Dynamical Systems and Zeta Functions of Function Fields

Daniel Nichols

Follow this and additional works at: https://scholarworks.umass.edu/dissertations_2

Part of the Number Theory Commons

Recommended Citation
https://scholarworks.umass.edu/dissertations_2/941

This Open Access Dissertation is brought to you for free and open access by the Dissertations and Theses at ScholarWorks@UMass Amherst. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact scholarworks@library.umass.edu.
DYNAMICAL SYSTEMS AND ZETA FUNCTIONS OF FUNCTION FIELDS

A Dissertation Presented
by
DANIEL NICHOLS

Submitted to the Graduate School of the University of Massachusetts Amherst in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2017

Mathematics and Statistics
DYNAMICAL SYSTEMS AND ZETA FUNCTIONS OF
FUNCTION FIELDS

A Dissertation Presented

by

DANIEL NICHOLS

Approved as to style and content by:

________________________________________
Siman Wong, Chair

________________________________________
Tom Weston, Member

________________________________________
Paul Gunnells, Member

________________________________________
David Mix Barrington, Member

________________________________________
Farshid Hajir, Department Chair
Mathematics and Statistics
ACKNOWLEDGMENTS

Of the many people to whom I owe sincere thanks, first and foremost is my advisor, Dr. Siman Wong. Throughout my time as a graduate student I have relied on his guidance and encouragement. I truly could not have asked for a more supportive mentor, or for a better role model as a researcher and teacher.

I am also very grateful to Drs. Paul Gunnells, Tom Weston, and David Mix Barrington for serving on my dissertation committee, and to many other wonderful people among the UMass mathematics department faculty and staff. In particular I should thank Dr. Hans Johnston, who helped immensely with the computational aspects of these projects, and Lian Duan, with whom I had many helpful discussions about arithmetic geometry.

Finally, I would like to thank Brad and Susan Nichols, my parents and biggest fans.
ABSTRACT

DYNAMICAL SYSTEMS AND ZETA FUNCTIONS OF FUNCTION FIELDS

MAY 2017

DANIEL NICHOLS

B.Sc., RENSSELAER POLYTECHNIC UNIVERSITY
M.Sc., UNIVERSITY OF MASSACHUSETTS AMHERST
Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Siman Wong

This doctoral dissertation concerns two problems in number theory. First, we examine a family of discrete dynamical systems in $\mathbb{F}_2[t]$ analogous to the $3x + 1$ system on the positive integers. We prove a statistical result about the large-scale dynamics of these systems that is stronger than the analogous theorem in $\mathbb{Z}$. We also investigate $mx + 1$ systems in rings of functions over a family of algebraic curves over $\mathbb{F}_2$ and prove a similar result there.

Second, we describe some interesting properties of zeta functions of algebraic curves. Generally $L$-functions vanish only to the order required by their root number. However, we demonstrate that for a certain class of quaternion extensions of $\mathbb{F}_p(t)$,
the zeta function vanishes at a higher order than the root number demands, indicating some other phenomenon at work.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>ACKNOWLEDGMENTS</th>
<th>iv</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>ix</td>
</tr>
</tbody>
</table>

## CHAPTER

### 1. INTRODUCTION

#### 2. $mx + 1$ SYSTEMS IN FUNCTION FIELDS OVER $\mathbb{F}_2$

| 2.1 Background: the $3x + 1$ problem                                                                 | 6   |
| 2.2 The $mx + 1$ problem in $\mathbb{F}_2[t]$                                                      | 10  |
| 2.3 Analogue of Terras’ theorem for $\mathbb{F}_2[t]$                                           | 13  |
| 2.4 The $mx + 1$ problem in the ring of functions on an algebraic curve                           | 26  |
| 2.5 Analogue of Terras’ theorem for $R_r$                                                       | 28  |
| 2.6 Experimental Data                                                                       | 37  |
| 2.6.1 $\mathbb{F}_2[t]$                                                                      | 37  |
| 2.6.1.1 Stopping times                                                                      | 39  |
| 2.6.2 $R_r$                                                                                  | 41  |
| 2.7 Future work                                                                             | 42  |
3. ORDERS OF VANISHING OF L-FUNCTIONS AT THE POINT $s = 1/2$ ........................................... 44

3.1 L-functions ................................................................. 44
3.2 The zeta function of a function field .................................. 46
3.3 Algebraic curves over a finite field .................................... 47
  3.3.1 The zeta function of an algebraic curve ......................... 50
3.4 The search for fields with root number $\pm 1$ ....................... 51
  3.4.1 Witt’s criterion ....................................................... 52
  3.4.2 Global fields and the Hasse Principle .......................... 54
3.5 A family of $\mathbb{F}_p(t)$ extensions with anomalous order of vanishing .... 57
  3.5.1 The zeta function of $L/K$ ......................................... 60
    3.5.1.1 Computing $\# C(\mathbb{F}_{p^2})$ .......................... 61
    3.5.1.2 The zeta function ............................................. 66
3.6 Future work ............................................................... 67

APPENDICES

A. GAMBLER’S RUIN COMPUTATIONS FOR TERRAS’ THEOREM ANALOGUE IN $R$ ................. 68
B. LIST OF FUNCTION FIELDS .................................................. 77
C. MAGMA CODE FOR WORKING WITH QUATERNION EXTENSIONS OF $\mathbb{F}_p(t)$ ................ 95

BIBLIOGRAPHY ................................................................. 101
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>12</td>
</tr>
<tr>
<td>Trajectory of $f = t^2 + 1$ when $m = t^2 + t + 1$. This sequence repeats with period 8.</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>24</td>
</tr>
<tr>
<td>Using Rouche’s theorem to prove that $g_d(z)$ has a unique real root in the unit disk.</td>
<td></td>
</tr>
<tr>
<td>2.3</td>
<td>25</td>
</tr>
<tr>
<td>Finite stopping time probability $P_d$ in $\mathbb{F}_2[t]$.</td>
<td></td>
</tr>
<tr>
<td>2.4</td>
<td>36</td>
</tr>
<tr>
<td>Finite stopping time probability $P_d$ in $R_r$.</td>
<td></td>
</tr>
<tr>
<td>2.5</td>
<td>39</td>
</tr>
<tr>
<td>Degree plot of three disjoint trajectories which appear to diverge.</td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td>40</td>
</tr>
<tr>
<td>Frequency of long stopping times $(\sigma(f) &gt; 10^5)$ for various $m \in \mathbb{F}_2[t]$.</td>
<td></td>
</tr>
<tr>
<td>2.7</td>
<td>41</td>
</tr>
<tr>
<td>Distribution of stopping times among polynomials of degree &lt; 20 for four values of $m$.</td>
<td></td>
</tr>
<tr>
<td>2.8</td>
<td>42</td>
</tr>
<tr>
<td>Density of long stopping times $(\sigma(f) &gt; 10^5)$ for various $m \in R_r$.</td>
<td></td>
</tr>
<tr>
<td>2.9</td>
<td>43</td>
</tr>
<tr>
<td>Frequency of cycles with $\lambda = 2^k$ in set of polynomials up to degree $d$.</td>
<td></td>
</tr>
<tr>
<td>A.1</td>
<td>75</td>
</tr>
<tr>
<td>Using Rouche’s theorem to prove that $g_d(z)$ has a unique real root inside the unit disk.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 1
INTRODUCTION

In this thesis we present the results of two distinct projects in number theory. First, we examine a family of function field dynamical systems analogous to the famous $3x + 1$ problem in $\mathbb{Z}$. Second, we construct explicitly a family of octic function fields of finite characteristic whose zeta functions behave in an unexpected way. The common element shared between these two projects is the principle that many arithmetic problems in $\mathbb{Z}$ have more tractable analogues in $\mathbb{F}_p[t]$.

The integer $3x + 1$ problem concerns the dynamical system defined by iteration of the $3x + 1$ map $T : \mathbb{Z} \to \mathbb{Z}$ defined

$$T(x) = \begin{cases} x/2, & \text{if } x \text{ even} \\ (3x + 1)/2, & \text{if } x \text{ odd.} \end{cases}$$

The Collatz conjecture states that repeated iterations of this map starting from any positive integer $x$ will eventually reach 1. While this conjecture remains unproven, the large-scale stochastic behavior of this system is fairly well understood. Terras [20] in 1976 used a one-dimensional random walk stochastic model to prove that for almost all $x \in \mathbb{Z}$, there exists some positive integer $\sigma(x)$ such that $T^{\sigma(x)}(x) < x$. We call $\sigma(x)$ the stopping time of $x$, and if no such integer exists, we write
\(\sigma(x) = \infty\). One proof of this result proceeds by showing that the **parity sequence** of a uniformly chosen integer \(x < 2^N\) is uniformly distributed in the set of length-\(N\) binary sequences. Roughly speaking, the probability that such a sequence will be so heavily biased that \(\sigma(x) = \infty\) approaches zero as \(N\) grows towards infinity.

In \(\mathbb{F}_2[t]\) we can choose any polynomial \(m\) with constant term 1 and define an \(mx+1\) map \(T : \mathbb{F}_2[t] \to \mathbb{F}_2[t]\) just like the map described above, but with the integers 3 and 2 replaced by \(m\) and \(t\) respectively. Dynamical systems generated by maps of this form have been previously studied by Hicks, Mullen, Yucas, and Zavislak [9] and by Matthews and Leigh [12] among others. In this setting, the systems are slightly easier to handle, and can be even more accurately modeled by a one-dimensional random walk. The analogue of the Collatz conjecture for a given polynomial \(m\) is generally easier to resolve. However, there are still unanswered questions about the distribution of divergent trajectories and cyclic orbits.

The main result of this project is the following theorem for \(mx+1\) systems in \(\mathbb{F}_2[t]\) analogous to that of Terras for \(3x+1\) in \(\mathbb{Z}\).

**Theorem.** Let \(m \in \mathbb{F}_2[t]\) with \(\deg m = d\) and let \(P_m\) be the asymptotic probability that a randomly chosen polynomial in \(\mathbb{F}_2[t]\) has finite \(mx+1\) stopping time. That is,

\[
P_m = \lim_{N \to \infty} P(\sigma(f) < \infty | \deg f < N).
\]

If \(d \leq 2\), then \(P_m = 1\). If \(d > 2\), then \(P_m \in (1/2, 1)\) is the unique real root of the polynomial \(g_d(z) = z^d - 2z + 1\) inside the unit disk.
This theorem is more general than Terras’ $3x + 1$ version in that it covers all values of $m$, and stronger in that it gives the exact probability that a randomly chosen $f \in \mathbb{F}_2[t]$ has finite $\sigma(f)$, rather than just a lower bound. We use the same method of proof as that described above for the original Terras’ theorem, with some additional details.

We then go on to define a new type of dynamical system in coordinate rings of a certain family of algebraic curves. These new systems are a bit more complicated than traditional $mx + 1$ systems, but they share some of the same characteristics. For a given polynomial $r(t) \in \mathbb{F}_2[t]$, let $R_r$ be the coordinate ring of the algebraic curve $x^2 + tx + r(t)$ over $\mathbb{F}_2$. This is a natural generalization from the previous result because $\mathbb{F}_2[t]$ is the coordinate ring of a genus 0 algebraic curve. In this setting we again prove a sharper and more general analogue of Terras’ theorem.

**Theorem.** For $m \in R_r$ of degree $d$, let $P_d$ be the probability that a randomly chosen polynomial in $R_r$ has finite $mx + 1$ stopping time. That is,

$$P_d = \lim_{N \to \infty} P(\sigma(f) < \infty | \deg f < N).$$

If $d \leq 4$, then $P_d = 1$. If $d > 4$, then $P_d \in (3/4, 1)$ is the unique real root of the polynomial $g_d(z) = z^d - 4z + 3$ that lies inside the unit disk.

Lastly, we present some experimental data obtained from our C++ implementation of these polynomial $mx + 1$ systems.

We then turn to our second project, an investigation into the orders of vanishing of certain $L$-functions. An $L$-function is a meromorphic function $L(X, s)$ which
encodes information about an arithmetic object $X$ such as a field extension or Galois representation. The definition of $L(X, s)$ depends on the category of $X$, but in general it is defined as the continuation of a Dirichlet series on some half-plane, and the “completed” $L$-function $\Lambda(X, s)$ should satisfy a functional equation of the form $\Lambda(X, s) = W(X)\Lambda(X, 1 - s)$ where $W(X)$ is a complex number of unit magnitude called the **root number**. Examples of $L$-functions include the Riemann zeta function, the Dedekind zeta function of a number field, the zeta function of a function field, and the Artin $L$-function of a Galois representation.

As a general principle, we expect an $L$-function to vanish at the central point $s = 1/2$ to the lowest order compatible with its root number. For example, if the root number is $-1$, then the functional equation $\Lambda(X, s) = -\Lambda(X, 1 - s)$ requires the function to have at least a simple zero at $s = 1/2$. If an $L$-function vanishes at a higher order than this, it is likely due to some unusual arithmetic property of $X$. The zeroes and poles of $L(X, s)$ have arithmetic significance, so the order of vanishing at $s = 1/2$ of $L(X, s)$ may give us useful arithmetic information about $X$.

We set about constructing a catalog of function field extensions whose $L$-functions vanish at $s = 1/2$ to at least order 2, while the order required by their root numbers is no greater than 1. To do this, we make use of the fact that if $E/F$ is a global field extension with Galois group $G \simeq Q_8$, then the root number of the zeta function of $E/F$ must be $\pm 1$. Under these conditions the expected order of vanishing of $Z(E/F, s)$ is either 0 or 1. To enumerate quaternionic extensions of $\mathbb{F}_p(t)$ we make use of **Witt’s criterion** [10], which states that a biquadratic extension $K(\sqrt{a}, \sqrt{b})$ extends to a quaternion extension $L/K$ if and only if the quadratic form $aX^2 + bY^2 +$
\( abZ^2 \) is \( K \)-equivalent to \( X^2 + Y^2 + Z^2 \). When \( K \) is a global field such as \( \mathbb{F}_p(t) \), the Hasse principle makes this a fairly simple calculation. Witt’s criterion also gives us an explicit formula for a primitive element \( \alpha \) which generates \( L/K \).

From here we proceed in two different directions. First, we use Magma to generate a large number of low-genus quaternion extensions of \( \mathbb{F}_p(t) \) for relatively small \( p \) and to compute the zeta functions of these extensions. The only practical limit here is the computational difficulty of computing zeta functions, which scales exponentially with the genus. We present in appendices some Magma code for generating these extensions and a list of some field extensions with their orders of vanishing.

Second, we prove the following theorem, explicitly constructing an infinite family of \( L \)-functions with anomalous order of vanishing at \( s = 1/2 \).

**Theorem.** Let \( p \equiv 5 \pmod{8} \), let \( w \in (\mathbb{F}_p)^\times \), and let \( K = \mathbb{F}_p(t) \). Let \( a = t + w^2 \) and let \( b = t \). Then the biquadratic extension \( K_{a,b,1} = K(\sqrt{a}, \sqrt{b}) \) extends to a genus 2 quaternion extension \( L = K(\alpha) \), where

\[
\alpha^2 = 1 + \frac{ab^2 + w^2}{2ab^2} \sqrt{b} + \frac{ab^2 - w^2}{2wb^2} \sqrt{a} \sqrt{b}.
\]

Furthermore, the zeta function of \( L/K \) is

\[
Z(L/K, s) = \frac{(1 - p^{1-2s})^2}{(1 - p^{-s})(1 - p^{1-s})}
\]

which vanishes to order 2 at \( s = 1/2 \), while the root number must be \( \pm 1 \).

This is accomplished by counting the points on a hyperelliptic curve model \( Y^2 = X(X^4 - 1) \).
CHAPTER 2

mx + 1 SYSTEMS IN FUNCTION FIELDS OVER \( \mathbb{F}_2 \)

2.1 Background: the 3x + 1 problem

The 3x + 1 function is defined on the set of positive integers as follows:

\[
T(x) = \begin{cases} 
  \frac{x}{2}, & x \equiv 0 \text{ mod } 2 \\
  \frac{3x+1}{2}, & x \not\equiv 0 \text{ mod } 2 
\end{cases}
\]

We denote by \( T^k(x) \) the integer obtained by applying the transformation \( T \) to \( x \) in succession \( k \) times. We call the sequence \( \{T^k(x)\}_{k=0}^{\infty} \) the trajectory of \( x \). It is easy to see that the trajectory of \( x = 1 \) has period 2:

\[
\{T^k(1)\} = 1, 2, 1, 2, 1, 2, \ldots
\]

We call the cycle which contains 1 the trivial cycle. Every trajectory must behave in one of the following ways:

1. The sequence enters the trivial cycle. That is, \( T^k(x) = 1 \) for some \( k \).

2. The sequence enters a nontrivial cycle, i.e. a cycle not containing 1.
3. The sequence diverges. That is, \( \lim_{k \to \infty} T^k(x) = \infty \).

The Collatz conjecture states that (1) is the only one of these possibilities which actually occurs.

**Conjecture 2.1.1** (Collatz). *For every positive \( x \in \mathbb{Z} \), there exists some \( k \) such that \( T^k(x) = 1 \).*

Though this conjecture can be stated in very simple terms, it has so far resisted all attempts at a proof. Even significantly weaker conjectures have not been solved. For example, the following two conjectures remain unproven [11].

**Conjecture 2.1.2** (Finite Cycles Conjecture). *The \( 3x+1 \) function has finitely many cycles, i.e. there are finitely many purely periodic orbits on the integers.*

Notice that if the Collatz conjecture is true, then the only cycle is the trivial cycle, so this conjecture must be true also.

**Conjecture 2.1.3** (Divergent Trajectories Conjecture). *The \( 3x+1 \) function has no divergent trajectory. Equivalently, for any integer \( x \), the trajectory of \( x \) is bounded.*

Again this is clearly implied by the Collatz conjecture. The difficulty of proving such apparently simple statements is a testament to the complexity of the pseudo-random behavior of the \( 3x+1 \) function.

Generalizations of the \( 3x+1 \) problem include the class of so-called \( mx+1 \), functions, where 3 is replaced in the definition above by some other odd positive integer \( m \). For \( m = 5 \), it is conjectured that divergent trajectories do exist. That is,
there exists some \( x \) such that \( \{ T^k(x) \} \) is infinite and nonrepeating. However, this too remains unproven.

We now introduce some additional terminology to help understand this dynamical system. For every positive integer \( x \), the stopping time \( \sigma(x) \) is defined to be the minimum number of steps required for the trajectory starting at \( x \) to reach a number less than \( x \). That is, \( \sigma(x) = \inf \{ k > 0 : T^k(x) < x \} \). If there is no such \( k \), we set \( \sigma(x) = \infty \). Notice that if \( x \) is even, then necessarily \( \sigma(x) = 1 \). If every integer \( x \) has \( \sigma(x) < \infty \), then the Collatz conjecture must be true. On the other hand, any \( x \) with \( \sigma(x) = \infty \) would provide a counterexample to both Conjecture 2.1.1 and Conjecture 2.1.3.

Next, we assign to each positive integer \( x \) a parity sequence \( \{ p_0, p_1, p_2, \ldots \} \), where \( p_k = 0 \) if \( T^k(x) \) is even and \( p_k = 1 \) if \( T^k(x) \) is odd. That is, \( p_k \) is the parity of \( T^k(x) \), which indicates whether \( 2T^{k+1}(x) = 3T^k(x) + 1 \) or whether \( 2T^{k+1}(x) = T^k(x) \). For example, the first six terms of the parity sequence of \( x = 7 \) are \( 1, 1, 1, 0, 1, 0 \).

Terras [20] proved the following theorem concerning stopping times. A simpler proof was provided soon after by Everett [5].

**Theorem 2.1.1.** Almost every positive integer \( x \) has \( \sigma(x) < \infty \). That is,

\[
\lim_{N \to \infty} P(\sigma(x) < \infty \mid 0 < x \leq N) = 1.
\]

Everett’s proof proceeds by first showing that the parity sequences of integers \( 0 < x \leq 2^N \) are distributed uniformly in the set of length-\( N \) binary sequences. That is, given any sequence \( \{ p_0, p_1, \ldots, p_{n-1} \} \) in \( \{0, 1\} \), there is a unique number
0 < x ≤ 2^N such that the first N terms of the parity sequence of x are \( p_0, p_1, \ldots, p_{n-1} \).

