December 2012

The Class Equation of GL2(Fq)

Lindsey Mathewson
University of Wisconsin-Milwaukee

THE CLASS EQUATION OF $GL_2(\mathbb{F}_q)$

by

Lindsey Mathewson

A Thesis Submitted in
Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE
in
MATHEMATICS

at

The University of Wisconsin-Milwaukee
December 2012

ABSTRACT

The Class Equation of $GL_2(\mathbb{F}_q)$

by

Lindsey Mathewson

The University of Wisconsin-Milwaukee, 2012
Under the Supervision of Professor Willenbring

In this thesis, we discuss the conjugacy classes of the general linear group of 2×2 matrices over a prime field. We find the number of conjugacy classes and the class equation for $GL_2(\mathbb{F}_q)$, for general prime q. We then look at some applications of the class equation, which includes finding the number of orbits when $GL_2(\mathbb{F}_q)$ acts on $(GL_2(\mathbb{F}_q))^s$ by conjugation. Included in this thesis is the Maple Code for generating the class equation for any prime.

Table of Contents

List of Figures

ACKNOWLEDGMENTS

First I would like to thank my thesis advisor, Dr. Jeb Willenbring, for introducing me to this problem and for helping me to understand the material needed to prove the results in this thesis. Also, thank you for encouraging me to learn how to use Maple in order to see patterns related to this problem. I would also like to thank my other committee members, Dr. Yi Ming Zou and Dr. Gabriella Pinter, for their input and suggestions.

Thank you to all of the professors who have taught the classes I have taken in college and graduate school. The knowledge I have gained from those classes has been vital in understanding how to think about the problem in this thesis.

Lastly, I would like to thank my friends and family who have always been supportive of me, including my decision to attend graduate school.

Chapter 1

Introduction

In this thesis, we discuss the conjugacy classes of the general linear group of 2×2 matrices over a prime field. This includes looking at the number of conjugacy classes as well as the class equation for this group. We use the relationship between the rational canonical form of a matrix and the matrix conjugates in order to find a formula for the number of conjugacy classes in $GL_2(\mathbb{F}_q)$. This is motivated by a generalized formula for the number of conjugacy classes proved by Feit and Fine in [5] and referenced in [1] and [10].

We again use the rational canonical forms to look at the sizes of the conjugacy classes by finding the class equation for the case when $n = 2$ for any given q prime. I have also included the Maple code for generating this equation.

Lastly, we address some results that rely on the class equation for $GL_2(\mathbb{F}_q)$. This includes finding the number of orbits when $GL_n(\mathbb{F}_q)$ acts on $(GL_n(\mathbb{F}_q))^s$ for some $s \in \mathbb{Z}^+$. This relies on a generalized result for the number of orbits when a finite group acts on a direct product of itself, which can be found in [9]. I also include various plots of data related to the equation for the number of orbits.

Chapter 2

Preliminaries

We will denote the finite field of q elements by $\mathbb{F}_q$ and the general linear group over a finite field by $GL_n(\mathbb{F}_q)$. This is the group of $n \times n$ invertible matrices with entries in $\mathbb{F}_q$. Note that we will only deal with the case where q is prime.

Let G be a group, X be a set. Let $g \in$ and $x \in X$. A map $\phi : G \times X \to X$ (where $\phi(g, x)$ is denoted by $g \cdot x$) is a *group action* of G on X if (*i.*) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for each $g_1, g_2 \in G$, $x \in X$ and (*ii.*) $1 \cdot x = x$ for each $x \in X$ where 1 denotes the identity in G. Define the *orbit* of x to be $Orb(x) = \{g \cdot x : g \in G\}$ and the *stabilizer* of x in G to be $Stab(x) = \{g \in G : g \cdot x = x\}$. Now consider the map $G \times G \to G$ defined by $g \cdot x = gxg^{-1}$ where $g, x \in G$. In this case, G acts on itself and the map is called *conjugation*.

A *conjugacy class* $C(x)$ for some element x in a group G is $C(x) = \{gxg^{-1} : g \in G\}$. It is the collection of all conjugates of x. Note that for $x \in G$, $C(x) = Orb(x)$ when G acts on itself by conjugation. Matrices that are conjugates are called *similar* matrices. In other words, for matrices A, $B \in GL_n(\mathbb{F}_q)$, A is similar to B if there exists a matrix $P \in GL_n(\mathbb{F}_q)$ such that $A = PBP^{-1}$. We write that $A \sim B$. Since this is an equivalence relation, A and B are similar if and only if $C(A) = C(B)$ where $C(A)$ and $C(B)$ are the conjugacy classes of A and B respectively. Note that non-invertible matrices K and L can also be similar if there exists some $Q \in GL_n(\mathbb{F}_q)$ such that $K = QLQ^{-1}$. In this case, $GL_n(\mathbb{F}_q)$ acts on the set of all matrices with entries in $\mathbb{F}_q$, which we will denote $M_n(\mathbb{F}_q)$.

One fact that will be useful in this thesis is the Orbit-Stabilizer Theorem. Suppose G is a group and suppose G acts a set X. For $x \in X$, the theorem says that $|G| = |Orb(x)| \cdot |Stab(x)|$. This will be proved later in this thesis.

The class equation is the order of the group written as the sum of the cardinalities of the conjugacy classes. We can do this because conjugacy classes partition a group. Let G be a finite group and let $Z(G) = \{g \in G : g = xgx^{-1} \text{for all } x \in G\}$. $Z(G)$ is referred to as the *center* of G. For $g \in Z(G)$, g commutes with everything in G, so the stabilizer of g is the whole group. By the Orbit-Stabilizer Theorem, we get that the orbit of x (meaning the conjugacy class containing x) has only one element, namely x. So $|Z(G)|$ is the number of conjugacy classes consisting of one element. So the class equation is

$$|G| = |Z(G)| + \textstyle\sum_{i=1}^{n} |C(x_i)|$$

where $x_1, \ldots, x_n$ are representatives of all n distinct conjugacy classes in G where $|C(x_i)| > 1$ for each $i \in \{1, \ldots, n\}$ [4].

Let F be a field. Let $f(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0 \in F[x]$ be a monic polynomial. The *companion matrix* of f, denoted C_f, is the $k \times k$ matrix with 1 in every entry on the subdiagonal, the additive inverses of the non-leading coefficients on the last column in descending order from $-b_0$ to $-b_{k-1}$, and zero elsewhere. For this particular f, its companion matrix is

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & & 0 & -b_0 \\ 1 & 0 & & & & -b_1 \\ 0 & 1 & 0 & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \\ & & & & 0 & \\ 0 & \cdots & & 0 & 1 & -b_{k-1} \end{pmatrix}$$

Let $a_1, \ldots, a_n$ be monic polynomials in $F[x]$ such that a_i divides a_{i+1} for each $i \in \{1, \ldots, n-1\}$. Let C_{a_i} be the companion matrix for a_i for each $i \in \{1, \ldots, n\}$. A matrix is said to be in *rational canonical form* if it is a matrix with blocks of companion matrices on the diagonal in descending order (as shown below) and zero elsewhere.

$$R = \begin{pmatrix} C_{a_1} & & & \\ & C_{a_2} & & \\ & & \ddots & \\ & & & C_{a_n} \end{pmatrix}$$

Each a_i is referred to as an *invariant factor* of R.

Chapter 3

Motivation and previous results

Over the past 50 years, various results have been proven with regards to the conjugacy classes in the general linear group over a finite field (as well as the orbits when $GL_n(\mathbb{F}_q)$ acts on $M_n(\mathbb{F}_q)$). This has included various formulas for the number of conjugacy classes (or orbits).

In [5], Feit and Fine show that

$$1 + \sum_{n=1}^{\infty} p_n(q)x^n = \prod_{i=1}^{\infty} \frac{1-x^i}{1-qx^i}$$

where $p_n(q)$ is the number of conjugacy classes in $GL_n(\mathbb{F}_q)$. This same formula can be found in [1] and [10].

