Distribution Agreement

Signature:

______________________________ __________

Alexis Newton Date

Low-degree points on some rank 0 modular curves

By

Alexis Newton
Doctor of Philosophy

Mathematics

David Zureick-Brown, Ph.D.
Advisor

Parimala Raman, Ph.D.
Committee Member

Suresh Venapally, Ph.D.
Committee Member

Accepted:

Kimberly J. Arriola, Ph.D.
Dean of the James T. Laney School of Graduate Studies

Date

Low-degree points on some rank 0 modular curves

By

Alexis Newton
B.A., High Point University, NC, 2018
M.A., Wake Forest University, NC, 2020

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
2025

Abstract

Low-degree points on some rank 0 modular curves
By Alexis Newton

Let E be an elliptic curve defined over a number field K. We present some new progress on the classification of the finite groups which appear as the torsion subgroup of $E(K)$ as K ranges over quartic, quintic and sextic number fields. In particular, we concentrate on determining the quartic, quintic and sextic points on certain modular curves $X_1(N)$ for which the rank of the Jacobian is zero.

Low-degree points on some rank 0 modular curves

By

Alexis Newton
B.A., High Point University, NC, 2018
M.A., Wake Forest University, NC, 2020

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
2025

Acknowledgments

To David Zureick-Brown, thank you for your patience and unwavering support in achieving my goals. The instruction, advice, and guidance provided was invaluable to my success.

To my committee members, Parimala Raman and Suresh Venapally, thank you for the feedback and comments on each version of this work.

To Jeremy Rouse and Jenny Sharpe, I could not have asked for better undergraduate and master's advisors. You truly helped me see the worth in myself as a researcher and a scholar.

To my collaborator Michael Cerchia, thank you for always being willing to sit for hours in a coffee shop with me (and for watching my cats).

To Holly Paige Chaos, Jasmine Camero, Santiago Arango-Piñeros, and Robert Hernandez, the friendship (and help) you provided was immeasurable. Graduate school would have been insurmountable without you.

To Mom and Dad, you inspire me daily. The phone calls and the love you send are a driving force in my life as a researcher, teacher, and human being. I know that my life path would be so different without you.

Contents

List of Figures

Chapter 1

Introduction

A classical theorem of Barry Mazur [9] states that the torsion subgroup of an elliptic curve, $E(\mathbb{Q})_{\text{tors}}$, is isomorphic to one of 15 different groups over the rational numbers:

Theorem 1.0.1 (Mazur [9], 1978)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups.*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && \textit{for } 1 \leq N \leq 10 \textit{ or } N = 12 \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && \textit{for } 1 \leq N \leq 4. \end{aligned}$$

Since modular curves parameterize elliptic curves, we can restate Mazur's theorem. Let K be a number field. Let $Y_1(N)$ be the curve parameterizing pairs (E, P), where E/K is an elliptic curve, and P is a point of exact order N on E, and let $Y_1(M, N)$ (with $M|N$) be the curve parameterizing E/K such that $E(K)_{\text{tors}}$ contains $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$. Let $X_1(N)$ and $X_1(M, N)$ be the smooth compactifications of $Y_1(N)$ and $Y_1(M, N)$. Then $X_1(N)$ and $X_1(2, 2N)$ have rational points for exactly the values of N appearing in Mazur's theorem.

This prompts the question, if we fix $d \geq 1$, can we say something about the groups which can occur as $E(K)_{\text{tors}}$ for K a field extension of $\mathbb{Q}$ of degree d?

Merel [10] showed in 1996 that for every integer $d \geq 1$, there is a constant $N(d)$ such that for all $K/\mathbb{Q}$ of degree at most d and all E/K,

$$\#E(K)_{\text{tors}} \leq N(d).$$

Thus the size of $E(K)_{\text{tors}}$ is dependent only on the degree of the field extension of K over $\mathbb{Q}$.

We can further ask for a classification of such groups. For the case of quadratic extensions, when $d = 2$, Kamienny [7] and Kenku-Momose [8] find that $E(K)_{\text{tors}}$ must be one of 26 groups for E an elliptic curve over a quadratic number field K:

Theorem 1.0.2 (Kamienny-Kenku-Momose, 1980's). *Let E be an elliptic curve over a quadratic number field K. Then $E(K)_{tors}$ is one of the following groups.*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && \textit{for } 1 \leq N \leq 16 \textit{ or } N = 18, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && \textit{for } 1 \leq N \leq 6, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}, && \textit{for } 1 \leq N \leq 2, \textit{ or} \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Similarly, the cubic case where $d = 3$ has also be completely classified by Derickx, Etropolski, Morrow, van Hoeij, and Zurieck-Brown [5].

Let $K/\mathbb{Q}$ be a cubic extension and E/K be an elliptic curve. Then $E(K)_{\text{tors}}$ is isomorphic to one of 26 different groups. It is important to note that this set of groups overlaps but is distinct from the 26 groups found in the quadratic case. Another notable difference with this case is the existence of a singular sporadic point discovered by Najman [11]. Derickx, Etropolski, Morrow, van Hoeij, and Zurieck-

Brown [5] show that there exist infinitely many $\mathbb{Q}$-isomorphism classes for each such torsion subgroup listed below, except for $\mathbb{Z}/21\mathbb{Z}$. In this case, the base change of the elliptic curve 162b1 to $\mathbb{Q}(\zeta_9)^+$ is the unique elliptic curve over a cubic field with $\mathbb{Z}/21\mathbb{Z}$-torsion.

Theorem 1.0.3 (Derickx–Etropolski–Morrow–van Hoeij–Zurieck-Brown [5], 2020)**.** *Let $K/\mathbb{Q}$ be a cubic extension and E/K be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following 26 groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && \textit{with } 1 \leq N \leq 21, N \neq 17, 19, \textit{ and} \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && \textit{with } 1 \leq N \leq 7. \end{aligned}$$

Finally, significant progress has been made on the quartic case where $d = 4$. Jeon, Kim, and Park [6] find that as K varies over all quartic number fields and E varies over all elliptic curves over K, the group structures which appear infinitely often as $E(K)_{\text{tors}}$ are one of 38 groups.

Theorem 1.0.4 (Jeon–Kim–Park [6], 2006)**.** *If K varies over all quartic number fields and E varies over all elliptic curves over K, the group structures which appear* *infinitely often as $E(K)_{tors}$ are exactly the following:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && N = 1-18, 20-22, 24 \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && N = 1-9, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}, && N = 1-3, \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N\mathbb{Z}, && N = 1-2, \\ &\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, && \\ &\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, && \end{aligned}$$

Following this result, it was the initial goal of this dissertation to complete the classification of the finite groups that appear as the torsion subgroup of $E(K)$ for K a quartic number field. However, recent work (December 2024) of Maarten Derickx and Filip Najman [3] completed this classification. Detailed in this dissertation is the work completed on classifying quartic torsion up to December 2024, with some further results over quintic and sextic number fields using the same methods.

Thus for the quartic case, Maarten Derickx and Filip Najman [3] show that the group structures which appear as $E(K)_{\text{tors}}$ are one exactly the groups that appear infinitely often. This means that there are no cases of sporadic quartic torsion.