This is what justifies the use of a one-dimensional random walk to model the large-scale properties of the 3\( x + 1 \) dynamical system. Specifically, we can model \( \log T^N(x) \) as

\[
\log_2 T^N(x) \lesssim \log_2 x - \left( N - \sum_{i=0}^{N-1} X_i \right) + \left( \log_2 \frac{5}{3} \right) \sum_{i=0}^{N-1} X_i
\]

where \( X_i \) are IID (independent, identically distributed) Bernoulli random variables with \( P(X_i = 0) = P(X_i = 1) = 1/2 \). Let \( b_3 = 1 + \log_2 \frac{5}{3} \). Then

\[
\log_2 \left( \frac{T^k(x)}{x} \right) \lesssim b_3 \left[ \sum_{i=0}^{N-1} X_i - \frac{1}{b_3} N \right].
\]

Therefore the probability that \( T^k(x) \geq x \) for all \( k > 0 \) (or equivalently the probability that \( \sigma(x) = \infty \)) is bounded by the probability that the partial sums of a series of Bernoulli random variables satisfy \( \sum_{i=0}^{N-1} X_i > N/b_3 \) for all \( N \).

Uniformly distributed binary sequences tend to be about half 1’s and half 0’s. Roughly speaking, the number of binary sequences which consistently have enough ones such that \( T^k(x) \) is always greater than \( x \) have density zero. Everett used this method to complete the proof of Theorem 2.1.1.

Because the multiplicative random walk is not perfectly accurate, this only provides an upper bound (which happens to be 0) on the probability of infinite stopping time. For higher values of \( m \), e.g. \( m = 5 \), we have \( 0 < P(\sigma(x) = \infty) < 1/2 \), and in
these cases we can only obtain an upper bound for the probability of infinite stopping time. We state a version of this fact in the following theorem.

**Theorem 2.1.2.** Let $m > 1$ be an odd positive integer and let $P_m$ be the probability that a randomly chosen positive integer $x$ has infinite $mx + 1$ stopping time. Then

$$\frac{1}{2} \geq P_m \geq P\left(\sum_{i=0}^{N-1} X_i > \frac{1}{b_m} N \quad \forall N > 0\right)$$

where $X_i$ are IID Bernoulli variables with $p = 1/2$, and $b_m = \log(m + 2/3)$.

This explains how the tendency of this stochastic model for $mx + 1$ is influenced by $b_m$.

### 2.2 The $mx + 1$ problem in $\mathbb{F}_2[t]$

We now turn to a class of similar $mx + 1$ dynamical systems in $\mathbb{F}_2[t]$ which can also be modeled by a random walk. Like those who have previously studied these systems, we are motivated by the principle that problems concerning $\mathbb{F}_p[t]$ are often easier to solve than the corresponding problems in $\mathbb{Z}$, since we can often exploit the rich algebraic structure of polynomial rings over a field to simplify both numerical computations and theoretical analysis. The random walk model for $mx + 1$ systems turns out to be even more accurate in $\mathbb{F}_2[t]$ than in the integer case. We show that in a certain sense the random walks associated to these polynomial $mx + 1$ problems interpolate between those of the traditional $mx + 1$ problems in $\mathbb{Z}$, providing examples of a more general class of pseudo-random dynamical systems.
Let \( m \in \mathbb{F}_2[t] \) be a fixed odd polynomial (meaning \( m(0) = 1 \)). The \( mx + 1 \) map \( T : \mathbb{F}_2[t] \to \mathbb{F}_2[t] \) is defined by the formula

\[
T(f) = \begin{cases} 
\frac{f}{t}, & f \equiv 0 \mod t \\
\frac{mf+1}{t}, & f \not\equiv 0 \mod t,
\end{cases}
\]

Iteration of this function defines a discrete dynamical system on \( \mathbb{F}_2[t] \). Given a starting element \( f \in \mathbb{F}_2[t] \), we call the sequence \( \{f, T(f), T^2(f), T^3(f), \ldots\} \) the trajectory of \( x \). Each trajectory must either become cyclic at some point or else diverge, meaning

\[
\lim_{k \to \infty} \deg T^k(f) = \infty.
\]

When we view each element of \( \mathbb{F}_2[t] \) as sequence of binary coefficients, there is a natural set bijection between \( \mathbb{F}_2[t] \) and the ring of nonnegative integers with binary representation. In that sense, the \( mx + 1 \) system in \( \mathbb{F}_2[t] \) can be viewed as a dynamical system on the positive integers similar to the one defined by the original \( 3x + 1 \) function. It is natural to consider the analogue of the Collatz conjecture in this setting. That is, for a given polynomial \( m \in \mathbb{F}_2[t] \), does every \( mx + 1 \) trajectory in \( \mathbb{F}_2[t] \) eventually reach 1?

Hicks, Mullen, Yucas, and Zavislak [9] were able to prove that for \( m = t + 1 \), all sequences eventually reach 1. Therefore the conjecture is true when \( m = t + 1 \). However, for most choices of \( m \) we can easily find nontrivial cycles. For example, when \( m = t^2 + t + 1 \), the trajectory of \( f = t^2 + 1 \) is cyclic with period 8, as shown in Figure 2.1. The existence of this cycle disproves the Collatz conjecture analogue for \( m = t^2 + t + 1 \).
Figure 2.1. Trajectory of $f = t^2 + 1$ when $m = t^2 + t + 1$. This sequence repeats with period 8.

<table>
<thead>
<tr>
<th>$k$</th>
<th>$T^k(f)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$t^2 + 1$</td>
</tr>
<tr>
<td>1</td>
<td>$t^3 + t^2 + 1$</td>
</tr>
<tr>
<td>2</td>
<td>$t^4 + 1$</td>
</tr>
<tr>
<td>3</td>
<td>$t^5 + t^4 + t^3 + t + 1$</td>
</tr>
<tr>
<td>4</td>
<td>$t^6 + t^4$</td>
</tr>
<tr>
<td>5</td>
<td>$t^5 + t^3$</td>
</tr>
<tr>
<td>6</td>
<td>$t^4 + t^2$</td>
</tr>
<tr>
<td>7</td>
<td>$t^3 + t$</td>
</tr>
<tr>
<td>8</td>
<td>$t^2 + 1$</td>
</tr>
</tbody>
</table>

There are also trajectories which seem very likely to diverge. The trajectory of $f = t^6 + t^2 + t + 1$ does not repeat a value within the first two billion iterations. Figure 2.6.1 in section 2.6.1 shows a plot of this trajectory, along with two others that seem to diverge. Matthews and Leigh [12] were able to exhibit a polynomial with a provably divergent trajectory when $m = t^2 + 1$, and it is easy to apply their construction to all $m$ of the form $t^n + 1$ for even $n \geq 2$. Experimental data confirms our expectation that a higher-degree polynomial $m$ causes a higher rate of apparently-divergent trajectories.

We want to understand the dynamics of $mx + 1$ for a given polynomial $m$. Since the Collatz conjecture analogue is likely false for $\deg m > 1$, we instead consider the following two questions:

1. Do divergent $mx + 1$ trajectories exist? If so, what is the density of divergent trajectories in the set of all trajectories?
2. Do cyclic trajectories exist? If so, how are cycle lengths distributed?

In order to investigate the first of these questions, we define the stopping time \( \sigma(f) \) to be the minimum number of steps before the trajectory of \( f \) reaches a polynomial of lower degree than \( f \). That is,

\[
\sigma(f) = \inf \{ k > 0 : \deg T^k(f) < \deg f \}.
\]

Note that if \( m \) is even (i.e. \( m(0) = 0 \)) then necessarily \( \sigma(f) = 1 \). If the trajectory of \( f \) never reaches a polynomial of lower degree, we set \( \sigma(f) = \infty \). Clearly if \( \sigma(f) < \infty \) for all \( f \), then the Collatz conjecture analogue must be true. On the other hand, if there exists any \( f \) with \( \sigma(f) = \infty \), then the trajectory of \( f \) cannot reach 1 and so the conjecture must be false.

### 2.3 Analogue of Terras’ theorem for \( \mathbb{F}_2[t] \)

Our goal is to prove an analogue of Theorem 2.1.1 for \( mx + 1 \) systems in \( \mathbb{F}_2[t] \). We use a method similar to Everett’s proof, but our theorem is stronger in that it gives precise predictions for the density of divergent trajectories.

**Theorem 2.3.1.** Let \( m \in \mathbb{F}_2[t] \) with \( \deg m = d \) and let \( P_m \) be the asymptotic probability that a randomly chosen polynomial in \( \mathbb{F}_2[t] \) has finite \( mx + 1 \) stopping time. That is,

\[
P_m = \lim_{N \to \infty} P \left( \sigma(f) < \infty \mid \deg f < N \right).
\]

If \( d \leq 2 \), then \( P_m = 1 \). If \( d > 2 \), then \( P_m \in (1/2, 1) \) is the unique real root of the polynomial \( g_d(z) = z^d - 2z + 1 \) inside the unit disk.
First, we define the **parity sequence** of $f$ to be $\{p_0, p_1, p_2, \ldots\}$, where $p_k = (T^k(f))(0)$. That is, $p_k$ is the constant term of $T^k(f)$, which indicates whether $tT^{k+1}(f) = mT^k(f) + 1$ or $tT^{k+1}(f) = T^k(f)$. To prove Theorem 2.3.1, we follow the outline used by Everett [5] to prove the corresponding result for the $3x + 1$ system in $\mathbb{Z}$. We prove that the parity sequence of a uniformly-chosen polynomial in $\mathbb{F}_2[t]$ is uniformly distributed in the set of sequences in $\{0, 1\}$. Then we prove that almost all such sequences correspond to polynomials with finite stopping time.

If we want to find the first $N$ terms of the parity sequence of a polynomial $f \in \mathbb{F}_2[t]$, we only need to consider the lowest $N$ coefficients of $f$. The higher coefficients will have no effect until later in the sequence. In fact, the parity sequences of all polynomials in the set $\{g + t^Nq : q \in \mathbb{F}_2[t]\}$ must have the same first $N$ terms. Therefore, there is a well-defined set function

$$\Phi_m : \mathbb{F}_2[t]/t^N \rightarrow \{0, 1\}^N$$

which maps each element of $\mathbb{F}_2[t]/t^N$ to the first $N$ terms of its $m$-parity sequence. We claim that this function is one-to-one.

**Lemma 2.3.2.** The map $\Phi_m$ described above is a set bijection. That is, every sequence $\{p_0, p_1, \ldots, p_{N-1}\}$ with $p_i \in \{0, 1\}$ is the first $N$ terms of the parity sequence of a unique polynomial $f \in \mathbb{F}_2[t]$ with $\deg f < N$. Specifically, the parity sequence determines the initial polynomial $f$ and its $N$-th iterate $T^N(f)$ as follows, up to choice of $q_N$:  

14
\[
f = g_{N-1} + t^N q_N, \quad \text{deg } g_{N-1} < N
\]
\[
T^N(f) = h_{N-1} + m^{s(N)} q_N, \quad \text{deg } h_{N-1} < ds(N)
\]

where \(d = \text{deg } m\) and \(s(N) = \sum_{i=0}^{N-1} p_i\). Therefore, parity sequences of polynomials in \(\mathbb{F}_2[t]\) of degree \(< N\) are distributed uniformly in \(\{0,1\}^N\).

Note that \(s(N)\) is just the number of 1’s which appear in the first \(N\) terms of the parity sequence of \(f\), which is the number of multiplications that occur in the first \(N\) steps of the trajectory of \(f\).

First, an informal explanation. Suppose we know the first term \(p_0\) of the parity sequence of \(f\). Using this, we can determine whether \(f\) is ‘odd’ or ‘even’. That is, we can find \(f\) modulo \(t\). If we also know \(p_1\), we can ‘lift’ our knowledge of \(f\), obtaining \(f\) modulo \(t^2\). We also learn the parity of \(f_1\). If we know \(p_2\), we gain one more degree of precision in \(f\) and \(T(f)\), and additionally we learn the parity of \(T^2(f)\). More generally, if we know \(f\) modulo \(t^{k+1}\) and we know \(p_k\), we can perform a sort of lift and find the value of \(f\) modulo \(t^{k+2}\), and we also learn a bit more about \(f_{k+1}\). In effect, there is an algorithm which constructs the unique polynomial of degree \(< N\) with a given parity sequence \(\{p_0,p_1,\ldots,p_{N-1}\}\). To prove the theorem, we just need to describe this algorithm and verify that it works.

\textit{Proof.} We proceed by induction on \(N = 1, 2, \ldots\). The base case is \(N = 1\). If \(p_0 = 0\), then \(f = tq_1\) and so \(T(f) = q_1\). If \(p_0 = 1\), then \(f = 1+tq_1\) and \(T(f) = (m+1)/t+mq_1\).

Now assume the theorem is true for all values up to \(N\). We argue that it is true for \(N+1\). There are four cases to consider, depending on the values of \(h_{N-1}(0)\) and \(p_N\) in \(\{0,1\}\).
**Case 1:** \( h_{N-1}(0) = 0, \ p_N = 0 \). That is, the \( N \)-th term of the trajectory is ‘even’ and \( q_N \) is also even. Let \( q_N = t q_{N+1} \). Then the next term is

\[
f_{N+1} = \frac{f_N}{t} = \frac{h_{N-1} + m^{s(N)} q_N}{t} = \frac{h_{N-1}}{t} + m^{s(N)} q_{N+1}
\]

We can rewrite the initial polynomial as

\[
f = g_{N-1} + t^{N+1} q_{N+1}.
\]

Since \( \deg h_{N-1}/t < s(N) \deg m \) and \( \deg g_{N-1} < N + 1 \), the theorem holds in this case.

**Case 2:** \( h_{N-1}(0) = 0, \ p_N = 1 \). That is, the \( N \)-th term of the trajectory is odd and \( q_N \) is also odd. Let \( q_N = 1 + t q_{N+1} \). Then the next term is

\[
f_{N+1} = m \frac{[h_{N-1} + m^{s(N)} q_N] + 1}{t} = m h_{N-1} + m^{s(N+1)} + 1 \quad + m^{s(N+1)} q_{N+1}
\]

Let \( h_N = \frac{m h_{N-1} + m^{s(N+1)} + 1}{t} \). Since \( \deg h_{N-1} < 2 s(N) \), we have \( \deg h_N < (\deg m) s(N + 1) \) as required. We rewrite the initial polynomial as

\[
f = g_{N-1} + t^N (t q_{N+1} + 1) = (g_{N-1} + t^N) + t^{N+1} q_{N+1}.
\]

Clearly \( \deg (g_{N-1} + t^N) < N + 1 \), so the theorem holds in this case.
**Case 3:** $h_{N-1}(0) = 1$, $p_N = 0$. That is, the $N$-th term of the trajectory is even and $q_N$ is odd. Let $q_N = 1 + t q_{N+1}$. Then the next term is

$$f_{N+1} = \frac{h_{N-1} + m s^{(N)} q_N}{t} = \frac{h_{N-1} + m s^{(N)}}{t} + m s^{(N+1)} q_{N+1}$$

Let $h_N = (h_{N-1} + m^X)/t$. Since $\deg h_{N-1} < 2s(N + 1)$, we have $\deg h_N < s(N + 1) \deg m$ as required. Next we rewrite the initial polynomial as

$$f = g_{N-1} + t^N q_N = g_{N-1} + t^N + t^{N+1} q_{N+1}.$$ 

And we know $g_{N-1} + t^N$, has degree less than $N + 1$, so the theorem holds in this case.

**Case 4:** $h_{N-1}(1) = 1$, $p_N = 1$. That is, the $N$-th term of the trajectory is odd and $q_N$ is even. Let $q_N = t q_{N+1}$. Then the next term is

$$f_{N+1} = \frac{m \left[ h_{N-1} + m s^{(N)} q_N \right] + 1}{t} = \frac{m h_{N-1} + 1}{t} + m s^{(N+1)} q_{N+1}.$$ 

Let $h_N = (m h_{N-1} + 1)/t$. This has degree $< 2s(N + 1)$ as required. Lastly, we rewrite the initial polynomial:
\[ f = g_{N-1} + t^N q_N \]
\[ = g_{N-1} + t^{N+1} q_{N+1}. \]

The theorem is satisfied because \( \deg g_{N-1} < N + 1 \).

This proves that knowing \( f \) modulo \( t^N \) together with the parity sequence term \( p_N \) is sufficient to uniquely identify \( f \) modulo \( t^{N+1} \). Therefore, every length-\( N \) parity sequence must arise from some polynomial in \( \mathbb{F}_2[t]/t^N \). There are \( 2^N \) polynomials of degree \( < N \), and there are \( 2^N \) binary sequences of length \( N \). So by cardinality, the surjective map \( \Phi_m : \mathbb{F}_2[t]/t^N \to \{0,1\}^N \) is a set bijection.

We have shown that the parity sequence of a randomly chosen polynomial \( f \in \mathbb{F}_2[t] \) of degree less than \( M \) is distributed uniformly in \( \{0,1\}^N \). Now we describe how the parity sequence of \( f \) determines the degree of \( T^N(f) \). If the parity sequence of \( f \) is \( \{p_k\} \), then

\[ \deg T^N(f) = \deg f - N + d \sum_{k=0}^{N-1} p_k. \]

Since \( \{p_k\}_{k=0}^{N-1} \) is uniformly distributed in \( \{0,1\}^N \), we can write

\[ \deg T^N(f) - \deg f \approx d \sum_{k=0}^{N-1} X_k - N \]

where \( X_k \) are IID uniform Bernoulli random variables. This leads immediately to the following theorem:
Theorem 2.3.3. The probability that a randomly chosen \( f \in \mathbb{F}_2[t] \) has finite \( mx + 1 \) stopping time is

\[
P(\sigma(f) < \infty) = P\left( \exists N > 0 : \sum_{k=0}^{N-1} X_k < \frac{1}{d}N \right)
\]  

(2.1)

where \( X_i \) are IID uniform Bernoulli random variables and \( d = \deg m \).

We will now show that this probability is the root of a certain simple polynomial which depends only on \( d = \deg m \), thus proving Theorem 2.3.1.

Lemma 2.3.4. For \( k = 0, \ldots, N - 1 \), let \( X_k \) be IID uniform Bernoulli variables and let \( P_d \) be defined

\[
P_d = P\left( \exists N > 0 : \sum_{k=0}^{N-1} X_k < \frac{1}{d}N \right).
\]

Then \( P_1 = P_2 = 1 \), and for \( d > 2 \), \( P_d \) is the unique real root of the polynomial \( g_d(z) = z^d - 2z + 1 \) lying inside the unit disk.

This is a version of the familiar ‘gambler’s ruin’ problem which has been studied extensively. Suppose you start with $0 and repeatedly play a simple game. Each time you play, you either gain $\((d - 1)\) or lose $1, each with probability 1/2. The question we seek to answer is this: what is the probability that you will ever have less than $0 at the conclusion of a game? If the gambler ever drops below $0, we say that he or she is ‘ruined’. For a thorough analysis of this problem, see Ethier [4].

Proof. First, note that if \( d = 1 \), each time the game is played, the gambler either loses $1 or stays even. The only way for the gambler to never drop below his or her
initial value is to never lose at all, so the probability of avoiding ruin through the first $N$ games is $2^{-N}$. Clearly in this case the probability of ruin is 1.

