UNIVERSITÉ DU LUXEMBOURG

Faculty of Science, Technology and Medicine

Bachelor in Mathematics

Experimental Mathematics 3

Counting Points On Curves Over Finite Fields

Written by
Kim Da Cruz
Dylan Mota
Clara Popescu

Supervised by
Prof. Dr. Gerard van der Geer
Bryan Advocaat

Summer Semester 2021

Abstract

In this experimental mathematics project, we will calculate the number of solutions of an equation in two or three variables over a given finite field for various examples. After some experimentation and key observations, we try to find a closed formula for the number of solutions and we then try to find a similarity between the results of the examples.

In other words, we want to find a general formula for the number of solutions that works for all kind of curves over any finite field.

Contents

1 Introduction

If we look at equations in two variables, that are of the type $f(x, y) = 0$ over the real numbers, then we know, since Descartes that we get a curve. Such equations can also be treated over finite fields of cardinality q and the number of solutions is then finite, since the number of elements in the field is finite. In this project, we will focus on these equations, and we will try to find an explicit formula for the number of solutions, that holds for any given smooth curve over any finite field $\mathbb{F}_q$. Indeed, it is by experimenting and doing heuristics by computer and even by hand that we see some patterns arise.

1.1 Finite Fields

Before starting with our experimentation, let us recall some useful properties of finite fields that will occur throughout this project. The references are the lecture notes from the course "Théorie des nombres et applications à la cryptographie" given by Lassina Dembele. Note that the proofs are left out here.

Proposition 1.1. Let K be a field and $f \in K[x]$ an irreducible polynomial of degree $n \geqslant 0$. Then by setting

$$L := K[x]/\left(f(x)\right),$$

we have the following properties:

(a) L is a finite field that contains K.

(b) There exists $\alpha \in L$ such that $f(\alpha) = 0$, i.e. L contains a zero of f.

(c) Let $\alpha \in L$ be a zero of f, then every $x \in L$ is of the form

$$x = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1},$$

where $b_i \in K$ for all $i \in \{0, \ldots, n-1\}$.

Theorem 1.2. Let p be a prime number and $n \geqslant 1$ an integer.

(a) The number of elements of any finite field K is of the form p^n, where p is the characteristic of K.

(b) There exists a finite field with p^n elements, where any two such fields are isomorphic. We denote this (up to isomorphism) unique field by $\mathbb{F}_{p^n}$.

(c) Let $K \subseteq \mathbb{F}_{p^n}$ be a subfield. Then there exists $m|n$ such that $\#K = p^m$.

(d) Let $m|n$. Then there exists a unique subfield $K \subseteq \mathbb{F}_{p^n}$ with p^m elements and K is the set of all elements $a \in \mathbb{F}_{p^n}$ satisfying $a^{p^m} = a$.

Let us look at an example, where we apply the above notions.

Example 1.3. Consider the finite field $\mathbb{F}_2$. The only polynomial of degree 2 that is irreducible in $\mathbb{F}_2$ is $f(x) = x^2 + x + 1$. From the above Proposition 1.1, we get that $L = \mathbb{F}_2[x]/(f(x))$ is a field containing $\mathbb{F}_2$. Moreover, L has dimension 2, so it follows that it has at most $2^2 = 4$ elements.

By Theorem 1.2, we know that L is the only finite field of 4 elements, which we denote by $\mathbb{F}_4$. Now in order to find the elements of $\mathbb{F}_4$, we look at Proposition 1.1, which says that every element of $\mathbb{F}_4$ is given by

$$x = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1},$$

where α is a zero of f and $b_i \in \mathbb{F}_2$ for all $i = 0, \ldots, n-1$. Hence,

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}.$$

Before we move on to the experimental part, we end this recall with a property of the multiplicative group of a finite field.

Proposition 1.4. Let K be a finite field with p^n elements, where p is a prime and $n \in \mathbb{N}_{\geq 1}$. Then the multiplicative group $K^\times$ is a cyclic group of order p^{n-1}.

2 Counting Points on Curves over Finite Fields

Throughout this document, we suppose that x, y and z are unknown variables in a given finite field and let $n \in \mathbb{N}$ and p be a prime number. Moreover, in the following examples, our goal will be to determine a closed formula for the number of solutions of a given equation over a finite field.

