

An unexplored approach is to find a number field K over which we have extra automorphisms, meaning $\mathrm{Aut}(X) \subseteq \mathrm{Aut}(X_K)$; these extra automorphisms will allow for further curve quotient possibilities. If the above decomposition

holds, then we can choose K to be a number field over which the 2-dimensional abelian variety A or A' splits. The recent work [BSS+16] gives a database of genus 2 curves of small discriminant. By ranging over this database and comparing Weil-zeta functions, we may be able to find the genus 2 curve defining the abelian variety A or A', and once we have equations for the defining curve, we can compute the number field K and proceed with taking curve quotients.

5.6.2 The Cursed Examples

Up to conjugacy, there are 4 maximal subgroups of $\mathrm{GL}_2(\mathbf{F}_{13})$ that have surjective determinant, namely $G_6, N_{sp}(13), N_{nsp}(13)$ and G_7. Zywina handles the cases concerning the subgroups of G_6, and the other three subgroups correspond to the outstanding cases.

Baran [Bar14] showed that the modular curves $X_{N_{sp}}(13)$ and $X_{N_{nsp}(13)}$ are both isomorphic to the genus 3 curve C defined in $\mathbf{P}^2_{\mathbf{Q}}$ with equation

$$(y-z)x^3+(2y^2+zy)x^2+(-y^3+zy^2-2z^2y+z^3)x+(2z^2y^2-3z^3y)=0.$$

Baran gives the morphism from the above model to the j-line. The 7 known rational points on C all correspond to cusps and CM points on $X_{N_{sp}}(13)$ and $X_{N_{nsp}(13)}$. Conjecturally, C has no other rational points, which is equivalent to saying that there does not exist a non-CM elliptic curve over $\mathbf{Q}$ with $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to a subgroup of $N_{sp}(13)$ and $N_{nsp}(13)$.

Banwait and Cremona [BC14] have shown that $X_{G_7}(13)$ is isomorphic to the genus 3 curve C' defined in $\mathbf{P}^2_{\mathbf{Q}}$ with equation

$$4x^3y-3x^2y^2+3xy^3-x^3z+16x^2yz-11xy^2z+5y^3z+3x^2z^2+9xyz^2+y^2z^2+xz^3+2yz^3=0.$$

The authors also give the morphism from the modular curve to the j-line. The

4 known rational points on C' correspond to a CM points and three non-CM points. Conjecturally, C' has no other rational points, which is equivalent to saying that [Zyw15, Theorem 1.8(iv)] gives necessary and sufficient condition on when $\rho_{E,13}(G_{\mathbf{Q}})$.

We check that: the known points on C do not pull back to points $X_{G_3,N_{sp}}(26)$, the point $(0:0:1)$ on C pulls back to the CM point corresponding to $j = 0$ on $X_{G_3,N_{nsp}}(26)$, and the known points on C' do not pullback to points on $X_{G_3,G_7}(26)$. Following the above conjectures, we formulate our own concerning the composite-$(2,13)$ image of Galois.

Conjecture 5.6.3. *There does not exist a non-CM elliptic curve* E *over* $\mathbf{Q}$ *with square discriminant such that* $(\rho_{E,2} \times \rho_{E,13})(G_{\mathbf{Q}})$ *is simultaneously non-surjective.*

Chapter 6

Entanglements

An elliptic curve E over K has (m_1, m_2)-entanglement fields if $K(E[m_1]) \cap K(E[m_2]) \neq K$ for a relatively prime pair $m_1, m_2 \in \mathbf{N}$. We say that E/K has (m_1, m_2)-abelian entanglement (resp. (m_1, m_2)-nonabelian entanglement) if $K(E[m_1]) \cap K(E[m_2]) = L$ where L/K is an abelian (resp. nonabelian) extension. In this chapter, we complete the classification of the $(2, 3)$—nonabelian entanglement fields for elliptic curves over $\mathbf{Q}$ using Theorem 5.1.15 and [BJ16], and we also provide a conjectural classification of $(2, 3)$-abelian entanglement fields for elliptic curves over $\mathbf{Q}$. Using Theorem 5.1.12, we also find non-CM elliptic curves with $(2, 7)$-entanglement fields of degree 3, and finally, we exhibit an infinite family of elliptic curves over $\mathbf{Q}$ with $(2, p^n)$-entanglement fields of degree 3 where p is a prime such that $3|p - 1$.

An important tool in our study of entanglements is Goursat's topological lemma (see [Rib76, Lemma 5.2.1] for proof).

Lemma 6.0.4 (Goursat's lemma)**.** *Let* G_0 *and* G_1 *be groups and* $G \subseteq G_0 \times G_1$ *a subgroup satisfying*

$$\pi_i(G) = G_i \quad (i \in \{0, 1\}),$$

where π_i *denotes the canonical projection onto the* i^{th}*-factor. Then there ex-*

ists a normal group Q *and surjective homomorphisms* $\psi_0 \colon G_0 \to Q$, $\psi_1 \colon G_1 \to Q$ *for which*

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi_0(g_0) = \psi_1(g_1)\}.$$

The idea is to use our results concerning composite level modular curves to find possibilities for entanglement. Then we apply Goursat's lemma to eliminate the cases where entanglement cannot occur from a group theoretic viewpoint. From here, we compute division fields using MAGMA and check for entanglements.

To demonstrate the technique, we first present a result proving the lack of entanglement fields for a family of elliptic curves over $\mathbf{Q}$.

Lemma 6.0.5. *Let* E *be a non-CM elliptic curve over* $\mathbf{Q}$ *with square discriminant. Then* $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[5]) = \mathbf{Q}$*, so* $E/\mathbf{Q}$ *does not have* $(2,5)$*-entanglement field.*

Proof. From Table A.1 and Proposition 5.1.2, we find that the composite-$(2,5)$ image must be either conjugate to $G_3 \times G_9$ or $G_1 \times G_9$; in the latter case, entanglement is not possible since $\mathbf{Q}(E[2]) \cong \mathbf{Q}$. The subgroup G_9 do not contain an index 3 normal subgroup, hence Lemma 6.0.4, implies that there does not exists a subgroup $G \leq \mathrm{GL}_2(\mathbf{F}_2) \times \mathrm{GL}_2(\mathbf{F}_5)$ that projects onto the mod 2 and mod 5 image. Therefore, these curves cannot have entanglement fields via the Galois correspondence. □

6.1 $(2,3)$-entanglement

In a recent work [BJ16], Brau and Jones exhibit a modular curve of level 6 over $\mathbf{Q}$ whose $\mathbf{Q}$-rational points correspond to j-invariants of elliptic curves E over $\mathbf{Q}$ with $\mathbf{Q}(E[2]) \subseteq \mathbf{Q}(\zeta_3, \Delta_E^{1/3})$ and hence have $(2,3)$-entanglement fields.

The construction of their modular curve begins with finding the unique index 6 normal subgroups $\mathcal{N} \leq \mathrm{GL}_2(\mathbf{F}_3)$ defined by

$$\mathcal{N} := \left\{ \left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right) : x^2 + y^2 \equiv 1 \mod 3 \right\} \sqcup \left\{ \left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right) : x^2 + y^2 \equiv -1 \mod 3 \right\}.$$

The authors observe that $\mathcal{N}$ fits into the exact sequence

$$1 \longrightarrow \mathcal{N} \hookrightarrow \mathrm{GL}_2(\mathbf{F}_3) \xrightarrow{\theta} \mathrm{GL}_2(\mathbf{F}_2) \longrightarrow 1.$$

Their modular curve of level 6 corresponds to the subgroup $H' \leq \mathrm{GL}_2(\mathbf{Z}/6\mathbf{Z})$ coming from the graph of θ

$$H' := \{(g_2, g_3) \in \mathrm{GL}_2(\mathbf{F}_2) \times \mathrm{GL}_2(\mathbf{F}_3) : g_2 = \theta(g_3)\}.$$

The points lying in the image of the $j(X_{H'})$ correspond to j-invariants of elliptic curves over $\mathbf{Q}$ satisfying the above division field condition. We state a stronger version of their result concerning this curve in the following theorem.