In order to handle degrees $d > 1$, we must start with a simplified version of the problem where the gambler is said to ‘win’ if he or she ever reaches a value of at least $W$. In this version, the sequence of games ends either when the gambler is ruined (by reaching a value below $0$) or wins (by holding a value of at least $W$). It is easy to see that the game must end eventually (with either a win or a loss) with probability 1. If the gambler plays enough games, he or she can expect to eventually see every finite subsequence of wins and losses, including $W$ wins in a row (which certainly wins the game, regardless of previous events) and $W$ losses in a row (which certainly loses). Therefore the probability of playing the game forever is zero; eventually the gambler will win or lose. We label $P_{d,W}$ the probability of ruin in a game with upper limit $W$. The probability of ruin in an open-ended game with no upper limit is then $P_d = \lim_{W \to \infty} P_{d,W}$.

For $k$ in $\mathbb{Z}$, let $U_k$ be the probability of ruin (before reaching $W$) starting from a value of $k$. The value we are trying to compute is $P_{d,W} = U_0$. Clearly $U_k = 1$ for all $k \leq -1$, and $U_k = 0$ for all $k \geq W$. For all other $k$, the values of $U_k$ satisfy a simple recurrence relation:

$$U_k = \frac{1}{2} U_{k-1} + \frac{1}{2} U_{k+d-1}.$$ 

The auxiliary polynomial is $g_d(z) = z^d - 2z + 1$. When $d > 2$, this polynomial is separable. But when $d = 2$, the polynomial has a root of multiplicity 2 at $z = 1$, so this must be handled differently.
First, consider the case $d = 2$. In this case, $U_k$ must have the form $U_k = c_1 + c_2 k$ for some constants $c_j$. We want to calculate $P_{2,W} = U_0 = c_1$, which we can do by solving a linear system of 2 equations:

$$\begin{bmatrix} 1 & -1 \\ 1 & W \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$  

We can easily invert the matrix and obtain $P_{2,W} = U_0 = c_1 = \frac{W}{W+1}$. Therefore, the probability of ruin in a game with no upper limit is $P_2 = \lim_{W \to \infty} U_0 = 1$.

We now move to the case $d > 2$, in which $g_d(z)$ has a root at $\lambda_1 = 1$ and $d - 1$ other distinct roots $\lambda_2, \lambda_3, \ldots, \lambda_d$. All solutions to the recurrence equation have the form $U_k = \sum_{j=1}^{d} c_j \lambda_j^k$ for some constants $c_j$. Using the known conditions $U_{-1} = 1$ and $U_W = U_{W+1} = \ldots = U_{W+d-1} = 0$, we can find the needed values of $c_j$ by solving the following linear system:

$$\begin{bmatrix} \lambda_1^{-1} & \lambda_2^{-1} & \lambda_3^{-1} & \ldots & \lambda_d^{-1} \\ \lambda_1^W & \lambda_2^W & \lambda_3^W & \ldots & \lambda_d^W \\ \lambda_1^{W+1} & \lambda_2^{W+1} & \lambda_3^{W+1} & \ldots & \lambda_d^{W+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{W+d-1} & \lambda_2^{W+d-1} & \lambda_3^{W+d-1} & \ldots & \lambda_d^{W+d-1} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$  

This system can be solved analytically using Cramer’s rule. Let $A$ be the $d \times d$ matrix above and let $b$ be the column vector on the right-hand side of the system. Using Cramer’s rule, we write
\[ U_0 = \sum_{i=1}^{d} c_i = \frac{\sum_{i=1}^{d} \det A_i}{\sum_{i=1}^{d} \lambda_i^{-1}A_{1,i}} \]  \hspace{1cm} (2.2) 

where \( A_i \) is the matrix formed by replacing the \( i \)-th column of \( A \) with \( b \), and \( A_{i,j} \) is the \( i, j \) cofactor of \( A \). Because \( b \) in this case is just the first standard basis vector, we have \( \det A_i = A_{1,i} \) for each \( 1 \leq i \leq d \). We compute \( A_{1,1} \) as an example; the others follow the exact same pattern.

\[
\det A_1 = \det \begin{bmatrix}
1 & \lambda_2^{-1} & \lambda_3^{-1} & \cdots & \lambda_d^{-1} \\
0 & \lambda_2^W & \lambda_3^W & \cdots & \lambda_d^W \\
0 & \lambda_2^{W+1} & \lambda_3^{W+1} & \cdots & \lambda_d^{W+1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \lambda_2^{W+d-1} & \lambda_3^{W+d-1} & \cdots & \lambda_d^{W+d-1}
\end{bmatrix}
\]

\[
= \det \begin{bmatrix}
\lambda_2^W & \lambda_3^W & \cdots & \lambda_d^W \\
\lambda_2^{W+1} & \lambda_3^{W+1} & \cdots & \lambda_d^{W+1} \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_2^{W+d-1} & \lambda_3^{W+d-1} & \cdots & \lambda_d^{W+d-1}
\end{bmatrix}
\]

\[
= \prod_{j=2}^{d} \lambda_j^W \det \begin{bmatrix}
1 & 1 & \cdots & 1 \\
\lambda_2 & \lambda_3 & \cdots & \lambda_d \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_2^{d-1} & \lambda_3^{d-1} & \cdots & \lambda_d^{d-1}
\end{bmatrix}
\]

The matrix in the last row above is a Vandermonde matrix with parameters \( \lambda_2, \lambda_3, \ldots, \lambda_d \), so its determinant is \( \prod_{2 \leq j < k \leq d} (\lambda_k - \lambda_j) \). More generally, for any
\[ 1 \leq i \leq d, \text{ let } B_i \text{ be the determinant of the } (d - 1) \times (d - 1) \text{ Vandermonde matrix with parameters } \lambda_1, \ldots, \lambda_{i-1}, \lambda_{i+1}, \ldots, \lambda_d. \text{ Then} \]

\[
B_i = \prod_{1 \leq j < k \leq d, j, k \neq i} (\lambda_k - \lambda_j)
\]

And since \( \prod_{j=1}^{d} \lambda_j = 1 \), we can write

\[
\det A_i = (-1)^{1+i} \prod_{1 \leq j \leq d, j \neq i} \lambda_j^{W} B_i
\]

\[
= (-1)^{1+i} \lambda_i^{-W} B_i.
\]

At last we can rewrite equation 2.2 as follows:

\[
U_0 = \frac{\sum_{j=1}^{d} (-1)^{1+j} B_j \lambda_j^{-W}}{\sum_{j=1}^{d} (-1)^{1+j} B_j \lambda_j^{-1-W}}.
\]

The true probability of ruin \( P_d \) is the limit of this quantity as \( W \) approaches infinity. The dominant term in both the numerator and denominator is the root \( \lambda_i \) with the smallest magnitude among the roots of \( g_d(z) = z^d - 2z + 1 \), assuming there exists a real root inside the unit circle. In fact, it is easy to show that \( g_d(z) \) must have exactly one root inside the unit circle, and that this root is real and lies in the interval \((1/2, 1)\). Using Descartes’ rule of signs, we determine that there are two positive real roots of \( g_d(z) \), one of which is \( z = 1 \). Since \( g_d'(1) = d - 2 > 0 \), we know that \( g_d(1-\epsilon) < 0 \) for small positive epsilon. On the other hand, \( g_d(1/2) = (1/2)^d > 0 \), so the other real root must lie in the interval \((1/2, 1)\).
Figure 2.2. Using Rouche’s theorem to prove that $g_d(z)$ has a unique real root in the unit disk.

Next, we use Rouche’s theorem to prove that there is only one root within the unit circle. Let $f(z) = z^d$ and let $h(z) = -2z + 1$. For small positive $\epsilon$, consider the circle $C_\epsilon = \{z \in \mathbb{C} : |z| = 1 - \epsilon\}$. The function $f$ maps $C_\epsilon$ to a smaller circle $|z| = (1 - \epsilon)^d$. Define $m_f(\epsilon) = (1 - \epsilon)^d$. Then $|f(z)| = m_f(\epsilon)$ for all $z \in C_\epsilon$. The other function $h$ maps $C_\epsilon$ to a circle of radius $2(1 - \epsilon)$ centered at $z = 1$. The point on this circle closest to the origin is the point $z = -1 + 2\epsilon$, with magnitude $|-1 + 2\epsilon| = 1 - 2\epsilon$. Define $m_h(\epsilon) = 1 - 2\epsilon$. Then for all $z \in C_\epsilon$, $|h(z)| \geq m_h(\epsilon)$. See Figure 2.2.

We claim that for small positive $\epsilon$, $m_h(\epsilon) > m_f(\epsilon)$ and therefore that $|h(z)| > |f(z)|$ for all $z \in C_\epsilon$. Notice that $m_h(0) = m_f(0) = 1$. Calculating the derivatives of the two functions, we see that $m_h'(0) = -2$ and $m_f'(0) = -d$. By continuity, since $m_h'(0) > m_f'(0)$, $m_h(\epsilon)$ must be greater than $m_f(\epsilon)$ for small positive values of epsilon. Since $|h(z)| > |f(z)|$ for all $z \in C_\epsilon$, $g_d(z) = h(z) + f(z)$ must have the
same number of roots within $C_{\epsilon}$ as $h(z)$. The function $h(z) = 1 - 2z$ has one root at $z = 1/2$. Therefore, for small positive $\epsilon$, $g_d(z)$ has a unique root inside the circle $|z| = 1 - \epsilon$, which must be the previously mentioned real root lying in the interval $(1/2, 1)$. The value of this root is the probability of ruin $P_d$.

We have now completed the proof of Theorem 2.3.1. Figure 2.3 shows the values of $P_d$ for $d$ up to 8, accurate to 4 decimal places. Lastly, we prove two simple corollaries following Theorem 2.3.1.

**Theorem 2.3.5.** If $\deg m \leq 2$, then with the probability that a randomly chosen polynomial will have a divergent $mx + 1$ trajectory is zero.

**Proof.** Let $N = 2^{1+\deg f}$. This is the number of elements of $\mathbb{F}_2[t]$ of degree $\leq \deg f$. Let $S_0 = \{ f \}$. With probability 1, there is some $k_1 > 0$ such that $\deg T^{k_1}(f) \leq \deg f$. Without loss of generality, let $k_1$ be the lowest index which satisfies this condition. If $T^{k_1}(f) \in S_0$, then we have returned to a previously visited polynomial and therefore we have found a cycle; otherwise, let $S_1 = S_0 \cup \{ T^{k_1}(f) \}$.

Now with probability 1 there is some minimal $k_2 > k_1$ such that $\deg T^{k_2}(f) \leq \deg T^{k_1}(f) \leq \deg f$. If $T^{k_2}(f) \in S_1$, then we have found a cycle. If not, let $S_2 = S_1 \cup \{ T^{k-2}(f) \}$.

<table>
<thead>
<tr>
<th>$d$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_d$</td>
<td>1</td>
<td>1</td>
<td>0.6180</td>
<td>0.5437</td>
<td>0.5188</td>
<td>0.5087</td>
<td>0.5041</td>
<td>0.5020</td>
</tr>
</tbody>
</table>
When we iterate the process described above \( N \) times, either we find a cycle, or \( S_N \) contains every polynomial of degree \( \leq \deg f \) (by cardinality). Now with probability 1 there exists \( k_{N+1} \) such that \( \deg T^{k_{N+1}}(f) \leq \deg f \). This polynomial must have already been visited by the sequence, so this trajectory is a cycle. 

**Theorem 2.3.6.** For any positive integer \( N \), we can find a polynomial \( f \in F_2[t] \) such that \( \deg T^k(f) \geq \deg f \) for all \( 0 < k \leq N \). That is, for any value of \( N \), we can find a polynomial whose stopping time is at least \( N \).

**Proof.** Simply create the vector \([1, 1, \ldots, 1]\) \( \in \{0, 1\}^N \) and use the bijection \( \Phi : F_2[t]/t^N \to \{0, 1\}^N \) to find the polynomial \( f \) of degree \( < N \) with this parity sequence. The sequence is made entirely of ones, so

\[
\deg T^N(f) = \deg f + N(-1 + \deg m).
\]

2.4 The \( mx+1 \) problem in the ring of functions on an algebraic curve

In the previous section we investigated \( mx+1 \) systems in \( F_2[t] \). As we pointed out in the introduction, \( F_2[t] \) is the ring of regular functions of the affine line over \( F_2 \), so it is natural to try to define \( mx+1 \) systems on rings of functions of other algebraic curves over \( F_2 \). We denote by \( R_r \) the ring \( F_2[x, t]/(x^2 + tx + r(t)) \), where \( r(t) \in F_2[t] \) is some irreducible polynomial. This is the ring of regular functions on the hyperelliptic curve \( x^2 + tx + r(t) = 0 \).
Any element \( f \in R_r \) has a unique representation of the form \( f(x, t) = f_0(t) + xf_1(t) \) for some \( f_0, f_1 \in \mathbb{F}_2[t] \). Our goal is to define a transformation map \( T : R_r \to R_r \) analogous to the 3x + 1 map in \( \mathbb{Z} \). We choose a polynomial \( m \in R_r \) and define

\[
T(f) = \begin{cases} 
\frac{mf + x + 1}{t}, & f \equiv 1 + x \mod t \\
\frac{f + x}{t}, & f \equiv x \mod t \\
\frac{f + 1}{t}, & f \equiv 1 \mod t \\
\frac{f}{t}, & f \equiv 0 \mod t.
\end{cases}
\]

Let \( m(x, t) = m_0(t) + xm_1(t) \). Because the ideal \( x^2 + tx + r(t) \) is zero, we have

\[
mf + 1 + x = [m_0f_0 + m_1f_1r + 1] + x[m_0f_1 + m_1f_0 + tf_1m_1 + 1].
\]

In order to make sure that \( mf + 1 + x \) is always divisible by \( t \) when \( f \equiv 1 + x \mod t \), we require that \( m \equiv x \mod t \).

Repeated iteration of \( T \) defines a discrete dynamical system in \( R_r \). The trajectory of a given polynomial \( f \) is the sequence \( T^k(f) \), \( k = 0, 1, 2, \ldots \). Each trajectory must either diverge or fall into a cycle (which may be the trivial cycle, \( \{0\} \)). There are two parameters that will influence the behavior of the trajectories: the polynomial \( r \in \mathbb{F}_2[t] \) which determines the algebraic curve, and the polynomial \( m \in R_r \) used to define the map \( T \) on \( R_r \). The more interesting of these is \( m \), so we will fix \( r(t) = t^2 + t + 1 \) and study how the dynamics are affected by \( m \). As with the \( mx + 1 \) systems in \( \mathbb{F}_2[t] \), we expect that the probability of finding a divergent trajectory will grow with the degree of \( m \).
We define the stopping time $\sigma(f)$ to be the minimum number of steps required before the trajectory of $f$ reaches a polynomial of lower degree than $f$. Note that by the ‘degree’ of $f \in R_r$ we always mean the total $t$-degree of $f$, i.e. $\deg f = \max \{\deg f_0, \deg f_1\}$ when $f$ is written as $f_0(t) + x f_1(t)$. Finally, we define the parity sequence of $f$ to be the sequence $p_0, p_1, p_2, \ldots$ where $p_k = (T^k(f))(x, 0)$. That is, $p_k \in \{0, 1, x, 1 + x\}$ is the congruence class of $T^k(f)$ modulo $t$. We will later use the fact that when $T^k(f) \not\equiv 1 + x \mod t$, $T^{k+1}(f) = (T^k(f) + p_k)/t$.

2.5 Analogue of Terras’ theorem for $R_r$

Our ultimate goal is to prove the following analogue of Terras’ theorem in this setting.

**Theorem 2.5.1.** For $m \in R_r$ of degree $d$, let $P_d$ be the probability that a randomly chosen polynomial in $R_r$ has finite $mx + 1$ stopping time. That is,

$$P_d = \lim_{N \to \infty} P(\sigma(f) < \infty | \deg f < N).$$

If $d \leq 4$, then $P_d = 1$. If $d > 4$, then $P_d \in (3/4, 1)$ is the unique real root of the polynomial $g_d(z) = z^d - 4z + 3$ that lies inside the unit disk.

Note that like Theorem 2.3.1, this is stronger than the analogous result for the integer $3x + 1$ system because it provides numerical values for the probability of divergence. Just as in Section 2, our first step is to prove that the parity sequence of a randomly chosen polynomial is distributed uniformly. The parity sequences
of all polynomials in the set \( \{ g + t^Nq : q \in R_r \} \) must have the same first \( N \) terms. Therefore, there is a well-defined function

\[
\Phi_m : R_r / t^N \longrightarrow \{0, 1, x, 1 + x\}^N
\]

which maps each element of \( R_r / t^N \) to the first \( N \) terms of its parity sequence.

However, we require a special lemma before we can prove that this map is a bijection. Our proof of the analogous result in \( \mathbb{F}_2[t] \) relied on the fact that \( \deg fg = \deg f + \deg g \) for all \( f, g \in \mathbb{F}_2[t] \). In \( R_r \), we can no longer depend on this assumption, but we can prove a weaker version of this rule by accepting an additional restriction on \( m \).

**Lemma 2.5.2.** Let \( m = m_0 + xm_1 \) and \( f = f_0 + xf_1 \) be elements of \( R_r \). If \( \deg m_1 - \deg m_0 < -1 \), then \( \deg mf = \deg m + \deg f \).

For the rest of this paper, when we consider an \( mx + 1 \) system in \( R_r \), we always assume \( m \) satisfies this condition.

**Proof.** Note that since \( \deg m_1 < \deg m_0 \), we always have \( \deg m = \deg m_0 \). Label \( g = mf = g_0 + xg_1 \). To prove this lemma, we just need to carefully examine the summands of \( g_0 \) and \( g_1 \) to determine which has the greatest degree and therefore determines the degree of the sum.

Let \( \mu = \deg m_1 - \deg m_0 \) and let \( \delta = \deg f_1 - \deg f_0 \). We must consider three cases:

**Case 1:** \( \delta \leq \mu \). Since \( \delta \leq \mu < -1 \), we know that \( \deg f_0 > \deg f_1 \), and so the total degree of \( f \) is \( \deg f = \deg f_0 \).
We know that $g_0 = m_0 f_0 + r m_1 f_1$. Since $\deg m_0 > \deg m_1 + 1$ and $\deg f_0 > \deg f_1 + 1$, we see that $\deg m_0 f_0 > \deg m_1 f_1 r$. Therefore $m_0 f_0$ is the dominant term, and so the degree of $g_0$ is $\deg g_0 = \deg m_0 + \deg f_0$.

Now $g_1 = m_0 f_1 + m_1 f_0 + t m_1 f_1$. In this case the dominant term is $m_1 f_0$, so $\deg g_1 = \deg m_1 + \deg f_0$. Since $\deg m_0 > \deg m_1$, we have $\deg g_0 > \deg g_1$ and therefore the total degree of $g$ is $\deg g = \deg m_0 + \deg f_0$.

Putting all of this together, we see that $\deg g = \deg m_0 + \deg f_0 = \deg m + \deg f$.

**Case 2:** $\mu < \delta < -2 - \mu$. Recall that $g_0 = m_0 f_0 + r m_1 f_1$. Using the fact that $\delta < -2 - \mu$, we can see that

$$\deg f_1 - \deg f_0 < -2 - \deg m_1 + \deg m_0$$

and therefore

$$\deg f_1 + \deg m_1 + 2 < \deg f_0 + \deg m_0.$$ 

So the dominant term in $g_0$ is $f_0 m_0$, and so $\deg g_0 = \deg f_0 + \deg m_0$.

Next, consider $g_1 = m_0 f_1 + m_1 f_0 + t m_1 f_1$. Since $\delta > \mu$, we have

$$\deg f_1 + \deg m_0 > \deg f_0 + \deg m_1$$

so the term $f_1 m_0$ dominates the term $f_0 m_1$. Furthermore, since $\mu < -1$, we have $\deg m_0 > \deg m_1 + 1$, so $f_1 m_0$ also dominates $f_1 m_1 t$. Therefore $\deg g_1 = \deg f_1 + \deg m_0$. 

30
In this case, we don’t know whether $\delta$ is positive, negative, or zero. So we can’t be sure about which component of $f$ is dominant. However, we have proved that $\deg g_0 = \deg f_0 + \deg m_0$ and that $\deg g_1 = \deg f_1 + \deg m_0$. So either way, $\deg g = \deg f + \deg m$.