2.1 Examples

Example 2.1. Consider the equation $y^2 + y = x^3 + 1$ over $\mathbb{F}_2$ and let N_n denote the number of solutions of this equation over the finite field $\mathbb{F}_{2^n}$ given by

$$N_n = \#\left\{(x,y) : x, y \in \mathbb{F}_{2^n},\ y^2 + y = x^3 + 1\right\} + 1.$$

Note that in the above formula, we have to add 1 in virtue of the point at infinity. Now, in order to find a closed formula for N_n, we try to construct it *experimentally*. Hence, let us first compute N_1 and N_2.

- We have $N_1 = \#\{(x,y) : x, y \in \mathbb{F}_2,\ y^2 + y = x^3 + 1\} + 1$. To calculate N_1, we first solve the equation $y^2 + y = x^3 + 1$ over $\mathbb{F}_2$ and we get the set of solutions

$$\mathcal{S} = \{(1,0), (1,1)\}.$$

  Therefore, $N_1 = 2 + 1 = 3$.

- We have $N_2 = \#\{(x,y) : x, y \in \mathbb{F}_4,\ y^2 + y = x^3 + 1\} + 1$. Now we solve the equation $y^2 + y = x^3 + 1$ over $\mathbb{F}_4 = \{0, 1, a, a+1\}$ and we obtain

$$\mathcal{S} = \{(1,0), (1,1), (0,a), (0,a+1), (a,0), (a,1), (a+1,0), (a+1,1)\}.$$

  Hence, $N_2 = 8 + 1 = 9$.

Since two values are not enough to deduce a closed formula for N_n, we calculate the proceeding values using Sage. Below follows a table of the first eight values of N_n.

n	1	2	3	4	5	6	7	8
N_n	3	9	9	9	33	81	129	225

Table 1: The first eight values of N_n computed with Algorithm 1.

We do not see immediately a pattern for N_n, that is why we are going to distinguish between the following two cases.

1. **For odd n**: In Table 1, we see a certain pattern, that is

$$N_3 = 4N_1 - 3, \quad N_5 = 4N_3 - 3, \quad N_7 = 4N_5 - 3.$$

   So for $n \geqslant 3$, we can assume that N_n is given by the following recursive formula

$$N_n = 4N_{n-2} - 3, \quad \text{where } N_1 = 3.$$

After having found a recursive formula, it might also be interesting to find a direct formula. By looking individually at each N_n, we observe that

$$N_1 = 3 = 2^1 + 1, \;\; N_3 = 9 = 2^3 + 1, \;\; N_5 = 33 = 2^5 + 1, \;\; N_7 = 129 = 2^7 + 1.$$

Hence, we can assume in this case that N_n is given by the formula

$$N_n = 2^n + 1. \tag{1}$$

2. **For even *n***: Let us examine N_n closely and try to use equation (1). Thus,

$$\begin{aligned} N_2 &= 9 = 2^2 + 1 + 4 = 2^2 + 1 + (-2)^{2/2+1}, \\ N_4 &= 9 = 2^4 + 1 - 8 = 2^2 + 1 + (-2)^{4/2+1}, \\ N_6 &= 81 = 2^6 + 1 + 16 = 2^2 + 1 + (-2)^{6/2+1}, \\ N_8 &= 225 = 2^8 + 1 - 32 = 2^2 + 1 + (-2)^{8/2+1}. \end{aligned}$$

Hence, we can assume in this case that N_n is given by the formula

$$N_n = 2^n + 1 + (-2)^{\frac{n}{2}+1}. \tag{2}$$

Since we want to find a general formula that works for every n, but the formulas for odd and even n are different, we have to combine (1) and (2). So for $k \in \mathbb{N}$, we have

$$N_{2k+1} = 2^{2k+1} + 1 \;\text{ and }\; N_{2k} = 2^{2k} + 1 + (-2)^{k+1}.$$

This allows us to write

$$N_n = 2^n + 1 + x_n(-2)^{\frac{n}{2}+1}, \quad \text{where } x_n = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ 1 & \text{if } n \text{ is even.} \end{cases}$$

Moreover, we can see that

$$x_n(-2)^{\frac{n}{2}+1} = -2x_n(-2)^{\frac{n}{2}} = -x_n(-2)^{\frac{n}{2}} - x_n(-2)^{\frac{n}{2}}.$$

