Distribution Agreement

Signature:

Tomer Reiter

Date

Isogenies of Elliptic Curves and Arithmetical Structures on Graphs

By

Tomer Reiter

Doctor of Philosophy

Mathematics

David Zureick-Brown

Advisor

John Duncan

Committee Member

Raman Parimala

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the James T. Laney School of Graduate Studies

Date

Isogenies of Elliptic Curves and Arithmetical Structures on Graphs

By

Tomer Reiter

B.S., Carnegie Mellon University, 2015

M.AS., University of Cambridge, 2016

M.S., Emory University, 2018

Advisor: David Zureick-Brown, Ph.D.

An abstract of

A dissertation 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

Doctor of Philosophy

in Mathematics

2021

Abstract

Isogenies of Elliptic Curves and Arithmetical Structures on Graphs

By Tomer Reiter

In this thesis, we prove two results that come from studying curves. The first is a classification result about elliptic curves. Let $\mathbb{Q}(2^\infty)$ be the compositum of all quadratic extensions of $\mathbb{Q}$. Torsion subgroups of rational elliptic curves base changed to $\mathbb{Q}(2^\infty)$ were classified by Laska, Lorenz, and Fujita. Recently, Daniels, Lozano-Robledo, Najman, and Sutherland classified torsion subgroups of rational elliptic curves base changed to $\mathbb{Q}(3^\infty)$, the compositum of all cubic extensions of $\mathbb{Q}$. We classify cyclic isogenies of rational elliptic curves base changed to $\mathbb{Q}(2^\infty)$, for all but finitely many elliptic curves over $\mathbb{Q}(2^\infty)$.

Next we turn to arithmetical structures, which Lorenzini introduced to model degenerations of curves. Let G be a connected undirected graph on n vertices with no loops but possibly multiedges. Given an arithmetical structure $(\mathbf{r}, \mathbf{d})$ on G, we describe a construction which associates to it a graph G' on $n-1$ vertices and an arithmetical structure $(\mathbf{r}', \mathbf{d}')$ on G'. By iterating this construction, we derive an upper bound for the number of arithmetical structures on G depending only on the number of vertices and edges of G. In the specific case of complete graphs, possibly with multiedges, we refine and compare our upper bounds to those arising from counting unit fraction representations.

Isogenies of Elliptic Curves and Arithmetical Structures on Graphs

By

Tomer Reiter

B.S., Carnegie Mellon University, 2015

M.AS., University of Cambridge, 2016

M.S., Emory University, 2018

Advisor: David Zureick-Brown, Ph.D.

A dissertation 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
Doctor of Philosophy
in Mathematics
2021

Acknowledgments

I would like to begin by thanking my advisor David Zureick-Brown. He has guided me through the mathematical research process, offered invaluable advice throughout, and taught me much about arithmetic geometry. David suggested both of the problems that would eventually turn into the theorems in this thesis. I would also like to thank him, John Duncan, and Raman Parimala for being on my dissertation committee.

I would like to thank my collaborator and friend Chris Keyes for his contributions to the theorem on arithmetical structures. It was fantastic working on this problem with him, and it was also a pleasure organizing board game nights together.

I would also like to thank the graduate students who befriended me during my time at Emory, including Alexander Clifton, Brad Elliott, Jayanth Guhan, Maryam Khaqan, and Juvaria Tariq. I could not have done this research and written this dissertation without their help and kindness, and they provided a metaphorical shoulder to lean on.

To the PROMYS founders and especially Glenn Stevens, thank you for creating the program that would kindle my passion for mathematics.

Finally, I would like to thank the rest of my friends and my family for their support. To my grandmother, who said she "will sleep well tonight" knowing that I had successfully defended my thesis, thank you for your unwavering belief in my mathematical ability. To my parents, who took on the same stress as I did at times, thank you for your constant love and support. To my sister Ayelet, thank you for reassuring me in my times of distress, and for always supporting my career decisions. Lastly, thank you to my wife Campbell for always being there for me, having empathy for my mathematical and non-mathematical problems, and for helping me find my self-confidence when my research was challenging. I love you and I will do my best to always support your career the incredible way you have supported mine.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Arithmetic geometry began by asking the simple question "How do you find the integer solutions to polynomial equations?" As those with experience in mathematics will say however, simple does not mean easy. One polynomial equation that has been studied throughout history, at least as far back as Pythagoras and the Greeks, is $a^2 + b^2 = c^2$. We often learn small integral solutions to this equation in school, such as $a = 3, b = 4, c = 5$ and $a = 5, b = 12, c = 13$. One can even parametrize all positive integral solutions to this equation. To generate all solutions, we pick relatively prime $n, m \geq 1$ and set

$$a = n^2 - m^2, b = 2nm, c = n^2 + m^2.$$

It is possible to arrive at this parametrization purely algebraically. We will instead sketch a more insightful argument that generalizes to other conics.

By clearing denominators we see that integer solutions to $a^2 + b^2 = c^2$ can be thought of as rational solutions to $x^2 + y^2 = 1$. So we consider the latter equation, which we recognize as the unit circle. We know the point $P = (-1, 0)$ is on the curve and will use this point to generate all other rational points on the circle. Consider a line through P with slope t, $y = tx + t$. Whenever t is a rational number, the line will intersect the circle at a point with rational coordinates. Furthermore, the line through P and any rational point on the circle clearly has rational slope. We can then write every point on the circle in terms of a single rational parameter t. Rewriting $t = n/m$ will result in the parametrization above. This is one of the first examples of a proof in the field of arithmetic geometry. We use the geometric properties of the circle and projection onto the y-axis to find the arithmetic solutions to the equation.

There is much recent work and still much unknown in this field, capturing the interest of the entire mathematical community. Fermat's Last Theorem states that $x^n + y^n = z^n$ has no non-trivial integral solutions when $n > 3$. Fermat stated this around 1637, and famously claimed that he knew a proof that was too large to fit in the margin. Hundreds of years later, Wiles published a proof of the theorem [Wil95] using arithmetic geometry techniques and definitions that had since been developed. Among these definitions was that of elliptic curves, which is now a central object in arithmetic geometry. In the 1960s, Birch and Swinnerton-Dyer made a conjecture that the algebraic and analytic rank of an elliptic curve are equal. In 2000, this became one of the Clay Mathematics Institute's Millennium Prize Problems and consequently one of the most well-known open mathematical problems. While all curves are of interest in arithmetic geometry, since they are so central, we now define elliptic curves.

Definition. Concretely, an *elliptic curve* over a field K with characteristic not equal to 2 or 3 are the solutions to the equation

$$E\colon y^2 = x^3 + ax + b$$

for some $a, b \in K$, together with a abelian group structure on the solutions. We denote these points by $E(K)$. To add two points $P, Q \in E(K)$, take the line L from P to Q, take the third point of intersection with E, and reflect it over the x-axis.

Of course, to be precise we consider the projective version of E with a point at infinity. This point at infinity is the zero element of the group of points.

To be completely precise, an elliptic curve is a smooth, projective, algebraic curve of genus one, together with a specified base point.

In addition to having interest within the field of arithmetic geometry, elliptic curves have found applications in other areas. The most practical of these is in cryptography. One highly utilized form of encryption is RSA, which uses modular arithmetic to create public and private keys. The security of RSA comes from the fact that it is computationally hard to factor large numbers. In particular, it is easy to generate two large prime numbers and to compute powers of numbers modulo the product of these primes. If someone could factor this product, they could decrypt any encoded messages. Elliptic curve cryptography is a similar scheme of encryption, but uses elliptic curves instead. For elliptic curve cryptography, the security comes from the fact that given points P and Q on an elliptic curve, with Q an integer multiple of P, it is computationally challenging to determine the number n so that $[n]P = Q$.

1.2 Results

Our first result is a classification theorem concerning isogenies of elliptic curves. We prove the theorem from the perspective of Galois representations of elliptic curves. In Chapter 2, we discuss some bacgkround including the definition of isogenies and how the perspective of Galois representations is useful in proving classification theorems of this type. In Chapter 3, we discuss previous work related to the result and prove the following theorem.

Theorem 3.1.1. Let E be an elliptic curve over $\mathbb{Q}$ without CM, and E' be its base change to $\mathbb{Q}(2^\infty)$. Then for all but finitely many E', the set of possible degrees of $\mathbb{Q}(2^\infty)$-rational cyclic isogenies of E' is

$$\{n \in \mathbb{Z} | 1 \leq n \leq 18, \text{ or } n = 20, 21, 24, 25, 27, 32, 36, 37\}.$$

Next, we turn our attention to bounding the number of arithmetical structures on graphs. In Chapter 4, we provide some brief background on graph theory. In Chapter 5, we prove the following theorem.

Theorem 5.1.1. Let G be a connected, undirected graph on n vertices, with no loops but possible multiedges. Then the following is an upper bound for the number of arithmetical structures on G.

$$\#A(G) \leq \frac{n!}{2} \cdot \#E(G)^{2^{n-2}-1} \cdot \#E(G)^{2^{n-1} \cdot \frac{1.538 \log(2)}{(n-1)\log(2)+\log(\log(\#E(G)))}}.$$

Chapter 2

Background - Isogenies of Elliptic Curves

In 1977, Mazur [Maz77a] proved that there are precisely 15 possible torsion subgroups for an elliptic curve over $\mathbb{Q}$. This set off a series of classification theorems for elliptic curves. We discuss some of these generalizations to this classification in Chapter 3. One could unify all of these problems through the lens of Galois representations. In particular, one could ask the following question.

Question 2.0.1 (Mazur's Program B)**.** Given a "nice" field $K/\mathbb{Q}$, and a subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, classify the elliptic curves E whose Galois representation ρ_E satisfies $\mathrm{im}(\rho_E) \subseteq G$.

Part of answering the question involves defining what a "nice" field is in this context. In the next two chapters, we will make a case that the field $\mathbb{Q}(2^\infty)$, and more generally $\mathbb{Q}(d^\infty)$ for all d, should be considered "nice" fields. In this background chapter we recall definitions and theorems about elliptic curves, their isogenies, and their Galois representations. We will see how an answer to Mazur's Program B can be translated to an answer to many other classification theorems.

Notably, much progress on Question 2.0.1 has been made recently. Specific cases of interest have been analyzed, for example by Bilu, Parent, and Robolledo in [BPR13]. The case of 2-adic images was completed by Rouse and Zureick-Brown [RZB15], and the general ℓ-adic case is in preparation by Rouse, Sutherland, and Zureick-Brown [RSZB]. In the next chapter, we will show how a partial answer to Question 2.0.1 for $K = \mathbb{Q}$ is enough to give a classification result for isogenies of elliptic curves over $\mathbb{Q}(2^\infty)$.

2.1 Elliptic Curves

In this section, we will recall some of the facts about elliptic curves most relevant to our discussion. If the reader is comfortable with torsion subgroups, isogenies, j-invariants, and twists, they are encouraged to proceed to the next section.

We now turn to the foundational structure theorem for elliptic curves over $\mathbb{Q}$. If this theorem is unfamiliar to the reader, we encourage them to look to [ST15] to learn about elliptic curves.

Definition. Let $K/\mathbb{Q}$ be a field and E an elliptic curve over K. We define $E[n]$ to be the n-torsion points of E over $\overline{\mathbb{Q}}$, that is the points of E which have order dividing n in the group.

Note that since the group law for elliptic curves is defined by birational polynomials, $E[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$.

Theorem 2.1.1 (Mordell's Theorem)**.** *Given an elliptic curve E, the group of rational points of E over $\mathbb{Q}$ is a finitely generated abelian group.*

In particular, we can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$, where $r < \infty$ is the rank of the elliptic curve and T is the torsion subgroup, a finite abelian group. The cornerstone classification result for elliptic curves concerns this torsion subgroup. We state it here, and in the next section we will see how this can be interpreted as a consequence of an answer to Mazur's Program B.

Theorem 2.1.2 (Mazur's Theorem)**.** *Let E be an elliptic curve and T its torsion subgroup over $\mathbb{Q}$. Then T is isomorphic to one of the following groups.*

- $\mathbb{Z}/n\mathbb{Z}$ *with* $1 \leq n \leq 10$ *or* $n = 12$.
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ *with* $1 \leq n \leq 4$.

Note that so far this discussion has been for elliptic curves over $\mathbb{Q}$. The Mordell-Weil Theorem [Wei29] generalized Mordell's Theorem [Mor22] to arbitrary number fields. This generalization also applies to arbitrary abelian varieties, but this will be less of a concern for our discussion. Mazur's Theorem [Maz77a] has also been generalized for elliptic curves over larger fields, which we will discuss further in the next chapter. We now discuss various equivalences of elliptic curves.

Definition. Let E be an elliptic curve over $\mathbb{Q}$ in Weierstrass form $y^2 = x^3 + ax + b$. Then the *$j-$invariant* is defined by

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

One can also define the j-invariants for elliptic curves not in Weierstrass form. The j-invariant is useful in many ways, but we will primarily be using it due to the following theorem.

Theorem 2.1.3. *Given two elliptic curves defined over $\mathbb{Q}$, there is an isomorphism of varieties between them defined over $\overline{\mathbb{Q}}$ if and only if their j-invariants are equal. [Sil09]*

In light of this, we further look into isomorphic elliptic curves.

Definition. Given elliptic curves E and E' over $\mathbb{Q}$, we say E' is a *twist* of E if they are isomorphic over $\overline{\mathbb{Q}}$. Let E be in Weierstrass form with equation $y^2 = x^3 + ax + b$. Then the *quadratic twist of E by d* is $dy^2 = x^3 + ax + b$. We will denote this by E^d.

In fact, every twist of an elliptic curve whose j-invariant is not equal to 0 or 1728 is a quadratic twist [Sil09]. The j-invariants corresponding to elliptic curves with complex multiplication are 0 and 1728, which will not be our primary interest. Note that over $\mathbb{Q}(\sqrt{d})$, there is an isomorphism between E and E^d taking (x, y) to $(x, y/\sqrt{d})$. Thus, in particular, any isomorphism of non-CM elliptic curves is defined over the compositum of all of the quadratic extensions of $\mathbb{Q}$. This field is precisely $\mathbb{Q}(2^\infty)$, and we will return to this fact in the next chapter.

We next turn our attention to isogenies.

Definition. Let E_1 and E_2 be elliptic curves. An *isogeny* is a morphism of curves $\phi\colon E_1 \to E_2$ which satisfies $\phi(O) = O$, where O is the identity element of the group of points on the corresponding elliptic curve. The *degree* of ϕ is its degree as a morphism of curves.