Theorem 6.1.1 ([BJ16] Theorem 1.4)**.** *Let E be a non-CM elliptic curve over $\mathbf{Q}$ with j-invariant of the form*

$$j_E = 2^{10}3^3t^3(1 - 4t^3)$$

where $t \in \mathbf{Q} \setminus \{0\}$. Then E has surjective mod 2 image of Galois and $(2,3)$-nonabelian entanglement fields

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}).$$

Proof. By [BJ16, Remark 1.5], E has the property that $\mathbf{Q}(E[2]) \subseteq \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \subseteq \mathbf{Q}(E[3])$. We show that the mod 2 image must be surjective, in particular, we show that $\mathbf{Q}(E[2])$ cannot be isomorphic to $\mathbf{Q}$, $\mathbf{Q}(\zeta_3)$, or $\mathbf{Q}(\Delta_E^{1/3})$. Using

[Zyw15, Theorem 1.2.ii], we construct the modular curve

$$X\colon 2^{10}3^3t^3(1-4t^3) = \frac{256(s+1)^3}{s},$$

whose rational points correspond to elliptic curves over $\mathbf{Q}$ with $\rho_{E,2}(G_{\mathbf{Q}})$ conjugate to a subgroup of G_2 and $\mathbf{Q}(E[2]) \subseteq \mathbf{Q}(\zeta_3, \Delta_E^{1/3})$. This modular curve is isomorphic to a rank 0 elliptic curve, and we compute that the only points on X are CM points. Hence E cannot have $\rho_{E,2}(G_{\mathbf{Q}})$ conjugate to G_2, in particular $\mathbf{Q}(E[2])$ cannot be isomorphic to $\mathbf{Q}(\zeta_3)$. Since $\{I\} \subset G_2$, we immediately have that there do not exist non-CM elliptic curves over $\mathbf{Q}$ with $\rho_{E,2}(G_{\mathbf{Q}})$ conjugate to G_1 and $\mathbf{Q}(E[2]) \subset \mathbf{Q}(\zeta_3, \Delta_E^{1/3})$.

To complete the proof, we need to find the $\mathbf{Q}$-points on the curve

$$X\colon s^2 + 1728 = 2^{10}3^3t^3(1-4t^3).$$

Through simple manipulation, we find a model for X as

$$X'\colon s^2 = 2^6 3^3(2t-1)^2(4t^2+2t+1)^2.$$

Notice that X' is not geometrically irreducible. In fact, $X' \times \overline{\mathbf{Q}}$ is the intersection of two conics in three distinct points, two of which are quadratic points. Moreover, we only find one $\mathbf{Q}$-rational point $(0, 1/2)$ on X' since 3 is not a square. Since the point $(0, 1/2)$ corresponds to a CM elliptic curve, there does not exist non-CM elliptic curves over $\mathbf{Q}$ with $\rho_{E,2}(G_{\mathbf{Q}})$ conjugate to G_3 and $\mathbf{Q}(E[2]) \subset \mathbf{Q}(\zeta_3, \Delta_E^{1/3})$. Therefore, E must have surjective mod 2 image of Galois and $(2,3)$-nonabelian entanglement fields. □

Brau and Jones pose the question [BJ16, Question 1.1] of classifying the triples (E, m_1, m_2) with E an elliptic curve over a number field K and m_1, m_2 a pair of relatively prime integers for which the (m_1, m_2)-entanglement is non-

abelian over K. We ask whether the elliptic curves defined in Theorem 6.1.1 are the only ones defined over $\mathbf{Q}$ with non-abelian $(2,3)$-entanglement fields. By constructing covers of the modular curve $X_{H'}$, we find another family of elliptic curves with such entanglement fields and provide a complete answer to [BJ16, Question 1.1] in the case where $K = \mathbf{Q}$ and $(m_1, m_2) = (2,3)$.

Theorem 6.1.2. *There exist infinitely many non-CM elliptic curves* E *over* $\mathbf{Q}$ *with composite-*$(2,3)$ *image of Galois conjugate to* $\mathrm{GL}_2(\mathbf{F}_2) \times G_3$ *and non-abelian entanglement fields*

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) = \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \cong \mathbf{Q}(x(E[3])).$$

Furthermore, there do not exist non-CM elliptic curves with j*-invariant outside of those from Theorem 6.1.1 and those given in [Mor] with* $(2,3)$*-nonabelian entanglement fields.*

Proof. Let G_3 be the level 3 applicable subgroup from List 5.1.5. There exists a unique index 6 normal subgroup of G_3, namely

$$G' := \left\langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \right\rangle.$$

Since $G' \leq \mathcal{N}$, we have the following exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{N} & \hookrightarrow & \mathrm{GL}_2(\mathbf{F}_3) & \xrightarrow{\theta_1} & \mathrm{GL}_2(\mathbf{F}_2) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \longrightarrow & G' & \hookrightarrow & G_3 & \xrightarrow{\theta_2} & \mathrm{GL}_2(\mathbf{F}_2) & \longrightarrow & 1 \end{array}$$

Let

$$H'' := \{(g_2, g_3) \in \mathrm{GL}_2(\mathbf{F}_2) \times G_3 : g_2 = \theta_2(g_3)\}$$

denote the graph of θ_2. Since $H'' \leq H'$, there is a map between the modular

curves $X_{H''} \to X_{H'}$. Using List 5.1.5, we can construct a model for the level 6 modular curve corresponding to H''

$$X_{H''}\colon 2^{10}3^3s^3(1-4s^3) = \frac{27(t+1)(t+9)^3}{t^3}.$$

The curve $X_{H''}$ is a genus 0 curve endowed with a rational point, hence isomorphic to $\mathbf{P}^1_{\mathbf{Q}}$. The rational points on the curve $X_{H''}$ correspond to elliptic curves over $\mathbf{Q}$ with composite-$(2,3)$ image conjugate to a subgroup $\mathrm{GL}_2(\mathbf{F}_2) \times G_3$ and $\mathbf{Q}(E[2]) \subseteq \mathbf{Q}(\zeta_3, \Delta_E^{1/3})$. Since these curve have surjective mod 2 image, the composite-$(2,3)$ image condition implies that $[\mathbf{Q}(E[2]) : \mathbf{Q}] = 6$ and that $[\mathbf{Q}(E[3]) : \mathbf{Q}] \leq 12$, and the entanglement assumption tells us that either $\mathbf{Q}(E[2]) \cong \mathbf{Q}(x(E[3]))$ or $\mathbf{Q}(E[2]) \cong \mathbf{Q}(E[3])$. We claim that the latter isomorphism cannot occur.

Suppose that there exists an elliptic curve $E/\mathbf{Q}$ with Weierstrass equation $y^2 = x^3 + Ax + B$ such that the above $(2,3)$-composite image condition holds and that $\mathbf{Q}(E[2]) \cong \mathbf{Q}(E[3])$. Unraveling the assumptions, we find that $f(x) = x^3 + Ax + B$ is the minimal polynomial of the number field $\mathbf{Q}(E[2])$, and we claim that the 3-division polynomial $\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$ is divisible by $f(x)$. Since the roots of $\psi_3(x)$ correspond to the x-coordinate of $E(\overline{\mathbf{Q}})[3]$ and $\mathrm{Gal}(\mathbf{Q}(E[3]/\mathbf{Q})) \cong S_3$, we have that $\psi_3(x)$ must factor as into the product of a cubic and linear polynomial. Moreover, the cubic factor must be $f(x)$; otherwise, $\mathbf{Q}(E[3])/\mathbf{Q}$ would not be and S_3 extension. Thus, we have shown that

$$\begin{aligned}\psi_3(x) &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\ &= (x^3 + Ax + B)(3x + \alpha),\end{aligned}$$

where $\alpha \in \mathbf{Q}$. Since the cubic term in $\psi_3(x)$ has zero coefficient, $\alpha = 0$, which yields a contradiction. Therefore, there cannot exists such an elliptic

curve $E/\mathbf{Q}$ with the above $(2,3)$-composite image condition holds and that $\mathbf{Q}(E[2]) \cong \mathbf{Q}(E[3])$. Moreover, the rational points on $X_{H''}$ classify elliptic curves with non-abelian entanglement fields

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) = \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \cong \mathbf{Q}(x(E[3])).$$

The latter statement follows from the fact that the only applicable subgroup of level 3 that has an index 6, normal subgroup are G_3, $H_{3,1}$, and $H_{3,2}$. Above, we showed an elliptic curve cannot have $(2,3)$-composite level conjugate to $GL_2(\mathbf{F}_2) \times H_{3,1}$ or to $GL_2(\mathbf{F}_2) \times H_{3,2}$ and $(2,3)$-nonabelian entanglement fields. Therefore, $X_{H''}$ is the only cover of $X_{H'}$ with infinitely many $\mathbf{Q}$-rational points.

□

We now present examples of elliptic curves over $\mathbf{Q}$ with both types of $(2,3)$-nonabelian entanglement.

Example 6.1.2.1. Using Theorem 6.1.1, consider the elliptic curve

$$E: y^2 = x^3 - 1296/49x + 2592/49.$$

Using MAGMA, we check that E has surjective $(2,3)$-composite level image, meaning that $\rho_{E,2}(G_{\mathbf{Q}}) \cong GL_2(\mathbf{F}_2)$ and that $\rho_{E,3}(G_{\mathbf{Q}}) \cong GL_2(\mathbf{F}_3)$.

Example 6.1.2.2. Using Theorem 6.1.2, consider the elliptic curve

$$E': y^2 = x^3 - \frac{2^7 3^4 5^3 23^3 31^3 127^3 499^3 2411^3 28537^3 243712877^3 18685628639}{997^2 3541^2 1163159^2 246161437^2 2472465553^2 79027955033892}x + \frac{2^8 3^4 5^3 23^3 31^3 127^3 499^3 2411^3 28537^3 243712877^3 18685628639}{997^2 3541^2 1163159^2 246161437^2 2472465553^2 79027955033892}$$

Using MAGMA, we check that E has $(2,3)$-composite level image conjugate to $GL_2(\mathbf{F}_2) \times G_3$ and has $(2,3)$-nonabelian entanglement $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(x(E[3]))$.