However, it is difficult to find one x_n such that

$$-x_n(-2)^{\frac{n}{2}} - x_n(-2)^{\frac{n}{2}} = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ (-2)^{\frac{n}{2}+1} & \text{if } n \text{ is even.} \end{cases}$$

Therefore, we try to find x_{n_1} and x_{n_2} such that

$$-x_{n_1}(-2)^{\frac{n}{2}} - x_{n_2}(-2)^{\frac{n}{2}} = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ (-2)^{\frac{n}{2}+1} & \text{if } n \text{ is even.} \end{cases}$$

By setting $x_{n_1} := 1$ and $x_{n_2} := (-1)^n$, it is easy to verify that x_{n_1} and x_{n_2} satisfy the above given condition. Hence,

$$\begin{aligned} N_n &= 2^n + 1 - (-2^{\frac{n}{2}}) - (-1)^n(-2^{\frac{n}{2}}) \\ &= 2^n + 1 - (i\sqrt{2})^n - (-i\sqrt{2})^n \\ &= 2^n + 1 - \alpha^n - \overline{\alpha}^n, \qquad \text{where } \alpha = i\sqrt{2}. \end{aligned}$$

Moreover, it is important to remark that one can also use another approach to find a formula for N_n in the case where n is odd. However, this strategy does not require experimentation, but a more *theoretical* thinking. Below, we are going to give a proof for (1) and explain why this approach does not work when n is even.

For this method, we will look separately at the two sides of the equation

$$y^2 + y = x^3 + 1, \quad \text{where } x, y \in \mathbb{F}_q \text{ and } q = 2^n.$$

Let us first analyse the **left hand side** of the above equation. With $\mathbb{F}_q$ being a vector space over $\mathbb{F}_2$, it is easy to check that the map $\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ given by $y \longmapsto y^2 + y$ is a linear map. Then, one might ask what the kernel of φ looks like. Since any quadratic equation has 2 solutions, the kernel of the linear map φ is given by

$$\ker(\varphi) = \{y \in \mathbb{F}_{2^n} : y^2 + y = 0\} = \mathbb{F}_2 = \{0, 1\}.$$

Thus, φ being a linear map over $\mathbb{F}_2$ with its kernel consisting of two elements implies that its image in $\mathbb{F}_q$ consists of $\frac{2^n}{2} = 2^{n-1}$ elements. This means that the number of elements is halved under this map, i.e. that y and $y + 1$ go to the same element.

Now, let us look at the **right hand side** of the equation. For the moment, let us forget about the "+1" and look at what happens when we send x to x^3. Restricting ourselves to the non-zero elements of $\mathbb{F}_q$, we see that they form a multiplicative group, denoted by $\mathbb{F}_q^\times$ and that is cyclic of order $2^n - 1$. One can easily check that the map $\phi : \mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times$ given by $x \longmapsto x^3$ is a homomorphism of groups. Then, the kernel of ϕ consists of the solutions of $x^3 = 1$ in $\mathbb{F}_q^\times$ and is given by

$$\ker(\phi) = \{x \in \mathbb{F}_q^\times : \ x^3 = 1\}.$$

Hence, looking for the solutions of $x^3 = 1$ in $\mathbb{F}_q^\times$, means that we have to look for elements of order 3 in $\mathbb{F}_q^\times$. We conclude that the kernel of ϕ only consists of elements whose order divides 3.

For example, if $n = 3$, then we consider the cyclic group $\mathbb{F}_8^\times$, which has 7 elements. If there is an element of order 3, then it lies in the kernel. From Group Theory, we know that the order of an element divides the order of a group. In this case, the order of the group is 7, which is not divisible by 3. That is why we conclude that there are no elements of order 3 in this group and that the kernel is empty.

In general, 3 is a divisor of $2^n - 1$ if and only if *n is even.* In this case, $\# \ker(\phi) = 3$ since we are in a cyclic group with $n \equiv 0 \mod 3$. This means that every element of the image of ϕ is taken 3 times. However, if *n is odd*, then 3 does not divide $2^n - 1$. This means, that there are no elements of order 3. Thus, the map ϕ has no kernel and is a bijection on $\mathbb{F}_q$.

Finally, we conclude that if n is odd, then $N_n = 2^n + 1$ and if n is even, then ϕ is not a bijection and that is why we have to find N_n using the experimental approach.

