DISSERTATION

THREE PROJECTS IN ARITHMETIC GEOMETRY: TORSION POINTS AND CURVES OF LOW GENUS

Submitted by

Catalina Camacho-Navarro

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2019

Doctoral Committee:

Advisor: Rachel Pries

Jeff Achter
Renzo Cavalieri
Chris Peterson
Marcela Velasco

ABSTRACT

THREE PROJECTS IN ARITHMETIC GEOMETRY:
TORSION POINTS AND CURVES OF LOW GENUS

This paper is an exposition of three different projects in arithmetic geometry. All of them consider problems related to smooth curves with low genus and the torsion points of their Jacobians. The first project studies curves over finite fields and two invariants of the p-torsion part of their Jacobians: the a-number (a) and p-rank (f). There are many open questions in the literature about the existence of curves with a certain genus g and given values of a and f. In particular, not much is known when $g = 4$ and the curve is non-hyperelliptic. This is the case that we focus on here; we collect and analyze statistical data of curves over $\mathbb{F}_p$ for $p = 3, 5, 7, 11$ and their invariants. Then, we study the existence of Cartier points, which are also related to the structure of $J[p]$. For curves with $0 \leq a < g$, the number of Cartier points is bounded, and it depends on a and f.

The second project addresses the problem of computing the endomorphism ring of a supersingular elliptic curve. This question has gained recent interest as the basis of alternative cryptosystems that hope to be resistant to quantum attacks. Our strategy is to generate these endomorphism rings by finding cycles in the ℓ-isogeny graph which correspond to generators of the ring. We were able to find a condition for cycles to be linearly independent and an obstruction for two of them to be generators.

Finally, the last chapter considers the Galois representations associated to the n-torsion points of elliptic curves over $\mathbb{Q}$. In concrete, we construct models for the modular curves associated to applicable subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and find the rational points on all of those which result in genus 0 or 1 curves, or prove that they have infinitely many. We also analyze the curves with a hyperelliptic genus 2 model and provably find the rational points on all but seven of them.

ACKNOWLEDGEMENTS

First of all, I would like to thank my advisor, Rachel Pries, for her support and guidance that were fundamental to make this thesis possible. Throughout my graduate studies, Dr. Pries provided invaluable opportunities and encouragement for me to develop as a researcher, for which I am deeply grateful.

I also thank the professors that shared their knowledge and feedback with me all of these years, inside or outside the classroom. I would particularly like to thank Jeff Achter, for being an important part of my academic growth.

I would like to thank my co-authors on two of the projects that are featured in this dissertation and from whom I learned so much: Efrat Bank, Kirsten Eisenträger, Wanlin Li, Travis Morrison, Jackson S. Morrow, Jennifer Park, Jack Petok and David Zureick-Brown. I really appreciate their commitment and willingness to share their expertise.

I am also very grateful to Universidad de Costa Rica, for supporting my graduate studies at Colorado State University.

I want to extend my gratitude to everyone that gifted me with their friendship and support during this process. Here I include my fellow graduates students, specially Derek Handwerk, Jessica Gehrtz, Casey Pinckney, Ben Sencindiver, Karleigh Pine and Sam Pine. I would also like to thank my friends at LASSO, for giving me the sense of family and community that turned out to be invaluable.

Finally, I thank my family for their love, encouragement and understanding. To my parents Sonia and Ricardo, that raised me to be kind to myself and to others. To Leo, Tere and Isaac for giving me the best reason to go back.

DEDICATION

To my family.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

This dissertation is divided into three main chapters; each one corresponding to a project in arithmetic geometry. The topics that these encompass are, broadly speaking: the a-number, p-rank and Cartier points of smooth curves of genus 4; the ℓ-isogeny graphs of supersingular elliptic curves; and images of Galois for elliptic curves over $\mathbb{Q}$. Although the projects are very different from one another, they share some features. For example, they all study properties of curves with low genus g: elliptic curves, hyperelliptic modular curves with $g \leq 2$ and non-hyperelliptic curves with $g = 4$, defined either over $\mathbb{Q}$ or $\mathbb{F}_p$.

An additional common feature is the analysis of curves from the perspective of the torsion points of their Jacobians. The two most important invariants studied in Chapter 2 are the a-number and the p-rank. For a curve of genus g defined over a field of characteristic $p > 0$, these invariants come from the structure of the p-torsion part of the Jacobian. In Chapter 3, the properties of the ℓ-torsion subgroup of the supersingular elliptic curves play a main role in the construction and analysis of the ℓ-isogeny graph. Additionally, in Chapter 4 the goal is to understand the Galois group of the field extension obtained by adjoining to $\mathbb{Q}$ the coordinates of all the n-torsion points of an elliptic curve, for certain n.

Chapter 2 corresponds to an individual project suggested by my advisor Rachel Pries. Here we study the p-rank and a-number of non-hyperelliptic genus 4 curves over a field of characteristic $p > 0$. If X is a curve of genus g, these two invariants give information about the p-torsion part of the Jacobian J of X, which is a principally polarized abelian variety of dimension g. The structure of $J[p]$ as a group scheme is called the Ekedahl–Oort type. It gives rise to the stratification of $\mathcal{A}_g$, the moduli space of principally polarized abelian varieties of dimension g. This stratification yields one on $\mathcal{M}_g$, the moduli space of smooth curves of genus g. There are many open questions about

which strata occur for given g and p. For example, it is known by [6] that for any p and any f with $0 \leq f \leq g$, there is a genus g curve with p-rank f. If $g \leq 3$ and $p \geq 3$, then every Ekedahl–Oort type occurs, but it is not known if this is also true for $g \geq 4$.

Another open question, as stated by Pries in [23], is the following: For all p, does there exist a smooth curve of genus 4 with p-rank 0 and a-number at least 2? The work that we will describe in Chapter 2 is motivated by these and other similar questions. Concretely, we build a data base of non-hyperelliptic genus 4 curves over $\mathbb{F}_p$ for $p = 3, 5, 7, 11$. These curves are given by the equations provided by Kudo and Harashita in [12], we refer to them as *curves in standard form*. Then we sort the curves by their a-number and p-rank. In particular, we were able to identify all of the curves in standard form with $a = 3$ for $p = 3, 5$.

To find a and f we first recall that the a number corresponds to the dimension of the kernel of the Cartier operator $\mathcal{C}$ on $H^0(X, \Omega^1_X)$. The p-rank, on the other hand, is the stable rank of the Frobenius operator $\mathcal{F}$ on $H^1(X, \mathcal{O}_X)$. These two operators are dual of each other, and since the Hasse–Witt matrix H determines the action of Frobenius, if we know H, then we can easily compute a and f. In [12] the authors provide a method to determine the Hasse–Witt matrix of a complete intersection given by two homogeneous polynomials in $\mathbb{P}^3$.

Once we collect our data, we focus on studying the existence of Cartier points. A point P in a smooth curve X of genus g is a Cartier point if the subspace of regular differentials on X that vanish at P is stable under the Cartier operator. Notice that if W is such subspace, then for it to be stable under $\mathcal{C}$ we must have $\mathcal{C}(W) = 0$ or $\mathcal{C}(W) = W$. If the first case occurs then we say that P is of Type 1 and it is of Type 2 otherwise. These points happen to be related to the p-torsion part of the Jacobian. In fact, Baker uses them in [2] to give an alternative proof of Ekedahl's theorem on the bound of the genus of a superspecial curve (Theorem 2.2.6).

Baker also proves that the number of Cartier points is bounded for non-superspecial curves. The bound depends on p, a, f and g, but for $g = 4$, it is at most 7. We study the bounds of Type 1 and Type 2 points separately and we are interested in determining when are these bounds attained.

To do this, we develop algorithms to compute the Cartier points of non-hyperelliptic curves of genus 4 over $\mathbb{F}_p$. For example, we prove that the total bound is sharp when $a = 3$ and $p = 7$, and that is never sharp for curves in standard form when $a = 3$ and $p = 3$.

Chapter 3 is based on the paper "Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms" [3], written in collaboration with Efrat Bank, Kirsten Eisenträger, Travis Morrison and Jennifer Park. This is the conclusion of a project led by Eisenträger and Park as part of the Women in Numbers 4 Workshop held at Banff, Alberta, Canada in August 2017. In this paper we studied the ℓ-isogeny graph for supersingular elliptic curves over a field of characteristic $p > 0$, as a strategy to compute the endomorphism ring of such an elliptic curve. This last problem is equivalent to finding isogenies between two of the elliptic curves and it is the basis of the cryptosystem SIKE, which is one of the current candidates (as of October 2019) participating in the Post-Quantum Cryptography competition organized by NIST. Since the actual difficulty of the basic problem is still unknown, it is important to conduct research on the matter to detect possible attacks, both in the classical and post-quantum set ups. The paper has two main results: a condition for cycles on the graph to correspond to linearly independent endomorphisms and an obstruction to generate the full endomorphism ring. We also show concrete examples where these results are applied.

Chapter 4 includes joint work with Wanlin Li, Jackson Morrow, Jack Petok and David Zureick-Brown. In May 2017, Zureick-Brown organized a group project workshop on the topic of Galois representations of elliptic curves over $\mathbb{Q}$, held at Emory University. The goal was to determine subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, that contain the image of Galois under the $\pmod n$ representation , where n is the product of prime powers for primes less than 13. To do this, we built on progress made in [25], [37], [29] and [18] that completed the work with the prime and prime power level subgroups. Each such subgroup H is attached to a modular curve whose rational non-cuspidal points correspond to elliptic curves that have image of Galois contained in H. We analyze all genus $0, 1$ and 2 modular curves of composite level $m_1 m_2$ with $m_i = \ell_i^{p_i} < 37$, $\ell < 13$ and $\ell_1 \neq \ell_2$. For

the genus 0 and 1 curves we determine which ones had infinitely many points, sporadic points or neither. We know by Faltings theorem that curves of genus $g \geq 2$ have finitely many rational points. We identify at least 4 and at most 11 genus 2 curves with sporadic points.

Chapter 2

The a-number, p-rank and Cartier points of genus 4 non-hyperelliptic curves

2.1 Introduction

Let X be a smooth projective genus g curve over a field k of characteristic p. The Torelli map associates X with its Jacobian J_X, a principally polarized abelian variety of dimension g. The map embeds the moduli space $\mathcal{M}_g$ of curves of genus g into $\mathcal{A}_g$, the moduli space of principally polarized abelian varieties of dimension g over k. In consequence, it allows us to study the stratification of $\mathcal{M}_g$ by looking at the group scheme structure of $J_X[p]$, the p-torsion part of the Jacobian. This is called the Ekedahl–Oort stratification. For $g = 2, 3$, the Torelli locus is open and dense in $\mathcal{A}_g$. For $p \geq 3$ and $g \leq 3$this can be used to show that all Ekedahl–Oort types occur for the Jacobians of smooth curves $X/\overline{\mathbb{F}}_p$ ([21]). The same is not known for $g \geq 4$.

Motivated by this and other similar open questions related to the p-torsion part of the Jacobian, we study smooth irreducible curves with $g = 4$. We focus on the non-hyperelliptic kind. In particular, we looked at a-number and the p-rank: two invariants of $J_X[p]$.

In order to obtain a database of smooth, irreducible, genus 4 non-hyperelliptic curves, we restrict our analysis to what we definedas curves in *standard form*. Recall that if X is a curve with the above properties, then it has a model given by the zero locus of a quadratic and a cubic homogeneous polynomials in $k[x, y, z, w]$. Kudo and Harashita show in [12] that under some assumptions, the defining equations can be simplified to reduce the number of cases. The curves given by these simplified equations are in *standard form*.

We gather a statistical sample of curves in standard form defined over $\mathbb{F}_p$ for $p \in \{3, 5, 7, 11\}$. For each of them we find the Hasse–Witt matrix H and use it to compute the a-number and p-rank:

the a-number is $g - \text{rank}(H)$ and the p-rank is $f = \text{rank}\left(HH^{(p)} \cdots H^{(p^{g-1})}\right)$. As one should expect, the majority of curves appear in the sample are ordinary, and the percentages decrease as the a-number increases (or similarly, as the p-rank decreases).

Another important topic explored in this chapter is the concept of Cartier point. We say that $P \in X(\overline{k})$ is a Cartier point if the hyperplane of regular differentials of X vanishing at P is stable under the Cartier operator. Baker introduces the definition in [2] and remarks that they are related to the p-torsion points of the Jacobian. In particular, the author uses them to give an alternative proof of a theorem by Ekedahl [5], which states that the genus of a curve with $a = g$ in characteristic p is at most $p(p-1)/2$.

When X has a-number $0 < a < g$ then there is an upper bound on the number of Cartier points of X given by Baker. If $a \neq 0$ then we classify Cartier points in Type 1 and Type 2 (see Definition 2.5.5). The maximum number of Type 1 points depends on the a-number and the maximum number of Type 2 points depends on the p-rank. We are interested in determining the conditions under which these bounds are attained when X is non-ordinary. Therefore, we develop algorithms to find all of the Cartier points on curves in standard form and apply them to our database.

The Cartier points are particularly interesting when $a = g - 1$, because we can assign multiplicity to each of them. This is why we later focus on curves with $a = 3$. We find all of the curves in standard form with $a = 3$, defined over $\mathbb{F}_p$ for $p = 3, 5$ and a subset of them over $\mathbb{F}_7$. We explore the possible degrees and multiplicity distributions of these points.

Here are some of the most relevant conclusions from our work, concerning non-hyperelliptic genus 4 curves in standard form:

1. In our smooth sample, the are no curves with $(a, f) = (1, 0)$ over $\mathbb{F}_p$ for $p \in \{3, 5, 7, 11\}$. (Corollary 2.4.2).

2. There are, up to $\mathbb{F}_3$-isomorphism, exactly 27 curves with a-number 3 over $\mathbb{F}_3$ in standard form. All of them have p-rank 1. (Corollaries 2.4.4 and 2.4.3).

3. There are, up to $\mathbb{F}_5$-isomorphism, exactly 134 curves with $a = 3$ over $\mathbb{F}_5$. (Corollary 2.4.7).

4. In our smooth sample, no curve with a-number 2 reaches the bound of 6 Type 1 Cartier points. Moreover, the maximum number of Type 1 points attained on curves with a-number 2 is 3 for $p \in \{5, 7, 11\}$ and 2 for $p = 3$. (Corollary 2.5.16).

5. In our smooth sample no curve with p-rank 2 or 3 reaches the bound of 6 Type 2 Cartier points. The maximum number of points that occurs is 3 and 4, respectively. (Corollary 2.5.18).

6. When $a = 3$, the bound on Type 1 points is sharp for$p \in \{5, 7, 11\}$ and the total bound for both Types is sharp for 7. (Corollaries 2.5.17 and 2.5.19).

7. There are no curves in standard form over $\mathbb{F}_3$ with $a = 3$ that attain either of the upper bounds for Cartier points. (Lemma 2.6.2).

2.2 Preliminaries

This section includes the background information related to the Cartier operator, Hasse–Witt matrix, p-rank and a-number of a curve. Unless otherwise stated, p will be an odd prime number and k a perfect field of characteristic p.

2.2.1 The a-number and the p-rank

Let X be a smooth irreducible curve of genus g over k. Denote by J_X the Jacobian variety associated to X. Then J_X is an abelian variety of dimension g isomorphic to $\mathrm{Pic}^0_{X/k}$, equipped

with a principal polarization. We define the *multiplication-by-p* morphism $[p]$ as

$$\begin{aligned} [p] : J_X &\to J_X \\ P &\mapsto pP. \end{aligned}$$

The kernel of $[p]$ is the p-torsion part of the Jacobian, denoted by $J_X[p]$. It is known that $[p]$ is a proper flat morphism of degree p^{2g} and factors through the relative Frobenius morphism $\mathrm{Fr} : J_X \to J_X^{(p)}$ as $[p] = \mathrm{Vr} \circ \mathrm{Fr}$, where Vr is the Verschiebung morphism from $J_X^{(p)}$ to J_X, which is the dual of Fr.

The p-torsion part of the Jacobian is also a group scheme and here we will study two important invariants associated to it: the p-rank and the a-number. The first one is defined as the integer f such that $\#J_X[p](k) = p^f$. Equivalently, f is

$$f = \dim_k \mathrm{Hom}(\mu_p, J_X[p]), \tag{2.2.1}$$

where $\mu_p \cong \mathrm{Spec}(k[x]/(x^p - 1))$ is the kernel of the Frobenius morphism on the multiplicative group scheme $\mathbb{G}_m$.

Similarly, the a-number a is

$$a = \dim_k \mathrm{Hom}(\alpha_p, J_X[p]), \tag{2.2.2}$$

where $\alpha_p \cong \mathrm{Spec}(k[x]/x^p)$ is the kernel of Frobenius on the additive group scheme $\mathbb{G}_a$. It is well known that $0 \leq f \leq g$ and $1 \leq a + f \leq g$.

By the Torelli Theorem, X is completely determined by J_X together with its principal polarization, this means that we can define the a-number and the p-rank as invariants of X (see [16], for example). In Section 2.2.2 we will see equivalent definitions for both of these invariants, related to the Cartier–Manin matrix and the Hasse–Witt matrix.

Example 2.2.1. If E is an elliptic curve over k, then it is isomorphic to its Jacobian. If we consider the possibilities for the group structure of $E[p](\overline{k})$ then only the following can occur (see [28]): $E[p](\overline{k}) \cong \mathbb{Z}/p\mathbb{Z}$, or $E[p](\overline{k})$ is trivial. If the first is true, then $\#E[p](\overline{k}) = p$ so the p-rank is 1 and consequently the a-number is 0. If this happens, then E is called *ordinary*. On the other hand, if $\#E[p](\overline{k}) = 1$, then the p-rank is 0, the a-number is 1 and E is *supersingular*.

Example 2.2.1 only describes the group structure of the p-torsion of E. However, as mentioned above, $E[p]$ is actually a group scheme so one could ask: if two elliptic curves are of the same type (ordinary or supersingular) do they have isomorphic p-torsion? It turns out that the answer is yes. In other words, the group scheme structure of the p-torsion part of a smooth genus 1 curve is determined by its p-rank and its a-number. The same is true for the p-torsion of the Jacobian of a curve X with $g = 2$, but not if $g \geq 3$. For instance, if $g = 3$ then there are two isomorphism classes for $J_X[p]$ when $f = 0$ and $a = 2$ (see [21] for details).

2.2.2 The Cartier and Frobenius operators

Suppose that x is a separating variable of $k(X)/k$, then every $t \in k(X)$ can be written as

$$t = t_0^p + t_1^p x + \ldots + t_{p-1}^p x^{p-1}, \tag{2.2.3}$$

with $t_i \in k(X)$.

Definition 2.2.2. The Cartier operator $\mathcal{C}$ is defined on Ω_X^1 by

$$\mathcal{C}(tdx) = t_{p-1}dx, \tag{2.2.4}$$

for t as in (2.2.3).

For t in $k(X)$ and $\omega, \omega_1, \omega_2 \in \Omega_X^1$, the operator $\mathcal{C}$ satisfies the following properties (see for example, [24]):

1. $\mathcal{C}(\omega_1 + \omega_2) = \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2)$.

2. $\mathcal{C}(dt) = 0$.

3. $\mathcal{C}(t^p\omega) = t\mathcal{C}(\omega)$.

From (1) and (3) we see that $\mathcal{C}$ is $1/p$-linear and induces a well defined map $\mathcal{C} : H^0(X, \Omega^1_X) \to H^0(X, \Omega^1_X)$ on the k-vector space of regular differentials.

Definition 2.2.3. If $B = \{\omega_1, \ldots, \omega_g\}$ is a k-basis for $H^0(X, \Omega^1_X)$ and $\mathcal{C}(\omega_j) = \sum_{i=1}^g c_{ij}\omega_i$ then the Cartier–Manin matrix of X with respect to this basis is the matrix $(c^p_{ij})_{ij}$.

Definition 2.2.4. The absolute Frobenius of X is the morphism $\mathcal{F} : X \to X$ given by the identity on the underlaying topological space and $t \mapsto t^p$ on $\mathcal{O}_X$. Let $\mathcal{F}_X$ be the induced endomorphism in $H^1(X, \mathcal{O}_X)$.

The Frobenius endomorphism is p-linear, that is $\mathcal{F}_X(a\xi) = a^p\mathcal{F}_X(\xi)$ for all $a \in k$ and all $\xi \in H^1(X, \mathcal{O}_X)$.

Definition 2.2.5. Let $B' = \{\xi_1, \ldots, \xi_g\}$ be a k-basis of $H^1(X, \mathcal{O}_X)$ and $\mathcal{F}_X(\xi_j) = \sum_{i=1}^g a_{ij}\xi_i$ for some $a_{ij} \in k$. Then the Hasse–Witt matrix of X with respect to B' is the matrix $(a_{ij})_{ij}$.

The space $H^1(X, \mathcal{O}_X)$ is the dual of $H^0(X, \Omega^1_X)$ and there is a perfect paring $<,>$ on $H^1(X, \mathcal{O}_X) \times H^0(X, \Omega^1_X)$ such that $< \mathcal{F}_X\xi, \omega >=< \xi, \mathcal{C}\omega >^p$. When the Hasse–Witt matrix is constructed with respect a basis B' of $H^1(X, \mathcal{O}_X)$ which is the dual basis of $B = \{\omega_1, \ldots, \omega_g\}$ of $H^0(X, \Omega^1_X)$, then the Cartier–Manin matrix M with respect to B is the transpose of the Hasse–Witt matrix H with respect to B'.

Now we can revisit the concepts of the a-number and p-rank from Section 2.2.1, which can be defined in terms of the matrix H. By Serre [27], the p-rank f is the stable rank of the Frobenius and since this operator is p-linear, it implies that

$$f = \text{rank}\left(HH^{(p)}\cdots H^{\left(p^{g-1}\right)}\right), \tag{2.2.5}$$

where $H^{(i)}$ is the matrix obtained by raising every entry of H to the i-th power. On the other hand, by Oort [13]

$$a = g - \text{rank}(H) = g - \text{rank}(M). \tag{2.2.6}$$

Generically $f = g$, in which case X is said to be *ordinary*. The other extreme case is when X is *superspecial* and it occurs when $a = g$ or equivalently, when the Cartier operator is identically 0 on $H^0(X, \Omega^1_X)$.

In Example 2.2.1 we saw that a supersingular elliptic curve E has p-rank 0 and a-number $1 = g$, so it is also superspecial. For a curve X of genus $g > 1$, Equation 2.2.5 implies that X could have $f = 0$ even when $a \neq g$.

In Section 2.3.2 we describe how to explicitly find the Hasse–Witt matrix when X is the complete intersection of two homogeneous polynomials and use it to compute the p-rank and a-number.

2.2.3 Previous results

In this section we review some of the main and more recent results with respect to genus g curves of positive characteristic and possible values for the a-number and p-rank that occur. Let m be the rank of the Cartier operator. The first three theorems give an upper bound to the genus of X depending on m and p.

Theorem 2.2.6 (Ekedahl [5],Theorem 1.1)**.** *Let X be a smooth curve of genus g over an algebraically closed field k of characteristic $p > 0$. If X is superspecial then*

1. $g \leq \frac{1}{2}(p^2 - p)$ *and*

2. $g \leq \frac{1}{2}(p - 1)$ *if X is hyperelliptic and* $(p, g) \neq (2, 1)$.

An example where this bound is realized is the Hermitian curve given by

$$X : x^p + x = y^{p+1}. \tag{2.2.7}$$

It is known that X is superspecial, and by the genus formula $g = \frac{p(p-1)}{2}$.

Baker gives in [2] an alternative proof for Theorem 2.2.6, based on the existence of Cartier points. We discuss this concept in Section 2.5. Independently, Re later provides a generalization of this result to any value of m:

Theorem 2.2.7 (Re [24], Theorem 3.1 and Proposition 3.1)**.** *Let X be a smooth complete curve of genus g over an algebraically closed field of characteristic $p > 0$. Suppose that the Cartier operator $\mathcal{C}$ has rank m. Then*

$$g \leq (m+1)p\frac{(p-1)}{2} + pm.$$

If X is also hyperelliptic then

$$g < \frac{p+1}{2} + mp.$$

In [33] Zhou gives a strengthening of Theorem 2.2.7 for the case when $m = 1$:

Theorem 2.2.8 (Zhou [33], Theorem 1.1)**.** *If $m = 1$, then*

$$g \leq p + \frac{p(p-1)}{2}.$$

In the case of hyperelliptic curves and p odd, Frei [7] proved that the bound can be even lower when $m = 1$.

