2018

Enumerating Curves of Genus 2 Over Finite Fields

Rose K. Steinberg
University of Vermont

Enumerating Curves of Genus 2 Over Finite Fields

Presented by

Rose K. Steinberg

to

The Faculty of the College of Arts and Sciences

of

The University of Vermont

In Partial Fulfillment of the Requirements
for the Degree of Bachelor of Arts in Mathematics
Honors College

May 11, 2018

Defense Date: April 26, 2018
Thesis Examination Committee:

Prof. Christelle Vincent, Advisor
Prof. Jonathan Sands, Committee Member
Prof. Matthew White, Chairperson
Prof. Rory Waterman, Dean of the College of Arts and Sciences

Abstract

In this thesis, we investigate curves over finite fields. More precisely, fixing a base field $\mathbb{F}_q$ and a genus g, we aim to enumerate a representative from each isogeny and isomorphism class of curves defined over that field and of that genus. As a step towards this goal, in this work we provide code that, given a finite field of any characteristic, generates a list of models of hyperelliptic curves of genus 2 which we can guarantee contains one representative from each isomorphism class of curves defined over that field. Furthermore, our code allows us to sort these models into isogeny classes. Finally, if the field is of odd characteristic, we can further sort the models into isomorphism classes.

As an application of our software, we obtain representatives for every isogeny class of hyperelliptic curves of genus 2 defined over the finite field $\mathbb{F}_2$. We also give a model for each isogeny and isomorphism class of hyperelliptic curves of genus 2 defined over $\mathbb{F}_3$. In these investigations, we discovered that Theorem 5 of *Isomorphism Classes of Genus-2 Hyperelliptic Curves Over Finite Fields* by Encinas, Menezes, and Masqué may be more accurately stated as giving the number of isomorphism classes of *pointed* hyperelliptic curves rather than isomorphism classes of hyperelliptic curves.

Acknowledgements

I would like to thank the UVM Honors College and Dean Lisa Schnell for laying a pathway for me to complete a thesis as part of my undergraduate degree. The Honors College community has been a source of intellectual challenge, personal growth, and unending encouragement during my time at UVM. I would also like to thank the Mathematics and Statistics Department for providing me with interesting courses and enthusiastic instruction for the past four years. Finally, I would like to express my immense appreciation for the time and effort of my thesis committee: Professor Jonathan Sands of the Mathematics and Statistics Department, Professor Matthew White of the Physics Department, and most importantly, my thesis advisor Professor Christelle Vincent. Simply put, this thesis would not exist without her. Last spring, I did not know an undergraduate student could even attempt a thesis in Mathematics. Thanks to Professor Vincent's expertise in her field and her willingness to invest in a young math student, this project came to life. She has led me through the past year with understanding, positivity, and a sense of humor. I am honored to have had the opportunity to work with her.

Table of Contents

Chapter 1

Introduction

In this work we consider hyperelliptic curves of genus 2 defined over finite fields. Hyperelliptic curves, which are the only kind of curve in genus 2, are introduced in Corollary 4.1.1 in Chapter 4. (For a definition of *genus*, please refer to Definition 3.3.5.) Although hyperelliptic curves are a kind of projective plane curve, we begin this thesis with presenting the simpler theory of affine varieties and curves in Chapter 2, as a segue into the theory of projective varieties and curves in Chapter 3. Our purpose is to classify models for these curves into so-called isogeny and isomorphism classes, which are two natural equivalence relations on curves.

The first equivalence relation we will use to classify the curves is that of isogeny. Given a curve C, we can define its associated *Jacobian variety* as a certain abelian group compatible with the structure of the curve. Two curves are isogenous if their Jacobians admit a finite, surjective map between them. For simplicity in this thesis, we will use a different, but equivalent, definition for isogeny. Indeed it is the case that curves that are isogenous to each other share the same L-polynomial in their zeta-function, which is how we will verify if two curves are isogenous. We will define the zeta-function and sort curves into isogeny classes in Chapter 5.

The second equivalence class that we use to classify the curves under consideration is more strict than an isogeny relation, and is called an isomorphism relation. Two curves are roughly thought to be isomorphic if they have the same shape and are defined over the same finite field, however they are not identical in location. For example, the curves $y = x^2$ and $y = (x-2)^2$ are isomorphic because they are related by the translation $x \mapsto (x-2)$ and $y \mapsto y$. This notation is made precise by saying that two curves are isomoprhic if they are related by an invertible rational map. Curves that are isomorphic to each other will form what we will call an *isomorphism class.* We will sort curves into isomorphism classes in Chapter 6.

Due to limitations of the Magma software, we are able to enumerate the isogeny classes but *not* the isomorphism classes of curves of genus 2 over a finite field of characteristic 2. We carry out this classification for the field $\mathbb{F}_2$, and these results can be found in Section A.1. We are able to classify curves of genus 2 defined over fields of odd characteristic into isomorphism classes as well as isogeny classes. We find both the isogeny classes and the isomorphism classes of curves of genus 2 defined over $\mathbb{F}_3$ in in Section A.2. For curves defined over $\mathbb{F}_2$ and $\mathbb{F}_3$, we also identify which isogeny classes contain curves with no rational points.

1.1 Literature Review

There is significant interest in enumerating isomorphism classes and isogeny classes of curves for fixed genus and base field. For example, the L-functions and modular forms database [9] lists isogeny classes for abelian varieties defined over finite fields, and it lists isomorphism classes of curves of genus 2 over the rational field $\mathbb{Q}$ for certain relatively small conductors. Apart from this, mathematicians have listed curves with certain properties, for example, curves with many rational points in [6]. However, none of these sources list all curves of a chosen genus defined over a certain finite field, nor do they classify them into isomorphism classes and isogeny classes.

In some cases, curves of a certain form have been enumerated. For example, Lee [8] counts isomorphism classes of Picard curves over a field of characteristic 2, which are a certain kind of curve of genus 3, and proves the theorem:

Theorem 1.1.1 (Theorem 4.6 of [8]). *The number of isomorphism classes of Picard curves over a finite field $\mathbb{F}_q = \mathbb{F}_{2^m}$ is given by*

$$\begin{cases} q^2 + 2q - 2, & \text{if } m \text{ is odd}, \\ 3(q^2 - 5), & \text{if } m \equiv 2, 4 \pmod 6, \\ 3(q^2 - 3), & \text{if } m \equiv 0 \pmod 6. \end{cases} \tag{1.1}$$

In addition, in [8] the author also gives reduced forms for the equations of the curves he counts but does not organize them by isogeny class.

Apart from this, other authors have counted the number of isomorphism classes of curves with certain properties, but have not enumerated equations for the curves. For example, You and Zeng [14] count the number of isomorphism classes of hyperelliptic curves of genus 4 over $\mathbb{F}_q$:

Theorem 1.1.2 (Theorem 4 of [14]). *The number of isomorphism classes of hyper-*

elliptic curves of genus 4 over $\mathbb{F}_q$ is

$$2(q^7 - q^3 + q + 3) + |G_1| + |G_2| + (q-2)|G_3| + (q^2 - 2q - 2)|G_4| + (q^3 - q^2 - 1)|G_5|$$

where for $i = 1, 2, 3, 4, 5, 6$, G_i is the group of automorphisms of the curves contained in a certain set H_i.

We note that since hyperelliptic curves are a subset of all curves of genus 4, this work does not account for all curves of genus 4 over a given finite field. In addition, as we stated above, this work does not enumerate models for the curves it does cover.

Considering a different problem in [1], Eisenträger and Lauter give a construction for a genus-2 curve defined over a finite field with a certain number of rational points. Their method involves computing Igusa class polynomials and applying the Chinese Remainder Theorem. They also provide an algorithm that determines the endomorphism ring of the Jacobian of these genus 2 curves. A similar algorithm already exists for elliptic curves, which is the genus 1 case, however this is the first generalization of its kind to genus 2. While this algorithm created a way to construct curves of genus 2, because of its purpose (to construct a curve with a specified number of points) the computations are too onerous for this project, which is to list all curves regardless of their point count. Therefore we must use a different method so that the computations terminate within a reasonable time frame.

1.2 Methodology

The first step in this project is to create a list of the genus 2 curves defined over a certain finite field. While we do not need to generate *all* the curves, we do need to generate enough so that there is a representative from each and every isomorphism class of curves defined over that field. We do so using the software Magma and code we have written for this purpose, as described in Chapter 4. Once we have this list, we sort each curve into its isogeny class using the the point counts of certain base changes of the curve, as described in Chapter 5. Finally, we partition each isogeny class into isomorphism classes, again using Magma, as described in Chapter 6. As an added benefit of this project, we are able to give a model for a curve belonging to each isogeny class of curves of genus 2 defined over $\mathbb{F}_2$ and $\mathbb{F}_3$ with no rational points. We do so in Section 5.3.

1.3 Significant Findings

As described in Section 1.1, while others have studied certain aspects pertaining to the enumeration of curves of a fixed genus over finite fields, none have gone into as much detail as we have in this project. As far as we know, never before has anyone enumerated every isomorphism class of genus 2 defined over $\mathbb{F}_2$ and $\mathbb{F}_3$ because the computing power did not yet exist. Our work is a significant step in this direction. Using Magma and the code we wrote, we were able to generate and classify curves with a new degree of completeness.

This project has rendered several significant results. The first is a complete list of curves of genus 2 defined over $\mathbb{F}_2$, sorted into isogeny classes. This is a valuable contribution to the work found in [9].

The second significant result is a list of all the isogeny and isomorphism classes of genus 2 defined over $\mathbb{F}_3$. While we did not include every curve over $\mathbb{F}_3$, we can prove that we have at least one representative curve from all isogeny and isomorphism classes, and therefore that our list is complete.

Third, we used these isogeny classes to identify a model for curves of genus 2 with no rational points defined over $\mathbb{F}_2$ and $\mathbb{F}_3$. These results can be found in Section 5.3.

The final result has to do with the second finding. Previous literature [2] suggests that there are 54 isomorphism classes of curves of genus 2 defined over $\mathbb{F}_3$. However, our results give 69 such classes. We found that the authors of [2] use a different notion of isomorphism than is usual and discuss this discrepancy in Section 6.2.

Chapter 2

Affine Varieties and Curves

While we will mainly deal with projective curves in this thesis, we first introduce the simpler case of affine varieties and curves. Accordingly in this chapter we give an overview of the theory and its basic definitions and results. First, we introduce algebraic sets in Section 2.1. Then, we discuss ideals of algebraic sets in Section 2.2 and how to determine whether an algebraic set is reducible or irreducible in Section 2.3, which we use to define affine varieties. We then define the coordinate ring of an affine variety in Section 2.4. Finally, we define affine plane curves and several of their properties in Section 2.5. The concepts introduced in this chapter are standard and can be found for example in [4].

2.1 Algebraic Sets

In this section, we define algebraic sets, which are the most basic objects of algebraic geometry.

Definition 2.1.1. *Let $\mathbb{F}$ be a field, then $\mathbb{A}^n(\mathbb{F}) = \mathbb{F}^n$. We call $\mathbb{A}^n(\mathbb{F})$ the n-dimensional* *affine space.*

Definition 2.1.2. *Let $\mathbb{F}$ be a field and let $\mathbb{A}^n(\mathbb{F})$ be the n-dimensional affine space over $\mathbb{F}$. Let S be a set of polynomials in n variables with coefficients in $\mathbb{F}$. We define the algebraic set associated to S defined over $\mathbb{F}$ to be*

$$V(S) = \{(x_1, x_2, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}) : f(x_1, x_2, \ldots, x_n) = 0 \quad \forall f \in S\}. \tag{2.1}$$

Example 2.1.3. *The set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r, θ) satisfy the equation $r = \sin\theta$ is an algebraic set.*

We start with the equations for Cartesian coordinates as functions of the polar coordinates:

$$x = r\cos\theta, \quad y = r\sin\theta, \tag{2.2}$$

and divide both sides of the second equation by r

$$\frac{y}{r} = \sin\theta. \tag{2.3}$$

Since $r = \sin\theta$ and $\frac{y}{r} = \sin\theta$, we can say

$$r = \frac{y}{r}. \tag{2.4}$$

Multiplying both sides of this by r, we now have:

$$r^2 = y. \tag{2.5}$$

We know that Cartesian and polar coordinates satisfy the relation $r^2 = x^2 + y^2$, *so setting r^2 equal to $x^2 + y^2$, we end with:*

$$y = x^2 + y^2 \text{ or } x^2 + y^2 - y = 0. \tag{2.6}$$

This is a polynomial in 2 variables, and the set of points $r = \sin\theta$ is its zero locus. Therefore this set is the algebraic set associated with

$$S = \{x^2 + y^2 - y\}. \tag{2.7}$$

2.2 Ideals of Algebraic Sets

In this section we define an important quantity associated with any algebraic set, its ideal. This ideal is one of the main ways in which properties of algebraic sets are defined and investigated.

Definition 2.2.1. *Let $\mathbb{F}$ be a field and X be an algebraic set defined over $\mathbb{F}$ with $X \subseteq \mathbb{A}^n(\mathbb{F})$.*

Let

$$I(X) = \{f \in \mathbb{F}[x_1, x_2, \ldots, x_n] : f(x) = 0 \ \forall \ x \in X\} \tag{2.8}$$

This is the set of all polynomials that vanish on X. We call $I(X)$ the ideal of X.

Example 2.2.2. *Let $\mathbb{F}$ be a field, $X = V(S)$ be an algebraic set defined over $\mathbb{F}$, and let $I(X)$ be the ideal of X. If $S = \{y - x^2\}$, then we notice that*

$$I(X) \ni y - x^2, \quad 2y - 2x^2, \quad \pi y - \pi x^2, \quad xy - x^3, \ldots \tag{2.9}$$

In fact, $I(X) = \{ay - ax^2 : a \in \mathbb{F}[x, y]\}$.

Proposition 2.2.3. *Let X be an algebraic set. Then $I(X)$ is an ideal in the algebraic sense.*

Proof. To prove that a subset of polynomials is an ideal, we must show that the set is closed under addition and that if $f(x_1, \ldots, x_n) \in I(X)$ and $g(x_1, \ldots, x_n)$ is a polynomial then $(f \cdot g)(x_1, \ldots, x_n) \in I(X)$. First we show that if

$$f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in I(X), \tag{2.10}$$

then $f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n) \in I(X)$.

Let $(a_1, \ldots, a_n) \in X$. If $f(a_1, \ldots, a_n), g(a_1, \ldots, a_n) \in I(X)$ then by Definition 2.2.1, $f(a_1, \ldots, a_n) = 0$ and $g(a_1, \ldots, a_n) = 0$. We can add f and g and evaluate at $(a_1, \ldots, a_n)$ to find the result

$$(f + g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0 \tag{2.11}$$

for $(a_1, \ldots, a_n) \in X$, so the set is closed under addition.

Now we show that if $f(x_1, \ldots, x_n) \in I(X)$ and $g(x_1, \ldots, x_n)$ is any polynomial, then $f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n) \in I(X)$. If $f(x_1, \ldots, x_n) \in I(X)$ then by Definition 2.2.1, $f(a_1, \ldots, a_n) = 0$ for $(a_1, \ldots, a_n) \in X$. We multiply f by a polynomial g and evaluate at $(a_1, \ldots, a_n)$ to get

$$(f \cdot g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0 \cdot g(a_1, \ldots, a_n) = 0, \tag{2.12}$$

for $(a_1, \ldots, a_n) \in X$, so $f \cdot g$ in the ideal $I(X)$ (also by Definition 2.2.1). We have shown that the subset of polynomials is closed under addition and that if

$f(x_1, \dots, x_n) \in I(X)$ and $g(x_1, \dots, x_n)$ is a polynomial then $(f \cdot g)(x_1, \dots, x_n) \in I(X)$, so the subset of polynomials is an ideal. □

We end with a proposition that illustrates the importance of this ideal to the theory of algebraic sets.

Proposition 2.2.4 (Exercise 1.16 of [3]). *Let $\mathbb{F}$ be a field and let V and W be algebraic sets in $\mathbb{A}^n(\mathbb{F})$. Then $V = W$ if and only if $I(V) = I(W)$.*

2.3 Reducibility and Irreducibility

An important property of an algebraic set is whether it is reducible or irreducible. This distinction will inform the definition of affine varieties, which we introduce at the end of this section.

We begin by defining reducible algebraic sets.

Definition 2.3.1. *Let X be an algebraic set. If $X = X_1 \cup X_2$ with X_1, X_2 two nonempty algebraic sets and $X \neq X_1, X \neq X_2$, then X is reducible. Otherwise, X is irreducible.*

Whether X is irreducible depends on a certain property of its ideal.

Proposition 2.3.2 (Proposition 1 of Section 1.5 of [3]). *Let X be an algebraic set and let $I(X)$ be the ideal of X. X is irreducible if and only if $I(X)$ is a prime ideal.*

Example 2.3.3. *Let $V(X) = \{(0,0), (1,1)\}$. This is reducible since $X = X_1 \cup X_2$, where X_1 and X_2 are:*

$$X_1 = (0,0) = V(\{x, y\}) \tag{2.13}$$

and

$$X_2 = (1,1) = V(\{x-1, y-1\}). \tag{2.14}$$

While when $S = \{y - x^2\}$, $V(S)$ is irreducible by Proposition 2.3.2 because $y - x^2$ is a prime polynomial. As such, the ideal it generates is prime.