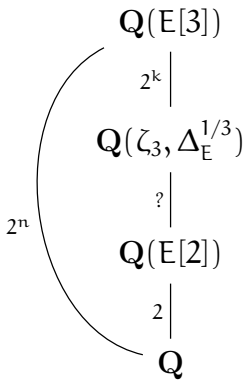
Now, we turn our attention to finding non-CM elliptic curves with $(2,3)$-abelian entanglement fields. From Table A.5, there exist 5 possibilities for simultaneous non-surjective composite-$(2,3)$ image of Galois excluding the case where $\rho_{E,2}(G_{\mathbf{Q}}) \cong G_1$. By using a similar method to the proof Lemma 6.0.5, an elliptic curve over $\mathbf{Q}$ with composite-$(2,3)$ image conjugate to $G_3 \times G_3$ or $G_3 \times \mathrm{GL}_2(\mathbf{F}_3)$ cannot have $(2,3)$-entanglement. Hence to find abelian entanglements, we must focus on the remaining cases occurring in Table A.5, where $\rho_{E,2}(G_{\mathbf{Q}})$ is conjugate to G_2**.** Ideally, we hoped that finding sequences as in the proof of Theorem 6.1.2 would lead to other entanglement fields. However, the condition on the elliptic curves coming from the points on $X_{H'}$ proves to be too restrictive.

Proposition 6.1.3. *There do not exist non-CM elliptic curves over* $\mathbf{Q}$ *with simultaneous non-surjective composite-*$(2,3)$ *image and* $\mathbf{Q}(E[2]) \subseteq \mathbf{Q}(\zeta_3, \Delta_E^{1/3})$.

Proof. Let E be a non-CM elliptic curve with composite-$(2,3)$ image conjugate to $G_2 \times G_i$ where G_i is from List 5.1.5. First, we determine whether there is an index 2, normal subgroups of G_i that is contained in $\mathcal{N}$; the subgroup G_3 is the only one that does not contain such a subgroup. In the remaining cases, we can construct a cover of the modular curve $X_{H'}$. We claim that the rational points on these covers are CM.

If there existed a non-CM rational point on this cover, then we could find a non-CM elliptic curve with above composite level image of Galois and division field condition. Unraveling these assumptions, the curve E has the

following division field diagram–



Moreover, the discriminant of E must be a rational cube, and hence $\mathbf{Q}(\zeta_3) \cong \mathbf{Q}(E[2])$. There are only two isomorphism classes of CM elliptic curves (with $j = 0$ and $j = 1728$) with this prescribed 2-torsion. Thus, we have a contradiction to our assumption that E does not have CM, and therefore, rational points on these covers are CM. □

Proposition 6.1.3 does not eliminate the possibility of mod 2 and mod 3 abelian entanglement fields, however, it limits the tools we can used to determine these field. In Table 6.1, we present all the relevant data these elliptic curve. Finally, we formulate conjectures concerning abelian mod 2 and mod 3 entanglement fields.

Conjecture 6.1.4. *There does not exist a non-CM elliptic curve over* $\mathbf{Q}$ *with composite-*$(2,3)$ *level image conjugate to* $G_2 \times G_1$ *and* $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \neq \mathbf{Q}$.

Conjecture 6.1.5. *There exist infinitely many non-CM elliptic curves over* $\mathbf{Q}$ *composite-*$(2,3)$ *level image conjugate to* $G_2 \times G_2$ *and* $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \neq \mathbf{Q}$.

Conjecture 6.1.6. *There exist infinitely many non-CM elliptic curves over* $\mathbf{Q}$ *composite-*$(2,3)$ *level image conjugate to* $G_2 \times G_3$ *and* $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \neq \mathbf{Q}$.

Table 6.1: Data for $(2,3)$-entanglements

$\rho_{E,2} \times \rho_{E,3}$	j_E	Type	Degree
$GL_2(\mathbf{F}_2) \times GL_2(\mathbf{F}_3)$	$2^{10}3^3t^3(1-4t^3)$	Non-abelian	6
$GL_2(\mathbf{F}_2) \times G_3$	See [Mor]	Non-abelian	6
$G_2 \times G_2$	$\frac{114255689955643907}{3176523000000}, \frac{847631113965283925958407}{15332469805107000000}, \frac{11889860484552117331305923177043814078781684566746393 47}{640942856894774789\ 22762987995687538659667187500000}, \frac{-80481680984375}{5489031744}, \frac{13234765204685122862987056268526749 27}{74261320452818905193085715200000 0}, \frac{39253921495219066964650336567063570877 9}{81784275118569084448509490368000000}, \frac{81380464566393747827620988893517039433378063506388498 47}{30404053875856236647993142857251347864941638830000 00}$	Abelian	2
$G_2 \times G_3$	$\frac{361682234074684125}{462672528510976}, \frac{216316108078942538756375}{133543125605802557232}$	Abelian	2
$G_2 \times G_4$	$\frac{2215302590656}{85766121}, \frac{1878025831622095609}{140478247931904}, \frac{5011623661897}{34012224}, \frac{16865845211125}{5489031744}, \frac{1906624}{729}, \frac{114255689955643907}{3176523000000}, \frac{96331796699876870743121893 21}{3017890031739\ 21081000000}, \frac{59801770244852639234784689672 89}{99865474584530191424000000}$	Abelian	2

Conjecture 6.1.7. *There exist infinitely many non-CM elliptic curves over* $\mathbf{Q}$ *composite-*$(2,3)$ *level image conjugate to* $G_2 \times G_4$ *and* $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \neq \mathbf{Q}$.

6.1.8 $(4,3)$-entanglement

Using Theorem 5.1.15, we find examples of non-CM elliptic curves over $\mathbf{Q}$ with $(4,3)$-abelian entanglement fields. The five possibilities in Theorem 5.1.15 occur when $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate to a subgroup of G_3 or G_4 where these subgroups have orders 12 and 16, respectively and when $\rho_{E,4}(G_{\mathbf{Q}})$ is conjugate to a subgroup of order 16. Since the order of the subgroups appearing in Theorem 5.1.15 are not prime, we cannot utilize Lemma 6.0.4 to group theoretically sieve out the possibilities for entanglement; hence, we use brute force for our computations. Below, we present examples of non-CM elliptic curves with $(4,3)$-abelian entanglement fields.

Example 6.1.8.1. The following elliptic curves have mod 3 image of Galois conjugate to a subgroup of G_4 and the property that $\mathbf{Q}(E[4]) \cap \mathbf{Q}(E[3]) \cong K$, where K is some quadratic number field:

$$E_1 \colon y^2 + xy = x^3 + \frac{1601806640625}{109730573419264}x + \frac{177978515625}{438922293677056},$$

$$E_2 \colon y^2 + xy = x^3 + \frac{9545682734772404224}{1825834888917081300825}x + \frac{2386420683693101056}{16432514000253731707425},$$

$$E_3 \colon y^2 + xy = x^3 - \frac{1224440064}{4952850538825}x - \frac{34012224}{4952850538825}.$$

Remark 6.1.9. There exist three families of elliptic curves with simultaneously non-surjective composite-$(4,3)$ image of Galois where $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate

to a subgroup of G_3. These curves have potential for mod 4 and mod 3 entanglement fields of degree 2, however, the coefficients of these curves limit our computation possibilities.

6.2 $(2, n)$-entanglement

In this section, we look at more general entanglement fields and provide examples of elliptic curves with interesting entanglement.

6.2.1 $(2, 7)$-entanglement

From Table A.2, the only possibility for simultaneous non-surjective composite-$(2, 7)$ image of Galois is $G_3 \times G_7 \leq \mathrm{GL}_2(\mathbf{F}_2) \times \mathrm{GL}_2(\mathbf{F}_7)$. The subgroup G_7 does contain an index 3, normal subgroup, so the points on the modular curve $X_{G_3,G_7}(14)$ correspond to j-invariants of elliptic curves with possible entanglement fields coming from $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[7])$. Since such an elliptic curve E has 7-division field of degree 252, it is computationally inefficient to study the subfields of $\mathbf{Q}(E[7])$ or even $\mathbf{Q}(x(E[7]))$. Hence, in order to perform computations, we need to find a subfield of $\mathbf{Q}(E[7])$ with manageable degree.

Since $Z(\mathrm{GL}_2(\mathbf{F}_7)) \leq G_7$ and $\#Z(\mathrm{GL}_2(\mathbf{F}_7)) = 6$, the fixed field $L := \mathbf{Q}(E[7])^{Z(\mathrm{GL}_2(\mathbf{F}_7))}$ is an index 6 subfield of $\mathbf{Q}(E[7])$. From [Ade01, Table 5.1], L is a degree 42 number field defined by the 7^{th}-modular polynomial $\Phi_7(X, j_E)$. For non-CM E coming from $X_{G_3,G_7}(14)$, we compute degree 3 subfields of L and check whether they are isomorphic to $\mathbf{Q}(E[2])$; below, we give two examples of non-CM elliptic curves with $(2, 7)$-entanglement fields of degree 3.