Theorem 2.2.9 (Frei [7], Theorem 3.1)**.** *Let $g \geq p$ where p is an odd prime. Then there are no smooth hyperelliptic curves of genus g defined over a field of characteristic p with a-number equal to $g - 1$.*

There are examples, however, of curves with a-number $g - 1$ that are non-hyperelliptic. In Proposition 2.4.6 we define a family of non-hyperelliptic curves genus 4 curves with $a = 3$ over $\mathbb{F}_3$. Also Zhou finds in [35] a family of Artin–Schreier curves with these properties. We refer to them again in Section 2.3

More generally, Pries [22] proves the existence of smooth curves with a-number $1, 2$ and 3, under certain conditions. For instance:

- If $g \geq 2$ then there is a family of smooth curves of genus g with p-rank $g-2$ and a-number 1. Furthermore, if the characteristic of the field is $p \geq 3$ then there exists a family of hyperelliptic curves with the same invariants.
- If $g \geq 3$ then there is a family of smooth curves of genus g with p-rank $g-3$ and a-number 1.
- If $p \geq 5$, there exists a family of smooth curves of genus g with p-rank $g-2$ and a-number 2.
- For $p \geq 3$ and g odd $g \not\equiv 1 \mod p$ with $g > 6(p-1)$ there exist genus g and p-rank $g-3$ curves with a-number $a = 2$ and with $a = 3$.

2.3 Genus 4 non-hyperelliptic curves

There are currently many open questions concerning the existence of curves with certain p-ranks and a-numbers, given a fixed genus g. Pries states some of them in [23]. For instance, there exist curves of genus 2 and 3 with any possible p-rank and a-number over fields of characteristic p, with the exception of superspecial curves of genus x2 when $p = 2$ and superspecial curves of genus 3 when $p = 2, 3$. For $g \geq 4$, however, it is not known if this happens. For example, consider Question 3.6 in [23]: *For all p, does there exist a smooth curve of genus 4 with p-rank 0 and a-number at least 2?*

One can find in the literature partial answers to the last and similar questions. For example, suppose that $p = 3$. Then by Ekedahl's Theorem (2.2.6), there is no superspecial curve of genus 4, so there are no curves of a-number 4. In [34], Zhou (building on work from [7], [9] and [22]) shows that in characteristic 3, there are genus 4 curves with a-number a and p-rank f for all $a \leq 2$ and

$f \leq a$ and for $(a, f) = (3, 1)$. As an example, Zhou studies the family of genus 4 Artin-Schreier curves over an algebraically closed field k of characteristic 3, given by:

$$y^3 - bx^3(y^2 + y) = x^5 + cx^3 + dx^2 + 1, \tag{2.3.1}$$

with $b, c, d \in k$ and $bd \neq 0$. The author shows that every such curve has a-number 3 and p-rank 1. In fact, he computes the Ekedahl-Oort types to show that the corresponding locus of $\mathcal{M}_g$ is non empty of codimension at most 6. In Section 2.5.3 we provide additional examples of genus 4 curves with a-number 3 and p-rank 1 over $\mathbb{F}_3$, which are not Artin–Scheier curves. We know by Theorem 2.2.9 that there are no a-number 3 and p-rank 0 genus 4 hyperelliptic curves, so one can ask whether it is possible to have a non-hyperelliptic genus 4 with those invariants.

Kudo and Harashita [12], also studied genus 4 curves, they prove two results related to non-hyperelliptic superspecial curves of genus 4 with $p = 7$ and $p = 5$.

Theorem 2.3.1 (Kudo and Harashita [12], Theorem A)**.** *Any superspecial curve of genus* 4 *over* $k = \mathbb{F}_{25}$ *is isomorphic to*

$$2yw + z^2 = 0,\ x^3 + a_1y^3 + a_2w^3 + a_3zw^2 = 0,$$

in $\mathbb{P}^3$ *, where* $a_1, a_2 \in \mathbb{F}_{25}^{\times}$ *and* $a_3 \in \mathbb{F}_{25}$.

Theorem 2.3.2 (Kudo and Harashita [12], Theorem B)**.** *There is no superspecial curve of genus* 4 *in characteristic* 7.

2.3.1 Defining equations of genus 4 non-hyperelliptic curves

We are interested in studying genus 4 non-hyperelliptic curves over k. Our strategy is to construct a large database of them; here we explain how we achieve that. If X is a genus 4, smooth, irreducible and non-hyperelliptic curve, then the canonical map embeds X into $\mathbb{P}^3_k$ as the inter-

section of the zero loci of a quadratic and a cubic homogeneous polynomial in four variables (see [10]). One might start by looking at the k-vector spaces of quadratic and cubic homogeneous polynomials, picking an element of each and checking whether they define a curve with the desired conditions. However, these vector spaces have dimensions 10 and 20, respectively, so it is not computationally feasible to construct a curve this way. Instead we will begin by restricting our computations to what we will define as genus 4 curves in *standard form*. These are based on fixed quadratic forms and simplified cubic forms explored by Kudo and Harashita [12]. In this section we will present this definition and remark on how under certain conditions, every curve can be written as such.

Quadratic forms and reduction of cubics

Every quadratic form has a symmetric matrix associated to it. Two quadratic forms over k are equivalent if their matrices are conjugate. We claim that any irreducible quadratic form in $k[x, y, z, w]$ is equivalent to one of $F_1 = 2xw + 2yz$, $F_2 = 2xw + y^2 - \epsilon z^2$ or $F_d = 2yw + z^2$ with some $\epsilon \notin (k^\times)^2$.

Notice that the symmetric matrices associated to F_1, F_2 and F_d are, respectively:

$$N1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad N2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\epsilon & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad D = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Indeed, let B and B' represent equivalent quadratic forms. Then there exists an invertible matrix C such that $B = C^T B' C$, hence $\det(B) = \det(B') \det(C)^2$. This implies that the quadratic forms over k with full rank are classified by whether or not their discriminant is a square in $k^\times$. Since $\det(N1) = 1$ and $\det(N2) = \epsilon$ we can fix these representatives of the equivalence classes.

On the other hand, a quadratic form can still be irreducible if its rank is 3. By the same reasoning as above, quadratic forms in three variables are equivalent to one of:

$$D_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -\upsilon & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad D_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

for some υ non-square in $k^\times$. Let us assume that $F \in k[x, y, z, w]$ is a quadratic form of rank 3 with no x terms in it. Then a priori F is equivalent to $2yw - \upsilon z^2$ or $2yw + z^2$. However, these two are equivalent by the change of variables $(x \to x, y \to y, z \to z, w \to -\upsilon w)$. Therefore we can assume that $\upsilon = -1$. This completes the proof of our claim.

Now we can assume that X has a model given by $V(F, G)$, with F being one of F_1, F_2 or F_d, and G a homogeneous polynomial of degree 3. The possible values of G can be reduced by changes of variables, induced by the action of the orthogonal similitude groups associated to the quadratic forms. This is done in detail in Section 4 of [12]. The simplified equations provide the following definition.

Definition 2.3.3. Let $F_1 = 2xw + 2yz$, $F_2 = 2xw + y^2 - \epsilon z^2$ or $F_d = 2yw + z^2$ with $\epsilon \notin (k^\times)^2$. We say that a curve X of genus 4 over k is in *standard form* if it is non-hyperelliptic, irreducible, smooth and $X = V(F, G)$ with

(Case D) $F = F_d$ and

$$G = a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x + a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2,$$

for $a_i \in k$ and $a_0, a_6 \in k^\times$, with $b_1, b_2 \in \{0, 1\}$ and the leading coefficient of $r = a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw$ is 1 or $r = 0$; or

(Case N1i) $F = F_1$ and

$$G = (a_1y + a_2z)x^2 + a_3yzx + y^3 + a_4z^3 + b_1y^2z + a_5yz^2 + (a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3,$$

for $a_i \in k$ with $a_1 \neq 0$, $a_2 \neq 0$ and for $b_1 \in \{0\} \cup k^\times/(k^\times)^2$ and $b_2 \in \{0, 1\}$; or

(Case N1ii) $F = F_1$ and

$$G = (a_1y + a_2z)x^2 + a_3yzx + b_1y^2z + b_2yz^2 + (a_4y^2 + a_5yz + b_3z^2)w + (a_6y + a_7z)w^2 + a_8w^3,$$

for $a_i \in k$ with $a_1a_2 \neq 0$ and for $b_1, b_3 \in \{0, 1\}$ and $b_2 \in \{0\} \cup k^\times/(k^\times)^2$; or

(Case N2) $F = F_2$ and

$$G = (a_1y + a_2z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1y(y^2 - \epsilon z^2) + a_4y(y^2 + 3\epsilon z^2) + a_5z(3y^2 + \epsilon z^2) + (a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3,$$

for $a_i \in k$, with $(a_1, a_2) \neq (0, 0)$ and $b_1, b_2 \in \{0, 1\}$ and ϵ a non-trivial fixed representative of $k^\times/(k^\times)^2$,

Let $\vec{a} \in k^{20}$ be denoted by $G_{\vec{a}}$ the cubic whose coefficients correspond to the entries of $\vec{a}$, assigned to the monomials of degree 3 in $k[x, y, z, w]$ in graded lexicographic order. This means that we consider $x > y > z > w$ and to order the monomials we first compare the exponents of x, then those of y and so on. So, every genus 4 non-hyperelliptic can be written as $X = V(F, G)$, where F is one of F_1, F_2, F_d. One can ask if there is a way of always reducing the cubic G by a change of variable so that X is in standard form. This is addressed in Lemma 2.3.4.

Lemma 2.3.4 (Lemmas 4.3.1, 4.4.1 and 4.5.1 in [12])**.** *Let X be a non-hyperelliptic genus 4 curve over k given by $X = V(F, G)$, where F is one of F_1, F_2, F_d. Then X can be written in standard form if it satisfies one of the following conditions:*

(A1) $F = F_1$ and X has a k-rational point $P = [x, y, z, w]$ such that

$$w = 1,\ R_y(y, z) := \frac{\delta}{\delta y} P(-yz, y, z, 1) \neq 0 \text{ and } R_z(y, z) := \frac{\delta}{\delta z} P(-yz, y, z, 1) \neq 0.$$

(A2) $F = F_2$ and X has a k-rational point $P = [x, y, z, w]$ such that $w = 1$, and

$$R_y(y, z) := \frac{\delta}{\delta y} P\left(-\frac{y^2 - \epsilon z^2}{2}, y, z, 1\right) \neq 0 \text{ and}$$
$$R_z(y, z) := \frac{\delta}{\delta z} P\left(-\frac{y^2 - \epsilon z^2}{2}, y, z, 1\right) \neq 0.$$

(A3) $F = F_d$ and k has more than 5 elements..

It is shown in [12] that the conditions (A1), (A2) are satisfied for q sufficiently large: they are true for all curves with at least 36 and 37 points, respectively. By the Hasse–Weil bound, this is guaranteed is $q > 127$.

2.3.2 Hasse–Witt Matrix of genus 4 non-hyperelliptic curves

Let $X = V(F, G)$ be the complete intersection on $\mathbb{P}^3_k$ defined by homogeneous polynomials F and G in $k[x, y, z, w]$ of degrees d and c, respectively. Following [10] and [2] we see that $H^1(X, \mathcal{O}_X) \cong H^3(\mathbb{P}^3, \mathcal{O}^3_{\mathbb{P}}(-c - d))$, where the basis $\mathcal{B}$ of $H^1(X, \mathcal{O}_X)$ that corresponds to the coordinates x, y, z, w is associated to the basis of $H^3(\mathbb{P}^3, \mathcal{O}^3_{\mathbb{P}}(-c - d))$ given by

$$\{x^k y^l z^m w^n : (k, l, m, n) \in (\mathbb{Z}_{<0})^4 \text{ and } -k - l - m - n = c + d\}. \tag{2.3.2}$$

Using this fact, Kudo and Harashita [12] present an algorithm to compute the Hasse–Witt of such curves, which can be generalized to compute the corresponding matrix for any complete intersection over a perfect field of positive characteristic.

Proposition 2.3.5 (Kudo and Harashita [12], Prop. 3.1.4)**.** *Let X of genus g be defined as above and suppose $(FG)^{p-1} = \sum c_{i_1,i_2,i_3,i_4} x^{i_1} y^{i_2} z^{i_3} w^{i_4}$. Then the Hasse–Witt matrix of X is given by*

$$\begin{bmatrix} c_{-k_1p+k_1,-l_1p+l_1,-m_1p+m_1,-n_1p+n_1} & \cdots & c_{-k_rp+k_1,-l_rp+l_1,-m_rp+m_1,-n_rp+n_1} \\ \vdots & & \vdots \\ c_{-k_1p+k_r,-l_1p+l_r,-m_1p+m_r,-n_1p+n_r} & \cdots & c_{-k_rp+k_r,-l_rp+l_r,-m_rp+m_r,-n_rp+n_r} \end{bmatrix} \tag{2.3.3}$$

Notice that this computation gives a matrix H that represents the action of $\mathcal{F}_X$ by left matrix multiplication. Let $\mathbf{v}$ be the column vector corresponding to an element of $H^1(X, \mathcal{O}_X)$ expressed in terms of the basis $\mathcal{B}$. Then the image of $\mathbf{v}$ under $\mathcal{F}_X$ is given by $H \cdot \mathbf{v}^{(p)}$, since $\mathcal{F}_X$ is p-linear.

In the next section, we use Proposition 2.3.5 together with the equations from Section 2.3 to compute examples of non-hyperelliptic smooth curves of genus 4 with a-number 3.

2.4 A database of curves in standard form over $\mathbb{F}_p$

In this section we construct a database of genus 4 curves in standard form (Definition 2.3.3) over $\mathbb{F}_p$ for $p \in \{3, 5, 7, 11\}$. We restrict our data collection to non-ordinary and non-superspecial curves, that is, curves with a-number equal to $1, 2$ or 3. First let us explain the notation used:

- Let $\vec{a} \in \mathbb{F}_p^{20}$. We denote by $G_{\vec{a}}$ the cubic whose coefficients correspond to the entries of $\vec{a}$, assigned to the monomials of degree 3 in $\mathbb{F}_p[x, y, z, w]$ in graded lexicographic order, with $x > y > z > w$. For example, the vector $\vec{a} = (1, 1, 2, 0, 0, 1, 0, 2, 0, 2, 1, 1, 1, 2, 0, 0, 1, 0, 1, 0)$ corresponds to the cubic $x^3 + x^2y + 2x^2z + xyz + 2xz^2 + 2xw^2 + y^3 + y^2z + y^2w + 2yz^2 + z^3 + zw^2$.

- For each one of the cases D, N1i, N1ii and N2 in Definition 2.3.3 we define a subset of $\mathbb{F}_p^{20}$ such that for all $\vec{a}$ in that subset, the cubic $G_{\vec{a}}$ has the necessary conditions. If we denote each subset by $\mathbf{D}_p, \mathbf{N1i}_p, \mathbf{N1ii}_p$ and $\mathbf{N2}_p$ we have:

  1. $\vec{a} \in \mathbf{N1i}_p$ iff $\vec{a} = (0, a_1, a_2, 0, 0, a_3, 0, 0, 0, 0, 1, b_1, a_6, a_5, a_7, a_8, a_4, b_2, a_9, a_{10})$ with a_i and b_1 as in Definition 2.3.3, Case N1(i).

  2. $\vec{a} \in \mathbf{N1ii}_p$ iff $\vec{a} = (0, a_1, a_2, 0, 0, a_3, 0, 0, 0, 0, b_1, a_4, b_2, a_5, a_6, 0, b_3, a_7, a_8)$ with a_i and b_i as in Definition 2.3.3, Case N1(ii).

  3. $\vec{a} \in \mathbf{N2}_p$ iff
     $\vec{a} = (0, a_1, a_2, 0, a_3, 0, 0, -\epsilon a_3, 0, 0, b_1 + a_4, a_5, \epsilon(3a_4 - b_1), a_7, a_8, \epsilon a_5, b_2, a_9, a_{10})$ with a_i, b_i an ϵ as in Definition 2.3.3, Case N2.

  4. $\vec{a} \in \mathbf{D}_p$ iff $\vec{a} = (a_0, 0, 0, 0, a_1, a_4, 0, a_2, a_5, a_3, a_6, 0, 0, a_9, 0, 0, a_7, b_1, b_2, a_8)$ with a_i an b_i as in Definition 2.3.3, Case D.

We can count the number of elements of each of the sets above. The computations are shown in Table 2.1.

Table 2.1: Cardinality of the sets $\mathbf{D}_p$, $\mathbf{N1i}_p$, $\mathbf{N1ii}_p$, $\mathbf{N2}_p$.

Set	Cardinality
$\mathbf{D}_p$	$4p^3(p-1)^2(p^5+p-2)$
$\mathbf{N1i}_p$	$6p^8(p-1)^2$
$\mathbf{N1ii}_p$	$12p^6(p-1)^2$
$\mathbf{N2}_p$	$4p^7(p-1)$

To construct a curve in standard form we select an element $\vec{a}$ in one of the subsets above together with the corresponding $F \in \{F_1, F_2, F_d\}$ and verify if $V(F, G_{\vec{a}})$ is non-singular, irreducible

and has genus 4. In practice, we implement the algorithm in `Magma`, where we check each of the conditions as follows:

- Irreducibility: using the intrinsic `Magma` function `IsIrreducible`, which verifies the condition by a Gröbner basis computation. It is important to note that this does not check if the curve is irreducible after a base extension.

- Genus: the command `Genus` computes the arithmetic genus of the projective normalization of the curve.

- Nonsingularity: in this case we took two different approaches, but both determine if the curve (given as the zero set of homogeneous polynomials) is non-singular over the algebraic closure of its field of definition:

  (1) Using `Magma`'s command `IsNonsingular`.

  (2) Implementing Algorithm `DetermineNonSingularity` (Algorithm 3.2.1 in [12]), which is based on solving a radical membership problem on the minors of the Jacobian matrix of $V(F, G_{\vec{a}})$. The later is done by a `RadicalMembership` algorithm ([12], Appendix A)

Next, suppose that $X = V(F, G_{\vec{a}})$ is a curve in standard form, then we need to determine its a-number and p-rank. We do this by computing the Hasse–Witt matrix H of X with respect to the basis of $H^1(X, \mathcal{O}_X)$ given by (2.3.2), as in Proposition 2.3.5. The a-number is equal to $4 - \text{rank}(H)$ and the p-rank f is the rank of $HH^{(p)} \cdots H^{\left(p^{g-1}\right)}$. In our case, since F and $G_{\vec{a}}$ are defined over $\mathbb{F}_p$, then $f = \text{rank}(H^g)$.

2.4.1 Collecting the data

We collected two kinds of data of curves over $\mathbb{F}_p$:

Sampling search: We apply the above procedure to random samples of tuples in $\mathbf{D}_p$, $\mathbf{N1i}_p$, $\mathbf{N1ii}_p$ and $\mathbf{N2}_p$ for $p \in \{3, 5, 7, 11\}$ in order to gather statistical information. In addition, we classify the curves by a-number and p-rank.

We want to obtain a large sample, so in order to keep track of the computations we design an algorithm that allows us to build the sample in batches of given size. Let $\mathbf{S}$ be one of the sets above, then in `Magma` we define a *Sampled set* to store the tuples that have already been sorted.

1. Pick some n to be the size of the batch.

2. Build a *Current sample* by picking a random element $\mathbf{v}$ of $\mathbf{S}$, using the intrinsic `Random` command, then verify if $\mathbf{v}$ is in *Sampled set*, if it is not, then add it to *Current sample*. Repeat until the size of *Current sample* is n.

3. Verify the irreducibility, genus and smoothness conditions on the curves given by each tuple in the *Current sample* and then sort the ones that satisfy them by a-number.

4. Add the *Current sample* to the *Sampled set*.

Remark 2.4.1. When we analyze the samples of curves in our data, we will often compare the number of curves with certain p-rank and/or a-number with the total of smooth curves in standard form obtained. In our search we classify the curves with a-number $0, 1, 2$ and 3. We ignore the curves with $a = 4$ (that is, the superspecial ones) because they represent a very small proportion of the curves and hence they do not affect the percentages in a significant way. In fact, by Theorems 2.2.6 and 2.3.2 we know that there are no superspecial curves of genus 4 in characteristic 3 or 7. By Theorem 2.3.1 every such curve in characteristic 5 is isomorphic to one of $24^2 \times 5$ given curves over $\mathbb{F}_{25}$. Also, our focus will be studying the occurrence of Cartier points (see Section 2.5), and we already know that superspecial curves have infinitely many of them (Baker [2]). Here is how we will refer to our different samples:

- **Total set**: the set $\mathbf{D}_p$, $\mathbf{N1i}_p$, $\mathbf{N1ii}_p$ or $\mathbf{N2}_p$, depending on the case.

- **Sampled set**: the subsets of the sets above that are included in our random search.
- **Smooth sample**: the set of cubics from the sampled set that give smooth, irreducible, genus 4 curves (excluding superspecial curves, see Remark 2.4.1).
- **Singular sample**: the set of cubics from the sampled set that give curves that fail either one of the conditions for smoothness, irreducibility or genus.

If we do not specify the subcase, then **Sampled set**, **Smooth sample** and **Singular sample** will refer to the total samples throughout the four cases. The analysis of this data is done in Section 2.4.2.

Exhaustive search: In order to focus on the analysis of some aspects of genus 4 curves with a-number 3, we apply the procedure above to all the tuples in $\mathbf{D}_p, \mathbf{N1i}_p, \mathbf{N1ii}_p$ and $\mathbf{N2}_p$, but only store the smooth, irreducible curves with $a = 3$. We did this for $p = 3, 5$. The search is also done for $p = 7$ but only for tuples in $\mathbf{D}_7$ and a subset of $\mathbf{N1i}_7$, because of the long computing times. It is important to remark that after the search, we classify the curves by $\mathbb{F}_p$-isomorphism classes. For details on the analysis and results obtained from this search see Section 2.4.3.

2.4.2 Summary of results of sampling search

In this section we display the overall results from the sampling search. The sizes of our final Sampled sets by case are shown in Table 2.2.

Table 2.2: Total samples size over $\mathbb{F}_p$.

p	D	N1i	N1ii	N2	Total sample
3	52704	92123	34992	6447	186266
5	179728	179970	179434	179970	719102
7	215957	225193	206890	214998	863038
11	89999	91100	89999	90000	361098

In Table 2.3 we list the number of curves with p-ranks $f = 0, 1, 2, 3$ and a-number $a = 1, 2, 3$, over $\mathbb{F}_p$ for $p \in \{3, 5, 7, 11\}$. We include the totals for the singular samples and the ordinary curves (that is, those with a-number 0). From this classification we have the following statement:

Corollary 2.4.2. *In our data set of genus* 4 *curves in standard form there are no curves with* p*-rank* 0 *and* a*-number* 1*, when* $p \in \{3, 5, 7, 11\}$.

Proof. See Table 2.3. □

Table 2.3: Sample of curves in standard over $\mathbb{F}_p$.

a	f	3	5	7	11
Sampled set		186266	719102	863038	361098
Singular sample		92654	251584	191925	81845
0		56983	370476	529394	253627
1	0	0	0	0	0
1	1	1679	3592	1652	217
1	2	4134	14615	10687	2146
1	3	23485	74585	76142	23044
	Total	29298	92792	88481	25407
2	0	1157	183	44	3
2	1	2095	790	231	21
2	2	3379	3231	1624	194
	Total	6631	4204	1899	218
3	0	0	10	0	0
3	1	700	36	5	1
	Total	700	46	5	1
Smooth sample		93612	467518	619779	279253

Next we discuss the results from the search for each p. We include the sizes of the total set, sampled set, smooth sample and singular sample, normalized by $\log_p$. Then we show the break down of curves with $a = 1, 2, 3$ and specify the percentage of the sampled set and smooth sample they represent.

Case $p = 3$.

We checked a total of 186266 tuples, which corresponds to approximately 71% of all the possible tuples. We saw that 50.26% of them gave smooth curves and 19.66% of the total had a-number $a = 1, 2, 3$. Table 2.4 contains the sizes of the total set and the samples obtained from the search, normalized by $\log_3$. Notice that we were able to sort all of the cubics from the total sets $\mathbf{D}_3$ and $\mathbf{N1ii}_3$. In Table 2.5 we show the number of curves sorted by a-number and p-rank. We remark that there are no curves of p-rank 0 with a-numbers 1 or 3.

Table 2.4: Sizes of samples for curves over $\mathbb{F}_3$ normalized by $\log_3$.

	$\mathbf{D}_p$	$\mathbf{N1i}_p$	$\mathbf{N1ii}_p$	$\mathbf{N2}_p$	Total
Total set	9.8965	10.8928	9.5237	8.8928	11.3585
Sampled set	9.8965	10.4048	9.5237	7.9840	11.0457
Smooth sample	9.3967	9.8705	8.1561	7.5868	10.4194
Singular sample	9.1123	9.6658	9.2946	7.0379	10.4101

Table 2.5: Curves in standard form over $\mathbb{F}_3$ from a sample of size 186266 tuples.

a	f	Total curves	% of sample	% of smooth sample
Singular sample		92654	49.74	-
0		56983	30.59	60.871
1	0	0	0	0
1	1	1679	0.90	1.794
1	2	4134	2.22	4.416
1	3	23485	12.61	25.088
	Total	29298	15.73	31.297
2	0	1157	0.62	1.236
2	1	2095	1.12	2.238
2	2	3379	1.81	3.610
	Total	6631	3.56	7.083
3	0	0	0	0
3	1	700	0.38	0.748
	Total	700	0.38	0.748
	Total smooth	93612	50.26	100.00

Case $p = 5$.