**Case 3: $\delta \geq -2 - \mu$.** In this case, $\delta \geq 0$ because $\mu < -1$, so necessarily $\deg f = \deg f_1$. Now consider the degree of $g$. The term $f_1 m_0$ in $g_1$ is not dominated by either term of $g_0$. Since $\delta \geq 0$, we know that $\deg f_1 \geq \deg f_0$ and therefore the degree of $f_1 m_0$ is not less than the degree of $f_0 m_0$. Also, since $\mu < -1$, we know that $\deg m_0 \geq \deg m_1 + 2$, and so the degree of $f_1 m_0$ is not less than the degree of $f_1 m_1 q$. Therefore $\deg g = \deg g_1$. Now we need only find out which term of $g_1$ is dominant.

Because $\mu < -1$, we have $\deg m_0 > \deg m_1 + 1$, so the term $f_1 m_0$ dominates $f_1 m_1 t$. Lastly, since $\mu < 0$ and $\delta \geq 0$, the term $f_1 m_0$ dominates $f_0 m_1$. Therefore, $f_1 m_0$ is the dominant term in $g_1$. In conclusion,

\[
\deg g = \deg g_1 \\
= \deg f_1 + \deg m_0 \\
= \deg f + \deg m
\]

Having proven the desired result in all three cases, we have completed the proof of this lemma.

Now we are equipped to prove that $\Phi_m$ is a bijection.
Theorem 2.5.3. The map $\Phi_m$ described above is a set bijection. That is, every sequence $\{p_0, p_1, \ldots, p_{N-1}\}$ with $p_i \in \{0, 1, x, 1+x\}$ is the first $N$ terms of the parity sequence of a unique polynomial $f \in R_r$ with $\deg f < N$. Specifically, the parity sequence determines the initial polynomial $f$ and its $N$-th iterate $f_N$ up to choice of $q_N$:

$$f = g_{N-1} + t^N q_N, \quad \deg g_{N-1} < N$$

$$f_N = h_{N-1} + m^{s(N)} q_N, \quad \deg h_{N-1} < s(N) \deg m$$

where $s(N)$ is defined

$$s(N) = \# \{0 \leq k < N : p_k = 1 + x\}.$$ 

Note that $s(N)$ is just the number of $1 + x$ terms which appear in the first $N$ terms, which is the number of multiplications that occur in the first $N$ steps of the sequence starting from $f$.

As in $\mathbb{F}_2[t]$, the proof takes the form of an algorithm that yields the unique polynomial in $R_r$ of degree $< N$ with a given parity sequence $\{p_0, p_1, \ldots, p_{N-1}\}$. In proving this theorem, we will often be working modulo $t$, and we will frequently use the fact that $m \equiv x \mod t$. Also, we can rewrite the quotient ring $R_r/(t) = \mathbb{F}_2[x,t]/(x^2 + tx + r, t)$ as simply $\mathbb{F}_2[x,t]/(x^2 + 1, t)$.

Proof. We prove the theorem by induction on $N = 1, 2, \ldots$. First consider $N = 1$. There are four cases:

1. If $p_0 = 0$, then $f = tq_1$ and $T(f) = q_1$, so $g_0 = 0$. 

32
2. If \( p_0 = 1 \), then \( f = 1 + tq_1 \) and \( T(f) = q_1 \), so \( g_0 = 1 \).

3. If \( p_0 = x \), then \( f = x + tq_1 \) and \( T(f) = q_1 \), so \( g_0 = x \).

4. If \( p_0 = 1 + x \), then \( f = 1 + x + tq_1 \) and \( T(f) = (m(1 + x) + 1 + x)/t + mq_1 \), so \( g_0 = 1 + x \).

Each of the above cases gives us a unique \( g_0 \) from among the elements of \( R_r \) of degree < 1, as needed. Next, we assume the theorem holds for some \( N \geq 1 \) and argue that it holds for \( N + 1 \). Let \( q_N = tq_{N+1} + v \), meaning \( v \) is the element of \( \{0, 1, x, 1 + x\} \) equivalent to \( q_N \) modulo \( t \). Here there are just two cases.

**Case 1:** \( v = 0 \) or \( v = 1 + x \). In this case, \( m^{s(N)}q_N \equiv x^pv \equiv v \mod t \), so \( T^N(f) \equiv h_{N-1} + v \mod t \). If \( h_{N-1} + v \not\equiv 1 + x \mod t \), then

\[
T^{N+1}(f) = \frac{h_{N-1} + m^{s(N)}q_N + p_N}{t} = \frac{h_{N-1} + m^{s(N)}v + p_N}{t} + m^{s(N+1)}q_{N+1}.
\]

We now define \( h_N = (h_{N-1} + m^{s(N)}v + p_N)/t \). Referring to Lemma 2.5.2, we determine that \( \deg h_N < s(N) \deg m \), as required.

If instead \( h_{N-1} + v \equiv 1 + x \mod t \), then

\[
T^{N+1}(f) = \frac{m(h_{N-1} + m^{s(N)}q_N) + 1 + x}{t} = \frac{mh_{N-1} + m^{s(N+1)}v + 1 + x}{t} + m^{s(N+1)}q_{N+1}.
\]

Once again we see that the degree of \( h_N = (mh_{N-1} + m^{s(N+1)}v + 1 + x)/t \) satisfies the condition of the theorem.
Case 2: \( v = 1 \) or \( v = x \). In this case,

\[
m^s(N)q_N \equiv x^s(N)v \equiv \begin{cases} 
  v, & \text{if } s(N) \text{ even} \\
  xv, & \text{if } s(N) \text{ odd}
\end{cases} \mod t.
\]

So in order to make \( T^N(f) = h_{N-1} + m^s(N)q_N \) be equivalent to \( 1 + x \mod t \), one of the following must be true:

- \( s(N) \) even, \( h_{N-1} + v \equiv 1 + x \mod t \)
- \( s(N) \) odd, \( h_{N-1} + xv \equiv 1 + x \mod t \).

If so, then

\[
T^{N+1}(f) = \frac{mT^N(f) + 1 + x}{t} = \frac{mh_{N-1} + m^s(N+1)v + 1 + x}{t} + m^s(N+1)q_{N+1}
\]

and we define \( h_N = (mh_{N-1} + m^s(N+1)v + 1 + x)/t \), which has degree \(< s(N + 1) \deg m \). If neither of those two possibilities occurs, then

\[
T^{N+1}(f) = \frac{h_{N-1} + m^s(N)(v + tq_N) + p_N}{t} = \frac{h_{N-1} + m^s(N+1)v + p_N}{t} + m^s(N+1)q_N.
\]

So \( h_N = (h_{N-1} + m^s(N)v + p_N)/t \) satisfies \( \deg h_N < s(N + 1) \deg m \) as required.

We have established that a vector \( \vec{p} = (p_0, p_1, \ldots, p_{N-1}) \in \{0, 1, x, t + x\}^N \) determines a unique polynomial \( g_{N-1} \in R_r \) of degree \(< N \) such that \( \vec{p} \) is the first \( N \) terms
of the parity sequence of \( f \), and that all polynomials in \( R_r \) that satisfy this are of the form \( g_{N-1} + t^N q_N \) for some \( q_N \). There are \( 4^N \) polynomials of degree \( < N \) and there are \( 4^N \) elements of \( \{0, 1, x, 1 + x\}^N \). So by cardinality, the surjective map \( \Phi \) is a bijection.

We have now shown that the parity sequence of a randomly chosen \( f \in R_r \) of degree \( < N \) is distributed uniformly in \( \{0, 1, x, 1 + x\}^N \). Following the same outline as the \( \mathbb{F}_2[t] \) proof, we can then model the degree of \( T^k(f) \) as a random walk:

\[
\deg T^k(f) = \deg f - N + (\deg m) \sum_{k=0}^{N-1} X_k
\]

where \( X_k \) are IID Bernoulli random variables. The difference is that this time, \( X_k \) takes the value 1 with probability \( 1/4 \) and 0 otherwise. So the probability that a randomly chosen \( f \in R_r \) has finite stopping time is equal to

\[
P \left( \exists N > 0 : \sum_{k=0}^{N-1} X_k < \frac{N}{d} \right)
\]

where \( d = \deg m \). This is just another version of the gambler’s ruin problem, so we can prove the following result using the same methods as in \( \mathbb{F}_2[t] \).

**Lemma 2.5.4.** For \( d > 0 \), let \( P_d \) be defined

\[
P_d = P \left( \exists N > 0 : \sum_{k=0}^{N-1} X_k < \frac{N}{d} \right)
\]
where \( X_i \) are IID Bernoulli variables taking the value 1 with probability 1/4 and 0 otherwise. If \( d \leq 4 \), then \( P_d = 1 \). If \( d > 4 \), then \( P_d \) is the unique root of \( g_d(z) = z^d - 4z + 3 \) inside the unit disk, which is real and lies in the interval \((3/4, 1)\).

This time, the gambler repeatedly plays a game which pays out \( d - 1 \) dollars with probability 1/4, and \(-1\) dollars with probability 3/4. The stopping time corresponds to the number of games before the gambler goes broke. The proof is essentially the same as that of the analogous result in \( \mathbb{F}_2[t] \). In this case the linear recurrence relation is

\[
U_k = \frac{3}{4}U_{k-1} + \frac{1}{4}U_{k+d-1}
\]

and our goal is to find the value of \( U_0 \), representing the probability of ruin (depending on \( W \)) starting from a value of 0. As in Section 2.3, we solve the system using Cramer’s rule and then take the limit of this quantity as \( W \to \infty \) to find the probability of ruin in a game with no upper limit.\(^1\) Figure 2.4 shows the probability of finite stopping time for \( m \) of degree up to 8, accurate to 4 decimal places.

**Figure 2.4.** Finite stopping time probability \( P_d \) in \( R_r \)

<table>
<thead>
<tr>
<th>( d )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P_d )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0.8882</td>
<td>0.8343</td>
<td>0.8046</td>
<td>0.7867</td>
</tr>
</tbody>
</table>

Once again, we prove some corollaries of this result.

\(^1\)Full details of this proof are given in Appendix ??.
Theorem 2.5.5. Let $d \leq 4$ and let $m \in R_r$ of degree $d$. Then a randomly chosen polynomial $f \in R_r$ has finite $mx + 1$ stopping time with probability 1.

We use exactly the same proof as in Theorem 2.3.5, with the minor difference that $N = 4^{1+\deg f}$ instead of $2^{1+\deg f}$.

Theorem 2.5.6. For any positive integer $N$, we can find a polynomial $f \in R_r$ such that $\sigma(f) > N$.

Proof. Simply create the vector $[1 + x, 1 + x, \ldots, 1 + x] \in \{0, 1, x, 1 + x\}^N$ and use the bijection $\Phi_m : R_r/t^N \to \{0, 1 x, 1 + x\}^N$ to find the polynomial $f$ of degree $< N$ with this parity sequence. The sequence is made entirely of ones, so

$$\deg T^N(f) = \deg f + N(-1 + \deg m)$$

(once again we rely on Lemma 2.5.2).

2.6 Experimental Data

Our C++ implementation of the $mx + 1$ system in $\mathbb{F}_2[t]$ uses integer arrays to represent elements of $\mathbb{F}_2[t]$, with each coefficient stored as a single bit. With polynomials represented this way, arithmetic in $\mathbb{F}_2[t]$ can be programmed entirely using fast bitwise logical operations. Source code for this project can be found at github.com/nichols/polynomial-mxplus1.

2.6.1 $\mathbb{F}_2[t]$ 

For multiple values of $m \in \mathbb{F}_2[t]$, we computed the trajectory $\{T^k(f)\}$ of each polynomial $f \in \mathbb{F}_2[t]$ of degree $< 20$. Each trajectory was computed for $10^5$ steps,
or until a cycle was detected (using Brent’s cycle-finding algorithm [2]). For those polynomials with stopping time \( \sigma(f) \leq 10^5 \), we recorded the value of \( \sigma(f) \); for the rest, we recorded \( \sigma(f) > 10^5 \). We conjecture that many if not most of these polynomials have \( \sigma(f) = \infty \).

The running time of a single iteration of the \( mx + 1 \) map \( T(f) \) is linear in the degree of \( f \). Most trajectories tend to either converge quickly to a cycle or else increase linearly in degree indefinitely. For polynomials of the latter type, the running time of computing the first \( N \) terms of a trajectory is quadratic in \( N \). Accordingly, the small set of apparently divergent trajectories occupied most of the running time of our computations. Figure 2.5 shows three different apparently divergent trajectories for \( m = t^2 + t + 1 \). Notice that all in all three trajectories, the degree appears to increase linearly with slope \( 2/5 \). Every long acyclic trajectory we observed fits this pattern.

With regard to stopping times, our data supports the theoretical predictions on Theorem 2.3.1 for all the \( m \) we tested of degree not equal to 2. For quadratic \( m \), we found a significant number of polynomials with stopping times greater than \( 10^5 \). This does not contradict the theorem’s predictions that almost all \( f \in \mathbb{F}_2[t] \) should have finite \( mx + 1 \) stopping time for \( \deg m \leq 2 \). But it does suggest that the density may converge to zero very slowly.

On the subject of cycle lengths, all the cycles we observed had periods divisible by four, and nearly all were powers of 2. We observed some interesting patterns in the distribution of periods.
**Figure 2.5.** Degree plot of three disjoint trajectories which appear to diverge

![Degree Plot](image)

\[ \text{Divergent trajectories, } m = t^2 + t + 1 \]

\[ f = t^6 + t^5 + t^4 + 1 \]

\[ f = t^8 + t^5 + t^3 + 1 \]

\[ f = t^8 + t^6 + t^4 + t^2 + 1 \]

---

### 2.6.1.1 Stopping times

Figure 2.6 shows the number of polynomials with \( \sigma(f) > 10^5 \) for each choice of \( m \in F_2[t] \). Notice that for \( \deg m \neq 2 \), we find almost exactly the number of infinite stopping times predicted by Theorem 2.3.1. When \( \deg m = 2 \), the theorem predicts that the asymptotic density of infinite stopping time trajectories should be zero, but we found a significant number of polynomials which have stopping times \( \sigma(f) > 10^5 \).

There are two possible explanations for this phenomenon.

1. The probability of choosing a polynomial \( f \) of degree \( < N \) with \( \sigma(f) = \infty \) converges to zero very slowly as \( N \to \infty \). That is, there may be many low-degree polynomials with infinite stopping time, but the frequency decreases to zero as the degree increases.
Figure 2.6. Frequency of long stopping times ($\sigma(f) > 10^5$) for various $m \in \mathbb{F}_2[t]$

2. There are a significant number of polynomials which have very high finite stopping times – in this case, with $\sigma(f) > 10^5$. That is, the distribution of finite stopping times could have a “long tail”.

To put it another way, Theorem 2.3.1 states that when $\deg m \leq 2$,

$$P_d = \lim_{N \to \infty} \left[ \lim_{M \to \infty} P(\sigma(f) > M \mid \deg f < D) \right] = 0.$$

We found that for both quadratic $m$, this quantity is not close to zero when $M = 10^5$ and $D = 20$, so we would need to increase at least one of these two variables to see evidence of convergence to zero. Figure 2.7 shows the distribution of known stopping times in polynomials of degree $< 20$ for $m = t^2 + 1$ and $m = t^2 + t + 1$, with $m = t + 1$ and $m = t^3 + 1$ presented for comparison. For $m \neq 2$, most trajectories either quickly descend below their initial degree, or apparently diverge. But for quadratic $m$, we see a broader distribution of stopping times. This is yet another reason why the
most interesting $mx + 1$ systems in $F_2[t]$ are those generated by quadratic $m$, and in particular $m = t^2 + t + 1$.

**Figure 2.7.** Distribution of stopping times among polynomials of degree $< 20$ for four values of $m$.

<table>
<thead>
<tr>
<th>$\sigma(f)$</th>
<th>$t + 1$</th>
<th>$t^2 + 1$</th>
<th>$t^2 + t + 1$</th>
<th>$t^3 + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – 50</td>
<td>1048573</td>
<td>900255</td>
<td>930844</td>
<td>642494</td>
</tr>
<tr>
<td>50 – 100</td>
<td>0</td>
<td>413</td>
<td>12315</td>
<td>0</td>
</tr>
<tr>
<td>100 – 150</td>
<td>0</td>
<td>0</td>
<td>724</td>
<td>0</td>
</tr>
<tr>
<td>150 – 200</td>
<td>0</td>
<td>1</td>
<td>90</td>
<td>0</td>
</tr>
<tr>
<td>200 – 250</td>
<td>0</td>
<td>0</td>
<td>36</td>
<td>0</td>
</tr>
<tr>
<td>250 – 300</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>300 – 350</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>350 – 400</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>400 – 450</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$&gt; 10^5$</td>
<td>2</td>
<td>147906</td>
<td>104549</td>
<td>406081</td>
</tr>
</tbody>
</table>

2.6.2 $R_r$

For each polynomial $f = f_0(t) + xf_1(t) \in R_r$ with $\deg f < 10$, we computed the trajectory of $f$ up to $10^5$ iterations of the $mx + 1$ function. We carried out this process for several choices of $m = m_0 + xm_1$ with $m_0, m_1 \in F_2[t]$. Figure 2.8 shows the density of polynomials with long stopping times for each $m$. Much like the $F_2[t]$ case, the data generally agrees with our predictions, though we do see a higher than expected occurrence of high stopping times when the degree of $m$ is a particular value. In $R_r$, the most interesting $m$ polynomials seem to be those of degree 4.
Figure 2.8. Density of long stopping times \( (\sigma(f) > 10^5) \) for various \( m \in R_r \).

<table>
<thead>
<tr>
<th>( m )</th>
<th>( t^2 + t + 1 )</th>
<th>( t^2 + 1 )</th>
<th>( t + 1 )</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>( t^2 + t + 1 )</td>
<td>0.04 0.04 0.04 0.04 0.04 0.04 0.04</td>
<td>0.04 0.04 0.04 0.04 0.04 0.04 0.04</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.03 0.01 0.01 0.10 0.11 0.07 0.08 0.05 0.04 0.05 0.04 0.14</td>
</tr>
<tr>
<td>( t^2 + 1 )</td>
<td>0.04 0.04 0.04 0.04 0.04 0.04 0.04</td>
<td>0.04 0.04 0.04 0.04 0.04 0.04 0.04</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.03 0.01 0.01 0.10 0.11 0.07 0.08 0.05 0.04 0.05 0.04 0.14</td>
</tr>
<tr>
<td>( t + 1 )</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.03 0.01 0.01 0.10 0.11 0.07 0.08 0.05 0.04 0.05 0.04 0.14</td>
</tr>
<tr>
<td>1</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.01 0.01 0.01 0.07 0.07 0.07</td>
<td>0.00 0.03 0.01 0.01 0.10 0.11 0.07 0.08 0.05 0.04 0.05 0.04 0.14</td>
</tr>
</tbody>
</table>

2.7 Future work

The occurrence of infinite \( mx + 1 \) stopping times in \( \mathbb{F}_2[t] \) and \( R_r \) is described by Theorems 2.3.1 and 2.5.1. However, it would be interesting to investigate further the distribution of finite stopping times – especially in the case \( m = t^2 + t + 1 \) in \( \mathbb{F}_2[t] \), where we expect to see lots of very large finite stopping times.

We also have some data on the distribution of periods in \( \mathbb{F}_2[t] \) which does not yet have a theoretical explanation. For \( m = t^2 + t + 1 \), nearly all observed periods were powers of 2. And for each integer \( k \), the frequency of \( k \)-cycles up to degree \( d \) seems to increase gradually and then diminish as \( d \) increases, as shown in Figure 2.9. Perhaps this pattern can be explained analytically.