Remark. Note that isogenies are also group homomorphisms. This is proved directly in [Sil09]. Furthermore, every morphism of curves is either constant or surjective. We will only be interested in non-constant isogenies, so all of our isogenies will be surjective.

2.2 Galois Representations of Elliptic Curves

In this section, we will define a very useful tool for answering the classification questions discussed to this point, which is Galois representations. We will then shift our point of view by using these Galois representations and see why an answer to Question 2.0.1 would for example give us a proof of Mazur's Theorem 2.1.2.

Let $K/\mathbb{Q}$ be a field and E an elliptic curve. As mentioned in Section 2.1, $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and in particular the n-torsion points are defined by some polynomial equation. Hence, we get an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K) = G_K$ on $(\mathbb{Z}/n\mathbb{Z})^2$. Here we can write this as a representation

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

Definition. The *mod n Galois representation associated with E* is $\rho_{E,n}$ as defined above. The *ℓ-adic Galois representation*

$$\rho_{E,\ell^\infty}\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is defined by taking the inverse limit of $\rho_{E,n}$ with n ranging over powers of ℓ. By taking the inverse limit instead over all n, we get the *Galois representation*

$$\rho_E\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Next, we define some distinguished possibilities for the images of these Galois representations.

Definition. We define each of the following up to conjugacy. The *Borel* mod n, $B(n) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is the group of upper triangular matrices. We also define

$$B_1(n) = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

We will repeatedly use the fact that an elliptic curve over K has a K-rational cyclic isogeny of degree n if and only if the image of its Galois representation is contained in $B(n)$. It is also true that an elliptic curve has a K-rational n-torsion point if and only if the image of its Galois representation is contained in $B_1(n)$. We will give brief explanations for one direction of these implications. We fix two points

P and Q which generate $E[n]$ such that given $\sigma \in G_K$ and

$$\rho_{E,n}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we have $\sigma(P) = aP + cQ$ and $\sigma(P) = bP + dQ$.

Let E be an elliptic curve a K-rational n-torsion point. Then for all $\sigma \in G_K$, we have $\sigma(P) = P$, since $P \in E(K)$ and in particular G_K fixes P. Thus, $\text{im}(\rho_{E,n}) \subseteq B_1(n)$.

Now let E be an elliptic curve with a K-rational cyclic isogeny, that is an isogeny $\phi\colon E \to E'$ with $\ker\phi$ being a cyclic subgroup of E generated by P over $\overline{\mathbb{Q}}$. Then $\sigma(P) \in \ker(\phi)$ and so is a multiple of P. Hence, $\text{im}(\rho_{E,n}) \subseteq B(n)$.

These generate some strong reasons why an answer to Question 2.0.1 would be so significant. A complete answer would also give a full classification of orders of torsion points of elliptic curves over any fixed field $K/\mathbb{Q}$. In particular, given a field K, there is an elliptic curve E with a torsion point of order n if and only if there is an elliptic curve with a Galois representation whose image is contained in $B(n)$ after reducing modulo n. One can further refine the subgroup $B(n)$ to identify which torsion subgroups arise. Similarly, a solution to Mazur's Program B 2.0.1 would classify the possible degrees of K-rational cyclic isogenies for a fixed K. As we will see in the next chapter, much progress has been made on Question 2.0.1 over $\mathbb{Q}$. We will see how even this answer is enough to classify isogenies of elliptic curves over $\mathbb{Q}(2^\infty)$.

Here we provide some intuition as to why considering classification problems through the lens of Galois representations is also tractable.

Theorem 2.2.1 (Serre, [Ser72]). *Let E be an elliptic curve over a number field K without complex multiplication.Then the image of its Galois representation in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is open.*

Note that with the topology of $\widehat{\mathbb{Z}}$, this in particular means that the index of $\rho_E(G_K)$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is finite. Hence, for large primes ℓ, $\rho_{E,\ell}$ is surjective. Now assume that there was a fixed, relatively small, bound B such that for all $\ell > B$, all elliptic curves have surjective mod ℓ Galois representations. Then we could give an answer to Question 2.0.1 by computing the answer explicitly for possible images mod small primes and in some cases their powers. This in itself is a challenging problem, and we will discuss some of the progress on this problem in the next chapter.

In fact, we have the following conjectures.

Conjecture. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then for all primes $\ell > 37$, $\rho_{E,\ell}$ is surjective.

In practice, it is enough to consider the primes up to 13, and note some exceptional cases at $\ell = 17$ and $\ell = 37$. We will see this come up in the next chapter.

This leaves us with the problem of classifying elliptic curves with prescribed mod ℓ image of Galois. To tackle this problem, we turn to modular curves. We recall the classical modular curves.

Definition. Let $N \geq 1$. Then we define the following congruence subgroups.

$$\Gamma_0(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \colon \gamma \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \colon \gamma \equiv \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \colon \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

Recall that congruence subgroups have an action on the upper half plane $\mathbb{H}$ by linear fractional transformations. Let Γ be one of the congruence subgroups above. Then taking the quotient of this action, $\mathbb{H}/\Gamma$, forms a modular curve after compactifying. Taking $\Gamma = \Gamma_0(N), \Gamma_1(N), \Gamma(N)$ produces the modular curves $X(N), X_0(N), X_1(N)$ respectively. The points of $X_1(N)$ are roughly in correspondence with elliptic curves together with a specified torsion point of order N. The points of $X_0(N)$ are roughly in correspondence with elliptic curves together with a cyclic isogeny corresponding to a cyclic subgroup of order N. Finally, $X(N)$ classifies elliptic curves together two torsion points which generate $E[N]$. Viewing modular curves in this way, one can define modular curves algebraically, see for example [DI95].

Chapter 3

Isogenies of Elliptic Curves over $\mathbb{Q}(2^\infty)$

3.1 Introduction

The structure of elliptic curves is one of the most studied aspects of arithmetic geometry. This area of research began with Mordell's Theorem [Mor22], which states that the group of rational points on an elliptic curve is a finitely-generated abelian group. The Mordell-Weil theorem [Wei29] generalizes this to arbitrary abelian varities over number fields, and in particular to elliptic curves over number fields. One goal that came about from these results is classifying the possibilities for the torsion structure of elliptic curves. Over $\mathbb{Q}$, Mazur [Maz77a] proved such a classification over $\mathbb{Q}$, giving a list of 15 abelian groups which can appear as the torsion group of a rational elliptic curve.

There has also been progress on these questions over other number fields. Kenku and Momose [KM88] began classifying torsion structures of elliptic curves over arbitrary quadratic number fields, and Kamienny [Kam86] completed the classification. In fact, there are only a finite number of possibilities of torsion structures over arbitrary quadratic number fields. There are also results of this type for cubic fields, see for example Jeon, Kim and Schweizer [JKS04] and Jeon, Kim and Lee [JKL11]. The classification has since been completed by Derickx, Etropolski, Morrow, and Zureick-Brown [DEMZB20]. Furthermore, one can refine all of these results by instead considering elliptic curves over $\mathbb{Q}$ base changed to these number fields, see for example Chou [Cho19], Lozano-Robledo [LR13] [LR18] and Najman [Naj16].

There has also been progress recently in studying torsion structures of rational elliptic curves base changed to specific infinite extensions of $\mathbb{Q}$. Namely to the fields $\mathbb{Q}(d^\infty)$ which are defined as the compositum of all number fields of degree d. The possible torsion subgroups for rational elliptic curves base changed to $\mathbb{Q}(2^\infty)$ were classified by Laska and Lorenz [LL85], and Fujita [Fuj04], [Fuj05], of which it turns out there are only finitely many possibilities. Furthermore a similar classification has been done for $\mathbb{Q}(3^\infty)$ by Daniels, Lozano-Robledo, Najman and Sutherland [DLRNS18].

The question of classifying isogenies of elliptic curves has also been considered. Many have contributed to this problem, and Kenku [Ken82] completed the classification. We can unify all of these questions about torsion and isogenies through the lens of Galois representations. For each elliptic curve E, we have an associated Galois representation $\rho_E\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\widehat{\mathbb{Z}})$. Mazur's Program B [Maz77b] is an ongoing attempt to classify elliptic curves over a fixed number field with prescribed image of its Galois representation. This generalizes classifying torsion structures, as having an n-torsion point is equivalent to having mod n image of Galois contained in a certain subgroup of $\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$. From this perspective, a natural next classification question is to classify cyclic isogenies of elliptic curves over larger fields, as this is equivalent to having an image of Galois contained in the Borel modulo the degree of the isogeny. Over $\mathbb{Q}$ there has already been much progress on Mazur's Program B, by for example Rouse and Zureick-Brown [RZB15] and Rouse, Sutherland, and Zureick-Brown [RSZB].

In this chapter, we use the ideas from Mazur's Program B to classify cyclic isogenies of rational elliptic curves base changed to $\mathbb{Q}(2^\infty)$. Note that for the fields $\mathbb{Q}(d^\infty)$ with $d > 1$, quadratic twists of elliptic curves become isomorphic. In particular, over these fields any pair of elliptic curves with the same j-invariant with $j \neq 0, 1728$ are isomorphic. With this in mind, we can state the following.

Theorem 3.1.1. *Let E be an elliptic curve over $\mathbb{Q}$ without CM, and E' be its base change to $\mathbb{Q}(2^\infty)$. Then for all but finitely many E', the set of possible degrees of $\mathbb{Q}(2^\infty)$-rational cyclic isogenies of E' is*

$$\{n \in \mathbb{Z} | 1 \leq n \leq 18, \ \textit{or } n = 20, 21, 24, 25, 28, 32, 36, 37\}.$$

Remark. The degrees above which do not already appear as the degree of a cyclic isogeny of an elliptic curve over $\mathbb{Q}$ are $20, 24, 28, 32, 36$. [Ken82] For each of the degrees $20, 24, 32, 36$, there are infinitely many elliptic curves which have this degree of an isogeny over $\mathbb{Q}(2^\infty)$. There are only finitely many elliptic curves over $\mathbb{Q}(2^\infty)$ with a 28-isogeny.

In Section 3.2, we discuss the effect on the image of Galois of base changing to $\mathbb{Q}(2^\infty)$. In Section 3.3, we prove that there cannot be isogenies with degrees equal to powers of large primes. In Sections 3.4 and 3.5, we examine what happens at smaller primes. Finally, we consider the remaining degrees in Section 3.6 to conclude Theorem 3.1.1.

3.2 The Image of Galois After Base Change

We recall the setup for Galois representations of elliptic curves. For E an elliptic curve, over $\mathbb{Q}$ or $\mathbb{Q}(2^\infty)$, as usual we define $E[n] = E(\overline{\mathbb{Q}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. Then we have a Galois representation mod n for E, denoted

$$\rho_{E,n}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(E[n]) \cong \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

For each prime ℓ there is a corresponding ℓ-adic Galois representation whose codomain is $\operatorname{GL}_2(\mathbb{Z}_\ell)$, obtained by taking an inverse limit.

As usual, for any of the above, we define the Borel subgroup to be any subgroup of $\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})$ conjugate to the group of upper triangular matrices, and the split Cartan to be any subgroup conjugate to the group of diagonal matrices. We will denote the Borel subgroup by $B(n)$. When $n = \ell$ is prime, we also define, up to conjugacy, the non-split Cartan to be a subgroup of matrices isomorphic to $\mathbb{F}_{\ell^2}^\times$, which we denote $N_{ns}(\ell)$. We recall the fact that the mod n image of Galois for an elliptic curve E is contained in $B(n)$ if and only if E has an isogeny of degree n. Here and throughout this article, by isogeny we mean K-rational cyclic isogeny for the appropriate field K.

This allows us to shift perspectives; instead of classifying elliptic curves with prescribed isogenies we will classify elliptic curves with prescribed images of Galois. Since we are considering rational elliptic curves, it suffices to classify the elliptic curves whose images of Galois corresponding to the curves having an isogeny over $\mathbb{Q}(2^\infty)$. Then the problem is reduced to finding all points on the corresponding modular curves X_H. Following [RZB15], we define $Y(n), X(n)$ to be the moduli space parametrizing elliptic curves and its smooth compactification, respectively and we define X_H to be the quotient of $X(n)$ by H. By Lemma 2.1 in [RZB15], an elliptic curve E has image of Galois contained in a subgroup conjugate to H if and only if there is an ι such that $(E, \iota) \in X_H(\mathbb{Q})$. In this paper, Rouse and Zureick-Brown give a complete classification of the possible 2-adic images of Galois over $\mathbb{Q}$, and classify the rational points on the corresponding curve. Much work has been done to this effect by Bilu, Parent, Robolledo [BPR13] and Rouse, Sutherland, Zureick-Brown [RSZB] and others for all primes up to 13. We will leverage these classifications to study isogenies of elliptic curves over $\mathbb{Q}(2^\infty)$.

So, we first examine in general how the image of Galois of an elliptic curve $E/\mathbb{Q}$ changes when we base change E to $\mathbb{Q}(2^\infty)$.

Lemma 3.2.1. *Let E be an elliptic curve, E' its base change to $\mathbb{Q}(2^\infty)$ and let $n > 1$. Denote by G the image of $\rho_{E,n}$, and H the image of $\rho_{E',n}$. Then H is normal in G and $G/H \cong (\mathbb{Z}/2\mathbb{Z})^m$, where m is maximal among quotients of G of this form.*

Proof. First we prove the quotient is of this form. As noted above, we have the diagram:

$$\begin{tikzcd}
& \mathbb{Q}(2^\infty)(E[n]) \arrow[dl, dash, "H"'] \arrow[dr, dash, "(\mathbb{Z}/2\mathbb{Z})^\infty"] & \\
\mathbb{Q}(2^\infty) \arrow[dr, dash, "(\mathbb{Z}/2\mathbb{Z})^\infty"] & & \mathbb{Q}(E[n]) \arrow[dl, dash, "G"'] \\
& \mathbb{Q} &
\end{tikzcd}$$

First note that it is clear that H is a normal subgroup of G, this follows from general Galois theory. Now let $L = \mathbb{Q}(E[n]) \cap \mathbb{Q}(2^\infty)$. Then we claim we have the following diagram:

$$\begin{tikzcd}
& L(E[n]) \arrow[dl, dash, "H"'] \arrow[dr, dash] & \\
L \arrow[dr, dash] & & \mathbb{Q}(E[n]) \arrow[dl, dash, "G"'] \\
& \mathbb{Q} &
\end{tikzcd}$$

that is, that $\mathrm{Gal}(L(E[n])/L) \cong H$. In fact, it suffices to show this claim as then we can use finite Galois theory.