In [1], Benson, Feit, and Howe use a computer and the above formula to calculate these coefficients to explicitly find the number of conjugacy classes for a variety of values of n. Below is a sample of what is included in [1].

$$p_2(q) = q^2 - 1$$
$$p_{16}(q) = q^{16} - q^7 - q^6 - q^5 + 2q^3 + q^2 - q$$
$$p_{32}(q) = q^{32} - q^{15} - q^{14} - q^{13} - q^{12} - q^{11} - q^{10} + q^9 + 2q^8 + 4q^7 + 3q^6 - 4q^4 - 3q^3 + q^2 + q$$

After observing this data, one of the facts that they discover is that q^n is a good approximation for the number of conjugacy classes in $GL_n(\mathbb{F}_q)$.

In [10], Stong finds a similar formula for the number of orbits where $GL_n(\mathbb{F}_q)$ acts on in the set of $n \times n$ matrices with entries in $\mathbb{F}_q$ by conjugation (as opposed to $GL_n(\mathbb{F}_q)$ acting on itself). This is

$$1 + \sum_{n=1}^{\infty} r_n(q)x^n = \prod_{i=1}^{\infty} \frac{1}{1-qx^i}$$

where $r_n(q)$ is the number of orbits when $GL_n(\mathbb{F}_q)$ acts on $M_n(\mathbb{F}_q)$ by conjugation.

In addition to the formula found by Stong, Carlitz and Hodges find a different formula for the number similar matrices with entries in $\mathbb{F}_q$ in [2]. Note that this is the same as the number of orbits where $GL_n(\mathbb{F}_q)$ acts on in the set of $n \times n$ matrices with entries in $\mathbb{F}_q$ by conjugation. They find that the number of classes of similar $n \times n$ matrices with entries in $\mathbb{F}_q$ is

$$\sum_S q^{k_1+\cdots+k_n}$$

where $S = \{(k_1, \ldots, k_n) \in (\mathbb{Z}^+ \cup \{0\})^n : k_1 + 2k_2 + \cdots + nk_n = n\}$.

In [10], Stong also finds asymptotic results for the number of rational canonical forms in $GL_n(\mathbb{F}_q)$ and $M_n(\mathbb{F}_q)$ as $n \to \infty$. Note that this corresponds to the number of conjugacy classes in $GL_n(\mathbb{F}_q)$ and the number of orbits when $GL_n(\mathbb{F}_q)$ acts on $M_n(\mathbb{F}_q)$ by conjugation. For example, as $n \to \infty$, there are

$$r(q,n) = q^n + \frac{1}{2}\left(\frac{1}{1-q^{\frac{1}{2}}} + \frac{(-1)^n}{1+q^{\frac{1}{2}}}\right)q^{\frac{n}{2}} + \mathcal{O}(q^{\frac{n}{3}})$$

rational canonical forms in $GL_n(\mathbb{F}_q)$. Similarly, he finds the number of $n \times n$ matrices with entries in $\mathbb{F}_q$ that are in rational canonical form as $n \to \infty$.

Note that some of these same topics (rational canonical forms, conjugacy classes, and partitioning the general linear group) are addressed in [7]. Fulman also discusses various combinatorial facts about $GL_n(\mathbb{F}_q)$. This includes finding the number of unipotent matrices in $GL_n(\mathbb{F}_q)$.

Beyond these results, there is extensive literature concerning the general linear group over a finite field, including [6]. Thank you to Dr. Yi Ming Zou for pointing out this particular paper. These groups are examples of finite groups of Lie type [3].

Chapter 4

Counting the conjugacy classes of $GL_2(\mathbb{F}_q)$

Proposition 4.0.1. *The number of conjugacy classes in $GL_n(\mathbb{F}_q)$ is equal to the number of distinct rational canonical forms in $GL_n(\mathbb{F}_q)$.*

Proof. For any $n \times n$ matrix M over a field F, M is similar to a matrix Q in rational canonical form [4]. Additionally, Q is the unique matrix in rational canonical form similar to M [4]. Also, two matrices A and B are similar if and only if they have the same rational canonical form [4]. So, the number of conjugacy classes in $GL_n(\mathbb{F}_q)$ is equal to the number of distinct rational canonical forms in $GL_n(\mathbb{F}_q)$. $\square$

This fact is also mentioned in [7] and [10]. Note that $GL_n(\mathbb{F}_q)$ is finite. In fact, $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1})$ [4]. So $GL_n(\mathbb{F}_q)$ has finitely many conjugacy classes that partition the group.

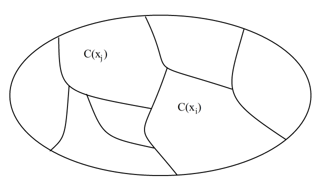

Figure 4.1: Partition of a group by conjugacy classes

List the conjugacy classes as $C(x_1), C(x_2), \ldots, C(x_m)$.

For each conjugacy class $C(x_i)$, there is some $y_i \in GL_n(\mathbb{F}_q)$ that is in rational canonical form.

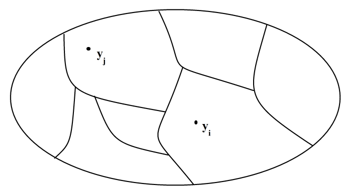

Figure 4.2: Partition of a group by conjugacy classes, each containing a rational canonical form matrix

Proposition 4.0.2. *There are $q^2 - 1$ conjugacy classes in $GL_2(\mathbb{F}_q)$.*

Proof. Consider the possible 2×2 invertible rational canonical forms. There are two possibilities. If $R \in GL_2(\mathbb{F}_q)$ is in rational canonical form, either $R = \lambda I$ for some $\lambda \in \mathbb{F}_q \setminus \{0\}$ where I is the identity matrix or $R = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$ and $a \neq 0$. In the first case, there are $q - 1$ possibilities for R since $\mathbb{F}_q \setminus \{0\}$ has $q - 1$ elements. For the second case, there are $q - 1$ choices for a and q choices for b. So there are $q(q - 1)$ possibilities for R. Adding these two together, we get $(q - 1) + q(q - 1) = q^2 - 1$ conjugacy classes in $GL_2(\mathbb{F}_q)$. $\square$

Note that this is consistent with the results in [5] and [1].

Example 4.0.3. Consider $GL_2(\mathbb{F}_2)$. $|GL_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 6$.

$$\begin{aligned} GL_2(\mathbb{F}_2) &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \\ &= \{x_1, x_2, x_3, x_4, x_5, x_6\} \end{aligned}$$

Note that $x_1^{-1} = x_1$, $x_2^{-1} = x_2$, $x_3^{-1} = x_6$, $x_4^{-1} = x_4$, $x_5^{-1} = x_5$, and $x_6^{-1} = x_3$. Also, by computing conjugates and using the fact that conjugacy classes partition a group, it can be shown that there are three conjugacy classes: $C(x_1) = \{x_1\}$, $C(x_2) = C(x_4) = C(x_5) = \{x_2, x_4, x_5\}$, and $C(x_3) = C(x_6) = \{x_3, x_6\}$.

It remains to determine which of the six elements are in rational canonical form.