We are now ready to define our main object of study, with which we will be working for the remainder of this chapter.

Definition 2.3.4. *An affine variety is an irreducible algebraic set.*

2.4 Coordinate Rings

In this section, we begin by defining the coordinate ring of an affine variety. This will form the set of regular functions on the variety. From there, we define various other sets of functions of interest on a variety.

Definition 2.4.1. *Let V be an affine variety defined over a field $\mathbb{F}$, by which we mean that $V \subseteq \mathbb{A}^n(\mathbb{F})$ for some n. The coordinate ring of V is defined to be*

$$\Gamma(V) = \mathbb{F}[x_1, \dots, x_n]/I(V). \tag{2.15}$$

Because V is a variety, its ideal $I(V)$ is prime and therefore $\Gamma(V)$ is a domain. As a consequence $\Gamma(V)$ has no zero divisors, so we can form its field of fraction:

Definition 2.4.2. *Let V be an affine variety and let $\Gamma(V)$ be its coordinate ring. We define $k(V)$, the field of fractions of $\Gamma(V)$, to be the function field of V:*

$$k(V) = \left\{ f = \frac{a}{b} : a, b \in \Gamma(V) \right\}. \tag{2.16}$$

Remark 2.4.3. *If $f \in k(V)$ then the representation $f = \frac{a}{b}$ is not unique. Indeed, let $V = V(x_0x_3 - x_1x_2)$. Then we have*

$$f = \frac{x_0}{x_1} = \frac{x_2}{x_3} \tag{2.17}$$

where $x_0, x_1, x_2, x_3 \in \Gamma(V)$, as we will se in Example 2.4.5 below.

Definition 2.4.4. *Let V be an affine variety, $\Gamma(V)$ be the coordinate ring of V, and let $k(V)$ be the function field of V. We say that $f \in k(V)$ is defined at $P \in V$ if there exist $a, b \in \Gamma(V)$ with $f = \frac{a}{b}$ and $b(P) \neq 0$. If f is not defined at P then f has a pole at P.*

Example 2.4.5. *Let $V = V(x_0x_3 - x_1x_2)$, $\Gamma(V) = \mathbb{F}[x_0, x_1, x_2, x_3]/(x_0x_3 - x_1x_2)$ and let $k(V)$ be the function field of V. On V, $x_0x_3 - x_1x_2 = 0$, so:*

$$x_0x_3 = x_1x_2 \tag{2.18}$$

$$x_0 = (x_1x_2)/x_3 \tag{2.19}$$

$$\frac{x_0}{x_1} = \frac{x_2}{x_3}. \tag{2.20}$$

As a consequence, $f(x_0, x_1, x_2, x_3) = \frac{x_0}{x_1}$ and $g(x_0, x_1, x_2, x_3) = \frac{x_2}{x_3}$ represent the same element of $k(V)$.

We have that $P = (0, 0, 1, 1) \in V$. Then $f = \frac{x_0}{x_1} = \frac{x_2}{x_3}$ is defined at P because $f = \frac{x_2}{x_3}$ and $x_3(0, 0, 1, 1) = 1 \neq 0$. However, one can show that if $x_1 = x_3 = 0$, then f is not defined at P. For example f has a pole at $x = (1, 0, 1, 0) \in V$.

Definition 2.4.6. *Let V be an affine variety and let $k(V)$ be the function field of V. Let P be a point on V. Let $\mathcal{O}_P(V)$ be the set of functions in $k(V)$ that are defined at*

P. $\mathcal{O}_P(V)$ is called the local ring of V at P.

In summary, we can say that $\Gamma(V)$ contains the functions that are defined at every point of V, $\mathcal{O}_P(V)$ contains the functions that are defined at a fixed point P, and $k(V)$ contains the functions that are defined at some points of V, but not necessarily everywhere. Therefore we have the relation

$$\Gamma(V) \subset \mathcal{O}_P(V) \subset k(V). \tag{2.21}$$

.

Definition 2.4.7. *Let V be an affine variety, P be a point on V, and let $k(V)$ be the function field of V. Let $\mathcal{O}_P(V)$ be the local ring of V at P We define the maximal ideal of V at P to be*

$$m_P(V) = \{f \in k(V) : f(P) = 0\} \subset \mathcal{O}_P(V). \tag{2.22}$$

Example 2.4.8. *Let $V = \mathbb{A}^1(\mathbb{C})$, then $I(V) = (0)$ because the only polynomial that vanishes at all points of $\mathbb{C} = \mathbb{A}^1(\mathbb{C})$ is the zero polynomial. Then we have $\Gamma(V) = \mathbb{C}[x]/(0) = \mathbb{C}[x]$ and $k(V) = \mathbb{C}(x)$, the field of rational functions.*

If P is the point $x = 0$ on V, then $\mathcal{O}_P(V)$ is the ring of all rational functions without a factor of x in the denominator.

Let $f \in \mathcal{O}_P(V)$. Recall from calculus that a rational function is infinitely differentiable on its domain. Therefore, we can write a Taylor series centered at $x = 0$ for f since $x = 0$ is in the domain.

For example,

$$\frac{1}{1-x} = 1 + x + x^2 + ... \in \mathcal{O}_P(V) \tag{2.23}$$

Based on this, we can say $\mathcal{O}_P(V) = \{$*all rational functions with a Taylor series centered at* $x = 0\}$.

Now let $\frac{f(x)}{g(x)} \in k(V)$, *then*

$$\frac{f(x)}{g(x)} = \frac{f(x)}{x^m h(x)} \tag{2.24}$$

for some nonnegative integer m, *with* $\frac{f(x)}{h(x)} \in \mathcal{O}_P(V)$. *We conclude that the elements of* $k(V)$ *are of the form*

$$a_{-m}x^{-m} + a_{-m+1}x^{-m+1} + \ldots + a_0 + a_1x + \ldots \tag{2.25}$$

for some nonnegative integer m.

We summarize the discussion in the following table:

Elements of	have the form
$\Gamma(V)$	$\sum\limits_{i=0}^{m} a_ix^i$
$\mathcal{O}_P(V)$	$\sum\limits_{i=0}^{\infty} a_ix^i$
$k(V)$	$\sum\limits_{i=-m}^{\infty} a_ix^i$

In the table above, although all elements are of that form, we note that not all elements of that form belong to the set. For example, $\sum\limits_{i=0}^{\infty} n!x^n$ *is of the form* $\sum\limits_{i=0}^{\infty} a_ix^i$,*but it is not an element of* $\mathcal{O}_P(V)$ *since it does not represent a rational function.*

2.5 Affine Plane Curves

We now turn our attention to curves that are a subset of $\mathbb{A}^2$. Not only are they some of the simplest curves, but as we restrict our attention to the case of genus 2 they are the only curves we need to consider in this work. In this section we describe several of their important properties.

Definition 2.5.1. *Let $\mathbb{F}$ be a field. Two polynomials $f(x,y), g(x,y) \in \mathbb{F}[x,y]$ are said to be equivalent if there exists a nonzero $\lambda \in \mathbb{F}$ such that $f(x,y) = \lambda g(x,y)$. This forms an equivalence relation on the set of polynomials in $\mathbb{F}[x,y]$. An affine plane curve is an equivalence class of such nonconstant polynomials, via $C = V(f(x,y))$, for any $f(x,y)$ in the equivalence class.*

In other words, an affine plane curve is simply an affine variety in $\mathbb{A}^2$ which is not a point. We are interested only in a certain kind of nice plane curves, which we now define.

Definition 2.5.2. *Let C be a plane curve given by the polynomial $f(x,y) = 0$. A point $P = (x,y)$ on C is simple if*

$$\frac{\partial f}{\partial x}(P) \neq 0 \tag{2.26}$$

or

$$\frac{\partial f}{\partial y}(P) \neq 0. \tag{2.27}$$

Then our nice curves are:

Definition 2.5.3. *A plane curve with only simple points is called nonsingular.*

Recall that we define the maximal ideal of a variety at a point P in Definition 2.4.7. When C is a plane curve and P is a simple point on C, the ideal is especially pleasing:

Proposition 2.5.4. *Let C be a plane curve and P be a simple point on C. Then the maximal ideal of C at P is a principal ideal.*

Proof. By [3, Theorem 1 of Section 3.2], P is a simple point on C if and only if $\mathcal{O}_P(C)$ is a discrete valuation ring. By definition (see [3, Proposition 4 of Section 2.5] and the discussion that follows), the maximal ideal of a discrete valuation ring is maximal. □

In turn, the generators of this principal ideal play an important role in the theory; in particular we will use them in Section 3.3 when we define the genus of C.

Definition 2.5.5 (Proposition 4 of Section 2.5 of [3])**.** *Let C be a plane curve and P be a simple point on C. Then any generator of the maximal ideal of C at P is called a uniformizing parameter of C at P.*

The uniformizing parameter of a curve at a point is crucial to the definition of the order of vanishing of a function at that point.

Theorem 2.5.6 (Proposition 4 of Section 2.5 of [3])**.** *Let C be a plane curve, P a simple point on C, and t a uniformizing parameter of C at P. Then every $z \in k(C)$ can be written uniquely as $z = u \cdot t^n$ where $u \in \mathcal{O}_P(C)$ but $u \notin m_P(C)$ (so $u(P) \neq 0$) and n is an integer.*

The significance of this theorem is the following:

Definition 2.5.7. *Let C be a plane curve and let P be a simple point on C. If $f \in k(C)$ then the order of vanishing of f at P, $\mathrm{ord}_P(f)$, is the integer n given by Theorem 2.5.6.*

Chapter 3

Projective Varieties and Curves

The focus of this thesis is projective varieties and more precisely, projective curves, which we introduce in this chapter. We begin by presenting the projective space in Section 3.1. We then define projective plane curves, birational equivalence, and weighted projective plane curves in Section 3.2. We will use birational equivalence in Chapter 4 to determine which curves are necessary to include in order to ensure we have at least one curve from each isomorphism class. Furthermore, it will turn out that the curves we classify in Chapters 5 and 6 are all weighted projective plane curves. In Section 3.3 we define an important invariant of curves, the genus and give formulae to compute it for plane curves. Finally, in Section 3.4 we describe the point counting process we will use to later sort curves into isogeny classes. Once again, we have used reference [4] for standard definitions and theorems, and [5] for facts pertaining to weighted projective curves.

3.1 Projective Space

In this section we introduce projective space, which is the ambient space in which projective varieties live. In other words, the space $\mathbb{P}^n$ we introduce below plays for projective varieties the role that the space $\mathbb{A}^n$ plays for affine varieties.

Definition 3.1.1. *Let $\mathbb{F}$ be a field. We define the projective line over $\mathbb{F}$, $\mathbb{P}^1(\mathbb{F})$, to be*

$$\mathbb{P}^1(\mathbb{F}) = \{(X,Y) : X, Y \in \mathbb{F}, (X,Y) \neq (0,0)\}/\sim \tag{3.1}$$

where $(X_1, Y_1) \sim (X_2, Y_2)$ if there is $\lambda \neq 0, \lambda \in \mathbb{F}$ with

$$X_1 = \lambda X_2, \tag{3.2}$$

$$Y_1 = \lambda Y_2. \tag{3.3}$$

Example 3.1.2. *If $\mathbb{F} = \mathbb{R}$, then*

$$(1,2) \sim (2,4) \sim (-1,-2) \sim (1/2,1) \tag{3.4}$$

under the equivalence relation given in Definition 3.1.1.

To illustrate $\mathbb{P}^1$ more concretely, we give a natural representative for each equivalence class belonging to $\mathbb{P}^1$. Let $\mathbb{F}$ be a field and let first $(X,Y) \in \mathbb{P}^1(\mathbb{F})$ be such that $Y \neq 0$. In that case, taking $\lambda = 1/Y$, we have

$$(X,Y) \sim (X/Y,1) \sim (x,1), \tag{3.5}$$

where we let $x = X/Y$.

Now let $(X, 0) \in \mathbb{P}^1(\mathbb{F})$. If $(X, 0) \in \mathbb{P}^1(\mathbb{F})$, it follows that $X \neq 0$, since $(X, Y) \neq (0, 0)$. In that case, letting $\lambda = 1/X$, we have

$$(X, Y) \sim (1, 0). \tag{3.6}$$

Combining these, $\mathbb{P}^1(\mathbb{F})$ can be written as:

$$\mathbb{P}^1(\mathbb{F}) = \{(X, 1) : X \in \mathbb{F}\} \cup \{(0, 1)\} \tag{3.7}$$

or, more simply,

$$\mathbb{P}^1(\mathbb{F}) = \mathbb{F} \cup \infty \tag{3.8}$$

where ∞ is the point $(0, 1)$. This explains why we often think of $\mathbb{P}^1$ as the union of $\mathbb{A}^1$ with a point "at infinity."

We now move to $\mathbb{P}^2$, the projective plane.

Definition 3.1.3. *Let $\mathbb{F}$ be a field. We define the projective plane over $\mathbb{F}$, $\mathbb{P}^2(\mathbb{F})$, to be*

$$\mathbb{P}^2(\mathbb{F}) = \{(X, Y, Z) : X, Y, Z \in \mathbb{F}, (X, Y, Z) \neq (0, 0, 0)\}/\sim \tag{3.9}$$

where $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ if there exists $\lambda \neq 0, \lambda \in \mathbb{F}$ with

$$X_2 = \lambda X_1, \tag{3.10}$$

$$Y_2 = \lambda Y_1, \tag{3.11}$$

$$Z_2 = \lambda Z_1. \tag{3.12}$$

Once again, to illustrate $\mathbb{P}^2$ more concretely, we give a natural representative for each equivalence class belonging to $\mathbb{P}^2$. Let $\mathbb{F}$ be a field and let first $(X, Y, Z) \in \mathbb{P}^2(\mathbb{F})$ be such that $Z \neq 0$. In that case, taking $\lambda = 1/Z$, we have

$$(X, Y, Z) \sim (X/Z, Y/Z, 1) \sim (x, y, 1), \tag{3.13}$$

where we let $x = X/Z$ and $y = Y/Z$. We point out that this notation will appear again in Definition 3.2.1.

Now let $(X, Y, 0) \in \mathbb{P}^2(\mathbb{F})$ and suppose that $Y \neq 0$. In this case, taking $\lambda = 1/Y$, we have

$$(X, Y, Z) \sim (X/Z, 1, 0) \sim (x, 1, 0), \tag{3.14}$$

where this time we let $x = X/Y$. Finally, note that if $(X, 0, 0) \in \mathbb{P}^2(\mathbb{F})$, it follows that $X \neq 0$, since $(X, Y, Z) \neq (0, 0, 0)$, in that case, letting $\lambda = 1/X$, we have

$$(X, Y, Z) \sim (1, 0, 0). \tag{3.15}$$

We conclude that $\mathbb{P}^2(\mathbb{F}) = \mathbb{F}^2 \cup \mathbb{F} \cup (1, 0, 0)$.

Alternatively, if $Z = 0$, we notice that sending the triple $(X, Y, 0)$ to (X, Y) in $\mathbb{P}^1$ gives an isomorphism, and therefore

$$\mathbb{P}^2(\mathbb{F}) = \mathbb{F}^2 \cup \mathbb{P}^1(\mathbb{F}). \tag{3.16}$$

We often think therefore of $\mathbb{P}^2$ as $\mathbb{A}^2$ with a copy of $\mathbb{P}^1$ “at infinity.”

$\mathbb{P}^1$ and $\mathbb{P}^2$ are examples of a more general space. Finally, we give the definition of the n-dimensional projective space.

Definition 3.1.4. *Let $\mathbb{F}$ be a field. We define the n-dimensional projective space over $\mathbb{F}$, $\mathbb{P}^n(\mathbb{F})$, to be*

$$\mathbb{P}^n(\mathbb{F}) = \{(X_0, \ldots, X_n) : X_0, \ldots, X_n \in \mathbb{F}, (X_0, \ldots, X_n) \neq (0, \ldots, 0)\}/\sim \tag{3.17}$$

where $(X_0, X_1, \ldots, X_n) \sim (X_0', X_1', \ldots, X_n')$ if there exists $\lambda \neq 0, \lambda \in \mathbb{F}$ with

$$X_0 = \lambda X_0', \tag{3.18}$$

$$X_1 = \lambda X_1', \tag{3.19}$$

$$\ldots, \tag{3.20}$$

$$X_n = \lambda X_n'. \tag{3.21}$$

We note that as before, we can show that $\mathbb{P}^n(\mathbb{F}) = \mathbb{F}^n \cup \mathbb{P}^{n-1}(\mathbb{F})$. In this case we think of $\mathbb{P}^n$ as $\mathbb{A}^n$ with a copy of $\mathbb{P}^{n-1}$ “at infinity.”

3.2 Projective Plane Curves

In this thesis we focus on a special kind of projective varieties, weighted projective plane curves. These objects are a generalization of projective plane curves, which are the analogues of the affine plane curves we have introduced in Section 2.5. We therefore begin by introducing projective plane curves for simplicity. We then introduce weighted projective space, and give a very quick introduction to the theory of weighted projective curves and varieties, following our presentation for affine varieties in Chapter 2.