So, it suffices to show that the Galois group in the bottom right of the diagram:

$$\begin{tikzcd}
 & \mathbb{Q}(2^\infty)(E[n]) \arrow[dl, dash, "H"'] \arrow[dr, dash, "(\mathbb{Z}/2\mathbb{Z})^\infty"] & \\
\mathbb{Q}(2^\infty) \arrow[dr, dash, "(\mathbb{Z}/2\mathbb{Z})^\infty"] & & L(E[n]) \arrow[dl, dash] \\
 & L &
\end{tikzcd}$$

is isomorphic to H. Note that $\mathbb{Q}(2^\infty)\cap L(E[n]) = \mathbb{Q}(2^\infty)\cap\mathbb{Q}(E[n])\cap\mathbb{Q}(2^\infty)(E[n]) = L$. So take $\sigma \in \mathrm{Gal}(L(E[n])/L)$. This extends to an element of $\mathrm{Gal}(\mathbb{Q}(2^\infty)(E[n])/\mathbb{Q}(2^\infty))$ as for each $\alpha \in \mathbb{Q}(2^\infty)(E[n])$, we can extend σ to $\mathrm{Gal}(L(E[n],\alpha)/L(\alpha))$ again by using finite Galois theory.

Now we show that G/H is $\mathbb{Z}/2\mathbb{Z}$ to the maximal power among quotients of G of this form. By the above it suffices to consider the following diagram.

$$\begin{tikzcd}
 & L(E[n]) \arrow[dl, dash, "H"'] \arrow[dr, dash, "\text{trivial}"] & \\
L \arrow[dr, dash, "(\mathbb{Z}/2\mathbb{Z})^m"'] & & \mathbb{Q}(E[n]) \arrow[dl, dash, "G"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Assume for sake of contradiction m is not maximal among quotients of G of this form. Then there is a subgroup $H' \subsetneq H$ of index 2, with H' normal in G and $G/H' \cong (\mathbb{Z}/2\mathbb{Z})^{m+1}$. So by the fundamental theorem of Galois theory there is an L' with $L \subsetneq L' \subseteq \mathbb{Q}(2^\infty)$ such that $[L' \colon L] = 2$. Then $\mathrm{Gal}(L'/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{m+1}$, so $L' \subseteq \mathbb{Q}(2^\infty)$, but it this is a contradiction since $L = \mathbb{Q}(2^\infty) \cap \mathbb{Q}(E[n])$. $\square$

We will use this lemma to first prove that for all primes $\ell \geq 17$, there are no degree ℓ isogenies in our setting, except for four exceptional j-invariants corresponding to $\ell = 17, 37$ for which the corresponding elliptic curves already had degree ℓ isogenies over $\mathbb{Q}$. For primes $\ell \leq 13$, for each possible image of Galois mod ℓ or a power of ℓ over $\mathbb{Q}$, we compute the new image of Galois over $\mathbb{Q}(2^\infty)$. In particular we are interested in the case where the image of Galois over $\mathbb{Q}$ was not contained in a Borel but over $\mathbb{Q}(2^\infty)$ it is. We make the following definition.

Definition 3.2.2. Let E be an elliptic curve without CM over $\mathbb{Q}$, n a positive integer, $G = \rho_{E,n}(G_\mathbb{Q})$. Also let E' be the base change of E to $\mathbb{Q}(2^\infty)$, and $H = \rho_{E',n}(G_{\mathbb{Q}(2^\infty)})$. If $G \not\subseteq B(n)$ and $H \subseteq B(n)$ then we say that E is **superficial** and G is **peripheral**.

So to rephrase the above, we will prove for all $\ell > 17$ there are no peripheral subgroups of $GL_2(\mathbb{F}_\ell)$. For primes $\ell \leq 13$ and all such powers, we classify the peripheral groups whose corresponding modular curves have a non-CM point, in other words all groups corresponding to some rational elliptic curve without CM. For a full classification of isogenies, we would then need to begin by computing all products of two groups corresponding to powers of distinct primes less than or equal to 13, where one subgroup is peripheral and the other is either peripheral or contained in a Borel. We compute the genus of the modular curves corresponding to these curves to conclude Theorem 3.1.1.

In the remaining sections we will classify the possible prime power degrees of isogenies for this set of all but finitely many elliptic curves.

3.3 Large Primes

Throughout, let E be an elliptic curve without complex multiplication. For primes $\ell \geq 17$, except for the four exceptional j-invariants, the ℓ-adic image of Galois of an elliptic curve is either surjective or contained in the normalizer of a non-split Cartan, see for example Proposition 1.13 in [Zyw15]. In the latter case, the index of the image in the normalizer of the non-split Cartan is at most 3. So, it suffices to prove that the maximal quotient, isomorphic to a power of $\mathbb{Z}/2$, of any such subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is not contained in $B(\ell)$.

Lemma 3.3.1. *Let $\ell \geq 17$ and assume $\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_\ell)$. Let E' denote the base change of E to $\mathbb{Q}(2^\infty)$. Then $\rho_{E',\ell}(G_{\mathbb{Q}(2^\infty)}) \not\subseteq B(\ell)$.*

Proof. Denote $G = \rho_{E,\ell}(G_{\mathbb{Q}})$ and $H = \rho_{E',\ell}(G_{\mathbb{Q}(2^\infty)})$. Then by Lemma 3.2.1 we have $G/H \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some m. We claim that $m = 1$. The map $\mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^m$ given by reduction modulo H is a surjection. Since the image is abelian, this map factors through the abelianization of $\mathrm{GL}_2(\mathbb{F}_\ell)$, which we denote by A. We claim $A \cong \mathbb{F}_\ell^\times$. By Theorem 8.3 in [Lan02], we have that the commutator $[\mathrm{SL}_2(\mathbb{F}_\ell), \mathrm{SL}_2(\mathbb{F}_\ell)] = \mathrm{SL}_2(\mathbb{F}_\ell)$. Thus, $[\mathrm{GL}_2(\mathbb{F}_\ell), \mathrm{GL}_2(\mathbb{F}_\ell)] = \mathrm{SL}_2(\mathbb{F}_\ell)$ and so $A \cong \mathbb{F}_\ell^\times$. So in particular there is a surjective map $\mathbb{F}_\ell^\times \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^m$, so $m \leq 1$ since $\mathbb{F}_\ell^\times$ is cyclic. Note that we have the surjections corresponding to the determinant map and the Legendre symbol

$$\mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathbb{F}_\ell^\times \longrightarrow \mathbb{Z}/2\mathbb{Z}.$$

By Lemma 3.2.1, m is maximal among quotients of this form, which implies $m = 1$. So we have that $[\mathrm{GL}_2(\mathbb{F}_\ell) \colon H] = 2$, but

$$[\mathrm{GL}_2(\mathbb{F}_\ell) \colon B(\ell)] = \frac{(\ell^2 - \ell)(\ell^2 - 1)}{\ell(\ell - 1)^2} = \ell + 1 > 2.$$

□

Before proving the normalizer of a non-split Cartan case, we first note the structure of its subgroups.

Lemma 3.3.2. *Let $\ell \geq 3$ be a prime and let H be a subgroup of the normalizer of a non-split Cartan of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Then H is generated by two elements.*

Proof. Let σ, α generate the normalizer of the non-split Cartan that H is contained in, where the subgroup generated by α is isomorphic to $\mathbb{F}_{\ell^2}^\times$. Denote $S = H \cap (\sigma\langle\alpha\rangle)$ and $A = H \cap (\langle\alpha\rangle)$. Then either $|S| = |A|$ or $|S| = 0$.

To see this, let $A = \{a_1, \dots, a_j\}$ and $S = \{s_1, \dots, s_k\}$. Then the elements $\sigma_1^{-1}\sigma_i \in A$ are distinct, so $|S| \leq |A|$. If $|S| \neq 0$, then the elements $\sigma_1 a_i \in S$ are distinct, so $|S| = |A|$.

Since A is a subgroup of a cyclic group, it is also cyclic. If $|S| = 0$, then H is generated by a generator of A. Otherwise $[H\colon A] = 2$, so H is generated by a generator of A and any element of S. □

Lemma 3.3.3. *Let $\ell \geq 17$ and assume $\rho_{E,\ell}(G_{\mathbb{Q}}) \subseteq N_{ns}(\ell)$, where $N_{ns}(\ell)$ is the normalizer of a non-split Cartan. Let E' denote the base change of E to $\mathbb{Q}(2^\infty)$. Then $\rho_{E',\ell}(G_{\mathbb{Q}(2^\infty)}) \nsubseteq B(\ell)$. In particular, together with Lemma 3.3.1, this implies that any elliptic curve without complex multiplication over $\mathbb{Q}$, after base change to $\mathbb{Q}(2^\infty)$, does not have an ℓ-power degree isogeny, except for those with the four exceptional j-invariants.*

Proof. Denote $G = \rho_{E,\ell}(G_{\mathbb{Q}})$ and $H = \rho_{E',\ell}(G_{\mathbb{Q}(2^\infty)})$. Then by Lemma 3.2.1 we have $G/H \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some m. We claim that $m \leq 2$. Again, reduction modulo H gives us the surjection $G \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^m$. Since the image is abelian, this map factors through the abelianization of G, which we denote by $A \cong G/[G,G]$. By Lemma 3.3.2, G is generated by two elements. Since A is a quotient of G, it is generated by the image of these elements via the reduction map. Since $A \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^m$, we have that $m \leq 2$.

Now we consider the orders of the groups involved. We have $\#B(\ell) = \ell(\ell-1)^2$ and $\#N_{ns}(\ell) = 2(\ell-1)(\ell+1)$. Since $\ell > 2$, we have that $\ell - 1$ and $\ell + 1$ are relatively prime, and so a necessary condition for H being contained in $B(\ell)$ is $(\ell+1) | [N_{ns}, H]$. This is not possible since $[N_{ns}\colon G] \leq 3$ and $[G\colon H] = 1, 2$, or 4. □

Remark. For CM elliptic curves, this behavior is quite different. For example, note that the elliptic curve

$$E\colon y^2 + y = x^3 - 57772164980x - 5344733777551611$$

which has CM by $\mathbb{Q}(\sqrt{-163})$ has mod ℓ image of Galois over $\mathbb{Q}$ equal to the normalizer of a split Cartan whenever $\left(\frac{-163}{\ell}\right) = 1$ and equal to the normalizer of the non-split Cartan otherwise, except at $\ell = 163$. For the former infinite class of primes, the split Cartan is an index 2 and therefore normal subgroup of the image of Galois. Hence, over $\mathbb{Q}(2^\infty)$, the image of Galois is a subgroup of the split Cartan which is a subgroup of the Borel. So CM elliptic curves have isogenies over $\mathbb{Q}(2^\infty)$ of prime degree for infinitely many primes.

3.4 ℓ-adic Images for $\ell = 3, 5, 7, 11, 13$

For small odd primes, Lemma 3.2.1 will suffice to compute the ℓ-adic images over $\mathbb{Q}(2^\infty)$. To see this, we recall the definition of the level of an image of Galois.

Definition. Given a subgroup G of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, usually an image of Galois, we define the *level* of G to be the smallest integer ℓ^k such that

$$\left\{M \in \mathrm{GL}_2(\mathbb{Z}_{\ell^k})\colon M \equiv I \pmod{\ell^k}\right\} \subseteq G.$$

Note that by Serre's open image theorem [Ser72], if G is an ℓ-adic image of Galois then G has finite level.

We have that for an elliptic curve E over $\mathbb{Q}$, if H is the ℓ-adic image of Galois over $\mathbb{Q}$ with level ℓ^k, the image over $\mathbb{Q}(2^\infty)$ is also of level ℓ^k. In particular, we have the following.

Lemma 3.4.1. *Let ℓ be an odd prime. For an elliptic curve E over $\mathbb{Q}$, if the ℓ-adic image of Galois over $\mathbb{Q}$ has level ℓ^k then the ℓ-adic image over $\mathbb{Q}(2^\infty)$ also has level ℓ^k.*

Proof. As usual, let G be the ℓ-adic image of Galois over $\mathbb{Q}$ and H the image over $\mathbb{Q}(2^\infty)$. Let $k' \geq k$. By 3.2.1, we have that $G(\ell^{k'})/H(\ell^{k'}) \cong (\mathbb{Z}/2\mathbb{Z})^m$ for some m.

Now define

$$N\colon = \{M \in \mathrm{GL}_2(\mathbb{Z}/\ell^{k'}\mathbb{Z}) | M \equiv I \pmod{\ell^k}\}.$$

By the definition of level, $N \subseteq G(\ell^{k'})$. Furthermore, N is a normal subgroup of $G(\ell^{k'})$ which can be checked using the definition of N. So $NH(\ell^{k'})$ is a subgroup of $G(\ell^{k'})$, and so we have $NH(\ell^{k'})/H(\ell^{k'}) \cong (\mathbb{Z}/2\mathbb{Z})^{m'}$, for some $m' \leq m$. Now by the second isomorphism theorem, we have

$$\frac{N}{N \cap H(\ell^{k'})} \cong (\mathbb{Z}/2\mathbb{Z})^{m'}$$

Since $\#N = \ell^{4(k'-k)}$, this implies $m' = 0$, so $N \cap H(\ell^{k'}) = N$, so $N \subseteq H(\ell^{k'})$. Hence, H has level ℓ^k. □

Remark. For the four exceptional j-invariants in [Zyw15], these elliptic curves all have ℓ-adic image of Galois with level equal to 17 or 37, so by 3.4.1 the level over $\mathbb{Q}(2^\infty)$ is also 17 or 37 respectively. Over $\mathbb{Q}$ these elliptic curves are already contained in the Borel, so these cannot be peripheral groups.

With this in mind we classify elliptic curves with ℓ-power isogenies. To do so, we consider each possible image of Galois whose corresponding modular curve has a rational non-cuspidal non-CM point, compute the image of Galois over $\mathbb{Q}(2^\infty)$ and record whether it is peripheral. Then for each of these subgroups (the images over $\mathbb{Q}$), we need to compute all of the rational points on the corresponding modular curve. This work has a long history, and recently Rouse, Sutherland, and Zureick-Brown completed it [RSZB].

For the first part, we enumerate all such images of Galois whose modular curves have a non-cuspidal, non-CM point as in [RZB15]. Then, for each such image G we execute the following procedure in Magma.