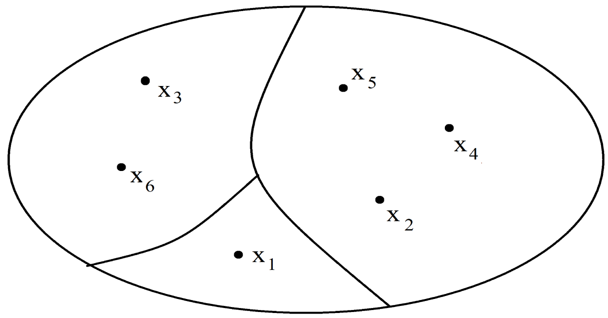

Figure 4.3: Partition of $GL_2(\mathbb{F}_2)$ by conjugacy classes

$$x_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} C_{p_1} & 0 \\ 0 & C_{p_2} \end{pmatrix} \text{ where } p_1(x) = p_2(x) = x - 1 \in \mathbb{F}_2[x].$$

$$x_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = C_q \text{ where } q(x) = x^2 - 1 \in \mathbb{F}_2[x].$$

x_3 is not in rational canonical form. If it was, it either *(i)* is a companion matrix or *(ii)* consists of two companion matrix blocks on the diagonal and zero elsewhere. x_3 is neither of these types of matrices. Similarly, neither x_4 nor x_5 are in rational canonical form.

$$x_6 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = C_r \text{ where } r(x) = x^2 - x - 1 \in \mathbb{F}_2[x].$$

So there are three matrices in $GL_2(\mathbb{F}_2)$ that are in rational canonical form. Additionally, these matrices are in distinct conjugacy classes. So the number of rational canonical form matrices is equal to the number of conjugacy classes in $GL_2(\mathbb{F}_2)$.

Chapter 5

The class equation for $GL_2(\mathbb{F}_q)$

To prove the class equation for when $n = 2$, we first prove a lemma.

Lemma 5.0.4. *For any odd prime q, half of the nonzero elements in $\mathbb{F}_q$ are perfect squares.*

Proof. Consider q odd prime. Note that for any $x \in \mathbb{F}_q$, $x^2 \equiv (q-x)^2 \mod q$. This is because $(q-x)^2 = (q^2 - 2xq + x^2) \equiv x^2 \mod q$.

Let $\phi : \mathbb{F}_q \setminus \{0\} \to \mathbb{F}_q \setminus \{0\}$ be given by $\phi(x) = x^2$. Then each element in imϕ has at least two elements that map to it. So there exist at most $\frac{q-1}{2}$ elements in imϕ. It remains to show that each element in imϕ has exactly two elements that map to it. This will prove that $|\text{im}\phi| = \frac{q-1}{2}$ and that half of all nonzero elements in $\mathbb{F}_q$ are perfect squares.

Seeking contradiction, suppose there exist $x, y \in \mathbb{F}_q \setminus \{0\}$ such that $x, y \leq \frac{q-1}{2}$, $x \neq y$, and $\phi(x) = \phi(y) \mod q$. Note that we can assume both x and y are less than $\frac{q-1}{2}$ because each element that is greater than $\frac{q-1}{2}$ has a corresponding element that is less than or equal to $\frac{q-1}{2}$ which maps to the same element under ϕ.

Without loss of generality, assume that $y < x$. Then $x^2 - y^2 \equiv 0(\mod q)$ since $\phi(x) = \phi(y)$. So $(x+y)(x-y) \equiv 0(\mod q)$. Since $\mathbb{F}_q$ is a field, it contains no zero-divisors. This implies that either $(x+y)$ or $(x-y)$ is equal to zero. Now $x - y \neq 0$ since $x, y \leq \frac{q-1}{2}$ and $x \neq y$. So $x + y \equiv 0(\mod q)$. This is a contradiction because it means either x or y is greater than $\frac{q-1}{2}$. So no such x and y exist.

So for each $y \in \text{im}\phi$, there exist exactly two elements, call them x and $q-x$, such that $\phi(x) = \phi(q-x) = y$. Therefore, for any odd prime q, half of all nonzero elements are perfect squares. $\square$

Note that finding which of these $\frac{q-1}{2}$ elements in $\mathbb{F}_q$ are prefect squares is a part of the theory of quadratic reciprocity.

We need one more fact before proceeding with the proof of the class equation in the case when $n = 2$. That is the Orbit-Stabilizer Theorem.

Lemma 5.0.5. ***Orbit-Stabilizer Theorem***
Let G be a group and $x \in G$. Suppose G acts on itself and let $Orb(x)$ be the orbit of x and $Stab(x)$ the stabilizer of x. Then $|G| = |Orb(x)| \cdot |Stab(x)|$.

Proof. Note that G acts on $Orb(x)$, $Orb(x) = \{g \cdot x : g \in G\}$, and $Stab(x) = \{g \in G : g \cdot x = x\}$. Let $S = Stab(x)$, $O = Orb(x)$ and let $\phi : G/S \to O$ be given by $gS \mapsto g \cdot x$ for $g \in G$. We must show that ϕ is a well-defined bijection.

Let $g_1S, g_2S \in G/S$. Suppose $\phi(g_1S) = \phi(g_2S)$. Then $g_1 \cdot x = g_2 \cdot x$, implying that $(g_2^{-1}g_1) \cdot x = x$ and that $g_2^{-1}g_1 \in S$. By law of cosets, $g_1S = g_2S$, so ϕ is injective.

Now let $y \in Orb(x)$. Then $y = z \cdot x$ for some $z \in G$. So $\phi(zS) = z \cdot x = y$, meaning ϕ is surjective.

Lastly it remains to show that ϕ is well-defined. Let $g_1, g_2 \in G$. Suppose $g_1S = g_2S$. Then $g_2^{-1}g_1 \in S$. So $(g_2^{-1}g_1) \cdot x = x$, implying that $g_1 \cdot x = g_2 \cdot x$. So ϕ is well-defined.

So we get that ϕ is a bijective map, giving us that $\frac{|G|}{|S|} = |G/S| = |O|$. $\square$

Lastly note that when the group action is conjugation, the orbit of g is the conjugacy class of g and the stabilizer of g is the centralizer of g where g is a group element.

Theorem 5.0.6. *The class equation for $GL_2(\mathbb{F}_q)$ is*

$$\begin{aligned}(q^2-1)(q^2-q) &= |GL_2(\mathbb{F}_q)| \\ &= [1][q-1] \\ &+ [q^2-q][\frac{1}{2}(q^2-q)] \\ &+ [q^2-1][q-1] \\ &+ [q^2+q][\frac{1}{2}(q-1)(q-2)]\end{aligned}$$

where each term in the sum is a product of the size of a conjugacy class and the number of conjugacy classes of that particular size.

This can be listed in table form as well, as found in [8].

Size of Conjugacy Class	Number of Conjugacy Classes
1	$q-1$
q^2-q	$\frac{1}{2}(q^2-q)$
q^2-1	$q-1$
q^2+q	$\frac{1}{2}(q-1)(q-2)$

Proof. Let q be an odd prime. Recall that each conjugacy class can be represented by a unique rational canonical form matrix. In the case where $G = GL_2(\mathbb{F}_q)$, all of the rational canonical forms in G are of the form

$$\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix} \text{ or } \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

where $a, b, c \in \mathbb{F}_q$ and $a, c \neq 0$.

In the second case, there are $q-1$ such matrices in $GL_2(\mathbb{F}_q)$ and they are all constant multiples of the identity matrix. So each of these is the only element in its conjugacy class. I will refer to these rational canonical forms as "Type 1" rational canonical forms. (Later I will give similar names to the different subcases of rational canonical forms in case one).

For the first case, we will find the order of the centralizer of $M = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$, whose elements are the matrices that commute with M. We will use this and the Orbit-Stabilizer Theorem to find the size of the conjugacy class of a given rational canincal form and the number of rational canonical forms that have conjugacy classes of that size.