Theorem 1.0.5 (Derrickx–Najman [3], 2024)**.** *If K varies over all quartic number fields and E varies over all elliptic curves over K, the group structures which appear* *as* $E(K)_{tors}$ *are exactly the following:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && \text{with } 1 \leq N \leq 24, N \neq 19, 23, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && \text{with } 1 \leq N \leq 9, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} && \text{with } 1 \leq N \leq 3, \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N\mathbb{Z} && \text{with } 1 \leq N \leq 2, \\ &\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}, && \\ &\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, && \end{aligned}$$

Using different techniques to Derickx and Najman [3], my collaborator Michael Cerchia and I confirm the classification for some N in the quartic case, as well as extend the classification for some N in the quintic and sextic cases:

Theorem 1.0.6 (Cerchia–Newton, 2024)**.** *For* $N = 25, 26, 27, 28, 34, 35$ *and* 40*, the modular curve* $X_1(N)$ *has no non-cuspidal quartic points.*

Theorem 1.0.7 (Cerchia–Newton, 2025)**.** *For* $N = 26, 27, 34$ *and* 40*, the modular curve* $X_1(N)$ *has no non-cuspidal quintic points.*

Theorem 1.0.8 (Cerchia–Newton, 2025)**.** *For* $N = 34$*, the modular curve* $X_1(N)$ *has no non-cuspidal sextic points.*

The code for each of these proofs can be found in the GitHub repository at `https://github.com/alexisnewton/Low-degree-points-on-some-rank-0-modular-curves`. The remainder of this dissertation will detail background material in Chapter 2, methods in Chapter 3, proofs in Chapter 4, and future work in Chapter 5.

Chapter 2

Background

2.1 Elliptic Curves

An elliptic curve E is a smooth, projective, algebraic curve of genus one, with a distinguished point $\mathcal{O}$.

Definition. For field K (with characteristic not 2 or 3) an elliptic curve defined over K can be written in Weierstrass form as

$$y^2 = x^3 + Ax + B$$

with $A, B \in K$, where the discriminant $\Delta(E) = -16(4A^3 + 27B^2) \neq 0$.

For simplicity, consider $K = \mathbb{Q}$. If (x_0, y_0) is a point on the curve $y^2 = f(x)$, then so is $(x_0, -y_0)$. Suppose that P and Q are points on E. To add these points, draw a line through P and Q. This line will intersect at a third point R, and if we reflect R across the x-axis, we get a new point $P + Q$. (If $P = Q$, we draw the tangent line to the curve there to find $P + Q$.)

We let $E(\mathbb{Q})$ be the set of rational points on E. The " + " operation of addding points as defined above has the following five properties.

1. If P and Q are in $E(\mathbb{Q})$, the $P + Q$ is also in $E(\mathbb{Q})$.

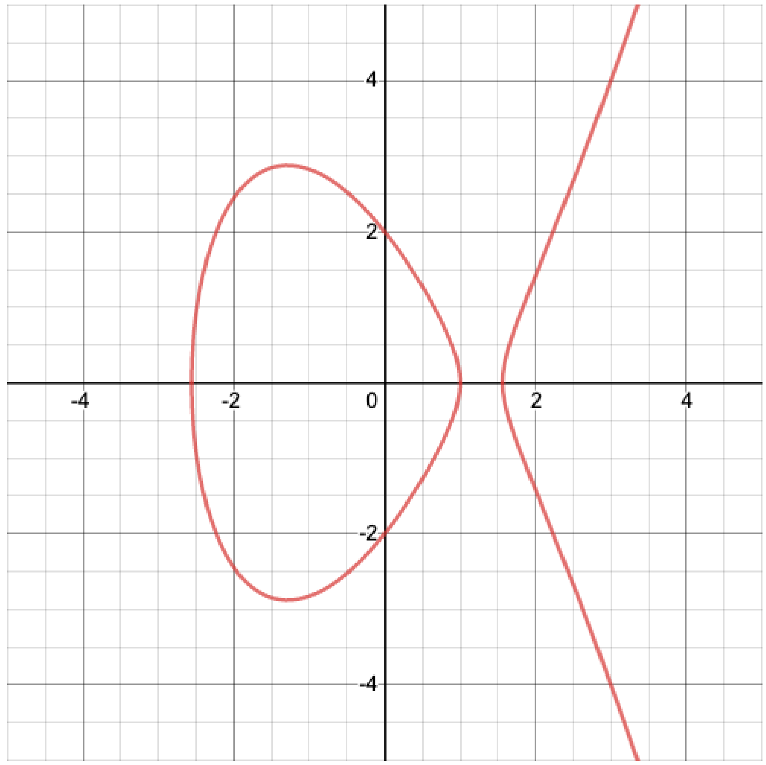


Figure 2.1: $E : y^2 = x^3 - 5x + 4, \Delta = 1088$

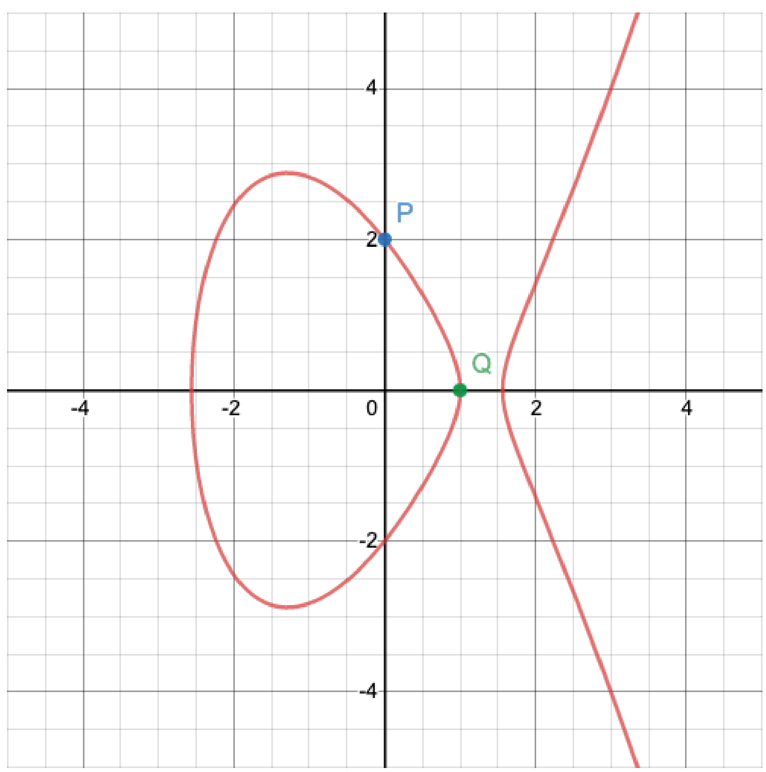


Figure 2.2: Suppose that P and Q are points on E.