We selected a random sample of 719102 tuples in $\mathbf{D}_5, \mathbf{N1i}_5, \mathbf{N1ii}_5$ and $\mathbf{N2}_5$. This is around 1.49% of the total set. A 61.01% of that sample corresponds to the Smooth sample, and 13.49% of the total are non-ordinary curves. In Table 2.6 we detail the sizes of our samples, normalized by $\log_5$. In Table 2.7 we show the results, sorted by a-number and p-rank.

Table 2.6: Sizes of samples for curves over $\mathbb{F}_5$ normalized by $\log_5$.

	$\mathbf{D}_p$	$\mathbf{N1i}_p$	$\mathbf{N1ii}_p$	$\mathbf{N2}_p$	Total
Total curves	9.7233	10.8360	9.2667	8.7227	10.9894
Sampled set	7.5177	7.5185	7.5166	7.5185	8.3792
Smooth sample	7.3462	7.3146	6.8105	7.3796	8.1116
Singular sample	6.6339	6.7270	7.2762	6.5194	7.7266

Table 2.7: Curves in standard form over $\mathbb{F}_5$ from a sample of 719102 tuples.

a	f	Total curves	% of sample	% of smooth sample
Singular sample		251584	34.99	-
0		370476	51.52	79.24
1	0	0	0.00	0.00
1	1	3592	0.50	0.76
1	2	14615	2.03	3.12
1	3	74585	10.37	15.95
	Total	92792	10.37	19.84
2	0	183	0.03	0.03
2	1	790	0.11	0.16
2	2	3231	0.45	0.69
	Total	4204	0.58	0.89
3	0	10	0.00	0.002
3	1	36	0.01	0.007
	Total	46	0.01	0.009
	Total smooth	467518	65.01	100

Case $p = 7$.

We analyzed a random sample of 863038 pairs of tuples in $\mathbf{D}_7$, $\mathbf{N1i}_7$, $\mathbf{N1ii}_7$ and $\mathbf{N2}_7$, which corresponds to 0.06% of the total. The smooth sample from this set has 619779 tuples and 90385 of them are curves in standard form with a-number $1, 2$ or 3. These correspond to 71.81% and 10.47% of the total, respectively. Table 2.8 contains the normalized sizes of the total and sampled sets, as well as the smooth and singular samples. In 2.9 we detail the distribution of these curves by a-number and p-rank.

Table 2.8: Sizes of samples for curves over $\mathbb{F}_7$ normalized by $\log_7$.

	$\mathbf{D}_p$	$\mathbf{N1i}_p$	$\mathbf{N1ii}_p$	$\mathbf{N2}_p$	Total
Total curves	9.6333	10.7623	9.1186	8.6332	10.8421
Sampled set	6.3121	6.3336	6.2901	6.3098	7.0241
Smooth sample	6.2188	6.2165	5.7756	6.2309	6.8539
Singular sample	5.3897	5.5162	6.0547	5.3082	6.3733

Table 2.9: Curves in standard form over $\mathbb{F}_7$ from a sample of 863038 tuples.

a	f	Total curves	% of sample	% of smooth sample
Singular sample		191925	22.24	-
0		529394	61.34	85.417
1	0	0	0.00	0.000
1	1	1652	0.19	0.267
1	2	10687	1.24	1.724
1	3	76142	8.82	12.285
	Total	88481	8.82	14.276
2	0	44	0.01	0.007
2	1	231	0.03	0.037
2	2	1624	0.19	0.262
	Total	1899	0.22	0.306
3	0	0	0.00	0.000
3	1	5	0.00	0.001
	Total	5	0.00	0.001
	Total smooth	619779	71.81	100

Case $p = 11$

In this case we did a random search that included 361098 tuples in $\mathbf{D}_{11}, \mathbf{N1i}_{11}, \mathbf{N1ii}_{11}$ and $\mathbf{N2}_{11}$, this is approximately 0.0002% of the total set. Of this sample, 77.33% are smooth and 7.10% of the total are non-ordinary. In Table 2.11 we can see the break-down of the curves with a-number $1, 2$ and 3. Notice that no a-number 2 or 3 curve has p-rank 0. For the sizes of the samples, normalized by $\log_{11}$ are displayed in Table 2.10.

Table 2.10: Sizes of samples for curves over $\mathbb{F}_{11}$ normalized by $\log_{11}$.

	$\mathbf{D}_p$	$\mathbf{N1i}_p$	$\mathbf{N1ii}_p$	$\mathbf{N2}_p$	Total
Total curves	9.5384	10.6677	8.9568	8.5384	10.7034
Sampled set	4.7573	4.7624	4.7573	4.7573	5.3367
Smooth sample	4.7128	4.7036	4.3903	4.7181	5.2295
Singular sample	3.8025	3.9163	4.5339	3.7522	4.7177

Table 2.11: Curves in standard form over $\mathbb{F}_{11}$ from a sample of 361098 tuples.

a	f	Total curves	% of sample	% of smooth sample
Singular sample		81845	22.67	-
0		253627	70.24	90.8234
1	0	0	0	0
1	1	217	0.06	0.0777
1	2	2146	0.59	0.7685
1	3	23044	6.38	8.2520
	Total	25407	7.04	9.0982
2	0	3	0	0.0011
2	1	21	0.01	0.0075
2	2	194	0.05	0.0695
	Total	218	0.06	0.0781
3	0	0	0	0
3	1	1	0.0003	0.0004
	Total	1	0.0003	0.0004
	Total smooth	279253	77.33	100.00

2.4.3 Summary of results from exhaustive search

In the cases $p = 3, 5$ we also have a complete list of all curves in standard form that have a-number 3. For $p = 7$ we have a subset of them: the ones in case D and those in case N1i where $(b_1, b_2) = (0, 0)$, we denote these lists by 7(D) and 7(N1i'). The information on these curves, classified by isomorphism classes, is shown in Table 2.12. A first conclusion that we can draw from this data is the following:

Corollary 2.4.3. *There are no genus* 4 *curves in standard form over* $\mathbb{F}_3$ *with* p*-rank* 0 *and* a*-number* 3.

Table 2.12: Isomorphism classes of curves in standard form with $a = 3$ over $\mathbb{F}_p$.

p-rank	3	5	7(D)	7(N1i')
0	0	36	9	2
1	27	98	56	27
Total	27	134	65	29

Case $p = 3$

There are a total of 1188 vectors $\vec{a}$ in $\mathbf{D}_3$, $\mathbf{N1i}_3$, $\mathbf{N1ii}_3$ and $\mathbf{N2}_3$ that give curves of genus 4 and a-number 3 over $\mathbb{F}_3$. We give a summary of the number of vectors classified by case and some restrictions that occur in the case D. We use `Magma` to classify these curves in $\mathbb{F}_3$-isomorphism classes, which we detail in Table 2.13 and Lemma 2.4.5.

Table 2.13: Isomorphism classes of genus 4 and $a = 3$ curves over $\mathbb{F}_3$.

Case	# Isomorphism classes	# p-rank 1	# p-rank 0
D	6	6	0
N1(i)	7	7	0
N1(ii)	3	3	0
N2	11	11	0
Total	27	27	0

Corollary 2.4.4. *There are, up to $\mathbb{F}_3$-isomorphism, exactly 27 curves of genus 4 with $a = 3$ in standard form.*

Proof. See Table 2.13. □

Lemma 2.4.5. *Let X be a curve in standard form with a-number 3 defined over $\mathbb{F}_3$. Then X is isomorphic to one of the following:*

- *$V(F_d, G)$ with*

$$G = x^3 + y^3 + xyz + c_1yz^2 + xw^2 + c_2w^3,$$

  where $c_1 \in \mathbb{F}_3^\times$ and $c_2 \in \mathbb{F}_3$.

- *$V(F_1, G)$ with*

$$G = x^2y + c_1y^3 + x^2z + c_2y^2w + c_3w^3 + c_4z^3 + z^2w,$$

  where $c_1 \in \{0, 1\}$, $c_2, c_3 \in \mathbb{F}_3^\times$ and $c_4 \in \mathbb{F}_3$.

- $V(F_2, G)$ *with*

$$G = x^2y + c_1y^3 + c_2x^2z + c_3z^3 + c_4yzw + c_5w^3 + c_6(z^2w + y^2w),$$

where $c_1, c_3 \in \mathbb{F}_3$*,* $c_2, c_4, c_5 \in \mathbb{F}_3^\times$ *and* $c_6 \in \{0, 1\}$.

In the case D, we identified some necessary conditions for $\vec{a}$ to give rise to a smooth curve with a-number 3. Recall from Definition 2.3.3 that the term in $G_{d,\vec{a}}$ where x is degree 1 is $r = a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw$ and it is 0 or has leading coefficient 1. The cubics that give a-number 3 curves have a_1, a_3 or a_4 as the leading coefficient of r. In fact, we show in Proposition 2.4.6 that there is a family of smooth curves of this form over $\overline{\mathbb{F}}_3$ which have a-number 3 and p-rank 1.

Proposition 2.4.6. *There exists a family of dimension* $d \leq 4$ *of genus* 4 *non-hyperelliptic smooth curves over* $\overline{\mathbb{F}}_3$ *with* a*-number* 3 *and* p*-rank* 1.

Proof. Let $k = \overline{\mathbb{F}}_3$ and let $\mathcal{X}$ be the family of curves given by $V(F, G)$ where

$$F = 2yw + z^2,\ G = a_0x^3 + xyz + a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + zw^2, \tag{2.4.1}$$

with $a_i \in k$ and $a_0, a_6 \in k^\times$.

Now consider the map

$$\begin{aligned} \mathcal{X} &\to (\mathbb{A}^1_k)^5 \\ V(F, G) &\mapsto (a_0, a_6, a_7, a_8, a_9), \end{aligned}$$

and let X_0 be the fiber in $\mathcal{X}$ over $(1, 1, 0, 0, 0)$. That is, $X_0 = V(F, G_0)$ with $G_0 = x^3 + xyz + y^3 + zw^2$. We see that X_0 is smooth because its Jacobian matrix

$$\text{Jac}(P) = \begin{bmatrix} 0 & 2w & 2z & 2y \\ yz & xz & xy + w^2 & 2zw \end{bmatrix}, \tag{2.4.2}$$

has rank 2 at every point of X_0. This implies that there is an open subset U of $(\mathbb{A}^1_k)^5$ such that every fiber above U is smooth. From here we can also see, by the genus formula, that the genus is 4 for all of them.

By Proposition 2.3.5 the Hasse–Witt matrix of every curve in this family is

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{2.4.3}$$

from where the a-number is 3 and the p-rank is 1.

Finally, we can show that any curve as in (2.4.1) can be reduced so that G has a coefficient $a_6 = 1$. Indeed, pick some d such that $d^5 = a_6^{-1}$ and apply the change of variables

$$(x, y, z, w) \to (x, d^4y, d^3z, d^2w). \tag{2.4.4}$$

Let $\tilde{F}$ and $\tilde{G}$ be the polynomials obtained from F and G after this change, respectively. Then $\tilde{F} = d^6F$ and

$$\tilde{G} = a_0x^3 + d^7xyz + a_6d^{12}y^3 + a_7d^9z^3 + a_8d^6w^3 + a_9d^{10}yz^2 + d^7zw^2. \tag{2.4.5}$$

So by multiplying $\tilde{G}$ by d^{-7} we obtain a cubic of the form

$$a_0'x^3 + xyz + y^3 + a_7'z^3 + a_8'w^3 + a_9'yz^2 + zw^2, \tag{2.4.6}$$

with $a_i' \in k$ and $a_0' \in k^\times$. Hence this family depends on 4 parameters, at most.

□

Case $p = 5$

From the exhaustive search we conclude that there are 134 $\mathbb{F}_5$-isomorphism classes of standard form curves over $\mathbb{F}_5$ with a-number 3. Table 2.14 contains the summary of the isomorphism classes and the number of curves with p-rank 1 and p-rank 0.

In addition, we found some necessary conditions on $\vec{a} \in \mathbf{D}_5$ for $V(F_d, G_{\vec{a}})$ to be a smooth genus 4 curve with $a = 3$. For instance, the leading coefficient of $r = a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw$ is never a_5 nor does it happen that $r = 0$. Also, all of these curves have $a_7 = a_9 = 0$.

Table 2.14: Isomorphism classes of genus 4 and $a = 3$ curves over $\mathbb{F}_5$.

Case	# Isomorphism classes	# p-rank 1	# p-rank 0
D	59	46	13
N1(i)	60	48	12
N1(ii)	6	4	2
N2	9	0	9
Total	134	98	36

Corollary 2.4.7. *There are, up to* $\mathbb{F}_5$*-isomorphism, exactly* 134 *curves of genus* 4 *and* $a = 3$ *in standard form.*

Proof. See Table 2.14. □

Case $p = 7$

The exhaustive search for all curves in standard form with $a = 3$ proved to be too time consuming for $p = 7$. So it was only possible to find the curves in the case D and a subset of N1 curves. We conclude from this search that there are at least 94 $\mathbb{F}_7$-isomorphism classes of curves of a-number 3, where 65 correspond to the case D and 29 to the N1. Now, we know by Lemma 4.5.1 in [12] that any smooth, irreducible, genus 4 curve $X = V(F_d, G)$ can be written in standard form. This is because condition (A3) is satisfied over $\mathbb{F}_7$ and G can be reduced by a change of variables to the form of Definition 2.3.3. This implies that the list of curves that we found in the case D actually includes all of the curves where the quadratic polynomial is degenerate.

Corollary 2.4.8. *There are, up to $\mathbb{F}_7$-isomorphism, exactly 65 genus 4 and a-number 3, smooth, irreducible, non-hyperelliptic curves over $\mathbb{F}_7$, given as $V(F, G)$, where G is a cubic homogeneous polynomial and F is a degenerate quadratic form. In addition, there are, up to $\mathbb{F}_7$-isomorphism, at least 29 genus 4 curve in standard form over $\mathbb{F}_7$ with a-number 3 where F is non-degenerate.*

Proof. Table 2.15 shows the total of □

In the case D there are 1440 curves with a-number 3, which are divided into 65 classes, 56 of them have p-rank 1 and 9 have p-rank 0. The subset of curves of the case N1 that we computed corresponds to those where the the cubic is of the form

$$G = (a_1y + a_2z)x^2 + a_3yzx + y^3 + a_4z^3 + a_5yz^2 + (a_6y^2 + a_7yz)w + (a_8y + a_9z)w^2 + a_{10}w^3,$$

for $a_i \in \mathbb{F}_7$ with $a_1 \neq 0$, $a_2 \neq 0$. There are 432 of these G such that $V(F_1, G)$ is a smooth genus 4 smooth curve with a-number 3, only 16 have p-rank 0. These curves are distributed in 29 $\mathbb{F}_7$-isomorphism class with 2 of them having p-rank 0 and 27 of p-rank 1.

Table 2.15: Isomorphism classes of genus 4 and $a = 3$ curves over $\mathbb{F}_7$.

Case	# Isomorphism classes	# p-rank 1	# p-rank 0
D	65	56	9
N1i'	29	27	2
Total	94	83	11

2.5 Cartier points

2.5.1 Definition and properties

Theorem 2.2.6 states that the genus of a superspecial curve in characteristic p is bounded by $p(p-1)/2$. Ekedahl [5] bases the proof of this result on the fact that a curve is superspecial if and only if its Jacobian is isomorphic to the product of supersingular elliptic curves (Oort, [19]). Baker, on the other hand, presents in [2] an alternative proof which makes use of an equivalent definition: a curve is superspecial if and only if the Cartier operator annihilates $H^0(X, \Omega^1_X)$. The other component of his proof is the existence of linear systems of dimension 1, associated to a certain type of points on X, defined as Cartier points.

Definition 2.5.1. A closed point P of X is said to be a Cartier point if the hyperplane of regular differentials vanishing at P is stable under the Cartier operator.

Theorem 2.2.6 is a corollary of the following result:

Theorem 2.5.2 (Baker [2], Theorem 2.8)**.** *Let X be a curve of genus g over an algebraically closed field of characteristic p.*

1. *If X has at least p distinct Cartier points, no two of which differ by a p-torsion point on J_X, then $g \leq p(p-1)/2$.*

2. *If X is hyperelliptic of genus g, p is odd, and some hyperelliptic branch point of X is a Cartier point, then $g \leq (p-1)/2$.*

Notation 2.5.3. *Let k be a field of characteristic p. Let X be a non-hyperelliptic curve of genus g over k embedded in $\mathbb{P}(H^0(X, \Omega^1_X)) = \mathbb{P}^{g-1}$ by a basis $\mathcal{B}' = \{\omega_1, \ldots, \omega_g\}$ of $H^0(X, \Omega^1_X)$. Suppose $x_1, \ldots, x_g$ are the coordinates of $\mathbb{P}^{g-1}$ given by this basis and that $\mathcal{B}$ is the basis of $H^1(X, \mathcal{O}_X)$ dual to $\mathcal{B}'$. Given a point $P = [a_1 : \ldots : a_g]$ of X we denote by $\mathbf{v}_P$ the vector $(a_1, \ldots, a_g)^T$ in $H^1(X, \mathcal{O}_X)$ expressed in terms of $\mathcal{B}$. Conversely, given a vector $\mathbf{w} = (b_1, \ldots, b_g)^T$ in $H^1(X, \mathcal{O}_X)$ expressed in terms of $\mathcal{B}$, let $Q_{\mathbf{w}}$ denote the point $[b_1 : \ldots : b_g]$. From here on, we consider the Hasse–Witt matrix H of X to be in terms of the basis $\mathcal{B}$, unless otherwise stated.*

Proposition 2.5.4. *Let X be a non-hyperelliptic curve of genus g over k embedded in $\mathbb{P}^{g-1}$ as in Notation 2.5.3. A point $P = [a_1 : \ldots : a_g]$ of $X(\overline{k})$ is a Cartier point if and only if there exists $c \in \overline{k}$ such that*

$$H\mathbf{v}_P^{(p)} = c\mathbf{v}_P, \tag{2.5.1}$$

where $\mathbf{v}_P^{(i)}$ indicates that each entry of the vector is raised to the i-th power.

Proof. Since X is embedded in $\mathbb{P}^{g-1}$ by $\{\omega_1, \ldots, \omega_g\}$ then $\omega_i(P) = a_i$, for $i = 1, \ldots, g$. A regular 1-form $\omega = b_1\omega_1 + \cdots + b_g\omega_g$ vanishes at P if and only if

$$b_1a_1 + \cdots + b_ga_g = 0. \tag{2.5.2}$$

Then the hyperplane of 1-forms vanishing at P is

$$L_P := \left\{(b_1, \ldots, b_g)^T : b_1a_1 + \cdots + b_ga_g = 0\right\}. \tag{2.5.3}$$

Let L_P^0 be the annihilator of L_P. We know that this is a 1-dimensional subspace of $H^0(X, \Omega^1_X)^* \cong H^1(X, \mathcal{O}_X)$, so it is generated by the vector $\mathbf{v} = (a_1, \ldots, a_g)^T$.

Now, L_P is stable under the action of $\mathcal{C}$ if $\mathcal{C}(\omega) \in L_P$, for every $\omega \in L_P$. By duality, this is equivalent to $\mathcal{F}_X(\mathbf{v}_P) = c\mathbf{v}_P$, that is, $H\mathbf{v}_P^{(p)} = c\mathbf{v}_P$.

□

Definition 2.5.5. We say that a Cartier point $P \in X$ as above is of *Type* 1 if $c = 0$ and of *Type* 2 otherwise.

Notice that if k is not algebraically closed, then the Cartier points of X/k might not be defined over k, but over some extension. In general we consider Cartier points as points in $X(\overline{k})$.

The next lemma gives us a way to find the Type 1 points.

Lemma 2.5.6. *A point P is a Type 1 Cartier point of X if and only if $H^{(1/p)}\mathbf{v}_P = 0$.*

Proof. By definition P is a Type 1 point of X if and only if $H\mathbf{v}^{(p)} = 0$. By applying the inverse of the p-th Frobenius morphism we see that this is equivalent to $H^{(1/p)}\mathbf{v}_P = 0$. □

Corollary 2.5.7. *Supose X is defined over $\mathbb{F}_p$. Then $P \in X$ is a Type 1 point if and only if $H\mathbf{v}_P = 0$.*

Suppose that X is defined over $\mathbb{F}_q$, with $p^r = q$ for some positive integer r. For a point $Q \in X$ we denote by $\sigma(Q)$ the action of the r-th power of the Frobenius morphism on Q. It turns out that the set of Cartier points is stable under the action of σ.

Lemma 2.5.8. *Let Q be a Cartier point of $X/\mathbb{F}_q$ and let $P = \sigma(Q)$. Then Q is a Cartier point of X if and only if $P := \sigma(Q)$ is a Cartier point of X. Furthermore, if $H\mathbf{v}_Q^{(p)} = c\mathbf{v}_Q$, then $H\mathbf{v}_P^{(p)} = c^q\mathbf{v}_P$.*

Proof. First we note that P is also a point on X, because $X = V(F, G)$ and F and G are defined over $\mathbb{F}_q$. Let H be the Hasse–Witt matrix of X. After scaling, we can assume that $\mathbf{v}_Q^{(q)} = \mathbf{v}_P$. Then

$$
\begin{aligned}
H\mathbf{v}_Q^{(p)} = &\quad c\mathbf{v}_Q &\iff\\
(H\mathbf{v}_Q^{(p)})^{(q)} = &\quad (c\mathbf{v}_Q)^{(q)} &\iff\\
H^{(q)}(\mathbf{v}_Q^{(p)})^{(q)} = &\quad c^q\mathbf{v}_Q^{(q)} &\iff\\
H(\mathbf{v}_Q^{(q)})^{(p)} = &\quad c^q(\mathbf{v}_Q)^{(q)} &\iff\\
H\mathbf{v}_P^{(p)} = &\quad c^q\mathbf{v}_P.
\end{aligned}
$$

Where the second to last equivalence is true because X is defined over $\mathbb{F}_q$ then so is H. □

We apply Lemma 2.5.8 to reduce the search of Cartier points to a computation of eigenvectors.

Lemma 2.5.9. *Suppose X is defined over $\mathbb{F}_p$ and H is its Hasse–Witt matrix. Let Q be a Cartier point of X defined over $\mathbb{F}_{p^e}$. There exists $\lambda \in \mathbb{F}_p$ such that $H^e\mathbf{v}_Q = \lambda\mathbf{v}_Q$.*

Proof. Since Q is a Cartier point in of X then $H\mathbf{v}_Q^{(p)} = c\mathbf{v}_Q$ for some $c \in \overline{\mathbb{F}}_p$. Now, since $Q \in X(\mathbb{F}_{p^e})$, then $c \in \mathbb{F}_{p^e}$. Let $P_i := \sigma^i(Q)$, then $P_1, P_2, \ldots, P_e = Q$ are distinct Cartier points. Also, after scaling we can assume that $\mathbf{v}_{P_i}^{(p)} = \mathbf{v}_{P_{i+1}}$. After applying i times the result from Lemma 2.5.8 with $q = p$, we get that $H\mathbf{v}_{P_i}^{(p)} = c^{p^i}\mathbf{v}_{P_i}$. To ease notation, we write $\mathbf{v}_i$ instead of $\mathbf{v}_{P_i}$. Then

$$
H^e\mathbf{v}_e = \quad H^e\mathbf{v}_{e-1}^{(p)} = H^{e-1}\left(H\mathbf{v}_{e-1}^{(p)}\right) = H^{e-1}\left(c^{p^{e-1}}\mathbf{v}_{e-1}\right) = c^{p^{e-1}}H^{e-1}\mathbf{v}_{e-2}^{(p)}.
$$

By an inductive process, we get that $H^e\mathbf{v}_Q = c^{p^{e-1}+p^{e-2}\cdots+p+1}\mathbf{v}_Q = c^{\frac{p^e-1}{p-1}}\mathbf{v}_Q$. Let $\lambda := c^{\frac{p^e-1}{p-1}}$. Since $c \in \mathbb{F}_{p^e}$ then λ is a $(p-1)$-root of unity, if $c \neq 0$ and $\lambda = 0$ if $c = 0$. Hence $\lambda \in \mathbb{F}_p$.

□

Baker provides in [2] an upper bound for the number of Cartier points on a smooth irreducible curve that is not ordinary nor superspecial. Recall that such points might only be defined on the curve after some base field extension.

Proposition 2.5.10 (Baker, [2] Prop. 3.3)**.** *Let X be a smooth, irreducible curve of genus g with p-rank f, which is not ordinary nor superspecial.*

1. *The number of Type 2 points on X is bounded by*

$$b := b_{g,p,f,\delta_X} = \min\left(2g-2, \delta_X \frac{p^f-1}{p-1}\right), \tag{2.5.4}$$

   where δ_X is 2 if X is hyperelliptic and 1 otherwise.