3.2.1 Projective Plane Curves

Although projective plane curves may be defined intrinsically, in this work to help exposition we define them as the homogenization of affine plane curves. In fact, as argued in Fulton [3, Section 4.3], there is a natural, general, one-to-one correspondence between projective varieties in $\mathbb{P}^n$ that are not contained in the space $\mathbb{P}^{n-1}$ "at infinity" and affine varieties in $\mathbb{A}^n$. We present here this correspondence in the special case of plane curves.

Recall from Definition 2.5.1 that an affine plane curve is given by a single polynomial in two variables. Similarly, a projective plane curve is given by a single homogeneous polynomial in three variables. Furthermore, given an affine plane curve given by a polynomial f, we can obtain the polynomial of associated projective plane curve in the following manner:

Definition 3.2.1 (Definition 1.18 of [4])**.** *Let $\mathbb{F}$ be a field. We associate to any polynomial f of degree d in $\mathbb{F}[x, y]$ the homogeneous polynomial $f^* \in \mathbb{F}[X, Y, Z]$, given by*

$$f^*(X, Y, Z) = Z^d f(X/Z, Y/Z). \tag{3.22}$$

We note that in this case, f^* is homogeneous of degree d.

We can now easily define the notion of projective plane curve:

Definition 3.2.2 (Definition 1.18 of [4])**.** *Let $f \in \mathbb{F}[x, y]$ define an affine plane curve. Then the projective plane curve associated to this curve is given by the homogeneous equation $f^*(X, Y, Z) = 0$ in $\mathbb{P}^2(\mathbb{F})$. In other words, a projective plane curve C is* *given by*

$$C = \{(X, Y, Z) \in \mathbb{P}^2(\mathbb{F}) : f^*(X, Y, Z) = 0\}. \tag{3.23}$$

We note that given a projective curve C^* given by a homogeneous polynomial f^*, we can obtain the associated affine curve C by dehomogenizing the polynomial f^* to obtain a polynomial f where $f(x, y) = f^*(x, y, 1)$.

Example 3.2.3. *Consider the affine plane curve $y = x^2$, given by $f(x, y) = y - x^2$. Then the associated homogeneous polynomial is*

$$\begin{aligned} f^*(X, Y, Z) &= Z^2 f\left(\frac{Y}{Z}, \frac{X}{Z}\right) \qquad (3.24) \\ &= Z^2\left(\frac{Y}{Z} - \frac{X^2}{Z^2}\right) \qquad (3.25) \\ &= ZY - X^2. \qquad (3.26) \\ & \qquad (3.27) \end{aligned}$$

We often write this as

$$ZY = X^2. \tag{3.28}$$

We now describe the points of the projective curve $f^*(X, Y, Z) = ZY - X^2 = 0$. If $Z = 0$, $X^2 = 0$ so $X = 0$. We know that $(X, Y, Z) \neq (0, 0, 0)$, so $Y \neq 0$. Therefore, when $Z = 0$, we have the single point $(0, Y, 0) \sim (0/Y, Y/Y, 0/Y) \sim (0, 1, 0)$ "at infinity." If $Z \neq 0$, then $(X, Y, Z) \sim (\frac{X}{Z}, \frac{Y}{Z}, 1)$ and letting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ form the affine curve $y = x^2$.

In light of this correspondence, to a projective curve C^* with associated affine curve C, we can therefore assign the function field $k(C)$. (This is not the standard definition of the function field of C^*, but it is equivalent.) This allows us to define:

Definition 3.2.4. *Two projective curves C_1^* and C_2^*, with respective associated affine curves C_1 and C_2, are birationally equivalent if and only if $k(C_1) \cong k(C_2)$.*

3.2.2 Weighted Projective Plane Curves

With this machinery in place, we are now ready to introduce weighted projective plane curves, which are how we will represent the curves we study in Chapters 4, 5, and 6.

Definition 3.2.5. *Let w_0, w_1, w_2 be three positive integers. We define*

$$\mathbb{P}(w_0, w_1, w_2) = \{(X, Y, Z) \in \mathbb{F}^3 : (X, Y, Z) \neq (0, 0, 0)\}/ \sim \tag{3.29}$$

where now $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ if there exists $\lambda \neq 0, \lambda \in \mathbb{F}$ such that

$$X_1 = \lambda^{w_0} X_2,$$
$$Y_1 = \lambda^{w_1} Y_2,$$
$$Z_1 = \lambda^{w_2} Z_2.$$

We note that $\mathbb{P}^2$ is just $\mathbb{P}(1, 1, 1)$.

Example 3.2.6. *Hyperelliptic curves of genus g are often naturally viewed as living in $\mathbb{P}(1, g + 1, 1)$. When $g = 2$, as in this work, the hyperelliptic curve therefore exists in the weighted projective space $\mathbb{P}(1, 3, 1)$. Explicitly, here the equivalence relation is*

$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ *if there is* $\lambda \neq 0, \lambda \in \mathbb{F}$ *with*

$$X_1 = \lambda X_2, \tag{3.30}$$

$$Y_1 = \lambda^3 Y_2, \tag{3.31}$$

$$Z_1 = \lambda Z_2. \tag{3.32}$$

With our ambient space in hand, we now proceed to quickly define the main quantities associated to weighted projective curves. As we saw in Section 2.2, the basic objects underlying the theory of affine varieties are polynomials. The weighted projective analogue are weighted-homogeneous polynomials, which we now introduce.

Definition 3.2.7 (Definition 3.0.7 of [5]). *Let* $\mathbb{F}[X_0, \ldots, X_n]$ *be the polynomial ring over* $\mathbb{F}$ *in* $n+1$ *variables, and let* $w_0, w_1, \ldots, w_n$ *be* $n+1$ *positive integers forming a vector of weights* $w = (w_0, w_1, \ldots, w_n)$*. Here we will consider the variable* X_i *to have weight* w_i*. Let* $f \in \mathbb{F}[X_0, \ldots, X_n]$*, then we say that* f *is* w*-weighted-homogeneous of degree* d *if each monomial in* f *is of weighted degree* d*, i.e. there exist* $c_i \in \mathbb{F}$ *and some* $m \in \mathbb{N}$ *such that*

$$f = \sum_{i=1}^{m} c_i \left(\prod_{j=0}^{n} x_j^{d_j^{(i)}} \right) \tag{3.33}$$

and, for all $0 \leq i \leq n$,

$$\sum_{j=0}^{m} w_j d_j^{(i)} = d. \tag{3.34}$$

To emphasize the weight of the variables, we write $f \in \mathbb{F}_w[X_0, \ldots, X_n]$*. Furthermore, we write* $\mathbb{F}_w[X_0, \ldots, X_n]_d \subset \mathbb{F}_w[X_0, \ldots, X_n]$ *to mean the additive group of all weighted-homogeneous polynomials of degree* d*.*

We now continue as in Chapter 2, and introduce the weighted projective version of every object we have introduced there, beginning with the notion of a weighted algebraic set:

Definition 3.2.8 (Definition 3.1.1 of [5])**.** *Let $S \subseteq \mathbb{F}_w[X_0, \ldots, X_n]$ be a set of homogeneous polynomials. Then the weighted projective algebraic set (associated to S) is*

$$V(S) = \{P \in \mathbb{P}(w_0, \cdots, w_n) : f(P) = 0 \textit{ for all } f \in S\}. \tag{3.35}$$

To such a set we can associate an ideal in the same way as we did in Definition 2.2.1, but restricting our attention to weighted homogeneous polynomials. (See [5, Definition 3.1.1], but note that there the author calls any algebraic set a variety and does not reserve the word "variety" for irreducible varieties.) In this setting, the ideal associated to a weighted projective algebraic set will be a weighted-homogeneous ideal by [5, Lemma 3.2.1] , where such an ideal is defined to be:

Definition 3.2.9 (Definition 3.0.9 of [5])**.** *We say that an ideal $I \lhd \mathbb{F}[X_0, \ldots, X_n]$ is w-weighted-homogeneous if it is generated by w-weighted homogeneous elements (of not necessarily the same degree).*

Then as in the theory of affine varieties, we can define a weighted projective algebraic set to be irreducible if it does not have a decomposition into nontrivial algebraic subsets. As before, this will correspond to the associated ideal being prime, where by [5, Lemma 3.0.12], a weighted homogeneous ideal is prime if and only if whenever $fg \in I$ with f and g two homogeneous polynomials, then $f \in I$ or $g \in I$. From there we may define the coordinate ring of a weighted projective variety:

Definition 3.2.10 (Definition 3.3.1 of [5])**.** *Let V be a non-empty weighted projective variety and let $I(V)$ be the ideal of that variety. Then define the weighted-homogeneous* *coordinate ring of V to be*

$$\Gamma(V) = \frac{\mathbb{F}[X_0, \ldots, X_n]}{I(V)}. \tag{3.36}$$

Finally, to recover the notion of the function field of V, which should coincide with the definition we gave for plane projective curves immediately before Definition 3.2.4, we define:

Definition 3.2.11. *Let V be an affine variety and let $\Gamma(V)$ be its coordinate ring. We define $k(V)$, the field of fractions $\Gamma(V)$, to be the function field of V:*

$$k(V) = \left\{ f = \frac{a}{b} : a, b \in \Gamma(V),\ a \text{ and } b \text{ homogeneous of the same degree} \right\}. \tag{3.37}$$

We can now define weighted projective plane curves in analogy to affine and projective plane curves:

Definition 3.2.12 (Definition 5.0.4 of [5])**.** *Let $f = f(X_0, X_1, X_2) \in \mathbb{F}_w[X_0, X_1, X_2]$ be an irreducible weighted-homogenous degree d polynomial. Then*

$$C_f = V(f) \subseteq \mathbb{P}(w_0, w_1, w_2) \tag{3.38}$$

is a degree-d weighted projective plane curve in $\mathbb{P}(w_0, w_1, w_2)$.

3.3 Differentials and the Genus

An important invariant of a projective curve is its genus; it is so important that in our later work we will organize the curves we enumerate by genus and base field. For a curve defined over $\mathbb{C}$, the genus is roughly the number of “handles” of the curve, but when the curve is defined over a finite field, as our curves will be, this intuition does not make sense. Instead, in order to define the genus, we must begin by giving the definition of a differential on a plane curve. We note that our definition of genus is standard, although for a more technical definition, we refer the reader to Definition 5.55 of [4].

Definition 3.3.1. *Let C be a weighted projective plane curve. We define $\Omega(C)$, the space of differentials of C, to be the quotient of the free $k(C)$-module on the symbols dx for $x \in k(C)$ by the relations:*

- *For any two $x, y \in k(C), d(x + y) = dx + dy$.*
- *For any $x \in k(C)$ and $\lambda \in \mathbb{F}, d(\lambda x) = \lambda dx$.*
- *For any two $x, y \in k(C), d(xy) = ydx + xdy$.*

We note that $\Omega(C)$ is both a $k(C)$-vector space and an $\mathbb{F}$-vector space if the curve C is defined over the field $\mathbb{F}$.

We now wish to define a subset of $\Omega(C)$, that of the holomorphic differentials. Recall that for C an affine plane curve, we defined a simple point and a uniformizing parameter in Definitions 2.5.2 and 2.5.5. Since these notions are local, they make sense for weighted projective curves as well.

Proposition 3.3.2. *Let C be a weighted projective plane curve, P a simple point on C, t a uniformizing parameter of C at P, and $\omega \in \Omega(C)$. Then there is $f \in k(C)$ such that $\omega = fdt$.*

Proof. By [3, Proposition 6 of Section 8.4], $\Omega(C)$ is one-dimensional over $k(C)$. □

This proposition will allow us to define the order of vanishing of a differential at a point.

Definition 3.3.3. *Let C be a weighted projective plane curve, P a simple point on C, and $\omega \in \Omega(C)$. Then the order of vanishing of ω on C at P, $\operatorname{ord}_P(\omega)$, is the order of vanishing of f on C at P, $\operatorname{ord}_P(f)$, for any f as in Proposition 3.3.2.*

With this definition, we are now ready to define the subset of $\Omega(C)$ that interests us.

Definition 3.3.4. *Let C be a weighted projective plane curve. Then the holomorphic differentials $\Omega^1(C)$ on C is the subset of elements ω of $\Omega(C)$ such that*

$$\operatorname{ord}_P(\omega) \geq 0 \quad \textit{for all } P \textit{ on } C. \tag{3.39}$$

With this somewhat complicated object in hand, it is now easy to define the genus:

Definition 3.3.5. *The genus of a (weighted projective plane) curve C defined over a field $\mathbb{F}$ is the dimension of $\Omega^1(C)$ as a vector space over the field $\mathbb{F}$.*

Thankfully, for plane curves there is an easy formula to compute the genus:

Theorem 3.3.6 (Theorem 5.3.6 of [5])**.** *Let C be a projective plane curve of degree d in $\mathbb{P}^2$ given by a polynomial $f^*(X, Y, Z) = 0$. If C is nonsingular then the curve has genus*

$$g = \frac{(d-1)(d-2)}{2}. \tag{3.40}$$

As we will be working with weighted projective curves, we must use the analagous result in this setting:

Theorem 3.3.7 (Theorem 5.3.7 of [5]). *Let C be a plane curve of degree d in the weighted projective plane $\mathbb{P}(w_0, w_1, w_2)$ given by a polynomial $f^*(X, Y, Z) = 0$. If C is nonsingular then the curve has genus*

$$g = \frac{1}{w_0 w_1 w_2}\left(\frac{(d-1)(d-2)}{2} - \left[\frac{b(C)}{2} + 1 - w_0 w_1 w_2\right]\right) \tag{3.41}$$

where $b(C)$ is given by

$$b(C) = (d-1)\sum_{i=1}^{3}(w_i - 1) + \sum_{i=1}^{3}\begin{cases}(w_i - 1) & \text{if } w_i | d;\\ \\ (w_0 w_1 w_2 - 1) & \text{if } w_i \not| d.\end{cases} \tag{3.42}$$

As we will see in Section 4.2, over a field of odd characteristic and when the genus is even, we can always write an affine model for a hyperelliptic curve of genus g of the form

$$y^2 = f(x),$$

for f of degree $2g+2$ or $2g+1$. However, the projectivization of this curve in the usual projective plane $\mathbb{P}^2$ is singular at infinity when the degree of f is strictly greater than 4. We can avoid this singularity by considering the weighted projective curve

$$Y^2 = f(X, Z)$$

in $\mathbb{P}(1, g+1, 1)$, where f is homogeneous of weight $2g+2$. This model is nonsingular. As an application of Theorem 3.3.7, we show that this model indeed gives a curve of genus g:

Example 3.3.8. *Let C be a plane curve given by a polynomial $f^*(X, Y, Z) = Y^2 -$*

$f(X,Z)$ for $f(X,Z)$ homogeneous of degree $2g+2$ and where Y is a variable of weight $g+1$. We apply Theorem 3.3.7 to find the genus of C. First, we note that $w_0 = 1, w_1 = g+1$ and $w_2 = 1$.

Next, we find $b(C)$:

$$b(C) = ((2g+2)-1)\sum_{i=1}^{3}(w_i - 1) + \sum_{i=1}^{3}\begin{cases} w_i - 1 & \textit{if } w_i|(2g+2); \\ w_0w_1w_2 - 1 & \textit{if } w_i \not|(2g+2). \end{cases}$$

$$b(C) = ((2g+2)-1)\sum_{i=1}^{3}(w_i - 1) + \sum_{i=1}^{3}(w_i - 1)$$

$$b(C) = (2g+1)((1-1)+(g+1-1)+(1-1)) + ((1-1)+(g+1-1)+(1-1))$$

$$b(C) = (2g+1)g + g$$

$$b(C) = 2g^2 + g + g$$

$$b(C) = 2g^2 + 2g.$$

Now, we find g_C, the genus of C:

$$
\begin{aligned}
g_C &= \frac{1}{w_0w_1w_2}\left(\frac{(d-1)(d-2)}{2} - \left[\frac{b(C)}{2} + 1 - w_0w_1w_2\right]\right)\\
g_C &= \frac{1}{1\cdot(g+1)\cdot 1}\left(\textit{(2g+2-1)}_{-}\textit{(2g+2-2)}2 - \left[\frac{2g^2+2g}{2} + 1 - (1\cdot(g+1)\cdot 1)\right]\right)\\
g_C &= \frac{1}{g+1}\left(\frac{(2g+1)(2g)}{2} - \left[\frac{2g^2+2g}{2} + 1 - (g+1)\right]\right)\\
g_C &= \frac{1}{g+1}\Big((2g+1)(g) - \big[(g^2+g) + 1 - g - 1\big]\Big)\\
g_C &= \frac{1}{g+1}\Big(2g^2 + g - \big[g^2 + g - g\big]\Big)\\
g_C &= \frac{1}{g+1}\Big(2g^2 + g - g^2\Big)\\
g_C &= \frac{1}{g+1}\Big(g^2 + g\Big)\\
g_C &= \frac{1}{g+1}(g(g+1))\\
g_C &= g.
\end{aligned}
$$

And indeed we see that the hyperelliptic curves we are considering have genus g.

3.4 Counting Points

As we will explain in Section 5.2, our method for sorting curves into isogeny classes will be to count their points over certain field extensions. While we will use Magma to count the points of our curves in this project, in this section we work out a short example to show explicitly what we mean. We first do the example by hand, and then demonstrate how we would complete the same process in Magma.