Example 6.2.1.1. The non-CM elliptic curves

$$E_1 : y^2 + xy = x^3 - 4/129825457969x - 1/1168429121721$$
$$E_2 : y^2 + xy = x^3 - 4/2209x - 1/19881$$

have abelian entanglement of degree 3 coming from the non-trivial intersection of $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[7])$.

6.2.2 $(2, p^n)$-entanglement

In [RS01], Rubin and Silverberg give explicit equations for elliptic curves over a field of characteristic $\neq 2, 3$ with prescribed mod 2 image of Galois. By constructing an elliptic curves over $\mathbf{Q}$ with special 2-division field, we exhibit an infinite family of elliptic curves with $(2, p^n)$-entanglement of degree 3.

Proposition 6.2.3. *Let p be a prime ≥ 5 such that $3|p-1$ and n a positive integer. Then there exist infinitely many elliptic curves over $E/\mathbf{Q}$ such that $\mathbf{Q}(E[2]) \cap \mathbf{Q}(\zeta_{p^n}) = L$, where L is the degree 3 number field of $\mathbf{Q}(\zeta_p)$ by our assumption on p. Furthermore, we give an explicit parametrization of such elliptic curves.*

Proof. Since $\varphi(p^n) = p^{n-1}(p-1)$ where φ is the Euler-totient function, the cyclotomic field $\mathbf{Q}(\zeta_{p^n})$ contains the degree 3 intermediate field L of $\mathbf{Q}(\zeta_p)$. Gauss [Gau66] showed that the minimal polynomial of L is

$$g(X) = X^3 + X^2 + (p-1)X/3 - ((p-1)/3 + kp)/9$$

where k is uniquely determined by the integral representation $4p = (3k-2)^2 + 27N^2$.

Let E be the elliptic curve with defining polynomial $g(X)$. Using the change of variables $(X, Y) \to (x - 1/3, y)$, we find a Weierstrass model of the

form

$$E\colon y^2 = x^3 - \frac{p}{3}x + \frac{p(2-3k)}{27}.$$

The construction of E forces the 2-division field $\mathbf{Q}(E[2])$ to be isomoprhic to L. Using [RS01, Theorem 1.1], the elliptic curve

$$\begin{aligned}\mathbf{E}_t\colon y^2 =& x^3 + \frac{(1727pt^2 + p + 9/4k^2t^2 - 9/4k^2 - 3kt^2 + 3k + t^2 - 1)}{(p - 9/4k^2 + 3k - 1)}x \\ & \frac{(-1727pt^3 - 5181pt^2 + 3pt + p - 9/4k^2t^3 - 27/4k^2t^2)}{(p - 9/4k^2 + 3k - 1)} + \\ & \frac{(-27/4k^2t - 9/4k^2 + 3kt^3 + 9kt^2 + 9kt + 3k - t^3 - 3t^2 - 3t - 1)}{(p - 9/4k^2 + 3k - 1)}\end{aligned}$$

has 2-torsion subgroup isomorphic to that of E for $t \in \mathbf{Q}$. The existence of the Weil pairing implies that elliptic curves of the form $\mathbf{E}_t$ have a degree 3, abelian entanglement field L. □

Remark 6.2.4. Above, we present the general equation for $\mathbf{E}_t$. For a specific prime p and unique k, the defining equation for $\mathbf{E}_t$ can be quickly computed using the MAGMA instrinsic `RubinSilverbergPolynomials(2,j)`, where `j` is the j-invariant of the elliptic curve E.

Chapter 7

Future Work

In this final section, we propose questions for future work.

7.0.5 Torsion in number fields

In combination with work of Maarten Derickx, we complete the classification of isomorphism classes of torsion subgroups that occur for elliptic curves E defined over cubic number fields K using the four-fold Mordell-Weil sieve (see Section 3.2.4). A natural question to our result is how far can we push our four-fold Mordell-Weil sieve technique.

Let K be some number field of degree d. Suppose we have some modular curve X of composite level N with gonality γ. The guiding question is to determine whether $\mathrm{Sym}^{\mathsf{d}}\mathsf{X}(\mathbf{Q})$ is all cuspidal or not. Recall that the optimal situation to utilize our four-fold Mordell-Weil sieve is when $\mathrm{rk}\,\mathsf{J}(\mathsf{X}) = 0$ and $\mathsf{d} < \gamma$. If our curve X satisfies these conditions, then our four-fold Mordell-Weil sieve will either prove that $\mathrm{Sym}^{\mathsf{d}}\mathsf{X}(\mathbf{Q}) = \emptyset$ or provide evidence supporting the existence of a sporadic point of degree d.

A more concrete goal is to compute $\Phi(4)$, which is the set of isomorphism classes for of torsion subgroups for elliptic curves E over some number field K

of degree ≤ 4. In [JKP06, Theorem 3.6], Jeon, Park, and Kim determine the 38 group structures for $E(K)[\text{tors}]$ which appear infinitely often as K varies over all quartic fields. The authors remark that all of these torsion structures already occur infinitely often as K varies over all bi-quadratic number fields.

In a recent work [Cho16], Chou classified the torsion structures that can occur for $E_K := E \times_{\mathbf{Q}} K$ when K is Galois with $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/4\mathbf{Z}$ or $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. His results show that torsion subgroup $\mathbf{Z}/15\mathbf{Z}$ only appears finitely often as K ranges over all Galois quartic number fields. This finiteness is attributed to the fact that there are only finitely many j-invariants of $E/\mathbf{Q}$ having a $\mathbf{Q}$-rational 15 isogeny. In the case of cubic torsion, Najman found the sporadic point on the symmetric cube of the modular curve $X_1(21)$ in his analysis of $\Phi_{\mathbf{Q}}(3)$. Since Chou restricts to Galois number fields, his results do not completely eliminate the possibility of sporadic quartic point occurring in analogous fashion as they do in the cubic case. Despite this assumption, we make the following conjecture:

Conjecture 7.0.6. *There exist 38 possible torsion structures, coming from [JKP06, Theorem 3.6], that appear for* $E(K)[\text{tors}]$ *where* K *ranges over all quartic number fields. Furthermore, all of these torsion subgroups occur infinitely often and over a biquadratic extension of* $\mathbf{Q}$.

7.0.7 Composite level images of Galois

In Theorem 5.1.12, we required the discriminant of E to be a rational square or equivalently that $\rho_{E,2}(G_{\mathbf{Q}})$ is conjugate to a subgroup of G_3. Recall from Section 5.1.17, this assumption allowed us to construct models for our composite level modular curves as hyperelliptic curves. From List 5.1.4, there are two (non-trivial) mod 2 images of Galois. We propose the following problem concerning the other possible image.

Problem 7.0.8. *Let* E *be a non-CM elliptic curve over* $\mathbf{Q}$ *with rational* 2*-torsion. Find the possible indicies (and their frequencies) for simultaneously non-surjective composite-*$(2, \ell)$ *level image of Galois for* $\ell = 5, 7, 11, 13$.

In Problem 7.0.8, the condition on the defining polynomial is equivalent to $\rho_{E,2}(G_{\mathbf{Q}})$ being conjugate to a subgroup of $G_2 \cong \mathbf{Z}/2\mathbf{Z}$. From List 5.1.4, the modular curve parametrizing such elliptic curves does not have a particularly useful form. Moreover, the composite-$(2, \ell)$ modular curves $X_{G_2,G}$ have higher genus than we previously encountered. For example, the composite-$(2, 5)$ modular curve X_{G_2,G_9} has genus 5, which is higher than that of any curve we computed in Table A.1. We remark that curves with such composite level image of Galois possess more potential for abelian entanglement fields from a group theoretic perspective.

From conversations with David Zureick-Brown and Andrew V. Sutherland, there has been recent work in progress on determining the possible $3, 5,$ and 7-adic images of Galois. In joint work with Jeremy Rouse and David Zywina, the authors have constructed maps to the j-line for all the genus 0 and some of the genus 1 with positive rank modular curves of $3, 5,$ and 7 power level. This recent works leads to the following problem.

Problem 7.0.9. *Let* E *be a non-CM elliptic curve over* $\mathbf{Q}$ *with square discriminant. Find the possible indicies (and their frequencies) for simulataneously non-surjective composite-*$(2, \ell^n)$ *level image of Galois for* $\ell = 3, 5, 7$ *and* n *sufficiently large.*

Using the above data, one could construct modular curves as we previously did and attempt to classify their rational points. These composite-$(2, \ell^n)$ level modular curves will have models as hyperelliptic curves of high genera. Although the genera grows, this geometric property allows one to use more computational tools such as: bounds on $\operatorname{rk} \operatorname{Jac}(\mathbf{Q})$, evaluation of Weil-zeta functions, counting local points on Jacobians, and étale descent.

