Utrecht
University

Faculty of Science

The Markov Equation over Finite Fields and its Applications

Master's Thesis

Ludo Dekker

Mathematical Sciences

Supervisor:

Prof. Dr. Gunther Cornelissen

Second Reader:

Dr. Valentijn Karemaker

June 2023

Acknowledgements

First of all, I would like to thank Gunther Cornelissen for being my supervisor, for suggesting this topic and for all meetings and advice during this project. These meetings were often very useful, but I also enjoyed them and I always left feeling more confident about this thesis. I would also like to thank Valentijn Karemaker for being the second reader of this thesis and providing valuable feedback. Moreover I also want to thank Marta Pieropan and Remy van Dobben de Bruyn who were both helpful when I had some questions about algebraic geometry.

I would also like to thank the people in the Mathematics library, where most of this thesis was written, for the positive atmosphere and the listening ears. I am glad that there was always something happening or someone to talk to even on the boring study days.

My parents and Anne also both deserve my appreciation, for which I would also like to thank them.

Contents

Introduction **1**

1 The Markov Equation **2**
1.1 Finding solutions 2
1.2 Generalized Markov Equation 4

2 Markov Equation over Finite Fields **7**
2.1 Point counting theorem 7
2.2 Squares in finite fields 7
2.3 Counting solutions 8

3 Zeta Functions **12**
3.1 General theory 12
3.2 Zeta functions of varieties 15
3.3 Markov surfaces 18
3.4 Conjectures 20

4 Markov Graphs **23**
4.1 Definition of Markov Graph 23
4.2 Cycles 25
4.3 Graph property experiments 29

5 Cryptography with Markov Graphs **32**
5.1 The pathfinding algorithm 32
5.1.1 Graph differences 32
5.1.2 Maximally elliptic coordinates 34
5.1.3 Steps in SPFA 36
5.2 Heuristics 36
5.2.1 Estimates for $H_1(p)$ 37
5.2.2 Estimates for $H_2(p)$ 38
5.3 Time complexity 39
5.3.1 General case 39
5.3.2 Smooth case 40

A Extra figures and code **42**
A.1 Some more graphs 42
A.2 Sage code 44
A.2.1 SPFA-related code 45

References **II**

Introduction

In 1879 Andrey Markov studied quadratic forms and continued fractions [20], [21] and found a remarkable relation between diophantine approximation theory and the integral solutions to the Markov Equation 1 now known as Markov's theorem. Since then these solutions have appeared in various settings such as number theory, combinatorics, classical groups and geometry [1].

$$X^2 + Y^2 + Z^2 = 3XYZ \tag{1}$$

One can use the technique of Vieta jumping to generate new solutions from some starting solution. This gives a natural way to make a graph out of the solutions where the edges are determined by the jumps. It was already shown in the original paper that all solutions in the natural numbers can be generated by following such edges from the smallest solution $(1, 1, 1)$. Recently interest has risen to similar graphs with the solutions over some finite field $\mathbb{F}_p$ [2], [6]. As the structure of the graph is defined entirely in terms of polynomials, the projection map from the solutions over $\mathbb{Z}$ to solutions over $\mathbb{F}_p$ also preserves edges in these graphs. When such a graph is connected it implies that all solutions over $\mathbb{F}_p$ can be lifted to a solution over $\mathbb{Z}$. Inspired by this algebraic statement that follows from a combinatorial property in this family of graphs the Markov graphs modulo p have gained more interest [8].

In this thesis, we begin with two preparatory chapters, followed by three independent chapters that can be understood in isolation. In Chapter 1 we will look at the Markov Equation over $\mathbb{Z}$ and introduce the Generalized Markov Equation. Chapter 2 focuses on counting solutions over finite fields to the Generalized Markov Equation, although some tools introduced in this chapter will also be used later to count edges. Chapter 3 revolves around the geometry of the variety defined by the Markov Equation. We will calculate the arithmetic zeta function of these varieties and verify two conjectures for this particular family of varieties. In Chapter 4 we introduce and study Markov graphs modulo p. We will first focus on cycles that appear in these graphs. We will then give an overview of different graph properties and look at the properties for the Markov graphs. Finally Chapter 5 looks at an article by Joseph H. Silverman that was published in November 2022 [30]. This article describes a path-finding algorithm in a graph very similar to the Markov graph. This algorithm shares resemblance to ideas from [2] that shows the Markov graph has a large connected component.

Chapter 1

The Markov Equation

The main focus of this thesis is the Markov Equation

$$x^2 + y^2 + z^2 = 3xyz. \tag{1}$$

In this chapter we will first look at some classical results related to the Markov Equation. In the second section we will look at the Generalized Markov Equation and prove some more geometrical lemmas that will become useful later in other chapters.

1.1 Finding solutions

First of all we will consider solutions to Equation 1 in the positive integers, such a solution we define to be a Markov triple. After inspection one might find

$$(1,1,1),(1,1,2),(1,2,5),(1,5,13),(2,5,29),(1,13,34),\ldots$$

But recognizing a pattern in these solutions is not an easy task. The ingenuity of Markov in studying this equation was a way to construct new solutions from some starting solution. We will now see how and why his construction of new solutions works.

We start off with the solution $(1,1,1)$. To simplify the search for new solutions we can consider the question if there are other solutions of the form $(1,1,t)$, which we can plug into the Markov equation and this gives us $t^2+2=3t$. This quadratic has two solutions, namely $t=1$ and $t=2$. So this gives us a new solution, $(1,1,2)$, and the old solution $(1,1,1)$. We can repeat this idea of looking for new solutions with two coordinates the same as some basis point. For instance we can now ask if there are more solutions of the form $(1,t,2)$, which gives in $t^2+5=6t$ and gives us solutions $t=1$ and $t=5$.

In general if we have some solution (a,b,c) to Equation 1, we can look for other solutions (a,b,t). We can plug this in to the Markov Equation and then we are left with

$$P(t) = t^2 - 3abt + a^2 + b^2 = 0, \tag{1.1.1}$$

and as we know that this quadratic has one integer zero, namely $t=c$ we see that the other zero c' of $P(t)$ must also be an integer. In particular we have that $cc' = a^2+b^2$ and $c+c' = 3ab$. From the first equation we see that c' is also positive and from the second equation we get that c' is an integer. If we would have $c=c'$, then we must have $4a^2+4b^2 = 9a^2b^2$. Therefore we see that $16 = (9a^2-4)(9b^2-4)$, which has no solutions over the positive integers. So we see that this procedure gives a new Markov triple.

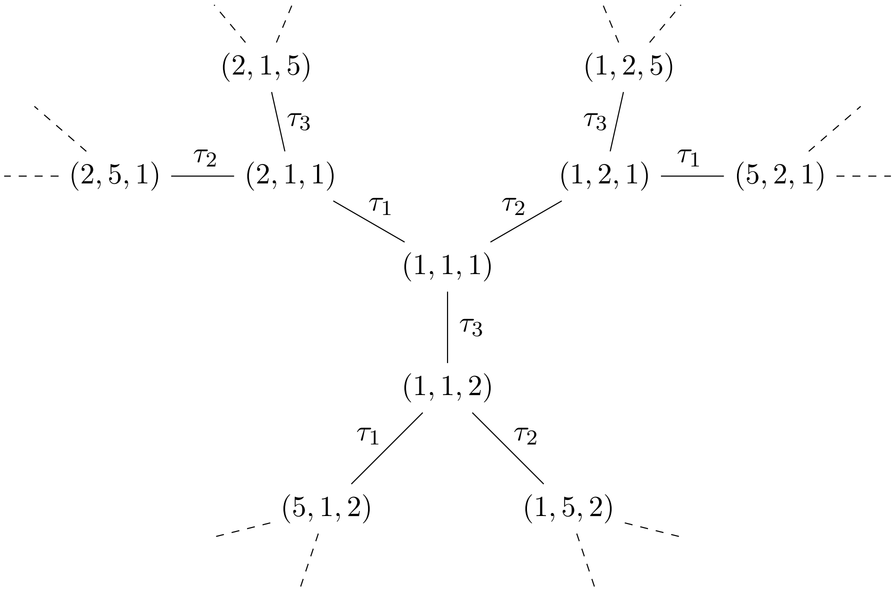
The construction starts with some solution and changes one of the three coordinates to create a new solution. We denote these changes of one coordinate by τ_1, τ_2, τ_3 that take a solution and give a different solution to the Markov Equation. As coordinates, they are defined by

$$\tau_1(a,b,c) = (3bc - a, b, c), \tag{1.1.2}$$

$$\tau_2(a,b,c) = (a, 3ac - b, c), \tag{1.1.3}$$

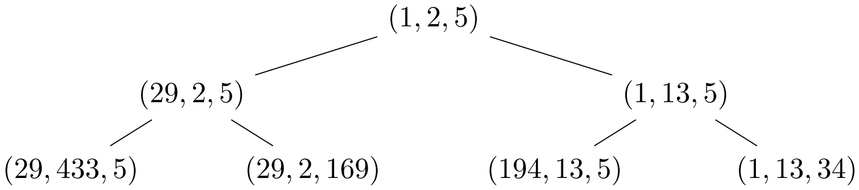
$$\tau_3(a,b,c) = (a, b, 3ab - c). \tag{1.1.4}$$

We can now make a graph with the solutions to the Markov equation as vertices and edges drawn from each solution P to $\tau_i(P)$ for $i = 1,2,3$. If we start with $(1,1,1)$ we can draw the points nearby to get the following figure.



(1.1.5)

Since the solution $(1,1,1)$ is totally symmetric we see that the three different branches from $(1,1,1)$ give the same solutions but in a different order. Moreover as $(1,1,2)$ has the same x- and y-coordinate we see that the two branches from $(1,1,2)$ away from $(1,1,1)$ will also be the same except that the first two coordinates are permuted. We can now draw just the branch from $(1,2,5)$ and then we get the following graph.



(1.1.6)

Here we indeed find all small solutions that we wrote down earlier, or at least some permutation. The following theorem indeed ensures us that we will find all solutions in this graph.

Theorem 1.1.1 (Markov, 1880). *All Markov triples can be constructed by repeatedly applying τ_1, τ_2 and τ_3 to $(1,1,1)$.*

Proof. We will prove this theorem by infinite descent. If particular we will show that if we have some solution (a,b,c) not equal to $(1,1,1)$, then for at least one $i \in \{1,2,3\}$ we lower the maximum value of the triple by applying τ_i. As the solutions are in the natural numbers repeating this lowering must end at some point and then we have made $(1,1,1)$. As all τ_i are of order 2 we can reverse this process by reversing the order of the τ_i that are applied to go from (a,b,c) to $(1,1,1)$.

Without loss of generality we can assume that $a \leq b \leq c$, as permuting the entries just permutes which τ_i to use. In particular we have $\sigma(\tau_i(P)) = \tau_{\sigma(i)}(\sigma(P))$ for a permutation σ of three elements, where σ acts on $\{1, 2, 3\}$ as the permutation of the numbers and on a solution P to the Markov equation by permuting the coordinates.
We will now show that $c > b$ from contradiction. If we have two coordinates that are the same then some permutation of (a, b, c) must be a solution to $x^2 + y^2 + z^2 = 3xyz$ and $x = y$, so we have $2x^2 + z^2 = 3x^2z$. Then we have that x^2 divides z^2, so x divides z. We write $z = kx$ for some positive integer k. Then we can divide by x and get $2 + k^2 = 3xk$, so we see that k must also divide 2. If $k = 1$ then we get $z = x$ and $3x^2 = 3x^3$, so $x = 1$, which corresponds to the solution $(1, 1, 1)$. By assumption (a, b, c) is not equal to this solution. If $k = 2$ then we have that $6x^2 = 6x^3$, so we get $x = 1$ and the solution $(1, 1, 2)$. In particular we see that $c = 2 > 1 = b$.
We will now show that τ_3 works for the descent. In particular as $a \leq b < c$ the maximum of this triple is c, and the new triple becomes (a, b, c') where we know that $c' = (a^2 + b^2)/c = 3ab - c$. For a contradition we now assume that $c' \geq c$, so we have $a^2 + b^2 \geq c^2$ and $3ab \geq 2c$. As $b \geq a$ we get that $2b^2 \geq c^2$, so we see that $2 > \frac{2b}{c} > \sqrt{2}$. Therefore we get from the Markov equation for (a, b, c) that

$$3 > \frac{a^2 + b^2 + c^2}{c^2} = \frac{3abc}{c^2} = 3a \cdot \frac{b}{c} > \frac{3a}{\sqrt{2}}.$$

Thus we must have that $a = 1$, so from $1 + b^2 = a^2 + b^2 \geq c^2$ and $c > b$ we get $1 + b^2 = c^2$, which cannot happen in the positive integers. Thus we conclude that $c' < c$. □

Corollary 1.1.2. *The entries in all Markov triples are all pairwise relatively prime.*

Proof. Clearly this statement holds for the Markov triple $(1, 1, 1)$. Moreover if this property holds for (a, b, c) then it also holds for $\tau_1((a, b, c)) = (3bc - a, b, c)$, since $\gcd(3bc - a, b) = \gcd(a, b) = 1$ and similarly $\gcd(3bc - a, c) = 1$. By symmetry it also holds for $\tau_2((a, b, c))$ and $\tau_3((a, b, c))$. As all Markov triples can be constructed by repeated application of the τ_i's to $(1, 1, 1)$ we see that all Markov triples must have this property. □

So far we have considered the solutions of the Markov equation over the positive integers, but we will now extend to all integers. First of all we consider the case where one of the three variables is equal to 0, then by symmetry we can consider the case where $x = 0$. Then we are left with $y^2 + z^2 = 0$, but as squares are non-negative this implies that $y = z = 0$. So if one the variables is 0 then the whole solution must be $(0, 0, 0)$ over the integers. If x, y, z are all not equal to 0, then $x^2 + y^2 + z^2$ must be positive so therefore xyz must also be positive. Therefore we see that $|x||y||z| = |xyz| = xyz$ and as we also have that $|x|^2 = x^2$ we see that for all integral solutions (x, y, z) to the Markov equation the triple $(|x|, |y|, |z|)$ must be a Markov triple. Moreover as xyz is positive there can either be zero or two negative numbers between x, y and z. So all integral solutions to 1 are either $(0, 0, 0)$ or in one of the four types $(x, y, z), (-x, -y, z), (-x, y, -z), (x, -y, -z)$ for some Markov triple (x, y, z).

1.2 Generalized Markov Equation

In this thesis we will consider a more general equation than the Markov Equation, namely

$$W_{a,b} : x^2 + y^2 + z^2 = axyz + b \tag{1.2.1}$$

and we will refer to this as the Generalized Markov Equation. Moreover we will write $W_{a,b}$ for the variety defined by this equation. There are two parameters in this equation, and with $a = 3$ and $b = 0$ we get the original Markov Equation back.

Lemma 1.2.1. *Let R be a ring, $a, b \in R$ and $\mathcal{M}_{a,b}(R)$ the set of solutions to the Generalized Markov Equation in R. Then the involutions τ_1, τ_2, τ_3 defined by*

$$\tau_1(x, y, z) = (ayz - x, y, z), \tag{1.2.2}$$
$$\tau_2(x, y, z) = (x, axz - y, z), \tag{1.2.3}$$
$$\tau_3(x, y, z) = (x, y, axy - z) \tag{1.2.4}$$

map $\mathcal{M}_{a,b}(R)$ to itself.

Proof. By symmetry we only have to verify that τ_1 preserves solutions. For $(x, y, z) \in \mathcal{M}_{a,b}(R)$ we have that

$$(ayz - x)^2 + y^2 + z^2 = x^2 + y^2 + z^2 - 2axyz + a^2y^2z^2 = a(ayz - x)yz + b.$$

□

Lemma 1.2.2. *For $a \in \mathbb{Z}_{>0}$ the set $\mathcal{M}_{a,0}(\mathbb{Z})$ is $\{(0, 0, 0)\}$ for all $a \notin \{1, 3\}$. Moreover the map $(x, y, z) \mapsto (3x, 3y, 3z)$ is a bijection from $\mathcal{M}_{3,0}(\mathbb{Z})$ to $\mathcal{M}_{1,0}(\mathbb{Z})$.*

Proof. First of all we note that we have an injective map $f_a : \mathcal{M}_{a,0}(\mathbb{Z}) \to \mathcal{M}_{1,0}(\mathbb{Z})$ defined by $(x, y, z) \mapsto (ax, ay, az)$. As the only solution to $W_{1,0}$ over $\mathbb{Z}/3\mathbb{Z}$ is $(0, 0, 0)$, we see that the map $(x, y, z) \mapsto (\frac{1}{3}x, \frac{1}{3}y, \frac{1}{3}z)$ is the inverse of f_3. So for $a \notin \{1, 3\}$ we can compose the map f_a to see that $g_a : \mathcal{M}_{a,0}(\mathbb{Z}) \to \mathcal{M}_{3,0}(\mathbb{Z})$ given by $(x, y, z) \mapsto (\frac{a}{3}x, \frac{a}{3}y, \frac{a}{3}z)$ is well-defined. But we already saw that solutions in $\mathcal{M}_{3,0}$ are either $(0, 0, 0)$ of a Markov triple with some minus-signs added. By Corollary 1.1.2 we see for all triples not equal to $(0, 0, 0)$ that the coordinates are relatively prime. But all elements in the image of g_a share a factor a is 3 does not divide a or a factor $a/3 > 1$ if 3 does divide a. So they are not relatively prime. Therefore the only element in the image of g_a is $(0, 0, 0)$ and $\mathcal{M}_{a,0}(\mathbb{Z})$ only contains the element $(0, 0, 0)$. □

This lemma can be seen as a motivation why a 3 should appear on the right-hand side of the Markov Equation 1 and no other integer.
We will now prove some basic properties of the variety $W_{a,b}$ over some field k.

Lemma 1.2.3. *Let k be some field, $a, b \in k$ and $\lambda \in k^\times$. Consider $W_{a,b}$ and $W_{a/\lambda,\lambda^2 b}$ over k. Then the map $(x, y, z) \mapsto (\lambda x, \lambda y, \lambda z)$ is an isomorphism of varieties from $W_{a,b}$ to $W_{a/\lambda,\lambda^2 b}$.*

Proof. Let (x, y, z) be a point in $W_{a,b}$, then

$$(\lambda x)^2 + (\lambda y)^2 + (\lambda z)^2 = \lambda^2(x^2 + y^2 + z^2) = \lambda^2 axyz + \lambda^2 b = a\lambda^{-1}(\lambda x)(\lambda y)(\lambda z) + \lambda^2 b,$$

so the map actually maps $W_{a,b}$ to $W_{a/\lambda,\lambda^2 b}$, and this map is defined by polynomials so it is a regular map. The inverse of this map is given by $(x, y, z) \mapsto (\lambda^{-1}x, \lambda^{-1}y, \lambda^{-1}z)$ which is also regular. □

A consequence of this lemma is that if we are interested in the algebraic variety $W_{a,b}$ over a field and a is non-zero, we can assume $a = 1$ by using the isomorphism with $\lambda = a$.

Lemma 1.2.4. *Let k be a field and $a, b \in k$ with $a \neq 0$. In characteristic 2 the variety $W_{a,b}$ is always singular. In all other characteristics the algebraic variety $W_{a,b}$ is singular if and only if $(a^2b - 4)b = 0$.*

Proof. As isomorphisms preserve singularities and $a \neq 0$ we can use the previous remark to assume $a = 1$.
We will first prove that $f(x, y, z) = x^2 + y^2 + z^2 - xyz - b$ is irreducible. On the contrary assume that $f(x, y, z) = P(x, y, z)Q(x, y, z)$ for non-constant polynomials P, Q. As the total degree of f is 3 we see that without loss of generalization we have P of total degree 1 and Q of total degree

2. Moreover we see that the degree of f in the variable x is 2 and f is monic as a polynomial in x, so both P and Q must have degree 1 in the variable x. We see that the same holds for y, z. Now we can write

$$P(x,y,z) = a_1x + a_2y + a_3z + a_4, \qquad Q(x,y,z) = b_1xy + b_2xz + b_3yz + b_4x + b_5y + b_6z + b_7$$

for $a_i, b_j \in k$. Then a_1, a_2, a_3 are all non-zero because of the degree in each variable of P, so by comparing the coefficients for x^2y, xy^2 and xz^2 we see that $b_1 = b_2 = b_3 = 0$, which contradict the total degree of Q being 2.
As $f(x,y,z)$ is irreducible, $W_{1,b}$ is also irreducible. The Jacobian for $W_{1,b}$ is

$$\begin{pmatrix} 2x - yz & 2y - xz & 2z - xy \end{pmatrix}.$$

In characteristic 2 the point $(0, 0, \sqrt{b})$ is singular.
If $b = 0$ then $(0, 0, 0)$ is a singular point and if $b = 4$ then $(2, 2, 2)$ is a singular point. Furthermore we can calculate that

$$2b^2 - 8b = 2(4 - z^2 - b)f + (xz^2 + bx - 4x - 2yz)(2x - yz) + (b - 4)y(2y - xz) + (z^3 - 4z)(2z - xy),$$

so if $2b^2 - 8b$ is non-zero then there are no singular points. □

Lemma 1.2.5. *Let k be a field and $a, b \in k$ with $a \neq 0$. Let $P_{a,b}$ the projective closure of $W_{a,b}$ defined by $t(x^2 + y^2 + z^2) = axyz + bt^3$ in $\mathbb{P}^3$ over k. Then $P_{a,b}$ is smooth if and only if $W_{a,b}$ is.*

Proof. If $W_{a,b}$ is singular then so is $P_{a,b}$. We take the chart $x = 1$, then we get $t(1 + y^2 + z^2) = ayz + bt^3$, then the Jacobian is

$$\begin{pmatrix} 2yt - az & 2zt - ay & 1 + y^2 + z^2 + 3bt^2 \end{pmatrix}.$$

If $t = 0$, then we get $az = 0$ and $ay = 0$, so $t = y = z = 0$. But then the last entry in the Jacobian does not vanish. By symmetry we also see in the charts $y = 1$ and $z = 1$ that there are no singular points with $t = 0$. So if $P_{a,b}$ is singular then that point must live in the chart $t = 1$, so $W_{a,b}$ is also singular. □

Chapter 2

Markov Equation over Finite Fields

In this chapter we will focus on counting solutions to the Generalized Markov Equation over finite fields. In the first section we will state the main theorem we will prove in this chapter. In the second section we will make some preparations related to squares in finite fields. In the third section we will give the proof for the main theorem.

2.1 Point counting theorem

We are interested in the Generalized Markov Equation 1.2.1 over finite fields. The following theorem states exactly how many solutions there are in all finite fields. Although this result was independently found in this thesis project, the cases $p > 2$ were all already known seventy years ago in [4].