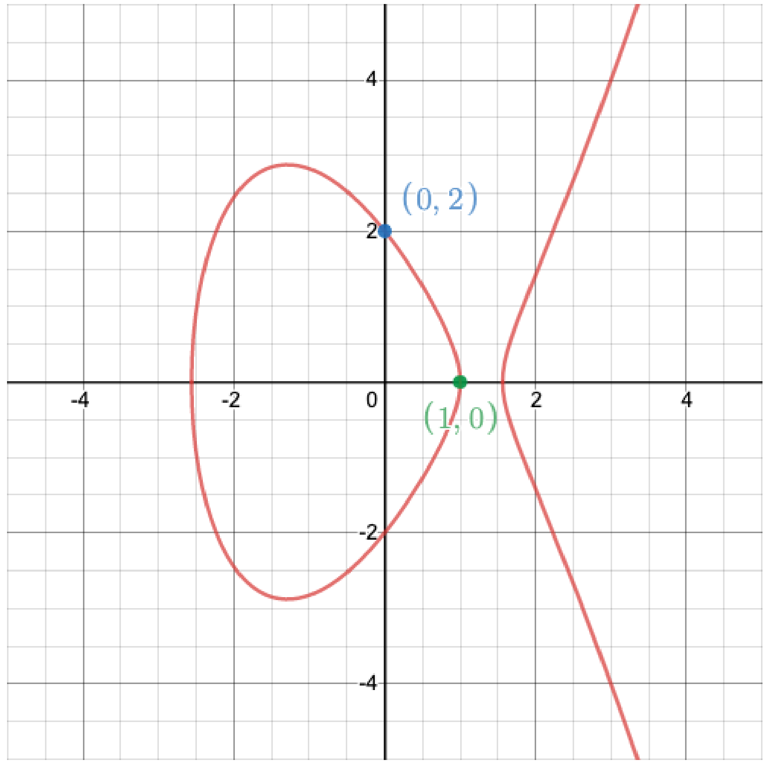


Figure 2.3: Let $P = (0, 2)$ and $Q = (1, 0)$

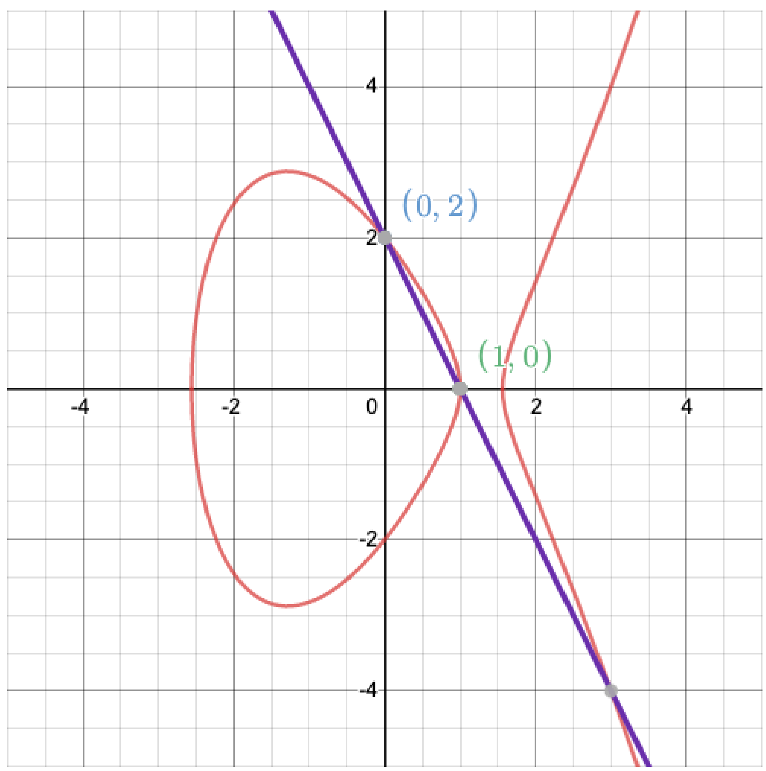


Figure 2.4: To add these points, draw a line through P and Q.

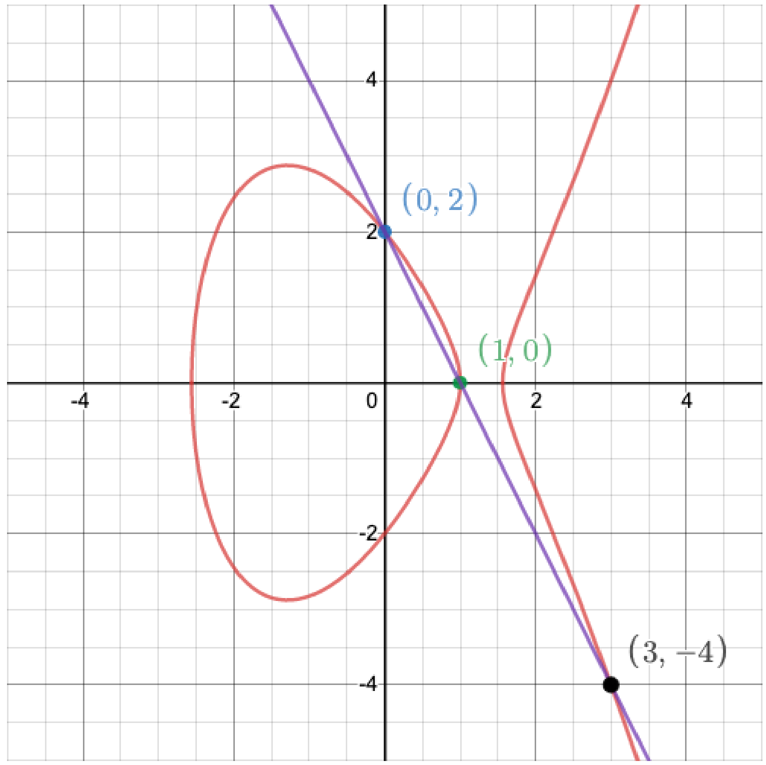


Figure 2.5: This line will intersect with a third point R.

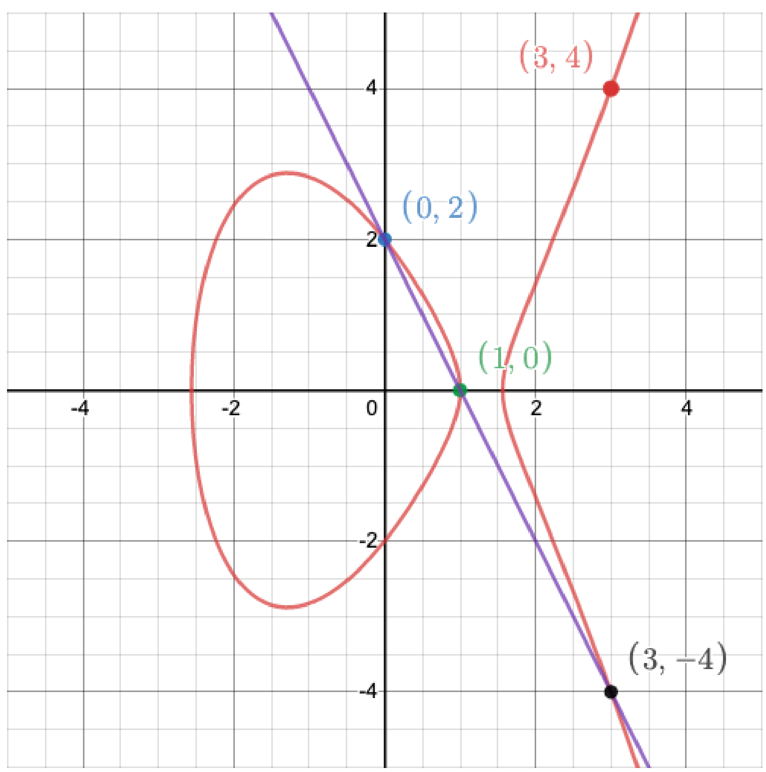


Figure 2.6: Reflect R across the x-axis.