1. Let ℓ^k be the level of G. Enumerate all normal subgroups of $G(\ell^k)$. Magma is

efficient at generating these.

2. For each normal subgroup N of $G(\ell^k)$, test whether $G(\ell^k)/N$ is congruent to a power of $\mathbb{Z}/2\mathbb{Z}$. This is computationally quite slow, and having Magma check this directly was not producing results quickly enough. Instead this can be checked by taking every generator of G, checking if it squares to an element of H, and then checking if commutators of pairs of generators of $G(\ell^k)$ are elements of H.

3. For each such normal subgroup N, check whether it is contained in $B(\ell^k)$. To do this, it suffices to check whether there is a point in $\mathbb{P}^1_{\mathbb{Z}/\ell^k\mathbb{Z}}$ fixed by N. For a discussion of this, see [Etr15]. Here we are interpreting $\mathbb{P}^1_{\mathbb{Z}/\ell^k\mathbb{Z}}$ as lines through the origin in $\mathbb{A}^2_{\mathbb{Z}/\ell^k\mathbb{Z}}$, on which N naturally acts. We check instead whether there is a line fixed by each element in a generating set for N.

4. If at least one such normal subgroup of $G(\ell^k)$ has been found, record the minimal subgroup among the list of all of them and the current value of k. If not, reduce modulo ℓ^{k-1}.

5. Replace k with $k-1$. Repeat steps $(1)-(5)$ until either an isogeny has been found or $k=1$ has been checked, in which case record that there is no isogeny.

6. Compare the highest degree of an ℓ-power isogeny of G with the highest degree isogeny obtained from steps $(1)-(6)$.

Following this procedure, we find a total of 11 possible images of Galois which are peripheral. We summarize the data below.

Level of G	Iso. deg. / $\mathbb{Q}$	Iso. deg. / $\mathbb{Q}(2^\infty)$	Genus	Description
3	1	3	0	$X_G \cong \mathbb{P}^1$
9	1	9	1	Elliptic curve of rank 0
5	1	5	0	$X_G \cong \mathbb{P}^1$
5	1	5	0	$X_G \cong \mathbb{P}^1$
25	1	25	22	Genus 22 curve
7	1	7	0	$X_G \cong \mathbb{P}^1$
7	1	7	1	Elliptic curve of rank 0
7	1	7	1	Elliptic curve of rank 0
49	1	49	94	Genus 94 curve
11	1	11	2	Genus 2 curve
13	1	13	3	Genus 3 curve

Table 3.4.1: Peripheral mod ℓ-power subgroups for $3 \leq \ell \leq 13$

There are two entries in this table of particular interest. The first is that with level 49 and isogeny degree over $\mathbb{Q}(2^\infty)$ equal to 49. If there were non-CM non-cuspidal points on this curve this would correspond to a degree of an isogeny that does not appear over $\mathbb{Q}$. This turns out not to be the case. The curve X_G is isomorphic to $X_0^+(7^4)$, which has no points as proved by Bilu, Parent, and Robolledo [BPR13]. On the other hand, over $Y_0(25)(\mathbb{Q})$ has genus 0 [Ken82], so the corresponding entry does not indicate a new possibility for an isogeny degree over $\mathbb{Q}(2^\infty)$. However, this entry corresponds to a modular curve isomorphic to $X_0^+(5^4)$, which also has no points and is also covered in [BPR13].

3.5 2-adic Images

For $\ell = 2$ and 2 power isogenies, more computation needs to be done. Lemma 3.4.1 is not in true general. In fact, we have the following.

Example 3.5.1. Let E be an elliptic curve over $\mathbb{Q}$ whose 2-adic image of Galois has level 2, and mod 2 image equal to $B(2)$. Then after base change to $\mathbb{Q}(2^\infty)$, using

Lemma 3.2.1, the image of Galois modulo 4 is generated by:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}.$$

In particular, this new image is contained in $B(4)$. So E', the base change of E to $\mathbb{Q}(2^\infty)$ has a degree 4 isogeny, while E does not.

On the other hand, this is the worst that can happen.

Lemma 3.5.2. *For an elliptic curve E over $\mathbb{Q}$, if the 2-adic image of Galois over $\mathbb{Q}$ has level 2^k, then E', the base change to $\mathbb{Q}(2^\infty)$, does not have any 2-power degree isogenies of degree 2^{k+2} or greater.*

Proof. As usual, let G be the ℓ-adic image of Galois over $\mathbb{Q}$ and H the image over $\mathbb{Q}(2^\infty)$. Let $N_k \colon = \{M \in \mathrm{GL}(\mathbb{Z}/2\mathbb{Z})^{k+2} | M \equiv I \pmod{2^k}\}$. Then by the second isomorphism theorem, we have $H(2^{k+2}) \cap N$ is a normal subgroup of N. Furthermore,

$$\frac{N_k}{H(2^{k+2}) \cap N_k} \cong \frac{N_k H(2^{k+2})}{H(2^{k+2})}$$

The right hand side is naturally a subset of $G(2^{k+2})/H(2^{k+2})$ which is congruent to a power of $\mathbb{Z}/2\mathbb{Z}$. So, it suffices to show that the minimal normal subgroup of N_k with quotient a power of $\mathbb{Z}/2\mathbb{Z}$ is not contained in the Borel. To see this, we first note that all of the N_k are isomorphic via

$$\begin{pmatrix} 1 + a2^k & b2^k \\ c2^k & 1 + d2^k \end{pmatrix} \mapsto \begin{pmatrix} 1 + a2^{k'} & b2^{k'} \\ c2^{k'} & 1 + d2^{k'} \end{pmatrix}$$

so it suffices to compute the specific case $k = 1$. We get that the minimal such subgroup of N_k is

$$N_k' \colon = \{M \in \mathrm{GL}(\mathbb{Z}/2\mathbb{Z})^{k+2} | M \equiv I \pmod{2^{k+1}}\}.$$

Note that N'_k is invariant under conjugation, so it suffices to check whether it is contained in any Borel, and it is clearly not contained in the subgroup of upper triangular matrices.

□

Example 3.5.3. To extend on Example 3.5.1, let E be an elliptic curve with 2-adic image of Galois of level 2^k and image equal to $B(2^k)$, with $k \geq 1$. Then E', the base change to $\mathbb{Q}(2^\infty)$, has image of Galois contained in $B(2^{k+1})$. In particular, this implies that if there is an elliptic curve over $\mathbb{Q}$ with an isogeny of degree $2d$ for some d, then over $\mathbb{Q}(2^\infty)$ this elliptic curve has an isogeny of degree $4d$. This accounts for every new entry in the list in Theorem 3.1.1, although it does not account for all the elliptic curves with the corresponding degrees of isogenies.

Now to compute all 2-power isogenies, we can simply follow the algorithm described in Section 3.4, with one step added beforehand. Let G be a potential 2-adic image of Galois over $\mathbb{Q}$, with level 2^k. Then first we compute $G(2^{k+1})$ which is the inverse image of $G(2^k)$ by the reduction modulo 2^k map. We compute $H(2^{k+1})$ as described in Section 3.4, and if this is contained in $B(2^{k+1})$ then G is peripheral. Otherwise, we follow the algorithm as usual. Magma code implementing these algorithms can be found at this webpage.

Of the 202 images of Galois with level a power of 2 which have a rational noncuspidal, non-CM point, 119 of these are peripheral. The following table summarizes the findings.

Level of G	Iso. degree / $\mathbb{Q}$	Iso. degree / $\mathbb{Q}(2^\infty)$	Number of images
2	2	4	2
4	2	4	3
4	2	8	4
4	4	8	5
8	2	8	31
8	2	16	2
8	4	8	23
8	8	16	18
16	2	16	5
16	8	16	17
16	8	32	2
16	16	32	5
32	16	32	2

Table 3.5.1: Peripheral mod 2^k subgroups

There are several peripheral subgroups whose modular curves are isomorphic to $\mathbb{P}^1$, hence there are infinitely many elliptic curves over $\mathbb{Q}(2^\infty)$ with a degree 32 isogeny.

3.6 Isogenies of Composite Degrees

In practice, when considering the ℓ-adic images of Galois representations, we record for each possible image over $\mathbb{Q}$ the maximal degree of an isogeny with degree a power of ℓ. With this in mind, we turn to our goal of detecting whether there are isogenies of degree $\ell_1^{k_1}\ell_2^{k_2}$ for $\ell_1 \neq \ell_2$ with $\ell_1, \ell_2 \leq 13$ over $\mathbb{Q}(2^\infty)$. To do this, we consider groups G which are formed by taking products of groups G_1, G_2 where the elliptic curves parameterized by X_{G_i} has an isogeny of degree $\ell_i^{k_i}$ over $\mathbb{Q}(2^\infty)$. This is sufficient since $G \subseteq B(\ell_1^{k_1}\ell_2^{k_2})$ if and only if $G_1 \subseteq B(\ell_1^{k_1})$ and $G_2 \subseteq B(\ell_2^{k_2})$.

To conclude Theorem 3.1.1, it suffices then to compute the genera of modular curves X_G for groups G as above with $\ell_1^{k_1}\ell_2^{k_2}$ corresponding to an isogeny of degree that does not already appear for elliptic curves over $\mathbb{Q}$. If the genus of such an X_G

is greater than 1, then by Falting's theorem there are only finitely many rational points on X_G. This implies that there are only finitely many $\mathbb{C}$-isomorphism classes of elliptic curves on X_G, but as discussed earlier for $j \neq 0, 1728$, this is the same as $\mathbb{Q}(2^\infty)$-isomorphism classes. We will also need to consider the case of composite numbers with 3 or more distinct small prime factors, but first we describe the results of the computation for 2 distinct prime factors.

Magma has the built in capability to form product groups, and to compute the genera of the corresponding modular curves, we use the function written by Sutherland and Zywina [SZ17]. We can also begin by filtering on pairs of subgroups G_1, G_2 where both X_{G_1}, X_{G_2} have infinitely many points, as otherwise X_G only has finitely many points. This leaves a relatively short list of product groups with corresponding modular curve having genus 0 or 1. Among this list, the associated degrees of $\mathbb{Q}(2^\infty)$ isogenies are $20, 24, 36$ with modular curves of genus 0, and $28, 40, 48, 72$ with modular curves of genus 1.

Next, we create models for these corresponding product groups. Let $G = G_1 \times G_2$ be a subgroup of interest. Sutherland and Zywina [SZ17] have computed explicit formulas computed for the maps from X_{G_i} to the j-line, we denote these by f_1, f_2. We warn the reader that in this chapter, Galois representations mod n act on a basis for $E[n]$ via left actions, whereas those in [RZB15] act on the right, so to compare groups one must first take transpositions. Since $G = G_1 \times G_2$, we have that X_G is the fiber product of X_{G_1} and X_{G_2} over $X(0)$.

In all cases we consider, the genus of $X_{G_i} = 0$, so a model for the affine part of X_G is $f(x) = g(y)$. This model will most likely be highly singular, so more work needs to be done to get a simplified model. In the case of the genus 0 curves for isogeny degrees $20, 24, 36$, the models have small enough degree, that the built in magma function Conic is able to desingularize the model. Magma can then check explicitly that there is a point on these genus 0 curves, and hence these modular curves X_G are isomorphic to $\mathbb{P}^1$. In particular, there are infinitely many elliptic curves with each of these degrees of isogenies after base changing to $\mathbb{Q}(2^\infty)$. Below are the generators of groups $G = G_1 \times G_2$ witnessing the corresponding isogeny degree for each of these cases.

Degree	Level of G	Generators of G
20	10	$\begin{pmatrix}1&5\\0&1\end{pmatrix}, \begin{pmatrix}9&6\\4&9\end{pmatrix}, \begin{pmatrix}5&6\\4&5\end{pmatrix}, \begin{pmatrix}5&4\\4&9\end{pmatrix}, \begin{pmatrix}3&0\\0&3\end{pmatrix}$
24	12	$\begin{pmatrix}7&0\\0&1\end{pmatrix}, \begin{pmatrix}5&0\\0&1\end{pmatrix}, \begin{pmatrix}5&0\\0&5\end{pmatrix}, \begin{pmatrix}11&0\\0&11\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}7&6\\0&7\end{pmatrix}$
36	18	$\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}11&0\\0&1\end{pmatrix}, \begin{pmatrix}13&12\\0&7\end{pmatrix}, \begin{pmatrix}17&0\\0&17\end{pmatrix}, \begin{pmatrix}13&6\\0&1\end{pmatrix}$

Table 3.6.1: Generators of groups G with $X_G \cong \mathbb{P}^1$

Note that the entries for degree 24 and 36 here are precisely the Borel groups modulo 12 and 18 respectively.

The genus 1 modular curves with isogeny degrees $28, 40, 48$ and 72 also have models with degrees low enough that the built in magma function EllipticCurve can find a model for the elliptic curve. To do so, we must supply the function with a point on the curve. Doing a brute force search for coordinates with numerators and denominators less than or equal to 10 suffices here. In all cases, the rank of the corresponding elliptic curve is 0, so there are at most finitely many examples of elliptic curves with image of Galois equal to the group G. Since there were already degree 14 isogenies over $\mathbb{Q}$, Example 3.5.3 implies 28-isogenies do arise in the $\mathbb{Q}(2^\infty)$ setting. For each of the remaining degrees $40, 48$ and 72, we can use magma to compute the number of points on the desingularized model we obtain for X_G. Since we start with a singular model, it is possible there are fewer non-singular points on X_G than on this elliptic curve. At the same time, we can compute the number of rational cusps on each of the curves X_G using Sutherland and Zywina's code [SZ17], this is done using group theory. On all of these curves, the number of rational cusps is equal to the number of points on the elliptic curve obtained from the model for X_G, hence there are no non-cuspidal points on X_G. In particular, there are no elliptic curves with these specific images of Galois G. This does not entirely eliminate the possibility of these degrees of isogenies appearing for elliptic curves base changed to $\mathbb{Q}(2^\infty)$.

To conclude Theorem 3.1.1, we need to consider isogeny degrees with 3 or more distinct prime factors. We can check using the same computational strategy that there are no images of Galois corresponding to these degrees that have genus 0 or 1, and this is sufficient to complete the proof.