2. *The number of Type 1 points on X is bounded by $2g-2$. Furthermore, if the a-number of X is $g-1$ then there is at least one Type 1 Cartier point on X.*

Let us explore the geometric meaning of this bound, following the proof of Proposition 2.5.10 in [2]. We will only be concerned with non-hyperelliptic curves, so here $\delta_X = 1$.

We know by Proposition 2.5.4 that $P \in X(\overline{k})$ is a Cartier point if and only if there exists $c \in \overline{k}$ such that

$$H\mathbf{v}_P^{(p)} = c\mathbf{v}_P. \tag{2.5.5}$$

Suppose that $c = 0$, then by Lemma 2.5.6 Equation (2.5.5) is equivalent to $H\mathbf{v}_P^{(1/p)} = 0$. This implies that the Type 1 points are those in the intersection of $X(\overline{k})$ and the subspace spanned by the kernel of $H^{(1/p)}$ in $\mathbb{P}^{g-1}$. This subspace is linear and has codimension at least 1, so it is contained in a hyperplane. From where we conclude that the number of points in the intersection is at most the degree of the curve $2g-2$.

On the other hand, if $c \neq 0$ then we can rewrite Equation (2.5.5) as $H\mathbf{w}^{(p)} = \mathbf{w}$ by setting $\mathbf{w} = \lambda\mathbf{v}_P$ for λ equal to some $(p-1)$-th root of c^{-1}. Now the element of $H^1(X, \mathcal{O}_X)$ given by $\mathbf{w}$ is fixed by the Frobenius operator. By definition the p-rank f is the dimension of the subspace of $H^1(X, \mathcal{O}_X)$ where $\mathcal{F}$ is bijective. So there are $p^f - 1$ non trivial solutions, that yield at most $\frac{p^f-1}{p-1}$ Type 2 points. We can improve this bound: after maybe doing a base extension on X one can choose a basis of $H^0(X, \Omega^1_X)$ given by $\{\xi_1, \ldots, \xi_g\}$ such that $\mathcal{C}(\xi_i) = \xi_i$ for $1 \leq i \leq f$. Assume

that the coordinates of a Type 2 point are given by this basis, then, in particular some coordinate, say x_g of every such point must be zero, since $f < g$. Then the point lies on the hyperplane $x_g = 0$. Again, there can only be $2g-2$ such points, so the number of Type 2 points is $\min\{2g-2, \frac{p^f-1}{p-1}\}$.

As a direct consequence of the existence of the upper bound on the number of Cartier points, we also get a bound on the degree of the field of definition of the point. In particular, we have Corollary 2.5.11 for the case $k = \mathbb{F}_q$.

Corollary 2.5.11. *Let X be a genus g non-hyperelliptic curve that is not ordinary nor superspecial, defined over $\mathbb{F}_q$.*

- *If P is a Type 1 Cartier point of X, then $P \in X(\mathbb{F}_{q^e})$ with $1 \leq e \leq 2g-2$.*
- *If P is a Type 2 Cartier point of X, then $P \in X(\mathbb{F}_{q^e})$ with $1 \leq e \leq b$, where b is as in Proposition 2.5.10.*

Proof. Let P be a Cartier point of X. Let e be the minimum positive integer such that $P \in X(\mathbb{F}_{q^e})$. By Lemma 2.5.8, the e distinct points $\{P, \sigma(P), \sigma^2(P), \ldots, , \sigma^{e-1}(P)\}$ are all Cartier points of the same type. By Proposition 2.5.10, there are at most $2g-2$ Type 1 points and b Type 2 points. Hence, if P is a Type 1 points (resp. Type 2), then $e \leq 2g-2$ (resp. $e \leq b$).

□

Type 1 points in the case $a = g-1$

The behavior of the Cartier points when the a-number is $g-1$ has an additional feature which is the multiplicity. In this case, the subspace S generated by the kernel of $H^{(1/p)}$ is a hyperplane, then assuming $X \nsubseteq S$, the intersection $X \cap S$ is proper. Then we can define the intersection multiplicity of $P \in X \cap S$, that is, of the Type 1 Cartier points. We use the definition from Miranda [17]. Let L be a homogeneous linear polynomial defining S and L_0 another linear polynomial that does not vanish at P. Then the multiplicity of P in $X \cap S$ is the order of the rational function $h = L/L_0$ at P. One can show that this does not depend on the choice of L_0. Let $P_1, \ldots, P_n$ be the points

in $X \cap S$. We denote each multiplicity distribution of the set of Type 1 Cartier points of X by a partition of $2g-2$. So if $(m_1, m_2, \ldots, m_n)$ denotes the multiplicity of the Type 1 points of X, then there is one point of multiplicity m_i for $i = 1, \ldots, n$ and $\sum_{i=1}^{n} m_i = 2g-2$.

Now we want to determine the possible fields of definition of the Type 1 points, depending on their multiplicity. Since L is defined over $\mathbb{F}_q$, the order of h at P is the same as the order of h at $\sigma(P)$. Therefore the multiplicity of P is preserved under σ. Similarly, the degree is preserved. Let d_i be the degree of the point P_i, then $P_i, \sigma(P_i), \sigma^2(P_i), \ldots, \sigma^{d_i-1}(P_i)$ are d_i points of the same degree and multiplicity. We use $[(m_1, m_2, \ldots, m_n), (d_1, \ldots, d_n)]$ to denote that the curve has n Type 1 points $P_1, \ldots, P_n$ where P_i has multiplicity m_i and degree d_i.

We pay special attention to those curves where the bounds on the Cartier points are attained, which for the case when $a = g-1$ implies that all the points in the intersection of S and X are of multiplicity one. It is not hard to see that there are exactly as as many possible degree distribution for those points as partitions of $2g-2$.

In Section 2.5.2 we discuss this bound in the case of genus 4 non-hyperelliptic curves and how the bound depends on the a-number and p-rank of the curve.

2.5.2 Cartier points on genus 4 curves

Suppose $q = p^r$ for some positive integer r and let $X = V(F, G)$ be a non-ordinary and non-superspecial smooth, irreducible genus 4 non-hyperelliptic curve over $\mathbb{F}_q$. We want to determine the sharpness of Baker's bound from Proposition 2.5.10 for the number of Cartier points on X. We will first make some remarks about the possible bounds depending on the a-number and the p-rank.

Corollary 2.5.12 (Type 2 Cartier points and the p-rank)**.** *Let X be a non-hyperelliptic curve of genus 4 defined over $\mathbb{F}_q$ with p-rank f.*

(i) There are at most 6 Type 2 points on X and they are defined over $\mathbb{F}_{q^e}$ for some $1 \leq e \leq 6$.

Moreover:

(ii) *if* $f = 0$*, then there are no Type* 2 *points;*

(iii) *if* $f = 1$*, then there is at most* 1 *Type* 2 *point and it must be defined over* $\mathbb{F}_q$*;*

(iv) *if* $f = 2$*, then there are at most* 6 *Type* 2 *points, at most* 3 *if* $p = 2$ *and at most* 4 *if* $p = 3$*.*

Proof. Parts *(i)*, *(ii)* and *(iv)* are direct consequences of the discussion following Proposition 2.5.10. Indeed, the minimum of $2g - 2 = 6$ and $\frac{p^f-1}{p-1}$ is 6, unless $f \leq 1$ or $p = 2, 3$ and $f = 2$.

For *(iii)*, let Q be a Type 2 Cartier point of X and suppose that $P = \sigma(Q) \neq Q$. By Lemma 2.5.8 we have that P is another Cartier point of Type 2, which is a contradiction. □

Corollary 2.5.13 (Type 1 points and the a-number)**.** *If* X *is non-hyperelliptic of genus* 4 *with* a*-number* $1, 2$ *or* 3 *defined over* $\mathbb{F}_q$*, then*

(i) X *has at most* 6 *Cartier points of Type* 1 *and they are defined over* $\mathbb{F}_{q^e}$ *for some* $e \leq 6$*. Moreover,*

(ii) *if* $a = 1$*, then there is at most one Type* 1 *Cartier point*

(iii) *if* $a = 3$*, there are exactly 6 Type* 1 *Cartier points on* X*, counting with multiplicity.*

Proof. Part *(i)* follows from Proposition 2.5.10 and Corollary 2.5.11, using $2g - 2 = 6$. Now, if $a = 1$, the kernel of $H^{(1/p)}$ has dimension 1, because $a = \dim(\ker(H))$. Then the kernel spans a point in $\mathbb{P}^3$, and this is the only possible Type 1 point. When $a = 3$, on the other hand, the subspace spanned by the same kernel is a hyperplane, so its intersection with X is not empty. □

In Table 2.16 we synthesize the possible bounds on the number of Cartier points on a non-ordinary non-superspecial non-hyperelliptic genus 4 curve, depending on the a-number a and the p-rank f.

Table 2.16: Upper bounds on the number of Cartier points.

a	f	# Type 1 points $\leq$	# Type 2 points $\leq$
3	1	6	1
	0	6	0
2	2	6	4 if $p = 3$ and 6 otherwise
	1	6	1
	0	6	0
1	3	1	6
	2	1	4 if $p = 3$ and 6 otherwise
	1	1	1
	0	1	0

Computing Cartier points

We explain here an algorithm to find the Cartier points on smooth, irreducible genus 4 non-hyperelliptic curves over $\mathbb{F}_p$, given their quadratic and cubic homogeneous polynomials. Before we detail the procedure, we will revisit some facts about Cartier points. Let $X = V(F, G)$ be a curve as before.

1. Let H be the Hasse–Witt matrix of X as in Proposition 2.3.5. Recall that H represents the action of Frobenius on $H^1(X, \mathcal{O}_X)$ with respect to the basis that corresponds to the coordinates x, y, z, w. This implies that we can use H and Proposition 2.5.4 to find the Cartier points of X, by solving $H\mathbf{v}^{(p)} = c\mathbf{v}$.

2. If $P \in X(\mathbb{F}_{p^e})$ is a Cartier point, then there exists some $\lambda \in \mathbb{F}_p$ such that $H^e\mathbf{v}_P = \lambda\mathbf{v}_P$ (Lemma 2.5.9).

3. If P is a Type 1 point, then $H\mathbf{v}_P = 0$ (Corollary 2.5.7).

4. The eigenvalues of H^e are exactly the e-powers of the eigenvalues of H. If λ is as in (2), then there exists an eigenvalue μ of H such that $\lambda = \mu^e \in \mathbb{F}_p$. In other words, in order for a Cartier point to be defined over $\mathbb{F}_{p^e}$, then there must be a μ such that $\mu^e \in \mathbb{F}_p$.

5. Let $h(x)$ be the characteristic polynomial of H. The splitting field of $h(x)$ is either $\mathbb{F}_p$, $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^3}$. Indeed, $h(x)$ has degree 4, but since H has rank at most 3, then x is a factor of $h(x)$.

We use these facts to compute the Type 1 and Type 2 Cartier points of X. Algorithm 2.5.15 is restricted to the case when $q = p$, to simplify the computations.

Algorithm 2.5.14. *[Type 1 Cartier points]*

Input: F and G in $\mathbb{F}_q[x, y, z, w]$.

Output: List of Type 1 Cartier points of $X = V(F, G)$.

1. *Compute the Hasse–Witt matrix H of X, as in Proposition 2.3.5.*

2. *Let $M = H^{(1/p)}$. Construct the linear forms $L_i = (M)_{i,1}x + (M)_{i,2}y + (M)_{i,3}z + (M)_{i,4}w$, for $1 \leq i \leq 4$.*

3. *Let I be the ideal generated by $\{L_1, L_2, L_3, L_4, F, G\}$ and let $T = V(I)$.*

4. *For each $1 \leq e \leq 6$, find the points in $T_e = T(\mathbb{F}_{q^e})$.*

5. *The set of Type 1 points is $\bigcup_e (T_e)$.*

Algorithm 2.5.15. *[Type 2 Cartier points]*

Input: F and G in $\mathbb{F}_p[x, y, z, w]$.

Output: List of Type 2 Cartier points of $X = V(F, G)$.

1. *Compute the Hasse–Witt matrix H of X, as in Proposition 2.3.5.*

2. *Compute $h(x)$, the characteristic polynomial of H and find the roots of $h(x)$ in its splitting field.*

3. *For each μ non-zero root of $h(x)$:*

   (a) *For each $1 \leq e \leq 6$ such that $\mu^e \in \mathbb{F}_p$:*

      i. *Let $M = H^e - \mu^e I$, where I is the identity matrix.*

      ii. *For $1 \leq i \leq 4$, construct the linear forms $L_i = (M)_{i,1}x + (M)_{i,2}y + (M)_{i,3}z + (M)_{i,4}w$.*

      iii. *Let I be the ideal generated by $\{L_1, L_2, L_3, L_4, F, G\}$ and $T = V(I)$.*

      iv. *For each point in $T(\mathbb{F}_{p^e})$, compute $H\mathbf{v}_P^{(p)}$. If this gives a multiple of $\mathbf{v}$, then P is a Type 2 Cartier point.*

2.5.3 Cartier points on standard curves over $\mathbb{F}_p$

In this section we present the results from our search of curves in standard form, related to their a-number, p-rank and Cartier points, both of Type 1 (T1) and Type 2 (T2). Recall that we analyzed two kinds of data: on the one side our sampling search provides a random set of standard form curves over $\mathbb{F}_p$ for $p \in \{3, 5, 7, 11\}$. On the other, we obtain a complete list of all of the curves in standard form over $\mathbb{F}_3$ and $\mathbb{F}_5$ and a partial list over $\mathbb{F}_7$. See Section 2.4 for more details.

Here is how this section is organized. First, we make a couple of observations regarding the bounds for the number of Cartier points in the case where X is defined over $\mathbb{F}_p$. Then we state Corollaries 2.5.16, 2.5.17 and 2.5.18 which we obtain from the analysis of the data. We summarize the statistical results from the sampling search first and the exhaustive search later, breaking down each of them case by case by p.

The upper bound of Type 1 points: Our data reflects that, as expected, it is hard to find curves that attain the bounds on the number of Type 1 and Type 2 Cartier points. For instance when the a-number is 1, a curve can have at most 1 Type 1 point, but most curves have zero (see Table 2.19). When $a = 2$ the bound is 6, but as stated in Corollary 2.5.16, all of the curves in our sample have 3 or fewer Type 1 Cartier points.

The bound on Type 1 points is also 6 when $a = 3$, but here we see a different behavior. This is mainly because in this case, the Type 1 points come from intersecting the curve with a hyperplane, which guarantees exactly 6 points, counting with multiplicity. Even though our statistical data does not give a large sample of a-number 3 curves over $\mathbb{F}_7$ and $\mathbb{F}_{11}$, we can see in Tables 2.21 and 2.19 that most curves attain the bound, except for $p = 3$.

The bound on Type 2 points: Similarly, it seems unlikely for a curve with p-rank $f > 0$ to reach the upper bound of Type 2 points. This is true even when $f = 1$ and thus the bound is 1. We can see in Table 2.20 that the majority of curves with p-rank 1 have no such points. The same happens when $f = 2$. In this case the bound is 6, but we did not find any curve with more than 2 Type 2 points, except when $p = 5$, where there exist 2 curves with 6 Type 2 points.

It is important to recall that the bound for Type 2 points in characteristic 3 is 4, not 6, and there are in fact 16 p-rank 3 curves that reach this bound.

Corollary 2.5.16. *In our sample of smooth curves, no curve with a-number 2 reaches the bound of 6 Type 1 Cartier points. Moreover, the maximum number of Type 1 Cartier points attained for curves with a-number 2 is 3 for $p \in \{5, 7, 11\}$ and 2 for $p = 3$.*

Proof. See Table 2.19. □

Corollary 2.5.17. *The bound on the number of Type 1 points is sharp for non-hyperelliptic smooth genus 4 curves over $\mathbb{F}_p$ when*

- *$p \in \{3, 5, 7, 11\}$ and $a = 1$.*
- *$p \in \{5, 7, 11\}$ and $a = 3$.*

Proof. See Table 2.19. □

Corollary 2.5.18. *In our sample of smooth curves, no curve with p-rank 2 or 3 reaches the bound of 6 Type 2 Cartier points when $p \in \{5, 7, 11\}$.*

Proof. See Table 2.20. □

Summary of results from the sampling search

In Tables 2.17 and 2.18 we show the percentages of curves from the smooth non-ordinary samples that attain the upper bound on the number of Type 1 and Type 2 Cartier points, respectively. Recall that in Section 2.5.2 we explained how the maximum number of Type 1 points depends on the a-number of the curve and in the case of Type 2, on the p-rank. Therefore, in Table 2.17 we organized the samples by a-number on the first column, the second column refers to the upper bound and for each p we specify the percentage of curves with the given a-number that attain that maximum. The format of Table 2.17 is the same, except that we sort the curves by their p-ranks instead.

Table 2.17: Percentage of curves that attain the upper bound on T1 points.

a	Upper bound	3	5	7	11
1	1	5327 / 29298	3896 / 92792	1918 / 88481	202 / 25407
		$= 18.18\ \%$	$= 4.20\ \%$	$= 2.17\ \%$	$= 0.80\ \%$
2	6	0 / 6631	0 / 4204	0 / 1899	0 / 218
		$= 0\ \%$	$= 0\ \%$	$= 0\ \%$	$= 0\ \%$
3	6	0 / 700	24 / 46	4 / 5	1 / 1
		$= 0\ \%$	$= 52.17\ \%$	$= 80\ \%$	$= 100\ \%$

Table 2.18: Percentage of curves that attain the upper bound on T2 points.

f	Upper bound	3	5	7	11
1	1	198 / 4474	146 / 3362	35 / 1888	0 / 239
		$= 4.43\ \%$	$= 4.34\ \%$	$= 1.85\ \%$	$= 0\ \%$
2	6	0 / 7513	0 / 13385	0 / 12311	0 / 2340
	(4 if $p = 3$)	$= 0\ \%$	$= 0\ \%$	$= 0\ \%$	$= 0\ \%$
3	6	0 / 23485	0 / 51914	0 / 76142	0 / 23044
		$= 0\ \%$	$= 0\ \%$	$= 0\ \%$	$= 0\ \%$

We know by Corollary 2.5.13 that the upper bound on the number of Type 1 Cartier points is given by $2g - 2 = 6$ if $a = 2, 3$ and 1 if $a = 1$. We want to determine for which a, f and p these bounds are attained. As we can see in Table 2.17 this does not happen for any of the curves with $a = 2$ that we found. In Table 2.19, we break down the number of curves over $\mathbb{F}_p$ by the number of Type 1 points they have.

On the other hand, the upper bound on the number of Type 2 points depends on the p-rank: it is $\min\{2g - 2, \frac{p^f-1}{p-1}\}$. As stated in Corollary 2.5.16, and observed in Table 2.20, it is unlikely that a curve of p-rank 2 or 3 reaches the bound of 6 Type 2 points.

Table 2.19: Summary of Type 1 points on samples of standard form curves.

a	#T1	3	5	7	11
1	0	23971	88896	86563	25205
1	1	5327	3896	1918	202
	Total	29298	92792	88481	25407
% that attains UB		18.18 %	4.20 %	2.17 %	0.80 %
2	0	1690	3158	1595	191
2	1	3268	832	262	25
2	2	1673	149	37	1
2	3	0	65	5	1
	Total	6631	4204	1899	218
% that attains UB		0 %	0 %	0 %	0 %
3	0	0	0	0	0
3	1	660	4	0	0
3	2	40	4	0	0
3	3	0	14	0	0
3	4	0	0	1	0
3	5	0	0	0	0
3	6	0	24	4	1
	Total	700	46	5	1
% that attains UB		0 %	52.17 %	80.00 %	100 %
	Sample size	186266	719102	863038	361098

Table 2.20: Summary of Type 2 points on samples of standard form curves.

f	#T2	3	5	7	11
0	0	1157	193	44	3
1	0	4276	4272	1853	239
1	1	198	146	35	0
	Total	4474	4418	1888	239
2	0	7137	17072	12071	2320
2	1	353	737	235	20
2	2	23	35	5	0
2	3	0	2	0	0
	Total	7513	17846	12311	2340
3	0	21951	71423	74504	22837
3	1	1394	3032	1597	204
3	2	117	113	41	3
3	3	14	15	0	0
3	4	9	2	0	0
	Total	23485	74585	76142	23044
Sample size		186266	719102	863038	361098

Case $p = 3$

From the sample of 186266 curves over $\mathbb{F}_3$ a total of 35472 have a-number $1, 2$ or 3. There are only two instances in which we identified curves that realize the (non-zero) upper bound on Type 1 and Type 2 points. These are when $a = 1$, for Type 1 points, and when $f = 3$ for Type 2 points, and the bounds are 1 and 4, respectively. Even so, we can observe in Tables 2.19 and 2.20 that most curves tend to have fewer Cartier points.

Case $p = 5$

Recall that we sampled a total of 719102 tuples over $\mathbb{F}_5$ and obtained 97042 curves of a-number $1 \leq a \leq 3$. As expected, most of these curves have a-number 1. In addition, only 3896 out of the 88896 curves with $a = 1$ have a Type 1 Cartier point. This is also expected because for each curve, there is only one point P such that $H\mathbf{v}_P = 0$, so it is unlikely for this point to also be on the curve.

Case $p = 7$

We sampled a total of 863200 random tuples, obtaining 619872 curves in standard form and 90403 of them with a-numbers $1, 2$ or 3. We note that the upper bounds for the number of Type 1 points are realized when $a = 1$ and $a = 3$, but not for $a = 2$, where the maximum number of points attained is 3. With respect to the Type 2 points, the (non-zero) upper bounds are only attained when the p-rank is 1. In particular, we get the following result:

Corollary 2.5.19. *Baker's bound on the total number of Cartier points for genus* 4 *curves with* $a = 3$ *and* p*-rank* 1 *is attained over* $\mathbb{F}_7$*.*

In our data there is only one curve with a-number 3 where both the bounds of Type 1 and Type 2 points are attained, we show it in Example 2.5.20. Another illustration of this can be found later in Example 2.6.9. We also include Examples 2.5.21, 2.5.22 and 2.5.23 where the maximum number of Type 1 points is reached, and Example 2.5.24, in which we see a curve with only 4 Type 1 points. The Hasse–Witt matrix in each example is computed with the basis given in Proposition 2.3.5.

Example 2.5.20. Let $X = V(F, G)$ be a genus 4 curve over $\mathbb{F}_7$ where

$$F = 2yz + 2xw,$$
$$G = 2x^2y + y^3 + x^2z + y^2z + 3z^3 + 2yzw + z^2w + 4yw^2 + 6zw^2 + 4w^3.$$

Notice that X belongs to the N1 case from Definition 2.3.3. We will see how this curves attains Baker's bound on Cartier points. First, the Hasse–Witt matrix of X is

$$\begin{bmatrix} 2 & 3 & 6 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Thus the a-number is 3 and the p-rank 1, in which case the total bound on the number of Cartier point is 7. By solving $H\mathbf{v} = c\mathbf{v}$ we see that the Type 2 point is $[1 : 0 : 0 : 0]$.

Also, the Type 1 points are those in the intersection of X and the hyperplane $2x+3y+6z+w = 0$. There are two such points defined over $\mathbb{F}_7$, they are $[0 : 0 : 1 : 1]$ and $[2 : 4 : 3 : 1]$. The other four points are two pairs of σ-conjugate defined over $\mathbb{F}_{49}$ which are $[6 : \alpha^{26} : \alpha^{22} : 1], [6 : \alpha^{38} : \alpha^{10} : 1]$ and $[4 : \alpha^{33} : \alpha^{23} : 1], [4 : \alpha^{39} : \alpha^{17} : 1]$, for α such that $\alpha^2 + 6\alpha + 3 = 0$.

Example 2.5.21. Let $X = V(F, G)$ be a genus 4 curve over $\mathbb{F}_7$ where

$$F = 2yz + 2xw,$$
$$G = 3x^2y + y^3 + 6x^2z + 2xyz + 3y^2z + 6yz^2 + z^3 + 2y^2w + 2yzw + z^2w + 2w^3.$$

The Hasse–Witt matrix of X is

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 5 & 2 & 4 & 1 \\ 6 & 1 & 2 & 4 \\ 2 & 5 & 3 & 6 \end{bmatrix}.$$

Thus X has a-number 3 and p-rank 1. However, there are no Type 2 points because the only vector, up to scalar multiplication, that satisfies $H\mathbf{v} = c\mathbf{v}$ for some $c \in \mathbb{F}_7$ is $\mathbf{v} = (0, 1, 4, 6)^T$, but the corresponding point in $\mathbb{P}^3$ with these coordinates is not on X.

The hyperplane spanned by the kernel of H is given by $x + 6y + 5z + 3w = 0$ and the points of X that intersect it, that is, the Type 1 points, are: $[1 : \beta^{11} : \beta^{13} : 1], [1 : \beta^{29} : \beta^{43} : 1]$ where $\beta^2 + 6\beta + 3 = 0$, and

$[\alpha^{500} : \alpha^{674} : \alpha^{1026} : 1], [\alpha^{500} : \alpha^{1826} : \alpha^{2274} : 1], [\alpha^{1100} : \alpha^{782} : \alpha^{1518} : 1]$, $[\alpha^{1100} : \alpha^{2318} : \alpha^{2382} : 1]$ where $\alpha^4 + 5\alpha^2 + 4\alpha + 3 = 0$.