Theorem 2.1.1. *Let p be prime, $n \in \mathbb{Z}_{>0}$ and $a, b \in \mathbb{Z}$. We write $q = p^n$ and let $N_q(a,b)$ be the number of points in $\mathbb{F}_q^3$ that satisfy $x^2 + y^2 + z^2 = axyz + b$. Then we have*

$$N_q(a,b) = \begin{cases} q^2 & \text{if } p = 2 \text{ and } a \text{ even,} \\ q^2 + 1 & \text{if } p = 2,\ a \text{ odd and } b \text{ even,} \\ q^2 + q(-1)^n + 1 & \text{if } p = 2,\ a, b \text{ both odd,} \\ q^2 + q\left(\frac{-b}{p}\right)^n & \text{if } p > 2 \text{ and } p|a, \\ q^2 + 1 + 3q\left(\frac{-1}{p}\right)^n & \text{if } p > 2,\ \gcd(a,p) = 1 \text{ and } p|b, \\ q^2 + 1 + 4q\left(\frac{a^2b-4}{p}\right)^n & \text{if } p > 2,\ \gcd(a,p) = 1 \text{ and } (\frac{b}{p})^n = 1, \\ q^2 + 1 + 2q\left(\frac{a^2b-4}{p}\right)^n & \text{if } p > 2,\ \gcd(a,p) = 1 \text{ and } (\frac{b}{p})^n = -1. \end{cases} \tag{2.1.1}$$

Remark 2.1.2. We can also rewrite the last three cases in Theorem 2.1.1 to

$$N_q(a,b) = q^2 + 1 + 3q\left(\frac{a^2b-4}{p}\right)^n + q\left(\frac{a^2b^2-4b}{p}\right)^n, \tag{2.1.2}$$

or even include the $p|a$ case by adding a $\left(\frac{a^2}{p}\right)$ factor to the second and third term.

2.2 Squares in finite fields

In this chapter we are interested in counting solutions to Equation 1 and Equation 1.2.1 over finite fields. As both equations are quadratic when we fix two of the coordinates the squares in finite fields will play a big role.

Definition 2.2.1. For q an odd prime power we define the Legendre symbol $\lambda_q : \mathbb{F}_q \to \{0, \pm 1\}$ for the finite field $\mathbb{F}_q$ by

$$\lambda_q(x) := \left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} 1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^\times, \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q, \\ 0 & \text{if } x = 0. \end{cases}$$

We note that this definition for q prime is the same as the classic Legendre symbol. This Legendre symbol is also multiplicative as $\mathbb{F}_q^\times$ is cyclic. Moreover we can see $\mathbb{F}_p$ as the prime field of $\mathbb{F}_q$, so we can also restrict λ_q to $\mathbb{F}_p$. The following lemma gives a relation between the values of λ_p and λ_q restricted to $\mathbb{F}_p$.

Lemma 2.2.2. *Let p be an odd prime, $n \in \mathbb{Z}_{>0}$ and write $q = p^n$. Then we have for all $x \in \mathbb{F}_p$ that $\lambda_q(x) = \lambda_p(x)^n$.*

Proof. First of all we note that this is true for $x = 0$. For $x \in \mathbb{F}_p^\times$ with $\lambda_p(x) = 1$ we see that x is still a square in $\mathbb{F}_q$. If $\lambda_p(x) = -1$ and n is odd we see that $\sqrt{x}$ can still not exist in $\mathbb{F}_q$, as $\sqrt{x}$ has even degree which would imply that $n = [\mathbb{F}_q : \mathbb{F}_p]$ is even, so we also have $\lambda_q(x) = -1$. If n is even we see that $\mathbb{F}_p(\sqrt{x}) = \mathbb{F}_{p^2}$ is a subfield of $\mathbb{F}_q$, so $\lambda_q(x) = 1 = \lambda_p(x)^n$. □

Lemma 2.2.3. *Let $p > 2$ be prime, $q = p^n$ and $C, D \in \mathbb{F}_q^\times$. Let $\lambda_q : \mathbb{F}_q \to \{0, \pm 1\}$ be the function that maps 0 to 0, other squares to 1 and non-squares to -1. Then we have that*

$$\sum_{z \in \mathbb{F}_q} \lambda_q(Cz^2 + D) = -\lambda_q(C). \tag{2.2.1}$$

Proof. First of all we note that as λ_q is multiplicative, it suffices to prove that $\sum_{z \in \mathbb{F}_q} \lambda_q(z^2+D) = -1$. If we consider $z^2 + D = y^2$, then we can make a coordinate change to $u = y + z$ and $v = y - z$ and we get the equation $uv = D$. As D is non-zero we see that u, v must also be non-zero and for every $u \in \mathbb{F}_q^\times$ there is a unique $v \in \mathbb{F}_q$ such that $uv = D$. Thus there are $q - 1$ solutions to $z^2 + D = y^2$.

If $-D$ is not a square then there are no solutions with $y = 0$, so for each (y, z) with $z^2 + D = y^2$ there is exactly one other y' such that y', z is a solution. As there are $q - 1$ solutions in total we see that there are $(q-1)/2$ different values for z such that $z^2 + D$ is a non-zero square. Moreover as $z^2 + D$ cannot be zero we see that for the other $q - (q-1)/2$ values of z we have that $z^2 + D$ is not a square. So we can calculate that

$$\sum_{z \in \mathbb{F}_q} \lambda_q(z^2 + D) = \frac{q-1}{2} - \frac{q+1}{2} = -1.$$

If $-D$ is a square, then we can make a similar calculation. There are two pairs (y, z) with $z^2 + D = 0$ and for all other solutions (y, z) there is a unique pair (y', z) that is also a solution. So we get two values of z where $z^2 + D = 0$, exactly $(q-3)/2$ values of z where $z^2 + D$ is a non-zero square. Therefore we get that

$$\sum_{z \in \mathbb{F}_q} \lambda_q(z^2 + D) = 2 \cdot 0 + \frac{q-3}{2} - (q - \frac{q-3}{2} - 2) = -1.$$

□

2.3 Counting solutions

We will now prove the following theorem. As indicated by the expression for $N_q(a, b)$, the proof will also contain a lot of case distinctions. We will fist consider the case where $p > 2$ and leave the characteristic 2 calculation to the end.

Theorem 2.1.1. *Let p be prime, $n \in \mathbb{Z}_{>0}$ and $a, b \in \mathbb{Z}$. We write $q = p^n$ and let $N_q(a,b)$ be the number of points in $\mathbb{F}_q^3$ that satisfy $x^2 + y^2 + z^2 = axyz + b$. Then we have*

$$N_q(a,b) = \begin{cases} q^2 & \textit{if } p = 2 \textit{ and } a \textit{ even,} \\ q^2 + 1 & \textit{if } p = 2,\ a \textit{ odd and } b \textit{ even,} \\ q^2 + q(-1)^n + 1 & \textit{if } p = 2,\ a, b \textit{ both odd,} \\ q^2 + q\left(\frac{-b}{p}\right)^n & \textit{if } p > 2 \textit{ and } p|a, \\ q^2 + 1 + 3q\left(\frac{-1}{p}\right)^n & \textit{if } p > 2,\ \gcd(a,p) = 1 \textit{ and } p|b, \\ q^2 + 1 + 4q\left(\frac{a^2b-4}{p}\right)^n & \textit{if } p > 2,\ \gcd(a,p) = 1 \textit{ and } (\frac{b}{p})^n = 1, \\ q^2 + 1 + 2q\left(\frac{a^2b-4}{p}\right)^n & \textit{if } p > 2,\ \gcd(a,p) = 1 \textit{ and } (\frac{b}{p})^n = -1. \end{cases} \tag{2.1.1}$$

Proof. We start with the case $p > 2$. For $y, z \in \mathbb{F}_q$ we can look if there exist $x \in \mathbb{F}_q$ such that (x, y, z) is a solution to the Genealized Markov Equation. As we have a quadratic equation in x this is determined by the determinant Δ of the polynomial. We see that

$$\Delta = a^2y^2z^2 - 4y^2 - 4z^2 + 4b,$$

and if $\Delta = 0$ then there is one solution triple with y, z as coordinates, if Δ is a non-zero square then there are two such triples and if Δ is not a square then there are no such solutions. So we see that the number of solutions with y, z as the last two coordinates is equal to $\lambda_q(\Delta) + 1$. So we see that

$$N_q(a,b) = \sum_{y,z \in \mathbb{F}_q} 1 + \lambda_q(\Delta) = q^2 + \sum_{y,z \in \mathbb{F}_q} \lambda_q(a^2y^2z^2 - 4y^2 - 4z^2 + 4b). \tag{2.3.1}$$

The general strategy in all cases will be to use Lemma 2.2.3 to simplify these sums, but we have to be careful which factors can vanish and note that we cannot use the lemma for those sums. As we have that $\Delta = (a^2y^2 - 4)z^2 + (4b - 4y^2)$ we split the sums over y depending on $a^2y^2 - 4$ and $4b - 4y^2$ being zero or non-zero. We can now calculate that

$$\begin{aligned} \sum_{y,z \in \mathbb{F}_q} \lambda_q(\Delta) &= \sum_{\substack{y,z \in \mathbb{F}_q \\ a^2y^2 = 4}} \lambda_q(\Delta) + \sum_{\substack{y,z \in \mathbb{F}_q \\ a^2y^2 \neq 4 \\ b = y^2}} \lambda_q(\Delta) + \sum_{\substack{y,z \in \mathbb{F}_q \\ a^2y^2 \neq 4 \\ b \neq y^2}} \lambda_q(\Delta) && (2.3.2) \\ &= \sum_{\substack{y,z \in \mathbb{F}_q \\ a^2y^2 = 4}} \lambda_q(4b - 4y^2) + \sum_{\substack{y,z \in \mathbb{F}_q \\ a^2y^2 \neq 4 \\ b = y^2}} \lambda_q((a^2y^2 - 4)z^2) + \sum_{\substack{y,z \in \mathbb{F}_q \\ a^2y^2 \neq 4 \\ b \neq y^2}} \lambda_q((a^2y^2 - 4)z^2 + (4b - 4y^2)) && (2.3.3) \\ &= \sum_{\substack{y \in \mathbb{F}_q \\ a^2y^2 = 4}} q\lambda_q(b - y^2) + \sum_{\substack{y \in \mathbb{F}_q \\ a^2y^2 \neq 4 \\ b = y^2}} (q-1)\lambda_q(a^2y^2 - 4) - \sum_{\substack{y \in \mathbb{F}_q \\ a^2y^2 \neq 4 \\ b \neq y^2}} \lambda_q(a^2y^2 - 4). && (2.3.4) \end{aligned}$$

We will now start to distinguish between the separate cases. We start off with $a = 0$. As p is odd the first sum vanishes. If $b = 0$ then there is one term in the middle sum and $q - 1$ in the last sum. So we see that

$$\sum_{y,z \in \mathbb{F}_q} \lambda_q(\Delta) = (q-1)\lambda_q(-4) - (q-1)\lambda_q(-4) = 0 = q\lambda_q(-b).$$

If we have $\lambda_q(b) = 1$ then there are two terms in the middle sum and $q - 2$ in the last sum, so we get

$$\sum_{y,z \in \mathbb{F}_q} \lambda_q(\Delta) = 2(q-1)\lambda_q(-4) - (q-2)\lambda_q(-4) = q\lambda_q(-4) = q\lambda_q(-b).$$

If we have $\lambda_q(b) = -1$ then there are only terms in the last sum so we get that

$$\sum_{y,z\in\mathbb{F}_q} \lambda_q(\Delta) = -q\lambda_q(-4) = q\lambda_q(-b).$$

We now continue to $a \neq 0$. Now there are two terms in the first sum, namely for $y = \pm 2a^{-1}$. This gives a contribution of $2q\lambda_q(a^2b-4)$. If $b = 0$ we get one term in the middle sum with $y = 0$ and $q-3$ in the last sum. In the last sum we want to use Lemma 2.2.3 again, but this sum takes al values of y except for $0, \pm 2a^{-1}$. So we get that

$$\sum_{\substack{y\in\mathbb{F}_q\\ a^2y^2\neq 4\\ b\neq y^2}} \lambda_q(a^2y^2-4) = \left(\sum_{y\in\mathbb{F}_q} \lambda_q(a^2y^2-4)\right) - \lambda_q(-4) - 2\lambda_q(0) = -\lambda_q(a^2) - \lambda_q(-1) = -1 - \lambda_q(-1).$$

We can combine this with Equation 2.3.4 to see that

$$\sum_{y,z\in\mathbb{F}_q} \lambda_q(\Delta) = 2q\lambda_q(a^2b-4) + (q-1)\lambda_q(-4) - (-1-\lambda_q(-1)) = 1 + 3q\lambda_q(-1).$$

Now if $\lambda_q(b) = -1$ we see that the middle sum in Equation 2.3.4 vanishes, so the last sum sums over all y except for $y = \pm 2a^{-1}$. As $\lambda_q(a^2y^2-4) = 0$ for such y we see that the missing terms are zero so we can use Lemma 2.2.3 to see that the sum is equal to $-\lambda_q(a^2) = -1$, so if we combine this with the contribution from the first sum we see that $\sum_{y,z\in\mathbb{F}_q} \lambda_q(\Delta) = 2q\lambda_q(a^2b-4) + 1$.
Now if $\lambda_q(b) = 1$ we get two terms in the middle sum from Equation 2.3.4. Moreover in the last sum there are $q-4$ terms and the terms missing are for $y = \pm 2a^{-1}$ and $y = \pm\sqrt{b}$. For $y = \pm 2a^{-1}$ we have $\lambda_q(a^2y^2-4) = 0$ and for $y = \pm\sqrt{b}$ we have $\lambda_q(a^2y^2-4) = \lambda_q(a^2b-4)$. So we see that

$$\sum_{y,z\in\mathbb{F}_q} \lambda_q(\Delta) = 2q\lambda_q(a^2b-4) + 2(q-1)\lambda_q(a^2b-4) - (-\lambda_q(a^2) - 2\lambda_q(a^2b-4)) = 1 + 4q\lambda_q(a^2b-4).$$

We will now proceed with the case $p = 2$. In characteristic 2 we cannot see if quadratics are solvable by only considering the discriminant. Therefore we must use a different approach. As $N_q(a,b)$ only depends on the parity of a and b we consider all four cases. If a is even, then we count solutions to $x^2 + y^2 + z^2 = b$ for $b \in \mathbb{F}_2$. We see that $b = b^2$ and because we work in characteristic 2 we can rewrite this to $(x+y+z+b)^2 = 0$. So we are left with a linear equation that has q^2 solutions.
For the case $a = 1, b = 0$ we get $x^2 + y^2 + z^2 = xyz$. If $xyz = 0$, then we get $3q-2$ solutions in $\mathbb{F}_q^3$ such that also $x^2 + y^2 + z^2 = 0$. Now we define

$$V = \{(x,y,z) \in (\mathbb{F}_q^\times)^3 : x^2 + y^2 + z^2 \neq 0\}.$$

As $x^2 + y^2 + z^2 = 0$ has q^2 solutions over $\mathbb{F}_q$ we see that

$$|V| = (q-1)^3 - (q^2 - (3q-2)) = (q-1)(q^2 - 3q + 3).$$

Moreover $\mathbb{F}_q^\times$ acts on V by scaling all three coordinates. In each orbit there is exactly one triple that is a solution to $x^2 + y^2 + z^2 = xyz$. Therefore we see that the total number of solutions is

$$3q - 2 + \frac{|V|}{|\mathbb{F}_q^\times|} = 3q - 2 + q^2 - 3q + 3 = q^2 + 1.$$

At last we consider the case $a = b = 1$. For $x = 0$ we get $(y+z+1)^2 = 0$, so q solutions. For $x = 1$ we get $y^2 + yz + z^2 = 0$. This a homogeneous equation, so it gives a solution with

$y = z = 0$ and we can count the other solutions by considering the equation in $\mathbb{P}^1$. Over $\mathbb{P}^1$ we see that y cannot be 0 as that implies $z = 0$, so we can assume $y = 1$ in a representative. This leaves us with $1 + z + z^2 = 0$. As this polynomial is quadratic and irreducible over $\mathbb{F}_2$, it has no zero's when n is odd and two different zero's when n is even. For odd n this means that the only solution with $x = 1$ is $(1, 0, 0)$, for n even this gives us two solutions for z, so when we get back to affine coordinates this gives $1 + 2(q - 1) = 2q - 1$ solutions.
We will now take $x = c$ fixed for some $c \in \mathbb{F}_q \backslash \mathbb{F}_2$. Then we are left with $y^2 + cyz + z^2 = 1 + c^2$. Now we let $V = \{(y, z) \in \mathbb{F}_q^2 : y^2 + cyz + z^2 \neq 0\}$. Then $\mathbb{F}_q^\times$ acts on this set and each orbit has exactly one solution to $y^2+cyz+z^2 = 1+c^2$, as $1+c^2 \neq 0$. Thus the number of solutions (c, y, z) is $|V|/|\mathbb{F}_q^\times|$. Now let $P(X) = X^2 + cX + 1$, if P has no roots then $y^2 + cyz + z^2 = 0$ if and only if $y = z = 0$, so $|V| = q^2 - 1$ and there are $q + 1$ solutions with $x = c$. If P has a root, then it has two different roots ω_1, ω_2 as $c \neq 0$. Moreover if $(y, z) \neq (0, 0)$ and $y^2 + cyz + z^2 = 0$ then $z \neq 0$, and also $P(y/z) = 0$. So $y/z = \omega_1$ or $y/z = \omega_2$. In both cases there are $q-1$ non-zero choices for z and a unique y to satisfy the equation. Therefore we see that $|V| = q^2-1-2(q-1) = (q-1)^2$, so there are $q - 1$ solutions with $x = c$.
It is now left to count for how many $c \in \mathbb{F}_q$ the polynomial P has roots. For such $c \in \mathbb{F}_q$ we can write $P(X) = (X - \omega_1)(X - \omega_2)$. If we compare coefficients we get $\omega_1\omega_2 = 1$ and $\omega_1 + \omega_2 = c$, so we can write $c = \omega_1 + \omega_1^{-1}$. We define $f : \mathbb{F}_q^\times \to \mathbb{F}_q$ by $x \mapsto x + x^{-1}$ and note that for some $c \in \mathbb{F}_q$ the polynomial P has roots if and only if $c \in \mathrm{Im}(f)$. If we have two $\alpha, \beta \in \mathbb{F}_q^\times$ with $f(\alpha) = f(\beta)$ then we get $(\alpha - \beta)(1 - \alpha\beta) = 0$. So if $\alpha \neq \beta$ then $\alpha = 1/\beta$. The only element in $\mathbb{F}_q^\times$ with $\alpha = 1/\alpha$ is $\alpha = 1$, so we see that all other elements of $\mathbb{F}_q^\times$ have a unique element with the same image. So therefore we see that $|\mathrm{Im}(f)| = 1 + (|F_q^\times| - 1)/2 = q/2$.
If n is even then we see that 1 is in the image of f. So there are $q/2 - 2$ different $c \in \mathbb{F}_q \backslash \mathbb{F}_2$ such that P has roots, and for the other $q/2$ values of $c \in \mathbb{F}_q \backslash \mathbb{F}_2$ we have that P is irreducible. So from $x = 0$ we get q solutions, $x = 1$ gives $2q - 1$ solutions, we have $q/2 - 2$ different values of x that give $q - 1$ solutions and for the last $q/2$ values of x they all give $q + 1$ solutions. So in total we have $q^2 + q + 1$ solutions.
At last we can use Lemma 2.2.2 to translate all λ_q back to expressions with classic Legendre symbols to obtain the result as stated in the theorem. □

Chapter 3

Zeta Functions

This chapter focuses on zeta functions. The first section will contain general theory about a classical type of zeta function, namely Dirichlet L-functions. In the second section we will continue with zeta functions related to algebraic varieties. We will then use the point counting theorem 2.1.1 to determine the Hasse-Weil zeta function related to the Generalized Markov Equation. In the last section we will look at various conjectures related to zeta functions and verify those for this particular case.

3.1 General theory

In this section we will be concerned with classical work of Euler, Dirichlet and Riemann in the eighteenth and nineteenth century about the Riemann zeta function and Dirichlet L-functions.

Definition 3.1.1. Let $q \in \mathbb{Z}_{\geq 1}$ and $\chi : \mathbb{Z} \to \mathbb{C}$ a function. If χ satisfies

(i) $\chi(ab) = \chi(a)\chi(b)$ for $a, b \in \mathbb{Z}$.

(ii) $\chi(a) = \chi(b)$ for $a, b \in \mathbb{Z}$ with $a \equiv b \bmod q$.

(iii) $\chi(a) = 0$ if and only if $\gcd(a, q) > 1$.

then we call χ a Dirichlet character modulo q. We call a Dirichlet character χ real if it is a real-valued function. If there exists some positive integer $d < q$ that divides q and a Dirichlet character χ' modulo d such that $\chi(a) = \chi'(a)$ for all a coprime to q then we say that χ is induced by χ'. If such a d does not exist then we say that χ is primitive. We say that a character χ is even or odd if is so as a function.

Example 3.1.2. A trivial example of a Dirichlet character is the function $\chi_0^{(q)}$ defined by $\chi_0^{(q)}(n) = 1$ if $\gcd(q, n) = 1$ and $\chi_0^{(q)}(n) = 0$ for all other n. We call $\chi_0^{(q)}$ the principal character modulo q. △

If we take $a = b = 1$ in the first condition from Definition 3.1.1 and combine this with the third condition we see that $\chi(1) = 1$ for all Dirichlet characters χ. For a Dirichlet character χ we also have $\chi(-n) = \chi(-1)\chi(n)$, and as $\chi(-1)^2 = \chi(1) = 1$ we see that every character is either odd or even. Moreover from Euler's theorem we see that for any Dirichlet character χ modulo q that $\chi(n)$ is either zero or some $\varphi(q)$-th root of unity. So for a Dirichlet character χ modulo q and $n \in \mathbb{Z}$ with $\gcd(q, n) = 1$ we have that $\chi(n)\overline{\chi(n)} = 1$. Moreover the function $\overline{\chi}$ defined by $\overline{\chi}(n) = \overline{\chi(n)}$ also defines a Dirichlet character modulo n and we have that $\chi\overline{\chi} = \chi_0^{(q)}$. For a real Dirichlet character χ we see that $\chi = \overline{\chi}$ and that χ can take only values $0, 1$ and -1.