This analysis leaves a finite number of elliptic curves left that have the potential of having a degree of an isogeny over $\mathbb{Q}(2^\infty)$ equal to an integer not appearing in the set in Theorem 3.1.1. Furthermore, we have an enumerable list of images of Galois that we can try to analyze. If we could find all points on all of their modular curves, this would produce a complete classification of $\mathbb{Q}(2^\infty)$-isogenies. Considering all of these images of Galois individually would be a monumental task, as there are many of them and the genus of the modular curve can be quite high, even exceeding 1000. Instead, we outline an approach that is more tenable.

- First, consider images of Galois at composite levels corresponding to the product of two ℓ-adic images of Galois. Say the factor groups are G_1, G_2 and the isogeny degrees are $\ell_1^{k_1}, \ell_2^{k_2}$.

- If $\ell_1^{k_1}\ell_2^{k_2}$ is on the list in Theorem 3.1.1, then we can ignore this product entirely. Even if it is not on the list, at least one of the two factor groups must be peripheral otherwise this would have already been the degree of an isogeny over $\mathbb{Q}$. This can be done as a first step computationally.

- If X_{G_1} or X_{G_2} has only finitely many points, say X_{G_1} does, we can enumerate elliptic curves corresponding to those points and then compute the image of

Galois for this curves mod $\ell_2^{k_2}$. Often k_2 will be 1, and we can employ the method used by Sutherland [Sut16].

- Among the remaining groups G, sort these by the isogeny degree and begin working through in ascending order of this degree.

- Within a specific isogeny degree, we can focus in even further. In particular, if we have two pairs $G = G_1 \times G_2$ and $G' = G'_1 \times G'_2$ with $G'_i \subseteq G_i$, then we first examine X_G. If there are no non-cuspidal non-CM points on X_G, then there are also none on X'_G.

- If there are no isogenies of degree $\ell_1^{k_1}\ell_2^{k_2}$, we do not need to check isogenies of degree $\ell_1^{k'_1}\ell_2^{k'_2}$ for pairs $k'_i \geq k_i$.

- Finally, a similar strategy can be followed for isogenies with degree having 3 or more distinct prime factors.

Even following this approach, the models of curves X_G can have very large degree and very large genus. For example, the process above produces a group G where a non-cuspidal non-CM point on X_G would correspond to a 35-isogeny, and the genus of X_G is 27. To analyze this list of curves, many approaches of analyzing modular curves will need to be employed, including strategies for reducing the model of X_G. For small genus curves, one could analyze this model directly. At this time, we have checked and not found any non-cuspidal non-CM points on any of the modular curves produced by this methodology up to genus 3. For the larger genus curves other tactics will need to be employed, like finding a map to a smaller genus curve, or using some of the information of the maps to the factor modular curves. In short, even using this strategy there is still considerable difficulty to completing the classification.

Chapter 4

Background - Arithmetical Structures on Graphs

In 1989, Lorenzini [Lor89] introduced the notion of arithmetical structures, which are graphs with some extra arithmetical data, to study degenerations of curves. There is significant interest in these arithmetical structures, and in some cases it is useful to enumerate or bound the number of distinct arithmetical structures that may arise when studying a set of curves. In his paper, Lorenzini proves that there are only finitely many arithmetial structures associated to a given graph. While this lemma was important for his discussion, the proof was not constructive. Since then, there has been interest in producing counts and bounds for the number of arithmetical structures on specific types of graphs. In the next chapter, we will prove a general upper bound based only on the number of edges and vertices of the graph. Since our approach does not use any arithmetic geometry of curves, we will define some of the important notions from graph theory.

4.1 Some Types of Graphs

Definition. A *graph* is a pair $G = (V, E)$ of sets where E is made up of 2-element sets of elements of V. We call V the *vertex set* of G and we will assume that V has finite order throughout. We call E the *edge set* of G.

Much of the time, one is interested in studying simple graphs, where each edge consists of two distinct vertices. An edge of the form $\{v, v\}$ is called a loop, and we will not be interested in graphs with loops. On the other hand, we will be interested in multigraphs.

Definition. A *multigraph* is identical to a graph except that E is a multiset. In particular, for two vertices $v, w \in V$, there may be multiple edges $\{v, w\} \in E$.

We will use graph to mean graph or multigraph. In order to obtain our result, it is vital to consider multigraphs.

Definition. A graph G is *connected* if there is a path along the edges between any pair of distinct vertices. In particular, given vertices $v \neq w$, either there is an edge between v and w or there is a sequence v_i, $1 \leq i \leq k$ for some k, and there is an edge between v and v_1, between v_i and v_{i+1} for $i < k$, and between v_k and w.

Definition. For a graph or multigraph G, we define the *degree* of a vertex to be the number of edges incident to it. So $d(v) = |\{e \in E \colon v \in E\}|$.

Next, we define several special types of graphs.

Definition. A *complete graph* on n vertices, denoted K_n, is a graph with $E = \{\{v, w\} \colon v, w \in V, v \neq w\}$. In the next chapter, we will also discuss a multigraph generalization of this.

A *path* on n vertices is denoted P_n. We can write $V = \{v_i \colon 1 \leq i \leq n\}$ for some ordering with $E = \{\{v_i, v_{i+1}\} \colon 1 \leq i \leq n-1\}$.

A *cycle* on n vertices a path with an edge added between the endpoints of the path.

A *star* is a graph where there is a central vertex that has an edge to each of the other vertices, and there are no other edges.

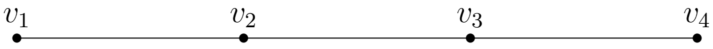


Figure 4.1.1: The graph P_4

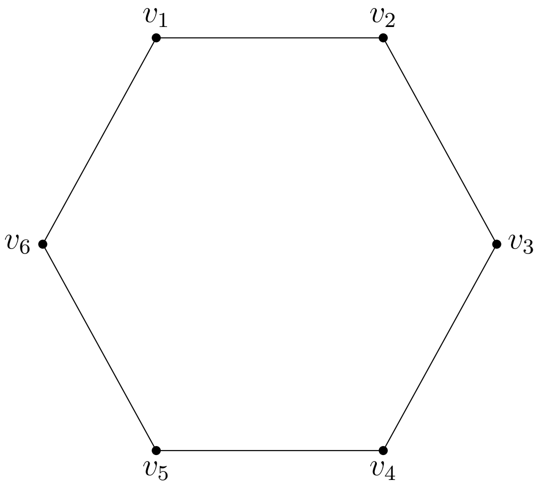


Figure 4.1.2: A cycle on 6 vertices

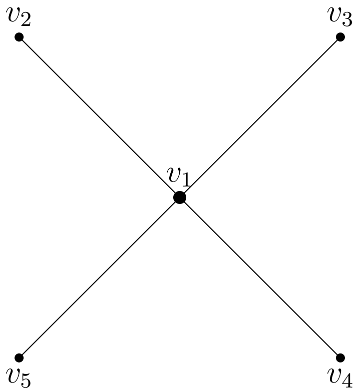


Figure 4.1.3: A star with 5 vertices

In addition to these graphs, there are some more cases that have been studied in the context of bounding the number of arithmetical structures. These include a path with a doubled edge and bidents. These graphs will not be central to our discussion, so we will not define them here.

Chapter 5

Bounding the Number of Arithmetical Structures on Graphs

5.1 Introduction

Let G be a connected undirected graph with n vertices labeled $v_1, \ldots, v_n$, containing no loops but possibly multiedges. Throughout this chapter, we use $E(G)$ to refer to the edge set of G, we use δ_{ij} to denote the number of edges between v_i and v_j, and we use $\deg v$ for the degree of the vertex v. An *arithmetical structure on* G is a pair $(\mathbf{r}, \mathbf{d}) \in \mathbb{N}^n \times \mathbb{N}^n$, such that $\gcd(\mathbf{r}) = \gcd(r_1, ..., r_n) = 1$, satisfying the system

$$\begin{aligned} r_1 d_1 &= r_2\delta_{12} + \cdots + r_n\delta_{1n} \\ r_2 d_2 &= r_1\delta_{21} + \cdots + r_n\delta_{2n} \\ &\vdots \\ r_n d_n &= r_1\delta_{n1} + \cdots + r_{n-1}\delta_{n(n-1)}. \end{aligned} \tag{5.1.1}$$

Equivalently, an arithmetical structure is the data of $\mathbf{r}, \mathbf{d} \in \mathbb{N}^n$ satisfying the matrix equation

$$\begin{pmatrix} -d_1 & \delta_{12} & \cdots & \delta_{1n} \\ \delta_{21} & -d_2 & \cdots & \delta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \delta_{n1} & \delta_{n2} & \cdots & -d_n \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5.1.2}$$

Note that specifying $\mathbf{r}$ such that $r_i \mid \sum_{j \neq i} r_j \delta_{ij}$ is sufficient to recover $\mathbf{d}$. Thus we may simply refer to $\mathbf{r}$ as an arithmetical structure on G. We use $A(G)$ to denote the set of arithmetical structures on a graph G.

We remark that we could extend this definition of an arithmetical structure to a graph with loops. We simply amend (5.1.1) by requiring

$$r_i d_i = \sum_{j=1}^{n} r_j \delta_{ij}$$

for all i. However, by absorbing δ_{ii} into d_i for each i, it can be seen that $\mathbf{r}$ defines an arithmetical structure on G_0, where G_0 is the graph obtained by removing all loops from G. Thus $A(G)$ is in one-to-one correspondence with $A(G_0)$, and for the remainder of this chapter we will assume G contains no loops.

While combinatorial in nature, arithmetical structures are related to the study of special fibers of relative proper minimal models of curves. They were introduced by Lorenzini, who proved that $A(G)$ is finite [Lor89]. Aside from certain special cases, little is known beyond finiteness about $\#A(G)$. Braun et. al. [BCC+18] succeeded in enumerating the number of arithmetical structures when G is a path or a cycle, where they found connections to the Catalan numbers and certain binomial coefficients. Archer et. al [ABDL+20] considered bidents — paths with two prongs at one end — and gave bounds again in terms of the Catalan numbers. Glass and Wagner [GW19] studied arithmetical structures on paths with a doubled edge, and formulated a conjecture for how $\#A(G)$ grows in this case, depending on the path length and the location of the doubled edge.

In this chapter, we introduce a construction in Section 5.2 to reduce an arithmetical structure on a graph G with n vertices into an arithmetical structure on an associated graph G' with $n-1$ vertices. Our primary application of this construction is to derive an explicit general upper bound for the number of arithmetical structures on a graph G, depending only on the number of vertices and edges.

Theorem 5.1.1. *Let G be a connected, undirected graph on n vertices, with no loops but possible multiedges. Then the following is an upper bound for the number of arithmetical structures on G.*

$$\#A(G) \leq \frac{n!}{2} \cdot \#E(G)^{2^{n-2}-1} \cdot \#E(G)^{2^{n-1} \cdot \frac{1.538 \log(2)}{(n-1)\log(2)+\log(\log(\#E(G)))}}.$$

Section 5.3 is devoted to the proof of Theorem 5.1.1.

Our construction generalizes the *smoothing* process used in [BCC$^+$18], [ABDL$^+$20], and [GW19]. In certain special cases, it is the inverse of Lorenzini's *blowup* construction [Lor89, 1.8], and extends observations made by Corrales and Valencia about the arithmetical structures on the *clique-star* transform of a graph [CV18].

In Section 5.4, we discuss the special case of graphs with n vertices and m edges between each pair of vertices, which we denote by mK_n. We first give a refinement of Theorem 5.1.1 before making connections between their arithmetical structures and Egyptian fractions. An *Egyptian fraction* describes an integer fraction a/m as the sum of unit fractions,

$$\frac{1}{x_1} + \cdots + \frac{1}{x_n} = \frac{a}{m}. \tag{5.1.3}$$

These representations have been studied from many angles over the years — for a brief survey see the introduction of [Ble72]. There also remain many open problems about Egyptian fractions, including the Erdös–Straus Conjecture, which concerns the existence of a representation for all m in the case where $a = 4$ and $n = 3$ in (5.1.3). See [Guy04] for more open problems related to Egyptian fractions.

We are interested in Egyptian fractions with $a = 1$,

$$\frac{1}{x_1} + \cdots + \frac{1}{x_n} = \frac{1}{m}, \tag{5.1.4}$$

In Theorem 5.4.2 we describe a one-to-one correspondence between integer solutions to (5.1.4) and $A(mK_n)$. This connection in the case of K_n was also noted in [HL20], in which the integers that can appear as the largest r-value for an arithmetical structure on K_n were partially classified. We may then use the known results about Egyptian fraction representations to give an asymptotic upper bound for $\#A(mK_n)$ which improves on Theorem 5.1.1.

5.2 A Recursive Construction

We now describe a construction which associates to an arithmetical structure $(\mathbf{r}, \mathbf{d})$ on G an arithmetical structure $(\mathbf{r}', \mathbf{d}')$ on an associated graph G' possessing $n - 1$ vertices. The process of obtaining G' is described precisely below in Construction 5.2.1.

Construction 5.2.1. Let G be a connected undirected graph with n vertices, with v_i and δ_{ij} having their usual meanings. For any choice of vertex v_i and positive ingeter s, we define a graph $G(v_i, s)$ as follows: $G(v_i, s)$ has $n - 1$ vertices, obtained by removing the i-th vertex from G, so

$$V\left(G(v_i, s)\right) = V(G) - \{\, v_i \,\}\,.$$

The edges of $G(v_i, s)$ are given by

$$\delta'_{jk} = \delta_{ij}\delta_{ik} + s\delta_{jk},$$

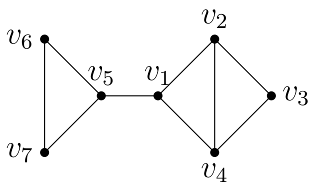
where δ'_{jk} denotes the number of edges between distinct vertices v_j and v_k in $G(v_i, s)$.

Remark. Alternatively, we could envision $G(v_i, s)$ as the union of $s(G - v_i)$ with the graph obtained by performing a star-clique type operation around v_i, in which v_i is removed from its star and $\delta_{ij}\delta_{ik}$ edges are added between each pair of distinct vertices v_j and v_k. This description makes more apparent that when $s = 1$ and the star of v_i is simple (i.e. $\delta_{ij} = 1$ for all v_j adjacent to v_i), Construction 5.2.1 is inverse to the clique-star transform described in [CV18, §5]. More precisely, using the notation of [CV18, §5], suppose G is a graph containing a clique C and $\widetilde{G} = cs(G, C)$ is its clique star transform with new vertex v. Then our construction applied to v with $s = 1$ recovers the original graph, i.e. $\widetilde{G}(v, 1) = G$.