Example 2.5.22. Let $X = V(F, G)$ be a genus 4 curve over $\mathbb{F}_7$ where

$$\begin{aligned} F &= y^2 + 4z^2 + 2xw, \\ G &= 6x^2y + 4xy^2 + y^3 + 3x^2z + 5y^2z + 2xz^2 + 2yz^2 + 5z^3 + 2yzw + z^2w + yw^2 \\ &\quad + zw^2 + 5w^3. \end{aligned}$$

The Hasse–Witt matrix of X is

$$H = \begin{bmatrix} 6 & 5 & 2 & 4 \\ 4 & 1 & 6 & 5 \\ 2 & 4 & 3 & 6 \\ 4 & 1 & 6 & 5 \end{bmatrix}.$$

This curve has p-rank 1 and no Type 2 Cartier points, since the only vector $\mathbf{v}$, up to scaling such that $H\mathbf{v} = c\mathbf{v}$ is $(1, 3, 5, 3)^T$, and these coordinates do not correspond to a point on X.

The Type 1 points are $[1 : 6 : 1 : 1], [3 : 0 : 3 : 1], [0 : \alpha^3 : \alpha^{23} : 1], [0 : \alpha^{21} : \alpha^{17} : 1]$, $[\alpha^{17} : 1 : \alpha^{31} : 1]$ and $[\alpha^{23} : 1 : \alpha^{25} : 1]$, where $\alpha^2 + 6\alpha + 3 = 0$.

Example 2.5.23. Let $X = V(F, G)$ be a genus 4 curve over $\mathbb{F}_7$ where

$$
\begin{aligned}
F =& y^2 + 4z^2 + 2xw, \\
G =& 3x^2y + 2xy^2 + 5y^3 + 2x^2z + 4y^2z + xz^2 + 3yz^2 + 4z^3 + 4y^2w + 6yzw + z^2w + \\
& 4yw^2 + 4zw^2 + w^3.
\end{aligned}
$$

The Hasse–Witt matrix of X is

$$
H = \begin{bmatrix} 2 & 2 & 3 & 3 \\ 3 & 3 & 1 & 1 \\ 6 & 6 & 2 & 2 \\ 6 & 6 & 2 & 2 \end{bmatrix}.
$$

The p-rank of X is 1, but there are no Type 2 points, as the only solution, up to scalar multiplication, of $H\mathbf{v} = c\mathbf{v}$ is $(1, 5, 3, 3)^T$, and this does not give a point on X.

The Type 1 points are $[1 : 6 : 6 : 1], [6 : 3 : 0 : 1]$ and $[\alpha^{178} : \alpha^{1202} : \alpha^{1071} : 1]$, $[\alpha^{1054} : \alpha^{1886} : \alpha^{153} : 1], [\alpha^{1246} : \alpha^{1214} : \alpha^{297} : 1], [\alpha^{1522} : \alpha^{1298} : \alpha^{2079} : 1]$ such that $\alpha^4 + 5\alpha^2 + 4\alpha + 3 = 0$.

Example 2.5.24. Let $X = V(F, G)$ be a genus 4 curve over $\mathbb{F}_7$ where

$$
\begin{aligned}
F &= y^2 + 4z^2 + 2xw. \\
G &= 3x^2y + 4xy^2 + 3y^3 + 5y^2z + 2xz^2 + yz^2 + 5z^3 + y^2w + 6yzw + 5zw^2 + 2w^3.
\end{aligned}
$$

The Hasse–Witt matrix of X is

$$H = \begin{bmatrix} 1 & 4 & 1 & 6 \\ 5 & 6 & 5 & 2 \\ 0 & 0 & 0 & 0 \\ 1 & 4 & 1 & 6 \end{bmatrix}.$$

In this case, X has p-rank 1, but the only eigenvector of H, up to scaling is $(1, 5, 0, 1)^T$, and this does not give a point on X. On the other hand, there are four Type 1 points: $[0 : \alpha^{14} : \alpha^{34} : 1]$, $[\alpha^7 : \alpha^{36} : \alpha^{34} : 1], [0 : \alpha^2 : \alpha^{46} : 1], [\alpha : \alpha^{12} : \alpha^{46} : 1]$, where $\alpha^2 + 6\alpha + 3 = 0$. The first two have multiplicity one and the others have multiplicity 2.

Case $p = 11$

The size of the random sample in this case is of 361098 tuples. Note that, once again, the upper bound for the Type 1 points is attained for some cases where $a = 1, 3$. On the other hand, none of the curves realize the bound of Type 2 points (except, of course when $f = 0$).

One important observation is that, from all sampled tuples, only one of them resulted in a curve with a-number 3. This curve also achieves the maximum of 6 Type 1 points.

Example 2.5.25. Let $X = V(F, G)$ be a genus 4 curve over $\mathbb{F}_{11}$ where

$$\begin{aligned} F =& z^2 + 2yw, \\ G =& 9x^3 + xy^2 + 4y^3 + 9xyz + 2xz^2 + 8z^3 + 7xzw + 8xw^2 + zw^2 + 3w^3. \end{aligned}$$

The Hasse–Witt matrix of X is

$$H = \begin{bmatrix} 1 & 5 & 3 & 10 \\ 7 & 2 & 10 & 4 \\ 2 & 10 & 6 & 9 \\ 4 & 9 & 1 & 7 \end{bmatrix}.$$

This curve has a-number 3 and p-rank 1. There are no Type 2 points. Indeed, the only solution, up to scalar multiplication of $H\mathbf{v} = c\mathbf{v}$ is $\mathbf{v} = (1, 7, 2, 4)^T$, and this does not give a point over X.

The Type 1 points are those on the intersection of X and the hyperplane with equation $x+5y+3z+10w = 0$, that is $[6 : 9 : 9 : 1]$, $[7 + 2\alpha + 7\alpha^2 + 9\alpha^3 + 10\alpha^4 : 6 + 4\alpha + 5\alpha^2 + 4\alpha^3 + 1\alpha^4 : 10 + 4\alpha^2 + 5\alpha^3 + 6\alpha^4 : 1]$ with $\alpha^5 + 10\alpha^2 + 9 = 0$, and its 4 conjugates.

2.6 Cartier points on curves over $\mathbb{F}_p$ with a-number 3 from exhaustive search

In Table 2.21 we display the information of curves in standard form over $\mathbb{F}_p$ for $p \in \{3, 5, 7\}$, obtained from the exhaustive search. For $p = 3, 5$ the search was done over all the possible tuples. For $p = 7$ we found all the curves in standard form in the degenerate case and all of those in the case N1i when the coefficients of y^2z and z^2w are 0. We denote these lists by 7(D) and 7(N1i'), respectively. In the second column, we list the total number of isomorphism classes of curves with a-number 3 found for each p. The third column indicates the total number of curves that attain the maximum of 6 Type 1 Cartier points. The last two columns correspond to the number of curves that reach the maximum of Type 2 points, over the total with the respective p-rank. Notice that all curves with $f = 0$ trivially reach this bound, since the bound is 0.

Table 2.21: Isomorphism classes in standard form with a-number 3 over $\mathbb{F}_p$.

p	Classes $a=3$	Attain max. of T1 $a=3$ (6)	Attain max. of T2 $f=0$ (0)	$f=1$ (1)
3	27	0	0/0	0/27
5	134	80	36/36	5/98
7(D)	65	48	9/9	0/56
7(N1i')	29	23	2/2	1/27

By Corollary 2.5.13, genus 4 curves with a-number 3 have exactly 6 Type 1 Cartier points, but only when we count with multiplicity. In the case $p = 3$ all curves have either 1 or 2 Type 1 points maximum; for $p = 5$, the curves show $1, 2, 3$ or 6 points, and for $p = 7$ we saw evidence of curves with any number of Type 1 points ranging from 1 to 6. Furthermore, we determine which multiplicity and degree distributions occur and show this information in Tables 2.22 and 2.23, up to $\mathbb{F}_p$-isomorphism classes. An important observation is that, over $\mathbb{F}_5$, every possible degree distribution for curves with 6 (distinct) Type 1 points occurs. Also, all except one of them occur among our sample over $\mathbb{F}_7$.

Table 2.22: Multiplicities and degree distribution of T1 points.

# T1 points	Multiplicity	Degree	3	5	7(D)	7(N1i')
6	(1,1,1,1,1,1)	(1,1,1,1,1,1)	0	1	0	0
6	(1,1,1,1,1,1)	(1,1,1,1,2,2)	0	6	2	1
6	(1,1,1,1,1,1)	(1,1,1,3,3,3)	0	4	1	4
6	(1,1,1,1,1,1)	(1,1,2,2,2,2)	0	9	1	4
6	(1,1,1,1,1,1)	(1,1,4,4,4,4)	0	8	0	3
6	(1,1,1,1,1,1)	(1,2,2,3,3,3)	0	13	5	2
6	(1,1,1,1,1,1)	(1,5,5,5,5,5)	0	10	2	12
6	(1,1,1,1,1,1)	(2,2,2,2,2,2)	0	3	4	2
6	(1,1,1,1,1,1)	(2,2,4,4,4,4)	0	8	1	5
6	(1,1,1,1,1,1)	(3,3,3,3,3,3)	0	10	2	4
6	(1,1,1,1,1,1)	(6,6,6,6,6,6)	0	9	5	11
5	(2,1,1,1,1)	(1,1,1,1,1)	0	0	0	0
5	(2,1,1,1,1)	(1,2,2,2,2)	0	0	1	0
5	(2,1,1,1,1)	(1,4,4,4,4)	0	0	2	1
5	(2,1,1,1,1)	(1,1,3,3,3)	0	0	0	0
5	(2,1,1,1,1)	(1,1,1,2,2)	0	0	2	1

Table 2.23: Multiplicities and degree distribution of T1 points (continued).

# T1 points	Multiplicity	Degree	3	5	7(D)	7(N1i')
4	(2,2,1,1)	(1,1,1,1)	0	0	0	0
4	(2,2,1,1)	(2,2,1,1)	0	0	2	0
4	(2,2,1,1)	(1,1,2,2)	0	0	1	0
4	(2,2,1,1)	(2,2,2,2)	0	0	0	0
4	(3,1,1,1)	(1,1,2,2)	0	0	3	2
4	(3,1,1,1)	(1,3,3,3)	0	0	0	0
4	(3,1,1,1)	(1,1,1,1)	0	0	3	1
3	(3,2,1)	(1,1,1)	0	0	0	0
3	(2,2,2)	(1,1,1)	0	4	1	0
3	(2,2,2)	(2,2,1)	0	10	0	0
3	(2,2,2)	(3,3,3)	0	12	2	0
3	(1,1,4)	(1,1,1)	0	0	0	0
3	(1,1,4)	(2,2,1)	0	0	0	0
2	(3,3)	(1,1)	10	0	0	0
2	(3,3)	(2,2)	11	0	0	1
2	(1,5)	(1,1)	0	8	0	0
2	(2,4)	(1,1)	0	0	0	0
1	(6)	(1)	6	19	0	0

2.6.1 Exhaustive search: case $p = 3$

We will now discuss the curves in standard form over $\mathbb{F}_3$ of a-number 3. Since we have a complete list of all of the isomorphism classes of these curves, we know that all of them have p-rank 1. As an illustration, we review the family of curves from Proposition 2.4.6.

Example 2.6.1. We use Proposition 2.5.4 to compute the Cartier points on the family of curves $C = V(F, G)$ over $k = \overline{\mathbb{F}}_3$ with

$$F = 2yw + z^2,\ G = a_0x^3 + xyz + a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + zw^2,$$

where $a_i \in k$ and $a_0, a_6 \in k^\times$. Notice that here $F = F_d$, hence X belongs to the degenerate case D.

The Hasse–Witt matrix H of each curve in this family is given by

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Even though the p-rank of the curve is 1, there are no Type 2 points. Indeed, if $\mathbf{v} = (a, b, c, d)^T$ is such that $H\mathbf{v} = c\mathbf{v}$ for some $c \in k$ then $a = c = d$, but $[0 : 1 : 0 : 0]$ is not a point on C, since $a_6 \neq 0$. Now, the hyperplane generated by the kernel of the Hasse–Witt matrix is given by $L := y = 0$, which intersects C at $P = [a : 0 : 0 : 1]$ where $a = \frac{-a_8}{a_0}$, hence there is only one Type 1 point.

In Lemma 2.4.5 we specify representatives for the isomorphism classes of curves in standard form over $\mathbb{F}_3$ with a-number 3. It turns out the all the curves from the same kind have the equal multiplicity and degree distribution of Type 1 points, as a consequence we get the next lemma. We show explicitly the points in Tables 2.24, 2.25 and 2.26.

Lemma 2.6.2. *Let $X = V(F, G)$ be a curve in standard form with a-number 3 over $\mathbb{F}_3$, then X has no Type 2 Cartier point and*

- *if $F = F_d = 2yw + z^2$, then X has exactly one Type 1 point of multiplicity 6;*

- *if $F = F_1 = 2xw + 2yz$, then X has exactly two Type 1 points of multiplicity 3, each defined over $\mathbb{F}_3$;*

- *if $F = F_2 = 2xw + y^2 + z^2$, then X has exactly two Type 1 points of multiplicity 3, each defined over $\mathbb{F}_9$.*

Proof. See Tables 2.24, 2.25 and 2.26. □

The proof of Lemma 2.6.2 follows from our classification of curves in standard form into isomorphism classes and direct computation of Cartier points. Here we give an overview of the heuristics that go into this procedure, in the degenerate case. The other two cases can be worked out in a similar way.

Example 2.6.3 (Cartier points in the case D)**.** Let $X = V(F, G)$ be a curve from Table 2.24. We know that $F = 2yw + z^2yw$ and that G is of the form

$$G = x^3 + y^3 + xyz + c_1yz^2 + xw^2 + c_2w^3,$$

where $c_1 \in \mathbb{F}_3^\times$ and $c_2 \in \mathbb{F}_3$.

We will show that X has no Type 2 Cartier points and that $[2 - c_1 - c_2 : 1 : 2 : 1]$ is the unique Type 1 Cartier point, and it has multiplicity 6.

By Proposition 2.3.5, the Hasse-Witt matrix of X with respect to the basis

$$\{x^{-2}y^{-1}z^{-1}w^{-1}, x^{-1}y^{-2}z^{-1}w^{-1}, x^{-1}y^{-1}z^{-2}w^{-1}, x^{-1}y^{-1}z^{-1}w^{-2}\}$$

of $H^1(X, \mathcal{O}_X)$ is H_1 in Table 2.27. We can see right away that X has no Type 2 Cartier points, since, up to scalar multiplication, the only vector such that $H_1\mathbf{v} = c\mathbf{v}$ for some $c \in \mathbb{F}_3$ is $\mathbf{v} = (0, 1, 0, 0)^T$, but these are not the coordinates of a point on X.

Now, the hyperplane S generated by the kernel of H_1 is the zero locus of $L = y + 2z + w$. Then by substituting $y = z - w$ in $F = 0$ we get $z^2 + 2zw + w^2 = 0$. If $w = 0$, then $z = y = 0$, but $[1 : 0 : 0 : 0] \notin X$, so assume $w = 1$. Then $z = 2$ and $y = 1$ and the Type 1 points of X are of the form $P = [\alpha : 1 : 2 : 1]$. To find α we evaluate G at P and get $\alpha = 2 - c_1 - c_2$. So there is a unique (not counting multiplicity) Type 1 point.

The fact that P is the only point on the intersection of S and X implies that it must have multiplicity 6. We can indeed verify this by considering a parametrization of X at P. If t is a local parameter at P, then there exists a neighborhood of P where the points of X are of the form $P_t = [\alpha - t : 1 : \phi_1(t) : \phi_2(t)]$ for some ϕ_1 and ϕ_2 regular at 0. In particular $\phi_1(0) = 2$. Then since $F(P_t) = 0$ we get $\phi_1^2(t) = \phi_2(t)$. Similarly, since $G(P_t) = 0$ we have

$$(\alpha - t)^3 + 1 + (\alpha - t)\phi_1 + c_1\phi_1^2 + (\alpha - t)\phi_1^4 + c_2\phi_1^6 = 0. \tag{2.6.1}$$

Let $\phi_1(t) = 2 + a_1 t + a_2 t^2 + \ldots$ be the expansion of ϕ_1 at 0. Then by comparing the coefficients of both sides of Equation 2.6.1 we find that $\phi_1(t) = 2 + c_1 t^3 + \ldots$. Now consider $h = L/y$, with respect to t the function h is

$$h(t) = 1 - \phi_1(t) + \phi_2^2(t) = c_1 t^6 + \textit{ (terms of higher order)}.$$

Hence h has vanishing order of 6 at $t = 0$, from where the multiplicity of P is 6.

In Tables 2.24, 2.25 and 2.26 we show the cubic polynomial for a representative of each isomorphism class in the cases D, N1 and N2, respectively. The curves are of the form $X = V(F, G)$. We also specify the Hasse-Witt for each representative (that can be found in Table 2.27) and the Type 1 Cartier points.

Table 2.24: Isomorphism classes of D curves with $a = 3$ over $\mathbb{F}_3$.

Representative G	Hasse–Witt matrix	T1 points
$x^3 + y^3 + xyz + yz^2 + xw^2$	H_1	$[1 : 1 : 2 : 1]$
$x^3 + y^3 + xyz - yz^2 + xw^2$	H_1	$[0 : 1 : 2 : 1]$
$x^3 + y^3 + xyz + yz^2 + xw^2 + w^3$	H_1	$[0 : 1 : 2 : 1]$
$x^3 + y^3 + xyz - yz^2 + xw^2 + w^3$	H_1	$[2 : 1 : 2 : 1]$
$x^3 + y^3 + xyz + yz^2 + xw^2 - w^3$	H_1	$[2 : 1 : 2 : 1]$
$x^3 + y^3 + xyz - yz^2 + xw^2 - w^3$	H_1	$[1 : 1 : 2 : 1]$

Table 2.25: Isomorphism classes of N1 curves with $a = 3$ over $\mathbb{F}_3$.

Representative G	Hasse–Witt matrix	T1 points
$x^2y + y^3 + x^2z + y^2w + z^2w - w^3$	H_2	$[1 : 2 : 1 : 1], [0 : 0 : 2 : 1]$
$x^2y + y^3 + x^2z - y^2w + z^2w - w^3$	H_3	$[0 : 2 : 0 : 1], [0 : 0 : 1 : 1]$
$x^2y + y^3 + x^2z + z^3 + y^2w + z^2w + w^3$	H_2	$[1 : 2 : 1 : 1], [1 : 1 : 2 : 1]$
$x^2y + y^3 + x^2z + z^3 - y^2w + z^2w + w^3$	H_3	$[0 : 0 : 1 : 1], [2 : 2 : 2 : 1]$
$x^2y + y^3 + x^2z - z^3 + y^2w + z^2w + w^3$	H_2	$[0 : 0 : 2 : 1], [1 : 0 : 1 : 0]$
$x^2y + y^3 + x^2z - z^3 + y^2w + z^2w - w^3$	H_2	$[1 : 1 : 2 : 1], [1 : 0 : 1 : 0]$
$x^2y + y^3 + x^2z - z^3 - y^2w + z^2w + w^3$	H_3	$[2 : 1 : 1 : 1], [1 : 0 : 1 : 0]$
$x^2y + x^2z + y^2w + z^2w + w^3$	H_2	$[1 : 2 : 1 : 1], [1 : 1 : 2 : 1]$
$x^2y + x^2z + y^2w + z^2w - w^3$	H_2	$[0 : 2 : 0 : 1], [0 : 0 : 2 : 1]$
$x^2y + x^2z - y^2w + z^2w + w^3$	H_3	$[0 : 2 : 0 : 1], [2 : 1 : 1 : 1]$

Table 2.26: Isomorphism classes of N2 curves with $a = 3$ over $\mathbb{F}_3$, with $\beta^2 + 2\beta + 2 = 0$.

Representative G	HW matrix	T1 points
$x^2y + y^3 + x^2z - z^3 - yzw - w^3$	H_4	$[\beta^5 : 1 : \beta^3 : 1], [\beta^7 : 1 : \beta : 1]$
$x^2y + x^2z - yzw - w^3$	H_4	$[0 : \beta^5 : \beta^7 : 1], [0 : \beta^7 : \beta^5 : 1]$
$x^2y + y^3 + x^2z - z^3 - yzw + w^3$	H_4	$[\beta^2 : 0 : \beta : 1], [\beta^6 : 0 : \beta^3 : 1]$
$x^2y + x^2z - z^3 - yzw + w^3$	H_4	$[\beta^2 : 0 : \beta : 1], [\beta^6 : 0 : \beta^3 : 1]$
$x^2y + y^3 + x^2z + z^3 - yzw + w^3$	H_4	$[1 : \beta^2 : \beta^6 : 1], [1 : \beta^6 : \beta^2 : 1]$
$x^2y - y^3 + x^2z - z^3 - yzw - w^3$	H_4	$[\beta^7 : \beta^2 : 1 : 0], [\beta^5 : \beta^6 : 1 : 0]$
$x^2y + x^2z + z^3 - y^2w - yzw + z^2w + w^3$	H_5	$[2 : 0 : \beta^2 : 1], [2 : 0 : \beta^6 : 1]$
$x^2y - y^3 + x^2z - y^2w - yzw + z^2w - w^3$	H_5	$[\beta^7 : \beta^5 : 1 : 1], [\beta^5 : \beta^7 : 1 : 1]$
$x^2y - x^2z - y^2w + yzw + z^2w + w^3$	H_5	$[\beta^2 : \beta^3 : \beta^7 : 1], [\beta^6 : \beta : \beta^5 : 1]$
$x^2y + x^2z - z^3 - y^2w - yzw + z^2w + w^3$	H_5	$[\beta^2 : \beta^3 : \beta^7 : 1], [\beta^6 : \beta : \beta^5 : 1]$
$x^2y - x^2z - z^3 - y^2w + yzw + z^2w - w^3$	H_5	$[0 : 2 : \beta^2 : 1], [0 : 2 : \beta^6 : 1]$

We compute the Hasse-Witt matrices for the representatives of the isomorphism classes using Proposition 2.3.5, with respect to the ordered basis of $H^1(X, \mathcal{O}_X)$

$$\{x^{-2}y^{-1}z^{-1}w^{-1}, x^{-1}y^{-2}z^{-1}w^{-1}, x^{-1}y^{-1}z^{-2}w^{-1}, x^{-1}y^{-1}z^{-1}w^{-2}\}.$$

Table 2.27: Hasse–Witt matrix for representatives over $\mathbb{F}_3$.

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad H_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 2 & 2 & 2 \end{bmatrix} \quad H_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 1 \end{bmatrix} \quad H_5 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 2 \end{bmatrix}$$

2.6.2 Exhaustive search: case $p = 5$

We found the set of Cartier points on all curves in standard form over $\mathbb{F}_5$ with a-number 3. There are some behaviors that are different from the case $p = 3$. For instance, there are isomorphism classes of curves that attain the bound on the number of Cartier points, both with $f = 1$ and $f = 0$. It also happens that some of them have Type 2 Cartier points (see Table 2.28 and Proposition 2.6.5). Another feature is that every degree distribution occurs when there are 6 distinct Type 1 points, as shown in Table 2.29.

Table 2.28: Number of Type 1 and 2 Cartier points over $\mathbb{F}_5$.

Case	Curves with n Type 1 points						Curves with Type 2
	1	2	3	4	5	6	1
D	14	0	26	0	0	19	0
N1i	3	7	0	0	0	50	4
N1ii	0	1	0	0	0	5	1
N2	2	1	0	0	0	6	0
Total	19	9	26	0	0	80	5

Table 2.29: Occurrence of field of definition Type 1 points over $\mathbb{F}_5$.

# T1 points	Multiplicity	Degree	D	N1i	N1ii	N2
6	(1,1,1,1,1,1)	(1,1,1,1,1,1)	0	1	0	0
6	(1,1,1,1,1,1)	(1,1,1,1,2,2)	2	3	1	0
6	(1,1,1,1,1,1)	(1,1,1,3,3,3)	1	3	0	0
6	(1,1,1,1,1,1)	(1,1,2,2,2,2)	1	8	0	0
6	(1,1,1,1,1,1)	(1,1,4,4,4,4)	0	1	1	0
6	(1,1,1,1,1,1)	(1,2,2,3,3,3)	5	6	1	1
6	(1,1,1,1,1,1)	(1,5,5,5,5,5)	0	9	0	1
6	(1,1,1,1,1,1)	(2,2,2,2,2,2)	1	1	0	1
6	(1,1,1,1,1,1)	(2,2,4,4,4,4)	4	2	0	2
6	(1,1,1,1,1,1)	(3,3,3,3,3,3)	2	5	2	0
6	(1,1,1,1,1,1)	(6,6,6,6,6,6)	0	0	0	0
3	(2,2,2)	(1,1,1)	4	0	0	0
3	(2,2,2)	(2,2,1)	10	0	0	0
3	(2,2,2)	(3,3,3)	12	0	0	0
2	(1,5)	(1,1)	0	7	0	1
1	(6)	(1)	14	3	0	0

Example 2.6.4. There are only 5 isomorphism classes of curves in standard form with a-number 3 over $\mathbb{F}_5$ that have a Type 2 Cartier point. Here we show the cubic polynomial of each curve, together with the Type 2 point. All of these curves have only 1 Type 1 Cartier point, which implies there are no p-rank 1 curves over $\mathbb{F}_5$ that reach the bound of 7 total Cartier points.