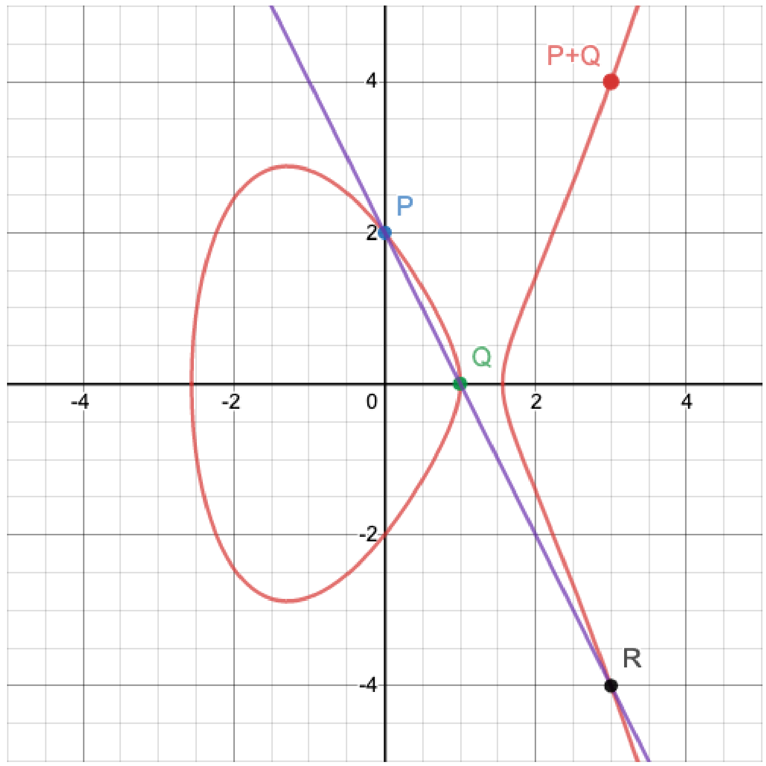


Figure 2.7: We get a new point $P + Q$.

2. If $P, Q, R \in E(\mathbb{Q})$, then $(P + Q) + R = P + (Q + R)$.

3. If $\mathcal{O} = (0 : 1 : 0)$, then $P + \mathcal{O} = P$ for all $P \in E(\mathbb{Q})$.

4. If $P = (x : y : z)$, let $-P = (x : -y : z)$. Then, $P + (-P) = \mathcal{O}$.

5. For all $P, Q \in E(\mathbb{Q})$, $P + Q = Q + P$.

Therefore under the operation of adding points, $E(\mathbb{Q})$ forms an abelian group. See Figure 2.7 for an explicit example.

More generally, we have the following result over a number field K.

Theorem 2.1.1 (Mordell-Weil, 1928)**.** *For an elliptic curve E, $E(K)$ is a finitely-generated abelian group, and $E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$ where $E(K)_{tors}$ is a finite abelian group and $r \geq 0, r \in \mathbb{Z}$.*

The number r is called the *rank* of $E(K)$. This is the number of independent points of infinite order on the curve. Notice that this implies $E(K)$ is finite if and only if $r = 0$. The set of points with finite order on E is called the torsion subgroup. It is denoted by $E(K)_{\text{tors}}$ and can be isomorphic to the following groups 15 groups when $K = \mathbb{Q}$.

Theorem 2.1.2 (Mazur [9], 1978)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups.*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && \textit{for } 1 \leq N \leq 10 \textit{ or } N = 12 \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && \textit{for } 1 \leq N \leq 4. \end{aligned}$$

2.2 Modular Curves

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The modular curves $X(N)$ are defined to be the quotients of the extended upper-half plane by the action of Γ.

Definition. Let N be a natural number. Define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

The modular curves associated with the above congruence subgroups will be denoted by $X(N)$, $X_0(N)$, and $X_1(N)$.

The non-cuspidal K-rational points of the modular curve $X_1(M, MN)$ classify elliptic curves E and independent points P and Q of order M and MN defined over K. If we let $M = 1$, then we may define $X_1(N) := X_1(1, N)$. The non-cuspidal K-rational points of the modular curve $X_1(N)$ classify elliptic curves over K which have a torsion point of exact order N defined over K.

For computational purposes, we need explicit equations for all of these modular curves. For $X_1(N)$, we use Andrew Sutherland's optimized equations generated from [14].

2.2.1 Intermediate Modular Curves

Definition. Let N be a natural number. Define

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

for $\langle a \rangle = \Delta \subseteq (\mathbb{Z}/N\mathbb{Z})^*$.

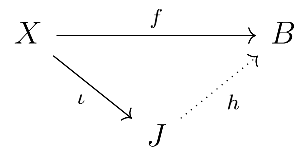
The modular curve associated with the above congruence subgroup will be denoted $X_H(N)$ For a subgroup $\Gamma_1(N) \subseteq H \subseteq \Gamma_0(N)$, we can form the "intermediate" modular curve $X_H(N)$. This curve is a quotient of $X_1(N)$ by a subgroup of $\mathrm{Aut}(X_1(N))$, and (roughly) parameterizes elliptic curves whose mod N Galois representation has image contained in H ([13], Lemma 2.1).

For $X_H(N)$, we use David Zywina's code from [16] to produce the modular curves X_H for a given subgroup H of $\mathrm{SL}_2(\mathbb{Z})$.

2.2.2 The Jacobian

Let X be a smooth, projective, and geometrically integral k-curve. Suppose that X has a k-point. Then there is a k-variety $J = \operatorname{Jac} X$ called the Jacobian of X such that $J(k)$ is naturally in bijection with $\mathrm{Pic}^0 X$

Theorem 2.2.1 (Thm 5.3.1, [12]). *Let X be a smooth, projective, and geometrically integral k-curve. Let $J = \operatorname{Jac} X$. Suppose that P is a k-point of X. Any morphism $f : X \to B$ from X to an abelian variety B satisfying $f(P) = O$ factors uniquely through J: i.e., there is a unique homomorphism $h : J \to B$ such that the following commutes:*



2.3 The Cuspidal Subscheme Lemma

The analysis of quartic, quintic, and sextic points relies on understanding the cuspidal subscheme of $X_1(N)$.

Lemma 2.3.1 (Derickx–Etropolski–Morrow–van Hoeij–Zurieck-Brown [5], 2020). *Let $N \geq 5$ be a positive integer, and let $R = \mathbb{Z}[1/2N]$.*

1. *The cuspidal subscheme of $X_1(N)_R$ is isomorphic to*

$$\bigsqcup_{d|N} (\mu_{N/d} \times \mathbb{Z}/d\mathbb{Z})'/[-1],$$

   where the prime notation refers to points of maximal order.

2. *The cuspidal subscheme of $X_0(N)_R$ is isomorphic to*

$$\bigsqcup_{d|N} (\mu_{\gcd(d,N/d)})'$$

   where the prime notation refers to points of maximal order.