Example 3.4.1. *Consider the projective curve $ZY^2 = X^3 + Z^3$ over the field $\mathbb{F}_5$. We* *now count its rational points. We do this in two steps.*

First, we will count the number of points with $Z = 0$*. This is the easiest task, because there is only one. Indeed if* $Z = 0$*, then* $X^2 = 0$*, so* $X = 0$*, and the only point at infinity is* $(0, Y, 0) \sim (0, 1, 0)$*.*

Then, in $\mathbb{F}_5^2$*, we will count the points where* $Z \neq 0$*. In that case* $(X, Y, Z) \sim (\frac{X}{Z}, \frac{Y}{Z}, 1)$ *so letting* $x = \frac{X}{Z}$ *and* $y = \frac{Y}{Z}$*, these are exactly the solutions to* $y^2 = x^3 + 1$ *when* $x, y \in \mathbb{F}_5$*. We will perform these steps both by hand and with Magma.*

In Table 3.1, we have found all possible values of x *and* x^3 *in* $\mathbb{F}_5$*. We have done the same in Table 3.2 for values of* y *and* y^2*.*

Table 3.1: Values of x*,* x^3 *in* $\mathbb{F}_5$

x	0	1	2	3	4
x^3	0	1	3	2	4

Table 3.2: Values of y*,* y^2 *in* $\mathbb{F}_5$

y	0	1	2	3	4
y^2	0	1	4	4	1

Starting with $x = 0$*:*

$$x = 0 \implies x^3 = 0. \tag{3.43}$$

Therefore,

$$y^2 = 0 + 1 = 1. \tag{3.44}$$

According to Table 3.2, $y^2 = 1$ *when* $y = 1$ *or* $y = 4$*. Therefore, the two solutions with* $x = 0$ *are (0,1) and (0,4).*

For $x = 1$*:*

$$x = 1 \implies x^3 = 1. \tag{3.45}$$

Therefore,

$$y^2 = 1 + 1 = 2. \tag{3.46}$$

According to Table 3.2, there is no value y *in* $\mathbb{F}_5$ *such that* $y^2 = 2$*, and therefore no point with* $x = 1$*.*

For $x = 2$*:*

$$x = 2 \implies x^3 = 3. \tag{3.47}$$

Therefore,

$$y^2 = 3 + 1 = 4. \tag{3.48}$$

According to Table 3.2, $y^2 = 4$ *when* $y = 2$ *or* $y = 3$*. Therefore, the two solutions with* $x = 2$ *are* $(2, 2)$ *and (2,3).*

For $x = 3$*:*

$$x = 3 \implies x^3 = 2. \tag{3.49}$$

Therefore,

$$y^2 = 2 + 1 = 3. \tag{3.50}$$

According to Table 3.2, there is no value y *in* $\mathbb{F}_5$ *for* y *such that* $y^2 = 3$*, and therefore no point with* $x = 1$*.*

For $x = 4$*:*

$$x = 4 \implies x^3 = 4. \tag{3.51}$$

Therefore,

$$y^2 = 4 + 1 = 5 = 0. \tag{3.52}$$

According to Table 3.2, $y^2 = 0$ when $y = 0$. Therefore, the solution with $x = 4$ is $(4, 0)$.

We now show how to obtain these solutions using the software Magma:

```
F5 := FiniteField(5);

testlist := [[x,y] :  x,y in $\mathbb{F}_5$ | $y^2$ eq $x^3+1$];

testlist
```

Which gives the output:

```
[0,1],[0,4],[2,2],[2,3],[4,0]
```

In our calculations by hand and according to Magma, we have found six total solutions, including the single solution when $Z = 0$:

$$(0, 1, 0), (0, 1, 1), (0, 4, 1), (2, 2, 1), (2, 3, 1), (4, 0, 1).$$

Chapter 4

Generating Hyperelliptic Curves

Our first task is to list models of hyperelliptic curves that we will later sort into isogeny and isomorphism classes in Chapters 5 and 6. To obtain complete lists, we need at least one model from each isomorphism class. This chapter outlines the process of generating models of hyperelliptic curves of a given genus and defined over a given finite field. It details both the theorems used to identify which models are necessary to include, as well as the methodology behind the code created to automatize the process. Unless otherwise noted, the source used for this chapter is [4].

In Section 4.1, we define the general form of a hyperelliptic curve and explain how our code will generate the necessary lists of models. In Section 4.2 we will identify which models are necessary to include based on the cardinality of the base field being considered.

4.1 Automation in Magma

We define a hyperelliptic curve to be a projective curve C admitting a map of degree two to $\mathbb{P}^1$, the projective line. We note that this map may only be definable over the algebraic closure of the base field of C. Using the Riemann-Roch theorem, one can show that every curve of genus 2 is hyperelliptic in this sense. Therefore, if we aim to enumerate curves of genus 2, we can focus on enumerating hyperelliptic curves.

It is well-known that over an algebraically closed field of odd characteristic, a hyperelliptic curve can be given the simple affine model $y^2 = f(x)$, for f of degree $2g + 1$. However, in this work we focus on finite fields, which are not algebraically closed, and include fields of characteristic two. As such, listing the possible models for hyperelliptic curves is much more delicate. We first note that a hyperelliptic curve can be guaranteed to have one of the "standard" models, $y^2 = f(x)$ in odd characteristic or $y^2 + h(x)y = f(x)$ in even characteristic, only if the genus is even [12, Footnote 1]. (In that case one can guarantee that the quotient of the hyperelliptic curve by its hyperelliptic involution has a rational point over the base field of the hyperelliptic curve.) Thankfully, as we work in genus 2 here, all curves we consider will have such a standard model.

In this case, we can use the following corollary:

Corollary 4.1.1 (Corollary 7.93 of [4]). *Let $\mathbb{F}$ be a field, $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$, and let genus $g \geq 2$. A hyperelliptic curve C_1 of genus g defined over $\mathbb{F}$ is birationally equivalent to a curve*

$$C_2 = V(y^2 + h(x)y + f(x)), \tag{4.1}$$

where $h(x) \in \mathbb{F}[x]$ is a polynomial of degree at most $g+1$, $f(x) \in \mathbb{F}[x]$ is a monic polynomial of degree $2g+1$ or $2g+2$, and there are no solutions $(x, y) \in \overline{\mathbb{F}} \times \overline{\mathbb{F}}$ which simultaneously satisfy the equation $y^2 + h(x)y = f(x)$ and the partial derivative equations $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$.

In light of Corollary 4.1.1, to attain our goal of generating a list of models containing at least one representative for each isomorphism class of hyperelliptic curves of a given genus, we must first generate all possible $f(x)$ and $h(x)$ polynomials satisfying the conditions described in Corollary 4.1.1 and with coefficients in a given finite field. Then, we must systematically form pairs $(f(x), h(x))$ that determine hyperelliptic curves of the form $y^2 + yh(x) = f(x)$ which satisfy the partial derivative conditions noted in Corollary 4.1.1. To accomplish this goal we write two functions which we now describe.

4.1.1 `AllPolys`$(\mathbb{F}_q, d)$ Function

Our first task is creating a function that can form all possible polynomials of a certain degree, with coefficients in a given finite field. Our function `AllPolys`$(\mathbb{F}_q, d)$ does so in several steps. Given a degree d and a finite field $\mathbb{F}_q$, we recall that the polynomial will have the form

$$a_d x^d + a_{d-1} x^{d-1} + a_{d-2} x^{d-2} + \cdots + a_1 x + a_0. \tag{4.2}$$

To obtain this form, we begin by generating all possible ordered lists of $d+1$ elements of $\mathbb{F}_q$; these will form the $d+1$ coefficients of the polynomial. However, whenever $a_d = 0$, we will obtain a polynomial of degree strictly less than d, which we do not want to output. Therefore as a last step we choose only the polynomials of degree equal to d to include in the output list.

Example 4.1.2. *Consider the case of degree $d = 2$ and the finite field $\mathbb{F}_2$. The polynomials we want to output have the form*

$$a_2x^2 + a_1x + a_0, \tag{4.3}$$

where the coefficients a_2, a_1, a_0 are the elements of $\mathbb{F}_2$. As such, they can take the values 0 and 1. We find all possible ordered lists of (a_2, a_1, a_0) to be

$$(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1). \tag{4.4}$$

These ordered lists generate the polynomials

$$0, x^2, x, x^2 + x, 1, x^2 + 1, x + 1, x^2 + x + 1. \tag{4.5}$$

Finally, we include only the polynomials whose degree is $d = 2$. Therefore, for degree $d = 2$ and finite field $\mathbb{F}_2$, we obtain the 4 polynomials

$$\{x^2, x^2 + x, x^2 + 1, x^2 + x + 1\}. \tag{4.6}$$

The function `AllPolys`$(\mathbb{F}_q, d)$ returns a list of polynomials of degree d. By iterating the function over different values of d, we can obtain all models described in Corollary 4.1.1 for any genus g and finite field $\mathbb{F}_q$.

4.1.2 $\texttt{MyHyperCurves}(\mathbb{F}_q, g)$ Function

We use the $\texttt{MyHyperCurves}(\mathbb{F}_q, g)$ function to generate hyperelliptic curves of genus g defined over a finite field $\mathbb{F}_q$. The first step is to define the $f(x)$ and $h(x)$ polynomials.

Our $f(x)$ polynomials are a concatenation (`cat` in Magma) of two lists of polynomials. Given a genus g and finite field $\mathbb{F}_q$, the first list is all the polynomials of degree $d = 2g + 1$ with coefficients in $\mathbb{F}_q$. The second list is all the polynomials of degree $d = 2g + 2$ with coefficients in $\mathbb{F}_q$. In Magma, this is written as

$$\texttt{AllPolys}(\mathbb{F}_q, 2g + 1) \text{ cat } \texttt{AllPolys}(\mathbb{F}_q, 2g + 2). \tag{4.7}$$

Our $h(x)$ polynomials are a concatenation of many lists of polynomials. We will once consider only polynomials with coefficients in $\mathbb{F}_q$. The degrees will now be $d = 0, 1, 2, \cdots (g+1)$. We then concatenate these lists together. A simplified notation of this process in Magma is

$$\texttt{AllPolys}(\mathbb{F}_q, 0) \text{ cat } \texttt{AllPolys}(\mathbb{F}_q, 1) \text{ cat } \cdots \text{ cat } \texttt{AllPolys}(\mathbb{F}_q, g + 1). \tag{4.8}$$

Now that we have the $f(x)$ and $h(x)$ polynomials, we can form hyperelliptic curves. Some combinations of $f(x)$ and $h(x)$ do not form hyperelliptic curves as they do not satisfy the partial derivative conditions. We use a Magma function, $\texttt{IsHyperellipticCurve}(f(x), h(x))$, to test every possible combination of $f(x)$ and $h(x)$ and if they form a hyperelliptic curve, we include them in the list. The function $\texttt{MyHyperCurves}(\mathbb{F}_q, g)$ returns this list for a given finite field $\mathbb{F}_q$ and genus g.

4.2 Identifying Necessary Models

The process described in Section 4.1 can be used to form a complete list of models of hyperelliptic curves of any genus and over any finite field. However, if the goal is only to give one representative for each isomorphism classes of curves, the list can be considerably shortened when working over a field of odd characteristic. We note that this is not the case for fields of even characteristic, in which case we must list all suitable pairs $(f(x), h(x))$ according to Corollary 4.1.1, to ensure that we obtain a representative from each isomorphism class.

Indeed, the method we give above generates a list that contains several duplicates that are birationally equivalent to each other. We use the following theorem in order to limit this kind of replication:

Theorem 4.2.1 (Theorem 7.94 of [4]). *Let $\mathbb{F}$ be an algebraically closed field of characteristic zero or of odd characteristic. Then a curve of genus g is hyperelliptic if and only if it is birationally equivalent to a curve $C = V(y^2 - f(x))$, where the polynomial $f(x) \in \mathbb{F}[x]$ has degree $2g + 1$ and no square factors.*

Because the fields we consider are not algebraically closed, there are two aspects of this theorem that we can use, and one that we cannot. We can indeed narrow down the list of hyperelliptic curves defined over a field of odd characteristic by only considering the $f(x)$ polynomial in their construction, and setting $h(x) = 0$. This is because it is always possible to complete the square over a field of odd characteristic. In addition, as discussed in Section 4.1, as we are working in even genus we may assume that the hyperelliptic curve has one of the standard models, since its quotient by the hyperelliptic involution has a rational point.

However, we cannot use this theorem to neglect $f(x)$ polynomials of degree $d = 2g+2$ because in its proof we find that the theorem assumes that the polynomial has a root in the given finite field. While this is always the case when $\mathbb{F}$ is algebraically closed, over finite fields there exist hyperelliptic curves with no rational branch points, in which case $f(x)$ must be taken to be of degree $d = 2g+2$.

In summary, when dealing with hyperelliptic curves of even genus defined over a field of odd characteristic, to ensure that we obtain a model for each isomorphism class of curves we need only include models of the form

$$y^2 = f(x) \tag{4.9}$$

for $f(x)$ of degree $d = 2g+1$ or $d = 2g+2$ as opposed to more general models of the form

$$y^2 + h(x)y = f(x). \tag{4.10}$$

This considerably shortens the list of curves we must sort without neglecting any isomorphism classes.

Example 4.2.2. *When $g = 2$ and we work over $\mathbb{F}_3$, the list of hyperelliptic curves formed when using the method described in Subsection 4.1.2 has 96,228 elements. When we use Theorem 4.2.1 to set $h(x) = 0$, the list shortens to 1,296 models.*

Shortening the list of models over $\mathbb{F}_3$ without sacrificing necessary models to represent all isomorphism classes enabled us to perform the processes described in Chapters 5 and 6 much more efficiently. We note that further speed ups are possible, but as they were not necessary for this project we did not implement them.

Chapter 5

Sorting Into Isogeny Classes

This chapter details the process of sorting curves into isogeny classes. In Section 5.1, we give an introduction to the zeta function and the L-polynomial. In Section 5.2, we explain how two curves are isogenous if their L-polynomials agree. The results of our computations can be found in the appendix. Unless otherwise noted, this chapter again uses [4] as a main reference.

5.1 Zeta Function and L-polynomial

We will determine the isogeny class of a curve using an object called the L-polynomial. In order to define this polynomial, we will first introduce the zeta function.

Definition 5.1.1 (Theorem 9.7 of [4])**.** *Let C be a curve defined over a finite field $\mathbb{F}_q$. For $i = 1, 2, \ldots$, let $N_i = \#C(\mathbb{F}_{q^i})$. We define the zeta function of C to be*

$$Z(C,t) = \exp\left(\sum_{i=1}^{\infty} \frac{N_i t^i}{i}\right). \tag{5.1}$$

While this definition might seem unwieldy at first sight, a beautiful theorem, first conjectured by Weil and later proved by Grothendieck, Artin and Verdier shows the following:

Theorem 5.1.2 (Proposition 9.8 of [4])**.** *Let C be a curve defined over a finite field $\mathbb{F}_q$ and let g be the genus of C. The zeta function of C is a rational function of t. More precisely, it can be written as*

$$Z(C,t) = \frac{L(t)}{(1-t)(1-qt)}, \tag{5.2}$$

where

$$L(t) = L_q(t) = \begin{cases} 1, & \text{for } g = 0, \\ 1 + \sum_{i=1}^{2g-1} a_i t^i + q^g t^{2g}, & \text{for } g \geq 1. \end{cases} \tag{5.3}$$

In addition, note that $L(t) \in \mathbb{Z}[t]$.

We define the numerator of the zeta-function, $L(t)$, to be the L-polynomial of C over $\mathbb{F}_q$. There are several properties of the L-polynomial that we will utilize for this project.

Proposition 5.1.3 (Proposition 9.9 of [4])**.** *Let C be a curve of genus g defined over $\mathbb{F}_q$. The L-polynomial of C has the following properties:*

1. *$L(t) = q^g t^{2g} L((qt)^{-1}) = 1 + a_{2g-1} q^{g-1} t + \cdots + q^g t^{2g}$;*

2. *$a_{2g-i} = q^{g-i} a_i$ for $i = 0, \ldots, g$.*

Thanks to this proposition, computing the L-polynomial, and therefore the zeta-function, reduces to a finite computation:

Corollary 5.1.4. *Because of this symmetry of the L-polynomial, we can conclude that in order to find the L-polynomial, it suffices to compute the point counts N_i of C, where*

$$N_i = \#C(\mathbb{F}_{q^i}), \tag{5.4}$$

for $i = 1, 2, \ldots, g$, where g is the genus of C.

To illustrate Theorem 5.1.2 and Proposition 5.1.3, we provide an example.