The integer \( 3x + 1 \) problem has been approached using many different tools and methods, including preimage trees [1]. It might be useful to apply this method to function field \( mx + 1 \) systems and try to prove some of the same results.
Figure 2.9. Frequency of cycles with $\lambda = 2^k$ in set of polynomials up to degree $d$

We may also be able to define $mx + 1$ systems in yet more rings and compare their stochastic behavior to that of $mx + 1$ systems in $\mathbb{Z}$ and in function fields. Any ring with a maximal ideal with $\mathbb{F}_2$ as its residue field lends itself easily to such a construction. But even rings without this property (like $R_r$) may admit generalized $mx + 1$ systems with similar statistical properties.
CHAPTER 3
ORDERS OF VANISHING OF \(L\)-FUNCTIONS AT THE POINT \(s = 1/2\)

3.1 \(L\)-functions

The Riemann zeta function is the complex function defined by the series

\[
\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.
\]

This function was first studied by Euler in the mid-18th century. However, Euler’s work predated the rise of complex analysis, so he considered it only as a real function. In 1859 Bernhard Riemann described the basic properties of the complex zeta function as we know it today, including its meromorphic continuation and the functional equation \(\zeta(s) = 2^s \pi^{s-1} \sin \left( \frac{\pi s}{2} \right) \Gamma(1 - s) \zeta(1 - s)\). He also began to investigate the deep connections between the locations of the zeros of \(\zeta(s)\) and the distribution of prime numbers in \(\mathbb{Z}\). A few decades later, Hadamard and de Vallée Poussin both independently used the zeta function to prove a major theorem on the distribution of prime numbers [8].
Theorem 3.1.1 (Prime number theorem). Let \( \pi(x) = \# \{ p \in \mathbb{Z} \mid p \leq x \} \) be the prime counting function. As \( x \) approaches infinity, this function grows at the same rate as \( x / \log(x) \). That is,

\[
\lim_{x \to \infty} \frac{\pi(x)}{x / \log(x)} = 1.
\]

This can be proven by computing a complex contour integral of a function related to \( \zeta(s) \). But in order to compute this integral, it is necessary to have some understanding of where the zeros of \( \zeta(s) \) are located.

Today we recognize Riemann’s zeta function as the archetype of a class of so-called \( L \)-functions, which are complex meromorphic functions encoding information about arithmetic objects. For an object \( X \) such as a number field, representation, or algebraic variety, we can define the \( L \)-function \( L(X,s) \) as a Dirichlet series on some half-plane. The exact details of the definition are dependent on the specific type of object under consideration, but there should always be a meromorphic continuation of \( L(X,s) \), and it should satisfy a functional equation similar to the one described above. \( L \)-functions are expected to have “interesting” values at the integers, meaning that for \( n \in \mathbb{Z} \), the value \( L(X,n) \) should be related to some arithmetic property of \( X \). The locations and orders of the zeroes of an \( L \)-function generally also have arithmetic significance.

The point \( s = 1/2 \) is particularly important because an \( L \)-function may be forced to vanish here by its functional equation. For instance, if the functional equation takes the form \( L(X,s) = -L(X,1-s) \), then this function is anti-symmetric on the real line about the point \( s = 1/2 \), and so it must have a zero at that point.
denote by $\rho_X$ the order of vanishing of the $L$-function $L(X, s)$ at the point $s = 1/2$. That is,

$$\rho_X = \text{ord}_{s=1/2} L(X, s) = \inf \left\{ n \in \mathbb{Z} \left| \lim_{s \rightarrow 1/2} \frac{L(X, s)}{(s - 1/2)^n} \neq 0 \right. \right\}.$$ 

It is generally believed [17] that an $L$-function should vanish to the lowest degree compatible with its functional equation unless there is some arithmetic reason for it to vanish to a higher order. If we find a family of objects whose $L$-functions frequently have an unusually high order of vanishing here, then this should reflect something notable or unusual about these objects. Constructing families of arithmetic objects with this property therefore seems like a worthwhile goal.

In the remainder of this section, we will focus on the zeta function of a function field extension, which is one type of $L$-function. We will see that this is closely related to the Artin $L$-function of a Galois representation and to the local zeta function of an algebraic curve over a finite field.

### 3.2 The zeta function of a function field

Let $\mathbb{F}_q$ be the finite field of $q = p^n$ elements where $p$ is an odd prime. An algebraic function field over $\mathbb{F}_q$ is a finite separable extension $K/\mathbb{F}_q(t)$. Function fields of this type are similar to number fields. In fact, we can define the zeta function of an algebraic function field in a manner very similar to the Dedekind zeta function of a number field, using an Euler product. The zeta function of a function field $K$ is defined to be
$$Z(K/\mathbb{F}_q(t), s) = \prod_p \left(1 - \frac{1}{N(p)^s}\right)$$

where $p$ runs over the prime ideals of the maximal order $\mathcal{O}_K$ (analogous to the ring of integers of a number field) and $N(p) = |\mathcal{O}_K/p|$ is the ideal norm. This zeta function can also be expressed as a Dirichlet series in terms of the divisors of $K$.

If $K/\mathbb{F}_q(t)$ is Galois with $G = \text{Gal}(K/\mathbb{F}_q(t))$, then for any complex representation $\chi$ of $G$ we can construct the Artin $L$-function $L(\chi, s)$. The function field zeta function $Z(K/\mathbb{F}_q, s)$ is then the product of the Artin $L$-functions of the irreducible representations of $G$. We will also see that a function field $K/\mathbb{F}_q(t)$ can be viewed as the field of functions of some algebraic curve $C$ over $\mathbb{F}_q$. This gives us an alternative formulation of the zeta function of $K$ which is often easier to work with.

### 3.3 Algebraic curves over a finite field

We now state some standard definitions and results about algebraic curves, following Silverman [18] and using mostly the same notation. Let $F$ be a perfect field (meaning that every irreducible polynomial in $F[x]$ is separable) and let $\bar{F}$ be an algebraic closure of $F$. We denote by $\mathbb{A}^n = \mathbb{A}^n(\bar{F})$ the $n$-dimensional affine space over $F$, meaning the vector space $\bar{F}^n$ but ignoring the special role played by the zero vector. We denote by $\mathbb{A}^n(F)$ the set of $F$-rational points of $\mathbb{A}^n$.

An affine algebraic curve is a set of the form $C = C_f = \{(x, y) \in \mathbb{A}^2 \mid f(x, y) = 0\}$ for some fixed irreducible polynomial $f \in F[x, y]$. We say $C$ is defined over $F$ if $f \in F[x, y]$. In this case, the set of $F$-rational points of $C$ is $C(F) = C \cap \mathbb{A}^2(F)$. The affine coordinate ring of $C$ is the ring $F[C] = F[x, y]/(f)$. The field of fractions of $F[C]$ is called the field of functions of $C$, written $F(C)$. This is an algebraic
extension of $F(x)$, i.e. an algebraic function field. If $F(C)$ is isomorphic to an algebraic function field $K$, then we say $C$ is a curve model for $K$. Two curves with isomorphic function fields are said to be isomorphic.

We denote by $\mathbb{P}^n = \mathbb{P}^n(\bar{F})$ the projective space of dimension $n$ over $F$, which is defined as the set of lines through the origin in $\mathbb{A}^{n+1}(F)$. Equivalently we can write $\mathbb{P}^n(F) = \mathbb{A}^{n+1}(F)/F^\times$, i.e. $(n+1)$-dimensional affine space modulo nonzero scalar multiplication. The set of $F$-rational points in this space is $\mathbb{P}^n(F) = \mathbb{A}^n(F)/F^\times \subset \mathbb{P}^n(\bar{F})$.

A projective algebraic curve is a set of the form $C = \{(x, y, z) \in \mathbb{P}^2 \mid f(x, y, z) = 0\}$ for some fixed irreducible homogeneous polynomial $f \in \bar{F}[x, y, z]$. We say $C$ is defined over $F$ if $f \in F[x, y, z]$. In this case, the set of $F$-rational points of $C$ is $C(F) = C \cap \mathbb{P}^2(F)$. A singularity is a point $P$ on the curve such that the three partial derivatives all vanish, or

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0.$$ 

If a curve has no singularities, it is said to be nonsingular or smooth.

For any non-homogeneous degree-$d$ polynomial $f(x, y)$, we can construct a homogeneous polynomial $g(x, y, z) = z^d f(x/z, y/z)$ such that $f(x, y) = g(x, y, 1)$. The affine curve $C_f$ is then just the intersection of the projective curve $C_g$ with the plane $z = 1$. We call $C_g$ the projective closure of $C_f$, and both are curve models for the same function field. In the rest of this section, we will often consider a curve given by a non-homogeneous polynomial, but we will keep in mind that most of the important properties of the curve are determined by its projective closure.
For a projective algebraic curve $C/F$, the divisor group $\text{Div}(C)$ is defined to be the free abelian group generated by the points of $C$, meaning

$$\text{Div}(C) = \left\{ \sum_{P \in C} a_P P \mid a_P \in \mathbb{Z} \forall P \right\}.$$  

If $C$ has infinitely many points, then we require that $a_P = 0$ for all but finitely many $P$. The degree of this divisor is defined to be the integer $\deg(D) = \sum_{P \in C} a_P$. The subgroup of degree-0 divisors is written $\text{Div}^0(C)$.

For any function $f \in F(C)$, we define the divisor of $f$ to be $D_f = \sum_{P \in C} \text{ord}_P(f) P$. Divisors of this form are called principal divisors and they form a subgroup of $\text{Div}^0(C)$ which we will label $\text{Prin}(C)$. The quotient group $\text{Div}(C)/\text{Prin}(C)$ is the divisor class group or Picard group $\text{Pic}(C)$. The quotient group $\text{Div}^0(C)/\text{Prin}(C)$ is called the degree zero Picard group. We will discuss the Picard group further in section 3.5.1.1 in the process of counting the points on a certain curve.

For any divisor $D = \sum_{P \in C} a_P P$, if all of the coefficients $a_P$ are non-negative, then we call $D$ an effective divisor and write $D \geq 0$. We define the set $L(D) = \{ f \in F(C)^\times \mid D_f + D \geq 0 \}$. This is a finite-dimensional $F$-vector space and we label its dimension $l(D)$. We can now state the Riemann-Roch theorem and define the genus of $C$, an important invariant.

**Theorem 3.3.1 (Riemann-Roch).** Let $C$ be an algebraic curve over a field $F$. There is an integer $g \geq 0$ and a divisor class $E \in \text{Pic}(C)$ such that for any $E \in \mathcal{E}$ and any $A \in \text{Div}(C)$ we have

$$l(A) = \deg(A) - g + 1 + l(E - A).$$
We call $g$ the **genus** of $C$ and we call $\mathcal{E}$ the **canonical class**. When $F$ is the field of complex numbers and $C$ is a Riemann surface, the genus is the number of “handles” of $C$. The Riemann sphere has genus 0, a simple torus has genus 1, and so on. We define the genus of a function field $K$ to be the genus of any curve model for $K$.

From now on we will work with finite fields $F = \mathbb{F}_q$ where $q = p^m$ for some nonnegative integer $m$. In this setting each algebraic curve $C$ will have a finite number of points $\#C(\mathbb{F}_q)$.

### 3.3.1 The zeta function of an algebraic curve

If $C$ is a nonsingular projective curve over $\mathbb{F}_q$, we define the zeta function of $C$ to be

$$Z(C/\mathbb{F}_q, s) = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n}(q^{-s})^n\right).$$

This zeta function is a rational function in $T = q^{-s}$ of the form

$$Z(C/\mathbb{F}_q, T) = \frac{P(T)}{(1 - T)(1 - qT)}$$

where $P(T)$ is a polynomial with $\deg P(T) = 2g$. Furthermore, $P(T)$ has the form

$$P(T) = \prod_{i=1}^{g}(1 - \alpha_i T)(1 - \bar{\alpha}_i T)$$

where the $\alpha_i$ are complex numbers with $|\alpha_i| = \sqrt{q}$. For any $n \geq 1$, the number of $\mathbb{F}_{q^n}$-rational points on $C$ is $\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{g}(\alpha^n + \bar{\alpha}^n)$. For a more detailed explanation of these results, see [7] section 10.7. As mentioned earlier,
$Z(C/F_q, s)$ is the same as the zeta function of the function field $F_q(C)$, and it is also equal to the product of the Artin $L$-functions of the irreducible representations of $\text{Gal}(F_q(C)/F_q(t))$, assuming the extension is Galois.

The logarithmic derivative of $Z(C/F_q, s)$ is the generating function for the sequence \{\#C(F_q^n)\}_{n=1}^\infty$. However, the zeta function is also related to many other properties of $C$. For example, the value $Z(F_q(C)/F_q(t), 1)$ appears in the class number formula for $F_q(C)$. Ramachandran [16] has shown that when $C$ is defined over $F_q^2$, the order $\text{ord}_{s=1/2} Z(C/F_q^2, s)$ determines the ranks of the étale cohomology groups $H^i(C, E)$ where $E/F_q$ is a certain supersingular elliptic curve.

The zeta function of an algebraic curve satisfies a functional equation of the form $Z(C, s) = W(C)s^{1/2}L(C, 1-s)$, where the root number $W(C)$ is a complex number with magnitude 1. If the root number is -1, then the zeta function is forced to vanish at the point $s = 1/2$, meaning that $\rho_C = \text{ord}_{s=1/2} Z(C, s) \geq 1$. On the other hand, if the root number is 1, then we expect that $\rho_C = 0$ because the functional equation does not require $Z(C, s)$ to vanish at this point. We would like to restrict our search to algebraic curves whose zeta functions have root number $\pm 1$. For all such curves we expect $\rho_C \leq 1$, so we are looking for an anomalous family where $\rho_C \geq 2$.

### 3.4 The search for fields with root number $\pm 1$

Let $L/K$ be a field extension with Galois group $G \cong Q_8$ and let $\theta$ be the unique degree 2 irreducible complex representation of $G$. As described by Frohlich ([6], chapter I), the Artin $L$-function of $\theta$ must have real root number $W(\theta) = \pm 1$. All of the other irreducible representations are degree 1, so they have trivial root number.
and do not affect the root number of $Z(L/K, s)$. Because of this fact, we can be sure that the root number of this function field is $W(L/K) = \pm 1$. Therefore one simple way to construct large numbers of fields with known root number $W = \pm 1$ is to generate fields with Galois group $Q_8$. We will describe a systematic construction of quaternionic function fields over $\mathbb{F}_q$, following Omar [14] who carried out a similar project for number fields. To construct and classify function fields which have quaternion Galois group, we make use of Witt’s criterion.

3.4.1 Witt’s criterion

Let $K$ be a field and let $a, b \in K$ be distinct nonzero squarefree elements. We call extensions of the form $K_{a,b} = K(\sqrt{a}, \sqrt{b})$ biquadratic. Extensions of this form have $\text{Gal}(K_{a,b}/K) = V_4$. Note that for any three coprime squarefree elements $a, b, c$, the biquadratic extensions $K(\sqrt{ac}, \sqrt{bc})$, $K(\sqrt{ab}, \sqrt{ac})$, $K(\sqrt{ab}, \sqrt{bc})$ are identical. Furthermore, if $K$ is the field of fractions of a ring $R$, then there is no loss of generality if we assume that $a, b, c$ are all elements of $R$. Therefore, the set of biquadratic extensions of $K$ is parameterized by the set of coprime triples of squarefree elements of $R$. We write $K_{a,b,c}$ for the biquadratic field associated with the triple $(a, b, c)$. Basic Galois theory tells us that every $Q_8$-extension must contain a unique biquadratic subextension which appears as the fixed field of the unique subgroup of order 2. Therefore we begin our search for quaternion extensions by examining biquadratic fields.

A ternary quadratic form over a field $K$ is a homogeneous polynomial of degree 2 in 3 variables. The most obvious example is the square of the Euclidean
norm in $\mathbb{R}^3$, or $Q(x, y, z) = x^2 + y^2 + z^2$. Every ternary quadratic form can be written as

$$Q(x, y, z) = \vec{x}^T A \vec{x}$$

where $\vec{x}$ is the column vector with entries $x, y, z$ and $A$ is a fixed $3 \times 3$ symmetric matrix. We say two quadratic forms $U$ and $V$ are equivalent over $K$ if there is an invertible linear transformation $T \in GL_3(K)$ such that $U(\vec{x}) = V(T \vec{x})$. Alternatively, the forms $U$ and $V$ are equivalent if they are defined by $3 \times 3$ matrices $A$ and $B$ respectively and there exists a matrix $P$ such that $B = P^T A P$.

As described by Jensen, Ledet, and Yui ([10], section 6.1), **Witt’s criterion** states that a biquadratic extension $K(\sqrt{a}, \sqrt{b})$ extends to a $Q_8$ extension if and only if the quadratic form $Q_{a, b}(X, Y) = aX^2 + bY^2 + abZ^2$ is $K$-equivalent to $X^2 + Y^2 + Z^2$. Furthermore, all $Q_8$ extensions lying above this biquadratic field must be of the form

$$K\left(\sqrt{r \left(1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{ab}\right)}\right)$$

where $r \in K^*$ and $P = (p_{ij})$ is a $3 \times 3$ matrix such that

$$P = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{bmatrix}, \quad P^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$  

This criterion reduces the problem of finding quaternion extensions to a simpler question about equivalence of ternary quadratic forms.
3.4.2 Global fields and the Hasse Principle

When $K$ is a global field such as $\mathbb{F}_p(t)$, we can use the Hasse-Minkowski theorem to quickly determine whether or not two quadratic forms are equivalent. This allows us to determine whether a given biquadratic field $K_{a,b}/K$ extends to a quaternion field. Since every quaternion field must contain a biquadratic subfield, every $Q_8$ extension can be constructed this way.

A **valuation** on a field $F$ is a map $v : F \to \mathbb{R} \cup \{\infty\}$ satisfying three properties:

1. $v(a) = \infty$ if and only if $a = 0$
2. $v(ab) = v(a) + v(b)$
3. $v(a + b) \geq \min\{v(a), v(b)\}$ with equality if $v(a) \neq v(b)$

The equivalence classes of valuations on a field $F$ are called the **places** of $F$. The field $\mathbb{F}_p(t)$ has exactly two types of places: a single infinite place represented by the valuation $v_\infty : f/g \mapsto \deg g - \deg f$, and a set of finite places corresponding to the prime ideals of $\mathbb{F}_p[t]$. For a prime ideal $p$ generated by an irreducible polynomial $r$, the place at $p$ is represented by the valuation $v_p : f \mapsto k$ where $k$ is the unique integer such that we can write $f = r^k g$ where $r \nmid g$. At each place $p$ we can form the **completion** $\mathbb{F}_p(t)_p = \lim_{\leftarrow m} \mathbb{F}_p[t]/(r)^m$, a local field with unique maximal ideal $p$.

We can now state the Hasse-Minkowski theorem. A thorough explanation is provided in ([15], chapter VI).

**Theorem 3.4.1** (Hasse-Minkowski). *Let $K$ be a global field. Two ternary quadratic forms on $Q_1(X,Y,Z)$ and $Q_2(X,Y,Z)$ are $K$-equivalent if and only if they are locally*
equivalent at each place \( p \) of \( K \), meaning that for every \( p \) their Hasse symbols \( S_pQ_1 \) and \( S_pQ_2 \) are identical.