Example 2.2. Consider the equation $x^3 + y^3 + z^3 = 0$ in the projective space[1] $\mathbb{P}^2$ over $\mathbb{F}_p$ and let N_p be the number of solutions of the equation in $\mathbb{P}^2$ over $\mathbb{F}_p$ given by

$$N_p = \#\left\{(0,0,0) \neq (x,y,z) : x,y,z \in \mathbb{F}_p,\ x^3 + y^3 + z^3 = 0\right\}.$$

In order to find a general formula for N_p, we consider the following two cases.

First, let us consider the case where $\boldsymbol{p \equiv 2 \mod 3}$. We try to find experimentally a formula for N_p by starting to compute N_2, N_5 and N_{11} by hand.

- For $p = 2$, the solutions of $x^3 + y^3 + z^3 = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_2$ are given by

  $$\mathcal{S} = \{(1,1,0),(1,0,1),(0,1,1)\}.$$

  Therefore, $N_2 = 3$.

- For $p = 5$, the solutions of $x^3 + y^3 + z^3 = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_5$ are given by

  $$\mathcal{S} = \{(0,1,4),(1,0,4),(1,4,0),(1,1,2),(1,2,1),(2,1,1)\}.$$

  Therefore, $N_5 = 6$.

- For $p = 11$, the solutions of $x^3 + y^3 + z^3 = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_{11}$ are given by

  $$\begin{aligned}\mathcal{S} = \{&(0,10,1),(1,4,1),(2,7,1),(3,3,1),(4,1,1),(5,8,1),\\ &(6,9,1),(7,2,1),(8,5,1),(9,6,1),(10,0,1),(10,1,0)\}.\end{aligned}$$

  Therefore, $N_2 = 12$.

In order to make more precise conclusions, we need more values. Hence, below follows a table of the first eight values of N_p calculated with Sage.

p	2	5	11	17	23	29	41	47
N_p	3	6	12	18	24	30	42	48

Table 2: The first 8 values of N_p computed with Algorithm 2.

From Tabel 2, we can assume that N_p is given by the formula

$$N_p = p + 1. \tag{3}$$

We now give a proof that (3) indeed holds for every $p \equiv 2 \mod 3$.

[1] We only look at $(x,y,z) \neq (0,0,0)$ and we consider that (x,y,z) and (cx,cy,cz) with $0 \neq c \in \mathbb{F}_p$ are the same.

Proof. Let p be a prime number such that $p \equiv 2 \mod 3$. Then $p \not\equiv 1 \mod 3$, so that $p - 1 \not\equiv 0 \mod 3$, which implies that $3 \nmid (p-1)$. We already know that the order of the multiplicative group of $\mathbb{F}_p$ is $p-1$ and that it is cyclic. Therefore, we have that $3 \nmid ord\left(\mathbb{F}_p^\times\right)$ and thus, the application

$$\begin{array}{rccc} \phi: & \mathbb{F}_p^\times & \longrightarrow & \mathbb{F}_p^\times \\ & x & \longmapsto & x^3 \end{array}$$

is a bijective homomorphism, thus an isomorphism. This implies that every element of $\mathbb{F}_p^\times$ has a different cube root. So, the number of solutions of $x^3 + y^3 + z^3 = 0$ is the same as for $x + y + z = 0$. In the projective space, $x + y + z = 0$ is the equation of a line. Now, let us find the number of solutions of this equation. By rewriting this equation as $y = -x - z$, we consider the two cases.

- If $x = 0$, this equation has one solution: $(0, y, -y)$ for some fixed $y \in \mathbb{F}_p^\times$.
- If $x \neq 0$, there are p possibilities for z so that the equation has p solutions: $(x, -x-z, z)$ for $z \in \mathbb{F}_p$ and $x \in \mathbb{F}_p$ fixed.

Thus, $N_p = \#\{(0,0,0) \neq (x,y,z) : x,y,z \in \mathbb{F}_p : x^3 + y^3 + z^3 = 0\} = p + 1$. □

Let us now look at the case $\boldsymbol{p \equiv 1 \mod 3}$. In order to find experimentally a formula for N_p, we need to calculate some values of N_p.