Example 5.1.5. *Let $\mathbb{P}^1$ be the projective line and let $\mathbb{F}_q$ be a finite field of cardinality q. Recall that*

$$\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \infty \tag{5.5}$$

Therefore, we find the number of points of $\mathbb{P}^1(\mathbb{F}_q)$ to be

$$\#\mathbb{P}^1(\mathbb{F}_q) = \#(\mathbb{F}_q \cup \infty) = q + 1 \tag{5.6}$$

because there are q finite points and one "point at infinity". In general, in the same manner, we can say

$$\#\mathbb{P}^1(\mathbb{F}_{q^i}) = \#(\mathbb{F}_{q^i} \cup \infty) = q^i + 1 \tag{5.7}$$

By Definition 5.1.1,

$$Z(\mathbb{P}^1, t) = \exp\left(\sum_{i=1}^{\infty} \frac{\#\mathbb{P}^1(\mathbb{F}_{q^i})t^i}{i}\right) \tag{5.8}$$

Substituting $\#\mathbb{P}^1(\mathbb{F}_{q^i}) = q^i + 1$, *we get*

$$Z(\mathbb{P}^1, t) = \exp\left(\sum_{i=1}^{\infty} \frac{(q^i + 1)(t^i)}{i}\right) \tag{5.9}$$

$$= \exp\left(\sum_{i=1}^{\infty} \frac{(qt)^i}{i} + \sum_{i=1}^{\infty} \frac{t^i}{i}\right) \tag{5.10}$$

Using the fact that $\ln(1-x) = -\sum_{i=1}^{\infty} \frac{x^i}{i}$, *we can simplify further:*

$$Z(\mathbb{P}^1, t) = \exp(-\ln(1-qt) - \ln(1-t)) \tag{5.11}$$

$$= \exp(\ln(1-qt)^{-1} + \ln(1-t)^{-1}) \tag{5.12}$$

$$= \exp(\ln(1-qt)^{-1}) \cdot \exp(\ln(1-t)^{-1}) \tag{5.13}$$

$$= (1-qt)^{-1} \cdot (1-t)^{-1} \tag{5.14}$$

$$= \frac{1}{(1-qt)(1-t)} \tag{5.15}$$

We see that $L(t) = 1$, *which agrees with Proposition 5.1.3 because* $\mathbb{P}^1$ *has genus* $g = 0$.

5.2 Using L-polynomials to Determine Isogeny Classes

In order to use the L-polynomial for our project, we use Theorem 2.3 of [7].

Definition 5.2.1 (Theorem 2.3 of [7])**.** *Two curves of the same genus* g *defined over the same finite field* $\mathbb{F}_q$ *are said to be isogenous if their* L*-polynomials agree.*

Remark 5.2.2. *Usually the notion of isogeny is reserved for abelian varieties; we* *explain how our notion of isogeny between curves is merely an abuse of language for the more usual meaning. Given two curves C_1 and C_2, we can form their Jacobian varieties J_1 and J_2, respectively, which are abelian varieties (see Milne [11], for example, for a full account of the theory of Jacobian varieties). In the theory of abelian varieties, an isogeny is a rational map from one abelian variety to another that sends the origin of one abelian variety to the origin of the other and that has finite kernel. We say two abelian varieties are isogenous if there is an isogeny between them, and this is an equivalence relation. By Theorem 1 of [13], two abelian varieties are isogenous if and only their L-polynomials are equal. By work of Weil, the L-polynomial of a curve is equal to that of its Jacobian. Therefore it follows that our definition of two curves being isogenous is equivalent to the usual definition of their Jacobians being isogenous.*

In order to test whether two curves are isogenous, we will utilize Corollary 5.1.4. We will compare the first g point counts of the two curves in order to conclude that they are isogenous. In order to do this, we created a function in Magma that executes the following steps for two hyperelliptic curves C_1 and C_2.

1. Compare the point counts of C_1 and C_2 over the finite fields $\mathbb{F}_{q^1}, \mathbb{F}_{q^2}, \cdots \mathbb{F}_{q^g}$ using the `BaseChange` function supplied by Magma.

2. Stop the comparison if at any point, the point counts do not match.

3. If the first g point counts match, determine the two curves to be isogenous.

5.2.1 Validation of Results

In the case of hyperelliptic curves of genus 2 defined over $\mathbb{F}_2$, the work of [9] tells us that we should obtain 20 isogeny classes. Using our program, we found all 20 isogeny classes and have summarized our results in Appendix A.1.

In the case of hyperelliptic curves of genus 2 defined over $\mathbb{F}_3$, we know that we should obtain 50 isogeny classes, again based on the work of [9]. Using our program, we found all 50 isogeny classes and have summarized our results in Appendix A.2.

5.3 Curves with No Rational Points

As an interesting result, we are now in a position to give models of curves with no rational points defined over the fields $\mathbb{F}_2$ and $\mathbb{F}_3$.

Recall that over $\mathbb{F}_2$, we are only able to classify curves into isogeny classes. According to our results, and corroborated by the data of [9], there is one isogeny class of curves of genus 2 defined over $\mathbb{F}_2$ with no rational point. In the notation of Appendix A.1, this is isogeny class 20, and in the notation of [9], this is the isogeny class labeled 2.2.ad_f. According to our computations, an example of a curve defined over $\mathbb{F}_2$ with no rational point is $y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + 1$.

According to our results, and again corroborated by the data of [9], there is again one isogeny class of curves of genus 2 defined over $\mathbb{F}_3$ with no rational point. In the notation of Appendix A.2, this is isogeny class 50, and in the notation of [9], this is isogeny class 2.3.ae_i. We note that this isogeny class contains only one isomorphism class, and therefore up to isomorphism, $y^2 = 2x^6 + x^5 + x^4 + x^3 + x + 2$ is the only hyperelliptic curve of genus 2 defined over $\mathbb{F}_3$ without a rational point.

Chapter 6

Sorting Into Isomorphism Class

In this chapter, we turn our attention to a more strict equivalence relation between curves, that of isomorphism. We begin in Section 6.1 by explaining the code we wrote to perform the classification of curves according to isomorphism classes. We note that due to the limitations of Magma, we are unable to compute the isomorphism classes for hyperelliptic curves defined over fields of even characteristic. However, our code will work for any field of odd characteristic, and we illustrate it here for the field $\mathbb{F}_3$.

Our results from this process differ from those of Theorem 5 of [2], which states there are 54 isomorphism classes for curves of genus 2 defined over a field of cardinality 3 and that have a rational branch point. Indeed, we find 32 such classes. We expand on this discrepancy further in Section 6.2. Finally, we present the isomorphism classes we have found in Appendix A.2.

Unless otherwise noted, again the source for general definitions in this chapter is [4].

6.1 Finding Isomorphism Classes

In this section we will explain the process we used to further sort the elements of an isogeny classes into isomorphism classes for curves of genus 2 over the finite field $\mathbb{F}_3$. We first begin with the definition of isomorphism:

Definition 6.1.1. *Two curves are isomorphic if there exists an invertible rational map between them.*

To classify the curves, the function we created in Magma utilizes a preset function in Magma called `IsIsomorphic`. Given two curves, C_1 and C_2, `IsIsomorphic` tests whether C_1 can be transformed into C_2 via invertible morphisms.

The function we created to sort curves into their isomorphism classes does so in several steps:

1. Choose the first isogeny class $isog_1$.

2. Create an empty set that will become the first isomorphism class, $isom_1$.

3. Choose the first curve in $isog_1$, C_1 and append it to isomorphism class $isom_1$.

4. Test each curve in $isog_1$ against curve C_1 using `IsIsomorphic`. If it is isomorphic to C_1, add it to $isom_1$ and remove it from $isog_1$ (temporarily, for the purposes of the function). If it is not, move to the next curve.

5. Once all curves in $isog_1$ have been tested against C_1, consider $isom_1$ complete and begin another isomorphism class to test the remaining curves in $isog_1$ against. Continue forming isomorphism classes in this way until all curves in $isog_1$ have been sorted into isomorphism classes.

6. Once $isog_1$ is empty, move onto $isog_2$. Repeat steps 2 to 5 for every isogeny class.

The output of this function is a list of isomorphism classes grouped by isogeny class.

6.2 Results for Genus 2 Curves Over $\mathbb{F}_3$

Based on the tables found in [9], we expected to find 50 isogeny classes of hyperelliptic curves of genus 2 defined over $\mathbb{F}_3$. Using the Magma program described in 5.2, we successfully found exactly 50. We then sorted these isogeny classes into isomorphism classes and found 69 total isomorphism classes defined over $\mathbb{F}_3$.

To verify the accuracy of our results, we compared what we obtained and the results given in [2], in which the authors count the number of isomorphism classes of hyperelliptic curves with a rational branch point and defined over a field of odd characteristic. In effect, this amounts to counting the number of isomorphism classes of curves that can be given by a model of the form $y^2 = f(x)$ for $f(x)$ of degree $2g+1$ (rather than counting those given by models of the form $y^2 = f(x)$ for $f(x)$ of degree $2g+1$ and $2g+2$, as required by the discussion following Theorem 4.2.1).

Running our code on hyperelliptic curves only of this form, we obtained 32 isomorphism classes of curves with a rational branch point. However in [2], the authors show:

Theorem 6.2.1 (Theorem 5 of [2]). *Let $\mathcal{H}$ be the set of equations of the form*

$$y^2 = x^5 + a_4x^3 + a_6x^2 + a_8x + a_{10} \tag{6.1}$$

where the discriminant of $y^2 = x^5 + a_4x^3 + a_6x^2 + a_8x + a_{10}$ is not zero. Let G be the group of transformations of the form $(x, y) \mapsto (\alpha^2 x, \alpha^5 y)$, $\alpha \in \mathbb{F}_q \backslash \{0\}$. $\mathcal{H}/G$ is the set of isomorphism classes of such curves. The number of isomorphism classes of genus 2 curves defined over $\mathbb{F}_q$ is $|\mathcal{H}/G| = 2q^3 + r(q)$, where $r(q)$ is given in the following table:

$r(q)$	$q \equiv 1 \pmod 8$	$q \not\equiv 1 \pmod 8, q \equiv 1 \pmod 4$	$q \not\equiv 1 \pmod 4$
$q \equiv 1 \pmod 5$	$2q + 10$	$2q + 6$	8
$q \not\equiv 1 \pmod 5$	$2q + 2$	$2q - 2$	0

From this theorem it follows that the number of isomorphism classes of curves defined over $\mathbb{F}_3$ with a rational root should be 54. After investigating this discrepancy, we found that the notion of isomorphism used by the authors of [2] does not agree with ours.

Since the number of isomorphism classes we find is smaller than the number of isomorphism classes found by the authors of [2], it follows that we consider certain curves to be isomorphic that the authors of [2] do not consider to be isomorphic. Indeed, upon more careful consideration, despite the fact that the authors specify that they will consider two curves to be isomorphic when they admit an isomorphism of varieties (which is the notion we use in this work), we find that the main reference they use in proving Theorem 5 does not use this same notion of isomorphism. The proof of Theorem 5 of [2] relies crucially on Proposition 1.2 of [10]. However, the work [10] concerns itself with *pointed* hyperelliptic curves, or in other words, hyperelliptic curves equipped with a rational branch point. As such, this reference considered two pointed hyperelliptic curves to be isomorphic if there is not only an isomorphism of varieties between them, but if this isomorphism sends the distinguished branch point of one curve to the distinguished branch point of the other curve.

We stress that this is not the customary definition of isomorphism of curves, and that indeed this notion is more restrictive as the isomorphism must satisfy an extra condition that is not satisfied by every isomorphism (that of sending the distinguished branch point of one curve to the distinguished branch point of the other curve). This explains completely why the reference [2] finds more isomorphism classes.

An example of two curves that our code sorted into the same isomorphism class but that would fall into two different classes according to [2] are the following. For the sake of this explanation, we call them C_1 and C_2.

$$C_1 : y^2 = x^5 + 1 \tag{6.2}$$

$$C_2 : y^2 = x^5 + x^3 + 1. \tag{6.3}$$

In order to prove that these two curves are isomorphic, as Magma claims they are, we may exhibit a map between them. We recall that while we use affine models throughout, these curves are really weighted projective curves. Since we seek an isomorphism of projective curves, we work with their weighted projective models:

$$C_1 : Y^2 = ZX^5 + Z^6 \tag{6.4}$$

and

$$C_2 : Y^2 = ZX^5 + Z^3X^3 + Z^6. \tag{6.5}$$

We now give the isomorphism we seek as a composition of several simple isomorphisms. The first isomorphism is

$$\begin{aligned}\phi_1 : C_1 &\to C_1' \\ X &\mapsto Z \\ Z &\mapsto X \\ Y &\mapsto Y\end{aligned}$$

We will first reverse X and Z in C_1. Reversing X and Z in C_1, we obtain:

$$C_1' : Y^2 = X^6 + XZ^5 \tag{6.6}$$

The next isomorphism is

$$\begin{aligned}\phi_2 : C_1' &\to C_2' \\ X &\mapsto X + 2Z \\ Z &\mapsto Z \\ Y &\mapsto Y.\end{aligned}$$

Note that the inverse of ϕ_2 is:

$$X \mapsto X - 2Z$$
$$Z \mapsto Z$$
$$Y \mapsto Y,$$

so ϕ_2 is invertible. We have

$$\begin{aligned}
C_2' : Y^2 &= (X+2Z)^6 + (X+2Z)Z^5 \\
Y^2 &= ((X+2Z)^3)^2 + (X+2Z)Z^5 \\
Y^2 &= (X^3 + (2Z)^3)^2 + (X+2Z)Z^5 \\
Y^2 &= (X^3 + 8Z^3)^2 + (X+2Z)Z^5 \\
Y^2 &= X^6 + X^3Z^3 + Z^6 + Z^5X + 2Z^6 \\
Y^2 &= X^6 + X^3Z^3 + Z^5X + 3Z^6 \\
C_2' : Y^2 &= X^6 + X^3Z^3 + Z^5X
\end{aligned}$$

where in the third line we use that $(X+2Z)^3 = X^3 + (2Z)^3$ in characteristic 3.

The last isomorphism is

$$\begin{aligned} \phi_3 : C_2' &\mapsto C_2 \\ X &\mapsto Z \\ Z &\mapsto X \\ Y &\mapsto Y \end{aligned}$$

And we find that

$$C_2 : Y^2 = Z^6 + Z^3X^3 + X^5Z \tag{6.7}$$

This is indeed the projective model for C_2. We now note that the composition $\phi_3 \circ \phi_2 \circ \phi_1$ is an isomorphism since each ϕ_i is an isomorphism, and a composition of isomorphisms is an isomorphism. Therefore, C_1 and C_2 are isomorphic.

However, the authors of [2] would not consider these two curves to be isomorphic, since the distinguished branch point $(1, 0, 0)$ on C_1 is not sent to the point $(1, 0, 0)$ on C_2. Indeed:

$$\begin{aligned} \phi_3 \circ \phi_2 \circ \phi_1(1, 0, 0) &= \phi_3 \circ \phi_2(0, 0, 1) \\ &= \phi_3(2, 0, 1) \\ &= (1, 0, 2) \neq (1, 0, 0). \end{aligned}$$

Therefore this isomorphism does not fix the distinguished branch point.

Bibliography

[1] Kristen Eisenträger and Kristin Lauter. *A CRT algorithm for constructing genus 2 curves over finite fields*, volume 21 of *Sem. Congr.*, pages 161–176. Soc. Math. France, Paris, 2010.

[2] L. Hernández Encinas, Alfred J. Menezes, and J. Muñoz Masqué. Isomorphism classes of genus-2 hyperelliptic curves over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):57–65, 2002.

[3] William Fulton. *Algebraic curves: An introduction to algebraic geometry.* Advanced Book Classics. Addison-Wesley Publishing Company, 1989.

[4] James William Peter Hirschfeld, Gábor Korchmáros, and Fernando Torres. *Algebraic curves over a finite field.* Princeton University Press, 2013.

[5] Timothy Hosgood. An introduction to varieties in weighted projective space. https://arxiv.org/pdf/1604.02441.pdf, 2016.

[6] Everett W. Howe, Kristin E. Lauter, Christophe Ritzenthaler, and Gerard van der Geer. Tables of curves with many points, 2009. [Online; accessed November 2017].

[7] Valentijn Karemaker and Rachel Pries. Fully maximal and fully minimal abelian varieties. https://arxiv.org/abs/1703.10076, 2017.

[8] Jong Won Lee. Isomorphism classes of Picard curves over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 16(1):33–44, 2005.

[9] The LMFDB Collaboration. The L-functions and Modular Forms Database. http://www.lmfdb.org, 2017. [Online; accessed November 2017].

[10] Paul Lockhart. On the discriminant of a hyperelliptic curve. *Transactions of the American Mathematical Society*, 342(2):729–752, 1994.

[11] James Milne. Jacobian varieties. http://www.jmilne.org/math/xnotes/JVs.pdf, 2018. [Online; accessed November 2017].

[12] Bjorn Poonen. *Computational aspects of curves of genus at least 2*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 283–306. Springer, 1996.

[13] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2:134–144, 1966.

[14] Lin You and Fugeng Zeng. The number of the isomorphism classes of hyperelliptic curves of genus four over finite fields. In *2010 Sixth International Conference on Information Assurance and Security*, pages 161–166, 2010.

Appendix A

Summary Tables for Isogeny and Isomorphism Classes

A.1 Genus 2 Curves Defined Over $\mathbb{F}_2$

We were able to obtain the isogeny classes, but not the isomorphism classes, for curves of genus 2 defined over $\mathbb{F}_2$. We were also able to organize these classes to match the label format found in [9]. Found in this section is a detailed list of these isogeny classes and their corresponding point counts and LMFDB labels from [9]. A complete list of curves from each of these classes can be found in Appendix B.