Example 3.1.3. A non-principal example of a real character modulo an odd prime p is the Legendre symbol as defined in 2.2.1 for $q = p$. Here we consider this as a function from $\mathbb{Z}$ by first reducing modulo p. We will write χ_p for this character. As $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic all Dirichlet characters modulo p are determined by their value at a generator of this group. As real characters can only take values 1 or -1 at a generator, we see that χ_p is the unique non-primitive character modulo p. △

Example 3.1.4. Modulo 4 there are just two characters, the principal character and the character defined by $\chi(3) = -1$. We will denote the non-principal character by χ_4. Moreover we will write χ_8 for the Dirichlet character modulo 8 that sends ± 1 both to 1 and ± 3 to -1. △

Lemma 3.1.5. *Let $n \in \mathbb{Z}_{\neq 0}$ then there is a unique Dirichlet character χ modulo $|4n|$ such that $\chi(p) = \left(\frac{n}{p}\right)$ for all odd primes p.*

Proof. We will first construct a function χ and show that it is a character modulo $|4n|$ and takes the right values on the primes, then we will show that this character is unique.
We write $n = (-1)^s 2^l \prod_{i=1}^{k_1} p_i \prod_{j=1}^{k_2} q_j$ where $l \in \mathbb{Z}_{\geq 0}$, p_i are all primes with $p_i \equiv -1 \bmod 4$ and q_j are all primes with $q_j \equiv 1 \bmod 4$. We choose $s \in \{0, 1\}$. Then define the function $\chi : \mathbb{Z} \to \mathbb{C}$ by

$$\chi(x) = \chi_0^{(4n)}(x)\chi_4(x)^s\chi_8(x)^l \prod_{i=1}^{k_1} \chi_4(x)\chi_{p_i}(x) \prod_{j=1}^{k_2} \chi_{q_j}(x).$$

As the product of a Dirichlet character modulo q_1 and a Dirichlet character modulo q_2 is another Dirichlet character modulo $\operatorname{lcm}(q_1, q_2)$, we see that χ is a character modulo $4n$. Here we use that the χ_8 factor only appears if $l > 0$, and then n is even so $8|4n$.
Now we will use that $\left(\frac{2}{p}\right) = \chi_8(p)$ and we have quadratic reciprocity for Legendre symbols. In particular we note that for a prime p with $p \equiv 1 \bmod 4$ we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \chi_p(q)$ and for a prime p with $p \equiv -1 \bmod 4$ that $\left(\frac{p}{q}\right) = \chi_4(q)\left(\frac{q}{p}\right) = \chi_4(q)\chi_p(q)$ for all odd primes q. At last we note that for odd primes p we also have $\left(\frac{-1}{p}\right) = \chi_4(p)$.
If an odd prime p divides n then we have $\chi_0^{(4n)}(p) = 0 = \left(\frac{n}{p}\right)$. If p is an odd prime that does not divide n then we have that

$$\begin{aligned}\chi(p) &= \chi_0^{(4n)}(p)\chi_4(p)^s\chi_8(p)^l \prod_{i=1}^{k_1} \chi_4(p)\chi_{p_i}(p) \prod_{j=1}^{k_2} \chi_{q_j}(p) \\ &= 1 \cdot \left(\frac{-1}{p}\right)^s \left(\frac{2}{p}\right)^l \prod_{i=1}^{k_1} \left(\frac{p_i}{p}\right) \prod_{j=1}^{k_2} \left(\frac{q_j}{p}\right) = \left(\frac{n}{p}\right).\end{aligned}$$

For uniqueness we use the classical result by Dirichlet that for every $a \in \mathbb{Z}$ with $\gcd(4n, a) = 1$ there is an odd prime p with $p \equiv a \bmod 4n$. Let χ' be a Dirichlet character modulo $4n$ with $\chi'(p) = \left(\frac{n}{p}\right)$ for all odd primes p. Then for any $a \in \mathbb{Z}$ we either have $\gcd(a, 4n) > 1$ and then $\chi'(a) = 0 = \chi(a)$ or we have $\gcd(a, 4n) = 1$ and there is some odd prime p with $p \equiv a \bmod 4n$, and therefore $\chi'(a) = \left(\frac{n}{p}\right) = \chi(a)$. So we see that $\chi' = \chi$ and therefore χ is unique. □

Definition 3.1.6. Let χ be a Dirichlet character modulo q. Then the Gauss sum $\tau(\chi)$ of χ is defined by

$$\tau(\chi) = \sum_{k=1}^{q} \chi(k)e^{2\pi ik/q}.$$

Lemma 3.1.7. *Let χ be a Dirichlet character modulo q and let χ' be the primitive Dirichlet character modulo q'. Then we have that*

(i) $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)}$,

(ii) $|\tau(\chi')| = \sqrt{q'}$,

Proof. For the first statement we can calculate that

$$\chi(-1)\overline{\tau(\chi)} = \overline{\chi}(-1)\sum_{k=1}^{q}\overline{\chi}(k)e^{-2\pi ik/q} = \sum_{k=1}^{q}\overline{\chi}(-k)e^{-2\pi ik/q} = \tau(\overline{\chi}).$$

For the second statement a proof can be found in [11]. □

Remark 3.1.8. For a real Dirichlet character χ we see that $\overline{\chi} = \chi$, so by the first statement in 3.1.7 we see that $\tau(\chi) = \chi(-1)\overline{\tau(\chi)}$, so if χ is even then $\tau(\chi)$ is real and if χ is odd then $\tau(\chi)$ is an imaginary number. If χ is also primitive then the second statement in 3.1.7 tells us there are two possible values $\tau(\chi)$. A classical result about the actual signs of such Gauss sums with characters that come from Legendre symbols can also be found in [11]. It can be shown for characters χ coming from Lemma 3.1.5 that if we take the primitive character χ' that induces χ, then we have $\tau(\chi')$ real and positive if $n > 0$ and $\tau(\chi')$ imaginary with positive imaginary part if $n < 0$.

We will now continue to the first examples of zeta functions that we will consider.

Definition 3.1.9. The L-function of a Dirichlet character χ modulo q is defined by

$$L(s,\chi) = \sum_{n=1}^{\infty}\chi(n)n^{-s}.$$

By comparison with an integral we see that $L(s,\chi)$ converges absolutely for all $s \in \mathbb{C}$ with $\Re(s) > 1$, so this actually defines a function on some open in $\mathbb{C}$. If we take χ to be the principal character modulo 1, then we see that $L(s,\chi) = \zeta(s)$, where is ζ is the Riemann zeta function. Dirichlet L-functions play a big role in the original proof for the Dirichlet prime number theorem. We will also see that they appear in the zeta functions related to the Generalized Markov Equation.

Theorem 3.1.10 (Euler product and Analytic Continuation)**.** *Let χ be a Dirichlet character modulo q and χ' a primitive Dirichlet character modulo q' that induces χ.*

(i) $L(s,\chi) = \prod_p (1-\chi(p)p^{-s})^{-s}$ for $s \in \mathbb{C}$ with $\Re(s) > 1$.

(ii) For $s \in \mathbb{C}$ with $\Re(s) > 1$ we have that

$$L(s,\chi) = L(s,\chi')\prod_{\substack{p\mid q \\ p\nmid q'}}(1-p^{-s}).$$

(iii) If χ' is not principal then $L(s,\chi')$ can be extended to an entire function on $\mathbb{C}$. Moreover $L(s,\chi')$ is non-zero for all $s \in \mathbb{C}$ with $\Re(s) \geq 1$.

(iv) If χ' is principal then $L(s,\chi') = \zeta(s)$ and it can be extended to a holomorphic function on $\mathbb{C}\backslash\{1\}$ with a pole of residue 1 at $s = 1$. Furthermore $L(s,\chi')$ is non-zero for all $s \in \mathbb{C}\backslash\{1\}$ with $\Re(s) \geq 1$.

Proof. A full proof for all these statements can be found in [11]. The first two statements are relatively easy to prove, the last two statements require more work. □

Theorem 3.1.11 (Functional Equation)**.** *Let χ be a primitive Dirichlet character modulo $q \geq 2$.*

(i) Let ζ be the Riemann zeta function. Let

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{1}{2}s\right)\zeta(s).$$

Then ξ has an analytic continuation to $\mathbb{C}$ and ξ satisfies $\xi(s) = \xi(1-s)$ for all $s \in \mathbb{C}$.

(ii) If χ is even let

$$\xi(s,\chi) = \left(\frac{q}{\pi}\right)^{s/2} \Gamma\left(\frac{1}{2}s\right) L(s,\chi) \text{ and } c(\chi) = \frac{\sqrt{q}}{\tau(\chi)}.$$

Else if χ is odd let

$$\xi(s,\chi) = \left(\frac{q}{\pi}\right)^{(s+1)/2} \Gamma\left(\frac{1}{2}(s+1)\right) L(s,\chi) \text{ and } c(\chi) = \frac{i\sqrt{q}}{\tau(\chi)}.$$

Then $\xi(s,\chi)$ has an analytic continuation to $\mathbb{C}$ and it satisfies $\xi(1-s,\overline{\chi}) = c(\chi)\xi(s,\chi)$.

Proof. A proof for the functional equation can be found in [10]. We note that in general it follows from Lemma 3.1.7 that $|c(\chi)| = 1$, and by Remark 3.1.8 we even have $c(\chi) = 1$ for primitive characters that induce characters that we see in Lemma 3.1.5. □

3.2 Zeta functions of varieties

In this section we will proceed to the twentieth century and consider two types of zeta functions related to algebraic varieties and schemes.

Definition 3.2.1. Let X be a scheme of finite type over the integers. The arithmetic zeta function ζ_X is defined by

$$\zeta_X(s) = \prod_{x\in|X|} (1 - N(x)^{-s})^{-1},$$

where $|X|$ denotes the set of closed points of X and $N(x)$ denotes the cardinality of the residue field of x.

In this thesis we often look at affine schemes, that is to say that we consider rings R isomorphic to $\mathbb{Z}[x_1,\dots,x_n]/I$, and consider $X = \operatorname{Spec}(R)$. Then the closed points of X are the maximal ideals $\mathfrak{m}$ of R and $N(\mathfrak{m})$ is the number of elements in $R/\mathfrak{m}$. We note that this number must be finite. To see this we note that $\mathfrak{m}$ can also be seen as an ideal of $\mathbb{Z}[x_1,\dots,x_n]$ with $I \subset \mathfrak{m}$. Since $\mathfrak{m}$ is maximal we see that $k := \mathbb{Z}[x_1,\dots,x_n]/\mathfrak{m}$ must be a field, and as $\mathbb{Q}$ is not finitely generated over $\mathbb{Z}$ as an algebra we must have that this field is in characteristic p for some prime p. So k is a field that is finitely generated as an $\mathbb{F}_p$-algebra. By Zariski's lemma this means that k is a finite field extension of $\mathbb{F}_p$ and therefore k is finite. For a maximal ideal $\mathfrak{m}$ in $\mathbb{F}_p[x_1,\dots,x_n]$ we will denote $d_{\mathfrak{m}} = [\mathbb{F}_p[x_1,\dots,x_n]/\mathfrak{m} : \mathbb{F}_p]$, so we have $N(\mathfrak{m}) = p^{d_{\mathfrak{m}}}$.
We write X_p for the variety $\operatorname{Spec}(\mathbb{Z}[x_1,\dots,x_n]/(I+(p))) = \operatorname{Spec}(\mathbb{F}_p[x_1,\dots,x_n]/I)$. As every maximal ideal in R contains a prime p, we see that we can group the closed points of X by which prime they contain, and therefore we get that $\zeta_X(s) = \prod_p \zeta_{X_p}(s)$.

Example 3.2.2. For $X = \operatorname{Spec}(\mathbb{Z})$ the closed points correspond with all maximal ideals of $\mathbb{Z}$, so we get that

$$\zeta_X(s) = \prod_{x\in|X|} (1 - N(x)^{-s})^{-1} = \prod_p (1-p^{-s})^{-1} = \zeta(s).$$

Here $\zeta(s)$ is the Riemann zeta function. △

Definition 3.2.3. Let X be a variety over some finite field $\mathbb{F}_q$ with q elements. We write $X(\mathbb{F}_{q^m})$ for the set of points in X defined over $\mathbb{F}_{q^m}$. Then Weil's zeta function $Z(X,T)$ attached to the variety X over $\mathbb{F}_q$ is defined by

$$Z(X,T) = \exp\left(\sum_{m=1}^{\infty} \frac{|X(\mathbb{F}_{q^m})|}{m} T^m\right).$$

Weil's zeta functions are the central object in the Weil Conjectures, which sparked a lot of interest in the second half of the twenteeth century. Although these are called the Weil Conjectures, they are proven. The Weil Conjectures for instance say that $Z(X,T)$ is a rational function in T and satisfies a function equation similar to 3.1.11. We will now show how the arithmetic zeta function and Weil's zeta function are related.

Definition 3.2.4. Let $R = \mathbb{F}_p[x_1, \ldots, x_n]$ and $\sigma : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ be the Frobenius map defined by $x \mapsto x^p$. For $\alpha \in \overline{\mathbb{F}}_p^n$ we define the cycle ξ_α of α to be the set $\{\sigma^i(\alpha) : i \in \mathbb{Z}\}$.

Let $\alpha \in \overline{\mathbb{F}}_p^n$ and write $k = [\mathbb{F}_p(\alpha_1, \ldots, \alpha_n) : \mathbb{F}_p]$. It is well-known that σ generates the Galois group $\mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$ and has order k if restricted to $\mathbb{F}_{p^k}$. So we see that $\sigma^k(\alpha) = \alpha$, and as by definition of k we have that $\sigma^\ell(\alpha) \neq \alpha$ for $\ell \in \{1, \ldots, k-1\}$, as that would imply that $[\mathbb{F}_p(\alpha_1, \ldots, \alpha_n) : \mathbb{F}_p] < k$. So we see that $|\xi_\alpha| = k$.
For an ideal I in R and $\alpha \in V(I)$, we have for all $f \in I$ that $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, so σ maps $V(I)$ to itself. Therefore we can also talk about the set of cycles in $V(I)$. Moreover we see that the cycles form a partition of $V(I)$, as two cycles containing the same element must be the same cycle and by construction there is a cycle ξ_α for every $\alpha \in V(I)$.

Lemma 3.2.5. *Let $R = \mathbb{F}_p[x_1, \ldots, x_n]$ and I some prime ideal in R. The map from maximal ideals $\mathfrak{m}$ containing I to the set of cycles in $V(I)$ defined by $\mathfrak{m} \mapsto V(\mathfrak{m})$ is a bijection.*

Proof. Let $\alpha \in V(I)$, then we define the $\mathbb{F}_p$-algebra morphism $\varphi_\alpha : R \to \overline{\mathbb{F}}_p$ by $x_i \mapsto \alpha_i$ for all i. We define $\mathfrak{p}(\alpha) = \ker \varphi_\alpha$. Then we have $R/\mathfrak{p}(\alpha) \cong \varphi_\alpha(R) = \mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$. As this is a field we see that $\mathfrak{p}(\alpha)$ is maximal and $N(\mathfrak{p}(\alpha)) = p^{|\xi_\alpha|}$. Moreover we see that $\mathfrak{p}(\alpha) = \mathfrak{p}(\sigma(\alpha))$, as for any $f \in R$ we have $f(\alpha) = 0$ if and only if $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$, as σ is a bijection. So for a cycle ξ with $\alpha \in \xi$ we define $\mathfrak{p}(\xi) := \mathfrak{p}(\alpha)$, and this is well-defined. Since α vanishes on I we see that $I \subset \mathfrak{p}(\alpha)$ and by construction we have $\alpha \in V(\mathfrak{p}(\alpha))$. In particular this also gives that $\xi_\alpha \subseteq V(\mathfrak{p}(\alpha))$ as $\mathfrak{p}(\alpha) = \mathfrak{p}(\sigma(\alpha))$.
Now let $\mathfrak{m}$ be a maximal ideal of R containing I and $\overline{\mathfrak{m}} = \overline{\mathbb{F}}_p \otimes_{\mathbb{F}_p} \mathfrak{m}$. Because a field extension is faithfully flat we see that $\overline{\mathfrak{m}} = \mathfrak{m}\overline{\mathbb{F}}_p$. Then $\overline{\mathfrak{m}}$ is an ideal in $\overline{\mathbb{F}}_p[x_1, \ldots, x_n]$, and we have that

$$\frac{\overline{\mathbb{F}}_p[x_1, \ldots, x_n]}{\overline{\mathfrak{m}}} \cong \overline{\mathbb{F}}_p \otimes_{\mathbb{F}_p} \frac{\mathbb{F}_p[x_1, \ldots, x_n]}{\mathfrak{m}} \cong \overline{\mathbb{F}}_p \otimes_{\mathbb{F}_p} \mathbb{F}_{p^{d_\mathfrak{m}}} \cong \left(\overline{\mathbb{F}}_p\right)^{d_\mathfrak{m}},$$

so $V(\mathfrak{m})$ contains $d_\mathfrak{m}$ points over $\overline{\mathbb{F}}_p$. Now for $\alpha \in V(\mathfrak{m})$ we see that $\mathfrak{m} \subseteq \mathfrak{p}(\alpha)$ as α vanishes on $\mathfrak{m}$ so $\mathfrak{m} \subseteq \ker \varphi_\alpha$. Since $\mathfrak{m}$ is maximal this means that $\mathfrak{m} = \mathfrak{p}(\alpha)$. So $\xi_\alpha \subseteq V(\mathfrak{m})$ and $|V(\mathfrak{m})| = d_\mathfrak{m} = |\xi_\alpha|$ so $V(\mathfrak{m}) = \xi_\alpha$.
So since $\mathfrak{p}(\xi)$ is a maximal ideal we see that $V(\mathfrak{p}(\xi))$ is some cycle and also contains the cycle ξ, so $V(\mathfrak{p}(\xi)) = \xi$.
So we have now seen that $V(\mathfrak{m})$ is indeed a cycle, and as $I \subset \mathfrak{m}$ we get $V(\mathfrak{m}) \subset V(I)$ so $V(\mathfrak{m})$ is a cycle in $V(I)$. For any cycle ξ we also have that $\mathfrak{p}(\xi)$ is a maximal ideal containing I in R. We saw that $\mathfrak{p}(V(\mathfrak{m})) = \mathfrak{m}$ and $\xi = V(\mathfrak{p}(\xi))$ so these are inverses, and we have a bijection. □

Corollary 3.2.6. *For X an affine scheme over $\mathbb{F}_p$ of finite type we have that*

$$|X(\mathbb{F}_{p^k})| = \sum_{\substack{x \in |X| \\ d_x \text{ divides } k}} d_x.$$

Proof. In the bijection of the last lemma, we saw that maximal ideals $\mathfrak{m}$ are sent to cycles ξ with $|\xi| = d_x$. Moreover we have $\alpha \in \mathbb{F}_{p^k}$ if and only if $\sigma^k(\alpha) = \alpha$. So we see that the cycle ξ_α is contained in $X(\mathbb{F}_{p^k})$ if and only if $|\xi_\alpha|$ divides k. $X(\mathbb{F}_{p^k})$ is a disjoint union of all cycles ξ with $|\xi|$ dividing k. Therefore we get that

$$|X(\mathbb{F}_{p^k})| = \sum_{\substack{\xi \text{ cycle in } V(I) \\ |\xi| \text{ divides } k}} |\xi| = \sum_{\substack{x \in |X| \\ d_x \text{ divides } k}} d_x.$$

□

Lemma 3.2.7. *Let X be an affine scheme and p some prime. Let $\zeta_{X_p}(s)$ be the arithmetic zeta function of X_p and $Z(X_p, T)$ Weil's zeta function. Then we have that*

$$\zeta_{X_p}(s) = Z(X_p, p^{-s}). \tag{3.2.1}$$

Proof. We use Corollary 3.2.6 and see that

$$\begin{aligned}\log \zeta_{X_p}(s) &= -\sum_{x\in|X|} \log(1 - N(x)^{-s}) = \sum_{x\in|X|}\sum_{k=1}^{\infty} \frac{1}{k} N(x)^{-ks} = \sum_{x\in|X|}\sum_{k=1}^{\infty} \frac{1}{k} p^{-d_x ks} \\ &= \sum_{m=1}^{\infty} p^{-ms}\Big(\sum_{x\in|X|, d_x|m} \frac{d_x}{m}\Big) = \sum_{m=1}^{\infty} \frac{p^{-ms}}{m}|X(\mathbb{F}_{p^m})| = \log Z(X_p, p^{-s}).\end{aligned}$$

□

Example 3.2.8. We consider $X = \mathbb{A}^n$ over $\mathbb{Z}$ we have $R = \mathbb{Z}[x_1, \ldots, x_n]$. If we try to use Definition 3.2.1 to calculate $\zeta_X(s)$, we require knowledge about all maximal ideals in R which seems to be non-trivial. However we can use Lemma 3.2.7, and as $|X(\mathbb{F}_{p^m})| = |\mathbb{F}_{p^m}|^n = p^{nm}$ we see that

$$\begin{aligned}\zeta_X(s) = \prod_p \zeta_{X_p}(s) &= \prod_p \exp\Big(\sum_{m=1}^{\infty} \frac{p^{-ms}}{m} p^{nm}\Big) = \prod_p \exp\Big(\sum_{m=1}^{\infty} \frac{p^{m(n-s)}}{m}\Big) \\ &= \prod_p (1 - p^{n-s})^{-1} = \zeta(s-n).\end{aligned}$$

△

Example 3.2.9. For $X = \mathbb{P}^n$ we can decompose $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^0$ as varieties, so in particular we also have that the closed points of X can be partitioned in this way. So we see that

$$\zeta_X(s) = \prod_{x\in|\mathbb{P}^n|} (1 - N(x)^{-s})^{-1} = \prod_{k=0}^{n}\prod_{x\in|\mathbb{A}^k|} (1 - N(x)^{-s}) = \prod_{k=0}^{n} \zeta(s-k).$$

△

In [29] for instance convergence of the arithmetic zeta function is discussed. In particular, $\zeta_X(s)$ has a pole at $s = \dim(X)$ and converges for $s \in \mathbb{C}$ with $\Re(s) > \dim(X)$. Also a meromorphic extension to $s \in \mathbb{C}$ with $\Re(s) > \dim(X) - \frac{1}{2}$ is discussed together with the poles in this region. We note that the dimension is defined as the Krull dimension of the ring, so for $X = \operatorname{Spec}(\mathbb{Z}[x, y, z]/(x^2 + y^2 + z^2 - 3xyz))$ we have $\dim(X) = 3$, contrary to the geometrical dimension 2 corresponding to the variety defined over $\mathbb{Q}$.

Remark 3.2.10. The arithmetic zeta function is defined for schemes over the integers. However for geometrical purposes one would also like to study a scheme X over the rationals. One could use a model $\mathcal{X}$ over the integers and try to define the zeta function of X by the arithmetic zeta function of $\mathcal{X}$. However this would not be well-defined as for instance $X^2 + Y^2 = 1$ and $X^2 + Y^2 = 9$ are models of the same variety over $\mathbb{Q}$, but have different reductions modulo 3. The Hasse-Weil zeta function attached to X does exactly this, as defined in [18]. If we have a model $\mathcal{X}$ with good reduction p, the factor in the Euler product of the Hasse-Weil zeta function is the same as the arithmetic zeta function of $\mathcal{X}_p$. To define the correct factors at primes with bad reduction cohomology theory is needed. For smooth varieties over $\mathbb{Q}$, bad reduction only happens at finitely many p, so one can find the Hasse-Weil zeta function up to finitely many polynomial factors in p^{-s} for the bad primes p without use of cohomology.

3.3 Markov surfaces

We will now combine the results in 2.1.1 and the relation in 3.2.7 to calculate the arithmetic zeta function corresponding to the scheme defined by the Generalized Markov Equation (Equation (1.2.1)) over the integers.