7.0.10 Entanglements

Finally, we pose problems relating to entanglement fields. As mentioned in the Remark in Section 6.1.8, we encounter computational hurdles in our analysis of mod 4 and mod 3 entanglement fields. One way to ameliorate this problem would be to construct a cover of our composite-$(4,3)$ level modular curves whose rational points classify ellipitic curves over $\mathbf{Q}$ with such entanglement. We also remark that when searching for mod 8 and mod 3 entanglement fields, we confront the same computational problems. Furthermore, we ask the following question.

Problem 7.0.11. *Determine if there exists a cover of the composite-*$(4,3)$ *level modular curves from Theorem 5.1.15 whose points correspond to elliptic curves over* $\mathbf{Q}$ *with mod 4 and mod 3 entanglement fields. If so, then determine the rational points on said curve. Furthermore, determine if there exists such covers of the composite-*$(8,3)$ *and composite-*$(16,3)$ *level modular curves.*

With solutions to Problem 7.0.9, we could ask a more "horizontally" flavored question, namely

Problem 7.0.12. *Determine the non-CM elliptic curves over* $\mathbf{Q}$ *that have mod 2 and mod* ℓ^n *abelian entanglement fields of degree 2 for* $\ell = 3,5,7$.

The technique for Problem 7.0.12 is analogous to that of Section 6.1, however, the computations will once again grow in difficulty. Using [Ade01], we can find smaller subfields of the ℓ^n-division fields and proceed as we did in Section 6.2.1.

Appendix

A.1 Tables for Theorem 5.1.12

In this appendix, we present the relevant tables for Theorem 5.1.12

Table A.1: Computations for composite $(2,5)$-level modular curves

G	Type	Equation for Model	Rational Points
G_9	$\mathbf{P}^1_{\mathbf{Q}}$		∞
G_4	Genus 2 hyperelliptic curve	$y^2 = (x+2)(x^2-20)(x^2+5x+5)$	$(-2,0)$
G_2	Genus 3 hyperelliptic curve	Not necessary	Not computed
G_1	Genus 5 hyperelliptic curve	Not necessary	Not computed
G_7	Genus 1 curve (not elliptic)	$y^2 = (8x^2-12x+7)(x^2+x-1)$	$\emptyset$
G_3	Genus 3 hyperelliptic curve	Not necessary	Not computed
G_8	Elliptic curve with rank zero	$y^2 = x^3+22x^2+125x$	$(0,0)$
G_6	Elliptic curve with rank zero	$y^2 = x^3-11x^2-x$	$(0,0)$
G_5	Elliptic curve with rank zero	$y^2 = x^3-11x^2-x$	$(0,0)$

Table A.2: Computations for composite $(2, 7)$-level modular curves

G	Type	Equation for Model	Rational Points
G_2	Genus 3 hyperelliptic curve	$y^2 = (x^3 - 2x^2 - x + 1)$ $(x^4 + 2x^3 - 9x^2 - 10x - 3)$	$\emptyset$
G_1	Genus 0 curve	Not necessary	$\emptyset$
G_7	$\mathbf{P}^1_{\mathbf{Q}}$		∞
G_5	Genus 2 hyperelliptic curve	$y^2 = -7(x^3 - 2x^2 - x + 1)$ $(x^3 - x^2 - 2x + 1)$	$\emptyset$
G_4	Genus 2 hyperelliptic curve	$y^2 = x(x + 1)(x^3 - 5x^2 - 8x - 1)$	$(0, 0), (0, -1)$
G_3	Genus 2 hyperelliptic curve	$y^2 = x(x - 1)(x^3 - 5x^2 - 8x - 1)$	$(0, 0), (0, -1)$
G_6	Genus 3 hyperelliptic curve	$y^2 = (64x^4 - 8x^3 + 3x^2 + 10x + 2)$ $(8x^3 + 8x^2 - 2x - 1)$	$(0, 3)$

Table A.3: Computations for composite $(2, 13)$-level modular curves

G	Type	Equation for Model	Rational Points
G_6	Elliptic curve with zero rank	$y^2 = x^3 + 6x^2 + 13x$	$(0, 0)$
G_1	Genus 5 hyperelliptic curve	Not necessary	Not computed
G_2	Genus 5 hyperelliptic curve	Not necessary	Not computed
G_3	Genus 5 hyperelliptic curve	Not necessary	Not computed
G_4	Elliptic curve with rank zero	Not necessary	Not computed
G_5	Elliptic curve with rank zero	Not necessary	Not computed

Table A.4: Computations for composite $(2, 11)$-level modular curves

G	Type	Equation for Model	Rational Points
G_1	Genus 0 curve	$x^2 + 1849$	$\emptyset$
G_2	Genus 0 curve	$x^2 + 24730729$	$\emptyset$
G_3	Genus 7 curve	(5.6.1)	$(2, 0, 0), ?$

A.2 Tables for Theorem 5.1.15

In this appendix, we present tables of data for Theorem 5.1.15 For Tables A.6 and A.8 we define the following elliptic curves:

$$\mathcal{E}_1\colon \begin{array}{c} y^2 = x^3 - 64902253044453104425107456x + \\ 191986392954657660058087864385226670080 \end{array},$$

$$\mathcal{E}_2\colon \begin{array}{c} y^2 = x^3 + 1340410876989014016x^2 + 177106467726008252502029 81 - \\ 24369854464x + 20183222015364729572390104581193239012822197007223357 44 \end{array},$$

$$\mathcal{E}_3\colon \begin{array}{c} y^2 = x^3 + 430718863653434975846 4x^2 + 54759035845044103198421100081 9 - \\ 2919253549056x + 21616888950779940925123976146397158102058265250894 \\ 80501104738304 \end{array},$$

$$\mathcal{E}_4\colon \begin{array}{c} y^2 = x^3 + 4946594365440x^2 + 76318058913079491601367 04x - \\ 350893557702179498927384423275954176 0 \end{array},$$

$$\mathcal{E}_5\colon \begin{array}{c} y^2 = x^3 + 230650788126150x^2 + 142767161544069038486922975 00x - \\ 130307013348668239100583626244805469625000 \end{array},$$

$$\mathcal{E}_6\colon \begin{array}{c} y^2 = x^3 + 6651780443200512x^2 + 894960602628788957256574776 1152x - \\ 205612320963061952367198624391648842627416064 0 \end{array},$$

$$\mathcal{E}_7\colon \begin{array}{c} y^2 = x^3 + 207868138850016x^2 + 873984963504676716070873804 8x - \\ 627479006845281837058101270726467415244 80 \end{array},$$

$$\mathcal{E}_8\colon\ y^2 = x^3 + 12991758678126x^2 + 34140037636901434221518508x - 153193116905586386000513005554845395880,$$

$$\mathcal{E}_9\colon\ \begin{array}{c} y^2 + 2176782336xy - 72857120983164885429450178 56y = x^3 - \\ 195177924725361868 80x^2 + 113884257337706588038077737207882317 82x - \\ 2000189454250339442572478745986318594403663273986202009 60 \end{array},$$

$$\mathcal{E}_{10}\colon\ y^2 = x^3 + 956871269597628x^2 - 18685767889415846670551494416x - 17879874443751930964575847005712682408845248.$$

Table A.5: Computations for composite $(2,3)$-level modular curves

(H, G)	Type	Equation for Model	Rational Points
(G_3, G_3)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(G_3, G_4)	Elliptic curve with rank zero	$y^2 = x^3 - 1728$	$(12, 0)$
(G_3, G_2)	Elliptic curve with rank zero	$y^2 = x^3 - 72x^2 - 432x$	$\emptyset$
(G_3, G_1)	Elliptic curve with rank zero	Not necessary	Not computed
(G_2, G_2)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(G_2, G_1)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(G_2, G_4)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(G_2, G_3)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(G_1, G_3)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(G_1, G_4)	Elliptic curve with rank zero	Not necessary	Not computed
(G_1, G_2)	Elliptic curve with rank zero	Not necessary	Not computed
(G_1, G_1)	Elliptic curve with rank zero	Not necessary	Not computed

Table A.6: Computations for composite $(4,3)$-level modular curves

(H_n, G)	Type	Equation for Model	Rational Points
$(H_9, \mathfrak{G})$	Elliptic curve with rank zero	$y^2 = x^3 - \frac{3}{8}x^2 + \frac{3}{64}x - \frac{9}{4095}$	$(12, 0)$
(H_9, G_3)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
$(H_{10}, \mathfrak{G})$	Elliptic curve with rank zero	$y^2 = x^3 - 8916100448256$	$\emptyset$
(H_{10}, G_3)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(H_{11}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_1$	$(-9,-4), (-1,4), (1,16), (-1,-4), (1,-16), (-9,4)$
(H_{11}, G_4)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(H_{11}, G_2)	Elliptic curve with rank zero	$\mathcal{E}_2$	$(-1,4), (-1,-4), (3,-4), (3,4)$
(H_{11}, G_1)	Genus 3 hyper-elliptic curve	Not necessary	Not computed
(H_{12}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_3$	$\emptyset$
(H_{12}, G_4)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(H_{12}, G_2)	Elliptic curve with rank zero	$\mathcal{E}_4$	$(-1/3,-8), (-1/3,8), (9,-8), (9,-8)$
(H_{12}, G_1)	Genus 3 hyper-elliptic curve	Not necessary	Not computed
(H_{13}, G_3)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
$(H_{13}, \mathfrak{G})$	Elliptic curve with rank zero	$y^2 = x^3 + 96x^2 + 3072x + 36864$	$(66,-24), (66,-24), (12,0)$
(H_{23}, G_3)	Elliptic curve with rank zero	Not necessary	Not computed
$(H_{23}, \mathfrak{G})$	Elliptic curve with rank zero	$y^2 + 16xy - 3072y = x^3 + 96x^2 + 3072x + 36864$	$(-15,3), (-15,-3), (12,0)$
(H_{24}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_5$	$\emptyset$