This result for intermediate curves is generally known. See Section 3.3 of [15]. We use the following code by Jeremy Rouse to determine the cuspidal subsheme for $X_H(N)$.

```
// Code by Jeremy Rouse, Wake Forest University
// let HH equal H the subgroup of (Z/NZ)* (make sure it includes -I)
HH:= //insert here

phiN := EulerPhi(N);
G := GL(2,Integers(N));

// This function does the same as genus, but it takes a subgroup.

function genus2(G)
  md := Modulus(BaseRing(G));
  H := SL(2,Integers(md));
  S := H![0,-1,1,0];
  T := H![1,1,0,1];
  phi, perm := CosetAction(H,G meet H);
  lst := [phi(S),phi(T),phi(S*T)];
  //printf "Permutation for S = %o.\n",phi(S);
  //printf "Permutation for T = %o.\n",phi(T);
  //printf "Permutation for S*T = %o.\n",phi(S*T);
  cs := [CycleStructure(lst[i]) : i in [1..3]];
  gen := -2*Degree(perm) + 2;
  einfty := #Orbits(sub<perm | lst[2]>);
  e2 := #Fix(lst[1]);
  e3 := #Fix(lst[3]);
  ind := Degree(perm);
  for j in [1..3] do
    for i in [1..#cs[j]] do
      gen := gen + (cs[j][i][1]-1)*cs[j][i][2];
    end for;
  end for;
  gen := gen div 2;
  printf "The genus = %o.\n",gen;
  genhur := 1 + (ind/12) - (e2/4) - (e3/3) - (einfty/2);
```

```
  printf "The Hurwitz formula is %o = 1 + %o/12 - %o/4 - %o/3 - %o/2.\n",
  genhur,ind,e2,e3,einfty;
  return gen, ind, einfty, e2, e3;
end function;
gengen, ind, einfty, e2, e3 := genus2(HH);

U, mp := UnitGroup(Integers(N));
lst := [ G![1,0,0,mp(U.i)] : i in [1..NumberOfGenerators(U)]];
lst := [ G![1,1,0,1] ] cat lst;
P := sub<G | lst>;
Q := sub<G | G![1,1,0,1]>;

A, B := CosetAction(G,HH);

galoisorbs := Orbits(A(P));
orbs := Orbits(A(Q));

mults := [];
for i in [1..#galoisorbs] do
  Append(~mults,#[ j : j in orbs | j subset galoisorbs[i]]);
end for;

orbitreps := OrbitRepresentatives(A(P));
rt := RightTransversal(G,HH);
mats := [];
for i in [1..#orbitreps] do
  // For each i, find a permutation g in B so that g(1) = orbitreps[i][2];
  ind := Index([ Image(A(rt[j]),1) eq orbitreps[i][2] : j in [1..#rt]],true);
  Append(~mats,rt[ind]);
end for;
```

```
printf "Subgroup has genus %o. It has %o cusps and %o Galois orbits
of cusps with sizes %o.\n",gengen,einfty,#galoisorbs,mults;
```

Chapter 3

Methods

3.1 Introduction

As our ultimate goal was initially to complete the classification of the finite groups which appear as the torsion subgroup of $E(K)$ for K a quartic number field, we first looked to the methods used in the cubic case [5]. Derickx, Etropolski, Morrow, van Hoeij, and Zurieck-Brown [5] first listed the N for which they needed to consider $X_1(N)$ and $X_1(2, 2N)$. Of these, all but two values of N had Jacobian with rank 0, which they delt with first. Hence we focus in on the curves with Jacobian rank 0 as well. From [5], these are the curves $X_1(N)$ where

$$N = 1, ..., 36, 38, ..., 42, 44, ..., 52, 54, 55, 56, 59, 60, 62, 64, 66, 68, 69, 70, 71, 72, 75, 76,$$
$$78, 81, 84, 87, 90, 94, 96, 98, 100, 108, 110, 119, 120, 132, 140, 150, 168, \text{ and } 180.$$

Recall that the gonality $\gamma(X)$ of X is the minimal degree of a finite K-morphism $X \to \mathbb{P}^1$. Let $d(X)$ denote the least integer for which the set $\{a \in X(K) \Big| [K(a) : K] = d\}$ of points of degree d on X is infinite.

Proposition 3.1.1 (Derickx–Sutherland [4], 2017)**.** *Let X/K be a nice curve whose*

Jacobian has rank zero. Then $d(X) = \gamma(X)$.

This implies that if the gonality is greater than or equal to 5 and the rank of the Jacobian of X is 0, then there are not infinitely many quartic points on the curve on X. In the case of modular curves $X_1(N)$, these are exactly the curves with level structure that corresponds to $N = 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 39, 42, 45, 51, 55,$ and 119. These are the cases we investigated first.

```
///////////////////////////////
// Equations for X_1(26), from Derickx--Sutherland
// Code proves that the gonality (mod p) is at least 5 for X_1(26)
//////////////////////////////

 F := Rationals();
 P<[t]> := ProjectiveSpace(F,9);
 A2<x,y> := AffineSpace(F,2);

 X:=Curve(A2,y^6 + (3*x^2 + 4*x - 2)*y^5 + (3*x^4 + 10*x^3 - 9*x +
  1)*y^4 + (x^6 + 7*x^5 + 8*x^4 - 14*x^3 - 11*x^2 + 6*x)*y^3 + (x^7
   + 4*x^6 - x^5 - 13*x^4 + 2*x^3 + 10*x^2 - x)*y^2 - (x^6 - 7*x^4
  - 4*x^3 + 2*x^2)*y - x^4 - x^3);
 Xp := ProjectiveClosure(X);

   p := 3;
 Cp<[T]> := Curve(Reduction(Xp,p));

 function divisorsOfDegree(C,d : seed := [])
   return
   &join[{ &+([tup[j] : j in [1..#part]]) : tup in
     CartesianProduct([Places(C,i) : i in part])}
      : part in Partitions(d)];
 end function;

```

```
divs := divisorsOfDegree(Cp,4);
#divs;
for D in divs do d := Dimension(RiemannRochSpace(D)); if d gt 1
  then D, d; end if; end for;
```

3.2 Direct Analysis

Let X be a smooth, proper, geometrically connected curve defined over a field K. For a positive integer d, define the d^{th}-symmetric power of X to be $X^{(d)} := X^d/S_d$ where S_d is the symmetric group on d letters.

The K-points of $X^{(d)}$ correspond to effective K-rational divisors on X of degree d. In particular, a point of X/K of degree d gives rise to a divisor of degree d, and thus a point of $X^{(d)}(K)$. We will often identify a degree d point of X with a divisor of degree d without distinguishing notation.

We use a method called Direct Analysis, as described in Derickx, Etropolski, Morrow, van Hoeij, and Zurieck-Brown [5] to show there are no non-cuspial quartic, quintic or sextic points on $X_1(N)$ for some values of N.

Let M equal the degree of the points we wish to study. When $X_1(N)$ has gonality at least $M+1$ and $J_1(N)(\mathbb{Q})$ has rank 0 over $\mathbb{Q}$ one can use Direct Analysis to investigate these curves $X_1(N)$. For values of N such that the genus of $X_1(N)$ and the size of $J_1(N)(\mathbb{Q})$ is not too large, it is possible to do this directly over $\mathbb{Q}$.