- $x^2y + y^3 + x^2z + 2xyz + 2yz^2 + z^3 + 2y^2w + 2yzw + yw^2 + w^3$, $[1 : 0 : 3 : 0]$.

- $2x^2y + y^3 + x^2z + xyz - yz^2 - z^3 + 2yzw - 2yw^2 + zw^2 - w^3$, $[0 : 0 : 1 : 2]$.
- $2x^2y+y^3+2x^2z+xyz+y^2z-2yz^2-2z^3+2y^2w-yzw+yw^2-2zw^2-2w^3$, $[1 : 3 : 2 : 4]$.
- $x^2y + y^3 - 2x^2z + y^2z - yz^2 - y^2w - yzw + z^2w - yw^2 - 2zw^2 - 2w^3$, $[1 : 2 : 0 : 0]$.
- $x^2y + 2x^2z - 2xyz + y^2z + yz^2 - 2y^2w + 2yzw + z^2w + yw^2 - 2zw^2 - 2w^3$, $[1 : 4 : 1 : 1]$.

Proposition 2.6.5. *There are no curves in standard form over $\mathbb{F}_5$ with p-rank 1 and a-number 3 that reach Baker's bound of 7 Cartier points.*

There are, up to $\mathbb{F}_5$-isomorphism, 17 curves in standard form with p-rank 0 and a-number 1 that reach the bound of 6 Type 1 Cartier points.

Proof. If a genus 4 curve with $a = 3$ has p-rank 0 then by Proposition 2.5.10, it has at most 6 Cartier points. If the p-rank is 1, then the curve has at most 7 Cartier points: 6 of Type 1 and 1 of Type 2. We use Algorithms 2.5.14 and 2.5.15 to compute the Cartier points on all N1, N2 and D curves with $a = 3$ over $\mathbb{F}_5$ and find that only 17 curves with p-rank 0 have a total of 6 Cartier points. Example 2.6.4 shows that the only curves with Type 2 Cartier points have fewer than 6 Type 1 points, hence the total of Cartier points is less than the upper bound for all the p-rank 1 curves. □

We know give examples of families of curves and their Cartier points.

Example 2.6.6. Let C be the genus 4 curve over $k = \mathbb{F}_5$ embedded in $\mathbb{P}^3$ as the zero locus of

$$F = 2yw + z^2 \text{ and} \tag{2.6.2}$$

$$G = \alpha x^3 + xyz + \beta y^3 + zw^2, \tag{2.6.3}$$

with $\alpha, \beta \in k^\times$. The computation of the Hasse–Witt matrix by Proposition 2.3.5 gives

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{2.6.4}$$

So C has a-number 3 and p-rank 1. The vectors such that $H\mathbf{v}^{(p)} = c\mathbf{v}$ for some $c \in k^\times$ are the scalar multiples of $(0,1,0,0)^T$, but $[0:1:0:0]$ is not a point on C. On the other hand, if $H\mathbf{v}^{(p)} = 0$ then $\mathbf{v}$ must be a scalar multiple of $(0,0,0,1)^T$, hence the only Cartier point is $[0:0:0:1]$ and it is of Type 1.

Example 2.6.7. Let X be the genus 4 curve over $\mathbb{F}_5$ embedded in $\mathbb{P}^3$ as the zero locus of

$$F = 2yw + z^2,\ G = ax^3 + xw^2 + by^3 + cw^3 + zw^2, \tag{2.6.5}$$

with $a, b \in \mathbb{F}_5^\times$ and $c \in \mathbb{F}_5$. By Proposition 2.3.5 the Hasse-Witt matrix of X is

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 3ab^2 & 4ab & 4a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{2.6.6}$$

If $H\mathbf{v} = c\mathbf{v}$ for some $c \neq 0$, then $\mathbf{v}$ must be in the subspace spanned by $(0,1,0,0)^T$. But $[0:1:0:0]$ is not a point on X. Therefore, X has no Type 2 point.

Now, suppose $P = [x_0, y_0, z_0, w_0]$ is a Type 1 Cartier point of X, and let $\mathbf{v} = \mathbf{v}_P$. Since P is also on the hyperplane generated by the kernel of H, then $3b^2y_0 + 4bz_0 + 4w_0 = 0$, from where $w_0 = 3b^2y_0 + 4bz_0$. By evaluating F at P we see that

$$b^2y^2 + 3byz + z^2 = 0,$$

hence $z_0 = 2by_0$. Note that $y_0 \neq 0$, because otherwise $P = [1 : 0 : 0 : 0]$, and this is not a point on X. So we can assume that $y_0 = 1$, and then $P = [x_0 : 1 : 2b : b^2]$. Evaluating P at G we get that

$$ax_0^3 + x_0 + 3b + cb = 0.$$

Therefore, X has $1, 2$ or 3 Type 1 Cartier points (counting without multiplicity), one for each of the roots of $ax^3 + x + 3b + cb$, that can be defined over $\mathbb{F}_5$, $\mathbb{F}_{5^2}$ or $\mathbb{F}_{5^3}$.

Example 2.6.8. Let X be the genus 4 curve over $\mathbb{F}_5$ embedded in $\mathbb{P}^3$ as the zero locus of

$$F = 2yw + z^2,\ G = 3a^2x^3 + xw^2 + bxyz + b^2ay^3 + aw^3 + zw^2, \tag{2.6.7}$$

with $a, b \in \mathbb{F}_5^\times$. The curve X is smooth and irreducible if $a \neq b$. By Proposition 2.3.5 the Hasse-Witt matrix of X is

$$H = \begin{bmatrix} 0 & 0 & 4ab^3 & 4b \\ 0 & 0 & 2a^3b^2 & 2a^2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 4b^3 & 4a^3b \end{bmatrix}. \tag{2.6.8}$$

So X has a-number and p-rank 1. There are no points on X such that the corresponding vector $\mathbf{v}$ is a solution to $H\mathbf{v}^{(5)} = c\mathbf{v}$ for c in $\mathbb{F}_5^\times$.

Now, suppose that $P = [x_0, y_0, z_0, w_0]$ is a Type 1 point. Then P is in the hyperplane given by $ab^2z + w = 0$, hence $w_0 = 4ab^2z$. If $z_0 = 0$, then $w_0 = 0$ and since $G(P) = 0$, we have $3a^2x_0^3 + ab^2y_0^3 = 0$. Clearly x_0 and y_0 cannot be zero, so let $y_0 = 1$ and then $P = [x_0 : 1 : 0 : 0]$ for x_0 a root of $3ax^3 + b^2 = 0$. This gives a Type 1 point over $\mathbb{F}_5$ and two over $\mathbb{F}_{25}$.

On the other hand, if we assume $z_0 = 1$ then $w_0 = 4ab^2$ and by substituting P in $F = 0$ we obtain $y_0 = 3a^3b^2$. Therefore $P = [x_0 : 3a^3b^2 : 1 : 4ab^2]$, with x_0 a root of

$3a^2x^3 + x(a^2 + 3a^3b^3) + 3a^2 + 4b^2$. For all possible (a, b), this polynomial has three distinct roots, either over $\mathbb{F}_5$, $\mathbb{F}_{25}$ or $\mathbb{F}_{125}$.

2.6.3 Exhaustive search: case $p = 7$

As mentioned in Section 2.4.2, for $p = 7$ we also computed all the a-number 3 curves of type D and of type N1i with $(b_1, b_2) = (0, 0)$. Table 2.30 shows the number of Cartier points on these curves.

Table 2.30: Number of Cartier points on known D and N1 genus 4 curves over $\mathbb{F}_7$.

Case	#Curves with n Type 1 points						#Curves with Type 2
	1	2	3	4	5	6	1
D	0	0	3	9	5	48	0
N1i'	0	1	0	3	2	23	1
Total	0	1	3	12	7	71	1

Table 2.31: Occurrence of field of definition Type 1 points over $\mathbb{F}_7$.

# T1 points	Multiplicity	Degree	7(D)	7(N1i')
6	(1,1,1,1,1,1)	(1,1,1,1,2,2)	2	1
6	(1,1,1,1,1,1)	(1,1,1,3,3,3)	1	4
6	(1,1,1,1,1,1)	(1,1,2,2,2,2)	1	4
6	(1,1,1,1,1,1)	(1,1,4,4,4,4)	0	3
6	(1,1,1,1,1,1)	(1,2,2,3,3,3)	5	2
6	(1,1,1,1,1,1)	(1,5,5,5,5,5)	2	12
6	(1,1,1,1,1,1)	(2,2,2,2,2,2)	4	2
6	(1,1,1,1,1,1)	(2,2,4,4,4,4)	1	5
6	(1,1,1,1,1,1)	(3,3,3,3,3,3)	2	4
6	(1,1,1,1,1,1)	(6,6,6,6,6,6)	5	11
5	(2,1,1,1,1)	(1,2,2,2,2)	1	0
5	(2,1,1,1,1)	(1,4,4,4,4)	2	1
5	(2,1,1,1,1)	(1,1,1,2,2)	2	1
4	(2,2,1,1)	(2,2,1,1)	2	0
4	(2,2,1,1)	(1,1,2,2)	1	0
4	(3,1,1,1)	(1,1,2,2)	3	2
4	(3,1,1,1)	(1,1,1,1)	3	1
3	(2,2,2)	(1,1,1)	1	0
3	(2,2,2)	(3,3,3)	2	0
2	(3,3)	(1,1)	0	0
2	(3,3)	(2,2)	0	1

In Section 2.4.2 we saw, through our random sample search, that the bound of Cartier points is attained for curves with a-number 3 over $\mathbb{F}_7$, as stated in Corollary 2.5.19. This was also reflected in our exhaustive search, with a curve over in the case N1i, shown in Example 2.6.9.

Example 2.6.9. Consider the curve $X = V(F, G)$ with

$$F = 2yz + 2xw,$$
$$G = 3x^2y + y^3 + 2x^2z - yz^2 + 2z^3 + y^2w + 3yzw - 3yw^2 - 3zw^2 + w^3.$$

The Hasse–Witt matrix of X is

$$\begin{bmatrix} 2 & 5 & 2 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The Type 1 Cartier points then are the points of intersection of X and the hyperplane

$$S : 2x + 5y + 2z + 6w = 0,$$

which are $[0 : 3 : 0 : 1]$, $[5 : 2 : 1 : 1]$, $[1 : 3b{+}2 : 3b + 5 : 1]$, $[1 : 4b{+}2 : 4b + 5 : 1]$, $[3 : 2b + 3 : 2b + 4 : 1]$ and $[3 : 5b + 3 : 5b + 4 : 1]$, where b is a primitive element of $\mathbb{F}_{49}$ such that $b^2 + 2 = 0$. Also, $[1 : 0 : 0 : 0]$ is the Type 2 Cartier point.

Chapter 3

Endomorphism rings of supersingular elliptic curves and ℓ-isogeny graphs

This chapter is based on the paper "Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms" [3], written in collaboration with Efrat Bank, Kirsten Eisenträger, Travis Morrison and Jennifer Park that started as part of the Women in Numbers 4 workshop (WIN4) held at Banff, Alberta, Canada in August 2017. The paper is to be published as part of the WIN4 conference proceedings. Motivated by the renewed interest on the potential use of supersingular elliptic curves based cryptosystems, Eisenträger and Park proposed a project to study the properties of the ℓ-isogeny graph of the supersingular elliptic curves over fields of positive characteristic. The main goal is to learn more about the hardness of the problem of computing the endomorphism ring of such curves.

3.1 Introduction

Ordinary elliptic curves and their group law constitute the basis for Elliptic Curve Cryptography (ECC), where one uses a subgroup of order n generated by an element Q, the private key is a number $d \in \{1, \dots, n-1\}$ and the public key is a point P such that $P = dQ$. Finding d is consider a “hard problem" (meaning there is no polynomial time algorithm to solve it) called the Discrete Logarithm Problem. However, ECC, as well as RSA, is known to be vulnerable under attacks with quantum computers, which is why there has been an interest in transitioning to new systems. In 2017, the National Institute of Standards and Technology (NIST) initiated the project Post-Quantum Cryptography Standardization, where proposals of cryptosystems are reviewed in order to determined their effectiveness in a post-quantum scenario. In January 2019 the Round 2

candidates were announced, with a supersingular elliptic curve based system as one of them. As the NIST report states: "*The basic security problem upon which SIKE relies, finding isogenies between supersingular elliptic curves, has not been studied as much as some of the security problems associated with other submissions.*" [1], p. 14).

The problem of finding isogenies between supersingular elliptic curves is equivalent to computing the endomorphism ring of a supersingular elliptic curve. Here, we study the hardness of this last problem by following a strategy first explored by Kohel in [11]: the ℓ-isogeny graph.

Let p and ℓ be distinct primes. In the ℓ-isogeny graph, every vertex corresponds to an $\overline{\mathbb{F}}_p$- isomorphism class of supersingular elliptic curves over $\mathbb{F}_{p^2}$ and each vertex is an ℓ-isogeny between such curves. This implies that every cycle at a vertex j can be seen as an element of the endomorphism ring of an elliptic curve E with j-invariant j. The idea is to find cycles that can generate $\mathrm{End}(E)$, which happens to be isomorphic to a maximal order in a quaternion algebra.

In Section 3.2 we cover the necessary background on supersingular elliptic curves, quaternion algebras and ℓ-isogeny graphs, along with some important results. In Section 3.3 we present a few questions that arise from the approach taken and the results obtained as partial answers to these questions: a condition for two cycles to be linearly independent and an obstruction to generate $\mathrm{End}(E)$. Finally in Section 3.4 we include examples for $p = 31, 101, 103$ where the results are applied.

3.2 Supersingular Elliptic curves

Let k be any field of characteristic different from 2 and 3, and let E an **elliptic curve** defined over k, that is, a non-singular curve of genus 1. We consider E as given by a short Weierstrass equation

$$y^2 = x^3 + a_1 x + a_2, \tag{3.2.1}$$

for some $a_1, a_2 \in k$, the base point at infinity is $O = [0 : 1 : 0]$. The $\overline{k}$-isomorphism classes of elliptic curves are classified by their j-invariant, which can be computed from (3.2.1) as $j = \frac{2^8 3^3 a_1}{2^2 a_1^3 + 3^3 a_2^2}$.

Elliptic curves have the structure of an abelian group. In particular, we can consider the isogeny from E to itself given by

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto mP, \end{aligned}$$

for some integer m, defined as the *multiplication by m map*. The kernel of this map is exactly the m-torsion subgroup of E, that is $E[m] := \{P \in E : mP = O\}$.

Suppose now that k has characteristic $p > 0$. Let $E[p](\overline{k})$ be the group of p-torsion points of E over $\overline{k}$. Then there are two possibilities: either $E[p](\overline{k}) = 0$ or $E[p](\overline{k}) = \mathbb{Z}/p\mathbb{Z}$ (Silverman [28]).

Definition 3.2.1. If E is an elliptic curve over a filed of characteristic $p > 0$, such that $E[p](\overline{k}) = 0$, then E is *supersingular*. Otherwise, E is *ordinary*.

Another characterization of supersingular elliptic curves comes from the structure of its endomorphism ring. In particular, End(E) is isomorphic to either:

- $\mathbb{Z}$,
- an order in an imaginary quadratic field, or
- or an order in a quaternion algebra.

When char$(k) = p > 0$, the first case does not happen, and E is supersingular exactly when End(E) is an order in a quaternion algebra. We will discuss more in Section 3.2.1.

In addition, all supersingular elliptic curves over k have a model that is defined over $\mathbb{F}_{p^2}$, and consequently their j-invariant is also in $\mathbb{F}_p^2$. Our new "hard problem" is going to be to compute

the endomorphism ring of a supersingular elliptic curve. The next result, due to Deuring, gives an important starting point to a solution:

Theorem 3.2.2. *[Deuring, 1941] Let $B_{p,\infty}$ be the unique, up to isomorphism, quaternion algebra over $\mathbb{Q}$ ramified exactly at p and infinity. Let E be a a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Then $End(E) \otimes \mathbb{Q} = B_{p,\infty}$ and $End(E)$ is a maximal order in $B_{p,\infty}$.*

Proof. See Voight [32], p. 733. □

In order to understand this result, we will review some basis theory of quaternion algebras.

3.2.1 Quaternion algebras

Let F be a field with char$(F) \neq 2$.

Definition 3.2.3. An F-algebra B is a quaternion algebra if there is a basis $1, i, j, k$ for B as an F-vector space such that

$$i^2 = a,\ j^2 = b,\ \text{and } k = ij = -ji. \tag{3.2.2}$$

for some $a, b \in F^\times$. We denote B by $\left(\frac{a,b}{F}\right)$.

The quaternion algebra B is generated by the elements i, j and has dimension 4 as an F-vector space. Since char$(F) \neq 2$ then B is also a central simple F-algebra. A typical example of a quaternion algebra is one formed by the 2×2 matrices over F, that we detail in Example 3.2.4.

Example 3.2.4. [Split matrix algebra] The set $M_2(F)$ of 2×2 matrices with coefficients in F is a quaternion algebra over F. Indeed $M_2(F) \simeq \left(\frac{-1,1}{F}\right)$, where the isomorphism is given by taking

$$i \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ j \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It turns out that every quaternion algebra over F is isomorphic to a matrix algebra over some extension of F. For instance in Proposition 3.2.5 we see what happens when $K = F(\sqrt{(a)})$.

Proposition 3.2.5. *Let $a, b \in F^\times$ and $K = F(\sqrt{a})$. Then*

a. if K/F is quadratic and $\alpha \mapsto \overline{\alpha}$ is the nontrivial element of Gal(K/F), there is an F-algebra isomorphism

$$\left(\frac{a,b}{F}\right) \simeq \left\{ \begin{pmatrix} \alpha & b\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in K \right\} \subset M_2(K), \text{ and}$$

b. if $K = F$ then

$$\left(\frac{a,b}{F}\right) \simeq M_2(F).$$

A direct consequence of Proposition 3.2.5 is that if $a \in (F^\times)^2$, then $\left(\frac{a,b}{F}\right) \simeq M_2(F)$. Also, if F is algebraically closed, then clearly every quaternion algebra is isomorphic to $M_2(F)$. If B is a quaternion algebra isomorphic to $M_2(F)$ we said that it is **split**. If B is not split, then it is a division algebra.

Following Theorem 3.2.2, we will be interested in quaternion algebras over $\mathbb{Q}$, specially definite quaternion algebras.

Definition 3.2.6. A **definite quaternion algebra over** $\mathbb{Q}$ is an algebra of the form

$$K = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

whose multiplication satisfies $i^2, j^2 \in \mathbb{Q}$, $i^2 < 0$, $j^2 < 0$ and $ij = -ji$.

Since $\mathbb{Q}$ is not algebraically closed it makes sense to ask: when is a (definite) quaternion algebra B over $\mathbb{Q}$ split? Moreover, for any prime p one can define the $\mathbb{Q}_p$-algebra $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$. In the same way, since ∞ is the place given by the usual absolute value and $\mathbb{R}$ is the corresponding completion of $\mathbb{Q}$ then $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R}$ is an $\mathbb{R}$-algebra.

Definition 3.2.7. A quaternion algebra B over $\mathbb{Q}$ splits at p (resp. ∞) if B_p (resp. ∞) is **split**. Otherwise, B is **ramified** at p (resp. ∞).

The quaternion algebras over $\mathbb{Q}$ are classified, up to isomorphism, by the places where they are ramified, which always form sets of even cardinality (Voight [32], p.192). So for every prime p there is a unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ that is ramified at p and ∞, and there is an explicit representation in each case we get the next result.

Theorem 3.2.8. *Let p be a prime. Then the unique quaternion algebra over $\mathbb{Q}$ ramified at p and ∞ is given by:*

(i) $B_{p,\infty} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ *if* $p = 2$*;*

(ii) $B_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 3 \mod 4$*;*

(iii) $B_{p,\infty} = \left(\frac{-2,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 5 \mod 8$ *and*

(iv) $B_{p,\infty} = \left(\frac{-p,-q}{\mathbb{Q}}\right)$ *if* $p \equiv 1 \mod 8$,

where q is a prime with $q \equiv 3 \mod 4$ and $\left(\frac{q}{p}\right) = -1$.

Proof. See Pizer [20], p. 368. □

Definition 3.2.9. Let B be a $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An order $\mathcal{O}$ of B is a subring of B that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{O} \otimes \mathbb{Q} = B$.

Let $\mathcal{O}$ be an order of a quaternion algebra B. Then there exist $\alpha, \beta \in B$ such that

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\alpha\beta.$$

Whenever it is clear from context, we denote $\mathcal{O}$ as $< 1, \alpha, \beta, \alpha\beta >$. Going back to the problem of finding End(E) and using Theorem 3.2.2, now our task is: given E over $\mathbb{F}_{p^2}$, find the elements of $B_{p,\infty}$ that generate $\mathcal{O} \cong$ End(E).

Theorem 3.2.2 gives a correspondence between maximal orders of $B_{p,\infty}$ and supersingular elliptic curves over $\mathbb{F}_{p^2}$. If $\mathcal{O}$ is a maximal order in $B_{p,\infty}$, there exist (up to isomorphism) one or

two supersingular elliptic curves such that the endomorphism ring is isomorphic to $\mathcal{O}$. There are two such curves if and only if the j-invariant is in $\mathbb{F}_{p^2} - \mathbb{F}_p$, in which case $\mathcal{O} \cong \text{End}(j) \cong \text{End}(\overline{j})$.

Our approach is to use the ℓ-isogeny graph for p, which was first explored by Kohel in [11], to find generators of $\mathcal{O}$. An isogeny is called an ℓ-isogeny if it has degree ℓ. Intuitively, this means that it is an ℓ-to-1 map.

3.2.2 The ℓ-isogeny graph

Let ℓ be a prime, such that $p \neq \ell$.

Definition 3.2.10. The ℓ-isogeny graph is constructed as follows.

- Vertices: set of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$, labeled by their j-invariants.
- Edges: ℓ-isogenies between such curves, constructed in this way: pick some j-invariant j and E such that $j(E) = j$. Each ℓ isogeny from E is determined by its kernel, so let H be a subgroup of E of order ℓ, then the isogeny $a : E \to E/H \cong E'$ corresponds to an edge from j to j', where $j' = j(E')$. It is important to remark that two ℓ-isogenies could have the same kernel: indeed, if we consider $u \in \text{Aut}(E')$, then the kernel of $a' = u \circ a$ is also H, but the two isogenies might be different. In the construction of $G(p, \ell)$ we make an arbitrary choice of ℓ-isogeny for each cyclic subgroup of $E[\ell]$ to represent each edge.

In practice we usually choose an elliptic curve for each j invariant. We denote by $E(j)$ the elliptic curve with j-invariant j and affine model $y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728}$, if $j \neq 0, 1728$. We set the affine models $y^2 = x^3 + 1$ and $y^2 = x^3 + x$ for $E(0)$ and $E(1728)$, respectively.

Let $G(p, \ell)$ be the ℓ-isogeny graph. Since $E[\ell]$, the ℓ-torsion subgroup of E, is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, there are $\ell + 1$ subgroups of E of order ℓ and hence $\ell + 1$ directed edges from each j. This implies that $G(p, \ell)$ is a $(\ell+1)$-regular, directed multigraph. Kohel [11] proved that $G(p, \ell)$ is connected in the supersingular case.

Lemma 3.2.11. Let $G = G(p, \ell)$ as in Definition 3.2.10, then

1. G is connected,
2. G is $(\ell + 1)$-regular and
3. $\#V = \left\lfloor \frac{p}{12} \right\rfloor + \varepsilon_p$, where

$$\varepsilon_p = \begin{cases} 0, & p \equiv 1 \mod 12 \\ 1, & p = 3 \\ 1, & p \equiv 5, 7 \mod 12 \\ 2, & p \equiv 11 \mod 12 \end{cases}$$

The number ε_p distinguishes the cases where 0 or 1728 are supersingular j-invariants: the first one occurs when $p \equiv 2 \mod 3$ and the later one when $p \equiv 3 \mod 4$. The $(\ell + 1)$ regularity of $G(p, \ell)$ has an exception at the vertices $E(0)$ and $E(1728)$ and their neighbors, due to the extra automorphisms. Two other important features of the graph are:

- Each cycle from $E(j)$ corresponds to an endomorphism of E, since it is a composition of ℓ-isogenies.
- The dual isogenies: let a be an edge from $E(j)$ to $E(j')$ and α its corresponding ℓ-isogeny. We say that the edge $\hat{a}$ from $E(j')$ to $E(j)$ is the dual of a if it corresponds to an isogeny of the form $u\hat{\alpha}$ for $u \in \text{Aut}(E(j))$.