(H_{25}, G_3)	Elliptic curve with rank zero	Not necessary	Not computed
(H_{26}, G_3)	Elliptic curve with rank zero	Not necessary	Not computed
$(H_{26}, \mathfrak{G})$	Elliptic curve with rank zero	$y^2 = x^3 + 27x^2 + 243x$	$(0,-1), (0,1), (12,0)$
(H_{27}, G_3)	Elliptic curve with rank zero	Not necessary	Not computed
$(H_{27}, \mathfrak{G})$	Elliptic curve with rank zero	Not necessary	Not computed
(H_{60}, G_3)	Genus 39 curve	Not necessary	Not computed
$(H_{60}, \mathfrak{G})$	Genus 16 curve	Not necessary	Not computed

Table A.7: Computations for $X_{H_n,G_4}(24)$

(H_n, G)	Type	Equation for Model	Rational Points
(H_{28}, G_4)	Elliptic curve with rank zero	$y^2 = x^3 - 46656$	$(12,0)$
(H_{29}, G_4)	Genus 2 hyper-elliptic curve	$y^2 = -2x^6 + 2$	$(12,0)$
(H_{35}, G_4)	Elliptic curve with rank zero	$y^2 = x^3 - 5832$	$(12,0)$
(H_{39}, G_4)	Elliptic curve with positive rank	$y^2 = x^3 - \frac{8303765625}{32768}$	∞
(H_{41}, G_4)	Genus 2 hyper-elliptic curve	$y^2 = 2x^6 - 2$	$(12,0)$
(H_{43}, G_4)	Elliptic curve with rank zero	$y^2 = x^3 + 46656$	$(255,-6), (255,6), (12,0)$
(H_{45}, G_4)	Elliptic curve with positive rank	$y^2 = x^3 + \frac{20179187015625}{2097152}$	∞
(H_{47}, G_4)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(H_{49}, G_4)	Elliptic curve with rank zero	$y^2 = x^3 - 5832$	$(12,0)$
(H_{50}, G_4)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(H_{30}, G_4)	$\mathbf{P}^1_{\mathbf{Q}}$		∞

(H_{31}, G_4)	$\mathbf{P}^1_{\mathbf{Q}}$		∞
(H_{40}, G_4)	Genus 2 hyperelliptic curve	$y^2 = 2x^6 + 2$	$(20, -1/2), (20, 0)$, $(20, -1/4)$
(H_{70}, G_4)	Genus 2 hyperelliptic curve	$y^2 = 2x^6 - 2$	$(12, 0)$
(H_{89}, G_4)	Genus 2 hyperelliptic curve	$y^2 = x^6 - 4x^3 + 8$	$\emptyset$
(H_{91}, G_4)	Genus 2 hyperelliptic curve	$y^2 = x^6 + 8$	$(255, 2), (225, -2)$ $(255, 1), (255, -1)$
(H_{93}, G_4)	Genus 2 hyperelliptic curve	$y^2 = x^6 - 4x^3 + 8$	$\emptyset$
(H_{97}, G_4)	Genus 2 hyperelliptic curve	$y^2 = x^6 - 4x^3 + 8$	$(12, -1/2), (12, 0)$, $(12, 1/2)$

Table A.8: Computations for $X_{H_n, G_3}(24)$

(H_n, G)	Type	Equation for Model	Rational Points
(H_{37}, G_3)	Elliptic curve with rank zero		$\emptyset$
(H_{42}, G_3)	Elliptic curve with rank zero		$\emptyset$
(H_{32}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_6$	$(0, 0)$
(H_{33}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_7$	$(0, 0)$
(H_{34}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_8$	$(0, 0)$
(H_{36}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_9$	$(0, 4), (0, 0)$, $(0, -4)$
(H_{44}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_{10}$	$(0, 0)$
(H_{48}, G_3)	Elliptic curve with rank zero	$\mathcal{E}_{10}$	$(0, 0)$

A.3 Applicable subgroup diagrams for Theorem 5.1.12

In this appendix, we give diagrams depicting the lattice of applicable subgroups for $\mathrm{GL}_2(\mathbf{F}_\ell)$ for the primes $\ell = 2, 3, 5, 7, 11, 13$. We decorate the cases where we cannot provably analyze the rational points on the modular curve $X_{G_3,G}(2\cdot\ell)$ with a tilde. Also the subgroups are hyperlinked to their definition given in Section 5.1.