For $p = 7$, the solutions of $x^3 + y^3 + z^3 = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_7$ are given by

$$\mathcal{S} = \{(0,3,1),(0,5,1),(0,6,1),(3,0,1),(3,1,0),(5,0,1),(5,1,0),(6,0,1),(6,1,0)\}.$$

Thus, $N_7 = 9$.

For $p > 7$, it is too much to calculate by hand, that is why we used Sage to obtain some more values of N_p and put them in the table below.

p	7	13	19	31	37	43	61	67
N_p	9	9	27	36	27	36	63	63

Table 3: The first 8 values of N_p computed with Algorithm 2.

By analysing in greater detail the values given in the above Table 3, we observe that

$$\begin{array}{ll} N_7 = 9 = 7 + 1 + 1, & N_{13} = 9 = 13 + 1 - 5, \\ N_{19} = 27 = 19 + 1 + 7, & N_{31} = 36 = 31 + 1 + 4, \\ N_{37} = 27 = 37 + 1 - 11, & N_{43} = 36 = 43 + 1 - 8, \\ N_{61} = 63 = 61 + 1 + 1, & N_{67} = 63 = 67 + 1 - 5. \end{array}$$

Therefore, we can assume that N_p is given by the formula

$$N_p = p + 1 - a, \quad \text{where } a \equiv 2 \mod 3.$$

Moreover, we have that for some integer b, a satisfies the equation

$$p = \frac{1}{4}a^2 + \frac{27}{4}b^2. \tag{4}$$

Finally, we want to find a formula of N_p that works for every prime p. Thus, we rewrite (4) as follows

$$p = \frac{a + i\sqrt{27}b}{2} \cdot \frac{a - i\sqrt{27}b}{2}.$$

Then, we set $\alpha := \dfrac{a + i\sqrt{27}b}{2}$ and remark that $p = \alpha \cdot \overline{\alpha}$. This decomposition gives us a formula that works for all prime numbers p and is given by

$$N_p = p + 1 - \alpha - \overline{\alpha}.$$

Example 2.3. Consider the equation $x^3y + y^3z + z^3x = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_2$ and let N_n denote again the number of solutions of this equation over $\mathbb{F}_{2^n}$, which is given by

$$N_n = \#\left\{(0,0,0) \neq (x,y,z) : x,y,z \in \mathbb{F}_{2^n},\ x^3y + y^3z + z^3x = 0\right\}.$$

In order to find a general formula of N_n, we calculate the values of N_n and try to find a pattern. Below follows a table, where we assemble the first eight values of N_n.

n	1	2	3	4	5	6	7	8
N_n	3	5	24	17	33	38	129	257

Table 4: The first 8 values of N_n computed with Algorithm 3.

We notice immediately that we have to consider the following two cases.

If $\boldsymbol{n \not\equiv 0 \mod 3}$, then

$$N_1 = 3 = 2^1 + 1 \qquad N_4 = 17 = 2^4 + 1 \qquad N_7 = 129 = 2^7 + 1$$
$$N_2 = 5 = 2^2 + 1 \qquad N_5 = 33 = 2^5 + 1 \qquad N_8 = 257 = 2^8 + 1$$

From this, we can assume that a closed formula of N_n is given by

$$N_n = 2^n + 1.$$

If $\boldsymbol{n \equiv 0 \mod 3}$, then

$$N_3 = 24 = (2^3 + 1) - (\underbrace{-15}_{=a_1})$$
$$N_6 = 38 = (2^6 + 1) - (\underbrace{27}_{=a_2})$$
$$N_9 = 528 = (2^9 + 1) - (\underbrace{-15}_{=a_3})$$
$$N_{12} = 4238 = (2^{12} + 1) - (\underbrace{-141}_{=a_4})$$
$$N_{15} = 31944 = (2^{15} + 1) - (\underbrace{825}_{=a_5})$$

Let us try find a relation between a_{k+2}, a_{k+1} and a_k, by expressing a_{k+2} as a linear combination of a_{k+1} and a_k. Thus, let us consider the following system

$$\begin{cases} a_3 = x \cdot a_1 + y \cdot a_2 \\ a_4 = x \cdot a_2 + y \cdot a_3. \end{cases}$$

By solving the above system, we obtain $x = -8$ and $y = -5$. So, we suppose that

$$a_{k+2} = -8a_k - 5a_{k+1}, \quad \text{where } a_1 = -15 \text{ and } a_2 = 27.$$

Indeed, this recursion holds for a_5 and a_6. Hence, we can assume that, if $n \equiv 0 \mod 3$ and k is such that $n = 3k$, then

$$N_{3k} = 2^{3k} + 1 - a_k,$$

where a_k is defined recursively by $a_{k+2} = -8a_k - 5a_{k+1}$ with $a_1 = -15$ and $a_2 = 27$.