We illustrate Construction 5.2.1 with an example.

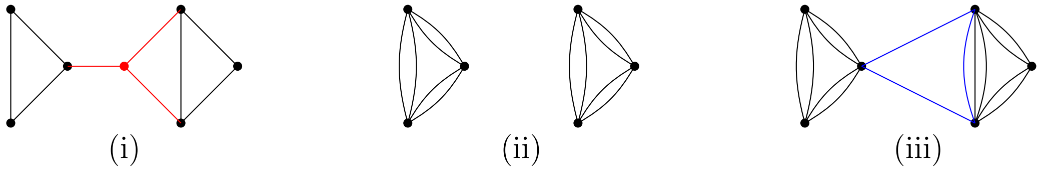
Example. Consider the graph G shown below in Figure 5.2.1.

Figure 5.2.1: G with vertices labeled.



Using Construction 5.2.1 with $i = 1$ and $s = 2$, we obtain $G' = G(v_1, 2)$. This is shown step-by-step in Figure 5.2.2. In step (i) we highlight v_1 and its incident edges in red to be removed. Step (ii) shows the graph $2(G - v_1)$ and finally step (iii) shows in blue the additional $\delta_{1j}\delta_{1k}$ edges added for each pair of remaining vertices.

Figure 5.2.2: Obtaining $G' = G(v_1, 2)$ from Construction 5.2.1.



Let $\mathbf{r} = (2, 1, 1, 2, 1, 1, 1)$, which gives an arithmetical structure on G with $\mathbf{d} = (2, 5, 3, 2, 4, 2, 2)$. We have $s = d_1 = 2$, and one may check that $\mathbf{r}' = (1, 1, 2, 1, 1, 1)$ gives an arithmetical structure on $G' = G(v_1, 2)$. This turns out to be an example of a more general phenomenon — for any arithmetical structure $\mathbf{r}$ on G, take $\mathbf{r}' = (r_1, \ldots, \widehat{r_i}, \ldots, r_n)$, where $\widehat{r_i}$ denotes removal of the i-th entry from the tuple. Then for the graph $G(v_i, d_i)$, we find $\mathbf{r}'$ satisfies the requirements of (5.1.1) for some appropriate $\mathbf{d}'$. Hence, it is an arithmetical structure after possible scaling. Lemma 5.2.2 verifies this observation in general.

Lemma 5.2.2. *Fix an arithmetical structure $(\boldsymbol{r}, \boldsymbol{d})$ on G and a vertex v_i of G, and let $G' = G(v_i, d_i)$ as given by Construction 5.2.1. Set $g = \gcd(r_1, \ldots, \widehat{r_i}, \ldots, r_n)$ and $\boldsymbol{r}' = (r_1/g, \ldots, \widehat{r_i/g}, \ldots, r_n/g)$. Then $\boldsymbol{r}'$ is an arithmetical structure on G'.*

Proof. It suffices to consider the case $i = 1$, as we can always renumber the vertices of G so that v_1 is removed. By (5.1.1), we have the system

$$\begin{aligned} r_2 d_2 &= \frac{r_2\delta_{12} + \cdots + r_n\delta_{1n}}{d_1}\delta_{21} + \cdots + r_n\delta_{2n} \\ &\vdots \\ r_n d_n &= \frac{r_2\delta_{12} + \cdots + r_n\delta_{1n}}{d_1}\delta_{n1} + \cdots + r_{n-1}\delta_{n(n-1)}. \end{aligned} \tag{5.2.1}$$

So for $2 \leq i \leq n$ we have:

$$\begin{aligned} r_i(d_1 d_i - \delta_{1i}^2) &= \delta_{1i}(r_2\delta_{12} + \cdots + r_n\delta_{1n}) + d_1 \sum_{2\leq j\leq n, i\neq j} r_j\delta_{ij} \\ &= \sum_{2\leq j\leq n, i\neq j} r_j(\delta_{i1}\delta_{1j} + d_1\delta_{ij}). \end{aligned} \tag{5.2.2}$$

Notice that Construction 5.2.1 gives $\delta'_{ij} = \delta_{i1}\delta_{1j} + d_1\delta_{ij}$, so we have

$$r_i(d_1 d_i - \delta_{1i}^2) = \sum_{2\leq j\leq n, i\neq j} r_j\delta'_{ij}$$

for all $2 \leq i \leq n$, which is precisely (5.1.1) on the new graph G'. If $g > 1$ then we need to divide each r_i by g to obtain another arithmetical structure, which corresponds to scaling (5.2.2) by $1/g$. Let $(r'_2, r'_3, \ldots, r'_n), (d'_2, d'_3, \ldots, d'_n)$ denote the new arithmetical structure on G'. Then explicitly, $r'_i = r_i/g$ and $d'_i = d_1 d_i - \delta_{1i}^2$. Since the r'_i are positive integers, the new numbers of edges between pairs of vertices are non-negative, and G' is clearly connected, we have that d'_i are also positive integers. Thus $(\mathbf{r}', \mathbf{d}')$ is an arithmetical structure on G'. □

Remark. If $(\mathbf{r}, \mathbf{d})$ is an arithmetical structure on G, $d_1 = 1$, and $G' = G(v_1, 1)$, then G with its arithmetical structure $(\mathbf{r}, \mathbf{d})$ is the blow up [Lor89, 1.8] of G' with its arithmetical structure $(\mathbf{r}', \mathbf{d}')$. In this case, one translates between our construction and Lorenzini's by taking $M = D' - A'$, where $D' = \operatorname{diag}(\mathbf{d}')$, A' is the adjacency matrix of G', and $\mathbf{q}^T = (\delta_{12}, \ldots, \delta_{1n})$. Then $M_{\mathbf{q}} = D - A$ is the matrix corresponding to the original arithmetical structure on G. As a consequence, we observe that when $d_1 = 1$, the critical groups of the arithmetical structures $\mathbf{r}$ on G and $\mathbf{r}'$ on G' are isomorphic. It may be interesting to study the relationships between the critical groups $(\mathbf{r}, \mathbf{d})$ on G and $(\mathbf{r}', \mathbf{d}')$ on $G(v_i, d_i)$ more generally.

In this chapter, when we have a fixed arithmetical structure $(\mathbf{r}, \mathbf{d})$ on G we will only be interested in the case where $s = d_i$ coming from Lemma 5.2.2, and as mentioned in the proof we can always renumber the vertices of G such that $i = 1$. Hence, for the remainder of this chapter we simply take $G' = G(v_1, d_1)$ when it will not create confusion. We will occasionally make use of the more general construction, as it is needed for the proof of Theorem 5.1.1.

Example (Paths)**.** Let P_n denote the path with n vertices, i.e. $\delta_{ij} = 1$ if $j = i \pm 1$ and $\delta_{ij} = 0$ otherwise. Arithmetical structures on paths have been studied extensively, and it has been shown that $\#A(P_n) = C_{n-1} = \frac{1}{n}\binom{2n-2}{n-1}$, where C_{n-1} denotes the $(n-1)$-th Catalan number [BCC$^+$18, Theorem 3].

If $n \geq 3$, we may apply Construction 5.2.1 at vertex i with $1 < i < n$ and find $P_n(v_i, 1) = P_{n-1}$. To see this, we check that for $j < k$, as long as $(j, k) \neq (i-1, i+1)$, we have $\delta'_{jk} = \delta_{jk}$, since one of δ_{ij} or δ_{ik} is 0. Then we have

$$\delta'_{(i-1)(i+1)} = \delta_{(i-1)i}\delta_{i(i+1)} + 1 \cdot \delta_{(i-1)(i+1)} = 1.$$

In particular, given an arithmetical structure $(\mathbf{r}, \mathbf{d})$ on P_n with $d_i = 1$ for some $1 < i < n$, we obtain an arithmetical structure $\mathbf{r}' = (r_1, \ldots, \widehat{r_i}, \ldots, r_n)$ on P_{n-1} $(r_1 = r_n = 1$ so we have automatically have $g = 1)$. This is precisely the *smoothing* process of [BCC$^+$18, Proposition 5], so one may view Construction 5.2.1 and Lemma 5.2.2 as a more general version of the smoothing of a path.

We conclude this section with another illustrative example which we will study in greater depth in Section 5.4.

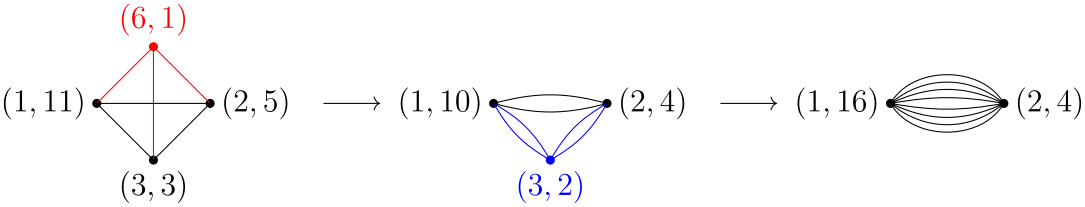
Example (complete (multi)graphs)**.** Let K_n denote the complete graph on n vertices. We will use mK_n to denote the complete graph K_n but instead with m edges between each two vertices. The regular nature of this graph allows for a concise description of the graph $mK_n(v_1, s)$ obtained from Construction 5.2.1 on mK_n.

After removing the vertex v_1 and all incident edges, we are left with $n-1$ vertices. The value of δ'_{ij} is given by $\delta'_{ij} = \delta_{1i}\delta_{1j} + s\delta_{ij} = m^2 + sm$. Thus, $mK_n(v_1, s) =$

$(m^2 + sm)K_{n-1}$.

We illustrate this below with the arithmetical structure $\mathbf{r} = (6, 3, 2, 1)$ on K_4, which gets reduced to the arithmetical structure $\mathbf{r}' = (3, 2, 1)$ on $K_4(v_1, 1) = 2K_3$, which is further reduced to $\mathbf{r}'' = (2, 1)$ on $2K_3(v_2, 2) = 8K_2$.

Figure 5.2.3: Applying Construction 5.2.1 twice to K_4. Vertices are labeled with their (r_i, d_i) values.



5.3 Upper Bounds on $\#A(G)$

In this section, we leverage Construction 5.2.1 inductively to derive an upper bound for the number of arithmetical structures on an arbitrary graph. To state our main result, recall the divisor function, which counts the number of positive divisors of an integer n, denoted here by $\sigma_0(n)$. This theorem is a strengthening of Theorem 5.1.1, so we will prove this instead.

Theorem 5.3.1. *Let G be a connected, undirected graph on n vertices, with no loops but possible multiedges. Suppose f is any monotonically increasing function such that $\sigma_0(m) \leq f(m)$ for all positive integers m. Then*

$$\#A(G) \leq \frac{n!}{2} \#E(G)^{2^{n-2}-1} \cdot f\left(\#E(G)^{2^{n-1}}\right). \tag{5.3.1}$$

We will now justify that Theorem 5.1.1 follows from Theorem 5.3.1. In [Nic88], an explicit upper bound for the divisor function is given to be

$$\sigma_0(m) \leq m^{\frac{1.538 \log(2)}{\log(\log(m))}}.$$

Note that the right hand side is monotonically increasing in m. Taking $f(m) = m^{\frac{1.538\log(2)}{\log(\log(m))}}$ produces the upper bound for $\#A(G)$ given by Theorem 5.1.1 in the introduction, so it follows directly from Theorem 5.3.1.

The proof of Theorem 5.3.1 proceeds by induction on the number of vertices of G. We take care of the base case, when $n = 2$, in Lemma 5.3.2. This is where the divisor function is introduced. We then prove an independent result in Theorem 5.3.3, which provides an upper bound for the r_i-values depending only on n and $\#E(G)$. Next we prove Theorem 5.3.1 using Lemma 5.3.2 and some of the ideas from the proof of Theorem 5.3.3. We conclude this section by comparing our result to the known values of $\#A(G)$ when $G = P_{n+1}$ is a path.

Lemma 5.3.2. *Let G be a graph with two vertices, v_1 and v_2. If (r_1, r_2) is an arithmetical structure on G then $r_1, r_2 \mid \#E(G)$ and so $r_1, r_2 \leq \#E(G)$. The total number of arithmetical structures on G is precisely $\sigma_0(\#E(G)^2)$.*

Proof. The divisibility statement follows from the fact that $r_1 \mid \#E(G)r_2$ and $\gcd(r_1, r_2) = 1$. For the second part, we provide a bijection between the set of arithmetical structures on G and divisors of $\#E(G)^2$, defined by sending

$$(r_1, r_2) \mapsto \frac{\#E(G)}{r_1} r_2$$

This is clearly well-defined. If (r_1, r_2) and (r_1', r_2') get mapped to the same integer then $r_1' r_2 = r_1 r_2'$ and since $\gcd(r_1, r_2) = \gcd(r_1', r_2') = 1$ we get $r_1 \mid r_1'$ and $r_1' \mid r_1$. Thus $r_1 = r_1'$ and $r_2 = r_2'$, so this map is injective.

To demonstrate surjectivity, let $\#E(G) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, and let $p_1^{\beta_1} \cdots p_k^{\beta_k}$ be a factor of $\#E(G)^2$. Then for each i, if $\beta_i \leq \alpha_i$, we add a factor of $p_i^{\alpha_i - \beta_i}$ to r_1, and otherwise we add a factor of $p_i^{\beta_i - \alpha_i}$ to r_2. This will result in the power of p_i in the image of (r_1, r_2) being β_i, and hence the (r_1, r_2) obtained by this procedure has image equal to $p_1^{\beta_1} \cdots p_k^{\beta_k}$. □

Remark. We consider order to matter when enumerating $A(G)$. For example, if G is the graph with two vertices and three edges ($G = 3K_2$ in the notation of Example 5.2), we count the arithmetical structures $\mathbf{r} = (1,3)$ and $\mathbf{r} = (3,1)$ separately. In this case, $\#A(G) = \sigma_0(3^2) = 3$.

With Construction 5.2.1 and Lemma 5.3.2 we can now give an upper bound for the largest possible r_1 value on a given graph G, which depends only on the number of vertices and edges. We will then prove Theorem 5.3.1.