For a matrix $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in GL_2(\mathbb{F}_q)$,

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix} = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

if and only if

$$\begin{pmatrix} y & xa+yb \\ w & za+wb \end{pmatrix} = \begin{pmatrix} az & aw \\ x+bz & y+bw \end{pmatrix}.$$

Note that $az = y$, so $z = a^{-1}y$. Also, $w = a^{-1}(xa+yb) = x+ba^{-1}y$ by commutativity of $\mathbb{F}_q$. So any matrix that commutes with M looks like $\begin{pmatrix} x & y \\ a^{-1}y & x+ba^{-1}y \end{pmatrix}$. Note that since this matrix is in $GL_2(\mathbb{F}_q)$, its determinant is nonzero. This gives us the following equation:

$$x^2 + ba^{-1}y - a^{-1}y^2 \neq 0$$

In other words,

$$ax^2 + byx - y^2 \neq 0$$

Now consider when $ax^2 + byx - y^2 = 0$. When this is true, we must eliminate possible values of x and y. Using the quadratic formula, we obtain

$$\begin{aligned} x &= \tfrac{-by \pm \sqrt{b^2y^2+4ay^2}}{2a} \\ &= \tfrac{-by \pm y\sqrt{b^2+4a}}{2a} \end{aligned}$$

If $b^2 + 4a$ is a perfect square, then $ax^2 + byx - y^2 = 0$ has a solution, so we must eliminate that combination of x and y, meaning that that particular matrix is not in the centralizer of M.

By the previous lemma, for any odd prime q, half of all non-zero elements in $\mathbb{F}_q$ are perfect squares. So for any fixed b, half of all nonzero values for a will make $b^2 + 4a$ a perfect square. This is because q is prime, so $4a$ generates $\mathbb{F}_q$, meaning that for $a_1, a_2 \in \mathbb{F}_q$ such that $a_1 \neq a_2$, $4a_1 \neq 4a_2$. So with b fixed, we have $\frac{q-1}{2}$ values of a that give solutions to $ax^2 + byx - y^2 = 0$.

Now there are three cases to consider when our rational canonical form is of the form $M = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ when $a, b \in \mathbb{F}_q$ and $a \neq 0$.

$$\text{(i) } b^2 + 4a \text{ is not a perfect square in } \mathbb{F}_q$$
$$\text{(ii) } b^2 + 4a = 0 \text{ in } \mathbb{F}_q$$
$$\text{(iii) } b^2 + 4a \text{ is a nonzero perfect square in } \mathbb{F}_q$$

I will refer to these as "Type 2," "Type 3," and "Type 4" rational canonical forms, respectively.

Consider case (i). Recall that we are considering matrices that look like

$$\begin{pmatrix} x & y \\ a^{-1}y & x + ba^{-1}y \end{pmatrix}.$$

Since $ax^2 + byx - y^2 = 0$ has no solutions for any $x, y \in \mathbb{F}_q$ when x and y are nonzero, there are $q^2 - 1$ such matrices. This quantity is obtained by q choices for each x and y and subtracting from that the one case where both are equal to zero. So there are $q^2 - 1$ elements in the centralizer of M. Since the centralizer is the stabilizer under conjugation, by the Orbit-Stabilizer Theorem, we get that there are

$$\frac{|GL_2(\mathbb{F}_q)|}{q^2-1} = \frac{(q^2-q)(q^2-1)}{q^2-1} = q^2 - q$$

elements in the conjugacy class of M if $b^2 + 4a$ is not a perfect square.

Also, since case (i) occurs half of the time with matrices of the form $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$ and $a \neq 0$, there are $\frac{1}{2}(q-1)q = \frac{1}{2}(q^2 - q)$ such conjugacy classes. This is the second component of the sum in the class equation.

Now consider case (ii). From $b^2 + 4a = 0$ and the quadratic equation we get that

$$x = \frac{-yb}{2a}$$

are the solutions for $ax^2 + byx - y^2 = 0$. So y completely determines x. There are q choices for y, so we must remove q pairs (x, y). This gives us $q^2 - q$ such matrices that commute with $M = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$. So the order of the conjugacy class of M in this case is

$$\frac{|GL_2(\mathbb{F}_q)|}{q^2-q} = \frac{(q^2-q)(q^2-1)}{q^2-q} = q^2 - 1$$

Now we must count the number of conjugacy classes of this size. It suffices to count the number of matrices in $GL_2(\mathbb{F}_q)$ that are of the form $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a \neq 0$ and $b^2 + 4a = 0$.

If $b = 0$, then $b^2 + 4a \neq 0$ since $a \neq 0$ implies that $4a \neq 0$ since q is prime. However, for any nonzero b, b^2 has an additive inverse that is nonzero and therefore there are $q-1$ choices for b. $a = (-4)^{-1}b^2$ is determined by b. So there are exactly $q-1$ such rational canonical forms in $GL_2(\mathbb{F}_q)$. This is the third part in the sum of the class equation.

Lastly, consider case (iii), when $b^2 + 4a = g^2$ for some $g \in \mathbb{F}_q$, $g \neq 0$. Then

$$x = \tfrac{y(-b \pm g)}{2a}$$

is when $ax^2 + byx - y^2 = 0$ has a solution. If $y = 0$, we have $x = y = 0$ and must eliminate one case. If $y \neq 0$, there are $q-1$ choices for y and two choices for $\pm g$ (g is fixed). So we have $2(q-1)$ more cases to remove. This gives a total of $2q-1$ cases, making the size of the centralizer of M $q^2 - (2q-1) = q^2 - 2q + 1 = (q-1)^2$. So by the Orbit-Stabilizer Theorem, the size of the conjugacy class in this case will be

$$\tfrac{|GL_2(\mathbb{F}_q)|}{(q-1)^2} = \tfrac{(q^2-q)(q^2-1)}{(q-1)^2} = \tfrac{q(q-1)(q-1)(q+1)}{(q-1)^2} = q(q+1) = q^2 + q$$

It remains to count the number of conjugacy classes of order $q^2 + q$. Note that for $GL_2(\mathbb{F}_q)$, there are $q^2 - 1$ conjugacy classes. This is the last case, so we can just sum up the other quantities of conjugacy classes and subtract them from $q^2 - 1$. This is because we know there can only be four different sizes of conjugacy classes by exhausting all cases for $b^2 + 4a$. The number of conjugacy classes of order $q^2 + q$ is

$$\begin{aligned} &(q^2-1) - [(q-1) + \tfrac{1}{2}(q^2-q) + (q-1)] \\ &= \tfrac{1}{2}q^2 - \tfrac{3}{2}q + 1 = \tfrac{1}{2}(q^2 - 3q + 2) \\ &= \tfrac{1}{2}(q-1)(q-2) \end{aligned}$$

This accounts for the fourth and final component in the summation of the class equation.

So far, we have proved the class equation for $GL_2(\mathbb{F}_q)$ where q is an odd prime. It lastly remains to show that this equation holds when $q = 2$. Evaluating at $q = 2$, we obtain

$$|GL_2(\mathbb{F}_2)| = 1 + 2(1) + 3(1) + 6(0) = 1 + 2 + 3$$

This is in fact the class equation for $GL_2(\mathbb{F}_2)$ $\square$

Chapter 6

Applications of the class equation

With this result and the orbit stabilizer theorem, we now know how many conjugates and commuting matrices a given matrix in $GL_2(\mathbb{F}_q)$ has by simply calculating its rational canonical form.

Corollary 6.0.7. *Let $M \in GL_2(\mathbb{F}_q)$ and let R be the rational canonical form of M.*
(i) If $R = cI$ for some $c \in \mathbb{F}_q \setminus \{0\}$ then M is its only conjugate and M commutes with every matrix in $GL_2(\mathbb{F}_q)$.
(ii) If $R = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$, $a \neq 0$, and $b^2 + 4a$ is not a perfect square in $\mathbb{F}_q$, then M has $q^2 - q$ conjugates and commutes with $q^2 - 1$ elements in $GL_2(\mathbb{F}_q)$.
(iii) If $R = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$, $a \neq 0$, and $b^2 + 4a = 0$ in $\mathbb{F}_q$, then M has $q^2 - 1$ conjugates and commutes with $q^2 - q$ elements in $GL_2(\mathbb{F}_q)$.
(iv) If $R = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$, $a \neq 0$, and $b^2 + 4a$ is a nonzero perfect square in $\mathbb{F}_q$, then M has $q^2 + q$ conjugates and commutes with $(q-1)^2$ elements in $GL_2(\mathbb{F}_q)$.