In the previous examples, we were able to find a formula for N_n that is of the form

$$N_n = 2^n + 1 - \alpha - \overline{\alpha}, \quad \text{where } \alpha\overline{\alpha} = 2.$$

So let us try to do the same in this example. After doing the calculations, we find that it is impossible to find one α that satisfies this relation. The same happens if we try to find α_1 and α_2 such that for $i \in \{1, 2\}$, $\alpha_i\overline{\alpha_i} = 2$ and

$$N_n = 2^n + 1 - \alpha_1 - \overline{\alpha_1} - \alpha_2 - \overline{\alpha_2}.$$

Hence, we need to find α_1, α_2 and α_3 such that for $i \in \{1, 2, 3\}$, $\alpha_i\overline{\alpha_i} = 2$ and

$$N_n = 2^n + 1 - \alpha_1 - \overline{\alpha_1} - \alpha_2 - \overline{\alpha_2} - \alpha_3 - \overline{\alpha_3}.$$

Thus, we set $a := \alpha_1 + \overline{\alpha_1}$, $b := \alpha_2 + \overline{\alpha_2}$ and $c := \alpha_3 + \overline{\alpha_3}$. From N_1, N_2 and N_3, we obtain the following system

$$\begin{cases} a + b + c = 0 \\ a^2 + b^2 + c^2 = 12 \\ a^3 + b^3 + c^3 = -15. \end{cases}$$

However, this system is difficult to solve, that is why we try to find α_1, α_2 and α_3 in an easier way. By definition of a, b and c, we have that α_1, α_2 and α_3 as well as their complements are respectively solutions of

$$x^2 - ax + 2 = 0, \quad x^2 - bx + 2 = 0, \quad x^2 - cx + 2 = 0.$$

Hence, they are all solutions of the equation

$$(x^2 - ax + 2)(x^2 - bx + 2)(x^2 - cx + 2) = 0,$$

which is equivalent to

$$x^6 - (a+b+c)x^5 + (ab+ac+bc+6)x^4 - (4(a+b+c)+abc)x^3 \\ + 2(ab+ac+bc+6)x^2 - 4(a+b+c)x + 8 = 0.$$

Thus, instead of solving the above system for a, b and c, we solve it for $a+b+c$, $ab+ac+bc$ and abc. After some easy calculations, we find

$$a+b+c=0, \quad ab+ac+bc=-6, \quad abc=-5.$$

Hence, we need to solve the equation

$$x^6+5x^3+8=0. \tag{5}$$

It is easy to check that the solutions of equation (5) are given by

$$x=\zeta^k\sqrt[3]{\frac{-5\pm i\sqrt{7}}{2}}, \qquad \text{where } \zeta=e^{\frac{2\pi i}{3}} \text{ and } k\in\{0,1,2\}.$$

In addition, for every $k\in\{0,1,2\}$,

$$\overline{\left(\zeta^k\sqrt[3]{\frac{-5+i\sqrt{7}}{2}}\right)}=\zeta^k\sqrt[3]{\frac{-5-i\sqrt{7}}{2}}.$$

Since α_1, α_2 and α_3 and their complements are solutions of (5), we can choose

$$\alpha_1:=\sqrt[3]{\frac{-5+i\sqrt{7}}{2}}, \quad \alpha_2:=\zeta\sqrt[3]{\frac{-5+i\sqrt{7}}{2}}, \quad \alpha_3:=\zeta^2\sqrt[3]{\frac{-5+i\sqrt{7}}{2}}.$$

We conclude that

$$N_n=2^n+1-\alpha_1-\overline{\alpha_1}-\alpha_2-\overline{\alpha_2}-\alpha_3-\overline{\alpha_3},$$

where α_1, α_2 and α_3 are given above and $\alpha_i\overline{\alpha_i}=2$ for $i\in\{1,2,3\}$.