Example 3.3.1. We will first make the calculation for the scheme $X = W_{3,0}$ defined by classical Markov Equation. First we look at X_2. Over $\mathbb{F}_{2^n}$ there are $2^{2n}+1$ solutions, so we get that

$$\zeta_{X_2}(s) = \exp\left(\sum_{m=1}^{\infty} \frac{2^{-ms}(2^{2m}+1)}{m}\right) = \frac{1}{(1-2^{2-s})(1-2^{-s})}$$

. For $p=3$ we see that there are 3^{2n} points over $\mathbb{F}_{3^n}$. So we get $\zeta_{X_3}(s) = (1-3^{2-s})^{-1}$. For $p>3$ we have exactly $p^{2n}+1+3p^n\left(\frac{-1}{p}\right)^n$ points over $\mathbb{F}_{p^n}$, so we see that

$$\zeta_{X_p}(s) = \exp\left(\sum_{m=1}^{\infty} \frac{p^{2m-ms}+p^{-ms}+3\left(\left(\frac{-1}{p}\right)p^{1-s}\right)^m}{m}\right) = \frac{1}{(1-p^{2-s})(1-p^{-s})(1-\left(\frac{-1}{p}\right)p^{1-s})^3}.$$

Moreover we note that $\left(\frac{-1}{p}\right) = \chi_4(p)$ for odd primes p, which we used in 3.1.5, and therefore we see that

$$\begin{aligned}\zeta_X(s) = \prod_p \zeta_{X_p}(s) &= (1-3^{-s})(1+3^{1-s})^3 \prod_p \frac{1}{(1-p^{2-s})(1-p^{-s})(1-\left(\frac{-1}{p}\right)p^{1-s})^3} \\ &= (1-3^{-s})(1+3^{1-s})^3\zeta(s-2)\zeta(s)L(s-1,\chi_4)^3.\end{aligned}$$

Here we have used the product expansions from Theorem 3.1.10 for the last equality. △

Example 3.3.2. For $a \in \mathbb{Z}_{\neq 0}$ we see for X defined by $W_{a,0}$ that there are p^{2n} points over $\mathbb{F}_{p^{2n}}$ if p divides a and $p^{2n}+1+3p^n\chi_4(p)^n$ points over $\mathbb{F}_{p^{2n}}$ if p does not divide a. With a calculation similar to the case $a=3$ we get

$$\zeta_X(s) = \zeta(s-2)\zeta(s)L(s-1,\chi_4)^3 \prod_{p|a}(1-p^{-s})(1-\chi_4(p)p^{1-s})^3.$$

△

Theorem 3.3.3. *Let $b \in \mathbb{Z}\backslash\{0,4\}$ and consider the scheme X defined by $W_{1,b}$. Let χ be the character that we get from Lemma 3.1.5 for $n = b-4$ and χ' the character that we get from that lemma with $n = b^2-4b$, then we have that*

$$\zeta_X(s) = \zeta(s-2)\zeta(s)L(s-1,\chi)^3L(s-1,\chi')P(2^{-s}). \tag{3.3.1}$$

Here $P(x) = 1$ if b is even and $P(x) = (1+2x)^{-1}$ if b is odd.

Proof. As $a=1$ we can use remark 2.1.2 to find $\zeta_{X_p}(s)$ for $p>2$. Let χ and χ' be the characters as defined in the theorem. Then we see that

$$\begin{aligned}\zeta_{X_p}(s) = \exp\left(\sum_{m=1}^{\infty}\frac{|X(\mathbb{F}_{p^m})|}{m}p^{-ms}\right) &= \exp\left(\sum_{m=1}^{\infty}\frac{p^{2m}+1+3(p\chi(p))^m+(p\chi'(p))^m}{m}p^{-ms}\right) \\ &= \frac{1}{(1-p^{2-s})(1-p^{-s})(1-\chi(p)p^{1-s})^3(1-\chi'(p)p^{1-s})}.\end{aligned}$$

Moreover for $p=2$ we see for even b that $\zeta_{X_2}(s) = ((1-2^{-s})(1-2^{2-s}))^{-1}$. As χ, χ' are both characters modulo some even number we see that $\chi(2) = \chi'(2) = 0$, so we see that

$$\zeta_X(s) = \prod_p \zeta_{X_p}(s) = \zeta(s-2)\zeta(s)L(s-1,\chi)^3L(s-1,\chi').$$

If b is odd we see that $\zeta_{X_2}(s) = ((1-2^{-s})(1+2^{1-s})(1-2^{2-s}))^{-1}$, which gives the same calculation except for an extra factor $(1+2^{1-s})^{-1}$ □

Remark 3.3.4. The characters χ and χ' are often not primitive. For b odd and χ' the character as defined above, we note that there is a character χ_1 modulo $|b^2 - 4b|$ that induces χ'. In particular we even have that $\chi_1(2) = -1$, so if we replace $L(s-1, \chi')$ by $L(s-1, \chi_1)$ for odd b we can forget about $P(2^{-s})$.

We have already seen that the variety $W_{a,b}$ is isomorphic over $\mathbb{Q}$ to the W_{1,a^2b}, but this isomorphism does not work over $\mathbb{Z}$ as we have to divide by a. But for all primes p that do not divide a the isomorphism exists over $\overline{\mathbb{F}}_p$, so the Euler factors agree for almost all primes. To calculate the arithmetic zeta function for the scheme defined by $W_{a,b}$ we can start with the zeta function for W_{1,a^2b} and then correct the factors at all primes dividing a. Therefore we see that for X the scheme over $\mathbb{Z}$ defined by $W_{a,b}$ Equation 3.3.1 holds up to some rational function in the variables p^{-s} for all primes p dividing $2a$.
Although we have all tools to calculate the arithmetic zeta function, we would need more information about the cohomology at bad primes to calculate the Hasse-Weil zeta function. To circumvent this one idea to find the Hasse-Weil zeta function is to localize at all primes p_i with bad reduction, so there are no closed points contained such primes.

$$\frac{\mathbb{Z}[X, Y, Z]}{(X^2 + Y^2 + Z^2 - aXYZ - b)} \tag{3.3.2}$$

$$\frac{\mathbb{Z}[X, Y, Z, p_1^{-1}, \ldots, p_n^{-1}]}{(X^2 + Y^2 + Z^2 - aXYZ - b)} \tag{3.3.3}$$

For this new scheme the reduction at a prime p_i contains no closed points so the corresponding Euler factor is 1. So to find the Hasse-Weil zeta function of this scheme we can use Theoren 3.3.3 for W_{1,a^2b} and remove all factors for the primes p_i.

Example 3.3.5. We consider the scheme defined by $W_{3,5}$. We use Theorem 3.3.3 for $b = 45$ to get the correct answer at all primes except for the bad primes $2, 3, 5$. We note that χ is the character modulo 164 induced by the Legendre symbol $\left(\frac{\cdot}{41}\right)$. As these have the same value at all odd primes we can use $\chi(x) = \left(\frac{x}{41}\right)$ and still have the correct factors at all good primes. For χ we get a character modulo $4 \cdot 45 \cdot 41 = 7380$. As we have $\left(\frac{45 \cdot 41}{p}\right) = \left(\frac{5 \cdot 41}{p}\right)$ for all good primes p we see that this character is induced by a character modulo $4 \cdot 5 \cdot 41$. Moreover this character is induced by a character modulo $5 \cdot 41 = 205$, and these agree at all good primes. Therefore we can also use $\chi'(x) = \left(\frac{x}{5}\right)\left(\frac{x}{41}\right)$ and have the same values at all good primes.
We know that for good primes p we indeed get the Euler factor

$$\zeta_{X_p}(s) = \frac{1}{(1 - p^{2-s})(1 - p^{-s})(1 - \chi(p)p^{1-s})^3(1 - \chi'(p)p^{1-s})}.$$

For $p = 2$ we get the Euler factor $((1 - 2^{2-s})(1 + 2^{1-s})(1 - 2^{-s}))^{-1}$, for $p = 3$ we get the factor $((1 - 3^{2-s})(1 - 3^{1-s}))^{-1}$ and at $p = 5$ we get $((1 - 5^{2-s})(1 - 5^{-s})(1 - 5^{1-s})^3)^{-1}$. So if we put this together we get

$$\zeta_X(s) = \prod_p \zeta_{X_p}(s) = \prod_p (1 - p^{-s})^{-1} \prod_p (1 - p^{2-s})^{-1} \prod_{p>3} (1 - \chi(p)p^{1-s})^{-3} \prod_{\substack{p \\ p \neq 3}} (1 - \chi'(p)p^{1-s})^{-1} \tag{3.3.4}$$

$$= \zeta(s)\zeta(s-2)L(s-1, \chi)^3 L(s-1, \chi')(1 - 2^{1-s})^3(1 + 3^{1-s})^3(1 - 3^{1-s}). \tag{3.3.5}$$

If we would instead want to find the Hasse-Weil zeta function $\zeta^{HW}(s)$ for the spectrum of the ring in Equation 3.3.3, then we get

$$\zeta^{HW}(s) = \prod_{p>5} \zeta_{X_p}(s) = \frac{\zeta(s)\zeta(s-2)L(s-1, \chi)^3 L(s-1, \chi')}{\prod_{p \leq 5}(1 - p^{2-s})^{-1}(1 - p^{-s})^{-1}(1 - \chi(p)p^{1-s})^{-3}(1 - \chi'(p)p^{1-s})^{-1}}.$$

△

3.4 Conjectures

Although zeta functions have been studied a lot in the last hunderd years, there are still a lot of conjectures related to zeta functions that have not been proven. As zeta functions are inspired by the Riemann zeta function there are various properties of the Riemann zeta function that are also expected to hold for other types of zeta functions. We will consider two conjectures and verify these for the zeta functions of Markov surfaces. The first conjecture is due to Hasse and Weil and was posed during the late thirties of the twentieth century [17]. In the first formulation this conjecture was only posed for curves. We use a more general and modern formulation of the conjecture described by Serre. For a more precise description of the functional equation we refer to the source.

Conjecture 3.4.1 (Hasse–Weil, [27]). *The Hasse-Weil zeta function ζ attached to some algebraic variety X has a meromorphic continuation to all of $\mathbb{C}$ and ζ satisfies a functional equation relating values at s and $\dim(X) + 1 - s$.*

Theorem 3.4.2. *The Hasse-Weil conjecture holds for the variety $W_{a,b}$.*

Proof. We can use 3.3.3 and see what ζ_X is up to some polynomial in p^{-s} for all primes p that divide a. We can use the second property in 3.1.10 to change characters to primitive characters by factoring out some rational functions in p^{-s} for primes dividing the periods of the Dirichlet characters. If we combine these two observations we see that we can write

$$\zeta_X(s) = \zeta(s-2)\zeta(s)L(s-1,\chi_1)^3 L(s-1,\chi_2) \prod_{p \mid 2ab(b-4)} P_p(p^{-s})$$

for rational functions $P_p(X)$ and primitive characters χ_1 and χ_2.
Now the first part follows from the third and fourth point in 3.1.10. For the second part we complete the zeta function to a function ξ by multiplying out $\prod_{p \mid 2ab(b-4)} P_p(p^{-s})$ and adding the correct prefactors that are also appear in 3.1.11. We have $c(\chi_1) = c(\chi_2) = 1$ by Remark 3.1.8. So we see that $\xi(s) = \xi_1(s-2)\xi_1(s)\xi_2(s-1)^3\xi_3(s-1)$ where we have $\xi_i(s) = \xi_i(1-s)$ for all i. Then we see that

$$\xi(3-s) = \xi_1(1-s)\xi_1(3-s)\xi_2(2-s)^3\xi_3(2-s) = \xi_1(s)\xi_1(s-2)\xi_2(s-1)^3\xi_3(s-1) = \xi(s).$$

As $\dim(W_{a,b}) = 2$ this is exactly the functional equation we wanted. □

The second conjecture we will look at is due to Tate [31]. We emphasize that the dimension of a scheme over $\mathbb{Z}$ is the Krull dimension, as opposed to the Hasse-Weil conjecture where we have the dimension of the variety.

Conjecture 3.4.3 (Tate). *If X is a regular scheme of finite type over $\mathbb{Z}$, then the order of $\zeta_X(s)$ at the point $s = \dim(X) - 1$ is equal to $Rank(\mathcal{O}_X^\times) - Rank(Pic(X))$.*

Instead of the affine variety $W_{a,b}$ we will now consider the projective closure $P_{a,b}$ as seen in Lemma 1.2.5. This lemma tells us that $P_{a,b}$ is smooth over $\mathbb{Q}$ as long as $a^2b \notin \{0,4\}$. We will keep the convention that a, b are integers such that $a^2b \notin \{0,4\}$ throughout the remainder of this chapter.

Theorem 3.4.4. *The Tate conjecture holds for the scheme $P_{a,b}$.*

Lemma 3.4.5. *The arithmetic zeta function $\zeta_{P_{a,b}}$ is related to $\zeta_{W_{a,b}}$ by*

$$\zeta_{P_{a,b}}(s) = \zeta(s-1)^3\zeta_{W_{a,b}}(s)$$

Proof. Let $M_q(a,b)$ be the number of points in $P_{a,b}$ over $\mathbb{F}_q$. If we take the chart $t=1$ we get $W_{a,b}$ back so we see that $M_q(a,b)-N_q(a,b)$ is equal to the number of points in the chart $t=0$. If we combine this with $t(x^2+y^2+z^2)=axyz+bt^3$ that defines $P_{a,b}$ we get $axyz=0$. As $a^2b\neq 0$ we see that this is equivalent to $xyz=0$. As $xyz=0$ is the union of three lines we see that this consists of $3q$ points, namely three times a line with $q+1$ points and three intersection points that are counted double. So we see that $M_q(a,b)=3q+N_q(a,b)$, and we can use Lemma 3.2.7 to see that

$$\begin{aligned}\zeta_{P_{a,b}}(s) &= \prod_p \exp\left(\sum_{m=1}^{\infty}\frac{p^{-ms}}{m}M_{p^m}(a,b)\right)=\prod_p \exp\left(\sum_{m=1}^{\infty}\frac{p^{-ms}}{m}(N_{p^m}(a,b)+3p^m)\right)\\ &= \prod_p \exp\left(\sum_{m=1}^{\infty}\frac{p^{-ms}}{m}N_{p^m}(a,b)\right)\prod_p \exp\left(\frac{3p^{m-ms}}{m}N_{p^m}(a,b)\right)=\zeta_{W_{a,b}}(s)\zeta(s-1)^3.\end{aligned}$$

□

Remark 3.4.6. From this lemma we also see that the Hasse-Weil conjecture holds for $P_{a,b}$, as we can add the three extra factors to complete $\zeta(s-1)^3$ which will then have the same symmetry as the ξ_2 and ξ_3 factors.

Lemma 3.4.7. *For $P_{1,b}$ and $W_{1,b}$ the Picard group depends only on the extension $\mathbb{Q}(\sqrt{b-4},\sqrt{b})$ of $\mathbb{Q}$ and all cases are given by Equation 3.4.1 to 3.4.5.*

$$\sqrt{b-4},\sqrt{b}\in\mathbb{Q} \qquad \mathrm{Pic}(P_{1,b})\cong\mathbb{Z}^7 \qquad \mathrm{Pic}(W_{1,b})\cong\mathbb{Z}^4 \tag{3.4.1}$$
$$\sqrt{b-4}\in\mathbb{Q},\sqrt{b}\notin\mathbb{Q} \qquad \mathrm{Pic}(P_{1,b})\cong\mathbb{Z}^6 \qquad \mathrm{Pic}(W_{1,b})\cong\mathbb{Z}^3 \tag{3.4.2}$$
$$\sqrt{b-4}\notin\mathbb{Q},\sqrt{b}\in\mathbb{Q} \qquad \mathrm{Pic}(P_{1,b})\cong\mathbb{Z}^3 \qquad \mathrm{Pic}(W_{1,b})\cong 0 \tag{3.4.3}$$
$$\sqrt{b-4}\notin\mathbb{Q},\sqrt{b(b-4)}\in\mathbb{Q} \qquad \mathrm{Pic}(P_{1,b})\cong\mathbb{Z}^4 \qquad \mathrm{Pic}(W_{1,b})\cong\mathbb{Z} \tag{3.4.4}$$
$$\sqrt{b-4},\sqrt{b},\sqrt{b(b-4)}\notin\mathbb{Q} \qquad \mathrm{Pic}(P_{1,b})\cong\mathbb{Z}^3 \qquad \mathrm{Pic}(W_{1,b})\cong 0 \tag{3.4.5}$$

Proof. As the Picard group of a variety is defined over $\mathbb{Q}$ we can use Lemma 1.2.3 to rescale $P_{a,b}$ to P_{1,a^2b} as an isomorphism of Picard groups. We will write $\overline{P_{a,b}}=\overline{\mathbb{Q}}\otimes_{\mathbb{Q}}P_{a,b}$. For the proof of this lemma we mainly rely on the computations from [7].
As $\overline{P_{a,b}}$ is a smooth cubic surface in $\mathbb{P}^3$ we have by theorem V.4.8 in [15] that $\mathrm{Pic}(\overline{P_{a,b}})\cong\mathbb{Z}^7$. In [7] they explicitly give seven generators of $\mathrm{Pic}(\overline{P_{a,b}})$ that are defined over $\mathbb{Q}(\sqrt{b},\sqrt{b-4})$. In the article they describe how the Galois group of this extension over $\mathbb{Q}$ acts on these generators. By [3] we see for projective varieties that the Picard group over $\mathbb{Q}$ is isomorphic to the Galois-fixed subgroup of the Picard group over $\overline{\mathbb{Q}}$.
There are at most four elements in $\mathrm{Gal}(\mathbb{Q}(\sqrt{b},\sqrt{b-4})/\mathbb{Q})$. Let σ be the element that sends $\sqrt{b-4}$ to $-\sqrt{b-4}$ and fixes $\sqrt{b}$. This only exists if $b-4$ and b^2-4b are not squares. Moreover we let τ be the element that fixes $\sqrt{b-4}$ and sends $\sqrt{b}$ to $-\sqrt{b}$. This only exists if b and $b(b-4)$ are both not squares. At last the element we define ρ as the element that sends $\sqrt{b}$ to $-\sqrt{b}$ and $\sqrt{b-4}$ to $-\sqrt{b-4}$. This only exists if both b and $b-4$ are not squares. If all three exist we note that $\rho=\sigma\tau$ and all three commute. In the article it is shown that if they exist σ and τ act on the basis as

$$\sigma=\begin{pmatrix}-1&-1&-1&0&-1&-1&-2\\-1&-1&-1&-1&0&-1&-2\\-1&-1&-1&-1&-1&0&-2\\0&-1&-1&-1&-1&-1&-2\\-1&0&-1&-1&-1&-1&-2\\-1&-1&0&-1&-1&-1&-2\\2&2&2&2&2&2&5\end{pmatrix},\quad \tau=\begin{pmatrix}1&0&0&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&0&-1&-1&-1\\0&0&0&-1&0&-1&-1\\0&0&0&-1&-1&0&-1\\0&0&0&1&1&1&2\end{pmatrix}$$

and ρ as the product of these two matrices. As these matrices are their own inverse we see from the trace that σ fixes a three-dimensional subspace and τ a six-dimensional subspace, moreover one can calculate that ρ fixes a four-dimensional subspace. For all five options of $b, b-4, b(b-4)$ being squares or non-squares (if two of the three are a square the last one must also be a square) we can see which of σ, τ, ρ actually exist in the Galois group and calculate the Galois-fixed subgroup of $\mathrm{Pic}(\overline{P_{1,b}})$ to determine $\mathrm{Pic}(P_{1,b})$.
We saw in the proof of Lemma 3.4.5 that $P_{1,b}$ is the union of $W_{1,b}$ and three lines. As these lines have codimension 1 in the surface $P_{1,b}$ we can use the exact sequence from theorem II.6.5 in [15] to see what happens when we remove these lines. In [7] it is also shown for the three lines $L_1 : x = t = 0$, $L_2 : y = t = 0$ and $L_3 : z = t = 0$ in $P_{a,b}$ that they correpond respectively to $e_7 - e_1 - e_4$, $e_7 - e_2 - e_5$ and $e_7 - e_3 - e_6$ in $\mathrm{Pic}(P_{1,b})$ where we use the same basis as we used for σ and τ. We get that

$$\mathrm{Pic}(W_{1,b}) \cong \mathrm{Pic}(P_{1,b})/\langle e_7 - e_1 - e_4, e_7 - e_2 - e_5, e_7 - e_3 - e_6\rangle.$$

□

Proof of Theorem 3.4.4. As $P_{a,b}$ is a projective variety, we see that $\mathcal{O}_X^\times$ consists only of constant functions. As we have a scheme over $\mathbb{Z}$ we see that the only invertible constants are ± 1 so we have $\mathrm{Rank}(\mathcal{O}_X^\times) = 0$. We also note that we are interested in the behaviour of $\zeta_{P_{a,b}}(s)$ around the point $s = \dim(P_{a,b}) - 1 = 2$. For this we need ideas from 3.3.3 but we have to be a bit more careful in what polynomials appear extra. We use Lemma 3.4.5 to relate this to the behaviour of $\zeta_{W_{a,b}}(s)$ around $s = 2$.
As we have a q^2 term in every possibility in 2.1.1, we see that $\zeta_{W_{a,b}}(s)$ differs from $\zeta(s)\zeta(s-1)L(s-1,\chi)^3L(s-1,\chi')$ only by factors of the form $1 \pm p^{1-s}$ or $1 \pm p^{-s}$ for primes p dividing $2a$. But at $s = 2$ these factors are non-zero, so we see that the order of the function at $s = 2$ does not change by these factors. This also means that we can assume $a = 1$, as the difference between in zeta functions of the affine varieties $W_{a,b}$ and W_{1,a^2b} only differs by factors that are non-zero at $s = 2$.
Moreover we can also assume χ and χ' to be primitive characters by the second point in Theorem 3.1.10 and the fact that these factors are non-zero at $s = 1$ (as the variable change $s \to s-1$ appears in the factors).
As $\zeta(2) = \frac{\pi^2}{6}$ and $\zeta(0) = -\frac{1}{2}$ we see that

$$\begin{aligned} \mathrm{ord}_{s=2}(\zeta_{P_{a,b}}(s)) &= \mathrm{ord}_{s=2}(L(s-1,\chi_1)^3)L(s-1,\chi_2)\zeta(s-1)^3) && (3.4.6)\\ &= 3\mathrm{ord}_{s=1}(L(s,\chi_1)) + \mathrm{ord}_{s=1}L(s,\chi_2) - 3. && (3.4.7)\end{aligned}$$

where χ_1 is the primitive character that induces the character from 3.1.5 for $n = b-4$ and χ_2 is the primitive character that induces the character from 3.1.5 for $n = b^2 - 4b$. When a primitive character χ is non-principal, the third point in 3.1.10 tells us that $\mathrm{ord}_{s=1}(L(s,\chi)) = 0$. If χ is principal and primitive then $L(s,\chi) = \zeta(s)$, and $\mathrm{ord}_{s=1}(\zeta(s)) = -1$. The primitive character that induces the character from 3.1.5 is principal exactly if $\left(\frac{n}{p}\right) \in \{0,1\}$ for all odd primes p, which happens only when n is a square. Now let s_n be 1 if n is a square and 0 if n is not a square, then we have that $\mathrm{ord}_{s=2}(\zeta_{P_{a,b}}(s)) = -3s_{b-4} - s_{b^2-4b} - 3$, which is the same as $-\mathrm{Rank}(\mathrm{Pic}(X_{1,b}))$ in all five cases in Lemma 3.4.7. □

Chapter 4

Markov Graphs

In the first chapter we have already seen graphs related to the solutions of the Markov Equation over $\mathbb{Z}$. In this chapter we will focus on similar graphs but with solutions in different rings. Lately there has been a lot of interest in such graphs over $\mathbb{F}_p$. These Markov graphs are studied for instance in [2],[8] and [6], or in more generality in [13].

4.1 Definition of Markov Graph

In this section we will define Markov graphs and see how some properties of the graph relate to some algebraic properties of solutions to the Markov Equation.

Definition 4.1.1. For a ring R we define $G(R)$ to be the undirected graph with vertex set the solutions $(x, y, z) \in R^3$ to the Markov Equation $X^2 + Y^2 + Z^2 = 3XYZ$ and the edges are all sets $\{P, \tau_i(P)\}$ of size 2 for $i \in \{1, 2, 3\}$. Here the τ_i are defined as in Lemma 1.2.1.