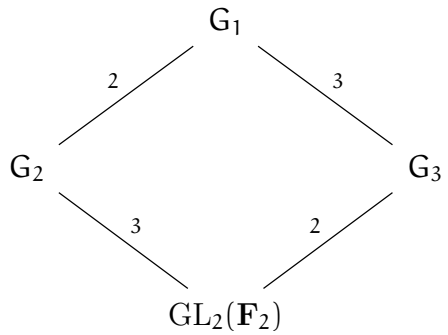


Figure A.1: Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{F}_2)$

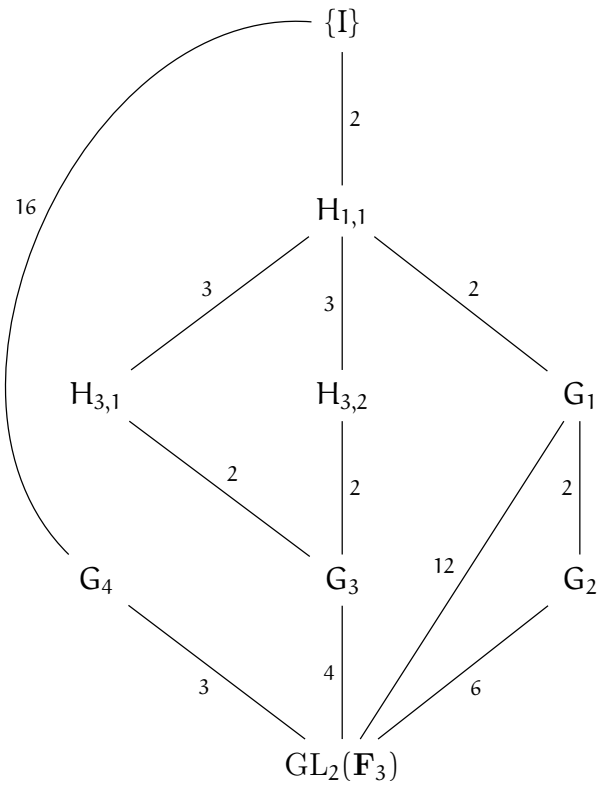


Figure A.2: Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{F}_3)$

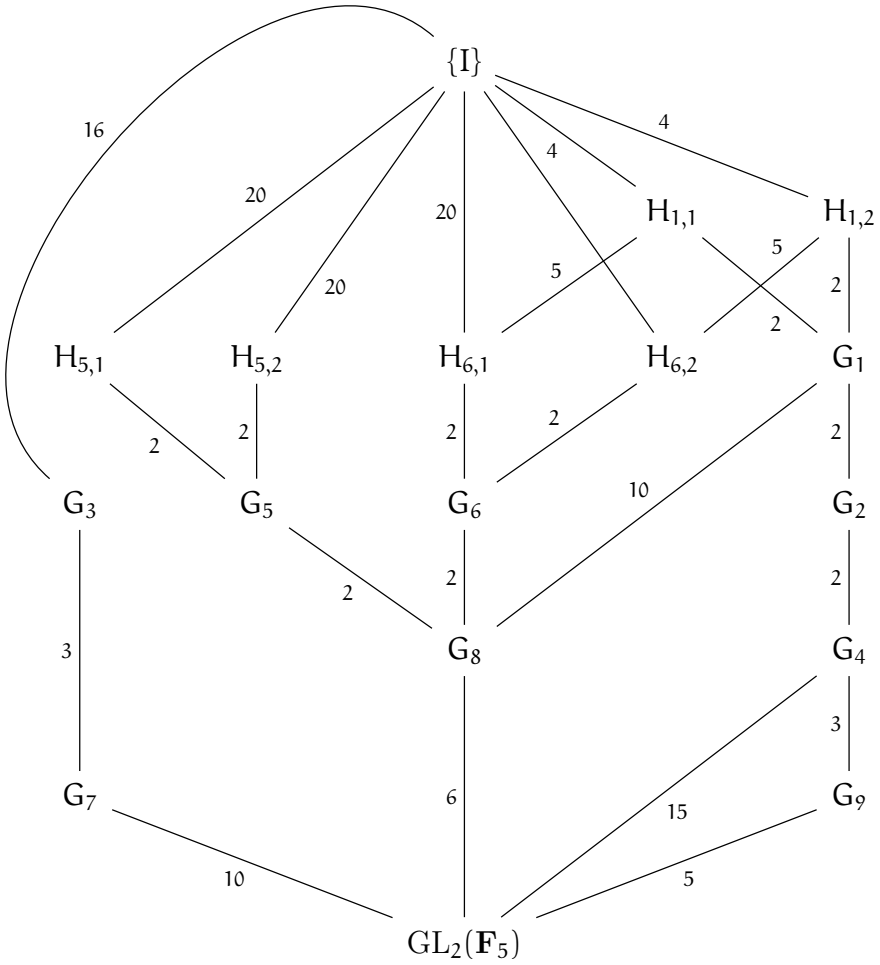


Figure A.3: Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{F}_5)$

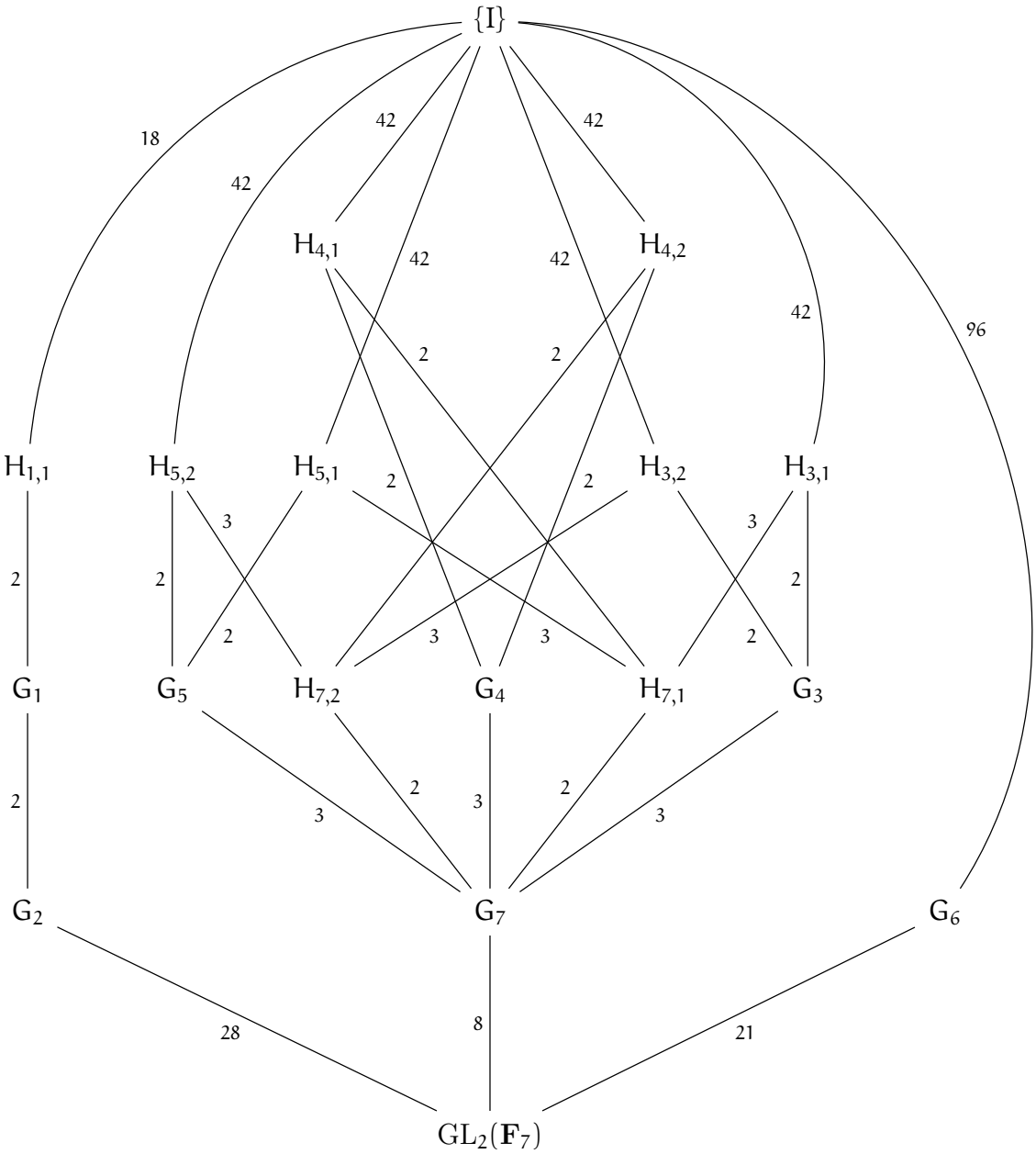


Figure A.4: Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{F}_7)$

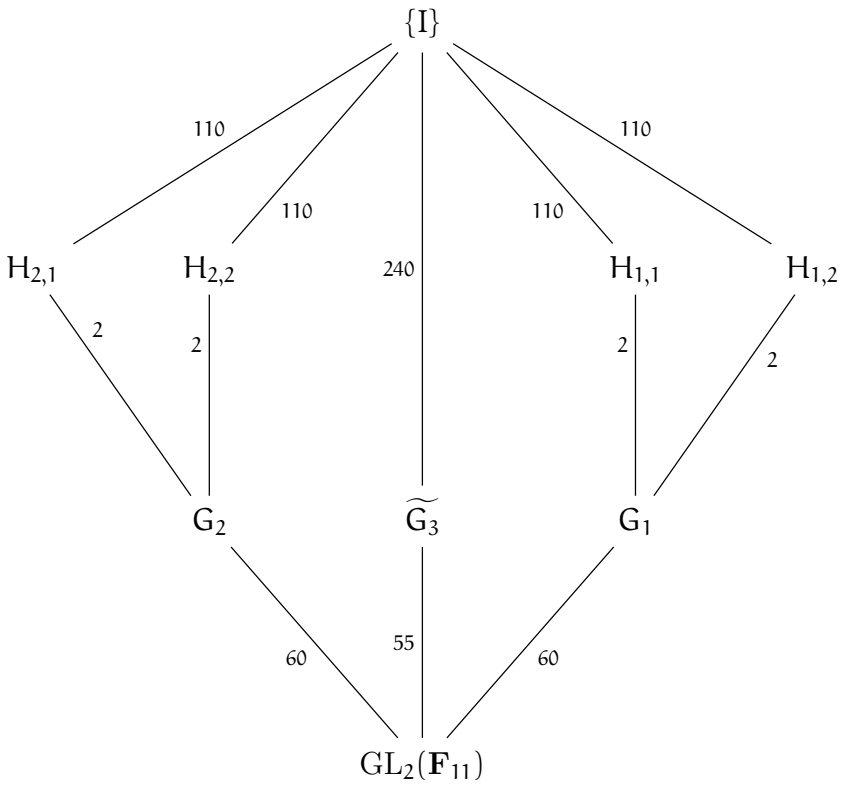


Figure A.5: Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{F}_{11})$

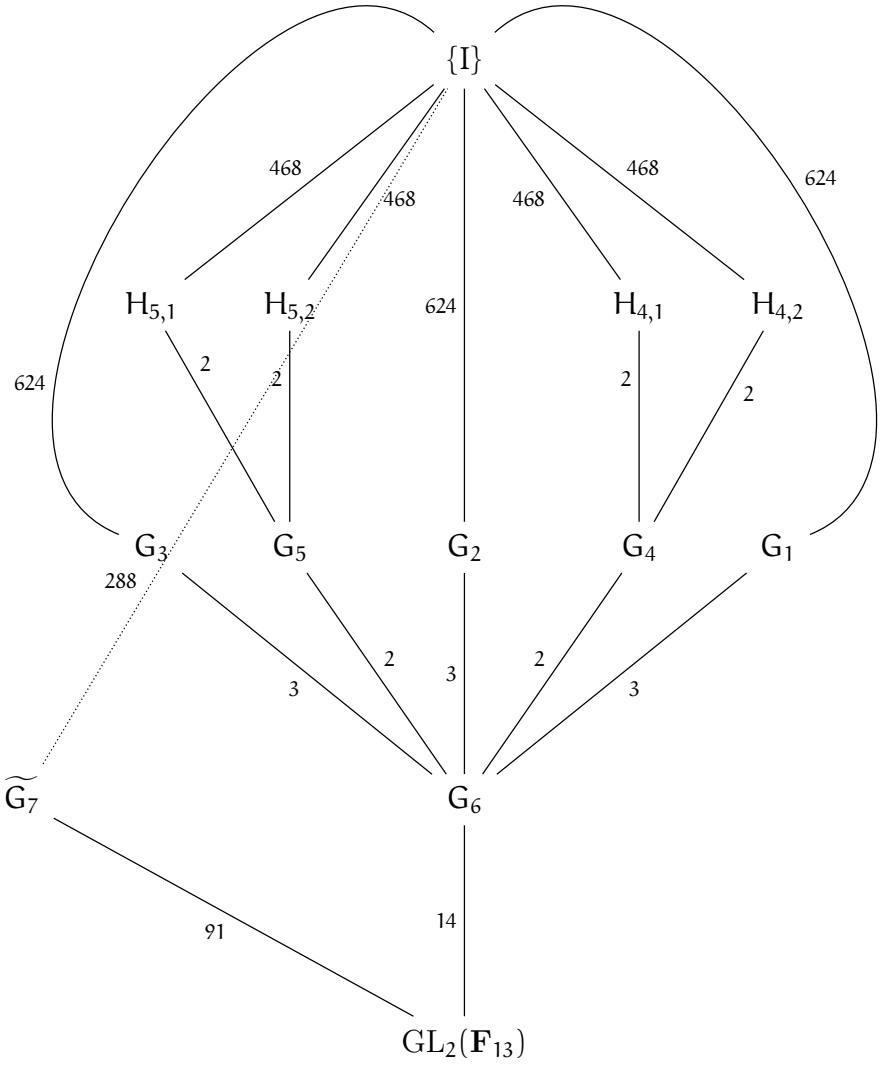


Figure A.6: Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{F}_{13})$

Bibliography

[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011. MR 1422373

[Ade01] Clemens Adelmann, *The decomposition of primes in torsion point fields*, vol. 1761, Springer Science & Business Media, 2001.

[Bar14] Burcu Baran, *An exceptional isomorphism between modular curves of level 13*, Journal of Number Theory **145** (2014), 273–300.

[BC14] Barinder Singh Banwait and John Cremona, *Tetrahedral elliptic curves and the local-global principle for isogenies*, preprint (2014).

[BJ16] Julio Brau and Nathan Jones, *Elliptic curves with 2-torsion contained in the 3-torsion field*, Proceedings of the American Mathematical Society **144** (2016), no. 3, 925–936.

[BPS12] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, preprint (2012).

[Bru03] Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.

[BS10] Nils Bruin and Michael Stoll, *The Mordell–Weil sieve: proving non-existence of rational points on curves*, LMS Journal of Computation and Mathematics **13** (2010), 272–306.

[BSS+16] Andrew R Booker, Jeroen Sijsling, Andrew V Sutherland, John Voight, and Dan Yasaki, *A database of genus 2 curves over the rational numbers*, preprint (2016).

[CG89] Kevin R Coombes and David R Grant, *On heterogeneous spaces*, Journal of the London Mathematical Society **2** (1989), no. 3, 385–397.

[Cho16] Michael Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, J. Number Theory **160** (2016), 603–628. MR 3425225

[Der12] Maarten Derickx, *Torsion points on elliptic curves and gonalities of modular curves*, Master's thesis Universiteit Leiden (2012).

[DKSS] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll, *Torsion points on elliptic curves over number fields of small degree*, in preparation (private communication).

[Duk97] William Duke, *Elliptic curves with no exceptional primes*, Comptes rendus de l'Académie des sciences. Série 1, Mathématique **325** (1997), no. 8, 813–818.

[DVH14] Maarten Derickx and Mark Van Hoeij, *Gonality of the modular curve* $\mathsf{X}_1(\mathsf{N})$, Journal of Algebra **417** (2014), 52–71.

[Fal94] Gerd Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182. MR 1307396

[Fre88] Georg Frey, *On the Selmer group of twists of elliptic curves with* $\mathbf{Q}$*-rational torsion points*, vol. XL, Canad. J. Math., 1988.

[FW01] E. Victor Flynn and Joseph L Wetherell, *Covering collections and a challenge problem of Serre*, Acta Arithmetica **98** (2001), no. 2,

197–205.

[Gau66] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, vol. 157, Yale University Press, 1966.

[Gre10] Aaron Greicius, *Elliptic curves with surjective adélic Galois representations*, Experimental Mathematics **19** (2010), no. 4, 495–507.

[Hal98] Emmanuel Halberstadt, *Sur la courbe modulaire* $\mathsf{X}_{\mathtt{ndép}}(\mathsf{11})$, Experimental Mathematics **7** (1998), no. 2, 163–174.

[HS00] Marc Hindry and Joseph H Silverman, *Diophantine geometry: an introduction*, vol. 201, Springer Science & Business Media, 2000.

[JKP06] Daeyeol Jeon, Chang Heon Kim, and Euisung Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), no. 1, 1–12. MR 2254548

[JKS04] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), no. 3, 291–301. MR 2069117

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Transactions of the American Mathematical Society **362** (2010), no. 3, 1547–1570.

[Kam92] Sheldon Kamienny, *Torsion points on elliptic curves and* q*-coefficients of modular forms*, Inventiones mathematicae **109** (1992), no. 1, 221–229.

[Kat80] Nicholas M Katz, *Galois properties of torsion points on abelian varieties*, Inventiones mathematicae **62** (1980), no. 3, 481–502.