The Hasse symbol of a ternary quadratic form \( Q \) is defined

\[
S_pQ = \prod_{1 \leq i \leq j \leq 3} \left( \frac{a_i a_j}{p} \right),
\]

where \( Q \) is written in diagonal form as \( Q(X, Y, Z) = a_1X^2 + a_2Y^2 + a_3Z^2 \), and \( \left( \frac{u,v}{p} \right) \) is the Hilbert symbol in \( K_p \), which is defined

\[
\left( \frac{u,v}{p} \right) = \begin{cases} 
1, & uX^2 + vY^2 - Z^2 = 0 \text{ has a nonzero solution in } K_p^3 \\
-1, & \text{otherwise.}
\end{cases}
\]

There is an easy formula for computing the Hilbert symbol. Let \( u, v \in K_p \) and let \( \pi \) be a uniformizer for \( p \), meaning a generator for the maximal ideal of \( K_p \). Write \( u = \pi^l \mu \) and \( v = \pi^m \nu \) with \( l, m \geq 0 \) and \( \mu, \nu \notin p \), and let \( \bar{\mu} \) and \( \bar{\nu} \) be the projections of \( \mu, \nu \) into the residue field \( \mathcal{O}_K/p \). Then

\[
\left( \frac{u,v}{p} \right) = (-1)^{lm(N-1)/2} \chi_p(\bar{\mu})^m \chi_p(\bar{\nu})^l
\]

where \( \chi \) is the quadratic character on the residue field and \( N \) is the size of the residue field. This formula leads immediately to a very useful property: if \( u, v \notin p \), then \( l = m = 0 \), and so \( \left( \frac{u,v}{p} \right) = 1 \). We make use of this fact to prove the following helpful lemma.
Lemma 3.4.2. The quadratic extension \( \mathbb{F}_q(t)(\sqrt{a}, \sqrt{b}) \) extends to a quaternion extension if and only if \( S_p Q_{a,b} = 1 \) for all primes \( p \) of \( \mathbb{F}_q(t) \) which contain either \( a \) or \( b \).

It is clear that for the base form \( T = X^2 + Y^2 + Z^2 \), the Hasse symbol is \( S_p T = 1 \) at every place \( p \). Therefore, \( K(\sqrt{a}, \sqrt{b}) \) satisfies Witt’s criterion if and only if \( S_p Q_{a,b} = S_p T = 1 \) for all \( p \). We can then show that \( S_p Q_{a,b} \) must be equal to 1 for all primes except for the finite set of primes which contain \( a \) or \( b \). Suppose we want to calculate \( S_p Q_{a,b} \). We write

\[
S_p Q_{a,b} = \left( \frac{a,a}{p} \right) \left( \frac{a,b}{p} \right) \left( \frac{a,ab}{p} \right) \left( \frac{b,b}{p} \right) \left( \frac{b,ab}{p} \right) \left( \frac{ab,ab}{p} \right) = \left( \frac{a,a}{p} \right) \left( \frac{b,b}{p} \right) \left( \frac{a,b}{p} \right).
\]

There are three cases depending on whether \( p \) contains either \( a \) or \( b \), both, or neither.

- If neither \( a \) nor \( b \) is contained in \( p \), then all of these Hilbert symbols are 1, and therefore the Hasse symbol is \( S_p Q_{a,b} = 1 \). Therefore, at any place which contains neither \( a \) nor \( b \), \( Q_{a,b} \) and \( T \) are locally equivalent forms.

- If \( a \in p \) but \( b \notin p \), then we have \( S_p Q_{a,b} = (-1)^{\frac{\deg p - 1}{2}} \chi_p(\bar{\beta}) \).

- If both \( a \) and \( b \) are contained in \( p \), then we have \( S_p Q_{a,b} = (-1)^{\frac{\deg p - 1}{2}} \chi_p(\bar{\alpha}) \chi_p(\bar{\beta}) \).

This is sufficient to prove the lemma. Accordingly, our algorithm to determine whether or not \( K = \mathbb{F}_q(t)(\sqrt{a}, \sqrt{b}) \) extends to a \( Q_8 \)-extension proceeds as follows:

1. Determine the primes \( p \) of \( \mathbb{F}_q(t) \) which divide at least one of \( a, b \).
2. For each of these, compute the Hasse symbol $S_p Q_{a,b}$ using the Hilbert symbol formula.

3. $K$ satisfies Witt’s criterion if and only if every one of these Hasse symbols is 1.

Using this method we can quickly check any pair $a, b \in \mathbb{F}_q[t]$ to determine whether there is a quaternion extension of $\mathbb{F}_q(t)$ containing $\mathbb{F}_q(t)(\sqrt{a}, \sqrt{b})$ as a subextension. Above each distinct biquadratic field which satisfies Witt’s criterion there is a parameterized family of quaternion extensions. A list of select low-genus quaternion extensions of $\mathbb{F}_p(t)$ for small $p$ is given in Appendix B, including many with $\rho_X$ greater than the order required by $W(X)$. Magma code for this computation is included in Appendix C.

### 3.5 A family of $\mathbb{F}_p(t)$ extensions with anomalous order of vanishing

We now exhibit a family of quaternion function fields whose zeta functions vanish at $s = 1/2$ to a higher order than expected, proving the following theorem:

**Theorem 3.5.1.** Let $p \equiv 5 \pmod{8}$, let $w \in (\mathbb{F}_p)^\times$, and let $K = \mathbb{F}_p(t)$. Let $a = t + w^2$ and let $b = t$. Then the biquadratic extension $K_{a,b,1} = K\left(\sqrt{a}, \sqrt{b}\right)$ extends to a genus 2 quaternion extension $L = K(\alpha)$, where

$$\alpha^2 = 1 + \frac{ab^2 + w^2}{2ab^2} \sqrt{b} + \frac{ab^2 - w^2}{2wb^2} \sqrt{a}\sqrt{b}.$$
Furthermore, the zeta function of $L/K$ is

$$Z(L/K, s) = \frac{(1 - p^{1-2s})^2}{(1 - p^{-s})(1 - p^{1-s})}$$

which vanishes to order 2 at $s = 1/2$, while the root number must be $\pm 1$.

The pair $(a, b) = (t + w^2, t)$ is necessarily a Witt pair in $\mathbb{F}_p$ when $p \equiv 1 \mod 4$. Since $a$ and $b$ are linear, the only primes where we need to check the Hasse symbol are $(a)$ and $(b)$. We find that the Hasse symbols at these primes are

$$S_{(a)} Q_{a,b} = \begin{pmatrix} a, a \\ (a) \end{pmatrix} \begin{pmatrix} a, b \\ (a) \end{pmatrix} = (-1)^{\frac{\deg(a) - 1}{2}} (-1)^{\frac{\deg(a) - 1}{2}} \chi(a)(\overline{\beta}) = \chi(a)(b).$$

$$S_{(b)} Q_{a,b} = \begin{pmatrix} a, b \\ (b) \end{pmatrix} \begin{pmatrix} b, b \\ (b) \end{pmatrix} = (-1)^{\frac{\deg(b) - 1}{2}} (-1)^{\frac{\deg(b) - 1}{2}} \chi(b)(\overline{\alpha}) = \chi(b)(a).$$

Since $p \equiv 1 \mod 4$, these two symbols are equal because of quadratic reciprocity. So in order for $(a, b)$ to be a Witt pair, we only need $b$ to be a square modulo $a$. Clearly this is the case for $(a, b) = (t + w^2, t)$.

We now need a transformation matrix $P \in GL_3(\mathbb{F}_p)$ such that $PAP^T = I_3$ where $A$ is the matrix of the form $Q_{a,b}$. One valid choice for $a, b$ of this form is
\[ P = \frac{1}{2wab^2} \begin{bmatrix} 0 & 2i w^2 ab & 2w ab \\ b(ab^2 - w^2) & a(ab^2 + w^2) & -iw(ab^2 + w^2) \\ -b(ab^2 + w^2) & ia(ab^2 - w^2) & w(ab^2 - w^2) \end{bmatrix} \] (3.1)

where \( i^2 = -1 \). Using this matrix and choosing \( r = 1 \), we see that the field

\[ L = \mathbb{F}_p(t) \left( \sqrt{1 + \frac{ab^2 + w^2}{2wb^2} \sqrt{b} + \frac{ab^2 - w^2}{2ab^2} \sqrt{ab}} \right) \] (3.2)

must have Galois group \( Q_8 \) over \( \mathbb{F}_p(t) \).

Our goal is now to compute the zeta function of this family of fields, which we can do by counting the \( \mathbb{F}_p^n \)-rational points on a curve model up to sufficiently large \( n \). But in order to know an upper limit on \( n \) for this calculation, we first need to prove the following theorem.

**Lemma 3.5.2.** Let \( p \equiv 5 \mod 8 \) and let \( K_{a,b,1} \) and \( L \) be as defined in Theorem 3.5.1. Then the genus of \( L/K \) is 2.

To prove that the genus of \( L \) is 2, we first show that the biquadratic subfield \( K \left( \sqrt{a}, \sqrt{b} \right) \) has genus zero. The defining polynomial of this biquadratic field over \( K = \mathbb{F}_p(t) \) is \( x^4 - (4t + 2w^2)x^2 + w^4 \). We can easily solve for \( t \) in terms of \( x \) and obtain \( t = (x^4 - 2w^2x^2 + w^4)/(4x^2) \), meaning that in fact \( K \) is isomorphic to \( \mathbb{F}_p(x) \), or that the projective line \( \mathbb{P}^1(\mathbb{F}_p) \) is a curve model for this field. Therefore the genus of \( K \left( \sqrt{a}, \sqrt{b} \right) \) is zero.
Now we want to define $L$ as a relative extension of $K \left( \sqrt{a}, \sqrt{b} \right) = \mathbb{F}_p(x)$. The quantity inside the square root given in equation 3.2 above can be written as

$$1 + \frac{ab^2 + w^2}{2wb^2} \sqrt{b} + \frac{ab^2 - w^2}{2ab^2} - \sqrt{ab} = \frac{(x^6 + 2wx^5 + w^2x^4 + 8wx^3 - w^4x^2 - 2w^5x - w^6)^2}{16wx^3(x - w)(x + w)^3(x^2 + w^2)}.$$ 

Since this quantity is used to define a quadratic extension, we can multiply by a square to eliminate the denominator and cancel out square factors. This allows us to write the quaternion extension as

$$L = \mathbb{F}_p(x) \left( \sqrt{wx(x + w)(x - w)(x^2 + w^2)} \right) = \mathbb{F}_p(x) \left( \sqrt{wx(x^4 - w^4)} \right).$$

An obvious curve model for this field is the hyperelliptic curve $y^2 = wx(x^4 - w^4)$. If we then apply the change of variables $X = x/w$, $Y = y/w^3$, we can rewrite this curve as $Y^2 = X(X^4 - 1)$, eliminating the dependence on $w$ entirely. Since the right-hand side is a quintic function of $x$, the genus of this curve must be 2.

### 3.5.1 The zeta function of $L/K$

We now want to compute the zeta function of $L/\mathbb{F}_p(t)$ (given $p \equiv 5 \pmod{8}$), which we can do by counting the points over $\mathbb{F}_p$ and $\mathbb{F}_p^2$ of a curve model for $L$. We will use the model $Y^2 = X(X^4 - 1)$ from the previous section, which we will label $C$. For any field $k$, let $\varphi : C[k] \to k$ be the map defined by $(X, Y) \mapsto X(X^4 - 1)$. Let $N_0 = \# \varphi^{-1}(0)$ and let $N_s = \# \{ X \in F_p^\times | X(X^4 - 1) \in (\mathbb{F}_p^\times)^2 \}$. Then $\#C[\mathbb{F}_p] = N_0 + 2N_s$. Note that for any $p \geq 5$ we have $N_0 = 5$. 

60
Now suppose \( p \equiv 5 \mod 8 \). We can write \( p = 4n + 1 \) where \( n \) is an odd positive integer. The group of units \((\mathbb{F}_p)^\times\) is cyclic of order \( 4n \), so there must be an element of order 4 which we will call \( i \). However, there is no element of order 8 because \( n \) is odd. Therefore \( i \) is not a square in \( \mathbb{F}_p^\times \). Let \( h(X) = X(X^4 - 1) = X(X + 1)(X - 1)(X + i)(X - i) \). Then clearly

\[
h(iX) = iX(iX + 1)(iX - 1)(iX + i)(iX - i) \\
= iXi(X - i)(iX + i)(X + 1)i(X - 1) \\
= i^\delta X(X - i)(X + i)(X + 1)(X - 1) \\
= ih(X).
\]

Since \( i \) is not a square, for \( X \neq 0 \) exactly one of \( \{ h(X), h(iX) \} \) is contained in \((\mathbb{F}_p^\times)^2 \). Therefore \( N_s = \frac{1}{2}(p - 5) \), and the total number of affine points is \( p \). Including the point at infinity, there are \( \#C(\mathbb{F}_p) = p + 1 \) points in the projective closure.

3.5.1.1 Computing \( \#C(\mathbb{F}_{p^2}) \)

We cannot use the above method to count the \( \mathbb{F}_{p^2} \)-rational points because in \( \mathbb{F}_{p^2} \) an element of order 8 does exist, which means there is some \( \delta \in \mathbb{F}_{p^2} \) such that \( \delta^2 = i \). However, we can still compute \( C(\mathbb{F}_{p^2}) \) in a different way.

**Lemma 3.5.3.** Let \( C/\mathbb{F}_p \) be the curve defined by \( Y^2 = X(X^4 - 1) \) with \( p \equiv 5 \mod 8 \). Then \( \#C(\mathbb{F}_{p^2}) = p^2 + 1 - 4p \).
Proof. In $\mathbb{F}_p^2$, we can use the change of variables $(X, Y) \mapsto \left( \frac{X+1}{\delta(X-1)}, \frac{Y}{\delta^3(X-1)} \right)$ to transform $C$ into a new curve

$$C_2 : \delta Y^2 = X^6 - 5X^4 + 5X^2 - 1$$

defined over $\mathbb{F}_p^2$. This curve is $\mathbb{F}_p^4$-equivalent to the curve

$$C_3 : Y^2 = X^6 - 5X^4 + 5X^2 - 1$$

defined over $\mathbb{F}_p$. Note that we must ascend to $\mathbb{F}_p^4$ to make $C_2$ and $C_3$ equivalent because $\delta$ does not have a square root in $\mathbb{F}_p^2$. The curves $C$ and $C_3$ are both defined over $\mathbb{F}_p$ and are equivalent in a quadratic extension of $\mathbb{F}_p^2$ but not in $\mathbb{F}_p^2$ itself. Therefore in $\mathbb{F}_p^2$ they differ only by a quadratic twist, and so $\#C(\mathbb{F}_p^2) + \#C_3(\mathbb{F}_p^2) = 2p^2 + 2$. This useful fact allows us to compute $\#C(\mathbb{F}_p^2)$ by dealing with the much easier curve $C_3$.

The Weil conjectures (see [18] chapter V) tell us that the number of points on a variety $X/\mathbb{F}_{p^k}$ is equal to the number of fixed points of $\text{Frob}_{p^k}$ acting on the set $X(\bar{\mathbb{F}}_p)$, which we can express in terms of the Frobenius traces on the cohomology groups $H^i(X)$. In the case of $C_3$ we write

$$\#C_3(\mathbb{F}_p^2) = \# \left[ C_3(\bar{\mathbb{F}}_p)^{\text{Frob}_{p^2}} \right]$$

$$= \sum_{i=0}^{2} (-1)^i \text{Tr} \left( \text{Frob}_{p^2} \mid H^i(C_3) \right)$$

$$= 1 - \text{Tr}(\text{Frob}_{p^2} \mid H^1(C_3)) + p^2.$$
Before going further we must define the Jacobian of an algebraic curve. For a curve $C$, the **Jacobian variety** $J(C)$ is the $g$-dimensional abelian variety identified with the degree zero Picard group $\text{Pic}^0(C) = \text{Div}^0(C)/\text{Prin}(C)$ consisting of divisor classes of degree zero. A full construction of the Jacobian of a genus 2 curve is carried out by Cassels and Flynn in [3] chapter 2. We will make use of the helpful fact that for any smooth projective curve $C/\mathbb{F}_q$, the curve $C$ and its Jacobian variety $J(C)$ have isomorphic first étale cohomology groups (see [13] Corollary 9.6). Therefore we have $\text{Tr}(\text{Frob}_{p^2} | H^1(C)) = \text{Tr}(\text{Frob}_{p^2} | H^1(J(C)))$, and the above equation can be rewritten as

$$\#C_3(\mathbb{F}_{p^2}) = 1 + p^2 - \text{Tr}(\text{Frob}_{p^2} | H^1(J(C))).$$

We have now reduced our point counting problem to computing $a_{p^2}(J(C_3)) = \text{Tr}(\text{Frob}_{p^2} | H^1(J(C_3)))$. This is possible because $C_3$ has the special property that $J(C_3)$ neatly splits into a product of two copies of a supersingular elliptic curve. We use the following result from [3] chapter 14:

**Theorem 3.5.4.** Let $C$ be a curve of genus 2 of the form $Y^2 = c_3 X^6 + c_2 X^4 + c_1 X^2 + c_0$ with no terms of odd degree in $X$. Then there are two maps from $C$ into the elliptic curves

$$E_1 : Y^2 = c_3 Z^3 + c_2 Z^2 + c_1 Z + c_0$$

$$E_2 : V^2 = c_0 U^3 + c_1 U^2 + c_2 U + c_3$$

given by $Z = X^2$ and by $(U, V) = (X^{-2}, Y X^{-3})$ respectively which extend to maps from $J(C)$. The Jacobian is therefore $\mathbb{F}_p$-isogenous to $E_1 \times E_2$, i.e. reducible.

63
In the case of $C_3$, the two elliptic curves are identical copies of the curve $E$ given by the equation $Y^2 = X^3 - 5X^2 + 5X - 1$. Therefore $J(C_3)$ is $\mathbb{F}_p$-isogenous to $E \times E$. By Tate’s isogeny theorem [19], this means that the number of points on the Jacobian is $\#J(C_3)(\mathbb{F}_{p^n}) = [\#E(\mathbb{F}_{p^n})]^2$ for all $n$. Now we can compute the zeta function of $J(C_3)$, and from there we can determine the value of $a_{p^2}(J(C_3))$.

For any elliptic curve $E$, knowing the Frobenius trace $a_p(E)$ allows us to count the points on $E$ over $\mathbb{F}_{p^n}$ for any $n$ using the formula

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - \alpha^n - \bar{\alpha}^n$$

where $\alpha, \bar{\alpha}$ are the two conjugate roots of the zeta function numerator $T^2 - aT + q$. In our case, $E$ is supersingular meaning $a_p(E) = 0$ and $\alpha = \pm i \sqrt{p}$. Therefore

$$\#E(\mathbb{F}_{p^n}) = \begin{cases} 
p^n + 1, & n \text{ odd} \\
p^n + 1 + 2(-1)^{k+1}p^k, & n = 2k \text{ even.} \end{cases}$$

To count the points of $J = J(C_3)$, we just square this quantity:

$$\#J(C_3)(\mathbb{F}_{p^n}) = \begin{cases} 
p^{2n} + 2p^n + 1, & n \text{ odd} \\
p^{2n} + 2p^n + 1 + 4p^n + 4(-1)^{k+1}p^k + 4(-1)^{k+1}p^{3k}, & n = 2k \text{ even.} \end{cases}$$

The zeta function of $J$ is then
\[ Z(J(C_3), T) = \exp \sum_{n=1}^{\infty} \frac{\#J(F_{p^n})}{n} T^n = \exp \left[ \sum_{n=1}^{\infty} \frac{p^{2n} + 2p^n + 1}{n} T^n + \sum_{k=1}^{\infty} \frac{4p^{2k} + 4(-1)^{k+1}p^k + 4(\frac{1}{2})^{k+1}p^{3k}}{2k} T^{2k} \right] \]

\[ = \frac{(1 + pT^2)^2(1 + p^3T^2)^2}{(1 - T)(1 - pT)^2(1 - p^2T)(1 - p^2T^2)^2}. \]

On the other hand, we know from the Weil conjectures that \( Z(J(C_3), T) \) has the form

\[ Z(J(C_3), T) = \prod_{i=1}^{2n} P_i(T)^{(-1)^i}, \quad P_i(T) = \exp \left[ - \sum_{n=1}^{\infty} \frac{\operatorname{Tr} \left( \operatorname{Frob}_{p^n} \mid H^i(J(C_3)) \right) T^n}{n} \right]. \]

Setting the two forms of the numerator equal to each other, we obtain

\[ \exp \left[ \sum_{n=1}^{\infty} \frac{\operatorname{Tr} \left( \operatorname{Frob}_{p^n} \mid H^1(J) \right) + \operatorname{Tr} \left( \operatorname{Frob}_{p^n} \mid H^3(J) \right) T^n}{n} \right] \]

\[ = \exp \left[ 2 \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(pT^2)^n}{n} + 2 \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(p^3T^2)^n}{n} \right]. \]

For our purposes, only the \( T^2 \) term is needed:

\[ \left[ \operatorname{Tr} \left( \operatorname{Frob}_{p^2} \mid H^1(J) \right) + \operatorname{Tr} \left( \operatorname{Frob}_{p^2} \mid H^3(J) \right) \right] \frac{T^2}{2} = -2(p + p^3) \frac{T^2}{1}. \]

Furthermore, we know that \( \operatorname{Tr} \left( \operatorname{Frob}_{p^2} \mid H^3(J(C_3)) \right) = p^2 \operatorname{Tr} \left( \operatorname{Frob}_{p^2} \mid H^1(J(C_3)) \right) \) by duality. Therefore we can write

\[ (1 + p^2) \operatorname{Tr} \left( \operatorname{Frob}_{p^2} \mid H^1(J) \right) = -4p(1 + p^2) \]
and so \( \text{Tr} (\text{Frob}_p | H^1(J)) = -4p \). This in turn gives us \( \#C(\mathbb{F}_p^2) = p^2 + 1 - 4p \), proving the lemma.