Isog. Class	LMFDB Label	Point Counts	First Curve in Class
1	2.2.a_a	(5,25)	$y^2 + y = x^5$
2	2.2.b_c	(10,40)	$y^2 + (x^2 + 1)y = x^5$
3	2.2.b_b	(9,27)	$y^2 + (x^3 + x^2 + 1)y = x^5$
4	2.2.b_d	(11,55)	$y^2 + (x^3 + x + 1)y = x^5$
5	2.2.c_c	(13,13)	$y^2 + (x^3 + x^2 + x + 1)y = x^5$
6	2.2.c_e	(15,45)	$y^2 + y = x^5 + x^4$
7	2.2.b_a	(8,16)	$y^2 + (x + 1)y = x^5 + x^4$
8	2.2.c_d	(14,28)	$y^2 + (x^2 + x + 1)y = x^5 + x^4$
9	2.2.d_f	(19,19)	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4$
10	2.2.a_c	(7,49)	$y^2 + y = x^5 + x^4 + x^3$
11	2.2.a_b	(6,36)	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^3$
12	2.2.ab_c	(4,40)	$y^2 + xy = x^5 + x^4 + x$
13	2.2.ab_a	(2,16)	$y^2 + (x^2)y = x^5 + x^4 + x$
14	2.2.a_ab	(4,16)	$y^2 + (x^2 + x)y = x^5 + x^4 + x$
15	2.2.ac_e	(3,45)	$y^2 + y = x^5 + x^4 + 1$
16	2.2.ac_d	(2,28)	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + 1$
17	2.2.ab_d	(5,55)	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + 1$
18	2.2.ac_c	(1,13)	$y^2 + y = x^5 + x^3 + 1$
19	2.2.ab_b	(3,27)	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + 1$
20	2.2.ad_f	(1,19)	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + 1$

A.2 Genus 2 Curves Defined Over $\mathbb{F}_3$

Outputs listed in this table are the polynomials $f(x)$ in the hyperelliptic curve form

$$y^2 = f(x). \tag{A.1}$$

Isog denotes the isogeny class number and *Isom* denotes the isomorphism class number. *Label* denotes the isomorphism and isogeny classes of each representative curve. For example, a curve in the isogeny class number 15 and the first isomorphism class within that isogeny class would be marked 15.1.

Label	Isog	Isom	Point Counts	First Curve $f(x)$
1.1	1	1	(12,144)	$x^5 + x$
1.2	1	2	(12,144)	$2x^6 + 2x^4 + x^3 + x^2 + 1$
2.1	2	3	(8,64)	$2x^5 + x$
2.2	2	4	(8,64)	$x^5 + 2x^4 + x^2 + x$
3.1	3	5	(8,128)	$x^5 + x^4 + x$
3.2	3	6	(8,128)	$x^5 + x^3 + x^2 + x + 1$
4.1	4	7	(22,132)	$2x^5 + x^4 + x$
4.2	4	8	(22,132)	$x^6 + x^5 + 2x^4 + 2x^2 + 1$
5.1	5	9	(16,128)	$x^5 + 2x^4 + x$
5.2	5	10	(16,128)	$x^5 + 2x^4 + 2x^3 + x + 1$
6.1	6	11	(6,132)	$2x^5 + 2x^4 + x$
6.2	6	12	(6,132)	$2x^6 + 2x^5 + 2x^4 + x + 1$
7.1	7	13	(14,196)	$2x^5 + x^3 + x$
8.1	8	14	(20,80)	$x^5 + x^4 + x^3 + x$
8.2	8	15	(20,80)	$2x^5 + 2x^4 + 2x^2 + x$
9.1	9	16	(4,48)	$2x^5 + x^4 + x^3 + x$
10.1	10	17	(4,80)	$x^5 + 2x^4 + x^3 + x$
10.2	10	18	(4,80)	$2x^5 + x^4 + x^2 + x$
11.1	11	19	(12,48)	$2x^5 + 2x^4 + x^3 + x$
12.1	12	20	(8,192)	$x^5 + x^4 + x^3 + x^2 + x$
12.2	12	21	(8,192)	$2x^6 + 2x^2 + 1$
13.1	13	22	(10,100)	$2x^5 + 2x^4 + x^3 + x^2 + x$
13.2	13	23	(10,100)	$2x^5 + 2x^4 + 2x^3 + x^2 + x$

Label	Isog	Isom	Point Counts	First Curve $f(x)$
14.1	14	24	(24,192)	$x^5 + 2x^4 + x^3 + 2x^2 + x$
14.2	14	25	(24,192)	$2x^6 + x^4 + 1$
15.1	15	26	(17,153)	$x^5 + 2x^4 + 1$
15.2	15	27	(17,153)	$x^5 + x^3 + 2x^2 + 1$
16.1	16	28	(28,112)	$2x^5 + x^3 + 1$
17.1	17	29	(9,153)	$2x^5 + x^4 + x^3 + 1$
17.2	17	30	(9,153)	$2x^5 + x^3 + x^2 + 1$
18.1	18	31	(14,84)	$x^5 + 2x^4 + x^3 + 1$
19.1	19	32	(15,105)	$x^5 + x^4 + x^2 + 1$
19.2	19	33	(15,105)	$2x^5 + 2x^4 + x^3 + x + 1$
20.1	20	34	(18,180)	$x^5 + x^4 + x^3 + x^2 + 1$
21.1	21	35	(27,81)	$2x^5 + 2x^4 + x^3 + x^2 + 1$
22.1	22	36	(7,105)	$2x^5 + 2x^4 + x^3 + 2x^2 + 1$
22.2	22	37	(7,105)	$2x^5 + x^4 + x + 1$
23.1	23	38	(29,145)	$2x^5 + x + 1$
24.1	24	39	(19,209)	$x^5 + 2x^4 + x + 1$
25.1	25	40	(5,65)	$x^5 + x^4 + x^3 + x + 1$
26.1	26	41	(10,180)	$2x^5 + x^2 + x + 1$
27.1	27	42	(13,65)	$2x^5 + x^4 + 2x^3 + x^2 + x + 1$
28.1	28	43	(11,209)	$2x^5 + 2x^4 + 2x^2 + x + 1$
29.1	29	44	(6,84)	$x^5 + 2x^4 + x^3 + 2x^2 + x + 1$
30.1	30	45	(4,112)	$2x^5 + x^3 + 2$
31.1	31	46	(3,81)	$2x^5 + 2x^4 + x^3 + x^2 + 2$

Label	Isog	Isom	Point Counts	First Curve $f(x)$
32.1	32	47	(5,145)	$2x^5 + x + 2$
33.1	33	48	(13,169)	$2x^6 + x^5 + 1$
33.2	33	49	(13,169)	$2x^6 + x + 1$
34.1	34	50	(21,105)	$x^6 + x^5 + x^4 + 1$
34.2	34	51	(21,105)	$2x^6 + x^2 + 1$
35.1	35	52	(35,105)	$x^6 + 2x^4 + 1$
36.1	36	53	(5,105)	$2x^6 + 2x^4 + 1$
36.2	36	54	(5,105)	$2x^6 + 2x^4 + 2x^3 + x + 1$
37.1	37	55	(36,144)	$x^6 + x^4 + x^2 + 1$
38.1	38	56	(9,225)	$2x^6 + x^4 + x^2 + 1$
39.1	39	57	(15,225)	$x^6 + 2x^4 + x^2 + 1$
39.2	39	58	(15,225)	$x^6 + x^5 + x^3 + x + 1$
40.1	40	59	(3,57)	$2x^6 + 2x^5 + x^4 + x^3 + x^2 + 1$
41.1	41	60	(9,81)	$2x^6 + x^5 + x^4 + 2x^2 + 1$
42.1	42	61	(25,225)	$2x^6 + 2x^4 + 2x^2 + 1$
43.1	43	62	(23,161)	$x^6 + x^5 + x^4 + x + 1$
44.1	44	63	(11,121)	$2x^6 + 2x^5 + x^3 + x + 1$
45.1	45	64	(34,68)	$x^6 + x^5 + 2x^4 + x^3 + x + 1$
46.1	46	65	(7,161)	$2x^6 + x^5 + 2x^4 + x^3 + x + 1$
47.1	47	66	(19,57)	$x^6 + 2x^5 + x^4 + 2x^3 + x + 1$
48.1	48	67	(3,105)	$2x^6 + x^4 + 2$
49.1	49	68	(4,144)	$2x^6 + 2x^4 + 2x^2 + 2$
50.1	50	69	(2,68)	$2x^6 + x^5 + x^4 + x^3 + x + 2$

Appendix B

Complete Results: Genus 2 Curves Defined over $\mathbb{F}_2$

In this appendix we list every model of hyperelliptic curves of genus 2 defined over $\mathbb{F}_2$, organized by isogeny class. *Label* denotes the isogeny class number and the curve number within that isogeny class. For example, the second curve in the fourth isogeny class would have the label 4.2.

Label	Curve
1.1	$y^2 + y = x^5$
1.2	$y^2 + y = x^5 + x^4 + x^2$
1.3	$y^2 + y = x^5 + x^4 + x$
1.4	$y^2 + x^3y = x^5 + x^4 + x$
1.5	$y^2 + y = x^5 + x^2 + x$
1.6	$y^2 + x^3y = x^5 + x^2 + x$
1.7	$y^2 + y = x^5 + 1$
1.8	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + 1$
1.9	$y^2 + y = x^5 + x^4 + x^2 + 1$
1.10	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4 + x^2 + 1$
1.11	$y^2 + y = x^5 + x^4 + x + 1$
1.12	$y^2 + x^3y = x^5 + x^4 + x^3 + x + 1$
1.13	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4 + x^3 + x + 1$
1.14	$y^2 + y = x^5 + x^2 + x + 1$
1.15	$y^2 + x^3y = x^5 + x^3 + x^2 + x + 1$
1.16	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^3 + x^2 + x + 1$
1.17	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5$
1.18	$y^2 + y = x^6 + x^5 + x^3$
1.19	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x^3$
1.20	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4 + x^2$
1.21	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^3 + x^2$

Label	Curve
1.22	$y^2 + y = x^6 + x^5 + x^4 + x^3 + x^2$
1.23	$y^2 + x^3y = x^6 + x$
1.24	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x$
1.25	$y^2 + x^3y = x^6 + x^5 + x^4 + x$
1.26	$y^2 + y = x^6 + x^5 + x^4 + x^3 + x$
1.27	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x$
1.28	$y^2 + x^3y = x^6 + x^5 + x^2 + x$
1.29	$y^2 + x^3y = x^6 + x^4 + x^2 + x$
1.30	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x^2 + x$
1.31	$y^2 + y = x^6 + x^5 + x^3 + x^2 + x$
1.32	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^3 + x^2 + x$
1.33	$y^2 + y = x^6 + x^5 + x^3 + 1$
1.34	$y^2 + y = x^6 + x^5 + x^4 + x^3 + x^2 + 1$
1.35	$y^2 + x^3y = x^6 + x^3 + x + 1$
1.36	$y^2 + y = x^6 + x^5 + x^4 + x^3 + x + 1$
1.37	$y^2 + x^3y = x^6 + x^5 + x^4 + x^3 + x + 1$
1.38	$y^2 + y = x^6 + x^5 + x^3 + x^2 + x + 1$
1.39	$y^2 + x^3y = x^6 + x^5 + x^3 + x^2 + x + 1$
1.40	$y^2 + x^3y = x^6 + x^4 + x^3 + x^2 + x + 1$
2.1	$y^2 + (x^2 + 1)y = x^5$
2.2	$y^2 + (x + 1)y = x^5 + x^4 + x^3$

Label	Curve
2.3	$y^2 + (x+1)y = x^5 + x^2$
2.4	$y^2 + (x^2+1)y = x^5 + x^2$
2.5	$y^2 + (x^3+x^2)y = x^5 + x^4 + x$
2.6	$y^2 + (x^2+1)y = x^5 + x^3 + x$
2.7	$y^2 + (x^3+x)y = x^5 + x^3 + x$
2.8	$y^2 + (x+1)y = x^5 + x^4 + x^3 + x$
2.9	$y^2 + (x^2)y = x^5 + x^4 + x^3 + x$
2.10	$y^2 + (x^3+x)y = x^5 + x^4 + x^3 + x$
2.11	$y^2 + (x+1)y = x^5 + x^2 + x$
2.12	$y^2 + xy = x^5 + x^4 + x^2 + x$
2.13	$y^2 + (x^2)y = x^5 + x^4 + x^2 + x$
2.14	$y^2 + xy = x^5 + x^3 + x^2 + x$
2.15	$y^2 + (x^2+1)y = x^5 + x^3 + x^2 + x$
2.16	$y^2 + (x^3+x^2)y = x^5 + x^3 + x^2 + x$
2.17	$y^2 + (x^3+x)y = x^5 + 1$
2.18	$y^2 + (x^3+x)y = x^5 + x^4 + 1$
2.19	$y^2 + xy = x^5 + x^4 + x^2 + 1$
2.20	$y^2 + xy = x^5 + x^3 + x^2 + 1$
2.21	$y^2 + (x^3+x^2)y = x^5 + x + 1$
2.22	$y^2 + (x^2)y = x^5 + x^4 + x + 1$
2.23	$y^2 + (x^2)y = x^5 + x^4 + x^3 + x^2 + x + 1$

Label	Curve
2.24	$y^2 + (x^3 + x^2)y = x^5 + x^4 + x^3 + x^2 + x + 1$
2.25	$y^2 + (x + 1)y = x^6 + x^5$
2.26	$y^2 + (x^2 + 1)y = x^6 + x^3$
2.27	$y^2 + (x^2 + 1)y = x^6 + x^3 + x^2$
2.28	$y^2 + (x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2$
2.29	$y^2 + (x^2 + 1)y = x^6 + x$
2.30	$y^2 + (x + 1)y = x^6 + x^5 + x$
2.31	$y^2 + (x^2)y = x^6 + x^4 + x^3 + x$
2.32	$y^2 + (x^2 + 1)y = x^6 + x^2 + x$
2.33	$y^2 + xy = x^6 + x^5 + x^2 + x$
2.34	$y^2 + (x^2)y = x^6 + x^4 + x^2 + x$
2.35	$y^2 + xy = x^6 + x^5 + x^4 + x^3 + x^2 + x$
2.36	$y^2 + (x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
2.37	$y^2 + xy = x^6 + x^5 + x^2 + 1$
2.38	$y^2 + xy = x^6 + x^5 + x^4 + x^3 + x^2 + 1$
2.39	$y^2 + (x^2)y = x^6 + x^4 + x + 1$
2.40	$y^2 + (x^2)y = x^6 + x^4 + x^3 + x^2 + x + 1$
3.1	$y^2 + (x^3 + x^2 + 1)y = x^5$
3.2	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^2$
3.3	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + x^2$
3.4	$y^2 + (x^3 + x + 1)y = x^5 + x^3 + x^2$

Label	Curve
3.5	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x$
3.6	$y^2 + (x^3 + x + 1)y = x^5 + x^2 + x$
3.7	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3 + x^2 + x$
3.8	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3 + x^2 + x$
3.9	$y^2 + (x^3 + x + 1)y = x^5 + 1$
3.10	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3 + 1$
3.11	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3 + 1$
3.12	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^2 + 1$
3.13	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x + 1$
3.14	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + x + 1$
3.15	$y^2 + (x^3 + x + 1)y = x^5 + x^3 + x + 1$
3.16	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^2 + x + 1$
3.17	$y^2 + (x^3 + x + 1)y = x^6 + x^5$
3.18	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4$
3.19	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^3$
3.20	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^3$
3.21	$y^2 + (x^3 + x + 1)y = x^6 + x^2$
3.22	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^2$
3.23	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^3 + x^2$
3.24	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^3 + x^2$
3.25	$y^2 + (x^3 + x^2 + 1)y = x^6 + x$

Label	Curve
3.26	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x$
3.27	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^3 + x$
3.28	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^3 + x$
3.29	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^2 + x$
3.30	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^2 + x$
3.31	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^3 + x^2 + x$
3.32	$y^2 + (x^3 + x + 1)y = x^6 + x^3 + x^2 + x$
4.1	$y^2 + (x^3 + x + 1)y = x^5$
4.2	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3$
4.3	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3$
4.4	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^2$
4.5	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x$
4.6	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + x$
4.7	$y^2 + (x^3 + x + 1)y = x^5 + x^3 + x$
4.8	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^2 + x$
4.9	$y^2 + (x^3 + x^2 + 1)y = x^5 + 1$
4.10	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^2 + 1$
4.11	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + x^2 + 1$
4.12	$y^2 + (x^3 + x + 1)y = x^5 + x^3 + x^2 + 1$
4.13	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x + 1$
4.14	$y^2 + (x^3 + x + 1)y = x^5 + x^2 + x + 1$

Label	Curve
4.15	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3 + x^2 + x + 1$
4.16	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3 + x^2 + x + 1$
4.17	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5$
4.18	$y^2 + (x^3 + x + 1)y = x^6 + x^4$
4.19	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^3$
4.20	$y^2 + (x^3 + x + 1)y = x^6 + x^3$
4.21	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^2$
4.22	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^2$
4.23	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^3 + x^2$
4.24	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^3 + x^2$
4.25	$y^2 + (x^3 + x + 1)y = x^6 + x$
4.26	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x$
4.27	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^3 + x$
4.28	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^3 + x$
4.29	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^2 + x$
4.30	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^2 + x$
4.31	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
4.32	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
5.1	$y^2 + (x^3 + x^2 + x + 1)y = x^5$
5.2	$y^2 + y = x^5 + x^3$
5.3	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4 + x^2$