Remark 6.0.8. Using the class equation for $GL_2(\mathbb{F}_q)$, we can find what number of conjugates and commuting matrices an element of $GL_2(\mathbb{F}_q)$ is most likely to have.

We can also consider what distribution of matrices $GL_2(\mathbb{F}_q)$ has when q is large by taking the limit as $q \to \infty$. We can figure out what percentage of the matrices has a given type of rational canonical form.

Corollary 6.0.9. *As $q \to \infty$, the probability that a matrix has rational canonical form of the form $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$, $a \neq 0$, and $b^2 + 4a$ is a nonzero perfect square in $\mathbb{F}_q$ is $\frac{1}{2}$. Similarly, as $q \to \infty$, the probability that a matrix has rational canonical form of the form $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ where $a, b \in \mathbb{F}_q$, $a \neq 0$, and $b^2 + 4a$ is not a perfect square in $\mathbb{F}_q$ is $\frac{1}{2}$.*

Proof. For each component in the sum of the class equation, we take the limit of that number of matrices over the size of the group as q approaches infinity as shown below.

$\lim_{q\to\infty} \frac{(1)(q-1)}{(q^2-1)(q^2-q)} = 0$

$\lim_{q\to\infty} \frac{(q^2-q)(\frac{1}{2}(q^2-q))}{(q^2-1)(q^2-q)} = \frac{1}{2}$

$\lim_{q\to\infty} \frac{(q^2-1)(q-1)}{(q^2-1)(q^2-q)} = 0$

$\lim_{q\to\infty} \frac{(q^2+q)(\frac{1}{2}(q-1)(q-2))}{(q^2-1)(q^2-q)} = \frac{1}{2}$

□

Additionally, we can use the class equation for $GL_2(\mathbb{F}_q)$ to find the number of orbits of $G^s = G \times \cdots \times G$ (s times) for $s > 0$ where $G = GL_2(\mathbb{F}_q)$ where G acts on G^s by conjugation of each component.

Corollary 6.0.10. *Let $G = GL_2(\mathbb{F}_q)$. The number of orbits of G^s where G acts on G^s by conjugation is*

$$(q^2-1)^{s-1}(q^2-q)^{s-1}[(q-1) + \tfrac{1}{2(q^2-q)^{s-2}} + \tfrac{q-1}{(q^2-1)^{s-1}} + \tfrac{(q-1)(q-2)}{2(q^2+q)^{s-1}}]$$

Proof. For a finite group H, let $\hat{H}$ be the set of conjugacy classes. For $C \in \hat{H}$, let z_C be the size of the centralizer of some $h \in C$. Note that we can do this because the Orbit-Stabilizer Theorem gives us that for any two elements in the same conjugacy class, their centralizers will be the same size. So $|C| = \frac{|H|}{z_C}$ by the Orbit-Stabilizer Theorem. Also, $|H^s/H| = \sum_{C\in\hat{H}} z_C^{s-1}$ where $|H^s/H|$ is the number of orbits where H acts on H^s by conjugation of each component [9].

Let $G = GL_2(\mathbb{F}_q)$. We wish to apply this to the class equation for G to find the number of orbits of G^s where G acts on G^s by conjugation. Note that $z_C^{s-1} = (\frac{|G|}{|C|})^{s-1}$.

So $|G^s/G| = \sum_{C\in\hat{G}}(\frac{|G|}{|C|})^{s-1}$. By applying the class equation for $GL_2(\mathbb{F}_q)$, we get that this is equal to

$$(\tfrac{|G|}{1})^{s-1}(q-1) + (\tfrac{|G|}{q^2-q})^{s-1}(\tfrac{1}{2}(q^2-q)) + (\tfrac{|G|}{q^2-1})^{s-1}(q-1) + (\tfrac{|G|}{q^2+q})^{s-1}(\tfrac{1}{2}(q-1)(q-2))$$
$$= |G|^{s-1}[(q-1) + \tfrac{\frac{1}{2}(q^2-q)}{(q^2-q)^{r-2}} + \tfrac{q-1}{(q^2-1)^{s-1}} + \tfrac{\frac{1}{2}(q-1)(q-2)}{(q^2+q)^{s-1}}]$$

Since $G = GL_2(\mathbb{F}_q)$, this equals

$$[(q^2-q)(q^2-1)]^{s-1}[(q-1) + \tfrac{\frac{1}{2}(q^2-q)}{(q^2-q)^{s-1}} + \tfrac{q-1}{(q^2-1)^{s-1}} + \tfrac{\frac{1}{2}(q-1)(q-2)}{(q^2+q)^{s-1}}]$$
$$= (q^2-q)^{s-1}(q^2-1)^{s-1}[(q-1) + \tfrac{1}{2(q^2-q)^{s-2}} + \tfrac{q-1}{(q^2-1)^{s-1}} + \tfrac{(q-1)(q-2)}{2(q^2+q)^{s-1}}]$$

This is the number of orbits of $G^s = G \times \cdots \times G$ (s times) where G acts on G^s by conjugation. In other words, this is the number of conjugacy classes. □

Next we give some plots of data obtained from this equation. First we fix q and plot various values of s and the number of orbits for that particular s. Next we fix s and plot data from a sample of values of q and the number of orbits for that particular q.

In the following plots, $f_q(s)$ denotes the number of orbits with q fixed. This means that

$$f_q(s) = (q^2-1)^{s-1}(q^2-q)^{s-1}[(q-1) + \tfrac{1}{2(q^2-q)^{s-2}} + \tfrac{q-1}{(q^2-1)^{s-1}} + \tfrac{(q-1)(q-2)}{2(q^2+q)^{s-1}}]$$

where q is a constant. Similarly, $f_s(q)$ denotes the number of orbits with s fixed. This means that

$$f_s(q) = (q^2-1)^{s-1}(q^2-q)^{s-1}[(q-1) + \tfrac{1}{2(q^2-q)^{s-2}} + \tfrac{q-1}{(q^2-1)^{s-1}} + \tfrac{(q-1)(q-2)}{2(q^2+q)^{s-1}}]$$

where s is a constant. The following are graphs of $f_q(s)$. Following that is a graph of plots for all fixed primes q between 2 and 101. Next are graphs of $f_s(q)$ and one for all fixed $s \in \{1, \ldots, 40\}$. Lastly, we create the surface for this two-variable equation and include some images of the surface when $s \in \{1, \ldots, 40\}$ and q is prime between 2 and 101.

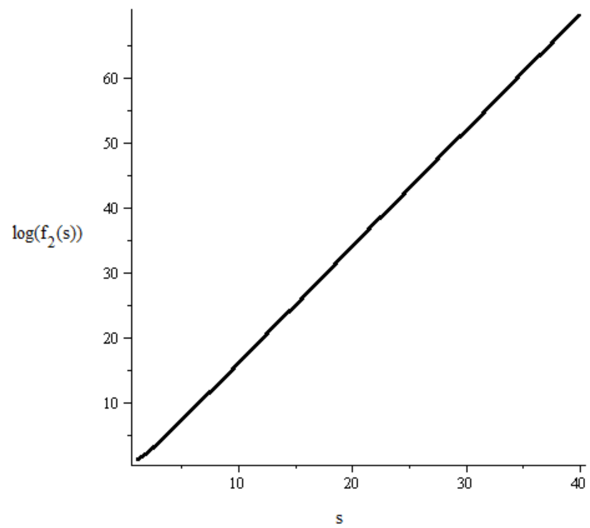

Figure 6.1: Plot for the number of orbits where $q = 2$ and s ranges from 1 to 40