### 3.5.1.2 The zeta function

The zeta function of the curve model \( C : Y^2 = X(X^4 - 1) \) over \( \mathbb{F}_p \) is given by

\[
Z(C, T) = \exp \left( \sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{p^n})}{n} T^n \right)
\]

where \( T = p^{-s} \). We know that this function has the form

\[
Z(C, T) = \frac{P(T)}{(1 - T)(1 - pT)}
\]

where \( P(T) = \prod_{i=1}^{g} (1 - \alpha_i T)(1 - \bar{\alpha}_i T) \) for some complex numbers \( \alpha_i \) of magnitude \( \sqrt{p} \). Using the formula \( \#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{g} (\alpha_i^n + \bar{\alpha}_i^n) \), we construct a system of two nonlinear equations in \( \alpha_1 \) and \( \alpha_2 \).

\[
\begin{align*}
\alpha_1 + \bar{\alpha}_1 + \alpha_2 + \bar{\alpha}_2 &= p + 1 - \#C(\mathbb{F}_p) = 0 \\
\alpha_1^2 + \bar{\alpha}_1^2 + \alpha_2^2 + \bar{\alpha}_2^2 &= p^2 + 1 - \#C(\mathbb{F}_p^2) = 4p.
\end{align*}
\]

The unique solution is \( \alpha_1 = -\alpha_2 = \pm \sqrt{p} \). Therefore the zeta function of this curve model (and therefore also of the function field) is

\[
Z(L, T) = Z(C, T) = \frac{(1 - pT^2)^2}{(1 - T)(1 - pT)}.
\]

Clearly this zeta function vanishes to order 2 at \( T = p^{-1/2} \) or at \( s = 1/2 \), completing at last the proof of Theorem 3.5.1.
3.6 Future work

In the future, it may be possible to isolate other families of function field extensions which have even higher order of vanishing. As shown in Appendix B, we found many such extensions empirically. However, it is challenging to create parameterized families for which we can compute the zeta function exactly. First it is necessary to find a $3 \times 3$ matrix which makes the quadratic form $aX^2 + bY^2 + abZ^2$ equivalent to $X^2 + Y^2 + Z^2$ like the one in equation 3.1, which is difficult in itself. Then the zeta function of the quaternion extension must be computed as in section 3.5.1.

An empirical approach to this problem relies on fast computation of zeta functions of these quaternion extensions of $\mathbb{F}_p(t)$. We collected preliminary data using Magma’s built-in routines for computing zeta functions, but this is only suitable for low-genus curves as the running time is exponential in the genus. Tuitman [21] has developed a new refinement of Kedlaya’s point counting algorithm which could greatly improve the speed of these zeta function calculations. However, in order to adapt this method to our problem, we first need a fast, reliable algorithm to lift our curves from $\mathbb{F}_p$ to $\mathbb{Q}$ without increasing the genus. Tuitman and his co-authors have developed methods for doing this for curves of genus up to 5 or gonality up to 4. For our purposes, we would need to develop a similar method for 8-gonal curves with Galois group $Q_8$. This is a very promising area for future investigation.
This appendix contains additional details from the proof of Theorem 2.5.1 in Section 2.5. In the ring $R_r = \mathbb{F}_2[x, t]/(x^2 + tx + r(t))$, we formulate the probability that a randomly chosen polynomial has finite $mx + 1$ stopping time as a version of the gambler’s ruin problem. To finish the proof, we need only prove the following lemma.

**Lemma A.0.1.** For $d > 0$, let $P_d$ be defined

$$P_d = P\left(\exists N > 0 : \sum_{k=0}^{N-1} X_k < \frac{N}{d}\right)$$

where $X_i$ are IID Bernoulli variables taking the value 1 with probability 1/4 and 0 otherwise. If $d \leq 4$, then $P_d = 1$. If $d > 4$, then $P_d$ is the unique root of $g_d(z) = z^d - 4z + 3$ inside the unit disk, which is real and lies in the interval $(3/4, 1)$.

### A.1 Solving a recurrence relation

As in $\mathbb{F}_2[t]$, we first use a recurrence relation to solve the alternate version of the game which ends if the gambler reaches a value of $W$. We label $U_k$ the probability
of ruin under these conditions given a starting value of $k$. Clearly $U_k = -1$ for all $k < 0$ and $U_k = 0$ for all $k \geq W$. For other values of $k$, we have the following linear recurrence relation.

$$U_k = \frac{3}{4}U_{k-1} + \frac{1}{4}U_{k+d-1}$$

Our goal is to find the value of $U_0$, representing the probability of ruin (depending on $W$) starting from a value of 0. If we then take the limit of this quantity as $W \to \infty$, we will learn the actual probability of ruin in a game with no upper limit.

The auxiliary polynomial for the recurrence is $g_d(z) = z^d - 4z + 3$, which is separable as long as $d \neq 4$. When $d = 4$ the root $z = 1$ has multiplicity 2, so we handle this case first. In this case, the solutions to the recurrence equation will take the form $U_k = c_1 + c_2k + c_3\lambda^k + c_4\bar{\lambda}^k$. Since we know that $U_{-1} = 1$ and $U_0 = U_{W+1} = U_{W+2} = 0$, we can find the specific solution we need by solving the following linear system:

$$
\begin{bmatrix}
1 & -1 & \lambda^{-1} & \bar{\lambda}^{-1} \\
1 & W & \lambda^W & \bar{\lambda}^W \\
1 & W + 1 & \lambda^{W+1} & \bar{\lambda}^{W+1} \\
1 & W + 2 & \lambda^{W+2} & \bar{\lambda}^{W+2}
\end{bmatrix}
\begin{bmatrix}
c_1 \\
c_2 \\
c_3 \\
c_4
\end{bmatrix}
= 
\begin{bmatrix}
1 \\
0 \\
0 \\
0
\end{bmatrix}.
$$

The quantity we are seeking is then $U_0 = c_1 + c_3 + c_4$. We label the $4 \times 4$ matrix above $A$. Using Cramer’s rule, we write
where }A_j\text{ is the determinant of }A\text{ with the column }j\text{ replaced by }[1,0,\ldots,0]. \text{ Next, we expand the determinant of }A\text{ in terms of the cofactors.}

\[
det A = A_{1,1} - A_{1,2} + \lambda^{-1}A_{1,3} + \bar{\lambda}^{-1}A_{1,4}.
\]

For this linear system, because the right-hand vector }b\text{ is just the first standard basis vector, the determinant of }A\text{ with the }j\text{-th column replaced by }b\text{ is the same as the } (1,j)\text{-cofactor of }A. \text{ That is, } \det A_i = A_{1,i}. \text{ This allows us to write }

\[
U_0 = \frac{A_{1,1} + A_{1,3} + A_{1,4}}{A_{1,1} - A_{1,2} + \lambda^{-1}A_{1,3} + \lambda^{-1}A_{1,4}}.
\]

We argue that }A_{1,1}\text{ dominates the other terms asymptotically as }W \to \infty, \text{ and therefore that } P_4 = \lim_{W \to \infty} U_0 = 1. \text{ We must express all four cofactors as functions of }W.
\[ A_{1,1} = \begin{vmatrix} W & \lambda^W & \bar{\lambda}^W \\ W + 1 & \lambda^{W+1} & \bar{\lambda}^{W+1} \\ W + 2 & \lambda^{W+2} & \bar{\lambda}^{W+2} \end{vmatrix} = \lambda^W \bar{\lambda}^W \begin{vmatrix} W & 1 & 1 \\ W + 1 & \lambda & \bar{\lambda} \\ W + 2 & \lambda^2 & \bar{\lambda}^2 \end{vmatrix} \]

\[ = \lambda^W \bar{\lambda}^W \left( \begin{vmatrix} W & \lambda & \bar{\lambda} \\ \lambda^2 & \bar{\lambda}^2 \\ W + 1 & \bar{\lambda} \\ W + 2 & \bar{\lambda}^2 \end{vmatrix} - \begin{vmatrix} W + 1 & \lambda \\ W + 2 & \lambda^2 \\ \lambda + 1 & \bar{\lambda} \\ \lambda + 2 & \bar{\lambda}^2 \end{vmatrix} \right) \]

\[ = \lambda^W \bar{\lambda}^W \left[ W (\lambda \bar{\lambda}^2 - \lambda^2 \bar{\lambda}) - (W \bar{\lambda}^2 + \lambda^2 - W \bar{\lambda} - 2\bar{\lambda}) + (W \lambda^2 + \lambda^2 - W \lambda - 2\lambda) \right] \]

\[ = \lambda^W \bar{\lambda}^W \left[ W (\lambda \bar{\lambda}^2 - \lambda^2 \bar{\lambda} + \lambda^2 - \bar{\lambda}^2 - \bar{\lambda} - \lambda) + \lambda^2 - (\bar{\lambda}^2 + 2\bar{\lambda} - 2\lambda) \right] \]

Now we use the fact that \( \lambda \) and \( \bar{\lambda} \) are the roots of \( x^2 + 2x + 3 \) and write

\[ A_{1,1} = 3^W \left[ W (3\bar{\lambda} - 3\lambda - 2\lambda - 3 + 2\bar{\lambda} + 3 + \bar{\lambda} - \lambda) - 2\lambda - 3 + 2\bar{\lambda} + 3 + 2\bar{\lambda} - 2\lambda \right] \]

\[ = 6(\bar{\lambda} - \lambda)W^3 + 4(\bar{\lambda} - \lambda)3^W. \]

\[ A_{1,2} = - \begin{vmatrix} 1 & \lambda^W & \bar{\lambda}^W \\ 1 & \lambda^{W+1} & \bar{\lambda}^{W+1} \\ 1 & \lambda^{W+2} & \bar{\lambda}^{W+2} \end{vmatrix} = -\lambda^W \bar{\lambda}^W \begin{vmatrix} 1 & 1 & 1 \\ 1 & \lambda & \bar{\lambda} \\ 1 & \lambda^2 & \bar{\lambda}^2 \end{vmatrix} \]

\[ = -3^W \left[ (3\bar{\lambda} - 3\lambda) - (\bar{\lambda}^2 - \bar{\lambda}) + (\lambda^2 - \lambda) \right] \]

\[ = -3^W \left[ 3\bar{\lambda} - 3\lambda + 3\bar{\lambda} + 3 - 3\lambda - 3 \right] \]

\[ = -6(\bar{\lambda} - \lambda)3^W. \]

71
\[
A_{1,3} = \begin{vmatrix} 1 & W & \lambda^W \\ 1 & W + 1 & \lambda^{W+1} \\ 1 & W + 2 & \lambda^{W+2} \end{vmatrix} = \lambda^W \begin{vmatrix} 1 & W & 1 \\ 1 & W + 1 & \lambda \\ 1 & W + 2 & \lambda^2 \end{vmatrix}
\]
\[
= \lambda^W \left( \begin{vmatrix} W + 1 & \lambda \\ W + 2 & \lambda^2 \end{vmatrix} - W \begin{vmatrix} 1 & \lambda \\ 1 & \lambda^2 \end{vmatrix} + \begin{vmatrix} 1 & W + 1 \\ 1 & W + 2 \end{vmatrix} \right)
\]
\[
= \lambda^W \left[ (W\lambda + \lambda^2 - W\lambda - 2\lambda) - W (\lambda^2 - W\lambda) + (W + 2 - W - 1) \right]
\]
\[
= \lambda^W (\lambda^2 - 2\lambda + 1)
\]
\[
= \lambda^W (-4\lambda - 2).
\]

\[
A_{1,4} = -\begin{vmatrix} 1 & W & \lambda^W \\ 1 & W + 1 & \lambda^{W+1} \\ 1 & W + 2 & \lambda^{W+2} \end{vmatrix} = -\lambda^W \begin{vmatrix} 1 & W & 1 \\ 1 & W + 1 & \lambda \\ 1 & W + 2 & \lambda^2 \end{vmatrix}
\]
\[
= -\lambda^W \left( \begin{vmatrix} W + 1 & \lambda \\ W + 2 & \lambda^2 \end{vmatrix} - W \begin{vmatrix} 1 & \lambda \\ 1 & \lambda^2 \end{vmatrix} + \begin{vmatrix} 1 & W + 1 \\ 1 & W + 2 \end{vmatrix} \right)
\]
\[
= -\lambda^W \left[ (W\lambda^2 + \lambda^2 - W\lambda - 2\lambda) - W (\lambda^2 - W\lambda) + (W + 2 - W - 1) \right]
\]
\[
= -\lambda^W (\lambda^2 - 2\lambda + 1)
\]
\[
= -\lambda^W (-4\lambda - 2).
\]

To summarize, the asymptotic growth rates of the cofactors are:
\[ A_{1,1} \sim W 3^W \]
\[ A_{1,2} \sim 3^W \]
\[ A_{1,3} \sim \lambda^W \]
\[ A_{1,4} \sim \bar{\lambda}^W. \]

It is clear that \( A_{1,1} \) dominates the other cofactors as \( W \to \infty \). Since the numerator and denominator have the same dominant term with the same coefficient, the probability of ruin in this case is

\[ P_4 = \lim_{W \to \infty} P_{4,W} = 1. \]

For \( d \neq 4 \) we have \( \gcd(f, f') = 1 \), so in this case the polynomial is separable. Therefore every solution must have the form \( U_k = c_1\lambda_1^k + c_2\lambda_2^k + \ldots + c_d\lambda_d^k \). The linear system we must solve is exactly the same as the one we found in \( F_2[t] \), except that the roots \( \lambda_i \) are now the roots of \( z^d - 4z + 3 = 0 \).

We can solve this system in the same way, using Cramer’s rule and Vandermonde determinants. The product of all the roots is still the constant term of \( g_d(z) \), which
in this case is $\prod_{j=1}^{d} \lambda_j = 3$. So $\det A_i = (-1)^{1+i} 3^W \lambda_i^{W} B_i$, and the solution to the recurrence relation is

$$P_{d,W} = U_0 = \sum_{j=1}^{d} c_j = \sum_{j=1}^{d} \frac{\det A_j}{\det A} = \frac{\sum_{j=1}^{d} (-1)^{1+j} 3^W \lambda_j^{-W} B_j}{\sum_{j=1}^{d} (-1)^{1+j} 3^W \lambda_j^{-W-1} B_j}$$

where $B_j$ are defined as Vandermonde determinants as before. Just as in $\mathbb{F}_2[t]$, if $\lambda_1$ is a real root with strictly smaller absolute value than all of the others, then the limit of the above quantity is

$$P_d = \lim_{W \to \infty} U_0 = \lambda_1.$$ 

### A.2 Roots of $g_d(z)$

We will now examine the polynomial $g_d(z) = z^d - 4z + 3$ and show that when $d \neq 4$, such a root does in fact exist. For $d = 2$, the polynomial $g_2(z) = z^2 - 4z + 3$ has roots at $z = 1$ and $z = 3$. Since $z = 1$ is the root with the smallest magnitude, the probability of ruin is 1. For $d = 3$, we write $g_3(z) = z^3 - 4z + 3 = (z - 1)(z^2 + z - 3)$. Using the quadratic formula, we find that the roots of $z^2 + z - 3$ are $z = -\frac{1}{2} \pm \frac{\sqrt{13}}{2}$, both of which have magnitude $> 1$. Since $z = 1$ is the root with the smallest magnitude, the probability of ruin is 1.

Only one case remains. When $d > 4$, we use Descartes’ rule of signs and determine that there are two positive real roots of $g_d(z)$, one of which must be $z = 1$. Since
Figure A.1. Using Rouche’s theorem to prove that $g_d(z)$ has a unique real root inside the unit disk.

$g'_d(1) = d - 4 > 0$, we know that $g_d(1 - \epsilon) < 0$ for small positive epsilon. On the other hand, $g_d(3/4) = (3/4)^d > 0$. Therefore, the other real root must lie in the interval $(3/4, 1)$.

Next, we use Rouche’s theorem to prove that there is only one root within the unit circle. Let $f(z) = z^d$ and let $h(z) = -4z + 3$. For small positive $\epsilon$, consider the circle $C_\epsilon = \{z \in \mathbb{C} : |z| = 1 - \epsilon\}$. The function $f$ maps $C_\epsilon$ to a smaller circle $|z| = (1 - \epsilon)^d$. Define $m_f(\epsilon) = (1 - \epsilon)^d$. Then $|f(z)| = m_f(\epsilon)$ for all $z \in C_\epsilon$.

The other function $h$ maps $C_\epsilon$ to a circle of radius $4(1 - \epsilon)$ centered at $z = 3$. The point on this circle closest to the origin is the point $z = -1 + 4\epsilon$, with magnitude $|-1 + 4\epsilon| = 1 - 4\epsilon$. Define $m_h(\epsilon) = 1 - 4\epsilon$. Then for all $z \in C_\epsilon$, $|h(z)| \geq m_h(\epsilon)$.

We claim that for small positive $\epsilon$, $m_h(\epsilon) > m_f(\epsilon)$ and therefore that $|h(z)| > |f(z)|$ for all $z \in C_\epsilon$. Notice that $m_h(0) = m_f(0) = 1$. Calculating the derivatives
of the two functions, we see that \( m_h'(0) = -4 \) and \( m_f'(0) = -d \). By continuity, since \( m_h'(0) > m_f'(0) \), \( m_h(\epsilon) \) must be greater than \( m_f(\epsilon) \) for small positive values of \( \epsilon \).

Since \( |h(z)| > |f(z)| \) for all \( z \in C_\epsilon \), \( g_d(z) = h(z) + f(z) \) must have the same number of roots within \( C_\epsilon \) as \( h(z) \). The function \( h(z) = 3 - 4z \) has one root at \( z = 3/4 \). Therefore, for small positive \( \epsilon \), \( g_d(z) \) has a unique root inside the circle \( |z| = 1 - \epsilon \), which must be the previously mentioned real root lying in the interval \((3/4, 1)\). Since this root has the smallest magnitude among roots of \( g_d(z) \), the value of this root is the probability of ruin \( P_d \).
APPENDIX B
LIST OF FUNCTION FIELDS

For a few small primes $p$, we present a list of some biquadratic extensions $K_{a,b,c}$ of $\mathbb{F}_p(t)$ satisfying Witt’s criterion. Recall that by $K_{a,b,c}$ we mean the biquadratic extension containing the quadratic extensions $K(\sqrt{ab}), K(\sqrt{bc})$, and $K(\sqrt{ac})$ for a triple of squarefree polynomials $(a, b, c)$. In this appendix we list such extensions where $a, b, c$ are all of degree $\leq 2$. For each such extension, we list the defining polynomial $f(x, t)$ of a quaternion extension of $L/\mathbb{F}_p(t)$ of (probable) minimum genus $g$, and the order of vanishing $\rho_L = \text{ord}_{s=1/2} \zeta(L/\mathbb{F}_p(t), s)$ of the zeta function of this extension.