Label	Curve
5.4	$y^2 + y = x^5 + x^4 + x^3 + x^2$
5.5	$y^2 + y = x^5 + x^4 + x^3 + x$
5.6	$y^2 + x^3y = x^5 + x^4 + x^3 + x$
5.7	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4 + x^3 + x$
5.8	$y^2 + y = x^5 + x^3 + x^2 + x$
5.9	$y^2 + x^3y = x^5 + x^3 + x^2 + x$
5.10	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^3 + x^2 + x$
5.11	$y^2 + x^3y = x^5 + x^4 + x + 1$
5.12	$y^2 + x^3y = x^5 + x^2 + x + 1$
5.13	$y^2 + y = x^6 + x^5$
5.14	$y^2 + y = x^6 + x^5 + x^4 + x^2$
5.15	$y^2 + y = x^6 + x^5 + x^4 + x$
5.16	$y^2 + y = x^6 + x^5 + x^2 + x$
6.1	$y^2 + y = x^5 + x^4$
6.2	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4$
6.3	$y^2 + y = x^5 + x^2$
6.4	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^2$
6.5	$y^2 + y = x^5 + x$
6.6	$y^2 + x^3y = x^5 + x$
6.7	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^3 + x$
6.8	$y^2 + y = x^5 + x^4 + x^2 + x$

Label	Curve
6.9	$y^2 + x^3y = x^5 + x^4 + x^2 + x$
6.10	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4 + x^3 + x^2 + x$
6.11	$y^2 + x^3y = x^5 + x^3 + x + 1$
6.12	$y^2 + x^3y = x^5 + x^4 + x^3 + x^2 + x + 1$
6.13	$y^2 + y = x^6 + x^5 + x^4 + x^3$
6.14	$y^2 + y = x^6 + x^5 + x^3 + x^2$
6.15	$y^2 + y = x^6 + x^5 + x^3 + x$
6.16	$y^2 + y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
7.1	$y^2 + (x + 1)y = x^5 + x^4$
7.2	$y^2 + (x^2 + 1)y = x^5 + x^4$
7.3	$y^2 + (x^2 + 1)y = x^5 + x^4 + x^2$
7.4	$y^2 + (x + 1)y = x^5 + x^3 + x^2$
7.5	$y^2 + xy = x^5 + x$
7.6	$y^2 + (x^2)y = x^5 + x$
7.7	$y^2 + (x + 1)y = x^5 + x^4 + x$
7.8	$y^2 + xy = x^5 + x^4 + x^3 + x$
7.9	$y^2 + (x^2 + 1)y = x^5 + x^4 + x^3 + x$
7.10	$y^2 + (x^3 + x^2)y = x^5 + x^4 + x^3 + x$
7.11	$y^2 + (x^3 + x^2)y = x^5 + x^2 + x$
7.12	$y^2 + (x + 1)y = x^5 + x^3 + x^2 + x$
7.13	$y^2 + (x^2)y = x^5 + x^3 + x^2 + x$

Label	Curve
7.14	$y^2 + (x^3 + x)y = x^5 + x^3 + x^2 + x$
7.15	$y^2 + (x^2 + 1)y = x^5 + x^4 + x^3 + x^2 + x$
7.16	$y^2 + (x^3 + x)y = x^5 + x^4 + x^3 + x^2 + x$
7.17	$y^2 + xy = x^5 + 1$
7.18	$y^2 + xy = x^5 + x^4 + x^3 + 1$
7.19	$y^2 + (x^3 + x)y = x^5 + x^2 + 1$
7.20	$y^2 + (x^3 + x)y = x^5 + x^4 + x^2 + 1$
7.21	$y^2 + (x^2)y = x^5 + x^3 + x + 1$
7.22	$y^2 + (x^3 + x^2)y = x^5 + x^3 + x + 1$
7.23	$y^2 + (x^2)y = x^5 + x^2 + x + 1$
7.24	$y^2 + (x^3 + x^2)y = x^5 + x^4 + x^2 + x + 1$
7.25	$y^2 + (x + 1)y = x^6 + x^5 + x^3$
7.26	$y^2 + (x^2 + 1)y = x^6 + x^4 + x^3$
7.27	$y^2 + (x + 1)y = x^6 + x^5 + x^4 + x^2$
7.28	$y^2 + (x^2 + 1)y = x^6 + x^4 + x^3 + x^2$
7.29	$y^2 + (x^2)y = x^6 + x$
7.30	$y^2 + (x^2 + 1)y = x^6 + x^4 + x$
7.31	$y^2 + xy = x^6 + x^5 + x^4 + x$
7.32	$y^2 + xy = x^6 + x^5 + x^3 + x$
7.33	$y^2 + (x + 1)y = x^6 + x^5 + x^3 + x$
7.34	$y^2 + (x^2 + 1)y = x^6 + x^4 + x^2 + x$

Label	Curve
7.35	$y^2 + (x + 1)y = x^6 + x^5 + x^4 + x^2 + x$
7.36	$y^2 + (x^2)y = x^6 + x^3 + x^2 + x$
7.37	$y^2 + xy = x^6 + x^5 + x^4 + 1$
7.38	$y^2 + xy = x^6 + x^5 + x^3 + 1$
7.39	$y^2 + (x^2)y = x^6 + x^3 + x + 1$
7.40	$y^2 + (x^2)y = x^6 + x^2 + x + 1$
8.1	$y^2 + (x^2 + x + 1)y = x^5 + x^4$
8.2	$y^2 + (x^3 + 1)y = x^5 + x^4$
8.3	$y^2 + (x^2 + x + 1)y = x^5 + x^3$
8.4	$y^2 + (x^3 + 1)y = x^5 + x^4 + x^3$
8.5	$y^2 + (x^2 + x + 1)y = x^5 + x^2$
8.6	$y^2 + (x^3 + 1)y = x^5 + x^2$
8.7	$y^2 + (x^3 + 1)y = x^5 + x^3 + x^2$
8.8	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^3 + x^2$
8.9	$y^2 + (x^2 + x + 1)y = x^5 + x$
8.10	$y^2 + (x^3 + x^2 + x)y = x^5 + x$
8.11	$y^2 + (x^3 + 1)y = x^5 + x^4 + x$
8.12	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^3 + x$
8.13	$y^2 + (x^3 + x^2 + x)y = x^5 + x^4 + x^3 + x$
8.14	$y^2 + (x^3 + 1)y = x^5 + x^4 + x^3 + x$
8.15	$y^2 + (x^3 + 1)y = x^5 + x^2 + x$

Label	Curve
8.16	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^2 + x$
8.17	$y^2 + (x^3 + x^2 + x)y = x^5 + x^4 + x^2 + x$
8.18	$y^2 + (x^2 + x + 1)y = x^5 + x^3 + x^2 + x$
8.19	$y^2 + (x^3 + x^2 + x)y = x^5 + x^3 + x^2 + x$
8.20	$y^2 + (x^3 + 1)y = x^5 + x^3 + x^2 + x$
8.21	$y^2 + (x^3 + x^2 + x)y = x^5 + 1$
8.22	$y^2 + (x^3 + x^2 + x)y = x^5 + x^4 + x^3 + 1$
8.23	$y^2 + (x^3 + x^2 + x)y = x^5 + x^4 + x^2 + 1$
8.24	$y^2 + (x^3 + x^2 + x)y = x^5 + x^3 + x^2 + 1$
8.25	$y^2 + (x^2 + x + 1)y = x^6 + x^4$
8.26	$y^2 + (x^2 + x + 1)y = x^6 + x^3$
8.27	$y^2 + (x^2 + x + 1)y = x^6 + x^2$
8.28	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^3 + x^2$
8.29	$y^2 + (x^2 + x + 1)y = x^6 + x$
8.30	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^3 + x$
8.31	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^2 + x$
8.32	$y^2 + (x^2 + x + 1)y = x^6 + x^3 + x^2 + x$
9.1	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4$
9.2	$y^2 + (x^3 + x + 1)y = x^5 + x^4$
9.3	$y^2 + (x^3 + x + 1)y = x^5 + x^3$
9.4	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3 + x^2$

Label	Curve
9.5	$y^2 + (x^3 + x^2 + 1)y = x^5 + x$
9.6	$y^2 + (x^3 + x + 1)y = x^5 + x$
9.7	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3 + x$
9.8	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + x^2 + x$
10.1	$y^2 + y = x^5 + x^4 + x^3$
10.2	$y^2 + y = x^5 + x^3 + x^2$
10.3	$y^2 + y = x^5 + x^3 + x$
10.4	$y^2 + x^3y = x^5 + x^3 + x$
10.5	$y^2 + y = x^5 + x^4 + x^3 + x^2 + x$
10.6	$y^2 + x^3y = x^5 + x^4 + x^3 + x^2 + x$
10.7	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4 + 1$
10.8	$y^2 + y = x^5 + x^4 + x^3 + 1$
10.9	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^2 + 1$
10.10	$y^2 + y = x^5 + x^3 + x^2 + 1$
10.11	$y^2 + x^3y = x^5 + x + 1$
10.12	$y^2 + y = x^5 + x^3 + x + 1$
10.13	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^3 + x + 1$
10.14	$y^2 + x^3y = x^5 + x^4 + x^2 + x + 1$
10.15	$y^2 + y = x^5 + x^4 + x^3 + x^2 + x + 1$
10.16	$y^2 + (x^3 + x^2 + x + 1)y = x^5 + x^4 + x^3 + x^2 + x + 1$
10.17	$y^2 + y = x^6 + x^5 + x^4$

Label	Curve
10.18	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4$
10.19	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^3$
10.20	$y^2 + y = x^6 + x^5 + x^2$
10.21	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^2$
10.22	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x^3 + x^2$
10.23	$y^2 + y = x^6 + x^5 + x$
10.24	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x$
10.25	$y^2 + x^3y = x^6 + x^5 + x^3 + x$
10.26	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^3 + x$
10.27	$y^2 + x^3y = x^6 + x^4 + x^3 + x$
10.28	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^2 + x$
10.29	$y^2 + y = x^6 + x^5 + x^4 + x^2 + x$
10.30	$y^2 + x^3y = x^6 + x^3 + x^2 + x$
10.31	$y^2 + x^3y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
10.32	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
10.33	$y^2 + y = x^6 + x^5 + x^4 + 1$
10.34	$y^2 + y = x^6 + x^5 + x^2 + 1$
10.35	$y^2 + y = x^6 + x^5 + x + 1$
10.36	$y^2 + x^3y = x^6 + x^5 + x + 1$
10.37	$y^2 + x^3y = x^6 + x^4 + x + 1$
10.38	$y^2 + x^3y = x^6 + x^2 + x + 1$

Label	Curve
10.39	$y^2 + y = x^6 + x^5 + x^4 + x^2 + x + 1$
10.40	$y^2 + x^3y = x^6 + x^5 + x^4 + x^2 + x + 1$
11.1	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^3$
11.2	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^2$
11.3	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x$
11.4	$y^2 + (x^3 + x^2 + x)y = x^5 + x^2 + x$
11.5	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^3 + x^2 + x$
11.6	$y^2 + (x^3 + x^2 + x)y = x^5 + x^4 + x^3 + x^2 + x$
11.7	$y^2 + (x^2 + x + 1)y = x^5 + 1$
11.8	$y^2 + (x^3 + x^2 + x)y = x^5 + x^4 + 1$
11.9	$y^2 + (x^3 + x^2 + x)y = x^5 + x^3 + 1$
11.10	$y^2 + (x^3 + 1)y = x^5 + x^4 + x^2 + 1$
11.11	$y^2 + (x^2 + x + 1)y = x^5 + x^3 + x^2 + 1$
11.12	$y^2 + (x^3 + 1)y = x^5 + x^4 + x^3 + x^2 + 1$
11.13	$y^2 + (x^3 + 1)y = x^5 + x + 1$
11.14	$y^2 + (x^2 + x + 1)y = x^5 + x^3 + x + 1$
11.15	$y^2 + (x^3 + 1)y = x^5 + x^3 + x + 1$
11.16	$y^2 + (x^2 + x + 1)y = x^5 + x^2 + x + 1$
11.17	$y^2 + (x^2 + x + 1)y = x^6$
11.18	$y^2 + (x^3 + 1)y = x^6$
11.19	$y^2 + (x^3 + 1)y = x^6 + x^3$

Label	Curve
11.20	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^4 + x^2$
11.21	$y^2 + (x^2 + x + 1)y = x^6 + x^3 + x^2$
11.22	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^4 + x^3 + x^2$
11.23	$y^2 + (x^3 + x^2 + x)y = x^6 + x$
11.24	$y^2 + (x^3 + 1)y = x^6 + x^5 + x$
11.25	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^4 + x$
11.26	$y^2 + (x^2 + x + 1)y = x^6 + x^3 + x$
11.27	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^3 + x$
11.28	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^3 + x$
11.29	$y^2 + (x^3 + x^2 + x)y = x^6 + x^4 + x^3 + x$
11.30	$y^2 + (x^2 + x + 1)y = x^6 + x^2 + x$
11.31	$y^2 + (x^3 + 1)y = x^6 + x^4 + x^2 + x$
11.32	$y^2 + (x^3 + 1)y = x^6 + x^4 + x^3 + x^2 + x$
11.33	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^3 + 1$
11.34	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^2 + 1$
11.35	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^2 + 1$
11.36	$y^2 + (x^3 + x^2 + x)y = x^6 + x^4 + x^2 + 1$
11.37	$y^2 + (x^3 + x^2 + x)y = x^6 + x^3 + x^2 + 1$
11.38	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^4 + x^3 + x^2 + 1$
11.39	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x + 1$
11.40	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^3 + x^2 + x + 1$

Label	Curve
12.1	$y^2 + xy = x^5 + x^4 + x$
12.2	$y^2 + xy = x^5 + x^3 + x$
12.3	$y^2 + (x^2)y = x^5 + x^3 + x$
12.4	$y^2 + (x^2)y = x^5 + x^2 + x$
12.5	$y^2 + (x + 1)y = x^5 + 1$
12.6	$y^2 + xy = x^5 + x^4 + 1$
12.7	$y^2 + (x^2 + 1)y = x^5 + x^4 + 1$
12.8	$y^2 + xy = x^5 + x^3 + 1$
12.9	$y^2 + (x^2 + 1)y = x^5 + x^4 + x^2 + 1$
12.10	$y^2 + (x + 1)y = x^5 + x^4 + x^3 + x^2 + 1$
12.11	$y^2 + (x + 1)y = x^5 + x + 1$
12.12	$y^2 + (x^2)y = x^5 + x + 1$
12.13	$y^2 + (x^2 + 1)y = x^5 + x^4 + x^3 + x + 1$
12.14	$y^2 + (x^2)y = x^5 + x^3 + x^2 + x + 1$
12.15	$y^2 + (x + 1)y = x^5 + x^4 + x^3 + x^2 + x + 1$
12.16	$y^2 + (x^2 + 1)y = x^5 + x^4 + x^3 + x^2 + x + 1$
12.17	$y^2 + (x^3 + x^2)y = x^6 + x$
12.18	$y^2 + xy = x^6 + x^5 + x$
12.19	$y^2 + (x^3 + x^2)y = x^6 + x^5 + x$
12.20	$y^2 + (x^2)y = x^6 + x^3 + x$
12.21	$y^2 + xy = x^6 + x^5 + x^4 + x^3 + x$

Label	Curve
12.22	$y^2 + (x^2)y = x^6 + x^2 + x$
12.23	$y^2 + (x^3 + x)y = x^6 + x^2 + x$
12.24	$y^2 + (x^3 + x)y = x^6 + x^4 + x^2 + x$
12.25	$y^2 + (x^3 + x)y = x^6 + x^5 + x^3 + x^2 + x$
12.26	$y^2 + (x^3 + x^2)y = x^6 + x^4 + x^3 + x^2 + x$
12.27	$y^2 + (x^3 + x^2)y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
12.28	$y^2 + (x^3 + x)y = x^6 + x^5 + x^4 + x^3 + x^2 + x$
12.29	$y^2 + xy = x^6 + x^5 + 1$
12.30	$y^2 + (x^2 + 1)y = x^6 + x^4 + x^3 + 1$
12.31	$y^2 + xy = x^6 + x^5 + x^4 + x^3 + 1$
12.32	$y^2 + (x + 1)y = x^6 + x^5 + x^4 + x^3 + 1$
12.33	$y^2 + (x + 1)y = x^6 + x^5 + x^2 + 1$
12.34	$y^2 + (x^3 + x)y = x^6 + x^5 + x^2 + 1$
12.35	$y^2 + (x^3 + x)y = x^6 + x^5 + x^4 + x^2 + 1$
12.36	$y^2 + (x^3 + x)y = x^6 + x^3 + x^2 + 1$
12.37	$y^2 + (x^2 + 1)y = x^6 + x^4 + x^3 + x^2 + 1$
12.38	$y^2 + (x^3 + x)y = x^6 + x^4 + x^3 + x^2 + 1$
12.39	$y^2 + (x^2)y = x^6 + x + 1$
12.40	$y^2 + (x^2 + 1)y = x^6 + x^4 + x + 1$
12.41	$y^2 + (x^3 + x^2)y = x^6 + x^4 + x + 1$
12.42	$y^2 + (x^3 + x^2)y = x^6 + x^5 + x^4 + x + 1$