Remark 4.1.2. As ring homomorphisms preserve polynomial expressions the map $G(R)$ is a functor from the category of rings to the category of graphs.

Example 4.1.3. For finite rings we see that $G(R)$ is a finite graph. We can for example draw the graph for $R = \mathbb{F}_4$, which has three connected components. In the appendix some larger graphs for $R = \mathbb{F}_5$ (Figure A.1) and $R = \mathbb{F}_7$ (Figure A.2) can be found.

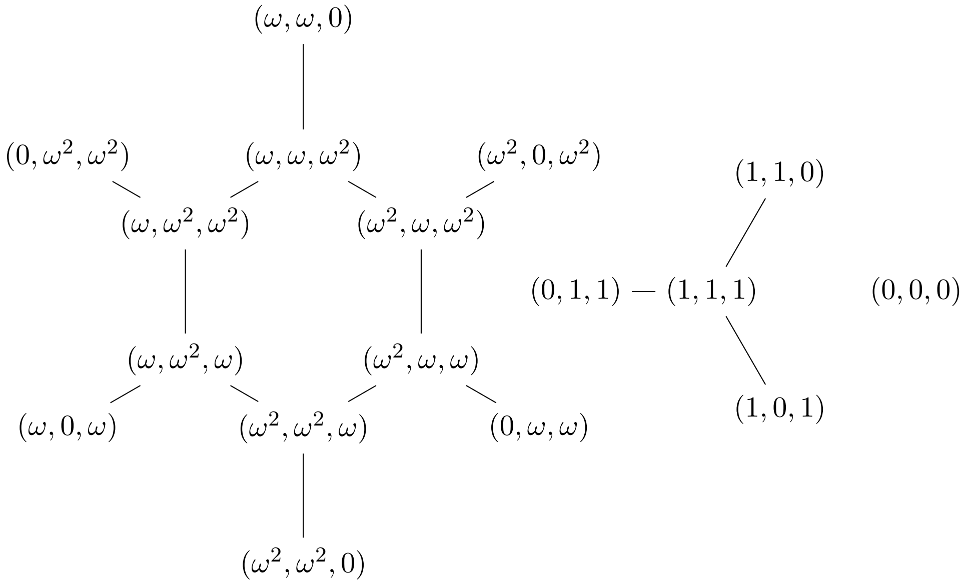
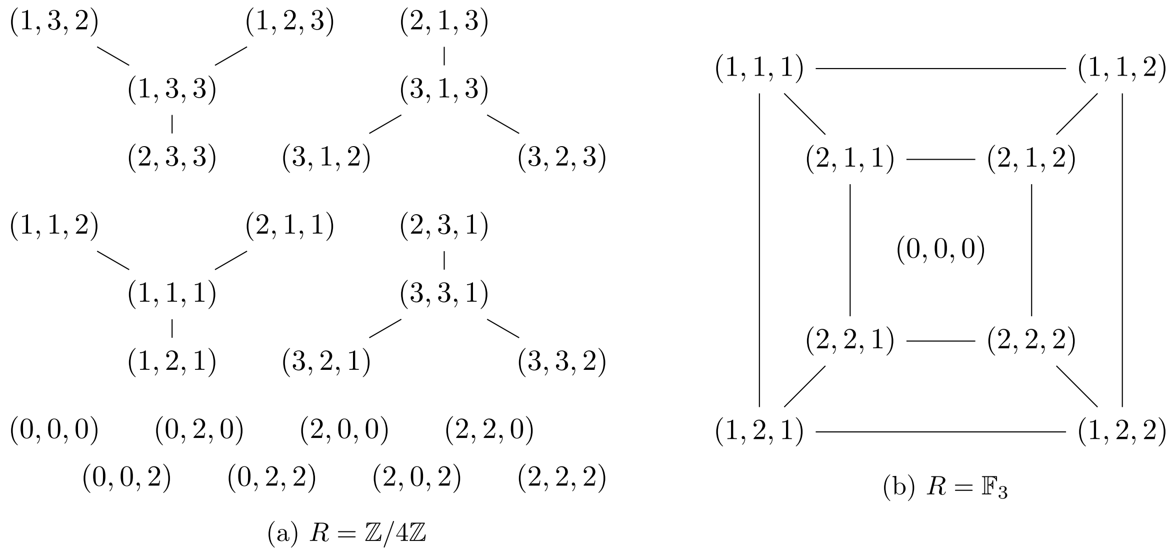

$(\omega, \omega, 0)$
$(0, \omega^2, \omega^2)$
$(\omega, \omega, \omega^2)$
$(\omega^2, 0, \omega^2)$
$(\omega, \omega^2, \omega^2)$
$(\omega^2, \omega, \omega^2)$
$(\omega, \omega^2, \omega)$
$(\omega^2, \omega, \omega)$
$(\omega, 0, \omega)$
$(\omega^2, \omega^2, \omega)$
$(0, \omega, \omega)$
$(\omega^2, \omega^2, 0)$
$(1, 1, 0)$
$(0, 1, 1)$ — $(1, 1, 1)$
$(0, 0, 0)$
$(1, 0, 1)$

Figure 4.1: The graph $G(\mathbb{F}_4)$, where $\mathbb{F}_4 = \mathbb{F}_2(\omega)$



(a) $R = \mathbb{Z}/4\mathbb{Z}$

(b) $R = \mathbb{F}_3$

Figure 4.2: Two more examples of $G(R)$.

△

Remark 4.1.4. As $\tau_i \circ \tau_i$ is the identity we see that any point in $G(R)$ has at most three neighbours and all neighbours of P are of the form $\tau_i(P)$. As $(0,0,0)$ is a solution to the Markov Equation and $\tau_i((0,0,0)) = (0,0,0)$ for all $i \in \{1,2,3\}$ we see that $(0,0,0)$ is not connected to any other vertex in $G(R)$.

Lemma 4.1.5. *Let R' be a subring of some ring R. Then $G(R')$ is an induced subgraph of $G(R)$ that is disconnected from the rest of $G(R)$.*

Proof. A vertex $P \in G(R')$ is some solution to the Markov Equation over R', and as $R' \subset R$ this also a solution over R. As the neighbours of P are of the form $\tau_i(P)$ and τ_i maps $(R')^3$ to $(R')^3$ the neighbours of P in $G(R)$ are vertices with coordinates in R'. □

We see that for the particular case $R' = \{0\}$ we get the second observation from Remark 4.1.4. In Figure 4.1 we can see the consequence of this lemma for the subring $\mathbb{F}_2$ of $\mathbb{F}_4$. The graph $G(\mathbb{F}_2)$ consists of the five points in the two smaller connected components of $G(\mathbb{F}_4)$.
As all Markov triples are generated by applying τ_i to $(1,1,1)$ over $\mathbb{Z}$, we can also see the values of such triples modulo 4 in Figure 4.2a. In particular this implies that there are no Markov numbers divisible by 4 or equal to 3 modulo 4. To generate all solutions over $\mathbb{Z}$ we had five orbits, starting with $(0,0,0)$, $(1,1,1)$, $(-1,-1,1)$, $(-1,1,-1)$ and $(1,-1,-1)$. If we compare this to $G(\mathbb{Z}/4\mathbb{Z})$ we see that there are seven solutions modulo 4 that do not have a lift to $\mathbb{Z}$.

Definition 4.1.6. For a prime p we define the Markov graph G_p modulo p to be the graph $G(\mathbb{F}_p)$ but with the point $(0,0,0)$ removed.

Lemma 4.1.7. *Let p be prime. Then every solution to the Markov Equation over $\mathbb{F}_p$ has some pre-image in $\mathbb{N}_0^3$ if and only if G_p is a connected graph.*

Proof. First of all we assume that every solution in $\mathbb{F}_p^3$ has a pre-image in the natural numbers. Let A, B be two vertices in G_p, then we consider their pre-images. As $(0,0,0)$ is not a vertex in G_p, the pre-images of A and B cannot be $(0,0,0)$. Therefore their pre-images are Markov triples. By Theorem 1.1.1 there is some path between these two pre-images constructed by applying τ_1, τ_2 and τ_3. We can apply these involutions in the same order to A and then we must end up at B. So between every two points in G_p there is a path, so G_p is connected.

Now we assume that G_p is connected. The solutions $(0,0,0),(1,1,1) \in \mathbb{F}_p^3$ have pre-images $(0,0,0),(1,1,1) \in \mathbb{N}_0^3$. Now let P be some other solution to the Markov Equation over $\mathbb{F}_p^3$. As G_p is connected there is some path from $(1,1,1)$ to P. If we apply the involutions in the same order to $(1,1,1) \in \mathbb{Z}^3$ we get some Markov triple that is a pre-image of P. □

Remark 4.1.8. As all integral solutions to the Markov Equation can be generated by applying different τ_i to $(1,1,1)$, $(1,-1,-1)$, $(-1,1,-1)$, $(-1,-1,1)$ or $(0,0,0)$ we see that a solution in $\mathbb{F}_p^3$ lift to the integers if and only if it is in the same connected component as one of these five points. So to have a local-global principle modulo p for the Markov Equation we need every vertex of G_p to be in the same connected component as one of $(1,1,1)$, $(1,-1,-1)$, $(-1,1,-1)$ or $(-1,-1,1)$.

Lemma 4.1.9. *For $p > 3$ the Markov graph G_p the number of vertices is equal to $p^2 + 3p\left(\frac{-1}{p}\right)$ and the number of edges is $\frac{1}{2}(3p^2 - 3p + 12) + \frac{1}{2}(9p + 3)\left(\frac{-1}{p}\right)$.*

Proof. The number of vertices follows immediately from Theorem 2.1.1. For the number of edges we will first count the number L_1 of points P with $\tau_1(P) = P$. So we look for points (x,y,z) with $x^2 + y^2 + z^2 = 3xyz$ and $3yz - x = x$. As $p > 2$ we see that $x = \frac{3}{2}yz$, so we can substitue the expression for x and we then get $4y^2 + 4z^2 = 9y^2z^2$. If $z = \pm\frac{2}{3}$ then there are no such solutions, and if $z = 0$ there is one solution $(0,0,0)$. For other values of z we have that $(9z^2 - 4)y^2 = 4z^2$ has two solutions if $9z^2 - 4$ is a square, and no solutions if $9z^2 - 4$ is not a square. So we see that there are $1 + \left(\frac{9z^2-4}{p}\right)$ solutions. So we can use Lemma 2.2.3 to see that the number of elements in $\{P : \tau_1(P) = P\}$ is equal to

$$1 + \sum_{\substack{z \in \mathbb{F}_p \\ z \notin \{0, \pm\frac{2}{3}\}}} 1 + \left(\frac{9z^2 - 4}{p}\right) = p - 2 - \left(\frac{9}{p}\right) - \sum_{z \in \{0, \pm\frac{2}{3}\}} \left(\frac{9z^2 - 4}{p}\right) = p - 3 - \left(\frac{-1}{p}\right).$$

Let E be the number of edges of G_p, V the number of vertices in G_p and L_i the number of points in G_p fixed by τ_i. For every vertex P we consider $\tau_1(P)$, then either $\tau_1(P) = P$ or there is some edge from $\tau_1(P)$ to P. We count every edge exactly twice this way as $\tau_1(\tau_1(P)) = P$. If we repeat this with τ_2 and τ_3 we count all edges, and we get $2E + L_1 + L_2 + L_3 = 3V$. Moreover by symmetry we have $L_1 = L_2 = L_3$, and as we have removed $(0,0,0)$ from the graph and $(0,0,0)$ is fixed by τ_i we get $L_1 = p - 4 - \left(\frac{-1}{p}\right)$. Thus we get $E = \frac{1}{2}(3p^2 + 6p + 15)$ for $p \equiv 1 \bmod 4$ and $E = \frac{1}{2}(3p^2 - 12p + 9)$ if $p \equiv 3 \bmod 4$. □

Remark 4.1.10. With very similar reasoning one can calculate that for $p > 3$ and $q = p^n$ the number of edges in $G(\mathbb{F}_q)$ is $\frac{1}{2}(3q^2 - 3q + 12) + \frac{1}{2}(9q + 3)\left(\frac{-1}{p}\right)^n$. For $q = 3^n$ one can calculate that the number of edges in $G(\mathbb{F}_q)$ is equal to $\frac{3}{2}(q - 1)(q + (-1)^n)$. With a different, but easier calculation, one can at last calculate for $q = 2^n$ that the number of edges in $G(\mathbb{F}_q)$ is equal to $\frac{3}{2}(q^2 - 2q + 2)$.

Remark 4.1.11. In the proof above we see that there are $L_p := p - 4 - \left(\frac{-1}{p}\right)$ vertices in G_p fixed by τ_1. If some vertex (x,y,z) is fixed by both τ_1 and τ_2, then we get $2x = 3yz$, $2y = 3xz$ and $x^2 + y^2 + z^2 = 3xyz$. So we see that $3xyz = 2x^2 = 2y^2 = x^2 + y^2 + z^2$, so $z = 0$. This also gives $x = y = 0$ so there are no such solutions in G_p. Thus we see that there are $3L$ vertices of degree 2 and the rest of the vertices has degree 3.

4.2 Cycles

In this section we will study cycles in the Markov graph G_p. As the Markov graph G_p has more edges than vertices for $p > 2$ there must exist cycles in the graph. Moreover computations for

n	# Word classes	Representatives in each class
1	0	
2	0	
3	0	
4	1	1212
5	0	
6	3	121212, 121323, 123123
7	2	1212313, 1213123
8	7	12121212, 12121313, 12121323, 12123123, 12123213, 12131213, 12132123
9	7	121212313, 121213123, 121231213, 121231323, 121232313, 121321323, 123123123
10	17	1212121212, 1212121313, 1212121323, ...
11	20	12121212313, 12121213123, 12121231213,...

Table 4.1: The number of equivalence classes of words for small fixed lengths.

small primes p show that there are often small cycles and that G_p is not bipartite for all primes between 11 and 2000. To study cycles we use the following ideas from [8].

As the edges in G_p are defined by the involutions τ_i, we can describe a path in G_p by some word in the three-letter alphabet $\{1,2,3\}$ that corresponds with the applied involutions. For a cycle in G_p we can also construct a word $w = w_1 w_2 \dots w_n$ this way, and then the starting point from this path must be a fixed point of $\tau_{w_m} \circ \cdots \circ \tau_{w_1}$. So if we want to know if there exists a cycle of length k in G_p, we can enumerate all words of length k and see if the polynomial equations defined by the fixed point have a solution. Then we will still have to check if this solutions give a proper cycle, as it may be possible that points are fixed by the involutions and the cycle is actually shorter than the length of the word.

Although there are 3^k words of length k in an alphabet with three letters, we can reduce the number of words significantly. As applying τ_i twice in a row does not change a solution, we do not have to look at words with the same letter twice a row. If we reverse the word or cyclically permute the letters we will also find the same cycle. Due to symmetry in the three coordinates in the Markov equation we see that applying a permutation to the alphabet should not change the answer to whether there exists such a cycle. Finally a word where some letter appears just once can also never correspond to a proper cycle, as that coordinate will be changed just once, so it can never return to the starting point. Using this symmetry we can consider equivalence classes of words. In Table 4.1 the number of such equivalence classes for small fixed lengths is shown. In particular we immediately see that there can not be any cycles of length $1, 2, 3$ or 5 in Markov graphs modulo p. We will first consider cycles of length 4.

Proposition 4.2.1. *There is a 4-cycle in G_p if and only if $p \equiv 1 \bmod 4$ or $p = 3$. Moreover in the case $p \equiv 1 \bmod 4$ there are exactly $\frac{3(p-1)}{2}$ different 4-cycles.*

Proof. We start with the word 1212, and we let $P = (x, y, z)$ be the starting point of the cycle. Then we can combine the three equations from $\tau_2 \circ \tau_1 \circ \tau_2 \circ \tau_1((x, y, z)) = (x, y, z)$ with the Markov Equation. The z-coordinate does not change so that gives $z = z$. Furthermore we get $27yz^3 = 6yz + 9xz^2$ and $6xz + 81yz^4 = 27yz^2 + 27xz^3$. For $p = 3$ we see that these equations always hold, so every point in G_3 is the starting point of a 4-cycle. We can indeed check this in Figure 4.2b. For $p > 3$ we can combine these equations we get $3z^4 = 0$, so $z = 0$. From the Markov equation we now get $x^2 + y^2 = 0$. This has non-zero solutions if and only if $p \equiv 1 \bmod 4$. So for $p > 3$ with $p \equiv 3 \bmod 4$ we cannot have 4-cycles. Moreover for $p \equiv 1 \bmod 4$ the point $(\lambda, \pm i\lambda, 0)$ is indeed a vertex in G_p for $\lambda \in \mathbb{F}_p^\times$ that satisfies all these equations. As long as $\lambda \neq -\lambda$ we can also see that this is a proper 4-cycle. There are $2(p-1)$ vertices in G_p with

$z = 0$ as we have two choices for i and $p-1$ choices for λ. So as all these points are in 4-cycles we have $\frac{2(p-1)}{4}$ different 4-cycles with z-coordinate 0. By symmetry we can do the same with x and y and we can therefore count that there are $\frac{6(p-1)}{4}$ different 4-cycles in G_p. □

As seen from the equations in the example above, a lot of factors 3 appear. As long as we assume $p > 3$ we can use Lemma 1.2.3 to rescale the Markov equation to $X^2 + Y^2 + Z^2 = XYZ$ and the involutions lose the factor 3. This simplifies calculations and results can still be calculated back to the original Markov equation by dividing all coordinates by 3. From this point on we use this renormalization in calculations. We proceed with 6- and 7-cycles.

Proposition 4.2.2. *For every $p > 3$ the graph G_p contains a 6-cycle.*

Proof. We will now continue to look for cycles of length 6 in G_p for $p > 3$. We start with the word 121212. Then you get $2z^4 = 2z^2$, so we have $z = 0$ or $z = \pm 1$. If we have $z = 0$ we also get $2x = 2y = 0$, so we only get $(0, 0, 0)$ which we have deleted from our graph. For $z = 1$ the extra equations for the cycle are all satisfied for all x, y, so we are only left with the Markov Equation. This leaves us with $x^2 + y^2 + 1 = xy$. Similarly to the point counting we can use Lemma 2.2.3 to see that there are $p - \left(\frac{-3}{p}\right)$ solutions.
To see how many of these solutions give proper 6-cycles we count how many fixed points we can have. If we add that $(x, y, z) = \tau_1(x, y, z)$ or $\tau_1 \circ \tau_2 \circ \tau_1(x, y, z) = \tau_1 \circ \tau_2 \circ \tau_1 \circ \tau_2(x, y, z)$ we get that $3y^2 = -4$. For the other four cases we get $3y^2 = -1$. As we have at most two values of x to complete a triple with some y and z we see that at most 8 cycles can not be proper. So for $p \geq 11$ there is always a proper 6-cycle. For $p = 5$ and $p = 7$ we see in Figure A.1 and Figure A.2 that there are also proper 6-cycles.

□

Remark 4.2.3. For the words 121323 and 123123 the equations become more difficult. For 121323 we get $z^4 - 5z^2 + 8 = 0$, $y^2 = (z^2 - 4)^2$ and $4x = yz - yz^3$. To solve for z we need -7 and at least one of $10 \pm \sqrt{-28}$ to be a square. This happens if p is a square in $\mathbb{F}_7$ and 2 is not a square modulo 8, but it can also happen for other primes. For 123123 we get $(z^2 - 3z + 3)(z^2 + 3z + 3) = 0$, $y^2 = 3 - z^2$ and $9x = yz^3 + 3yz$. For both $z^2 - 3z + 3$ and $z^2 + 3z + 3$ the polynomials has zeros if and only if p is a square modulo 3. Moreover we get $y^2 = 3 - z^2 = (z \pm 3)^2$, so there are always solutions for x, y to complete the triple if a good z exists.

Proposition 4.2.4. *For $p > 3$ the graph G_p contains a 7-cycle if and only if $p \equiv 1 \bmod 4$ or p is a square modulo 7.*

Proof. We start off with the word 1212313. To help with calculations we use a Sage program that calculates a Gröbner basis of the ideal generated by the Markov Equation and the three equations for being a fixed point of this word. This code can be found in the appendix A.4. We get that $yz^4 = 0$, if $z = 0$ then we see by Proposition 4.2.1 that $\tau_2 \circ \tau_1 \circ \tau_2 \circ \tau_1((x, y, 0)) = (x, y, 0)$, so this is not a proper cycle. If $y = 0$ then $z \neq 0$ and we get $z^2 = 2$. Then we see that

$$(x, 0, z) \overset{\tau_1}{\mapsto} (-x, 0, z) \overset{\tau_2}{\mapsto} (-x, -xz, z) \overset{\tau_1}{\mapsto} (-xz^2 + x, -xz, z) = (-x, -xz, z).$$

As τ_1 fixes $(-x, -xz, z)$ this is again not a proper cycle. So we see that there are no primes p such that there are proper 7-cycles with the word 1212313.
We continue to the word 1213123. We get $z^8 = z^4$, and if $z = 0$ we also get $x = y = 0$, so $z^4 = 1$. If we have $z^2 = -1$, then we get $y^2 = 1$ and $x = yz$. We can choose $y = 1$ and z a square root of -1 and then we see get that

$$(i, 1, i) \overset{\tau_1}{\mapsto} (0, 1, i) \overset{\tau_2}{\mapsto} (0, -1, -i) \overset{\tau_1}{\mapsto} (-i, -1, i) \overset{\tau_3}{\mapsto} (-i, -1, 0) \overset{\tau_1}{\mapsto} (i, -1, 0) \overset{\tau_2}{\mapsto} (i, 1, 0) \overset{\tau_3}{\mapsto} (i, 1, i)$$

and we therefore have a proper cycle in characteristic more than 2. We see that this cycle only exists for $p \equiv 1 \bmod 4$ as we need $i \in \mathbb{F}_p$. We proceed to the case $z^2 = 1$, then we get $x^4 = 1$. We start off with $x^2 = -1$, then we also get $y = 0$ and we get a proper 7-cycle for instance with

$$(i,0,-1) \overset{\mathcal{T}_1}{\mapsto} (-i,0,-1) \overset{\mathcal{T}_2}{\mapsto} (-i,i,-1) \overset{\mathcal{T}_1}{\mapsto} (0,i,-1) \overset{\mathcal{T}_3}{\mapsto} (0,i,1) \overset{\mathcal{T}_1}{\mapsto} (i,i,1) \overset{\mathcal{T}_2}{\mapsto} (i,0,1) \overset{\mathcal{T}_3}{\mapsto} (i,0,-1).$$

Now we go to the case $x^2 = 1$. Then we get $y^2 - xyz + 2 = 0$, which has discriminant $x^2z^2 - 8 = -7$. So we see that this polynomial has roots if p is a square modulo 7. In Figure A.2 we see that for $p = 7$ there are no 7-cycles. For all other primes $p > 2$ with p a square modulo 7 we can take $x = z = 1$ and y a root of $y^2 - y + 2$ and then we get

$$\begin{aligned}(1,y,1) &\overset{\mathcal{T}_1}{\mapsto} (y-1,y,1) \overset{\mathcal{T}_2}{\mapsto} (y-1,-1,1) \overset{\mathcal{T}_1}{\mapsto} (-y,-1,1) \overset{\mathcal{T}_3}{\mapsto} (-y,-1,y-1) \overset{\mathcal{T}_1}{\mapsto} (1,-1,y-1)\\ &\overset{\mathcal{T}_2}{\mapsto} (1,y,y-1) \overset{\mathcal{T}_3}{\mapsto} (1,y,1).\end{aligned}$$

□

Example 4.2.5. As words become longer, the difficulty of finding solutions seems to increase. We now try the first word of length 9, namely 121232313. We get $z(z-1)(z+1)(z^3-z-1)(z^3-z+1) = 0$. If $z = 0$ we get $y = x = 0$. If $z^2 = 1$ we get $y^2 = 1$ and $x^2 - xyz + 2 = 0$ and we indeed get a proper 9-cycle starting with $(x, 1, 1)$.