We can compute the finitely many pre-images of an Abel-Jacobi map

$$\iota : X_1(N)^{(M)}(\mathbb{Q}) \to J_1(N)(\mathbb{Q}).$$

To do this, we begin by fixing a base point $\infty \in X_1(N)(\mathbb{Q})$. We know that a divisor $D \in J_1(N)(\mathbb{Q})$ is in the image of the Abel-Jacobi map $E \mapsto E - M\infty$ if and only if the linear system $|D + M\infty| \neq \varnothing$. Thus we can compute $|D + M\infty|$ via Magma's

RiemannRoch intrinsic, and if $|D + M\infty| = \varnothing$ then we disregard it. Otherwise, it will contain a single effective divisor E of degree M. Thus as D ranges over $J_1(N)(\mathbb{Q})$, we eventually compute all of the effective degree M divisors (and hence the image of Abel-Jacobi).

However, direct analysis over $\mathbb{Q}$ is often slow for curves with high rank values, so instead, we work over $\mathbb{F}_p$ using the following diagram.

$$\begin{array}{ccc} X^{(M)}(\mathbb{Q}) & \xrightarrow{\iota} & J_X(\mathbb{Q}) \\ \downarrow{\scriptstyle \mathrm{red}_X} & & \downarrow{\scriptstyle \mathrm{red}_J} \\ X^{(M)}(\mathbb{F}_p) & \xrightarrow{\iota_p} & J_X(\mathbb{F}_p) \end{array}$$

This diagram commutes, so the image of ι_p contains the reduction of the image of ι, and it then suffices to:

1. Compute the image of ι_p.
2. Compute the preimage of im ι_p under red_J.
3. Compute which elements of $\mathrm{red}^{-1}(\mathrm{im}\ \iota_p)$ are in image of ι.

We refer to this approach as Direct Analysis over $\mathbb{F}_p$, as do Derickx, Etropolski, Morrow, van Hoeij, and Zurieck-Brown [5].

As an example, $X_1(26)$ has genus 10, and rank 0 with torsion subgroup $\mathbb{Z}/133\mathbb{Z} \oplus \mathbb{Z}/1995\mathbb{Z}$, and it is generated by differences of rational points There are 12 rational cusps and 0 quadratic, cubic, or quartic cusps on $X_1(26)$.

Working mod 3, there are 12 $\mathbb{F}_3$-points, 0 $\mathbb{F}_9$-points, 16-$\mathbb{F}_{27}$ points, and 12 $\mathbb{F}_{81}$-points. We compute that the images of the 12 $\mathbb{F}_{81}$-points are not in the image of the Abel-Jacobi map. Thus the modular curve $X_1(26)$ has no non-cuspidal quartic points. (See Appendix A for full code).

3.2.1 Intermediate Modular Curves

While Direct Analysis works in principle, we encounter several values of N where the genus of $X_1(N)$ and the size of $J_1(N)$ are prohibitively large.

Instead, we consider a morphism $X_1(N) \to X_H(N)$, where $X_H(N)$ is non-tetragonal (has no degree four map to $\mathbb{P}^1$) and perform the Direct Analysis on this intermediate curve $X_H(N)$.

Chapter 4

Results

Using Direct Analysis over $\mathbb{F}_p$ on $X_1(N)$ and $X_H(N)$, as described in Chapter 3, we obtain the following results using the computer algebra system Magma [1]. The code for each of these proofs can be found in the GitHub repository at `https://github.com/alexisnewton/Low-degree-points-on-some-rank-0-modular-curves`.

Theorem 4.0.1 (Cerchia-Newton, 2024). *For $N = 25, 26, 27, 28, 34, 35,$ and 40, the modular curve $X_1(N)$ has no non-cuspidal quartic points.*

Theorem 4.0.2 (Cerchia-Newton, 2025). *For $N = 26, 27, 34$ and 40, the modular curve $X_1(N)$ has no non-cuspidal quintic points.*

Theorem 4.0.3 (Cerchia-Newton, 2025). *For $N = 34$, the modular curve $X_1(N)$ has no non-cuspidal sextic points.*

The argument for each level N is detailed below. Code for $N = 26$ can be found in Appendix A. The rest of the code is located in the Github Respository (link)

4.1 The Case of $N = 25$

We show now that the modular curve $X_1(25)$ has no non-cuspidal quartic points. The curve $X_1(25)$ has genus 12 and is 5-gonal. We use Andrew Sutherland's optimized equations (cite) for $X_1(25)$. From the subscheme lemma, we know there are 10 rational cusps, 2 quartic cusps, and one degree-10 cusp. Via a Magma computation, $J_1(25)(Q)$ is cyclic of order 227555.

Over $\mathbb{F}_3$, we find

- 10 places of degree 1 on $X_1(25)$,
- 0 places of degree 2 on $X_1(25)$,
- 0 places of degree 3 on $X_1(25)$,
- 12 places of degree 4 on $X_1(25)$.

The 10 degree-1 points lift to $\mathbb{Q}$, so we compute with the 12 quartic points. Computing the inverse image of Abel-Jacobi succeeds. We compute that the images of the 12 $\mathbb{F}_{27}$-points under Abel–Jacobi do not meet the reduction of the global torsion.

4.2 The Case of $N = 26$

We show now that the modular curve $X_1(26)$ has no non-cuspidal quartic or quintic points. $X_1(26)$ has genus 10 and rank 0. The torsion subgroup is $\mathbb{Z}/133\mathbb{Z} \times \mathbb{Z}/1995\mathbb{Z}$, and is generated by differences of rational points.

There are 12 rational cusps, 0 quadratic or cubic cusps, and 2 sextic cusps.

Computing the inverse image of Abel–Jacobi succeeds. It is slow to do this directly, so instead, we work mod 3, and note that there are

- 12 places of degree 1 on $X_1(26)$,
- 0 places of degree 2 on $X_1(26)$,
- 16 places of degree 3 on $X_1(26)$,
- 12 places of degree 4 on $X_1(26)$,

- 48 places of degree 5 on $X_1(26)$.

We compute that the images of the 12 $\mathbb{F}_{81}$ points under Abel–Jacobi do not meet the reduction of the global torsion. Similarly combinations of the 12 $\mathbb{F}_3$-points and the 16 $\mathbb{F}_{27}$-points under Abel-Jacobi do not meet the reduction of the global torsion.

4.3 The Case of $N = 27$

We show now that the modular curve $X_1(27)$ has no non-cuspidal quartic or quintic points. $X_1(27)$ has genus 13, and rank 0. The torsion subgroup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/52497\mathbb{Z}$ is generated by differences of cusps. There are 9 rational cusps, 3 quadratic, 1 sextic and 1 degree 9. Computing the inverse image of Abel-Jacobi succeeds.

Over $\mathbb{F}_5$, we find

- 9 places of degree 1 on $X_1(27)$,
- 12 places of degree 2 on $X_1(27)$,
- 57 places of degree 3 on $X_1(27)$,
- 171 places of degree 4 on $X_1(27)$,
- 612 places of degree 5 on $X_1(27)$.

The 9 rational points lift. Through a counting argument we find that the images of the points under Abel–Jacobi do not meet the reduction of the global torsion.

4.4 The Case of $N = 28$

We show now that the modular curve $X_1(28)$ has no non-cuspidal quartic points. $X_1(28)$ has genus 10, and rank 0. The torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times$

$\mathbb{Z}/936\mathbb{Z}$ is generated by differences of cusps. There are 9 rational cusps, 3 quadratic, 1 cubic, and 2 sextic. Computing the inverse image of Abel-Jacobi succeeds.