[KL89] Victor A Kolyvagin and Dmitry Yu Logachëv, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–

196.

[KM+88] M.A. Kenku, F Momose, et al., *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J **109** (1988), 125–149.

[KSS] Sheldon Kamienny, William Stein, and Michael Stoll, *Torsion points on elliptic curves over quartic number fields*, preprint.

[Lan87] Serge Lang, *Elliptic functions*, Springer, 1987.

[LR13] Álvaro Lozano-Robledo, *On the field of definition of* $\mathfrak{p}$*-torsion points on elliptic curves over the rationals*, Mathematische Annalen **357** (2013), no. 1, 279–305.

[Mai03] James Mailhot, *Selmer groups for elliptic curves with isogenies of prime degree*, Ph.D. thesis, University of Washington, 2003.

[Maz77] Barry Mazur, *Rational points on modular curves*, Modular functions of one variable V, Springer, 1977, pp. 107–148.

[Mer96] Loic Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Inventiones mathematicae **124** (1996), no. 1, 437–449.

[Mor] Jackson S. Morrow, *Electronic transcript of computations for the manuscript "Elliptic curves over* $\mathbf{Q}$ *with non-surjective, composite image of Galois*, Available at https://www.dropbox.com/sh/hj52noxajkrckd6/AABeXoGzeg9cR3CKXhjjb_SSa?dl=0.

[MP07] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, preprint **11** (2007).

[Naj12] Filip Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(N)$, preprint (2012).

[Nér64] André Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Études Sci. Publ.Math. No.

21 (1964), 128.

[Par99] Pierre Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, Journal für die reine und angewandte Mathematik (Crelles Journal) **1999** (1999), no. 506, 85–116.

[Par03] ———, *No* 17*-torsion on elliptic curves over cubic number fields*, Journal de théorie des nombres de Bordeaux **15** (2003), no. 3, 831–838.

[Pet23] K. Petri, *Über die invariante Darstellung algebraischer Funktionen einer Veränderlichen.*, Mathematische Annalen **88** (1923), 242–289.

[PSS07] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2 + y^3 = z^7$, Duke Math. J. **137** (2007), no. 1, 103–158.

[Rib76] Kenneth A Ribet, *Galois action on division points of abelian varieties with real multiplications*, American Journal of mathematics (1976), 751–804.

[RS01] Karl Rubin and Alice Silverberg, *Mod 2 representations of elliptic curves*, Proceedings of the American Mathematical Society (2001), 53–57.

[RZB] Jeremy Rouse and David Zureick-Brown, *Electronic transcript of computations for the paper "Elliptic curves over* $\mathbf{Q}$ *and 2-adic images of Galois"*, Available at http://users.wfu.edu/rouseja/2adic/.

[RZB14] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over* $\mathbf{Q}$ *and 2-adic images of Galois*, accepted for publication in *Research in Number Theory*. (2014).

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae **15** (1972), no. 4, 259 331 (French).

[Sil09] Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer, 2009.

[Sko01] Alexei Skorobogatov, *Torsors and rational points*, no. 144, Cambridge University Press, 2001.

[Sto01] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277. MR 1829626 (2002b:11089)

[Sut12a] Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147. MR 2869053

[Sut12b] Andrew V. Sutherland, *Torsion subgroups of elliptic curves over number fields*, preprint (2012).

[Wan15] Jian Wang, *On the torsion strucutre of elliptic curves over cubic number fields*, Ph.D. thesis, University of Southern California, 2015.

[Was12] Lawrence C Washington, *Introduction to cyclotomic fields*, vol. 83, Springer Science & Business Media, 2012.

[Wet97] Joseph Loebach Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, University of California, Berkeley, 1997.

[Zyw10a] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bulletin of the London Mathematical Society **42** (2010), no. 5, 811–826.

[Zyw10b] ———, *Hilbert's irreducibility theorem and the larger sieve*, preprint (2010).

[Zyw11] ———, *On the surjectivity of mod ℓ representations associated to elliptic curves*, (preprint) (2011).

[Zyw15] ———, *On the possible images of the mod ℓ representations associated to elliptic curves over* $\mathbf{Q}$, Available at http://www.math.cornell.edu/~zywina/papers/PossibleImages/index.html.