The special family described in Theorem 3.5.1 is given by $(a, b, c) = (t + w^2, t, t)$ when $p \equiv 5 \mod 8$. Outside of this family we see many other extensions with $\rho_X > 1$, so it is possible that other families with unusually high $\rho_X$ can be constructed.

<table>
<thead>
<tr>
<th>$p = 3$</th>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$g$</th>
<th>$\rho_X$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t + 1$</td>
<td>$t$</td>
<td>$1$</td>
<td>$2$</td>
<td>$0$</td>
<td>$x^8 + 2x^6 + (2t^3 + t^2 + 1)/t^2x^4 + (t^8 + 2t^{10} + 2t^2 + t^4 + t + 2)/t^4x^2 + (t^{12} + 2t^3 + 2t^{12} + 2t^6 + t^2 + t^6 + t^8 + 2t^6 + 2t^3 + 2t^2 + t + 1)/(t^8 + 2t^7 + t^6)$</td>
<td></td>
</tr>
<tr>
<td>$t + 2$</td>
<td>$t$</td>
<td>$1$</td>
<td>$2$</td>
<td>$0$</td>
<td>$x^8 + 2x^6 + (2t^3 + t^2 + 2t + 1)/(t^4 + 2t + 1)x^4 + (t^8 + 2t^2 + t^3 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + t^10)/t^2x^2 + (t^{14} + t^{13} + 2t^{12} + 2t^6 + 2t^7 + t^6 + 2t^5 + 2t^4 + t^3 + 2t^2 + 2t + 1)/(t^8 + t^7 + t^6)$</td>
<td></td>
</tr>
<tr>
<td>$t + 2$</td>
<td>$t + 1$</td>
<td>$1$</td>
<td>$2$</td>
<td>$0$</td>
<td>$x^8 + 2x^6 + (2t^3 + t^2 + 2t + 1)/(t^4 + 2t + 1)x^4 + (t^8 + 2t^2 + t^3 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + t^10 + 2t^8 + 2t^7 + t^6)/(t^8 + t^7 + t^6 + 2t^5 + 2t^4 + 2t^3 + 2t^2 + t + 1)$</td>
<td></td>
</tr>
<tr>
<td>$t + 2$</td>
<td>$t + 1$</td>
<td>$t$</td>
<td>$2$</td>
<td>$0$</td>
<td>$x^8 + 2x^6 + (t^4 + t^3 + t^2)/(t^4 + 2t + 1)x^4 + (t^{10} + t^9 + t^6 + 2t^5 + 2t^4 + 2t^2)/(t^4 + t^3 + t^2)x^2 + (t^{10} + t^9 + 2t^8 + 2t^7 + t^6 + 2t^5 + 2t^4 + t^3 + 2t^2 + t + 1)/(t^10 + t^9 + t^8 + 2t^7 + 2t^6 + 2t^5 + t^4 + t^3 + t^2)$</td>
<td>continued . . .</td>
</tr>
<tr>
<td>(x)</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>(n)</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>10</td>
<td>20</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>7</td>
<td>28</td>
<td>70</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>10</td>
<td>55</td>
<td>165</td>
<td>330</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>13</td>
<td>91</td>
<td>300</td>
<td>690</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>16</td>
<td>126</td>
<td>455</td>
<td>1287</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>19</td>
<td>171</td>
<td>630</td>
<td>1930</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>22</td>
<td>220</td>
<td>816</td>
<td>2530</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>25</td>
<td>275</td>
<td>1001</td>
<td>3300</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>28</td>
<td>326</td>
<td>1240</td>
<td>4095</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>31</td>
<td>381</td>
<td>1520</td>
<td>5026</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>34</td>
<td>441</td>
<td>1890</td>
<td>6282</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>37</td>
<td>504</td>
<td>2316</td>
<td>7716</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>40</td>
<td>570</td>
<td>2790</td>
<td>9220</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>43</td>
<td>639</td>
<td>3294</td>
<td>10827</td>
<td></td>
</tr>
</tbody>
</table>

\(d = x^n + x^{n-1} + x^{n-2} + \ldots + x + 1\)
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$t+3$</td>
<td>$t+2$</td>
<td>$t+1$</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+4$</td>
<td>$t$</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+1$</td>
<td>$t$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+1$</td>
<td>$t$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+2$</td>
<td>$t+1$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+2$</td>
<td>$t+1$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+3$</td>
<td>$t+2$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+3$</td>
<td>$t+2$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+3$</td>
<td>$t+2$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+3$</td>
<td>$t+2$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$t+3$</td>
<td>$t+2$</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

$\phi^p = \phi^{p-1}$

$t^2 + 1$

$\phi^2 + \phi^1 + \phi^0 = \phi^{p+1}$

$\phi^2 + \phi^1 + \phi^0 = \phi^{p+1}$

$\phi^p = \phi^{p-1}$

$t^2 + 2$

$\phi^2 + \phi^1 + \phi^0 = \phi^{p+1}$

$\phi^2 + \phi^1 + \phi^0 = \phi^{p+1}$

$\phi^p = \phi^{p-1}$

$t^2 + 2$

$\phi^2 + \phi^1 + \phi^0 = \phi^{p+1}$

$\phi^2 + \phi^1 + \phi^0 = \phi^{p+1}$

$\phi^p = \phi^{p-1}$

continued...
<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>g</th>
<th>px</th>
</tr>
</thead>
<tbody>
<tr>
<td>(t^2 + 2)</td>
<td>(t + 2)</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>(t^2 + 2)</td>
<td>(t + 3)</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>(t^2 + 2)</td>
<td>(t + 3)</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>(t^2 + 2)</td>
<td>(t + 4)</td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>(t^2 + 4)</td>
<td>(t + 1)</td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>(t^2 + 2)</td>
<td>(t + 1)</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>(t^2 + 2)</td>
<td>(t + 1)</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>(t^2 + 2)</td>
<td>(t + 1)</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
</tbody>
</table>

continued...
<table>
<thead>
<tr>
<th>j</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
</tr>
<tr>
<td>1</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
</tr>
<tr>
<td>2</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
</tr>
<tr>
<td>3</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
</tr>
<tr>
<td>4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
</tr>
<tr>
<td>5</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
</tr>
<tr>
<td>6</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
</tr>
<tr>
<td>7</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
</tr>
<tr>
<td>8</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
</tr>
<tr>
<td>9</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
</tr>
<tr>
<td>10</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
<td>+4</td>
<td>+2</td>
</tr>
<tr>
<td>$a$</td>
<td>$b$</td>
<td>$c$</td>
<td>$g$</td>
<td>$px$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$t^2 + 3$</td>
<td>$t^2 + 2$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$p = 5$
\[ p = 5 \]

<table>
<thead>
<tr>
<th>( a )</th>
<th>( b )</th>
<th>( c )</th>
<th>( g )</th>
<th>( px )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( t^2 + 4 )</td>
<td>( t^2 + 3 )</td>
<td>( t^2 + 2 )</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>( t^2 + 4 )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + 2 )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + 2 )</td>
<td>( t^2 + 2 )</td>
<td>1</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + 2 )</td>
<td>( t^2 + 2 )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + 2 )</td>
<td>( t^2 + 2 )</td>
<td>1</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + 2 )</td>
<td>( t^2 + 2 )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>( t^2 + t )</td>
<td>( t^2 + t )</td>
<td>1</td>
<td>7</td>
<td>4</td>
</tr>
</tbody>
</table>

\[ \begin{align*}
\text{continued...} &
\end{align*} \]
<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>g</th>
<th>pX</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t^2 + t + 1$</td>
<td>$t^2 + 1$</td>
<td>$t + 3$</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>$2x^5 + x^4 + (t^2 + 2t^2 + t^2 + t + 1 + 2t^2 + t^2 + 2t^2 + 2t^2 + 2t^2 + 2t + 1)$</td>
<td>$t^2 + 2t$</td>
<td>$t + 1$</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>$2x^5 + x^4 + (t^2 + 2t^2 + t^2 + t + 1 + 2t^2 + t^2 + 2t^2 + 2t^2 + 2t^2 + 2t + 1)$</td>
<td>$t^2 + 2t$</td>
<td>$t + 1$</td>
<td>7</td>
<td>4</td>
</tr>
</tbody>
</table>

$2x^5 + x^4 + (t^2 + 2t^2 + t^2 + t + 1 + 2t^2 + t^2 + 2t^2 + 2t^2 + 2t^2 + 2t + 1) + (t^2 + 2t^2 + t^2 + t + 1 + 2t^2 + t^2 + 2t^2 + 2t^2 + 2t^2 + 2t + 1) + (t^2 + 2t^2 + t^2 + t + 1 + 2t^2 + t^2 + 2t^2 + 2t^2 + 2t^2 + 2t + 1) + (t^2 + 2t^2 + t^2 + t + 1 + 2t^2 + t^2 + 2t^2 + 2t^2 + 2t^2 + 2t + 1)

$...$
<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$g$</th>
<th>$p_X$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 2$</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t + 4$</td>
<td>$t + 2$</td>
<td>$t + 2$</td>
<td>$t + 1$</td>
<td>$t + 1$</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + 1$</td>
<td>$t + 1$</td>
<td>$t + 1$</td>
<td>$t + 1$</td>
<td>$t + 1$</td>
</tr>
</tbody>
</table>

continued...
<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$g$</th>
<th>$pX$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 3$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 3$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 3$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + 2$</td>
<td>$t^2 + 3$</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>

$p = 5$

\[
\begin{align*}
x^5 + x^4 + (2t^4 + t^3 + 2t^2 + 3t + 2)x^3 + (2t^2 + t + 1)x^2 + (2t^2 + t + 1)x + 1 & = 0 \\
x^5 + x^4 + (2t^4 + t^3 + 2t^2 + 3t + 2)x^3 + (2t^2 + t + 1)x^2 + (2t^2 + t + 1)x + 1 & = 0 \\
x^5 + x^4 + (2t^4 + t^3 + 2t^2 + 3t + 2)x^3 + (2t^2 + t + 1)x^2 + (2t^2 + t + 1)x + 1 & = 0
\end{align*}
\]

continued...
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>$t^2 + t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>$t^2 + t + 3$</td>
<td>$t + 3$</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>$t^2 + t + 3$</td>
<td>$t + 3$</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>

continued...
<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>g</th>
<th>pX</th>
<th>j</th>
</tr>
</thead>
<tbody>
<tr>
<td>t² + t + 3</td>
<td>t² + t + 2</td>
<td>t² + t</td>
<td>11</td>
<td>4</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
</tr>
<tr>
<td>t² + t + 3</td>
<td>t² + t + 2</td>
<td>t² + t + 1</td>
<td>11</td>
<td>4</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
</tr>
<tr>
<td>t² + t + 3</td>
<td>t² + t + 2</td>
<td>t² + t + 2</td>
<td>11</td>
<td>4</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
</tr>
<tr>
<td>t² + t + 3</td>
<td>t² + t + 2</td>
<td>t² + t + 2</td>
<td>11</td>
<td>4</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
</tr>
<tr>
<td>t² + 2t</td>
<td>t + 1</td>
<td>7</td>
<td>4</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
<td>4</td>
</tr>
<tr>
<td>t² + 2t</td>
<td>t² + 2</td>
<td>t + 4</td>
<td>11</td>
<td>4</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
</tr>
<tr>
<td>t² + 2t</td>
<td>t² + 3</td>
<td>1</td>
<td>7</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
<td>4</td>
</tr>
<tr>
<td>t² + 2t</td>
<td>t² + 3</td>
<td>1</td>
<td>7</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
<td>4</td>
</tr>
<tr>
<td>t² + 2t</td>
<td>t² + 3</td>
<td>1</td>
<td>7</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
<td>4</td>
</tr>
<tr>
<td>t² + 2t</td>
<td>t² + 3</td>
<td>1</td>
<td>7</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
<td>4</td>
</tr>
<tr>
<td>t² + 2t</td>
<td>t² + 3</td>
<td>1</td>
<td>7</td>
<td>x⁸ + x⁶ + (2t + 6 + 3t² + 3 + 3t⁴ + t⁵ + 4) + t² + 2 + 2t + 4 + t + 2</td>
<td>4</td>
</tr>
</tbody>
</table>

continued...
<table>
<thead>
<tr>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
<th>$g$</th>
<th>$pX$</th>
<th>$f$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t^2 + 2t + 2$</td>
<td>$t^2 + t$</td>
<td>$t^2 + 3$</td>
<td>11</td>
<td>4</td>
<td>$x^5 + x^4 + (2t^2 + 4t + 3)x^3 + 4t^3 + 2t^3 + 3t^2 + t^2 + 2t + 1$</td>
</tr>
<tr>
<td>$t^2 + 2t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>$x^4 + x^3 + (2t + 3)x^2 + 4t^2 + 3t + 2) + (t^2 + 4t + 2t + 1)$</td>
</tr>
<tr>
<td>$t^2 + 2t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>$x^4 + x^3 + (2t + 3)x^2 + 4t^2 + 3t + 2) + (t^2 + 4t + 2t + 1)$</td>
</tr>
<tr>
<td>$t^2 + 2t + 2$</td>
<td>$t^2 + t + 1$</td>
<td>$t + 1$</td>
<td>11</td>
<td>4</td>
<td>$x^5 + x^4 + (3t^2 + 3t + 1) + (t^2 + 4t + 2t + 1)$</td>
</tr>
<tr>
<td>$t^2 + 2t + 2$</td>
<td>$t^2 + t + 2$</td>
<td>$t$</td>
<td>11</td>
<td>4</td>
<td>$x^5 + x^4 + (2t + 3)x^2 + 4t^2 + 3t + 2)$ + (t^2 + 4t + 2t + 1)$</td>
</tr>
</tbody>
</table>

$p = 5$
APPENDIX C

MAGMA CODE FOR WORKING WITH QUATERNION EXTENSIONS OF $\mathbb{F}_p(t)$

WittsCriterion: This function tests whether $(a, b)$ is a Witt pair in the field $K$.

```magma
function WittsCriterion( K, a, b )
    primes := Factorization(LCM( Numerator( a ), Numerator( b ) ));
    for f in primes do
        r := f[ 1 ];
        if HilbertSymbol( a, b, r ) * HilbertSymbol( a, a, r ) * HilbertSymbol( b, b, r ) ne 1 then
            return false;
        end if;
    end for;
    return true;
end function;
```

SplitOff: Function to split off a hyperbolic plane from a ternary quadratic form $X$. This is nondeterministic since it uses the Magma function HasRationalPoint which randomly finds a rational point on a curve. This function is based on code from Markus Kirschmer of RWTH Aachen University.
function SplitOff(X)
C:= Conic(X);
ok, v:= HasRationalPoint(C);
error if not ok, "The form is anisotropic!";
v:= Vector(Eltseq(v)); // (v,v) = 0
ok:= exists(w){w: w in Basis(Parent(v)) | (v*X, w) ne 0 };  
assert ok;
w /:= (v*X, w);     // now (w,v) = 1
w +:= -(w*X, w)/2 *v; // now (w,w) = 0
M:= Matrix( [v,w] );
K:= KernelMatrix(X * Transpose(M)); // spit of <v,w>^perp
return VerticalJoin(M, K);
end function;

TrivMatrix: Given a Witt pair (a,b) over a field K, this function finds a matrix P such that \( PAP^T = I_3 \), where A is the diagonal matrix with coefficients a,b,ab. In other words, P is the matrix of a change of coordinates which makes the quadratic form \( aX^2 + bY^2 + abZ^2 \) equivalent to the form \( X^2 + Y^2 + Z^2 \). This function is based on code from Markus Kirschmer of RWTH Aachen University.

function TrivMatrix( K, a, b )
F:= DiagonalMatrix([K | a,b,a*b]);
G:= DiagonalMatrix([K | 1,1,1]);
S:= SplitOf(F);
T:= SplitOf(G); T:= ChangeRing(T, K);
// now we fix the last diagonal entry:
c := (S*F*Transpose(S))[3,3];
d := (T*G*Transpose(T))[3,3];
ok, e := IsSquare(c/d);
error if not ok, "Same determinants?";
S[3] /:= e;
P := T⁻¹ * S; // this should be the result.
assert P * F * Transpose(P) eq G; // final check
return P;
end function;

**WittDefiningPolynomial:** Assuming \((a, b)\) is a Witt pair in \(K\), this function finds the defining polynomial for a quaternion extension \(L/K\) containing \(K(\sqrt{a}, \sqrt{b})\). This is nondeterministic because of the random behavior of SplitOff.

```haskell
function WittDefiningPolynomial( K, a, b )
M := TrivMatrix( K, a, b );
p1 := M[1,1];
p2 := M[2,2];
p3 := M[3,3];
R<x> := PolynomialRing( K );
// hard-coded defining polynomial depending on a,b,p1,p2,p3
f := x^8-4*x^6-2*a*b*p3^2*x^4-2*b*p2^2*x^4-2*a*p1^2*x^4+6*x^4
+4*a*b*p3^2*x^2-8*a*b*p1*p2*p3*x^2+4*b*p2^2*x^2+4*a*p1^2*x^2
-4*x^2+a^2*b^2*p3^4-2*a*b^2*p2^2*p3^2-2*a^2*b*p1^2*p2^2
-2*a*b*p3^2+8*a*b*p1*p2*p3+b^2*p2^4-2*a*b*p1^2*p2^2-2*b*p2^2
+a^2*p1^4-2*a*p1^2+1;
```

97
FindLowGenusWittPoly: Given a witt pair \((a, b)\) in a field \(K\), this function generates \(n\) different quaternion extensions containing \(K(\sqrt{a}, \sqrt{b})\) and returns one of minimum genus.

```plaintext
function FindLowGenusWittPoly( K, a, b, n )

  mingenus := -1;
  mingenuspoly := 1;
  printf "found fields of genus ";
  for i in [ 1 .. n ] do
    f := WittDefiningPolynomial( K, a, b );
    F := FunctionField( f );
    g := Genus( F );
    printf " %o", g;
    if mingenus lt 0 or g lt mingenus then
      mingenus := g;
      mingenuspoly := f;
    end if;
    if g eq 2 then
      break i;
    end if;
  end for;
  //printf "\nminimal genus is %o.\n", mingenus;

return f;
end function;
```
return mingenuspoly, mingenus;
end function;

Zeta2: Given the zeta function of a curve $C/F_p$, this function computes the zeta function of $C/F_{p^2}$ using the identity $Z(C/F_{p^2}, s) = Z(C/F_p, s)Z(C/F_p, -s)$.

function Zeta2( Z )
V<s> := PolynomialRing( Integers( ) );
VZ := V ! Z ;
Z2sqr := VZ * Evaluate( VZ, -s );
Z2 := 0;
for i := 0 to ( Degree( Z2sqr ) div 2 ) do // deflate poly
    Z2 +:= Coefficient( Z2sqr, 2*i ) * s^i;
end for;
return Z2;
end function;

WittFieldZetas: Assuming $a, b$ is a witt pair in $K$, this function generates a quaternion extension of $F_p(t)$ containing $K(\sqrt{a}, \sqrt{b})$ of (probably) minimum genus. It then computes the zeta function of this field over $F_p$ and determines the order of vanishing at $s = 1/2$.

function WittFieldZetas( K, a, b )
p := Characteristic( K );
f, g := FindLowGenusWittPoly( K, a, b, 40 );
F := FunctionField( f );
printf "minimal polynomial for F/K is f = %o\n", f;
logfieldsize := g * Log( p ) / Log( 2 );
printf "\nGenus of F/K is %o\n", g;
printf "logfieldsize = %o\n", logfieldsize;
if logfieldsize le 32 then
    V<s> := PolynomialRing( Integers( ) );
    Z := Numerator( ZetaFunction( F ) );
    o1 := Valuation( Z, p*s^2 - 1 );
    printf "\nNumerator of Z(s) over F_p is z(s) = %o\n", Z;
    printf "Order of root at s=1/2 is %o\n", o1;
else
    printf "\nGenus is too high to compute zeta function. ";
    printf "(log2 p^g ~= %o)\n", logfieldsize;
    o1 := -1;
end if;
return g, o1;
end function;
BIBLIOGRAPHY