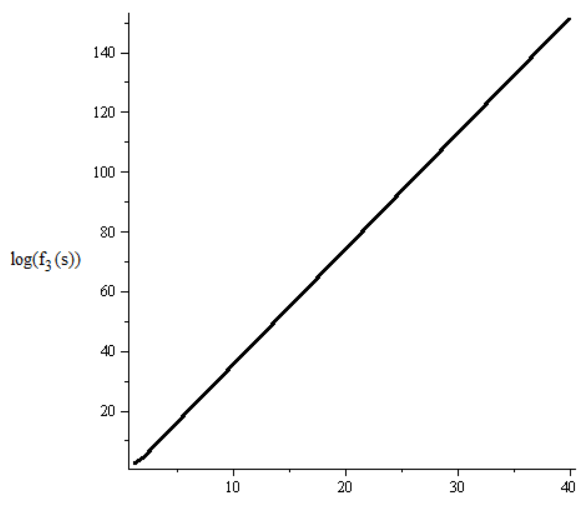

Figure 6.2: Plot for the number of orbits where $q = 3$ and s ranges from 1 to 40

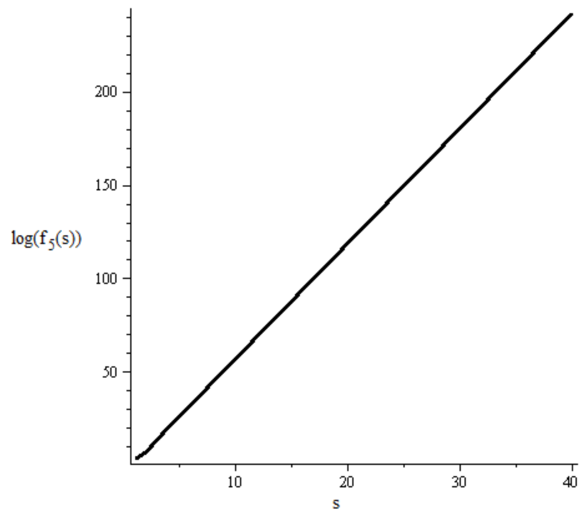

Figure 6.3: Plot for the number of orbits where $q = 5$ and s ranges from 1 to 40

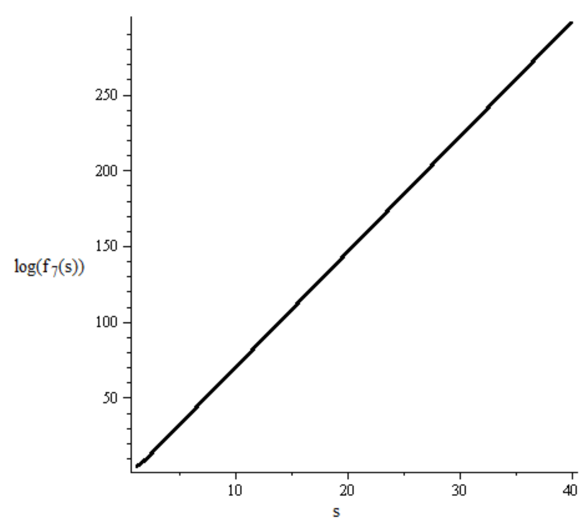

Figure 6.4: Plot for the number of orbits where $q = 7$ and s ranges from 1 to 40

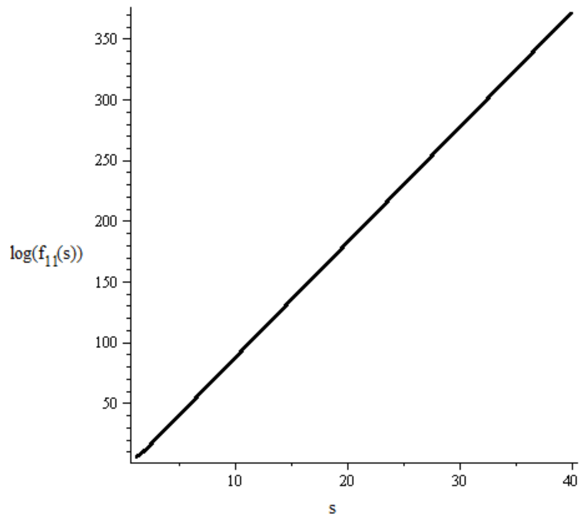

Figure 6.5: Plot for the number of orbits where $q = 11$ and s ranges from 1 to 40

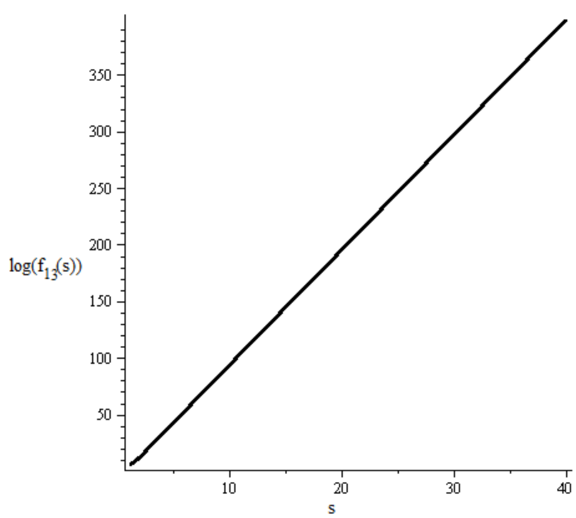

Figure 6.6: Plot for the number of orbits where $q = 13$ and s ranges from 1 to 40

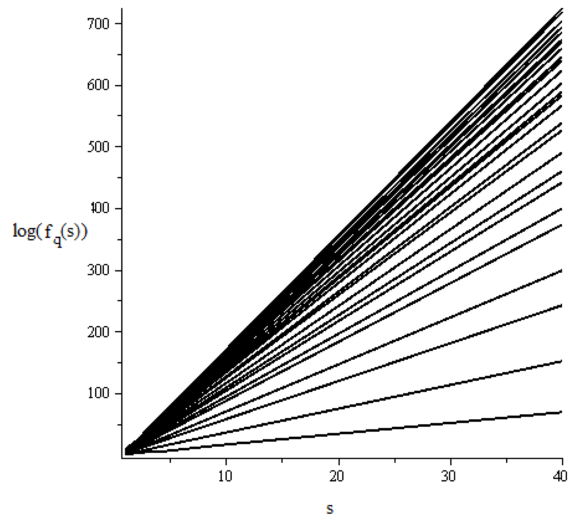

Figure 6.7: Various plots for the number of orbits with fixed q prime between 2 and 101 with s ranging from 1 to 40

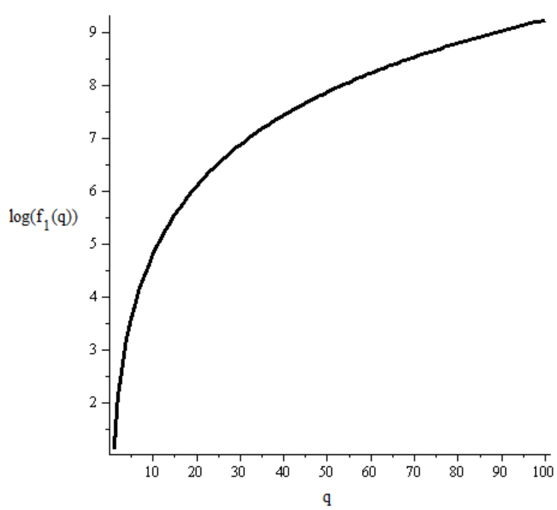

Figure 6.8: Plot for the number of orbits where $s = 1$ and q ranges over all primes strictly between 1 and 100