Label	Curve
12.43	$y^2 + (x+1)y = x^6 + x^5 + x^4 + x^3 + x + 1$
12.44	$y^2 + (x+1)y = x^6 + x^5 + x^2 + x + 1$
12.45	$y^2 + (x^2+1)y = x^6 + x^4 + x^2 + x + 1$
12.46	$y^2 + (x^2)y = x^6 + x^3 + x^2 + x + 1$
12.47	$y^2 + (x^3+x^2)y = x^6 + x^3 + x^2 + x + 1$
12.48	$y^2 + (x^3+x^2)y = x^6 + x^5 + x^3 + x^2 + x + 1$
13.1	$y^2 + (x^2)y = x^5 + x^4 + x$
13.2	$y^2 + xy = x^5 + x^2 + x$
13.3	$y^2 + xy = x^5 + x^4 + x^3 + x^2 + x$
13.4	$y^2 + (x^2)y = x^5 + x^4 + x^3 + x^2 + x$
13.5	$y^2 + (x^2+1)y = x^5 + 1$
13.6	$y^2 + (x+1)y = x^5 + x^3 + 1$
13.7	$y^2 + xy = x^5 + x^2 + 1$
13.8	$y^2 + (x^2+1)y = x^5 + x^2 + 1$
13.9	$y^2 + (x+1)y = x^5 + x^4 + x^2 + 1$
13.10	$y^2 + xy = x^5 + x^4 + x^3 + x^2 + 1$
13.11	$y^2 + (x+1)y = x^5 + x^3 + x + 1$
13.12	$y^2 + (x^2+1)y = x^5 + x^3 + x + 1$
13.13	$y^2 + (x^2)y = x^5 + x^4 + x^3 + x + 1$
13.14	$y^2 + (x+1)y = x^5 + x^4 + x^2 + x + 1$
13.15	$y^2 + (x^2)y = x^5 + x^4 + x^2 + x + 1$

Label	Curve
13.16	$y^2 + (x^2 + 1)y = x^5 + x^3 + x^2 + x + 1$
13.17	$y^2 + (x^3 + x)y = x^6 + x$
13.18	$y^2 + (x^2)y = x^6 + x^4 + x$
13.19	$y^2 + (x^3 + x)y = x^6 + x^4 + x$
13.20	$y^2 + (x^3 + x^2)y = x^6 + x^3 + x$
13.21	$y^2 + (x^3 + x^2)y = x^6 + x^5 + x^3 + x$
13.22	$y^2 + (x^3 + x)y = x^6 + x^5 + x^3 + x$
13.23	$y^2 + (x^3 + x)y = x^6 + x^5 + x^4 + x^3 + x$
13.24	$y^2 + (x^3 + x^2)y = x^6 + x^4 + x^2 + x$
13.25	$y^2 + xy = x^6 + x^5 + x^4 + x^2 + x$
13.26	$y^2 + (x^3 + x^2)y = x^6 + x^5 + x^4 + x^2 + x$
13.27	$y^2 + xy = x^6 + x^5 + x^3 + x^2 + x$
13.28	$y^2 + (x^2)y = x^6 + x^4 + x^3 + x^2 + x$
13.29	$y^2 + (x^3 + x)y = x^6 + x^5 + 1$
13.30	$y^2 + (x + 1)y = x^6 + x^5 + x^4 + 1$
13.31	$y^2 + (x^3 + x)y = x^6 + x^5 + x^4 + 1$
13.32	$y^2 + (x^2 + 1)y = x^6 + x^3 + 1$
13.33	$y^2 + (x^3 + x)y = x^6 + x^3 + 1$
13.34	$y^2 + (x^3 + x)y = x^6 + x^4 + x^3 + 1$
13.35	$y^2 + xy = x^6 + x^5 + x^4 + x^2 + 1$
13.36	$y^2 + (x^2 + 1)y = x^6 + x^3 + x^2 + 1$

Label	Curve
13.37	$y^2 + xy = x^6 + x^5 + x^3 + x^2 + 1$
13.38	$y^2 + (x+1)y = x^6 + x^5 + x^3 + x^2 + 1$
13.39	$y^2 + (x^2+1)y = x^6 + x + 1$
13.40	$y^2 + (x+1)y = x^6 + x^5 + x^4 + x + 1$
13.41	$y^2 + (x^2)y = x^6 + x^4 + x^3 + x + 1$
13.42	$y^2 + (x^3+x^2)y = x^6 + x^4 + x^3 + x + 1$
13.43	$y^2 + (x^3+x^2)y = x^6 + x^5 + x^4 + x^3 + x + 1$
13.44	$y^2 + (x^2+1)y = x^6 + x^2 + x + 1$
13.45	$y^2 + (x^3+x^2)y = x^6 + x^2 + x + 1$
13.46	$y^2 + (x^3+x^2)y = x^6 + x^5 + x^2 + x + 1$
13.47	$y^2 + (x^2)y = x^6 + x^4 + x^2 + x + 1$
13.48	$y^2 + (x+1)y = x^6 + x^5 + x^3 + x^2 + x + 1$
14.1	$y^2 + (x^2+x)y = x^5 + x^4 + x$
14.2	$y^2 + (x^2+x)y = x^5 + x^4 + x^3 + x$
14.3	$y^2 + (x^2+x)y = x^5 + x^2 + x$
14.4	$y^2 + (x^2+x)y = x^5 + x^3 + x^2 + x$
14.5	$y^2 + (x^2+x)y = x^5 + 1$
14.6	$y^2 + (x^2+x)y = x^5 + x^3 + 1$
14.7	$y^2 + (x^2+x)y = x^5 + x^4 + x^2 + 1$
14.8	$y^2 + (x^2+x)y = x^5 + x^4 + x^3 + x^2 + 1$
14.9	$y^2 + (x^2+x)y = x^6 + x$

Label	Curve
14.10	$y^2 + (x^2 + x)y = x^6 + x^3 + x$
14.11	$y^2 + (x^2 + x)y = x^6 + x^4 + x^2 + x$
14.12	$y^2 + (x^2 + x)y = x^6 + x^4 + x^3 + x^2 + x$
14.13	$y^2 + (x^2 + x)y = x^6 + x^4 + 1$
14.14	$y^2 + (x^2 + x)y = x^6 + x^4 + x^3 + 1$
14.15	$y^2 + (x^2 + x)y = x^6 + x^2 + 1$
14.16	$y^2 + (x^2 + x)y = x^6 + x^3 + x^2 + 1$
15.1	$y^2 + y = x^5 + x^4 + 1$
15.2	$y^2 + y = x^5 + x^2 + 1$
15.3	$y^2 + y = x^5 + x + 1$
15.4	$y^2 + y = x^5 + x^4 + x^2 + x + 1$
15.5	$y^2 + x^3y = x^6 + x^5 + x$
15.6	$y^2 + x^3y = x^6 + x^4 + x$
15.7	$y^2 + x^3y = x^6 + x^2 + x$
15.8	$y^2 + x^3y = x^6 + x^5 + x^4 + x^2 + x$
15.9	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4 + 1$
15.10	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^3 + 1$
15.11	$y^2 + y = x^6 + x^5 + x^4 + x^3 + 1$
15.12	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^2 + 1$
15.13	$y^2 + y = x^6 + x^5 + x^3 + x^2 + 1$
15.14	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x^3 + x^2 + 1$

Label	Curve
15.15	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x + 1$
15.16	$y^2 + y = x^6 + x^5 + x^3 + x + 1$
15.17	$y^2 + x^3y = x^6 + x^5 + x^3 + x + 1$
15.18	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^3 + x + 1$
15.19	$y^2 + x^3y = x^6 + x^4 + x^3 + x + 1$
15.20	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^2 + x + 1$
15.21	$y^2 + x^3y = x^6 + x^3 + x^2 + x + 1$
15.22	$y^2 + y = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
15.23	$y^2 + x^3y = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
15.24	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
16.1	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + 1$
16.2	$y^2 + (x^2 + x + 1)y = x^5 + x^3 + 1$
16.3	$y^2 + (x^2 + x + 1)y = x^5 + x^2 + 1$
16.4	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^3 + x^2 + 1$
16.5	$y^2 + (x^2 + x + 1)y = x^5 + x + 1$
16.6	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^3 + x + 1$
16.7	$y^2 + (x^2 + x + 1)y = x^5 + x^4 + x^2 + x + 1$
16.8	$y^2 + (x^2 + x + 1)y = x^5 + x^3 + x^2 + x + 1$
16.9	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x$
16.10	$y^2 + (x^3 + x^2 + x)y = x^6 + x^4 + x$
16.11	$y^2 + (x^3 + x^2 + x)y = x^6 + x^3 + x$

Label	Curve
16.12	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^4 + x^3 + x$
16.13	$y^2 + (x^3 + x^2 + x)y = x^6 + x^2 + x$
16.14	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^4 + x^2 + x$
16.15	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^3 + x^2 + x$
16.16	$y^2 + (x^3 + x^2 + x)y = x^6 + x^4 + x^3 + x^2 + x$
16.17	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + 1$
16.18	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + 1$
16.19	$y^2 + (x^3 + x^2 + x)y = x^6 + x^4 + 1$
16.20	$y^2 + (x^3 + 1)y = x^6 + x^4 + 1$
16.21	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^4 + 1$
16.22	$y^2 + (x^2 + x + 1)y = x^6 + x^3 + 1$
16.23	$y^2 + (x^3 + x^2 + x)y = x^6 + x^3 + 1$
16.24	$y^2 + (x^3 + 1)y = x^6 + x^4 + x^3 + 1$
16.25	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^4 + x^3 + 1$
16.26	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^4 + x^3 + 1$
16.27	$y^2 + (x^2 + x + 1)y = x^6 + x^2 + 1$
16.28	$y^2 + (x^3 + x^2 + x)y = x^6 + x^2 + 1$
16.29	$y^2 + (x^3 + 1)y = x^6 + x^2 + 1$
16.30	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^2 + 1$
16.31	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^4 + x^2 + 1$
16.32	$y^2 + (x^3 + 1)y = x^6 + x^3 + x^2 + 1$

Label	Curve
16.33	$y^2 + (x^3 + x^2 + x)y = x^6 + x^5 + x^3 + x^2 + 1$
16.34	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^3 + x^2 + 1$
16.35	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^3 + x^2 + 1$
16.36	$y^2 + (x^3 + x^2 + x)y = x^6 + x^4 + x^3 + x^2 + 1$
16.37	$y^2 + (x^2 + x + 1)y = x^6 + x + 1$
16.38	$y^2 + (x^3 + 1)y = x^6 + x^4 + x + 1$
16.39	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^4 + x + 1$
16.40	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^3 + x + 1$
16.41	$y^2 + (x^3 + 1)y = x^6 + x^4 + x^3 + x + 1$
16.42	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^4 + x^3 + x + 1$
16.43	$y^2 + (x^3 + 1)y = x^6 + x^2 + x + 1$
16.44	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^2 + x + 1$
16.45	$y^2 + (x^2 + x + 1)y = x^6 + x^4 + x^2 + x + 1$
16.46	$y^2 + (x^2 + x + 1)y = x^6 + x^3 + x^2 + x + 1$
16.47	$y^2 + (x^3 + 1)y = x^6 + x^3 + x^2 + x + 1$
16.48	$y^2 + (x^3 + 1)y = x^6 + x^5 + x^3 + x^2 + x + 1$
17.1	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + 1$
17.2	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + 1$
17.3	$y^2 + (x^3 + x + 1)y = x^5 + x^3 + 1$
17.4	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3 + x^2 + 1$
17.5	$y^2 + (x^3 + x^2 + 1)y = x^5 + x + 1$

Label	Curve
17.6	$y^2 + (x^3 + x + 1)y = x^5 + x + 1$
17.7	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3 + x + 1$
17.8	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + x^2 + x + 1$
17.9	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4$
17.10	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4$
17.11	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^3$
17.12	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^3$
17.13	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^2$
17.14	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^2$
17.15	$y^2 + (x^3 + x + 1)y = x^6 + x^3 + x^2$
17.16	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^3 + x^2$
17.17	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x$
17.18	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x$
17.19	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^3 + x$
17.20	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x$
17.21	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^2 + x$
17.22	$y^2 + (x^3 + x + 1)y = x^6 + x^2 + x$
17.23	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^3 + x^2 + x$
17.24	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^3 + x^2 + x$
17.25	$y^2 + (x^3 + x^2 + 1)y = x^6 + 1$
17.26	$y^2 + (x^3 + x + 1)y = x^6 + 1$

Label	Curve
17.27	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^3 + 1$
17.28	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^3 + 1$
17.29	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^2 + 1$
17.30	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^2 + 1$
17.31	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^3 + x^2 + 1$
17.32	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + 1$
17.33	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x + 1$
17.34	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x + 1$
17.35	$y^2 + (x^3 + x + 1)y = x^6 + x^3 + x + 1$
17.36	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^3 + x + 1$
17.37	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^2 + x + 1$
17.38	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^2 + x + 1$
17.39	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^3 + x^2 + x + 1$
17.40	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^3 + x^2 + x + 1$
18.1	$y^2 + y = x^5 + x^3 + 1$
18.2	$y^2 + y = x^5 + x^4 + x^3 + x^2 + 1$
18.3	$y^2 + y = x^5 + x^4 + x^3 + x + 1$
18.4	$y^2 + y = x^5 + x^3 + x^2 + x + 1$
18.5	$y^2 + x^3y = x^6 + x^3 + x$
18.6	$y^2 + x^3y = x^6 + x^5 + x^4 + x^3 + x$
18.7	$y^2 + x^3y = x^6 + x^5 + x^3 + x^2 + x$

Label	Curve
18.8	$y^2 + x^3y = x^6 + x^4 + x^3 + x^2 + x$
18.9	$y^2 + y = x^6 + x^5 + 1$
18.10	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + 1$
18.11	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x^3 + 1$
18.12	$y^2 + y = x^6 + x^5 + x^4 + x^2 + 1$
18.13	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4 + x^2 + 1$
18.14	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^3 + x^2 + 1$
18.15	$y^2 + x^3y = x^6 + x + 1$
18.16	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x + 1$
18.17	$y^2 + y = x^6 + x^5 + x^4 + x + 1$
18.18	$y^2 + x^3y = x^6 + x^5 + x^4 + x + 1$
18.19	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x + 1$
18.20	$y^2 + y = x^6 + x^5 + x^2 + x + 1$
18.21	$y^2 + x^3y = x^6 + x^5 + x^2 + x + 1$
18.22	$y^2 + x^3y = x^6 + x^4 + x^2 + x + 1$
18.23	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^4 + x^2 + x + 1$
18.24	$y^2 + (x^3 + x^2 + x + 1)y = x^6 + x^5 + x^3 + x^2 + x + 1$
19.1	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^3 + 1$
19.2	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^2 + 1$
19.3	$y^2 + (x^3 + x + 1)y = x^5 + x^2 + 1$
19.4	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^3 + x^2 + 1$

Label	Curve
19.5	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3 + x + 1$
19.6	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^2 + x + 1$
19.7	$y^2 + (x^3 + x + 1)y = x^5 + x^4 + x^2 + x + 1$
19.8	$y^2 + (x^3 + x + 1)y = x^5 + x^3 + x^2 + x + 1$
19.9	$y^2 + (x^3 + x^2 + 1)y = x^6$
19.10	$y^2 + (x^3 + x + 1)y = x^6$
19.11	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^3$
19.12	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^3$
19.13	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^2$
19.14	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^2$
19.15	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^3 + x^2$
19.16	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2$
19.17	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x$
19.18	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x$
19.19	$y^2 + (x^3 + x + 1)y = x^6 + x^3 + x$
19.20	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^3 + x$
19.21	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^2 + x$
19.22	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^2 + x$
19.23	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^3 + x^2 + x$
19.24	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^3 + x^2 + x$
19.25	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + 1$

Label	Curve
19.26	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + 1$
19.27	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^3 + 1$
19.28	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^3 + 1$
19.29	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^2 + 1$
19.30	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^2 + 1$
19.31	$y^2 + (x^3 + x + 1)y = x^6 + x^3 + x^2 + 1$
19.32	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + 1$
19.33	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x + 1$
19.34	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x + 1$
19.35	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^3 + x + 1$
19.36	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x + 1$
19.37	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^2 + x + 1$
19.38	$y^2 + (x^3 + x + 1)y = x^6 + x^2 + x + 1$
19.39	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^3 + x^2 + x + 1$
19.40	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^3 + x^2 + x + 1$
20.1	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + 1$
20.2	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + 1$
20.3	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^3 + 1$
20.4	$y^2 + (x^3 + x + 1)y = x^6 + x^3 + 1$
20.5	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^2 + 1$
20.6	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^2 + 1$

Label	Curve
20.7	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^3 + x^2 + 1$
20.8	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^3 + x^2 + 1$
20.9	$y^2 + (x^3 + x + 1)y = x^6 + x + 1$
20.10	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x + 1$
20.11	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^3 + x + 1$
20.12	$y^2 + (x^3 + x + 1)y = x^6 + x^4 + x^3 + x + 1$
20.13	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^2 + x + 1$
20.14	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^4 + x^2 + x + 1$
20.15	$y^2 + (x^3 + x^2 + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
20.16	$y^2 + (x^3 + x + 1)y = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$