Theorem 5.3.3. *Let $\mathbf{r}$ be an arithmetical structure on a graph G with n vertices. Reorder the vertices so that $r_1 \geq r_2 \ldots \geq r_n$. Then*

$$r_1 \leq \frac{1}{(n-1)!} \cdot \#E(G)^{3 \cdot 2^{n-2} - 2}$$

Proof. The case $n = 2$ reduces to $r_1 \leq \#E(G)$, which follows from Lemma 5.3.2, so we assume the statement is true for all graphs with $n-1$ vertices. Let G be a graph with n vertices and take $(r_1, r_2, \ldots, r_n)$ to be an arithmetical structure on G.

By (5.1.1), we have

$$r_1 d_1 = r_2 \delta_{12} + \cdots + r_n \delta_{1n}$$

and so

$$r_1 \leq \left(\sum_{i=2}^{n} \delta_{1i} \right) r_2 = \deg(v_1) r_2.$$

Since $(r_2/g, \ldots, r_n/g)$ is an arithmetical structure on $G(v_1, d_1)$, where g and G' are as in Lemma 5.2.2, we in turn have the inequality

$$r_1 \leq \deg(v_1) \cdot \left(\max_{(\mathbf{r}', \mathbf{d}') \in A(G)} \left(\max_{\mathbf{r}'' \in A(G(v_1, d_1'))} r_2'' \right) \right) \cdot \left(\max_{\mathbf{r}' \in A(G)} \gcd(\mathbf{r}') \right).$$

Here the nested maximum is over all possible arithmetical structures $(r_1', r_2', \ldots, r_n', d_1', d_2', \ldots, d_n') \in A(G)$, and over all possible arithmetical structure

$(r''_2, r''_3, \ldots, r''_n) \in A(G(v_1, d'_1))$. The second maximum is over all arithmetical structures $\mathbf{r}' \in A(G)$.

Since $g \mid r_2, \ldots, r_n$ and $\gcd(r_1, r_2, \ldots, r_n) = 1$, we have $\gcd(r_1, g) = 1$. Then by (5.1.1), we have for all $i > 1$,

$$\begin{aligned} r_i d_i &= \sum_{j \neq i} r_j \delta_{ij}, \text{ and so} \\ r_1 \delta_{1i} &= r_i d_i - \sum_{j>1, j\neq i} r_j \delta_{ij}. \end{aligned} \tag{5.3.2}$$

Since $\gcd(g, r_1) = 1$, and g divides the right hand side of Equation 5.3.2, we have $g \mid \delta_{1i}$, so $g \leq \delta_{1i}$. Summing over all $i \neq 1$, we get

$$(n-1)g \leq \sum_{i=2}^{n} \delta_{in} = d(v_1) \leq \#E(G),$$

so $g \leq \#E(G)/(n-1)$. Here we trivially bound $\deg(v_1) \leq \#E(G)$, and in general we can't do any better, since all edges in the graph could be incident to v_1.

By the inductive hypothesis we now have

$$\begin{aligned} r_1 &\leq \frac{\#E(G)^2}{n-1} \cdot \left(\max_{(\mathbf{r}', \mathbf{d}') \in A(G)} \left(\max_{\mathbf{r}'' \in A(G(v_1, d'_1))} r''_2 \right) \right) && (5.3.3) \\ &\leq \frac{\#E(G)^2}{(n-1)!} \left(\max_{(\mathbf{r}', \mathbf{d}') \in A(G)} \#E(G(v_1, d'_1)) \right)^{3 \cdot 2^{n-2} - 2} && (5.3.4) \end{aligned}$$

We will give an upper bound for this maximum. Using Construction 5.2.1, we have

$$\#E(G(v_1, d'_1)) \leq d'_1 e_{\neq 1} + \binom{\deg(v_1)}{2}$$

where $e_{\neq 1}$ is the number of edges on G not incident to v_1. The binomial coefficient arises from the final step of the construction for $G(v_1, d'_1)$, where at worst every pair of edges adjacent to v_1 will add a new edge in $G(v_1, d'_1)$. Now, we have again by

(5.1.1)

$$r_1'd_1' = r_2'\delta_{12} + ... + r_n'\delta_{1n} \leq \deg(v_1)r_2'$$

and so $d_1' \leq \deg(v_1)$. Therefore we have

$$\#E(G(v_1, d_1')) \leq \deg(v_1)(\#E(G) - \deg(v_1)) + \binom{\deg(v_1)}{2}$$

which is a quadratic function in $\deg(v_1)$, which has a maximum of $(2\#E(G)+1)^2/8 \leq \#E(G)^2$, so

$\#E(G(v_1, d_1')) \leq \#E(G)^2$. So 5.3.3 becomes

$$r_1 \leq \frac{\#E(G)^2}{n-1}\frac{1}{(n-2)!} \cdot \#E(G)^{3\cdot 2^{n-1}-4} = \frac{1}{(n-1)!}\#E(G)^{3\cdot 2^{n-1}-2}.$$

□

Proof of Theorem 5.3.1. We proceed by induction on n, the number of vertices. In the base case of $n = 2$, the inequality (5.3.1) is implied by Lemma 5.3.2. For the inductive step we assume that (5.3.1) is true for all graphs with $n-1$ vertices. First, note that by (5.1.1), for any arithmetical structure on G with $r_1 \geq r_2 \geq \cdots \geq r_n$, we have

$$d_1 = \frac{r_2}{r_1}\delta_{12} + \frac{r_3}{r_1}\delta_{13} + \cdots + \frac{r_n}{r_1}\delta_{1n} \leq \delta_{12} + \delta_{13} + \cdots + \delta_{1n} \leq \#E(G). \qquad (5.3.5)$$

In general, if i is an index where $r_i \geq r_j$ for all $j \neq i$, then the above argument also shows $d_i \leq \#E(G)$. Next we make the following observation. Fix a vertex v_i and also fix a prescribed value for d_i for an arithmetical structure. Once we have fixed these values, the graph G' referenced in Construction 5.2.1 is fixed. We claim there is at most one arithmetical structure on G which satisfies these criteria which reduced to any given arithmetical structure on G'. To see this, let $(r_1, r_2, \ldots, r_n)$

and $(r'_1, r'_2, \ldots, r'_n)$ be two arithmetical structures satisfying these criteria. Assume that $(r_1/g, r_2/g, \ldots, r_n/g) = (r'_1/g', r'_2/g', \ldots, r'_n/g')$, where g and g' are the gcd of $r_1, r_2, \ldots, r_n$ and $r'_1, r'_2, \ldots, r'_n$, and r_i and r'_i have now been removed. So, we have

$$d_i r_i = g \sum_{j \neq i} \frac{r_j}{g}$$

$$d_i r'_i = g' \sum_{j \neq i} \frac{r_j}{g'}$$

and hence we have $r_i g' = r'_i g$. By definition, $\gcd(g, r_i) = 1$, so $r_i \mid r'_i$ and $r'_i \mid r_i$, and $g = g'$. So the two arithmetical structures on G are equal.

This claim lets us bound the number of arithmetical structures on G as follows. For each vertex v_i, we count the number of arithmetical structures $(r_1, r_2, \ldots, r_n)$ where the maximum of the values of $\mathbf{r}$ is r_i. By (5.3.5) we have $d_i \leq \#E(G)$, so we get

$$\#A(G) \leq \sum_{i=1}^{n} \sum_{d_i=1}^{\#E(G)} \#A(G(v_1, d_i)).$$

By the same argument as in the proof of Theorem 5.3.3, the number of edges in G'_{d_i} is bounded by $\#E(G)^2$. So by induction, we have

$$\begin{aligned} \#A(G) &\leq \sum_{i=1}^{n} \sum_{d_i=1}^{\#E(G)} \frac{(n-1)!}{2} \#E(G)^{2^{n-2}-2} f\left(\#E(G)^{2^{n-1}}\right) \\ &= \frac{n!}{2} \#E(G)^{2^{n-2}-1} f\left(\#E(G)^{2^{n-1}}\right), \end{aligned}$$

completing the proof.

□

Remark. If more is known about the structure of the graph G then a much more accurate bound for $\#A(G)$ may be possible. As an extreme case, consider the path $G = P_{n+1}$ (see Example 5.2), where we have the exact count in terms of a Catalan number, $\#A(P_{n+1}) = C_n$ [BCC+18, Theorem 3]. This grows asymptotically as $4^n/(n^{3/2}\sqrt{\pi})$. On the other hand, the bound of Theorem 5.1.1 with $n+1$ vertices and $\#E(G) = n$ includes doubly exponential terms roughly of the form n^{2^n}, massively outpacing the Catalan numbers. Such a disparity in this case is not so surprising, given that a path has the minimal number of edges for a connected graph on n vertices and that in our result we assume nothing about G beyond the number of vertices and edges. Furthermore, in the bound in our result, the number of vertices is the variable that has the much bigger impact on the growth.

We will further discuss this disparity between Theorem 5.1.1 and the true value of $\#A(G)$ in Section 5.4 in the case where $G = mK_n$ (see Remark 5.4.1).

5.4 Arithmetical Structures on mK_n

5.4.1 Specializing to $G = mK_n$

Consider the special case of $G = mK_n$, as in Example 5.2. Recall that mK_n is the graph on n vertices with $\delta_{ij} = m$ for all $i \neq j$. Let $A_{\text{dec}}(mK_n)$ denote the subset of arithmetical structures $\mathbf{r} \in A(mK_n)$ such that $r_i \geq r_{i+1}$ for $1 \leq i < n$. Using the same proof strategy as that of Theorem 5.3.1, we can exploit the regularity of mK_n to give a refinement.

Corollary 5.4.1. *Let mK_n and $A_{\text{dec}}(mK_n)$ be as defined above. Then $\#A_{\text{dec}}(mK_n)$ is bounded above by*

$$\frac{(n-1)!}{2}\left(\prod_{k=0}^{n-4}(n-k)^{2^{n-3-k}-1}\right)\left(m^{2^{n-2}-1}\right)\left(f\left(m^{2^{n-1}}\prod_{k=3}^{n}k^{2^{k-2}}\right)+1\right), \tag{5.4.1}$$

where f is any monotonically increasing function that is an upper bound for σ_0. In particular, we may again take $f(x) = x^{\frac{1.538\log(2)}{\log(\log(x))}}$ as above.

Proof. The proof follows that of Theorem 5.3.1, proceeding by induction on n. The base case of $n = 2$ is again a consequence of Lemma 5.3.2, since $\#A_{\text{dec}}(mK_2) = \frac{\#A(mK_2)+1}{2}$. Assume (5.4.1) holds for mK_{n-1}. The key improvement to the argument in the proof of Theorem 5.3.1 is that we can refine (5.3.5) since $\delta_{1i} = m$ for all $2 \leq i \leq n$:

$$d_1 = m\left(\frac{r_2}{r_1} + \cdots + \frac{r_n}{r_1}\right) \leq (n-1)m.$$

After removing v_1, the same argument as in the proof of Theorem 5.3.1 gives

$$\#A_{\text{dec}}(mK_n) \leq \sum_{d_1=1}^{(n-1)m} \#A_{\text{dec}}\left((m^2 + d_1 m)K_{n-1}\right).$$

Since the upper bound in (5.4.1) is monotonic in m for fixed n, we can safely bound $\#A_{\text{dec}}(mK_n)$ above by $(n-1)m$ times the upper bound for $\#A_{\text{dec}}\left((nm^2)K_{n-1}\right)$ as follows:

$$\begin{aligned}
\#A_{\text{dec}}(mK_n) \leq (n-1)m \cdot \frac{(n-2)!}{2}\left(\prod_{k=0}^{n-5}(n-1-k)^{2^{n-4-k}-1}\right)\cdots \\
\cdots\left((nm^2)^{2^{n-3}-1}\right)\left(f\left((nm^2)^{2^{n-2}}\prod_{k=3}^{n-1}k^{2^{k-2}}\right)+1\right) \\
= \frac{(n-1)!}{2}\left(\prod_{k=1}^{n-4}(n-k)^{2^{n-3-k}-1}\right)\left(n^{2^{n-3}-1}\right)\cdots \\
\cdots\left(m^{1+2(2^{n-3}-1)}\right)\left(f\left(m^{2(2^{n-2})}n^{2^{n-2}}\prod_{k=3}^{n-1}k^{2^{k-2}}\right)+1\right) \\
= \frac{(n-1)!}{2}\left(\prod_{k=0}^{n-4}(n-k)^{2^{n-3-k}-1}\right)\left(m^{2^{n-2}-1}\right)\left(f\left(m^{2^{n-1}}\prod_{k=3}^{n}k^{2^{k-2}}\right)+1\right)
\end{aligned}$$

By induction this bound holds for all $n \geq 2$ and $m \geq 1$. □

Remark. For any fixed n, Corollary 5.4.1 improves on Theorem 5.1.1 by a factor of a constant depending on n, since $\#E(mK_n) = m\binom{n}{2}$. This is a substantial improvement if we hold m fixed and n is allowed to vary. Asymptotically however, this bound can be improved upon (see Corollary 5.4.3) using results on Egyptian fractions of Browning–Elsholtz [BE11] and Elsholtz–Planitzer [EP20], which we discuss in Subsection 5.4.2.

To see how the bound of Corollary 5.4.1 compares to reality, we can use Construction 5.2.1 to enumerate all the arithmetical structures on mK_n for several small values of m and n. This also serves as a proof of concept for how one might use the construction to produce an algorithm to generate all arithmetical structures on a given graph more generally.

Let (r_1, r_2, r_3) be a candidate for an arithmetical structure on mK_3, and assume that $r_1 \geq r_2 \geq r_3$. Then by Lemma 5.2.2 and Lemma 5.3.2, a necessary condition to be an arithmetical structure is that $r_2, r_3 \mid (m^2 + d_1 m)$. Assuming this, we fix an integer d_1, which by (5.3.5) is no more than $2m$. Next, we can check all possible pairs of r_2 and r_3 satisfying the divisibility above, and verify whether the corresponding $r_1 = m \cdot (r_2 + r_3)/d_1$ forms an arithmetical structure (r_1, r_2, r_3). The following conditions are necessary and sufficient for this to occur.

1. $r_1 \geq r_2$ which is equivalent to $(r_2 + r_3) \cdot m/d_1 \geq r_2$, or $mr_3 \geq (d_1 - m)r_2$.

2. Since $r_1 \in \mathbb{Z}$, $d_1 \mid m(r_2 + r_3)$.

3. By construction, $d_1 \in \mathbb{Z}$, but we also need that $d_2, d_3 \in \mathbb{Z}$. This is the same as

$$r_2 \mid mr_3 + m \cdot \frac{m}{d_1}(r_2 + r_3).$$

   The same is true with the roles of r_2 and r_3 reversed.