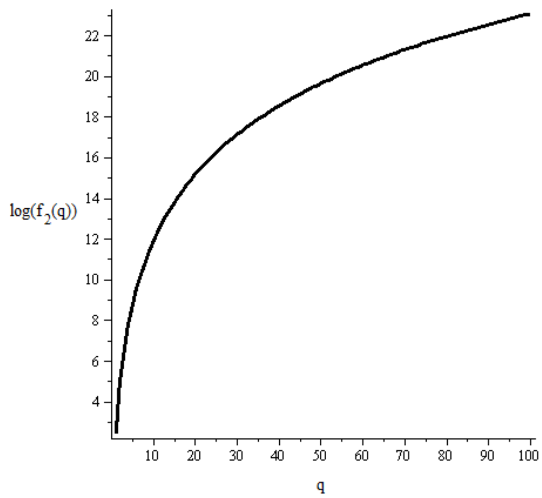

Figure 6.9: Plot for the number of orbits where $s = 2$ and q ranges over all primes strictly between 1 and 100

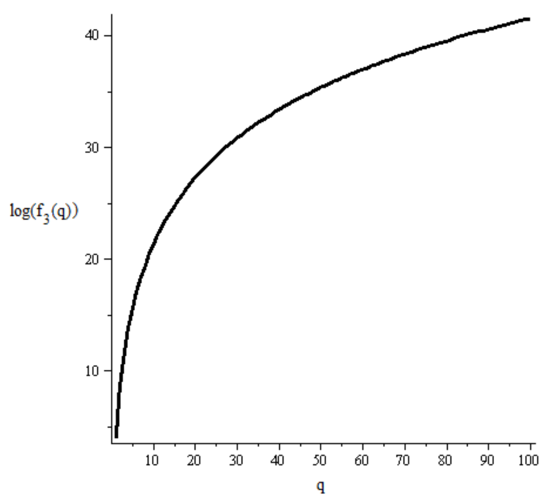

Figure 6.10: Plot for the number of orbits where $s = 3$ and q ranges over all primes strictly between 1 and 100

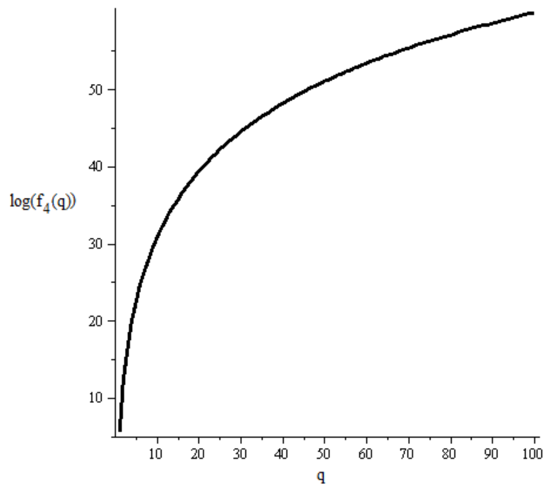

Figure 6.11: Plot for the number of orbits where $s = 4$ and q ranges over all primes strictly between 1 and 100

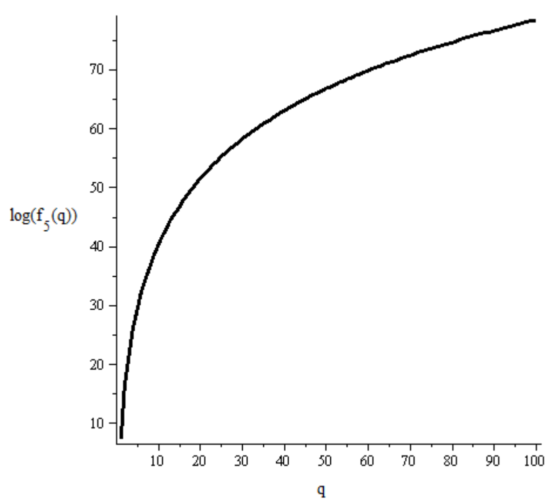

Figure 6.12: Plot for the number of orbits where $s = 5$ and q ranges over all primes strictly between 1 and 100

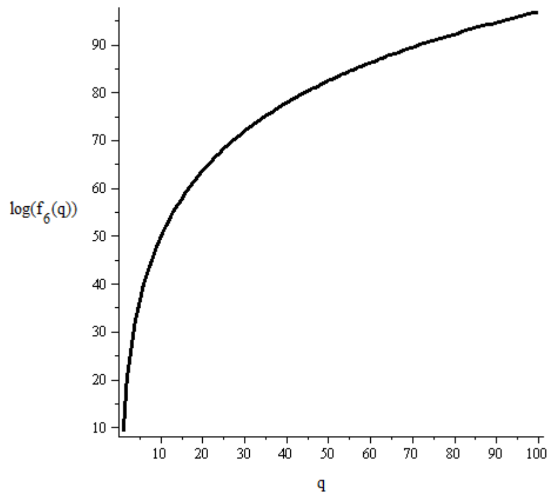

Figure 6.13: Plot for the number of orbits where $s = 6$ and q ranges over all primes strictly between 1 and 100

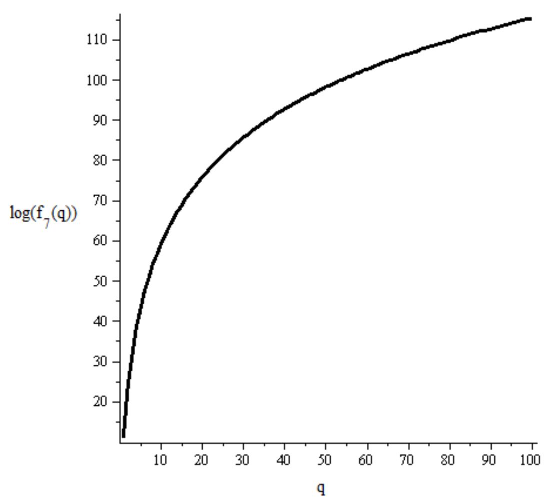

Figure 6.14: Plot for the number of orbits where $s = 7$ and q ranges over all primes strictly between 1 and 100

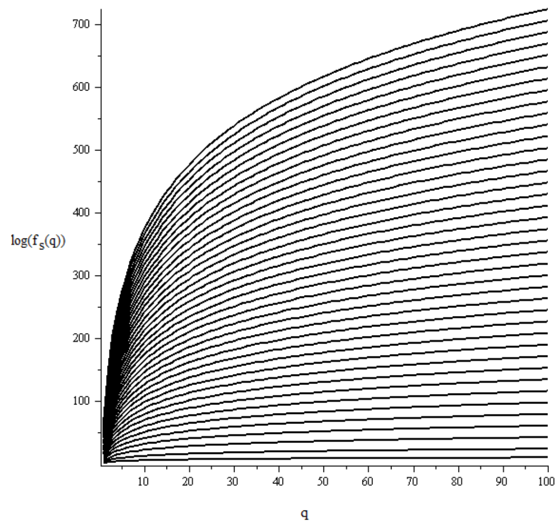

Figure 6.15: Various plots for the number of orbits with fixed $s \in \{1, \ldots, 40\}$ where q is prime between 2 and 101

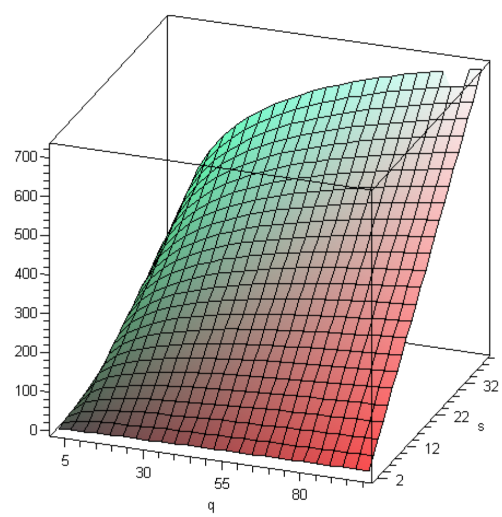

Figure 6.16: Surface where the variables are s and q and the z axis corresponds to the number of orbits in $(GL_2(\mathbb{F}_q))^s$