For $z^3 - z - 1 = 0$ we get $y^4 + (z^2-2)y^2 - z^2 + z + 1$. The question for which p the polynomial $P(z) := z^3 - z - 1$ has roots in $\mathbb{F}_p$ becomes a bit more difficult. The discriminant D of $P(z)$ is -23. If $P(z)$ has no roots in $\mathbb{F}_p$, the extension of $\mathbb{F}_p$ with a root is Galois and has degree 3. As the Galois group is a subgroup of S_3 we see that the Galois group of the extension is A_3. As all permutations are even permutations the product $\Delta = \prod_{1 \le i < j \le 3}(\alpha_i - \alpha_j)$ is invariant under the action of the Galois group and an element of $\mathbb{F}_p$, so as $D = \Delta^2$ we see that D must be a square in $\mathbb{F}_p$. So for all p such that -23 is not a square in $\mathbb{F}_p$, the polyomial $P(z)$ has at least one zero. However this will not give any triples (x, y, z), as solving for y requires $(z^2-2)^2 - 4(1+z-z^2) = z^2 - 3z$ to be a square, and we have $(-9z^2+2z+6)^2 = -23(z^2-3z)$ so as -23 is not a square we see that $z^2 - 3z$ is also not a square. So we must have that -23 is a square in $\mathbb{F}_p$, and $P(z)$ has zeros. As described in [28] this problem is related to coefficients of some modular form. It is shown that $P(z)$ has roots in $\mathbb{F}_p$ and -23 is a square modulo p if and only if we can write $p = a^2 + ab + 6b^2$ for $a, b \in \mathbb{Z}$. This also equivalent to whether the p'th coefficient in the q-expansion of the unique newform of level 23 and weight 1 is equal to 2.

At last we note that for $Q(z) = z^3 - z + 1$ we have $-Q(-z) = P(z)$, so they have the same number of roots over $\mathbb{F}_p$. △

As seen in the examples above the general problem for the existence of cycles of a fixed length can be translated to an algebraic problem by enumerating all (equivalence classes of) words and then determining whether certain ideals have a zero locus over $\mathbb{F}_p$. For polynomials of low enough degree we only get restrictions on primes modulo some integer n, but for higher degree the problems becomes more difficult. Finding solutions is not enough, as one needs to verify whether the solutions found actually contribute to a proper cycle, as solutions can sometimes be fixed by the involutions. In Table 4.2 it is shown for all words of length 7 and 9 which polynomials have to be solved over $\mathbb{F}_p$ to possibly find a cycle corresponding to that word.

Word	Polynomials that should be solved
1212313	$z = 0, y^2 = 2, x^2 = -y^2$ or $y = 0, z^2 = 2, x^2 = -z^2$
1213123	$z^2 = -1, y^2 = 1, x = yz$ or $z^2 = 1, y = 0, x^2 = -1$ or $z^2 = -1,\ y^2 - y + 2 = 0, x = z$ or $z^2 = -1, y^2 + y + 2 = 0, x = -z$
121212313	$z^2 = 3, y = 0, x^2 = -z^2$ or $z^2 = 1, y^6 - 4y^4 + 3y^2 + 4 = 0, x = ..$
121213123	$(z^2 - z - 1)(z^2 + z - 1)(z^4 - z^2 + 1) = 0, (z^2 - z - 1)(z^2 + z - 1)(y^2 + z^4) = 0,$ $y^6 + (z^2 + 1)y^4 + (3z^2 + 4)y^2 + (-z^{10} + 2z^8 - z^6 + 7z^4)$
121231213	$z = 0, y^4 - y^2 + 2 = 0, x^2 = -y^2$ or $z = 1, y = 0, x^2 = -1$ or $z = -1, y = 0, x^2 = -1$ or $z^2 = 2, y^6 - 2y^4 + y^2 + 2 = 0, x = ..$ or $z^3 - z - 2 = 0, y^2 = 1 - z^2, x = ..$ or $z^3 - z + 2 = 0, y^2 = 1 - z^2, x = ..$
121231323	$(z^5 - z^4 - 2z^3 + 3z^2 - z - 1)(z^5 + z^4 - 2z^3 - 3z^2 - z + 1) = 0$ and $y^4 + (z^8 - 4z^6 + 5z^4 - 3z^2 + 3)y^2 + (6z^{10} - 28z^8 + 41z^6 - 33z^4 + 33z^2) = 0$ $x = ..$, where some $1/33$ factors appear.
121232313	$z = 1, y^2 = 1, x^2 - xy + 2 = 0$ or $z = -1, y^2 = 1, x^2 + xy + 2 = 0$ or $z^3 - z - 1 = 0, y^4 + (z^2 - 2)y^2 + (-z^2 + z + 1) = 0, x = ..$ or $z^3 - z + 1 = 0, y^4 + (z^2 - 2)y^2 + (-z^2 - z + 1) = 0, x = ..$
121321323	$z^{28} - 10z^{26} + 41z^{24} - 82z^{22} + 66z^{20} + 5z^{18} + 53z^{16} - 228z^{14} + 82z^{12} + 299z^{10}$ $-99z^8 - 468z^6 + 417z^4 - 65z^2 + 4, y^2 = P(z^2), x = ..$
123123123	$z^{18} - z^{16} + 4z^{14} + z^{12} + z^{10} + z^8 + 28z^6 - 110z^4 + 93z^2 - 25$ $y^4 + P_1(z^2)y^2 + P_2(z^2) = 0, x = ..$

Table 4.2: The polynomials that have to be solved over $\mathbb{F}_p$ to find a base point for a loop corresponding with some word in the Markov graph. The coordinates are rescaled to satisfy $X^2 + Y^2 + Z^2 = XYZ$.

4.3 Graph property experiments

In this section we will look at various graph properties and discuss these properties for G_p. For various properties Table 4.3 shows these properties for small primes p. The properties are ordered from cases where theoretical results are known to cases where only partial results or just computations are known.

Connected graph

This is the most famous property of the Markov graph due to its connection with the Local-Global principle as discussed in Remark 4.1.8. In 2020 it was proven in [6] that G_p *is connected for all* $p > 3 \cdot 10^{27}$.

Planar graph

In [8] it is *proven that* G_p *is not planar for* $p > 7$. The general proof strategy consists of counting the number of points, edges, 4- and 6-cyles of G_p. For a planar graph with few small cycles the number of edges cannot be a lot more than the number of vertices, which shows the non-planarity for p large enough.

Eulerian graph

A graph is called Eulerian if there exists a path through G_p such that every edges is visited exactly once. If G_p is not connected then it is also not Eulerian. For a connected graph being Eulerian is equivalent to having even degree at every vertex. As $(1, 1, 1)$ has degree 3, we see that G_p *is not Eulerian for all primes* p.

Order, size, circuit rank

The order of a graph is the number n of vertices and the size of a graph is the number m of edges in the graph. These are both calculated for G_p in 4.1.9. The circuit rank r of a graph is the minimum number of edges that have to be removed to break all its cycles. If c is the number of connected components of G_p then $r = m - n + c$. So under the assumption that G_p is connected we get $c = 1$ and this also allows us to calculate r.

Girth

The girth of a graph is the length of the shortest cycle in the graph. By Propositions 4.2.1 and 4.2.2 we see that *the girth of G_p is 4 when $p \equiv 1 \bmod 4$ or $p = 3$ and the girth is 6 when $p \equiv 3 \bmod 4$ and $p \neq 3$.* At last there are no cycles in G_2 so then it has infinite girth.

Degree sequence

The degree sequence of a graph is the non-decreasing sequence of degrees of all vertices in the graph. By Remark 4.1.11 we see that *the degree sequence of G_p consists of $p^2 + 15$ threes and $3p - 15$ twos if $p \equiv 1 \bmod 4$. For $p \equiv 3 \bmod 4$ we get $p^2 - 6p + 9$ threes and then $3p - 9$ twos.*

Bipartite graph

A graph is called bipartite if it can be coloured in two colours such that no two neighbours have the same colour. A graph is bipartite if and only if it contains no odd cycles. In 4.2.4 we saw that there is an 7-cycle in G_p if and only if $p \equiv 1 \bmod 4$ or $\left(\frac{p}{7}\right) = 1$. This shows that G_p is *not bipartite for at least three quarters of the primes.* For all primes p with $7 < p \leq 100$ it is shown in Table 4.3 that G_p is not bipartite. We have also verified for all primes between 7 and 2000 that G_p is not bipartite.

Hamiltonian graph

A graph is called Hamiltonian if there exists a cycle that visits every vertex exactly once. For this property there does not seem to be a local obstruction. In Table 4.3 it seems like there are both large p for which G_p is Hamiltonian as well as large p for which G_p is non-Hamiltonian. However this table is not large enough to make real predictions. Verifying whether a graph is Hamiltonian is an NP-hard problem and for graphs where all vertices have at most degree 3 the fastest algorithm at this moment is [19] and solves the problem in $O(1.251^n)$ time, where n is the number of vertices in the graph. As G_p has $p^2 \pm 3p$ vertices this increases very fast. Because of this computational obstruction there are some values missing in the table where no answer was found within reasonable time.

Diameter

The diameter of a connected graph is the maximal distance between two vertices in the graph. The distance between two vertices is the length of the shortest path from one vertex to the other. As all vertices in G_p have at most 3 neighbours, we have for any vertex P of G_p that there are at most 3^n vertices at distance at most n to P. Therefore *the diameter of G_p becomes arbitrary large and a lower bound is given by $\log_3(p^2 - 3p)$.* In Table 4.3 the diameter is also shown for small values of p.

Independence number

The independence number of a graph is the size of the large set of vertices such that there are no edges between any two vertices. In G_p there are $3(p - 4 - (-1)^{(p-1)/2})$ vertices of degree 2,

p	Connected	Bipartite	Hamiltonian	Diameter	Independence number
5	1	0	1	6	16
7	1	1	0	6	12
11	1	0	0	10	34
13	1	0	0	12	80
17	1	0	1	13	132
19	1	0	1	12	117
23	1	0	1	12	185
29	1	0	?	16	356
31	1	0	?	14	328
37	1	0	0	16	568
41	1	0	1	17	678
43	1	0	0	15	658
47	1	0	1	14	790
53	1	0	?	16	1136
59	1	0	1	15	1260
61	1	0	?	17	1477
67	1	0	1	16	1618
71	1	0	1	17	1814
73	1	0	?	17	2103
79	1	0		16	2264
83	1	0		17	2503
89	1	0		19	3098
97	1	0		19	3692

Table 4.3: Various properties described for G_p if they are true (1), false (0), computer time-out (?) or some integer.

and as this number is even we can add edges between these vertices to make a 3-regular graph. As adding edges only decreases the independence number of a graph, we can use the bounds from [25] to see that this is at least one fourth of the number of vertices in G_p. As adding one edge lowers the independence number by at most 1 we can also use the upper bound and add the number of edges added. Let $\mu(G_p)$ denote the independence number of G_p, *then we get that*

$$\frac{p^2+3p(-1)^{(p-1)/2}}{4} \leq \mu(G_p) \leq \frac{p^2+3p(-1)^{(p-1)/2}}{2} + \frac{3}{2}(p-4-(-1)^{(p-1)/2}).$$

The value of $\mu(G_p)$ for small primes can also be seen in Table 4.3. It has been calculated for $97 \leq p \leq 233$ that the independence number divided by the number of vertices lies between 0.373 and 0.379. At this moment the fastest algorithm to calculate the independence number for G_p seems to be [32], which still runs in exponential time.

Expander graphs

Expander graphs are graphs with relatively few edges such that the minimum number of nodes that need to be removed to make the graph disconnected is relatively big. There are various definitions of expander graphs in literature, one possible choice is to talk about spectral expansion where some condition on the second largest eigenvalue of the adjacency matrix is imposed. As all vertices in G_p have degree at most 3 the graph has relatively few edges, and with numerical evidence it is suggested in [9] that the Markov graphs form a family of expander graphs.

Chapter 5

Cryptography with Markov Graphs

This chapter is focused around the article [30] that appeared in November 2022. In this paper an algorithm is presented that potentially breaks a cryptographic hash function described in [12] based on ideas from [5]. We will refer to this algorithm by the Silverman Path-Finding Algorithm, or SPFA in short.

For a precise definition of a cryptographic hash function one could for instance look in [14]. For this thesis it suffices to know that a hash function is a function that takes some key and an arbitrary long binary string that is mapped to a hash value which is a binary string of some length determined by the key. It should be hard to invert this function, so given a hash value it has to be hard to find a pre-image. Cryptographic hash functions have an important role in cybersecurity.

In 1995 the hash function named SHA-1 (Secure Hash Algorithm 1) was designed and it was later adopted by the U.S. National Institute of Standards and Technology (NIST) as a standard hash function. From around 2005 SHA-1 has not been considered secure anymore and the NIST organized an open competition from 2007 to develop a new hash function that could become the new standard. This inspired many authors to publish ideas for secure hash functions in the following years.

One such publication was [5] which uses a family of k-regular expander graphs for their hash function. This hash uses the key to determine which graph is used. The input string is then written in base $k-1$ and a walk is made in the graph from a fixed starting point, where the edge traversed is determined by the digits in the input string. The returned hash value is the final destination of the path defined by the input string. Later in 2021 it was suggested in [12] that one could use the family of Markov graphs for this hash function as they are believed to be a family of expander graphs. To break this hash function one should find a path between the starting point and some given point in the graph. This is exactly what SPFA does.

5.1 The pathfinding algorithm

We will describe in this section how SPFA works. We start off by describing slight differences between the graph where SPFA finds a path and the graph G_p we have looked at so far. Then we will see some background that SPFA heavily depends on. Finally we will describe the algorithm in detail.

5.1.1 Graph differences

We will denote G'_p for the graph SPFA is applied to. G'_p has the same set of vertices as G_p, but slightly different edges. Instead of the involutions τ_i the edges are defined by the rotations ρ_i

defined as

$$\begin{aligned}\rho_1(X,Y,Z) &= (X,Z,3XZ-Y)\\ \rho_2(X,Y,Z) &= (3XY-Z,Y,X)\\ \rho_3(X,Y,Z) &= (Y,3YZ-X,Z).\end{aligned}$$

Unlike the involutions, the rotations do not have order 2, as we can see in proposition 5.1.6. We make an undirected graph where all neighbours of a vertex P are given by $\rho_i(P), \rho_i^{-1}(P)$ for $i=1,2,3$. So we see that all vertices have degree at most 6.
The rotations are closely related to the involutions by

$$\rho_1 = (23)\circ\tau_2, \qquad \rho_2 = (13)\circ\tau_3, \qquad \rho_3 = (12)\circ\tau_1.$$

As seen in the first chapter, we have $\sigma\circ\tau_i = \tau_{\sigma(i)}\circ\sigma$ for all permuations $\sigma\in S_3$. This allows us to translate paths in G_p and G'_p to each other. Here an important role is played by the point $(1,1,1)$, as it is fixed by permutations. For $1\le j\le n$ let $i_j\in\{1,2,3\}$ and assume we have vertices P_1, P_2 such that

$$\rho_{i_1}\circ\rho_{i_2}\circ\cdots\circ\rho_{i_n}(P_1) = P_2.$$

Then we can use the fact that the rotations are a composition of a permutation and an involution. We write $\sigma_1=(23)$, $\sigma_2=(13)$, $\sigma_3=(12)$ and $\sigma_c=(123)$. Then we get

$$\begin{aligned}P_2 &= \rho_{i_1}\circ\rho_{i_2}\circ\cdots\circ\rho_{i_n}(P_1) = \sigma_{i_1}\circ\tau_{\sigma_c(i_1)}\circ\sigma_{i_2}\circ\tau_{\sigma_c(i_2)}\circ\cdots\circ\sigma_{i_n}\circ\tau_{\sigma_c(i_n)}(P_1)\\ &= \tau_{\sigma_{i_1}\sigma_c(i_1)}\circ\sigma_{i_1}\circ\sigma_{i_2}\tau_{\sigma_c(i_2)}\circ\ldots\sigma_{i_n}\circ\tau_{\sigma_c(i_n)}(P_1)\\ &= \tau_{i'_1}\circ\tau_{i'_2}\circ\cdots\circ\tau_{i'_n}\circ\sigma(P)\end{aligned}$$

Here we can use the commutation relation to pull all permutations to the right and in the process changing the indices of which involutions are applied. The permutation σ that is left is equal to $\sigma_{i_1}\sigma_{i_2}\ldots\sigma_{i_n}$. Although this calculation only starts with ρ_i, we perform a similar transformation if there also appear ρ_i^{-1} in the composition. To do this we can use the properties

$$\rho_1^{-1} = (23)\circ\tau_3, \qquad \rho_2^{-1} = (13)\circ\tau_1, \qquad \rho_3^{-1} = (12)\circ\tau_2.$$

So if we have a path from P_1 to P_2 with edges in G'_p, we can transform this into a path from $\sigma(P_1)$ to P_2 for some permutation $\sigma\in S_3$. If we have some function that finds paths between any two points in G'_p, we can create a path from $(1,1,1)$ to P_1 and a path from $(1,1,1)$ to P_2. Then we can make these into paths in G_p from $\sigma(1,1,1)$ to P_1 and $\sigma'(1,1,1)$ to P_2 for permutations σ,σ'. As $(1,1,1)$ is fixed by all permuations this means that we get two paths in G_p that can be concatenated to create a path from P_1 to P_2 in G_p.
We will see later that the paths created by the SPFA will be relatively long due to three segments where a rotation is repeated many times. Therefore we will note two observations how the transformation of such a path to a path in G_p can be done without considering each rotation separately. First of all we can use that

$$\rho_1\circ\rho_1 = \tau_3\circ\tau_2, \qquad \rho_2\circ\rho_2 = \tau_1\circ\tau_3, \qquad \rho_3\circ\rho_3 = \tau_2\circ\tau_1.$$

Moreover from the commutation relation we can also see that

$$\sigma\circ\tau_{i_1}\circ\tau_{i_2}\circ\cdots\circ\tau_{i_n} = \tau_{\sigma(i_1)}\circ\tau_{\sigma(i_2)}\circ\cdots\circ\tau_{\sigma(i_n)}\circ\sigma$$

for $\sigma\in S_3$ and $i_1,\ldots,i_n\in\{1,2,3\}$.

5.1.2 Maximally elliptic coordinates

An important idea in SPFA comes from studying what happens when we apply a rotation repeatedly to a vertex of G'_p. We will consider $\rho_1^n(x,y,z)$, but by symmetry similar patterns also exist for ρ_2 and ρ_3. As the first coordinate is fixed by ρ_1, we will consider this as a constant in the calculation of $\rho_1^n(x,y,z)$. Then the rotation ρ_1 is just a linear map acting on the last two coordinates with coefficients in $\mathbb{Z}[x]$. In particular we see that

$$\rho_1(x,y,z) = (x,z,3xz-y) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 3x \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}. \tag{5.1.1}$$

So to calculate the repeated application of ρ_1 we can diagonalize the 2×2-matrix acting on the y- and z-coordinate. We will write

$$L_x = \begin{pmatrix} 0 & 1 \\ -1 & 3x \end{pmatrix}$$

for this matrix. The characteristic polynomial of L_x is $T^2 - 3xT + 1$. The multiplicative order of the eigenvalues determines the size of the orbits of ρ_1 acting on some starting point. The following proposition will describe the relation between points sharing an orbit and an equation with these eigenvalues.

Proposition 5.1.1 ([30])**.** *Let $P = (x,y,z)$ and $P' = (x,y',z')$ be two vertices in G_p with $x \neq 0, \pm\frac{2}{3}$ and let λ_x be a root of $T^2 - 3xT + 1$. Then $\rho_1^n(P) = P'$ if and only*

$$\lambda_x^n = (y' - \lambda_x z')(y - \lambda_x z)^{-1}.$$

Proof. As $x \neq \pm\frac{2}{3}$ we see that the discriminant of $T^2 - 3xT + 1$ is non-zero so there are two different roots. This also implies that $\lambda_x \neq \pm 1$. As L_x has two different eigenvalues the matrix is diagonalizable. We can choose the following matrix U to diagonalize L_x.

$$U = \begin{pmatrix} 1 & \lambda_x \\ \lambda_x & 1 \end{pmatrix}, \quad U^{-1}L_xU = \frac{1}{1-\lambda_x^2}\begin{pmatrix} 1 & -\lambda_x \\ -\lambda_x & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 3x \end{pmatrix}\begin{pmatrix} 1 & \lambda_x \\ \lambda_x & 1 \end{pmatrix} = \begin{pmatrix} \lambda_x & 0 \\ 0 & \lambda_x^{-1} \end{pmatrix}$$

We can now combine this to see that

$$\rho_1^n(P) = P' \iff L_x^n \begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} y' \\ z' \end{pmatrix} \iff \begin{pmatrix} \lambda_x^n & 0 \\ 0 & \lambda_x^{-n} \end{pmatrix} U^{-1} \begin{pmatrix} y \\ z \end{pmatrix} = U^{-1} \begin{pmatrix} y' \\ z' \end{pmatrix} \iff \lambda_x^n = \frac{y' - \lambda_x z'}{y - \lambda_x z}$$

In the last step two things are happening. First of all we divide by $y - \lambda_x z$. If this factor is 0 then $x = 0$, which we excluded by assumption. The second thing happening in the last step is that we actually get two equations, one for the first coordinate and one for the second coordinate. The second equation that needs to hold is $\lambda_x^{-n}(z - \lambda_x y) = (z' - \lambda_x y')$, we again get that both factors are non-zero as $x \neq 0$. Moreover we have that

$$\frac{y' - \lambda_x z'}{y - \lambda_x z} \cdot \frac{z' - \lambda_x y'}{z - \lambda_x y} = \frac{-\lambda_x(y'^2 + z'^2) + (\lambda_x^2 + 1)y'z'}{-\lambda_x(y^2 + z^2) + (\lambda_x^2 + 1)yz} = \frac{\lambda_x(3xy'z' - y'^2 - z'^2)}{\lambda_x(3xyz - y^2 - z^2)} = \frac{\lambda_x x^2}{\lambda_x x^2} = 1,$$

so if one of the two equations hold the other one also holds. □

Remark 5.1.2. For implementation purposes we also note that for the points $P = (x,y,z)$ and $P' = (x',y,z')$ with $y \neq 0, \pm\frac{2}{3}$ we have $\rho_2^n(P) = P'$ if and only if $\lambda_y^n = (z' - \lambda_y x')(z - \lambda_y x)^{-1}$. For ρ_3 we get $\lambda_z^n = (x' - \lambda_z y')(x - \lambda_z y)^{-1}$.

From this proposition we also note that the number of elements in the ρ_1-orbit of a point with x-coordinate not equal to $0, \pm\frac{2}{3}$ is equal to the order of λ_x in $\mathbb{F}_{p^2}^\times$. This motivates the following definition.