In this way, it makes sense to look for elements of $B_{p,\infty}$ corresponding to cycles on the graph, starting at a fixed j.

3.2.3 Norm and Trace

Let ϕ be an element of $\text{End}(E)$. There exist unique t and n such that

$$\phi^2 - t\phi + [n] = 0. \tag{3.2.3}$$

We define t to be the *trace* of ϕ and n is the *norm* of ϕ and

$$x^2 - tx + n = 0 \tag{3.2.4}$$

is the *minimal polynomial* of ϕ, except when $\phi = [m]$, for some $m \in \mathbb{Z}$. In that case the minimal polynomial is $x^2 - m$ and the trace is 0. In order to identify a cycle of $G(p, \ell)$ with some ϕ, we need to find its norm and trace. The first one is easy to compute, due to the following lemma given by Deuring correspondence:

Lemma 3.2.12. *Let L be a cycle beginning and ending at a vertex j. Then the (reduced) norm of L interpreted as an element of $End(E(j))$ is ℓ^m, where m is the length of L.*

The trace, on the other hand, is more difficult to find, but there are some cases where the answer comes directly from the geometry of the graph. For example, if $E(j)$ has a unique self loop ϕ, then it must correspond to its own dual, so

$$\phi^2 = \phi \circ \hat{\phi} = [\ell],$$

and the trace of ϕ is 0.

An algorithm to compute the trace of an endomorphism.

As mentioned above, the task of computing the trace of an endomorphism is somewhat complicated. However, following the ideas in [11] and [26] we can deduce the existence of an algorithm that gives results in polynomial time:

Proposition 3.2.13. *Let L be a cycle beginning and ending at a vertex v corresponding to an elliptic curve E_v. Then the (reduced) trace of L interpreted as an element of End(E_v) can be computed in polynomial time.*

Here is an idea of the proof of Proposition 3.2.13. The complete proof can be found in the Appendix of [3].

Schoof [26] proofs the existence of an algorithm that computes in polynomial time the number of points in an elliptic curve over a finite field, given by a Weierstrass equation (where the characteristic of the field is not 2 nor 3). To do this, the author uses the facts that, if E is an elliptic curve over $\mathbb{F}_q$ and T is the trace of Frobenius ϕ_F then

$$E(\mathbb{F}_q) = q + 1 - T, \tag{3.2.5}$$

the minimal polynomial for Frobenius is

$$x^2 - Tx + q, \tag{3.2.6}$$

and by the Riemann hypothesis for elliptic curves, T is bounded by $2\sqrt{q}$.

The idea is that, if l is relatively prime to q then the relation

$$(\phi_l^2 - T\phi_l + q)P = 0, \tag{3.2.7}$$

where ϕ_l is the reduction mod l of ϕ_F, holds for all points $P \in E[l]$. Hence we check, for sufficiently many prime l's such that the product of all of them is larger than $4\sqrt{q}$, which values of T' satisfy the relation $(\phi_l^2 - T'\phi_l + q)P = 0$ for all $P \in E[l]$. Then T can be determined by the Chinese Reminder Theorem. In practice the computations of $(\phi_l^2 - T'\phi_l + q)P$ are done using the explicit formulas for the multiplication by T' map and $\phi_l(P)$, both of which are well known.

Kohel ([11], proof of Theorem 81) suggests modifying Schoof's algorithm to compute the trace of any endomorphism. To prove our result we go through Schoof's explanation and adjust it to our case for an endomorphism ϕ of trace t and norm n.

First, we know that the minimal polynomial is given by 3.2.4 and that we can compute n from the length of the cycle. Also, by [28] the trace t is given by $t = 1 + n - norm(\phi - 1)$, so it is bounded by $1 + \ell^m$, where m is the length of the corresponding cycle. Hence we can replicate Schoof's technique using this bound (avoiding the prime ℓ in the product) and the explicit formulas for the ℓ isogenies adapted from Vélu's [31] work.

Now that we find a way of computing both the trace and the norm of every cycle on the ℓ-isogeny graph, we want to determine under which conditions two cycles will correspond to elements on the quaternion algebra $B_{p,\infty}$ that would generate a maximal order. We address this in the next section.

3.3 Main results

The main results obtained in this paper are motivated by some natural questions, that arise from the approach of studying the ℓ-isogeny graph to construct endomorphism rings. These questions include:

1. Is there a criterion for when two cycles are linearly independent or dependent in $B_{p,\infty}$?

2. Is there a criterion for when the corresponding elements of two cycles generate a maximal order?

3. Are there always such cycles in the 2-isogeny graph?

We give a partial answer to Question 1: a condition for when two cycles correspond to linearly independent endomorphisms of End$(E) \subset B_{p,\infty}$. This is done in Section 3.3.1. Regarding Question 2, Section 3.3.2 describes an obstruction to generate the full endomorphism ring. In Example 3.4.3 we show that there exists at least one particular case in which the endomorphism ring can not be generated by cycles in the 2-isogeny graph, hence giving a negative answer to Question 3.

One key idea is that elements of $B_{p,\infty}$ are linearly dependent if and only if they commute. We eventually conclude that if two cycles have different vertex set, then they do not commute (see Corollary 3.3.3). Kohel [11] introduces the notion of a simple cycle and proves that they correspond to primitive endomorphisms. A less restrictive notion is that of a cycle with no backtracking.

Definition 3.3.1. A cycle $C = \{a_1, \ldots, a_e\}$ has no backtracking if a_{i+1} is not the dual of a_i for any $1 \leq i < e$.

In [3] it is shown that cycles with no backtracking correspond exactly to primitive endomorphisms.

3.3.1 A condition for linearly independent cycles

Suppose that $C = \{a_1, \ldots, a_e\}$ is a cycle with no backtracking, then either a_1 is not dual to a_e, or there is some k such that a_i is the dual of a_{e+1-i} for all $1 \leq i \leq k$. Theorem 3.3.2 states that under certain conditions, if the two cycles commute, then they are actually the same cycle repeated a possibly different number of times.

Theorem 3.3.2. *Suppose C_1 and C_2 are cycles in $G(p, \ell)$ through $E(j)$, α and β their corresponding endomorphisms on End$(E(j))$ that:*

1. *have no backtracking,*
2. *at least one of them does not have its first edge dual to its last and*
3. $\alpha\beta = \beta\alpha$.

Then there is a cycle with no backtracking passing through $E(j)$ which corresponds to $\gamma \in$ End$(E(j))$ and $u, v \in$ Aut$(E(j))$ which commute with γ such that $\alpha = u\gamma^a$ and either $\beta = v\gamma^b$ or $\beta = v\widehat{\gamma^b}$.

Proof. See [3] Theorem 4.10. □

This theorem implies that cycles with no backtracking with condition (2) can not be linearly dependent unless they can be defined as repetitions of the same cycle. We can relax condition (2) if we instead assume that no cycle contains a self-loop dual to itself and that their vertex set do not include $E(0)$ or $E(1728)$.

Corollary 3.3.3. *Suppose that two cycles C_1 and C_2 through $E(j)$ have no backtracking and that C_1 passes through a vertex through which C_2 does not pass. Suppose also that one cycle does not contain a self-loop which is dual to itself. Further assume that neither cycle passes through $E(0)$ or $E(1728)$. Then the corresponding endomorphisms in End$(E(j))$ are linearly independent.*

Proof. This is a consequence of Theorem 4.10 an Corollary 4.11 in [3]. □

3.3.2 Obstructions to generate the endomorphism ring

The next theorem is based on a result by Waterhouse, cited in McMurdy [15]. It evidences a feature of two cycles in the ℓ-isogeny graph that prevent them from generating the endomorphism ring of an elliptic curve.

Theorem 3.3.4. *Suppose two cycles in $G(p, \ell)$ both contain the same path between two vertices $E(j_1)$ and $E(j_2)$. Let α and β be the corresponding endomorphisms of $E(j_1)$. If the path between $E(j_1)$ and $E(j_2)$ passes through additional vertices, or if $j_1^p \neq j_2$, then $\{1, \alpha, \beta, \alpha\beta\}$ is not a basis for End$(E(j_1))$.*

Proof. See [3] Theorem 5.1. □

3.4 Examples

In this section we show three cases where the 2-isogeny graph can be used to find the endomorphism ring of supersingular elliptic curves. The graphs are based on examples given by Galbraith in [8]. To construct them we fix p to be the characteristic of the field. The supersingular j-invariants over $\mathbb{F}_{p^2}$ can be found by looking at the roots of the supersingular j-polynomial, whose

roots are exactly the supersingular j-invariants. Here is how we can obtain this polynomial: by Silverman [28] the elliptic curve given by $y^2 = x(x-1)(x-\lambda)$ has j-invariant

$$j = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \tag{3.4.1}$$

and it is supersingular if and only if λ is a root of

$$H_p(t) = \sum_{1=0}^{m} \binom{m}{i}^2 t^i. \tag{3.4.2}$$

We then compute the resultant of the polynomial $2^8(t^2 - t + 1)^3 - jt^2(t-1)^2$ and $H_p(t)$, which gives the supersingular j-polynomial. This algorithm is intrinsically implemented in SAGE [30], where the factors j and $j - 1728$ are removed, if they appear.

In order to determine the edges of the graph, we follow Definition 3.2.10. In practice we fix a j-invariant j and a curve $E(j)$, then compute the 2-torsion points of E and for each of them find the 2-isogeny whose kernel it generates. If ϕ is a 2-isogeny from $E(j)$ and j' is the j-invariant of $\phi(E(j))$, then there is and edge from $E(j)$ to $E(j')$.

Once we construct the graph we proceed to analyze different pairs of cycles that satisfy the conditions for linear independence from Corollary 3.3.3 do not present the obstruction condition from Theorem 3.3.4.

Example 3.4.1. If E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$ then by Theorem 3.2.2 End$(E) \otimes \mathbb{Q}$ is isomorphic to $B_{31,\infty}$, the quaternion algebra over $\mathbb{Q}$ ramified exactly at 31 and infinity. We know by Theorem 3.2.8 that $B_{31,\infty}$ is given by

$$B_{31,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij,$$

where $i^2 = -1$ and $j^2 = -31$.

The supersingular j-polynomial of $p = 31$ factors as $(j-2)(j-4)$ and since $31 \equiv 7 \mod 12$ then $1728 \equiv 23 \mod 31$ is supersingular j-invariant. Figure 3.1 shows the 2-isogeny graph with labeled edges.

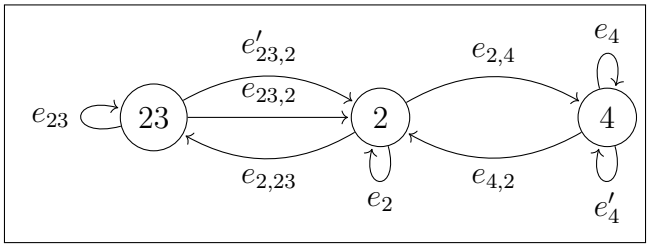

Figure 3.1: 2-isogeny graph for $p = 31$.

In this case it was possible to find pairs of cycles at every vertex that generate each of the maximal orders of $B_{31,\infty}$.

Table 3.1 contains, for each vertex, two cycles that correspond to elements that generate a maximal order in $B_{p,\infty}$. Hence these two cycles must generate the full endomorphism ring.

Table 3.1: Cycles that generate maximal orders in $B_{31,\infty}$.

Vertex	**Cycle**	**Trace**	**Norm**
2	e_2	0	2
	$e_{2,4}e_4e_{4,2}$	2	8
4	e_4	1	2
	$e_{4,2}e_2e_{2,4}$	0	8
23	e_{23}	2	2
	$e_{23,2}e_2e_{2,23}$	-1	8

With respect to the basis $< 1, i, j, ij >$ of $B_{31,\infty}$ defined above, the endomorphism rings of the supersingular curves over $\mathbb{F}_{31^2}$ correspond to the following maximal orders:

$$\text{End}(E(23)) \cong \left\langle 1, -i, -\frac{1}{2}i + \frac{1}{2}ij, \frac{1}{2} - \frac{1}{2}j \right\rangle,$$
$$\text{End}(E(2)) \cong \left\langle 1, \frac{1}{4}i\frac{1}{4}ij, 2i, \frac{1}{2} - \frac{1}{2}j \right\rangle,$$
$$\text{End}(E(4)) \cong \left\langle 1, \frac{1}{2} + \frac{1}{6}i + \frac{1}{6}j - \frac{1}{6}ij, \frac{5}{6}i + \frac{1}{3}j + \frac{1}{6}ij, -\frac{13}{6}i + \frac{1}{3}j + \frac{1}{6}ij \right\rangle.$$

Example 3.4.2 ($p = 103$)**.** The endomorphism rings of the supersingular elliptic curves over $\mathbb{F}_{103^2}$ are isomorphic to maximal orders of he unique quaternion algebra ramified at 103 and ∞, that is

$$B_{103,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \tag{3.4.3}$$

where $i^2 = -1$ and $j^2 = -103$.

On the other hand, the supersingular j-polynomial at 103 factors as

$$(j + 34)(j + 69)(j + 79)(j + 80)(j^2 + 63j + 69)(j^2 + 84j + 73), \tag{3.4.4}$$

hence there are at least four j-invariants over $\mathbb{F}_{103}$, namely $69, 34, 24$ and 23. In addition $103 \equiv 3 \mod 4$ implies that $1728 \equiv 80 \mod 103$ is a supersingular j-invariant. There are also two pairs of $\mathbb{F}_{103}$-conjugate j-invariants $(\alpha, \overline{\alpha})$ and $(\beta, \overline{\beta})$ that correspond to the roots of $(j^2 + 84j + 73)$ and $(j^2 + 63j + 69)$, respectively. Figure 3.2 shows the 2-isogeny graph.

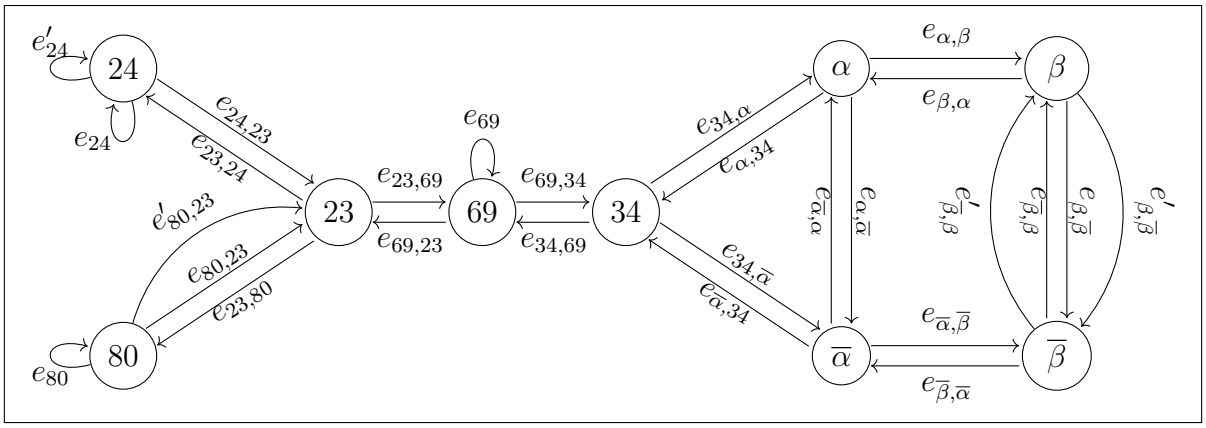

Figure 3.2: 2-isogeny graph for $p = 103$.

First we look at the j-invariants defined over $\mathbb{F}_{103}$. For each of them, we were able to find generators of the maximal orders corresponding to the endomorphism rings. We show the pairs of generating cycles for each vertex in Table 3.2.

Table 3.2: Cycles that generate maximal orders of $B_{103,\infty}$.

Vertex	Cycle	Trace	Norm
34	$e_{34,\overline{\alpha}}e_{\overline{\alpha},\alpha}e_{\alpha,34}$	-3	8
	$e_{34,69}e_{69}e_{69,34}$	0	8
69	e_{69}	0	2
	$e_{69,34}e_{34,\alpha}e_{\alpha,\overline{\alpha}}e_{\overline{\alpha},34}e_{34,69}$	-6	32
23	$e_{23,24}e_{24}e_{24,23}$	2	8
	$e_{23,80}e_{80}e_{80,23}$	-4	8
80	e_{80}	2	2
	$e_{80,23}e_{23,69}e_{69}e_{69,23}e_{23,80}$	0	32
24	e_{24}	-1	2
	$e_{24,23}e_{23,69}e_{69}e_{69,23}e_{23,24}$	0	32

These endomorphism rings are then isomorphic to the following maximal orders, where the basis is given as in (3.4.3).

$$\begin{aligned}
\text{End}(E(80)) &\cong \left\langle 1, i, \frac{1}{2}i + \frac{1}{2}ij, \frac{1}{2} + \frac{1}{2}j \right\rangle, \\
\text{End}(E(23)) &\cong \left\langle 1, 2i, \frac{3}{4}i + \frac{1}{4}ij, \frac{1}{2} - \frac{1}{2j} \right\rangle, \\
\text{End}(E(34)) &\cong \left\langle 1, \frac{17}{14}i + \frac{1}{14}ij \frac{15}{7}i - \frac{2}{7}ij, \frac{1}{2} - \frac{1}{2}j \right\rangle, \\
\text{End}(E(69)) &\cong \left\langle 1, \frac{1}{2} + \frac{1}{7}i + \frac{3}{14}j, \frac{1}{2} - \frac{16}{7}i + \frac{1}{14}j, \frac{1}{2} - \frac{17}{14}i - \frac{1}{14}j - \frac{1}{2}ij \right\rangle, \\
\text{End}(E(24)) &\cong \left\langle 1, \frac{1}{2} + \frac{3}{8}i + \frac{1}{8}ij, \frac{1}{2} - \frac{29}{8}i + \frac{1}{8}ij, -\frac{13}{8}i + \frac{1}{2}j + \frac{1}{8}ij \right\rangle.
\end{aligned}$$

In the case of α, β and their conjugates, it was not possible to find cycles that would generate the maximal orders. However we were able to use other tools to determine these endomorphism rings. First, note that conjugate pairs of j-invariants have isomorphic endomorphism rings,hence $\text{End}(\alpha) \cong \text{End}(\overline{\alpha})$ and $\text{End}(\beta) \cong \text{End}(\overline{\beta})$. By Theorem 3.2.2, the two remaining maximal orders of $B_{103,\infty}$ are each isomorphic to one of $\text{End}(\alpha)$ and $\text{End}(\beta)$.

For the vertex α we found an a pair of cycles that generate an order which is not maximal, these are

$$e_{\alpha,\beta} e'_{\beta,\overline{\beta}} e'_{\overline{\beta},\beta} e_{\beta,\alpha},$$

$$e_{\alpha,34} e_{34,69} e_{69} e_{69,34} e_{34,\alpha}$$

and the order is given by $\mathcal{O} = \left\langle 1, -\frac{1}{2} + \frac{17}{6}i - \frac{1}{6}j + \frac{1}{6}ij, -\frac{5}{2}i + \frac{1}{2}ij, -\frac{1}{2} - \frac{22}{3}i - \frac{11}{6}j - \frac{2}{3}ij \right\rangle$.

There is a unique maximal order containing $\mathcal{O}$, hence it corresponds to $\text{End}(E(\alpha)) \cong \text{End}(E(\overline{\alpha}))$. Finally, there is only one maximal order remaining in $B_{103,\infty}$, which is isomorphic to the endomorphism rings of $E(\beta)$ and $E(\overline{\beta})$.

The endomorphism rings of α and β are then isomorphic to:

$$\text{End}(E(\alpha)) \cong \left\langle -1, -\frac{1}{2} + \frac{1}{6}i - \frac{1}{6}j - \frac{1}{6}ij, 3i, \frac{5}{6}i - \frac{1}{3}j + \frac{1}{6}ij \right\rangle,$$
$$\text{End}(E(\beta)) \cong \left\langle 1, \frac{1}{2} + \frac{13}{10}i + \frac{1}{10}j - \frac{1}{10}ij, -\frac{12}{5}i + \frac{1}{5}j - \frac{1}{5}ij, \frac{1}{2} - \frac{3}{5}i + \frac{3}{10}j + \frac{1}{5}ij \right\rangle.$$

Example 3.4.3. The unique quaternion algebra ramified at 101 and ∞ is

$$B_{101,\infty} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \tag{3.4.5}$$

where $i^2 = -2$ and $j^2 = -101$.

We know that $E(0)$ is supersingular because $101 \equiv 2 \mod 3$. The supersingular j-polynomial at 101 factors as

$$(j + 35)(j + 37)(j + 42)(j + 44)(j + 80)(j + 98)(j^2 + 27j + 54). \tag{3.4.6}$$

From where the supersingular j-invariants over $\mathbb{F}_{101}$ are $0, 66, 64, 59, 57, 21$ and 3. We also denote by α and $\overline{\alpha}$ the roots of $j^2 + 27j + 54$ in $\mathbb{F}_{101^2}$. Figure 3.3 shows the 2-isogeny graph.

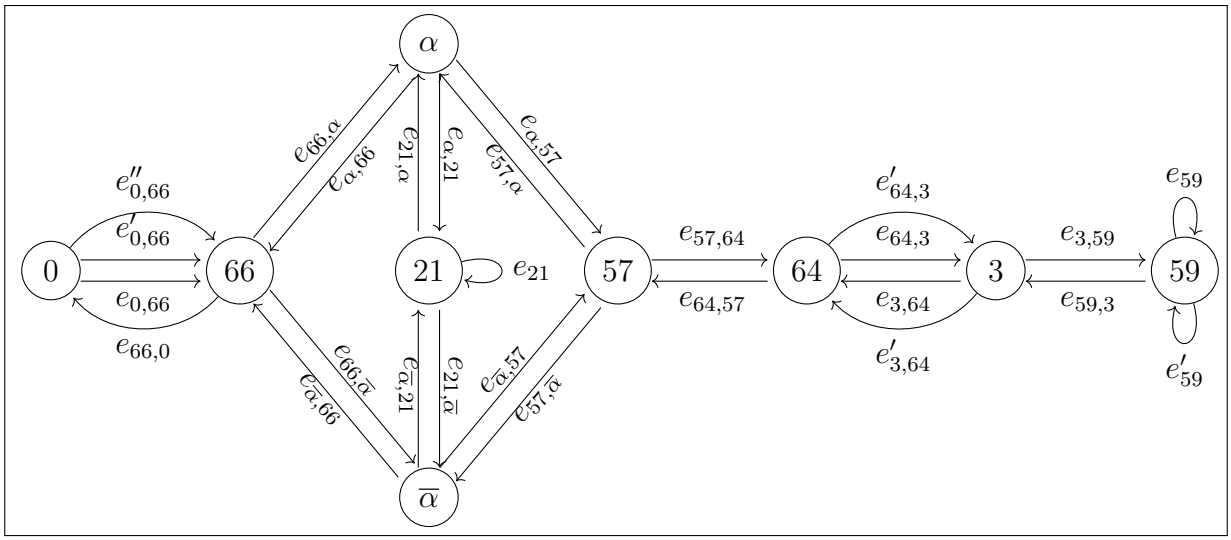

Figure 3.3: 2-isogeny graph for $p = 101$.

The cases where it was possible for us to find two cycles that generate the maximal order corresponding to End$(E(j))$ are $j = 3, 59, 64, 66$. In Table 3.3 we show the cycles for each vertex.

Table 3.3: Cycles that generate maximal orders in $B_{101,\infty}$.

Vertex	**Cycle**	**Trace**	**Norm**
3	$e_{3,59}e_{59}e_{59,3}$	2	8
	$e_{3,64}e'_{64,3}$	-1	4
59	e_{59}	-1	2
	$e_{59,3}e_{3,64}e_{64,3}e_{3,59}$	-8	16
64	$e_{64,57}e_{57,\alpha}e_{\alpha,66}e_{66,\overline{\alpha}}e_{\overline{\alpha},57}e_{57,64}$	10	64
	$e_{64,3}e'_{3,64}$	-1	4
66	$e_{66,0}e_{0,66}$	2	4
	$e_{66,\alpha}e_{\alpha,57}e_{57,\overline{\alpha}}e_{\overline{\alpha},66}$	5	16

The endomorphisms for these j-invariants are isomorphic to the following maximal orders:

$$\text{End}(E(3)) \cong \left\langle 1, \frac{1}{2} - \frac{13}{12}i + \frac{1}{12}ij, \frac{5}{6}i + \frac{1}{6}ij, \frac{5}{12}i - \frac{1}{2}j + \frac{1}{12}ij \right\rangle,$$

$$\text{End}(E(59)) \cong \left\langle 1, \frac{1}{2} + \frac{5}{12}i - \frac{1}{12}ij, -\frac{13}{6}i - \frac{1}{6}ij, -\frac{13}{12}i + \frac{1}{2}j - \frac{1}{12}ij \right\rangle,$$

$$\text{End}(E(64)) \cong \left\langle -1, -\frac{1}{2} - \frac{3}{5}i - \frac{1}{10}j + \frac{1}{10}ij, -\frac{1}{2} - \frac{21}{20}i + \frac{1}{5}j + \frac{1}{20}ij, \right.$$
$$\left. -\frac{67}{20}i - 1/10j - 3/20ij \right\rangle,$$

$$\text{End}(E(66)) \cong \left\langle 1, \frac{7}{10}i - \frac{1}{10}ij, \frac{1}{2} - \frac{29}{20}i - \frac{3}{20}ij, \frac{7}{20}i - \frac{1}{2}j - \frac{1}{20}ij \right\rangle.$$

For the vertices $21, 57, \alpha$ no two cycles were found that generate the full endomorphism ring. However, in each of these cases we were able to to generate an order from two cycles which happened to be contained in a unique maximal order. These cycles are listed in Table 3.4.