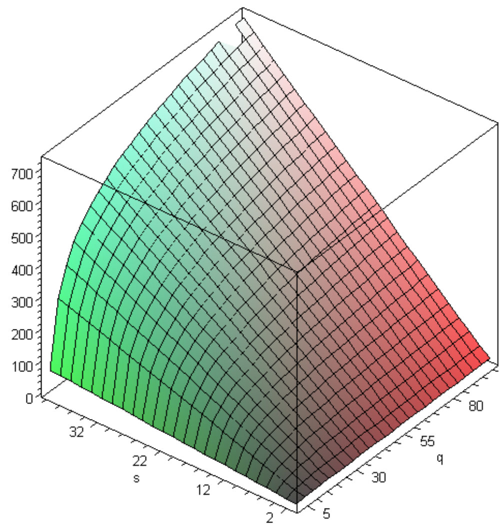

Figure 6.17: Surface where the variables are s and q and the z axis corresponds to the number of orbits in $(GL_2(\mathbb{F}_q))^s$

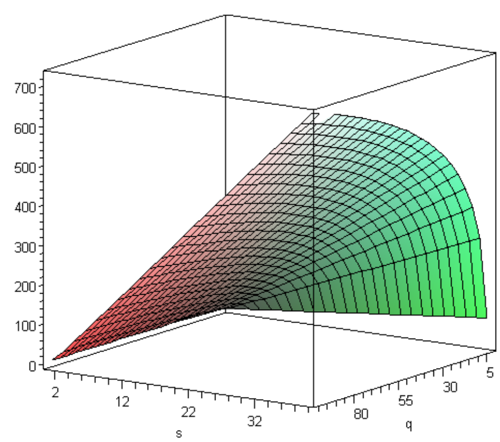

Figure 6.18: Surface where the variables are s and q and the z-axis corresponds to the number of orbits in $(GL_2(\mathbb{F}_q))^s$

Chapter 7

Maple code for generating the class equation

The following is the Maple code used to generate the class equation for an input prime q by generating all rational canonical forms of the group and using these to create the conjugacy classes. The sample below shows the code for $q = 5$, but that is the only line that needs to be altered in order to generate the class equation for any prime. Note that descriptions follow each section of the program.

```
> with(LinearAlgebra):
> with(LinearAlgebra[Modular]):
> q := 5:
> n := 2:
L := NULL:
for a from 0 to q-1 do
for b from 0 to q-1 do
L := L, Matrix(n,1,[[a],[b]])
od od:
L := [L]:
```

This creates a list of all two-dimensional vectors with entries in $\mathbb{F}_q$.

```
> S := NULL:
for a from 1 to nops(L) do
for b from 1 to nops(L) do
M := <L[a] | L[b]>:
S := S,M:
od od:
S := [S];
```

Next the Maple worksheet creates a list of all 2×2 matrices with entries in $\mathbb{F}_q$.

```
> nops(S):
G := NULL:
for i from 1 to nops(S) do
M := S[i]:
d := LinearAlgebra[Determinant](M) mod q:
if d=0 then G :=G else G := G,M end if:
end do:
G := [G];
GroupSize := nops(G);
```

Here we run a loop for testing each matrix in the list S and add it to list G if it has a nonzero determinant in $\mathbb{F}_q$. This means that $G = GL_2(\mathbb{F}_q)$.

```
> R := NULL:
for i from 1 to q-1 do
for j from 0 to q-1 do
M := Matrix(2,2,[[0,i],[1,j]]):
R := R,M:
od od:
for i from 1 to q-1 do
```

```
M := Matrix(2,2,[i,0],[0,i]):
R := R,M:
od:
R := [R];
NumberOfConjugacyClasses := nops(R);
```

This generates all rational canonical forms in $GL_2(\mathbb{F}_q)$ and gives as an output, the number of conjugacy classes.

```
> P2 := NULL:
for i from 1 to nops(R) do
C := NULL:
P2 := P2,C:
od:
P2 :=[P2]:
```

Now Maple makes a list of singleton sets, each containing exactly one unique rational canonical form.

```
> P := NULL:
for j from 1 to nops(R) do
M := R[j]:
C := P2[j]:
for i from 1 to nops(G) do
N := G[i]:
K := MatrixInverse(N):
K := Mod(q,K,integer[]):
g := N.M.K:
g := Mod(q,g,integer[]):
k :=1:
```

```
while k < nops(C) + 1 do
if Equal(g,C[k]) then k := nops(C) +2
else k := k+1
fi:
od:
if k = nops(C) + 1 then C := [op(C),g]
fi:
od:
P := P,C:
od:
P :=[P]:
for i from 1 to nops(P) do
ConjClass := P[i];
od;
ClassEquation := map(nops,P):
ClassEquation := sort(ClassEquation);
GrpSz := 0:
for i from 1 to nops(P) do
GrpSz := GrpSz + nops(P[i]):
od:
ClassEquationSum := GrpSz;
```

In this last step, we calculate the inverse of each matrix in G by converting its entries to elements in $\mathbb{F}_q$ with each step. Then we use this to calculate all conjugates of each rational canonical form matrix and add these to a list, this generating the conjugacy class. A loop is used to guarantee that repeats are not added to lists. This portion of the program then gives as an output, a vector of the sizes of conjugacy classes. This can be interpreted as the class equation.

Example 7.0.11. If we set $q := 5$ in the above code, we can get the following output.

$$ClassEquation :=$$
$$[1, 1, 1, 1, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 24, 24, 24, 24, 30, 30, 30, 30, 30, 30]$$
$$ClassEquationSum := 480$$

Note that there are 24 entries in this vector, corresponding to the 24 conjugacy classes in $GL_2(\mathbb{F}_5)$. Each entry in the vector represents the size of a conjugacy class. Also note that the Maple worksheet outputs the size of $GL_2(\mathbb{F}_5)$, which is $(5^2 - 1)(5^2 - 5) = (24)(20) = 480$.

Example 7.0.12. Similarly, set $q := 7$. The worksheet outputs

$$ClassEquation :=$$
$$[1, 1, 1, 1, 1, 1, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42, 42,$$
$$48, 48, 48, 48, 48, 48, 56, 56, 56, 56, 56, 56, 56, 56, 56, 56, 56, 56, 56, 56, 56]$$
$$ClassEquationSum := 2016$$

This vector represents the class equation for $GL_2(\mathbb{F}_7)$.

Bibliography

[1] Benson, D., Feit, W., & Howe, R. (1989). Finite linear groups, the Commodore 64, Euler and Sylvester. *American Mathematics Monthly*, *93*(9), 717-719.

[2] Carlitz, L. & Hodges, J. (1956). Distributions of matrices in a finite field. *Pacific Journal of Mathematics*, *6*(2), 225-230.

[3] Carter, R. W. (1993). *Finite groups of Lie type.* Chichester: John Wiley and Sons, Inc.

[4] Dummit, D. S. & Foote, R. M. (2004) *Abstract algebra.* (3rd ed.). John Wiley and Sons, Inc.

[5] Feit, W. & Fine, N. J. (1960). Pairs of commuting matrices over a finite field. *Duke Mathematics Journal*, *27*(1), 91-94.

[6] Flannery, D. L. & O'Brien, E. A. (2005). Linear groups of small degree over finite fields. *International Journal of Algebra and Computation*, *15*(3), 467-502.

[7] Fulman, J. (1997). Probability in the classical groups over finite fields: symmetric functions, stochastic algorithms, and cycle indices. *Harvard University.*

[8] Fulton, W. & Harris, J. (1996). *Representation theory.* (3rd ed.). Springer-Verlag New York Inc.

[9] Hero, M. W. & Willenbring, J. F. (2009). Stable Hilbert series as related to measurement of quantum entanglement. *Discrete Mathematics*, *309*(23-24), 6508-6514.

[10] Stong, R. (1988). Some asymptotic results on finite vector spaces. *Advances in Applied Mathematics*, *9*(2), 167-199.