Example 2.4. Consider the equation $y^2+y=x^5+1$ over $\mathbb{F}_2$ and the number of solutions of this equation over $\mathbb{F}_{2^n}$, which is given by

$$N_n=\#\left\{(x,y): x,y\in\mathbb{F}_{2^n},\ y^2+y=x^5+1\right\}+1.$$

We proceed as in the previous examples to calculate the values of N_n, which gives the following table.

n	1	2	3	4	5	6	7	8
N_n	3	5	9	33	33	65	129	193

Table 5: The first 8 values of N_n computed with Algorithm 4.

We see the following pattern:

$$\begin{array}{lll}
N_1=3=2^1+1, & N_6=65=2^6+1, & N_{11}=2049=2^{11}+1,\\
N_2=5=2^2+1, & N_7=129=2^7+1, & N_{12}=4353=2^{12}+1+256,\\
N_3=9=2^3+1, & N_8=193=2^8+1-64, & N_{13}=8193=2^{13}+1,\\
N_4=33=2^4+1+16, & N_9=513=2^9+1, & N_{14}=16385=2^{14}+1,\\
N_5=33=2^5+1, & N_{10}=1025=2^{10}+1, & N_{15}=32769=2^{15}+1.
\end{array}$$

It is clear that, if n is divisible by 4, then the formula we want to find is different than for every other n. That is why in a first step, we will consider the case, where ***n* is odd**, because then we can be sure that we have no multiples of 4. It is clear that in this case, we can assume that

$$N_n = 2^n + 1. \tag{6}$$

Let us now consider the case, where ***n* is even**. As observed before, in this case we have to distinguish between the following two cases.

- If $n \not\equiv 0 \mod 4$, then we can suppose that
$$N_n = 2^n + 1. \tag{7}$$
- If $n \equiv 0 \mod 4$, then we can assume that
$$N_n = 2^n + 1 + (-4)^{\frac{n}{4}+1} = 2^n + 1 - 2\left((-4)^{\frac{n}{4}} + (-4)^{\frac{n}{4}}\right). \tag{8}$$

We found formulas for the even multiples of 4 and the even numbers that are not multiples of 4, so let us now try to find a formula that works for all even numbers. From (7) and (8), we observe that we have to find x_n such that

$$N_n = 2^n + 1 - 2x_n\left((-4)^{\frac{n}{4}} + (-4)^{\frac{n}{4}}\right), \text{ where } x_n = \begin{cases} 0 & \text{if } n \not\equiv 0 \mod 4, \\ 1 & \text{if } n \equiv 0 \mod 4. \end{cases}$$

Notice that $i^n = 1$ if $n \equiv 0 \mod 4$ and that $i^n = -1$ if $n \equiv 2 \mod 4$ and n is even. Thus, we can write

$$N_n = 2^n + 1 - 2\left((-4)^{\frac{n}{4}} + i^n(-4)^{\frac{n}{4}}\right). \tag{9}$$

Finally, let us try to find a **general formula** that works for all n. If we compare (6) and (9), we observe that we must find x'_n such that

$$N_n = 2^n + 1 - 2x'_n\left(\sqrt{-4}^{\frac{n}{2}} + i^n\sqrt{-4}^{\frac{n}{2}}\right) \quad \text{where } x'_n = \begin{cases} 0 & \text{if } n \text{ is odd}, \\ 1 & \text{if } n \text{ is even}. \end{cases}$$

We can easily see that

$$\sqrt{-4}^{\frac{n}{2}} + i^n\sqrt{-4}^{\frac{n}{2}} + (-1)^n\left(\sqrt{-4}^{\frac{n}{2}} + i^n\sqrt{-4}^{\frac{n}{2}}\right) = \begin{cases} 0 & \text{if } n \text{ is odd}, \\ 2\left(\sqrt{-4}^{\frac{n}{2}} + i^n\sqrt{-4}^{\frac{n}{2}}\right) & \text{if } n \text{ is even}. \end{cases}$$

Thus, we obtain

$$\begin{aligned} N_n &= 2^n + 1 - \left(\sqrt{-4}^{\frac{n}{2}} + i^n\sqrt{-4}^{\frac{n}{2}} + (-1)^n\left(\sqrt{-4}^{\frac{n}{2}} + i^n\sqrt{-4}^{\frac{n}{2}}\right)\right) \\ &= 2^n + 1 - \left(\sqrt[4]{-4}\right)^n - \left(-\sqrt[4]{-4}\right)^n - \left(i\sqrt[4]{-4}\right)^n - \left(-i\sqrt[4]{-4}\right)^n. \end{aligned}$$

We can also rewrite N_n so that

$$N_n = 2^n + 1 - \alpha_1^n - \overline{\alpha_1}^n - \alpha_2^n - \overline{\alpha_2}^n,$$

where $\alpha_1 = \sqrt[4]{-4} = 1 + i$ and $\alpha_2 = i\sqrt[4]{-4} = -1 + i$.