Table 3.4: Cycles that generate non maximal orders of $B_{101,\infty}$.

Vertex	**Cycle**	**Trace**	**Norm**
21	e_{21}	0	2
	$e_{21,\alpha}e_{\alpha,66}e_{66,0}e'_{0,66}e_{66,\alpha}e_{\alpha,21}$	-8	64
57	$e_{57,64}e_{64,3}e_{3,59}e_{59}e_{59,3}e_{3,64}e_{64,57}$	-8	128
	$e_{57,\alpha}e_{\alpha,66}e_{66,\overline{\alpha}}e_{\overline{\alpha},37}$	-5	16
α	$e_{\alpha,21}e_{21}e_{21,\overline{\alpha}}e_{\overline{\alpha},57}e_{57,\alpha}$	5	32
	$e_{\alpha,66}e_{66,0}e'_{0,66}e_{66,\alpha}$	4	16

The maximal orders are

$$\text{End}(E(21)) \cong \left\langle -1, i, -\frac{1}{2} + \frac{1}{4}i - \frac{1}{4}ij, -\frac{1}{2} + \frac{1}{2}i - \frac{1}{2}j \right\rangle,$$
$$\text{End}(E(57)) \cong \left\langle 1, \frac{1}{2} - \frac{13}{28}i + \frac{1}{7}j + \frac{1}{28}ij, -\frac{53}{28}i - \frac{1}{14}j + \frac{3}{28}ij, \frac{1}{2} - \frac{11}{4}i - \frac{1}{4}ij \right\rangle,$$
$$\text{End}(E(\alpha)) \cong \text{End}(E(\overline{\alpha})) \cong \left\langle -1, 2i, -\frac{1}{2} + \frac{3}{8}i + \frac{1}{4}j - \frac{1}{8}ij, -\frac{7}{8}i + \frac{1}{4}j + \frac{1}{8}ij \right\rangle.$$

Finally, by Theorem 3.3.4, no two cycles through $j = 0$ generate a maximal order, but it is possible to determine which one corresponds to the endomorphism ring of $E(0)$ once we ruled out the other seven, this is

$$\text{End}(E(0)) \cong \left\langle -1, -\frac{1}{2} + \frac{7}{20}i + \frac{1}{20}ij, -\frac{1}{2} + \frac{9}{5}i + \frac{1}{2}j - \frac{1}{10}ij, -\frac{29}{20}i + \frac{1}{2}j + \frac{3}{20}ij \right\rangle.$$

Chapter 4

Composite level images of Galois and hyperelliptic modular curves of low genus

This chapter is based on work in collaboration with Wanlin Li, Jack Petok, Jackson S. Morrow and David Zureick-Brown started in May 2017 at a group project workshop held at Emory University, organized by Zureick-Brown. This work is still in progress and the results present here will be summarized in a paper to be submitted for publication in the near future.

4.1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication. For every positive integer n, the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induces an action on the n-torsion points of E and so there is a group representation $\rho_{E,n}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/nZ)$.

In recent years, Zureick–Brown, Rouse, Sutherland and Zywina have made significant progress towards classifying the subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ which contain subgroups that are conjugate to images of Galois for some elliptic curve. Based off work of Sutherland–Zywina, Morrow began the study of the composite-(m_1, m_2) image of Galois in the case where m_1 is a power of 2 and m_2 is a prime ≤ 13.

The focus of this project is to continue the study of composite-(m_1, m_2) image of Galois, where m_1 and m_2 are powers of primes $p_1, p_2 \leq 13$. To do this, we build from the work of the previous authors and use the fact that an elliptic curve E defined over Q with $j_E \notin \{0, 1728\}$, has $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to a subgroup of G if and only if j_E belongs to $\pi_H(X_H(\mathbb{Q}))$ (see Section 4.2.2). Then we construct models for the modular curves X_H and study the rational points on those that have genus equal to $0, 1$ or 2. These points correspond to either the elliptic curves

of our interest, elliptic curves with complex multiplication, or cusps. We use different methods to find the rational points, which we execute with the aid of the software `Magma`.

4.2 Background

This section includes a review on elliptic curves over number fields, their Galois representations and modular curves. We refer the reader to [27] and [29] for a more detailed description. First we will introduce some basic definitions and properties of elliptic curves.

4.2.1 Elliptic curves

Let k any field of characteristic different from 2 and 3, an **elliptic curve** E defined over k is nonsingular curve of genus 1. We can assume that E is defined by the homogenization of

$$y^2 = x^3 + a_1 x + a_2, \tag{4.2.1}$$

for some $a_1, a_2 \in k$, the base point at infinity is $O = [0 : 1 : 0]$.

We define the j-invariant of E as the quantity $j = \frac{2^8 3^3 a_1^3}{4a_3^3 + 27a_2^2}$. This invariant classifies the $\overline{k}$-isomorphism classes of elliptic curves.

An elliptic curve E is equipped with an additive group law, with O as the identity element, as follows:

Definition 4.2.1 (Group Law)**.** Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be the line through R and O. Then L' intersects E at R, O, and a third point. We denote that third point by $P + Q$ and the sum of P with itself m times by mP.

Definition 4.2.2. The N-torsion subgroup of E is given by

$$E[N] = \{P \in E(\overline{k}) : NP = O\}.$$

Definition 4.2.3. Let E and E' be elliptic curves. An isogeny from E to E' is a morphism

$$\phi : E \to E' \text{ satisfying } \phi(O) = O.$$

Two elliptic curves E and E' are *isogenous* if there is an isogeny $\phi : E \to E'$ such that $\phi(E) \neq O$.

In fact, if $\phi(E) \neq O$, the only other possibility is $\phi(E) = E'$.

Since elliptic curves have group structures, the set $\text{Hom}(E, E')$ of isogenies between two elliptic curves has a ring structure. In particular, we define the Endomorphism Ring of E as

$$\text{End}(E) = \text{Hom}(E, E) = \{\text{isogenies } E \to E\}. \tag{4.2.2}$$

Proposition 4.2.4. *The endomorphism ring of E, denoted End(E) is either*

- $\mathbb{Z}$*,*
- *an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$, $D < 0$ or*
- *an order in a quaternion algebra.*

Proof. See Silverman, [28], pp. 102. □

It turns out that when $\text{char}(k) = 0$, only the first two options are possible. For our purposes, we will study elliptic curves over $\mathbb{Q}$. When $\text{End}(E)$ is not isomorphic to $\mathbb{Z}$, we say that E has complex multiplication (CM).

4.2.2 Galois representations

Let E be an elliptic curve defined over $\mathbb{Q}$ without CM, with j-invariant j_E and let N be a positive integer. As shown in Silverman in [28], the N-torsion subgroup of E over $\overline{\mathbb{Q}}$ has the form

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

The absolute Galois group $\text{Gal}_{\mathbb{Q}} \cong \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on $E[N]$ and so we get an induced Galois representation

$$\rho_{E,N} : \text{Gal}_{\mathbb{Q}} \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z}), \tag{4.2.3}$$

where $\rho_{E,N}(\text{Gal}_{\mathbb{Q}})$ is the Galois group of the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the N-torsion points of E (see Serre [27]). This is defined as the $\mod N$ *Galois representation*.

Similarly, there are a representations associated to each one of the subgroups of E

$$E[tors] := \bigcup_{n\geq 1} E[n], \tag{4.2.4}$$

$$E[\ell^\infty] := \bigcup_{n\geq 1} E[\ell^n]. \tag{4.2.5}$$

Recall that $\hat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$, can be defined both as $\varprojlim \mathbb{Z}/N\mathbb{Z}$ and as the product $\prod_\ell \mathbb{Z}_\ell$, hence, for a fixed $\hat{\mathbb{Z}}$- basis of $E[tors]$ there is an induced $\mathbb{Z}_\ell$-basis for any prime ℓ, and for any positive integer N there is an induced $\mathbb{Z}/N\mathbb{Z}$-basis on $E[N]$.

The automorphism group of $E[tors]$ is isomorphic to

$$\prod_\ell \text{GL}_2(\mathbb{Z}_\ell) \cong \text{GL}_2(\hat{\mathbb{Z}}) \cong \varprojlim \text{GL}_2(\mathbb{Z}/N\mathbb{Z}). \tag{4.2.6}$$

We define the *adélic and ℓ-adic representations* induced by the action of $\text{Gal}_{\mathbb{Q}}$ on $E[tors]$ and $E[\ell^\infty]$ respectively as

$$\rho_E \quad : \quad \text{Gal}_{\mathbb{Q}} \mapsto \text{Aut}(E[tors]) \cong \text{GL}_2(\hat{\mathbb{Z}}), \tag{4.2.7}$$

$$\rho_{E,\ell^\infty} \quad : \quad \text{Gal}_{\mathbb{Q}} \mapsto \text{Aut}(E[\ell^\infty]) \cong \text{GL}_2(\mathbb{Z}_\ell). \tag{4.2.8}$$

By Serre's open image theorem ([27]) and with the hypothesis that E does not have CM, we get that $\rho_E(\text{Gal}_{\mathbb{Q}})$ is an open subgroup of $\text{GL}_2(\hat{\mathbb{Z}})$ and hence it is of finite index. This gives a starting point to Mazur's program B ([14]):

Given a number field K and a subgroup H of $GL_2(\hat{\mathbb{Z}}) = \prod_\ell GL_2(Z_\ell)$ classify all elliptic curves E/K whose associated Galois representation on torsion points maps $Gal(\overline{K}/K)$ into $H \subset GL_2(\hat{\mathbb{Z}})$.

We are interested in expanding the work of program B. The progress so far suggests that there exists a constant B, such that for every elliptic curve $E/\mathbb{Q}$, the index of $\rho_E(\mathrm{Gal}_\mathbb{Q})$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is bounded by B. In fact, Serre [27] shows that there exists a constant c_E such that $\rho_{E,\ell}(\mathrm{Gal}_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell > c_E$ and asks whether $c_E = c$ could be chosen independently of E. Moreover, the author conjectures that $c = 37$. Regarding this, Zywina [37] formulates the next conjecture:

Conjecture 4.2.5. *There is an absolute constant c such that for every non-CM elliptic curve E over $\mathbb{Q}$, we have $\rho_{E,\ell}(Gal_\mathbb{Q}) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell > c$.*

Following [18] we consider the inclusions

$$\rho_E(\mathrm{Gal}_\mathbb{Q}) \hookrightarrow \prod_{\ell \text{ prime}} \rho_{E,\ell^\infty}(\mathrm{Gal}_\mathbb{Q}) \subset \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell). \tag{4.2.9}$$

The image of $\rho_E(\mathrm{Gal}_\mathbb{Q})$ projects onto each ℓ-adic factor, so we look at the composite-(m_1, m_2) image $(\rho_{E,m_1} \times \rho_{E,m_2})(\mathrm{Gal}_\mathbb{Q})$, for all m_1, m_2 that are relatively prime.

For $H \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$ such that $\det(H) = \hat{\mathbb{Z}}^\times$ and $-I \in H$, the *level* of a subgroup is the least integer such that $H = \phi^{-1}(\phi(H))$, where the composition of ρ_E with the projection $\phi : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ given by reduction $\mod N$ is $\rho_{E,N}$. To each open subgroup $\overline{H}$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ we can attach a modular curve $X_{\overline{H}}$ (see [29] for definition and details). If $H \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$ is before and N is divisible by the level of H, we can define modular curve of H as $X_H := X_{\overline{H}}$. This curve does not depend on the choice of N or $\overline{H}$ and it is smooth, projective and geometrically closed. Suppose that H' is a subgroup $H \subset H' \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$, such that the determinant map on H' is surjective. Then there is a natural homomorphism $X_H \to X_{H'}$ of

degree $[H' : H]$. In particular, if $H' = \mathrm{GL}_2(\hat{\mathbb{Z}})$ then the map is

$$\pi_H : X_H \to \mathbb{P}^1_{\mathbb{Q}}. \tag{4.2.10}$$

The next two propositions, as stated by Sutherland and Zywina [29] and following the work of Zywina ([37], [36]) are key to determine if a given open subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ contains a conjugate of $\rho_E(\mathrm{Gal}_{\mathbb{Q}})$ for some non-CM elliptic curve E over $\mathbb{Q}$.

Proposition 4.2.6. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $j_E \notin \{0, 1728\}$, then $\rho_E(Gal_{\mathbb{Q}})$ is conjugate in $GL_2(\hat{\mathbb{Z}})$ to a subgroup of G if and only if j_E belongs to $\pi_G(X_G(\mathbb{Q}))$.*

Proposition 4.2.7. *Let E be an elliptic curve over $\mathbb{Q}$ for which $\rho_{E,N}$ is not surjective. Then $H = \pm\rho_{E,N}(Gal_{\mathbb{Q}}) \subset GL_2(\mathbb{Z}/N\mathbb{Z})$ has the following conditions:*

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

Definition 4.2.8. A subgroup with the conditions of Proposition 4.2.7 is called *applicable*.

4.2.3 Progress on Mazur's Program B

In the past few years there have been several result towards a complete classification of adélic representation for non-CM elliptic curves. Zywina [36] described all known, and conjecturally all, pairs (E, ℓ) such that $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is non-surjective. Rouse and Zureick-Brown computed in [25] all of the possible 2-adic images of Galois for non-CM elliptic curves over $\mathbb{Q}$. Also, Sutherland and Zywina [29] found all the prime level modular curves X_H where the set of rational points is infinite. The main focus of these works is to determine the rational functions as in (4.2.10) that

correspond to the j-invariants of non-CM elliptic curves for which the image of Galois is conjugate to a subgroup of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ where N is the level of H.

Following the computations from [36] and [25], Morrow [18] analyzed the $\mathbb{Q}$ points of composite level modular curves with level $N = \ell \cdot 2^n$. To do this, the author defines a composite-(m_1, m_2) level modular curve $X_{H_1,H_2}(m_1 \cdot m_2)$ as the normalization of the fibered product X in

$$\begin{array}{ccc} X & \longrightarrow & X_{H_2}(m_2) \\ \downarrow & & \downarrow{\scriptstyle j(H_2)} \\ X_{H_1}(m_1) & \xrightarrow[j(H_1)]{} & \mathbb{P}^1_{\mathbb{Q}} \end{array}$$

Figure 4.1: Fiber product of modular curves.

Where $H_i(m_i)$ is an applicable group of $\mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$. Hence, the rational points of $X_{H_1,H_2}(m_1 \cdot m_2)$ correspond to elliptic curves over $\mathbb{Q}$ with composite-(m_1, m_2) image conjugate to a subgroup $H_1 \times H_2 \subset \mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/m_1m_2\mathbb{Z})$. Morrow finds all the equations for the composite-$(2^n, \ell)$ level modular curves and determined their rational points for the tuples $(2, \ell)$ with $\ell = 3, 5, 7, 11, 13$ and $(m_1, 3)$ with $m_1 = 4, 8, 16$.

4.3 Main Results

For this project, we use the same strategy as Morrow's to analyze curves of the form $X_{H_1,H_2}(m_1 \cdot m_2)$ where H_1 and H_2 belong to the set of subgroups already studied in [25] and [36], m_1 and m_2 are powers of distinct primes ℓ_1 and ℓ_2 with $\ell_i \leq 13$ and $m_i \leq 37$. We focus our analysis on the modular curves of genus 0, 1 and 2 that arise this way. In particular, we want to address to questions:

1. Which subgroups of $\mathrm{GL}_2(\mathbb{Z}/m_1m_2)$ contain the image $\rho_E(G_K)$ for infinitely many E? Equivalently, which modular curves of composite (m_1, m_2)-level have infinitely many rational points?

2. Are there any curves of composite (m_1, m_2)-level curves that contain non-cuspidal and non-CM rational points?

To answer question (1) we need only to look at modular curves of genus 0 and 1, since smooth curves of genus ≥ 2 have finitely many rational points. We give a positive answer to question (2) by explicitly finding the rational points on modular curves of genus 1 and rank 0 and on some curves of genus 2. This last analysis is described in Section 4.4.

Theorem 4.3.1. *Let m_1, m_2 be powers of distinct primes $\ell_1, \ell_2 \leq 13$. Up to conjugacy, there are 81 open subgroups G of $\mathbf{GL}_2(\hat{\mathbb{Z}})$ of composite-(m_1, m_2) level satisfying $-I \in G$ and $\det(G) = \hat{\mathbb{Z}}^\times$ for which $X_G(m_1m_2)$ has infinitely many rational points. Of these 81 groups, there are 46 of genus 0 and 35 of genus 1.*

Proposition 4.3.2. *Let m_1, m_2 as before, up to conjugacy in $\mathbf{GL}_2(\hat{\mathbb{Z}})$:*

a) there are exactly 8 genus 1 modular curves $X_G(m_1m_2)$ with sporadic points.

b) there are at least 4 and at most 11 genus 2 modular curves $X_G(m_1m_2)$ with sporadic points.

The proofs of Theorem 4.3.1 and Part a) of Proposition 4.3.2 are part of the work done in [4]. Here we describe the analysis of genus 2 curves that completes the proof of Theorem 4.3.2. We have been able to provably find all of the rational points on the genus 2 modular curves with rank 0 and 1, and on all but 7 curves of rank 2.

4.4 Analysis of composite-(m_1, m_2) level modular curves of genus 2

There are 70 modular curves of genus 2, with 59, 14 and 7 of ranks 0, 1 and 2 respectively. We use Chabauty's method to find the rational points on all of the rank 0 and most of the rank 1 curves, for the other ones we apply ètale descent. For each of the modular curve we find a (possibly singular) model C and use the `Magma` intrinsic function `IsHyperelliptic` to obtain a smooth model C' and `Jacobian` to find $J_{C'}(\mathbb{Q})$.

We are also able to group theoretically compute the cusps of the modular curve. Once we find the rational points we determine which curves have sporadic points, that is, non-CM non-cuspidal points. We proceed in the following way: if the number of rational points is equal to the number of cusps, then this guarantees no sporadic points. If there are more cusps than rational points on then we pull these back from C' to C and verify if they are nonsingular. In every case we have that the number of nonsingular rational points on C plus the number of cusps equals the number of rational points on C', and since nonsingular points on C map to rational points on C, we only need to check if the image of these points under the j-map correspond to j-invariants of CM elliptic curves.

Rank 0

Since rank$(J_{C'}(\mathbb{Q}))$ is less than 2. we are able to apply `Chabauty0` on $J_{C'}(\mathbb{Q})$ to provably compute all the rational points on C'. From here we compare the number of cusps we the number of rational points as previously described. After this computation we conclude that there are no sporadic points on any genus 2 rank 0 modular curves of interest.

Rank 1

For all of the 14 curves it is possible to find a point P in $J_{C'}(\mathbb{Q})$ of infinite order, through a naive point search bounding the height of P. Hence we can implement the command `Chabauty(P)`

which returns all the rational points of C'. After applying the procedure described above the find that 10 curves have no non-cuspidal rational points but 4 have sporadic points:

- $X_{H_{10},H_{33}}(28)$ has two sporadic points with j-invariants $-38575685889/16384$ and $351/4$.
- $X_{H_{16},H_{24}}(20)$ has four sporadic points, two with j-invariant -36 and two $-64278657/1024$.
- $X_{H_{25},H_{132}}(45)$ has two sporadic points with j-invariants -23788477376 and 64.
- $X_{H_{29},H_{39}}(40)$ has two sporadic points with j-invariant -5000.

Rank 2 curves: There are 9 curves of rank 2 and at most 8 isomorphism classes. The method of Chabauty does not apply here, since it requires the rank of the Jacobian to be less than the genus of the curve. We proceed by étale descent, specifically using double étale covers. We were only able to find rational points on 2 of the curves, but on both cases they correspond to CM points. For the remaining 7 cases, 4 of the curves have no 2-torsion points on their jacobians, hence étale descent is actually not an option.

Bibliography

[1] Gorjan Alagic, Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. National Institute of Standards and Technology, 2019.

[2] Matthew H. Baker. Cartier points on curves. *Internat. Math. Res. Notices*, (7):353–370, 2000.

[3] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträeger, Travis Morrison, and Jennifer Park. Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms. *arXiv e-prints*, page arXiv:1804.04063, Apr 2018.

[4] Catalina Camacho-Navarro, Wanlin Li, Jackson S Morrow, Jack Petok, and David Zureick-Brown. Modular curves of low compostie level and genus zero subgroups. Work in progress.

[5] Torsten Ekedahl. On supersingular curves and abelian varieties. *Math. Scand.*, 60(2):151–178, 1987.

[6] Carel Faber and Gerard van der Geer. Complete subvarieties of moduli spaces and the Prym map. *J. Reine Angew. Math.*, 573:117–137, 2004.

[7] Sarah Frei. The s-number of hyperelliptic curves. In *Women in numbers Europe II*, volume 11 of *Assoc. Women Math. Ser.*, pages 107–116. Springer, Cham, 2018.

[8] Steven Galbraith. Isogeny graphs, algorithms and applications. http://iml.univ-mrs.fr/ati/geocrypt2013/slides/galbraith.pdf, 2013.

[9] Darren Glass and Rachel Pries. Erratum to: Hyperelliptic curves with prescribed p-torsion [mr2154252]. *Manuscripta Math.*, 133(3-4):545–546, 2010.

[10] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[11] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)–University of California, Berkeley.

[12] Momonari Kudo and Shushi Harashita. Superspecial curves of genus 4 in small characteristic. *Finite Fields Appl.*, 45:131–169, 2017.

[13] Ke-Zheng Li and Frans Oort. *Moduli of supersingular abelian varieties*, volume 1680 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998.

[14] Barry Mazur. Rational points on modular curves. In *Modular functions of one variable V*, pages 107–148. Springer, 1977.

[15] Ken McMurdy. Explicit representation of the endomorphism rings of supersingular elliptic curves. https://phobos.ramapo.edu/~kmcmurdy/research/McMurdy-ssEndoRings.pdf, 2014.

[16] James S. Milne. Jacobian varieties. www.jmilne.org/math/xnotes/JVs.pdf, 2012.

[17] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[18] Jackson S. Morrow. Composite images of Galois for elliptic curves over $\mathbf{Q}$ and entanglement fields. *Math. Comp.*, 88(319):2389–2421, 2019.

[19] Frans Oort. Which abelian surfaces are products of elliptic curves? *Math. Ann.*, 214:35–47, 1975.

[20] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[21] Rachel Pries. A short guide to p-torsion of abelian varieties in characteristic p. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 121–129. Amer. Math. Soc., Providence, RI, 2008.

[22] Rachel Pries. The p-torsion of curves with large p-rank. *Int. J. Number Theory*, 5(6):1103–1116, 2009.

[23] Rachel Pries. Current results on Newton polygons of curves. *arXiv e-prints*, page arXiv:1806.04654, Jun 2018.

[24] Riccardo Re. The rank of the Cartier operator and linear systems on curves. *J. Algebra*, 236(1):80–92, 2001.

[25] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois representations. *Research in Number Theory, Accepted*, 2015.

[26] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[27] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259 331, 1972.

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

[29] 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.

[30] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.3.0)*, 2019. `https://www.sagemath.org`.

[31] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[32] John Voight. Quaternion algebras. v.0.9.15. May 26, 2019.

[33] Zijian Zhou. A bound on the genus of a curve with Cartier operator of small rank. *arXiv e-prints*, page arXiv:1710.01058, Oct 2017.

[34] Zijian Zhou. Ekedahl-Oort strata on the moduli space of curves of genus four. *arXiv e-prints*, page arXiv:1812.04996, Dec 2018.

[35] Zijian Zhou. On the existence of curves with prescribed a-number. *arXiv e-prints*, page arXiv:1901.08375, Jan 2019.

[36] David Zywina. On the possible images of the mod ell representations associated to elliptic curves over Q. *arXiv e-prints*, page arXiv:1508.07660, Aug 2015.

[37] David Zywina. Possible indices for the Galois image of elliptic curves over Q. *arXiv e-prints*, page arXiv:1508.07663, Aug 2015.