Over $\mathbb{F}_3$, we find

- 9 places of degree 1 on $X_1(28)$,
- 3 places of degree 2 on $X_1(28)$,
- 5 places of degree 3 on $X_1(28)$,
- 12 places of degree 4 on $X_1(28)$.

The 9 rational points lift. Through a counting argument we find that the images of the points under Abel–Jacobi do not meet the reduction of the global torsion.

4.5 The Case of $N = 34$

We show now that the modular curve $X_1(34)$ has no non-cuspidal quartic, quintic or sextic points. $X_1(34)$ has genus 21, and rank 0. The torsion subgroup $\mathbb{Z}/8760\mathbb{Z} \times \mathbb{Z}/595680\mathbb{Z}$ is generated by differences of cusps. There are 16 rational and 2 degree-8 cusps. Computing the inverse image of Abel-Jacobi succeeds.

Over $\mathbb{F}_3$, we find

- 16 places of degree 1 on $X_1(34)$,
- 0 places of degree 2 on $X_1(34)$,
- 0 places of degree 3 on $X_1(34)$,
- 26 places of degree 4 on $X_1(34)$,
- 32 places of degree 5 on $X_1(34)$.

The 16 rational points lift. Through a counting argument we find that the images of the points under Abel–Jacobi do not meet the reduction of the global torsion.

4.6 The Case of $N = 35$

This is a complete determination of the quartic points on $X_H(35)$. The genus of $X_H(35)$ is 9, and it has rank 0. The torsion subgroup $\mathbb{Z}/1560\mathbb{Z}$ is generated by differences of cusps. There are 4 rational cusps, 2 quadratic and 2 quartic.

Over $\mathbb{F}_3$, we find

- 4 places of degree 1 on $X_1(35)$,
- 2 places of degree 2 on $X_1(35)$,
- 12 places of degree 3 on $X_1(35)$,
- 2 places of degree 4 on $X_1(35)$.

The 4 rational cusps lift to $\mathbb{Q}$. Through a counting argument we find that the images of the points under Abel–Jacobi do not meet the reduction of the global torsion.

4.7 The Case of $N = 40$

This is a complete determination of the quartic and quintic points on $X_H(40)$. The genus of $X_H(40)$ is 9, and it has rank 0. The torsion subgroup $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/60\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}$ is generated by differences of cusps. There are 8 rational cusps, 4 quadratic and 4 quartic cusps.

Over $\mathbb{F}_3$, we find

- 8 places of degree 1 on $X_1(40)$,
- 4 places of degree 2 on $X_1(40)$,
- 0 places of degree 3 on $X_1(40)$,
- 44 places of degree 4 on $X_1(40)$.

The 8 rational cusps lift to $\mathbb{Q}$. Through a counting argument we find that the images of the points under Abel–Jacobi do not meet the reduction of the global torsion.

Chapter 5

Future Work

An ongoing program of study is to classify higher degree points on $X_0(N)$ and other quotients of $X_1(N)$ and $X_1(M,N)$. While this will inevitably take the combined work of many, the classification of the quintic and sextic degree cases should be in reach in the next five years.

Problem. What are the non-cuspidal quintic points on $X_1(N)$?

Problem. What are the non-cuspidal sextic points on $X_1(N)$?

It is conjectured that the torsion on modular Jacobians is generated by differences of cusps. This is a conjecture of Conrad-Edixhoven-Stein [2] for the modular Jacobian $J_1(p)$ where p is a prime, which had been proved for all primes $p \leq 157$ except $p = 29, 97, 101, 109,$ and 113. Moreover, their conjecture is true for all primes p such that $J_1(p)(\mathbb{Q})$ has rank 0. Further work has been done for composite N for $N \leq 55, N \neq 54$ [5].

Problem. Prove the torsion on $J_1(N)(\mathbb{Q})$ is generated by the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of cusps.

On a more explicitly computational track, in several cases of using the intermediate curve X_H we needed a j-invariant map to rule out the existence of quartic points that could be lifts of sporadic points on X_H. This code proved hard to come by.

Problem. Write code to compute the j-invariant map for intermediate curves X_H.

Appendix A

Code

```
// This is a complete determination of the quartic points on X_1(26)
/*
 Here is a summary of the argument.

 X_1(26) has genus 10, and rank 0.
 The torsion subgroup is [133, 1995],
 and is generated by differences of rational points.

 There are phi(26)/2 = 12 rational cusps and 0 quadratic or cubic
   cusps, 2 sextic cusps.

 Computing the inverse image of Abel-Jacobi succeeds.
 It is slow to do this directly, so instead, we work mod 3, and note
   that
 there are 12 F_3 points, 0 F_9 points, and 16 F_27 points, 12 F_81
   points.

 We compute that the images of the 12 F_81 points under Abel--Jacobi
 do not meet the reduction of the global torsion. Similarly with
 combinations of the 16 F_27 points and 12 F_3 points.