4. $\gcd(r_1, r_2, r_3) = 1$. If $\gcd(r_2, r_3) = 1$ this is automatically satisfied.

Using Lemma 5.3.2, we can enumerate all the arithmetical structures on $(m^2 + d_1 m)K_2$ for $d_1 = 1, 2, \ldots, 2m$ and use conditions (1) — (4) above to determine which lift to arithmetical structures on mK_3. We have written code in Magma that implements this algorithm to enumerate $A_{\text{dec}}(mK_n)$, which can be found at this webpage. For $n > 3$, some extra steps need to be performed.

We can translate the conditions above for general n to recursively compute arithmetical structures on mK_n. Since $(r_2, r_3, \ldots, r_n)$ may have a common factor, we need to include an extra step in the algorithm. We recursively compute all possible arithmetical structures on $(m^2 + d_1 m)K_{n-1}$ for each d_1. However, we allow this function to return values of $(r_2, r_3, \ldots, r_n)$ with a common factor, but would otherwise be an arithmetical structure. We use this to generate a list of $(r_1, r_2, \ldots, r_n)$ satisfying conditions 1 through 3 above, and then at the end we check which of these satisfy condition 4.

Table 5.4.1 compares $\#A_{\text{dec}}(mK_n)$, enumerated by the methods described above, and the upper bound given by the floor of the right hand side of (5.4.1) for several small values of n and m. The comparison shows that the bound of Corollary 5.4.1 leaves much room for potential improvement, with its growth quickly outpacing the true value. The listed values were able to be computed reasonably quickly, but generating the full set of arithmetical structures on mK_n becomes computationally challenging even for small m values when $n > 3$.

n	m	$\#A_{\text{dec}}(mK_n)$	Right hand side of (5.4.1)
3	1	3	20
3	2	10	56
3	3	21	127
3	4	28	229
3	5	36	362
3	6	57	526
3	7	42	720
3	8	70	946
3	9	79	1201
3	10	96	1487
3	100	1106	142796
3	101	164	145584
4	1	14	688
4	2	108	23028
4	3	339	173664
4	4	694	717812
4	5	1104	2141953
4	6	1816	5209709
4	7	2021	11012969
4	8	3363	21019441
4	9	4053	37117341
4	10	5370	61657730
5	1	147	8567815

Table 5.4.1: A comparison of the value $\#A_{\text{dec}}(mK_n)$ with the bound given in Corollary 5.4.1.

Remark (Growth of $\#A_{\text{dec}}(mK_n)$)**.** This example will help illustrate why there is so much room for improvement. Given m_1, n, and an arithmetical structure on m_1K_n, Construction 5.2.1 gives us a way to produce an associated arithmetical structure on m_2K_{n-1}, where $m_2 = m_1^2 + s_1m_1$ for the appropriate value of s_1. Iterating this procedure, we can get an arithmetical structure on m_iK_{n-i+1}, where $m_i = m_{i-1}^2 + s_{i-1}m_{i-1}$ for $2 \leq i \leq n-1$. For each such i, we therefore have that $m_i \geq m_{i-1}^2 + m_{i-1}$. Using this inequality for each i, the result of this process is an arithmetical structure on $m_{n-1}K_2$ with $m_{n-1} \geq f^{n-2}(m_1) = O(m_1^{2^{n-2}})$, where $f(m) = m^2 + m$. Furthermore, this is only for a given arithmetical structure. If we are interested in generating a list of all arithmetical structures on m_1K_n, there are many choices for the value of s_1 at each step. If every arithmetical structure on each of these $m_{n-1}K_2$ came from an arithmetical structure on m_1K_n following this iterative procedure, then the comparison in Table 5.4.1 would be significantly closer. This is clearly not the case, and one challenge in improving the bounds given in Theorem 5.1.1 and Corollary 5.4.1 is that it is difficult to say which of which of these arithmetical structure on the base graphs such as $m_{n-1}K_2$ "lift" to arithmetical structures on the original graph, such as m_1K_n.

5.4.2 Connections to Egyptian fractions

The study of Egyptian fractions focuses on integer solutions to (5.1.4), for any given positive integers m and n. Such solutions are in one-to-one correspondence with arithmetical structures on the graph mK_n. This allows us to use the theory of Egyptian fractions to study arithmetical structures on mK_n. While this correspondence is well known in the $m = 1$ case, we have not encountered this in the literature for general m, so we provide an elementary proof.

Theorem 5.4.2. *The set $A(mK_n)$ is in one to one correspondence with solutions $(x_1, ..., x_n)$ to (5.1.4). Explicitly, the arithmetical structure $(\boldsymbol{r}, \boldsymbol{d}) \in A(mK_n)$ corresponds to the solution $(d_1 + m, \ldots, d_n + m)$ to (5.1.4).*

Proof. Let $(\mathbf{r}, \mathbf{d})$ be an arithmetical structure on mK_n and recognize that

$$\sum_{i=1}^{n} \frac{r_i}{m\sum_{j=1}^{n} r_j} = \frac{1}{m}.$$

Using the system (5.1.1) we may write

$$\frac{r_i}{m\sum_{j=1}^{n} r_j} = \frac{r_i}{mr_i + d_ir_i} = \frac{1}{m+d_i}.$$

Thus we have

$$\sum_{i=1}^{n} \frac{1}{m+d_i} = \frac{1}{m},$$

so by taking $x_i = m + d_i$ we have a solution to (5.1.4).

We now show that given a solution $\mathbf{x}$ to (5.1.4), we can find an arithmetical structure for which $x_i = m + d_i$. Setting $d_i = x_i - m$ in the system (5.1.1), we need the null space of

$$\begin{pmatrix} m - x_1 & m & \cdots & m \\ m & m - x_2 & \cdots & m \\ \vdots & \vdots & \ddots & \vdots \\ m & m & \cdots & m - x_n \end{pmatrix} \tag{5.4.2}$$

to have dimension exactly one. Subtracting the first row from all other rows, and scaling row i by $1/x_i$ for $i \geq 2$, we have that this matrix is row equivalent to

$$\begin{pmatrix} m - x_1 & m & m & \cdots & m \\ -x_1/x_2 & 1 & 0 & \cdots & 0 \\ -x_1/x_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -x_1/x_n & 0 & 0 & \cdots & 1 \end{pmatrix}$$

After subtracting the first row by multiples of m of the other rows, all entries are zero except the top left, which becomes

$$m - x_1 + \frac{mx_1}{x_2} + \cdots + \frac{mx_1}{x_n}.$$

Multiplying this expression by $x_2 \cdots x_n$ gives $m(x_1 \cdots x_{n-1} + \cdots + x_2 \cdots x_n) - x_1 \cdots x_n$, which is 0 by (5.1.4). Hence the matrix is reduced to

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ -x_1/x_2 & 1 & 0 & \cdots & 0 \\ -x_1/x_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -x_1/x_n & 0 & 0 & \cdots & 1 \end{pmatrix},$$

which clearly has rank $n-1$ and null space with dimension 1. An integral generator of the null space is

$$\mathbf{q} = (x_2 \cdots x_n, x_1 x_3 \cdots x_n, \ldots, x_1 \cdots x_{n-1})^T.$$

We construct an arithmetical structure by taking $\mathbf{r} = \mathbf{q}/\gcd(\mathbf{q})$ and setting $d_i = x_i - m$. These two processes, going from arithmetical structure on mK_n to a solution $\mathbf{x}$ to (5.1.4), are clearly inverse to one another. □

With Theorem 5.4.2, we can use known results bounding the number of Egyptian fraction representations for a given fraction to give a bound for $\#A_{\text{dec}}(mK_n)$ and compare this to that of Corollary 5.4.1. Modifying slightly the notation of [BE11], we define

$$f_n(a,m) = \#\left\{(x_1, \ldots, x_n) \in \mathbb{N}^n \colon x_1 \leq \cdots \leq x_n \text{ and } \frac{a}{m} = \frac{1}{x_1} + \cdots + \frac{1}{x_n}\right\} \quad (5.4.3)$$

to count the number of Egyptian fraction representations of a/m by n terms. Observe that an arithmetical structure $(\mathbf{r}, \mathbf{d})$ on mK_n satisfies $r_1 \geq \cdots \geq r_n$ if and only if $d_1 \leq \cdots \leq d_n$, so by the correspondence in the proof of Theorem 5.4.2, we have

$$f_n(1,m) = \#A_{\text{dec}}(mK_n).$$

The best known asymptotic bounds for $f_n(1,m)$ are given by Elsholtz–Planitzer [EP20, Theorems 1.1, 1.4], improving on Browning–Elsholtz [BE11, Theorems 2, 3], giving us the following corollary.

Corollary 5.4.3. *Let $n \geq 3$, $m \geq 1$, and fix $\epsilon > 0$. Then we have*

$$\begin{aligned} &\#A_{\text{dec}}(mK_3) \ll_\epsilon m^{\frac{3}{5}+\epsilon}, \\ &\#A_{\text{dec}}(mK_4) \ll_\epsilon m^{\frac{28}{17}+\epsilon}, \ \textit{and} \\ &\#A_{\text{dec}}(mK_3) \ll_\epsilon (nm)^\epsilon \left(n^{4/3}m^2\right)^{\frac{28}{17}2^{n-5}} \quad \textit{when } n \geq 5. \end{aligned}$$

Note that while this is an asymptotic improvement over Corollary 5.4.1, it does not give explicit constants. We also note that the exponential shape of the bounds in Corollaries 5.4.1 and 5.4.3 are somewhat similar. This may suggest that it would take a significant advance to close the large gap between the actual values and known bounds, as seen in Table 5.4.1.

Bibliography

[ABDL^{+}20] Kassie Archer, Abigail C. Bishop, Alexander Diaz-Lopez, Luis D. García Puente, Darren Glass, and Joel Louwsma. Arithmetical structures on bidents. *Discrete Math.*, 343(7):111850, 23, 2020.

[BCC^{+}18] Benjamin Braun, Hugo Corrales, Scott Corry, Luis David García Puente, Darren Glass, Nathan Kaplan, Jeremy L. Martin, Gregg Musiker, and Carlos E. Valencia. Counting arithmetical structures on paths and cycles. *Discrete Math.*, 341(10):2949–2963, 2018.

[BE11] T. D. Browning and C. Elsholtz. The number of representations of rationals as a sum of unit fractions. *Illinois J. Math.*, 55(2):685–696 (2012), 2011.

[Ble72] M. N. Bleicher. A new algorithm for the expansion of Egyptian fractions. *J. Number Theory*, 4:342–382, 1972.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[Cho19] Michael Chou. Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$. *Pacific J. Math.*, 302(2):481–509, 2019.

[CV18] Hugo Corrales and Carlos E. Valencia. Arithmetical structures on graphs. *Linear Algebra Appl.*, 536:120–151, 2018.

[DEMZB20] Maarten Derickx, Anastassia Etropolski, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *arXiv:2007.13929*, 2020.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

[DLRNS18] Harris B. Daniels, Álvaro Lozano-Robledo, Filip Najman, and Andrew V. Sutherland. Torsion subgroups of rational elliptic curves over the compositum of all cubic fields. *Math. Comp.*, 87(309):425–458, 2018.

[EP20] Christian Elsholtz and Stefan Planitzer. The number of solutions of the erdős-straus equation and sums of k unit fractions. *Proceedings of the Royal Society of Edinburgh: Section A Mathematics*, 150(3):1401–1427, 2020.

[Etr15] Anastassia Etropolski. Local-global principles for certain images of galois representations. *arXiv:1502.01288*, 2015.

[Fuj04] Yasutsugu Fujita. Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$. *Acta Arith.*, 115(1):29–45, 2004.

[Fuj05] Yasutsugu Fujita. Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$. *J. Number Theory*, 114(1):124–134, 2005.

[Guy04] Richard K. Guy. *Unsolved problems in number theory.* Problem Books in Mathematics. Springer-Verlag, New York, third edition, 2004.

[GW19] Darren Glass and Joshua Wagner. Arithmetical Structures on Paths With a Doubled Edge. *arXiv e-prints*, page arXiv:1903.01398, Mar 2019.

[HL20] Zachary Harris and Joel Louwsma. On arithmetical structures on complete graphs. *Involve*, 13(2):345–355, 2020.

[JKL11] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(273):579–591, 2011.

[JKS04] D. Jeon, C.H. Kim, and A. Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arithmetica*, 113:291–301, 2004.

[Kam86] S. Kamienny. Torsion points on elliptic curves over all quadratic fields. *Duke Math. J.*, 53(1):157–162, 1986.

[Ken82] M. A. Kenku. On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class. *J. Number Theory*, 15(2):199–202, 1982.

[KM88] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[LL85] Michael Laska and Martin Lorenz. Rational points on elliptic curves over $\mathbf{Q}$ in elementary abelian 2-extensions of $\mathbf{Q}$. *J. Reine Angew. Math.*, 355:163–172, 1985.

[Lor89] Dino J. Lorenzini. Arithmetical graphs. *Math. Ann.*, 285(3):481–501, 1989.

[LR13] Álvaro Lozano-Robledo. On the field of definition of p-torsion points on elliptic curves over the rationals. *Math. Ann.*, 357(1):279–305, 2013.

[LR18] Álvaro Lozano-Robledo. Uniform boundedness in terms of ramification. *Res. Number Theory*, 4(1):Paper No. 6, 39, 2018.

[Maz77a] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

[Maz77b] B. Mazur. Rational points on modular curves. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 107–148. Lecture Notes in Math., Vol. 601, 1977.

[Mor22] Louis J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Philos. Soc.*, 21:179–192, 1922.

[Naj16] Filip Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Lett.*, 23(1):245–272, 2016.

[Nic88] Jean-Louis Nicolas. On highly composite numbers. In *Ramanujan revisited (Urbana-Champaign, Ill., 1987)*, pages 215–244. Academic Press, Boston, MA, 1988.

[RSZB] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of galois for elliptic curves over $\mathbb{Q}$. *In preparation.*

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory*, 1:Paper No. 12, 34, 2015.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[Sut16] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:Paper No. e4, 79, 2016.

[SZ17] Andrew V. Sutherland and David Zywina. Modular curves of prime-power level with infinitely many rational points. *Algebra Number Theory*, 11(5):1199–1229, 2017.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929.

[Wil95] Andrew Wiles. Modular forms, elliptic curves, and Fermat's last theorem. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*, pages 243–245. Birkhäuser, Basel, 1995.

[Zyw15] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv:1508.07660*, 2015.