Definition 5.1.3. Let p be an odd prime. An element $t \in \mathbb{F}_p^\times$ is defined to be maximally elliptic if $T^2 - 3tT + 1$ has a zero λ_t in $\mathbb{F}_p$ that generates the multiplicative group $\mathbb{F}_p^\times$.

We note that for $t \in \{0, \pm\frac{2}{3}\}$ we have that $\lambda_t \in \{i, \pm 1\}$. So as λ_t has order at most 4, these exceptions to Proposition 5.1.1 are not maximally elliptic for $p > 5$.

Corollary 5.1.4. *Let $p > 5$ be prime and let $x \in \mathbb{F}_p$ be maximally elliptic, then for any two vertices $P = (x, y, z)$ and $P' = (x, y', z')$ in G_p there exists some $n \in \mathbb{Z}_{\geq 0}$ such that $\rho_1^n(P) = P'$.*

Proof. As seen in the proof of Proposition 5.1.1 we have $(y' - \lambda_x z')/(y - \lambda_x z) \neq 0$. As λ_x generates $\mathbb{F}_p^\times$ there must exist an n such that $\lambda_x^n = (y' - \lambda_x z')/(y - \lambda_x z)$. □

Remark 5.1.5. For $x \in \mathbb{F}_p$ the polynomial $T^2 - 3xT + 1$ in T does not always have roots in $\mathbb{F}_p$. However the roots do always exist over $\mathbb{F}_{p^2}$. If these roots live in $\mathbb{F}_{p^2}$ and have multiplicative order $p+1$ then all vertices with this x-coordinate live in the same ρ_1-orbit as we can use Lemma 2.2.3 to see for $x \neq 0, \pm\frac{2}{3}$ that there are $p - \left(\frac{9x^2-4}{p}\right) = p + 1$ vertices in G_p with this value as its first coordinate. Such x we call maximally hyperbolic.

Proposition 5.1.6. *The order of τ_1 as a function of all points of G_p for $p > 3$ is equal to $\frac{1}{2}(p^2 - 1)$ for $p \equiv 3 \bmod 4$ and equal to $\frac{1}{2}(p^3 - p)$ for $p \equiv 1 \bmod 4$.*

Proof. We start off with the case $p \equiv 3 \bmod 4$. In the proof of Theorem 2.1.1 we have seen that there are no solutions with the x-coordinate equal to $0, \pm\frac{2}{3}$. Then we can use Proposition 5.1.1 to see that the order of τ_1 on all points is equal to the least common multiple of the orders in $\mathbb{F}_{p^2}^\times$ of all roots λ_x of $T^2 - 3xT + 1$ over all $x \in \mathbb{F}_p \backslash \{0, \pm\frac{2}{3}\}$.
For such a x there are $p - \left(\frac{9x^2-4}{p}\right)$ points with this x-coordinate. As ρ_1 acts on this fibre and all orbits have the same length we see that the length of these orbits must divide either $p-1$ or $p+1$. Therefore the order of τ_1 must divide $\operatorname{lcm}(p-1, p+1) = \frac{1}{2}(p^2-1)$.
Now let $g \in \mathbb{F}_{p^2}^\times$ be a generator. For $g_1 = g^{p+1}$ we see that $g_1^p = g^{p^2+p} = g^{p+1} = g_1$, so $g_1 \in \mathbb{F}_p$ and for $x = \frac{1}{3}(g_1 + g_1^{-1})$ we have $\lambda_x = g_1$. Moreover we have $x \notin \{0, \pm\frac{2}{3}\}$ as that implies $g_1^2 \in \{\pm 1\}$ which does not happen for $p > 5$. So we see that on the points with x as the first coordinate ρ_1 has order $p - 1$.
For $g_2 = g^{p-1}$ we again write $x = \frac{1}{3}(g_2 + g_2^{-1})$ and we see that

$$x^p = 3^{-p}(g_2^p + g_2^{-p}) = 3^{-1}(g^{p^2-p} + g^{p-p^2}) = 3^{-1}(g_2^{-1} + g_2) = x,$$

so this x also lies in $\mathbb{F}_p$. We again have that $x \notin \{0, \pm\frac{2}{3}\}$ as $g_2^2 \notin \{\pm 1\}$ so we see that ρ_1 has order $p + 1$ on the points with x as the first coordinate. So we see that the order of ρ_1 on all points must be equal to $\operatorname{lcm}(p-1, p+1) = \frac{1}{2}(p^2 - 1)$.
We proceed to the case where $p \equiv 1 \bmod 4$. For $p > 5$ we also get that on the points with x-coordinate not $0, \pm\frac{2}{3}$ that ρ_1 has order $\frac{1}{2}(p^2 - 1)$. For $x = 0$ we see that L_x^4 is the identity matrix and acting on $(0, 1, i)$ we also have a point in G_p on which ρ_1 has order 4. For $x = \frac{2}{3}$ we see that L_x has eigenvalue 1 twice and is not diagonalizable. As a Jordan block we see that L_x^p is the indentity in $\mathbb{F}_p$. So the order of ρ_1 acting on points with the first coordinate equal to $\frac{2}{3}$ is some divisor of p. For $x = -\frac{2}{3}$ we see that L_x has a double eigenvalue -1 and is also not diagonalizable. Therefore L_x has order $2p$ over $\mathbb{F}_p$. Acting on the point $P = (-\frac{2}{3}, 0, \frac{2i}{3})$ we see that $\rho_1^p(P) = -P \neq P$ and $\rho_1^2(P) = (-\frac{2}{3}, \frac{4i}{3}, -2i) \neq P$ so ρ_1 acting on this point has order $2p$. So the order of ρ_1 acting on all points of G_p is equal to $\operatorname{lcm}(p-1, p+1, 4, 2p) = \frac{1}{2}(p^3 - p)$. For $p = 5$ we can separately check that the order is 60.

□

5.1.3 Steps in SPFA

As suggested by the title *A Heuristic Subsexponential Algorithm to Find Paths in Markoff Graphs over Finite Fields* of [30] SPFA depends on some different heuristics. There are two heuristic assumptions which are both related to maximally elliptic elements that will be used. As input for SPFA we need a prime $p > 5$ and two vertices $P, Q \in G'_p$, the output will be a path from P to Q in G'_p.

1. The first step consists of randomly applying ρ_1, ρ_3 to P until we reach a point P' such that the y-coordinate $y(P')$ of P' is maximally elliptic. We define $H_1(p)$ to be expected value of the number steps we have to perform until we find such a P'. The heuristic assumption here is that $H_1(p)$ is relatively small. We will look at $H_1(p)$ in more detail in the last section of this chapter.

2. Similarly to the first step ρ_1^{-1} and ρ_2^{-1} will be randomly applied to Q until a point Q' is found with a maximally elliptic z-coordinate $z(Q')$. Again the expected value of the number of steps here is equal to $H_1(p)$ by symmetry.

3. Let $F(X, Y, Z) = X^2 + Y^2 + Z^2 - 3XYZ$. In the third step randomly we sample maximally elliptic x_0 until there is a value such that $F(x_0, y(P'), Z) = F(x_0, Y, z(Q')) = 0$ has a solution $(y_0, z_0) \in \mathbb{F}_p^2$. The second Heuristic assumption is that the probability $1/H_2(p)$ that such a pair (y_0, z_0) exists is not too small. Then $H_2(p)$ is the expected number of samples we have to make until we find a good x_0.

4. We now define $P'' = (x_0, y(P'), z_0)$ and $Q'' = (x_0, y_0, z(Q'))$. Then by construction and Proposition 5.1.1 we see that P' and P'' are in the same ρ_2-orbit, P'' and Q'' are in the same ρ_1-orbit and Q'' and Q' are in the same ρ_3-orbit. We calculate these three paths by solving a discrete logarithm problem.

5. At last we combine paths from P to P', P' to P'', P'' to Q'', Q'' to Q' and Q' to Q to make a path from P to Q.

5.2 Heuristics

The two heuristic assumptions are both related to maximally elliptic coordinates of vertices in G_p. For a prime $p > 5$ we let $M_p^{(x)}$ be the Bernoulli-distributed random variable that indicates whether the x-coordinate of a vertex in G'_p is maximally elliptic. Here we choose the vertex uniformly at random in G'_p. Moreover let N_p be the Bernoulli-distributed random variable that indicates for uniformly random chosen $t, a, b \in \mathbb{F}_p$ whether t is maximally elliptic and there exist $y, z \in \mathbb{F}_p$ such that $F(t, a, z) = F(t, y, b) = 0$.
In [30] the author estimates $\mathbb{P}(M_p^{(x)} = 1)$ by $\frac{1}{2}\varphi(p-1)/(p-1)$ and $\mathbb{P}(N_p = 1)$ by $\frac{1}{8}\varphi(p-1)/p$. In this section we prove our own exact results for these probabilities in Corollary 5.2.3 and Corollary 5.2.6.

Lemma 5.2.1 ([30]). *For $p > 3$ the number of elements in $\mathbb{F}_p$ that are maximally elliptic is equal to $\frac{1}{2}\varphi(p-1)$.*

Proof. We note that if $\lambda \in \mathbb{F}_p^\times$ is a root of $P(T) = T^2 - 3xT + 1$, then so is λ^{-1} and this happens if and only if $3x = \lambda + \lambda^{-1}$. We write X_p for the set of primitive roots in $\mathbb{F}_p^\times$, then the map $f : X_p \to \mathbb{F}_p$ defined by $\lambda \mapsto \frac{1}{3}(\lambda + \lambda^{-1})$ is surjective onto the maximally elliptic elements in $\mathbb{F}_p$. Moreover we see for $\lambda, \mu \in X_p$ that $f(\lambda) = f(\mu)$ if and only if $(\lambda - \mu)(\lambda\mu - 1) = 0$. Since for any primitive root λ its inverse λ^{-1} is also a primitive root we see that f is 2-to-1 and the number of maximally elliptic elements in $\mathbb{F}_p$ is equal to $\frac{1}{2}|X_p| = \frac{1}{2}\varphi(p-1)$. □

Proposition 5.2.2. *Let $p > 5$ and let $\mathcal{M}(\mathbb{F}_p)_x^{gen}$ be the set of vertices in G_p such that the x-coordinate is maximally elliptic. Then we have that*

$$\#\mathcal{M}(\mathbb{F}_p)_x^{gen} = \frac{(p-1)\varphi(p-1)}{2}$$

Proof. As we have $p > 5$, we see that $0, \pm\frac{2}{3}$ are not maximally elliptic. For a maximally elliptic $x \in \mathbb{F}_p$ we see that $T^2 - 3xT + 1$ has two roots in $\mathbb{F}_p$, so the discriminant $9x^2 - 4$ of this polynomial is a non-zero square in $\mathbb{F}_p$. Moreover we see that the number of vertices in G_p with x as the first coordinate is equal to

$$\sum_{y\in\mathbb{F}_p} 1 + \left(\frac{9x^2y^2 - 4y^2 - 4x^2}{p}\right) = p + \sum_{y\in\mathbb{F}_p}\left(\frac{(9x^2-4)y^2 - 4x^2}{p}\right) = p - \left(\frac{9x^2-4}{p}\right) = p - 1.$$

So as there are $\frac{1}{2}\varphi(p-1)$ maximally elliptic elements in $\mathbb{F}_p$ we see that $\mathcal{M}(\mathbb{F}_p)_x^{\text{gen}}$ has exactly $\frac{1}{2}\varphi(p-1)(p-1)$ elements. □

Corollary 5.2.3. *For $p > 5$ the probability $\mathbb{P}\big(M_p^{(x)} = 1\big)$ is equal to*

$$\frac{(p-1)\varphi(p-1)}{2p^2 + 6p(-1)^{(p-1)/2}}.$$

Remark 5.2.4. The author in [30] estimates this probability to be $\varphi(p-1)/(2p-2)$. As we have

$$\frac{(p-1)\varphi(p-1)/(2p^2+6p(-1)^{(p-1)/2})}{\varphi(p-1)/(2p-2)} = \frac{1 - \frac{2}{p} + \frac{1}{p^2}}{1 + \frac{3(-1)^{(p-1)/2}}{p}} = 1 + \frac{1}{p}\left(\frac{-2 \mp 3 + p^{-1}}{1 \pm 3p^{-1}}\right)$$

we see that the estimate agrees quite well for large p.

5.2.1 Estimates for $H_1(p)$

In [30] the author takes some random point $(x_0, y_0, z_0) \in G'_p$ and randomly generate $i_n \in \{2, 3\}$ for $n \geq 1$ to define $(x_n, y_n, z_n) = \rho_{i_n}(x_{n-1}, y_{n-1}, z_{n-1})$. The author claims that we can view x_n as independent random element in $\mathbb{F}_p$. So therefore we can estimate $H_1(p)$ to be one over the probability that some x-coordinate of a point in G'_p is maximally elliptic, this would give

$$H_1(p) \approx \frac{1}{\mathbb{P}\big(M_p^{(x)} = 1\big)} = \frac{2p^2 \pm 6p}{(p-1)\varphi(p-1)},$$

where the sign is positive if $p \equiv 1 \bmod 4$ and negative for $p \equiv 3 \bmod 4$. For instance in [26] effective bounds are given that $n/\varphi(n) \leq \frac{5}{2}\log\log(n)$ for $n > 2000$, which shows that this approximation for $H_1(p)$ is less than $6\log\log(p)$ for $p > 2000$. Some experiments on this can be reproduced with the code in A.6.

As a different experiment we also generated 50 random primes p that have 256 bits. For each prime we simulated the process of randomly applying ρ_1 and ρ_3 to a random starting vertex until the y-coordinate is maximally elliptic 10000 times. This gave 50 estimates of $H_1(p)$ for different primes which are 6.6 on average and the largest value was 12.0. It should however be noted that a few time-outs appeared in the factoring of $p - 1$. As this happens when $p - 1$ has very large prime factors this skews the data in the experiment. It is however expected that in this case we would get a relatively low value of $H_1(p)$, as $\varphi(p-1)/(p-1)$ will be relatively big. As an extra verification we tried three Sophie Germain primes of 1024 bits, which should be the worst-case scenario for factoring $p - 1$, and after 10000 tries we got an approximate value for $H_1(p)$ of 3.6 for all three primes.

5.2.2 Estimates for $H_2(p)$

For the second probabilistic step in SPFA we are given some $a, b \in \mathbb{F}_p$ and want to find a maximally elliptic x_0 such that $F(x_0, a, Z) = F(x_0, Y, b) = 0$ has a solution for (Y, Z). We call a triple (x_0, a, b) a good triple if $F(x_0, a, Z) = F(x_0, Y, b) = 0$ has a solution. To solve for Z we get the equation

$$x_0^2 + a^2 + Z^2 - 3x_0aZ = 0,$$

which is a quadratic in the variable Z so this has a solution if and only if the discriminant is a square in $\mathbb{F}_p$. We define

$$\Delta_{x_0}(x) = 9x_0^2x^2 - 4(x_0^2 + x^2)$$

and we see that the discriminant is equal to $\Delta_{x_0}(a)$. By symmetry we see that there is a solution for Y if and only if $\Delta_{x_0}(b)$ is a square. So we see that (x_0, a, b) is a good triple if and only if $\Delta_{x_0}(a)$ and $\Delta_{x_0}(b)$ are both squares in $\mathbb{F}_p$. If we reverse the question by fixing x_0 and asking how many $a, b \in \mathbb{F}_p$ exist such that (x_0, a, b) is a good triple we can count this in the following lemma.

Lemma 5.2.5. *Let $p > 5$ and x_0 a maximally elliptic element of $\mathbb{F}_p$. Then the number of $(a, b) \in \mathbb{F}_p^2$ such that (x_0, a, b) is a good triple is equal to $\frac{1}{4}(p + 1)^2$.*

Proof. As we have seen before there is a solution (Y, Z) for a triple (x_0, a, b) if and only if $\Delta_{x_0}(a)$ and $\Delta_{x_0}(b)$ are both squares in $\mathbb{F}_p$. By symmetry we can count the number of $a \in \mathbb{F}_p$ such that $\Delta_{x_0}(a)$ is a square and then square that number to count the pairs (a, b). First of all we count how many $a \in \mathbb{F}_p$ there are such that $\Delta_{x_0}(a) = 0$, this gives the equation $(9x_0^2 - 4)a^2 = 4x_0^2$. As $p > 5$ we see that both $9x_0^2 - 4$ and $4x_0^2$ are non-zero squares. Thus there are two solutions for a such that $\Delta_{x_0}(a) = 0$. Furthermore we want to count a such that $\left(\frac{\Delta_{x_0}(a)}{p}\right) = 1$. So we see that the number of a such that $\Delta_{x_0}(a)$ is a square is equal to

$$1 + \sum_{a\in\mathbb{F}_p} \frac{1}{2} + \frac{1}{2}\left(\frac{\Delta_{x_0}(a)}{p}\right) = \frac{p+2}{2} + \frac{1}{2}\sum_{a\in\mathbb{F}_p}\left(\frac{(9x_0^2-4)a^2 - 4x_0^2}{p}\right) = \frac{p+2}{2} - \frac{1}{2}\left(\frac{9x_0^2-4}{p}\right) = \frac{p+1}{2}.$$

Here we again used Lemma 2.2.3 to simplify the sum over Legendre symbols. □

Corollary 5.2.6. *For $p > 5$ the probability $\mathbb{P}(N_p = 1)$ is equal to*

$$\frac{\varphi(p-1)(p+1)^2}{8p^3}$$

Remark 5.2.7. The author in [30] estimates this probability to be $\varphi(p - 1)/8p$. As we have

$$\frac{\varphi(p-1)(p+1)^2/8p^3}{\varphi(p-1)/8p} = 1 + 2p^{-1} + p^{-2}$$

we see that this estimate agrees quite well for large p.

We saw that $H_2(p)$ is the estimated number of x_0 we have to sample before we find one that is maximally elliptic and (x_0, a, b) is a good triple. If we consider all samples of x_0 as independent variables, the expected value of $H_2(p)$ equal to $8p^3/(\varphi(p - 1)(p + 1)^2)$. However this is not the case as a, b are both fixed in the process, so this is only an estimate. For small primes p there exist $(a, b) \in \mathbb{F}_p^2$ such that there are no maximally elliptic x_0 such that (x_0, a, b) is a good triple, so $H_2(p)$ can be infinite. Moreover with the same estimate for $n/\varphi(n)$ for $n \geq 2000$ as before we see that

$$\frac{8p^3}{\varphi(p-1)(p+1)^2} < \frac{20p^3}{(p-1)(p+1)^2}\log\log(p) < 20\log\log(p)$$

We looked at the following experiment for various primes p. We generate two random vertices in G'_p, and take a to be the y-coordinate of the first point and b to be the z-coordinate of the second point. Then we count how many maximally elliptic x_0 there are such that (x_0, a, b) is a good triple. From this we calculate the conditional probability $P_1 = \mathbb{P}(N_p = 1|t \text{ is maximally elliptic})$. For this we count all possibilities to get an exact value for P_1.

As $H_2(p)$ is the expected value of a geometric distribution, $H_2(p)$ is equal to one over the probability of success of the repeated Bernoulli process. So we want to know the probability of a uniformly sampled x_0 in $\mathbb{F}_p$ and a, b randomly sampled as coordinates of uniformly randomly sampled vertices that x_0 is maximally elliptic and (x_0, a, b) is a good triple. For this we can multiply the probability P_1 with the probability that x_0 is maximally elliptic. If we compare the estimated values in Corollaries 5.2.3 and 5.2.6 we expect that $P_1 \approx \frac{1}{4}$. This agrees quite well with Table 5.1.

p	431	433	439	443	449	457	461	463	467	479	487
$1/P_1$	4.016	4.355	4.047	3.998	4.254	4.368	4.278	4.094	3.985	3.984	4.035

Table 5.1: The value of P_1 for various p.

5.3 Time complexity

In this section we will focus on the time complexity of SPFA. We will first calculate the time complexity without the three discrete logarithms and the factoring of $p-1$. We will express our answers as bit complexity. Due to the probabilistic nature of the algorithm we consider the average time complexity. We will then determine the time complexity of the algorithm with all steps in the case that $p-1$ is k-smooth. This means that $p-1$ has no prime factors greater than k.

5.3.1 General case

To count the time complexity we count two different actions. We count how the number of random bits that have to be generated and we calculate the total time complexity of all steps in the algorithm without the factorization of $p-1$ and the three discrete logarithms.

First of all we will count how many random bits we expect to use. In the first step we apply random rotations to P and Q until some coordinate is maximally elliptic. As we choose between two rotations each time we need just one random bit. Moreover we expect to repeat this $H_1(p)$ times, so the first part needs $2H_1(p)$ random bits.

For the second part we sample random elements of $\mathbb{F}_p$ and expect to do this $H_2(p)$ times. As elements in $\mathbb{F}_p$ have $\log_2(p)$ bits we have to generate $\log_2(p)$ random bits. We see that the expected number of random bits is equal to $2H_1(p) + H_2(p)\log_2(p)$. We can use estimates from the previous subsection to get

$$2H_1(p) + H_2(p)\log_2(p) < 12\log\log(p) + 20\log\log(p)\log_2(p).$$

We now proceed to the time complexity of SPFA. The main goal is to prove the following proposition.

Proposition 5.3.1. *The SPFA algorithm has an average time complexity of*

$$O((\log(p))^3(\log\log(p))^2)$$

apart from the three discrete logarithms and the factorization of $p-1$.

Lemma 5.3.2. *To check whether an element in $\mathbb{F}_p$ is maximally elliptic has a time complexity of at most*

$$O(\log(p)^3 \log\log(p)).$$

Proof. As we want to express our answer in time, we also consider the time necessary to make a multiplication of two numbers of size around p. At the moment the algorithm in [16] is the fastest and runs in $O(\log(p)\log\log(p))$ time. We will write $M(n)$ for the time it takes for multiplication of integers less than n.

To check whether an element in $\mathbb{F}_p$ is maximally elliptic we first have to determine whether $T^2 - 3tT + 1$ has a root and if so we need to calculate this root. To check if such a root exist we need to know if the discriminant $9t^2 - 4$ is a square in $\mathbb{F}_p$. As described in [22] calculating a Jacobi symbol takes $O(\log(p)^2)$ time. To calculate a root we have to determine the square root of this discriminant, which can be calculated with in $O(\log(p)^3)$ time [22].

To verify whether some element λ in a generator of $\mathbb{F}_p^\times$ we can calculate $\lambda^{(p-1)/q}$ for all prime divisors q of $p-1$, then λ generates $\mathbb{F}_p^\times$ if and only if $\lambda^{(p-1)/q} \neq 1$ for all q. Such an exponentiation takes $O(M(p)\log(p))$ time. Moreover we can bound the number of different prime factors of $p-1$ by $\log(p-1)$ for $p > 7$. Therefore all these exponentiations take $O(M(p)\log(p)^2)$ time. So we see that the total time complexity is

$$O(\log(p)M(p)) + O(\log(p)^3) + O(\log(p)^2 M(p)) = O(\log(p)^3 \log\log(p)).$$

□

Proof of Proposition 5.3.1. In the first two steps of the algorithm we expect to $2H_1(p)$ times have a step where we have to verify whether an element in $\mathbb{F}_p$ is maximally elliptic and apply a rotation. This has a time complexity of $O(H_1(p)\log(p)^3\log\log(p))$, and by the estimation from the previous section we have $H_1(p) = O(\log\log(p))$, so we see that the first part already takes $O((\log(p))^3(\log\log(p))^2)$ time.