```

```
 One subtlety of this case is that it greatly speeds things up to work
 on a singular model.
*/

  N := 26;


  //////////////////////////////////////
  // Input the homebrewed functions
  ///////////////////////////////////////

  load "functions.m";


  /////////////////////////////////////
  // Equations for X_1(26), from Derickx--Sutherland
  //////////////////////////////////////

  F := Rationals();
  P<[t]> := ProjectiveSpace(F,9);
  A2<x,y> := AffineSpace(F,2);

  X:=Curve(A2,y^6 + (3*x^2 + 4*x - 2)*y^5 + (3*x^4 + 10*x^3 - 9*x + 1)*y^4 + (x^6 + 7*x^5 + 8*x^4 - 14*x^3 - 11*x^2 + 6*x)*y^3 + (x^7 + 4*x^6 - x^5 - 13*x^4 + 2*x^3 + 10*x^2 - x)*y^2 - (x^6 - 7*x^4 - 4*x^3 + 2*x^2)*y - x^4 - x^3);
  Xp := ProjectiveClosure(X);


  //////////////////
  // Compute the local torsion bound
  //////////////////
```

```

for p in [q : q in PrimesUpTo(40) | not q in PrimeDivisors(2*N) ]
  do
  torsData := {@@};
  for p in [3,5 ] do
      invs := Invariants(ClassGroup(Curve(Reduction(X,p))));
      torsData := torsData join {@invs@};
      <p,invs>;
  end for;

// 3 [ 665, 1995, 0 ]
// 5 [ 7, 133, 29925, 0 ]

   "The rational torsion subgroup is a subgroup of", torsBound(
  torsData); ; // [133, 1995]


  /////////////////////
  // Compute the known small degree points
  ////////////////////

  // Hard code as much as possible, since Magma changes
  // how it orders the output of "Support" mod different primes

  basePt := [-1 , 0 , 1];

  // mostly singular
  pts :=
  [
    [  0, 1, 0 ],
    [  0, 0, 1 ],
    [ -1, 0, 1 ],
    [  0, 1, 1 ],
```

```
  [  1, 0, 0 ],
  [ -1, 1, 1 ],
  [ -1, 1, 0 ]
];

// Verify that these generate the torsion
p := 3;
Cp<[T]> := Curve(Reduction(Xp,p));
  pic,mPic := ClassGroup(Cp);
basePt := &+Places(Cp![-1,0,1]);
divs := {@
       &+Places(Cp!pt) - Degree(&+Places(Cp!pt))*basePt
       : pt in pts @} ;

global, mGlobal :=
   sub<pic | [(Inverse(mPic))(divs[i]) : i in [1..#divs]]>;
Invariants(global); // [ 133, 1995 ]


////////////////////
// Compute the image of Abel--Jacobi mod 3
//////////////////////

"There are", [#Places(Cp,i) : i in [1..5]], "places of degree 1,
 2, 3, 4 and 5 over F_3"; // [ 12, 0, 16, 12, 48 ]
  // the 12 degree 1 points lift to Q so we compute with the 16
 cubic points, and 12 quartic

validQuarticImages := {@@};
for pl in Places(Cp,4) do
    D := Divisor(pl) - Degree(pl)*basePt;
    if Inverse(mPic)(D) in global then
      validQuarticImages :=
```

```
        validImages join {@Inverse(mPic)(D)@};
      end if;
  end for;
  "The rational places all lift to Q, and", #validQuarticImages, " of the other places are in the image of Abel--Jacobi"; // 0
//0
moreValidQuarticImages := {@@};
  for p in Places(Cp, 3) do
    for q in Places(Cp, 1) do
      D := Divisor(p) + Divisor(q) - 4*basePt;
      if Inverse(mPic)(D) in global then
        moreValidQuarticImages :=
        moreValidQuarticImages join {@Inverse(mPic)(D)@};
      end if;
    end for;
  end for;
  "There are", #moreValidQuarticImages, "of the other places (coming from two quadratics) in the image of Abel--Jacobi";
//0

  moreValidQuarticImages := {@@};
  for p1 in Places(Cp, 1) do
    for p2 in Places(Cp, 1) do
        for p3 in Places(Cp, 1) do
            for p4 in Places(Cp, 1) do
              D := Divisor(p1) + Divisor(p2) + Divisor(p3) + Divisor(p4) - 4*basePt;
              if Inverse(mPic)(D) in global then
                moreValidQuarticImages :=
                moreValidQuarticImages join {@Inverse(mPic)(D)@};
              end if;
            end for;
        end for;
```

```
    end for;
  end for;
  "There are", #moreValidQuarticImages, "of the other places (coming
    from a 4 degree 1 points) in the image of Abel--Jacobi";
 //1365

 //should be 15 choose 4 yay


////quintic

  validQuinticImages := {@@};
  for pl in Places(Cp,5) do
      D := Divisor(pl) - Degree(pl)*basePt;
      if Inverse(mPic)(D) in global then
        validQuinticImages :=
        validQuinticImages join {@Inverse(mPic)(D)@};
      end if;
  end for;
  "The rational places all lift to Q, and",  #validQuinticImages, "
   of the other places (coming from a quintic point) are in the
   image of Abel--Jacobi";
//0

   validQuinticImages := {@@};
  for p in Places(Cp, 4) do
    for q in Places(Cp, 1) do
      D := Divisor(p) + Divisor(q) - 5*basePt;
      if Inverse(mPic)(D) in global then
        validQuinticImages :=
        validQuinticImages join {@Inverse(mPic)(D)@};
      end if;
    end for;
```

```
  end for;
  "There are", #validQuinticImages, "of the other places (coming from 1 quartic and 1 rational) in the image of Abel--Jacobi";
//0


 moreValidQuinticImages := {@@};
  for p1 in Places(Cp, 3) do
    for p2 in Places(Cp, 1) do
        for p3 in Places(Cp, 1) do
              D := Divisor(p1) + Divisor(p2) + Divisor(p3) - 5*basePt;
              if Inverse(mPic)(D) in global then
                moreValidQuinticImages :=
                moreValidQuinticImages join {@Inverse(mPic)(D)@};
              end if;
        end for;
    end for;
  end for;
  "There are", #moreValidQuinticImages, "of the other places (coming from a 1 degree 3 point, 2 degree 1 points) in the image of Abel--Jacobi";
//0


moreValidQuinticImages := {@@};
  for p1 in Places(Cp, 1) do
    for p2 in Places(Cp, 1) do
        for p3 in Places(Cp, 1) do
            for p4 in Places(Cp, 1) do
              for p5 in Places(Cp, 1) do
                D := Divisor(p1) + Divisor(p2) + Divisor(p3) + Divisor(p4) + Divisor(p5) - 5*basePt;
```

```
                if Inverse(mPic)(D) in global then
                  moreValidQuinticImages :=
                  moreValidQuinticImages join {@Inverse(mPic)(D)@};
                end if;
              end for;
            end for;
        end for;
    end for;
  end for;
  "There are", #moreValidQuinticImages, "of the other places (coming
    from a 4 degree 1 points) in the image of Abel--Jacobi";
// n + k -1 choose k (picking k things from n with repitition)
  //should be 12 + 5 -1 choose 5 = 16 choose 5 =
  //4368
```

Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ISSN 0747-7171. doi: 10.1006/jsco.1996.0125. URL http://dx.doi.org/10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993).

[2] Brian Conrad, Bas Edixhoven, and William Stein. J1(p) has connected fibers. *Documenta Mathematica*, 8, 01 2003.

[3] Maarten Derickx and Filip Najman. Classification of torsion of elliptic curves over quartic fields, 2024. URL https://arxiv.org/abs/2412.16016.

[4] Maarten Derickx and Andrew V. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proceedings of the American Mathematical Society*, 145(10):4233–4245, April 2017. ISSN 1088-6826. doi: 10.1090/proc/13605. URL http://dx.doi.org/10.1090/proc/13605.

[5] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15 (7):1837–1864, November 2021. ISSN 1937-0652. doi: 10.2140/ant.2021.15.1837. URL http://dx.doi.org/10.2140/ant.2021.15.1837.

[6] Daeyeol Jeon, Chang Heon Kim, and Euisung Park. On the torsion of elliptic curves over quartic number fields. *Journal of the London Mathematical Society*, 74(1):1–12, 2006. doi: https://doi.org/10.1112/

S0024610706022940. URL https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/S0024610706022940.

[7] S. Kamienny. Torsion points on elliptic curves and q-coeffincients of modular forms. *Inventiones mathematicae*, 109(2):221–230, 1992. URL http://eudml.org/doc/144019.

[8] M. A. Kenku and Fumiyuki Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125 – 149, 1975. URL https://api.semanticscholar.org/CorpusID:16816807.

[9] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathematiques de l'IHES*, 47:33–186, 1977. URL http://eudml.org/doc/103950.

[10] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones Mathematicae*, 124(1-3):437–449, January 1996. doi: 10.1007/s002220050059.

[11] Filip Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $x_1(n)$. *Mathematical Research Letters*, 23, 11 2012. doi: 10.4310/MRL.2016.v23.n1.a12.

[12] Bjorn Poonen. Lectures on rational points on curves. 04 2006.

[13] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of galois, 2015. URL https://arxiv.org/abs/1402.5997.

[14] Andrew V. Sutherland. Constructing elliptic curves over finite fields with prescribed torsion. *Mathematics of Computation*, 81(278):1131–1147, August 2011. ISSN 1088-6842. doi: 10.1090/s0025-5718-2011-02538-x. URL http://dx.doi.org/10.1090/S0025-5718-2011-02538-X.

[15] David Zywina. Possible indices for the galois image of elliptic curves over q, 2022. URL https://arxiv.org/abs/1508.07663.

[16] David Zywina. Explicit open images for elliptic curves over $\mathbb{Q}$, 2024. URL https://arxiv.org/abs/2206.14959.