For the third step we expect to verify $H_2(p)$ times whether some element is maximally elliptic, which again has a time complexity of $O((\log(p))^3(\log\log(p))^2)$. In the last part need to calculate three square roots for the discrete logarithm which only has a time complexity of $O(\log(p)^3)$. We can add everything up to see that the algorithm has a time complexity of $O((\log(p))^3(\log\log(p))^2)$. □

Remark 5.3.3. The current algorithm with the best theoretical asymptotic time complexity to factor an integer n is the general number field sieve which has time complexity [23]

$$\exp\left(\left((64/9)^{1/3} + o(1)\right)(\log(n))^{1/3}(\log\log(n))^{2/3}\right).$$

As SPFA requires the factorization of $p-1$, this takes way more time than the part we count in 5.3.1. Computing a discrete logarithm is also a computationally hard task. The current best known time complexity for a discrete logarithm in $\mathbb{F}_p$ is

$$L_p\left[\frac{1}{3}, 1.923\right] = \exp\left(\left(1.923 + o(1)\right)(\log(n))^{1/3}(\log\log(n))^{2/3}\right).$$

according to [22].

5.3.2 Smooth case

In this subsection we will see why the total SPFA is quite fast when we work with a prime p where $p-1$ is smooth. This means that $p-1$ has only small prime factors. In particular we will assume $p-1$ to be k-smooth, which means that $p-1$ has no prime factors greater than k.

Proposition 5.3.4. *If $p-1$ is k-smooth SPFA has a time complexity of*

$$O(k\log(k)+k/\log(k)\cdot\log(p)\log\log(p)+\sqrt{k}\log(p)^2\log\log(p)+\log(p)^3(\log\log(p))^2).$$

Lemma 5.3.5. *If n is k-smooth we can factor it in a time complexity of*

$$O(k\log(k)+k/\log(k)\cdot\log(n)\log\log(n)+\log(n)^2\log\log(n))$$

Proof. To factor n we start off by using a sieve to find all primes less than k. This can be done in $O(k/\log\log(k))$ operations [24], so in bit complexity this takes

$$O(k/\log\log(k)M(k))=O(k\log(k))$$

time. This will give less than $2k/\log(k)$ primes, and for each prime we check whether it divides n. This takes $O(k/\log(k)M(n))=O(k/\log(k)\cdot\log(n)\log\log(n))$ time. At last we have less than $\log_2(n)$ primes that divide n, so to count the exponents for the prime factorization takes $O(\log(n)M(n))=O(\log(n)^2\log\log(n))$ time. If we add up these running times we see that this factorization can indeed be done in the proposed time complexity. All three terms can dominate the sum in the running time dependent on the relation between k and n. □

Lemma 5.3.6. *If $p-1$ is k-smooth we can calculate a discrete logarithm in*

$$O(\log(p)^3\log\log(p)+\sqrt{k}\log(p)^2\log\log(p))$$

time.

Proof. We write $p-1=\prod_{i=1}^n p_i^{e_i}$. We can use the Pohlig-Hellman algorithm for this problem that has a complexity of $O(\sum_{i=1}^n e_i(\log(p-1)+\sqrt{p_i}))$ group operations [22]. We estimate the two sums separately. For the first sum we have that

$$\sum_{i=1}^n e_i=\log\left(\prod_{i=1}^n 2^{e_i}\right)\leq\log_2\left(\prod_{i=1}^n p_i^{e_i}\right)=\log_2(p-1).$$

Moreover as $p-1$ is k-smooth we see that $p_i\leq k$ for all i, so we also get that

$$\sum_{i=1}^n e_i\sqrt{p_i}\leq\sum_{i=1}^n e_i\sqrt{k}\leq\sqrt{k}\log_2(p-1).$$

If we combine this we see that

$$\sum_{i=1}^n e_i(\log(p-1)+\sqrt{p_i})\leq(\log(p-1)+\sqrt{k})\log_2(p-1)$$

As the group operation is multiplication in $\mathbb{F}_p^\times$ we see that this takes $M(p)=O(\log(p)\log\log(p))$ time. If we multiply the number of group operations with this time we get our final time complexity. □

Proof of Proposition 5.3.4. We combine Proposition 5.3.1, Lemma 5.3.6 and Lemma 5.3.5 and add all the time complexities. □

Remark 5.3.7. If we would have some fixed $\epsilon>0$ such that $k\approx p^\epsilon$ then the time complexity in Proposition 5.3.4 is dominated by the $k\log(k)$ term. This arises from the factoring of $p-1$, which is therefore the bottleneck for SPFA.

Appendix A

Extra figures and code

A.1 Some more graphs

In this section we have two figures of Markov graphs G_p for $p = 5$ and $p = 7$. To create more figures one could use the code from A.3 and export these figures from Mathematica.

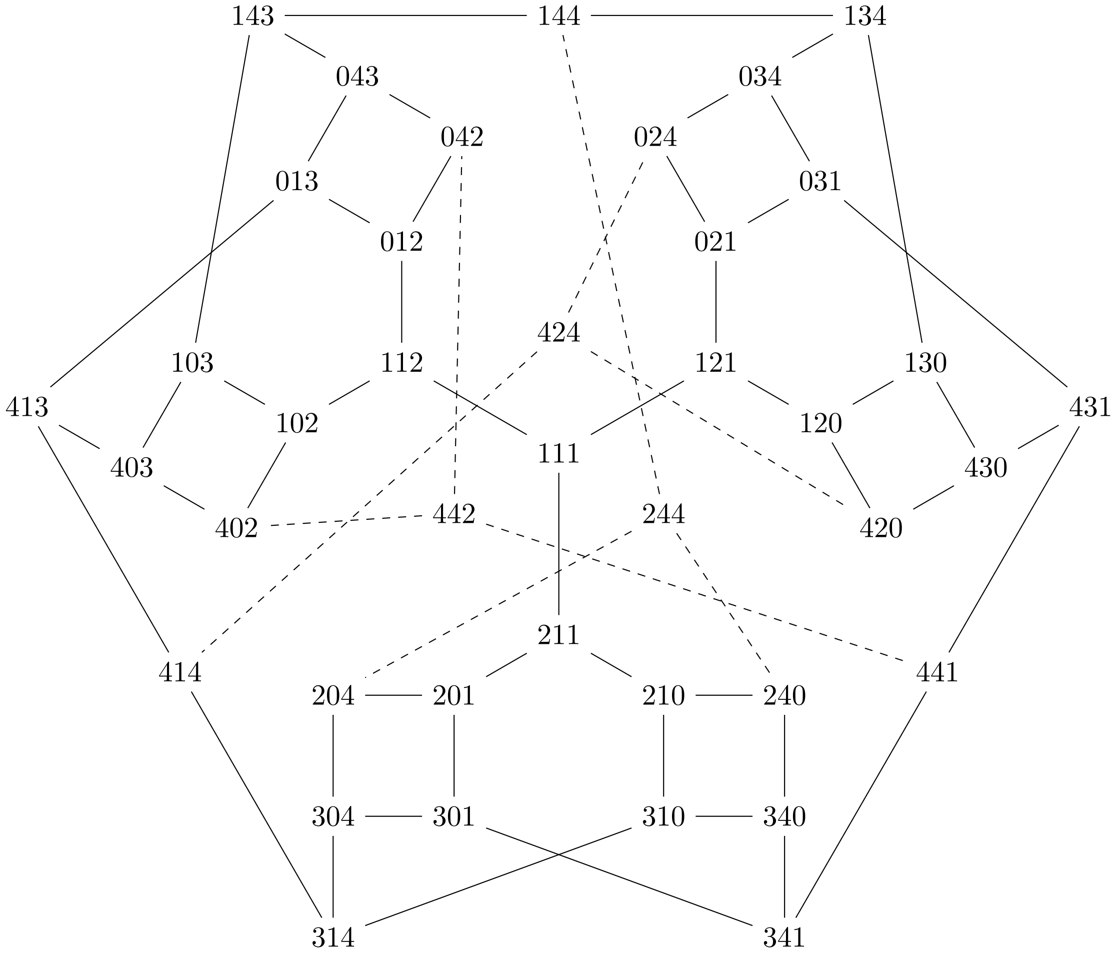


Figure A.1: The graph G_5

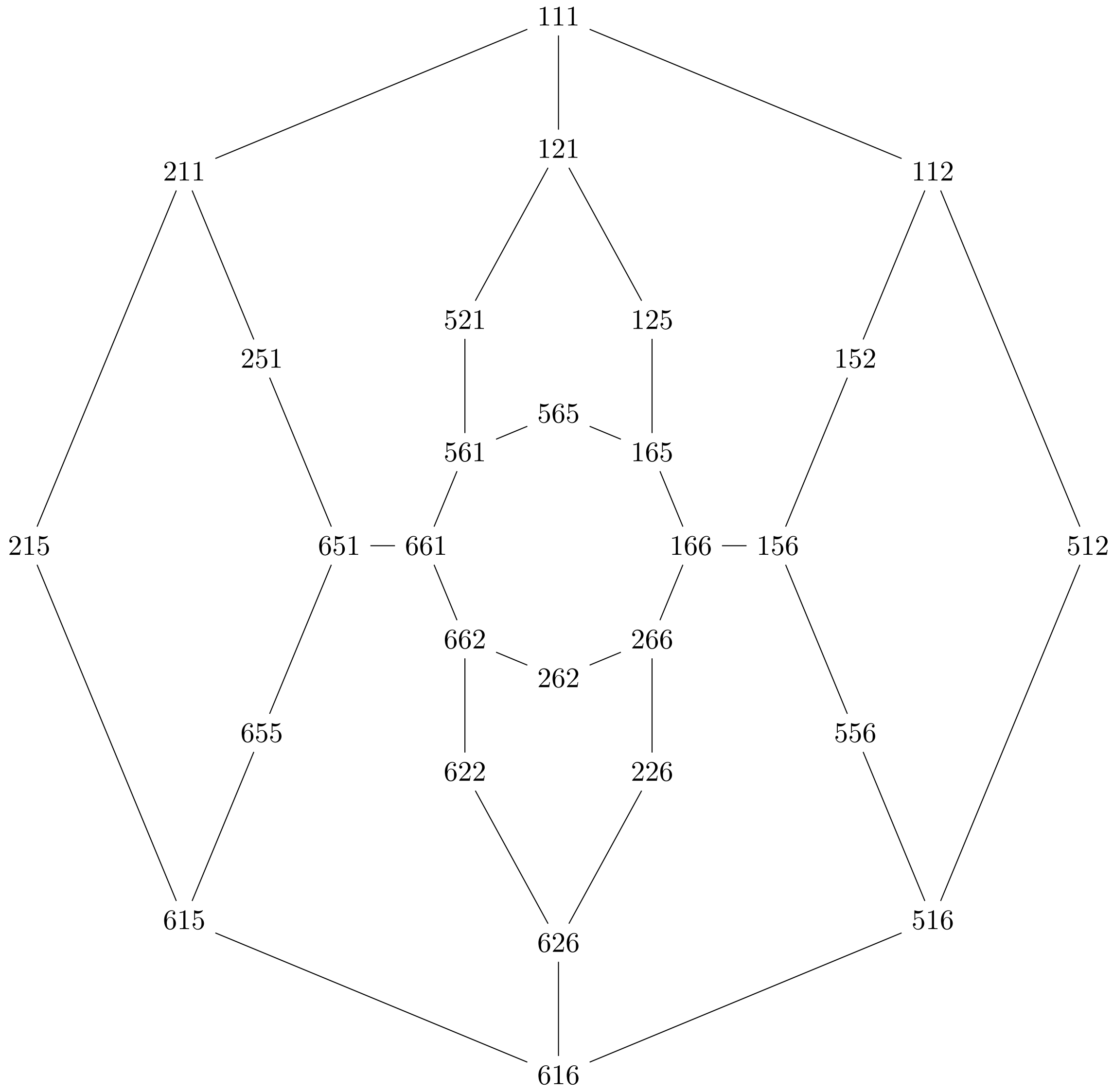


Figure A.2: The graph G_7

A.2 Sage code

In this section different Sage programs are listed that are used in various parts of this thesis. In this section code is listed that can be used to create the Markov graph G_p as an object in Sage. Moreover there is also code to export this to an object in Mathematica. At last there is also code to reproduce ideas from Section 4.2 and find ideals related to some word.

```
def tau1(A,a):
    return [a*A[1]*A[2]-A[0], A[1], A[2]]
def tau2(A,a):
    return [A[0], a*A[0]*A[2]-A[1], A[2]]
def tau3(A,a):
    return [A[0], A[1], a*A[0]*A[1]-A[2]]
```

Listing A.1: The involutions that are used in most other commands

```
def graphmaker(q,a,b):
    R = GF(q, "X")
    Points=[]
    Names={}
    if q%2 == 0:
        for x in R:
            for y in R:
                for z in R:
                    w = x^2+y^2+z^2-a*x*y*z-b
                    if w==0:
                        if x!=0 or y!=0 or z!=0:
                            Points.append((x,y,z))
    else:
        Squares={}
        for x in R:
            Squares[x]=[]
        for x in R:
            Squares[x^2].append(x)
        for y in R:
            for z in R:
                D = (a*y*z)^2-4*(y^2+z^2-b)
                for d in Kwadraten[D]:
                    x = (a*y*z+d)/2
                    if x!=0 or y!=0 or z!=0:
                        Points.append((x,y,z))
    Npoints = len(Points)
    for x in range(Npoints):
        Names[Points[x]]=x
    Edges=[]
    for x in range(Npoints):
        xedges=[]
        A = Points[x]
        n1 = Names[tau1(A,a)]
        n2 = Names[tau2(A,a)]
        n3 = Names[tau3(A,a)]
        for ni in [n1,n2,n3]:
            if ni!=x:
                xedges.append(ni)
        Edges.append(xedges)
    return Points, Edges, Names
```

Listing A.2: This function generates the graph of solutions for the Generalized Markov Equation over $\mathbb{F}_q$.

```
def mathematicagraph(Points, Edges):
    Npoints = len(Points)
    res = "Graph[{"
    for x in range(Npoints-1):
        res+="\"" +str(Points[x])+"\""+","
    res+="\""+str(Points[-1])+"\""+"},␣{"
    first = True
    for x in range(Npoints):
        E=Edges[x]
        for e in E:
            if e<x:
                if not first:
                    res+=",␣"
                res += "\""+str(Points[e])+"\""
                res += "\\[UndirectedEdge]"+"\""
                res += str(Points[x])+"\""
                first = False
    res+="},␣VertexLabels␣->␣Placed[Automatic,␣Above]]"
    return res
```

Listing A.3: This functions exports the graph from the previous function to a string that can be used in Mathematica.

```
def WordIdeal(word, alphabet,a):
    R.<x,y,z> = PolynomialRing(ZZ, 3, order='lex')
    P = [x,y,z]
    a1 = [x,y,z]
    for t in range(len(word)):
        letter = word[t]
        if letter==alphabet[0]:
            a1 = tau1(a1,a)
        elif letter==alphabet[1]:
            a1 = tau2(a1,a)
        elif letter==alphabet[2]:
            a1 = tau3(a1,a)
        else:
            print("One␣of␣the␣letters␣is␣not␣in␣the␣alphabet.")
    I = R.ideal([x^2+y^2+z^2-x*y*z,a1[0]-P[0],a1[1]-P[1],a1[2]-P[2]])
    return I
```

Listing A.4: This function needs a word and returns the ideal of the points which such a cycle starts.

A.2.1 SPFA-related code

In this subsection some code related to the SPFA can be found. In particular we have listed Sage functions to check whether some element in $\mathbb{F}_p$ is maximally elliptic and two functions that repeat the experiments from [30].

```
def MaximalEllipticQ(x,q,factors):
    A = 9*x*x-4
    if kronecker(A,q)!=1:
        return False
    sr = mod(A,q).sqrt()
    L = (3*x+sr)/2
    L = int(L)
    for f in factors:
        macht = (q-1)//f[0]
        T = pow(L,macht,q)
        if T==1:
            return False
    return True
```

Listing A.5: This function checks whether some element of $\mathbb{F}_p$ is maximally elliptic

```
def Heur2testcase(p, P, factors):
    tel=0
    while not MaximalEllipticQ(P[1],p,factors):
        a = randint(0,1)
        if a==0:
        P=rho1(P,p)
        tel+=1
        else:
        P=rho3(P,p)
        tel+=1
    return tel
def Heuristic2(p, N):
    factors = list((p-1).factor())
    tot = 0
    for x in range(N):
        P = RandomPointpgroot(p)
        tot+=Heur2testcase(p,P,factors)
return tot/N
```

Listing A.6: This function approximates $H_1(p)$ by simulation.

```
def Heuristic3case(t,a,b,p,factors):
    D1 = 9*a^2*t^2-4*(t^2+a^2)
    if kronecker(D1,p)==-1:
        return False
    D2 = 9*b^2*t^2-4*(t^2+b^2)
    if kronecker(D2,p)==-1:
        return False
    if MaximalEllipticQ(t,p,factors):
        return True
    return False
def Heuristic3(p, N):
    tot = 0
    factors = list((p-1).factor())
    for x in range(N):
        t = randint(0,p-1)
        a = randint(0,p-1)
        b = randint(0,p-1)
        if Heuristic3case(t,a,b,p,factors):
            tot+=1
    return tot/N
```

Listing A.7: This function approximates $H_2(p)$ by simulation.

```
# Table 6
N = 100000
for p in [17389,48611,55163,70687,104729,200560490131]:
    k3 = (2*(p-1)/euler_phi(p-1)).n()
    k4 = Heuristic2(p,N).n()
    print(”{:>13}␣␣{:>9.5f}␣␣{:>9.5f}”.format(p, k3,k4))

# Table 8
N = 100000
for p in [17389,48611,55163,70687,104729,200560490131]:
    k3 = (euler_phi(p-1)/(8*p-8)).n()
    k4 = Heuristic3(p,N).n()
    print(”{:>13}␣␣{:>9.5f}␣␣{:>9.5f}”.format(p, k3,k4))
```

Listing A.8: Here the experiments from [30] are repeated

Bibliography

[1] Martin Aigner. *Markov's Theorem and 100 Years of the Uniqueness Conjecture: A Mathematical Journey from Irrational Numbers to Perfect Matchings.* Jan. 2013.

[2] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. *Markoff Surfaces and Strong Approximation: 1.* 2016. arXiv: `1607.01530 [math.NT]`.

[3] Martin Bright. *The Picard group.* Mathematics Research Centre, University of Warwick, UK, Apr. 2008. eprint: `https://homepages.warwick.ac.uk/~maseap/arith/notes/picard.pdf`.

[4] Leonard Carlitz. "Certain Special Equations in a Finite Field." In: *Monatshefte für Mathematik* 58 (1954), pp. 5–12.

[5] Denis Charles, Kristin Lauter, and Eyal Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22 (Dec. 2008), pp. 93–113.

[6] William Chen. *Nonabelian level structures, Nielsen equivalence, and Markoff triples.* 2021. arXiv: `2011.12940 [math.NT]`.

[7] Jean-Louis Colliot-Thélène, Dasheng Wei, and Fei Xu. *Brauer-Manin obstruction for Markoff surfaces.* 2019. arXiv: `1808.01584 [math.NT]`.

[8] Matthew de Courcy-Ireland. *Non-planarity of Markoff graphs mod p.* Sept. 2022. arXiv: `2105.12411 [math.NT]`.

[9] Matthew de Courcy-Ireland and Seungjae Lee. *Experiments with the Markoff surface.* 2018. arXiv: `1812.07275 [math.NT]`.

[10] Harold Davenport. *Multiplicative Number Theory.* Lectures in advanced mathematics. Markham Publishing Company, 1967.

[11] Jan-Hendrik Evertse. *Lecture notes Analytic Number Theory, Chapter 4: The Riemann zeta function and L-functions.* 2020.

[12] Elena Fuchs et al. *A Cryptographic Hash Function from Markoff Triples.* 2021. arXiv: `2107.10906 [cs.CR]`.

[13] Elena Fuchs et al. *Orbits on K3 Surfaces of Markoff Type.* 2022. arXiv: `2201.12588 [math.AG]`.

[14] Shafi Goldwasser and Mihir Bellare. "Lecture Notes on Cryptography". In: July 2008. eprint: `https://cseweb.ucsd.edu/~mihir/papers/gb.pdf`.

[15] Robin Hartshorne. *Algebraic Geometry.* Vol. 52. Graduate Texts in Mathematics. Springer, 1977.

[16] David Harvey and Joris van der Hoeven. "Integer multiplication in time $O(n \log n)$". English. In: *Ann. Math. (2)* 193.2 (2021), pp. 563–617.

[17] Helmut Hasse. "Zetafunktion und L-funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus". In: *Akademie-Verslag* (1955).

[18] Marc Hindry. *Introduction to zeta and L-functions from arithmetic geometry and some applications.* 2010.

[19] Kazuo Iwama and Takuya Nakashima. "An Improved Exact Algorithm for Cubic Graph TSP". In: *Computing and Combinatorics*. Ed. by Guohui Lin. Springer Berlin Heidelberg, 2007, pp. 108–117.

[20] Andrey Markoff. "Sur les formes quadratiques binaires indéfinies". fre. In: *Mathematische Annalen* 15 (1879), pp. 381–406. URL: `http://eudml.org/doc/156864`.

[21] Andrey Markoff. "Sur les formes quadratiques binaires indefinies. (Second mémoire)". In: *Mathematische Annalen* 17 (1880), pp. 379–399. URL: `http://eudml.org/doc/156934`.

[22] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 2001.

[23] Carl Pomerance. "A Tale of Two Sieves". In: *Notices of the American Mathematical Society 43* (1996).

[24] Paul Pritchard. "Linear prime-number sieves: A family tree". In: *Science of Computer Programming* 9.1 (1987), pp. 17–35.

[25] Moshe Rosenfeld. "Independent sets in regular graphs". In: *Israel Journal of Mathematics* (Dec. 1964).

[26] John Barkley Rosser and Lowell Schoenfeld. "Approximate formulas for some functions of prime numbers". In: *Illinois J. Math.* 6 (1962), pp. 64–94. URL: `http://projecteuclid.org/euclid.ijm/1255631807`.

[27] Jean-Pierre Serre. "Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)". fre. In: *Séminaire Delange-Pisot-Poitou. Théorie des nombres* 11.2 (1969), pp. 1–15. URL: `http://eudml.org/doc/110758`.

[28] Jean-Pierre Serre. "On a theorem of Jordan". In: *Bulletin (New Series) of the American Mathematical society* 40 (Aug. 2003).

[29] Jean-Pierre Serre. "Zeta and L functions". In: *Arithmetical Algebraic Geometry* (1965). [= Oeuvres - Collected Papers II, Springer-Verlag, 1986].

[30] Joseph H. Silverman. *A Heuristic Subexponential Algorithm to Find Paths in Markoff Graphs Over Finite Fields*. 2022. arXiv: `2211.08511 [math.NT]`.

[31] John Tate. "Algebraic cycles and poles of zeta functions". In: *Arithmetical Algebraic Geometry* (1965). [= Collected works of John Tate, American Mathematical Society, 2016].

[32] Mingyu Xiao and Hiroshi Nagamochi. "Confining sets and avoiding bottleneck cases: A simple maximum independent set algorithm in degree-3 graphs". In: *Theor. Comput. Sci.* 469 (2013), pp. 92–104.