Example 2.5. Consider the equation $y^2 + y = x^3 + x + 1$ over $\mathbb{F}_2$ and

$$N_n = \# \left\{(x, y) : x, y \in \mathbb{F}_{2^n},\ y^2 + y = x^3 + x + 1\right\} + 1.$$

With the same calculations as before, we find the first eight values of N_n, which are given in the table below.

n	1	2	3	4	5	6	7	8
N_n	1	5	13	25	41	65	113	225

Table 6: The first 8 values of N_n computed with Algorithm 5.

We make the following observations

$$\begin{array}{lll} N_1 = 1 = 2^1 + 1 - 2, & N_6 = 65 = 2^6 + 1 + 0, & N_{11} = 2113 = 2^{11} + 1 + 64, \\ N_2 = 5 = 2^2 + 1 + 0, & N_7 = 113 = 2^7 + 1 - 16, & N_{12} = 4225 = 2^{12} + 1 + 128, \\ N_3 = 13 = 2^3 + 1 + 4, & N_8 = 225 = 2^8 + 1 - 32, & N_{13} = 8321 = 2^{13} + 1 + 128, \\ N_4 = 25 = 2^4 + 1 + 8, & N_9 = 481 = 2^9 + 1 - 32, & N_{14} = 16385 = 2^{14} + 1 + 0, \\ N_5 = 41 = 2^5 + 1 + 8, & N_{10} = 1025 = 2^{10} + 1 + 0, & N_{15} = 32513 = 2^{15} + 1 - 256. \end{array}$$

This time, it is not that easy to find a relation between all the numbers, therefore we try another method to find a formula for N_n. In all the previous examples, N_n was always of the form $N_n = 2^n + 1 +$ "some α's". Let us now try to find a similar formula, by finding an algebraic number α such that

$$N_n = 2^n + 1 - \alpha^n - \overline{\alpha}^n.$$

From N_1 and N_2, we observe that $\alpha + \overline{\alpha} = 2$ and $\alpha^2 + \overline{\alpha}^2 = 0$. If we choose $x, y \in \mathbb{R}$ such that $\alpha = x + yi$, then we obtain the following system

$$\left\{ \begin{array}{l} x + yi + x - yi = 2 \\ x^2 + 2xyi - y^2 + x^2 - 2xyi - y^2 = 0 \end{array} \right. \iff \left\{ \begin{array}{l} x = 1 \\ x^2 - y^2 = 0 \end{array} \right.$$

Solving this system gives $\alpha = 1 + i$. Finally, we obtain

$$N_n = 2^n + 1 - \alpha^n - \overline{\alpha}^n,$$

where $\alpha = 1 + i$ with $|\alpha| = 2$. It is easy to check that this formula holds for all n.

Example 2.6. We now go back to Example 2.2 and this time, we consider the number of solutions of the equation over the field $\mathbb{F}_{p^n}$, which is given by

$$N_n = \# \left\{(0, 0, 0) \neq (x, y, z) : x, y, z \in \mathbb{F}_{p^n},\ x^3 + y^3 + z^3 = 0\right\}.$$

In all the previous examples, we always found a formula for N_n that is of the form $N_n = p^n + 1 - \alpha^n - \overline{\alpha}^n$, with $\alpha\overline{\alpha} = p$, so let us try to do the same here. We start with the cases for $p = 7$ and $p = 13$.

Note that in Example 2.2, we have already done all the work for $n = 1$ and we found

$$N_1 = p + 1 - \alpha - \overline{\alpha}, \qquad \text{where } \alpha = \frac{a + i\sqrt{27}b}{2},$$

with $\alpha\overline{\alpha} = p$.

Let us take a look if $\alpha = \frac{a + i\sqrt{27}b}{2}$ with the condition $\alpha\overline{\alpha} = p$ satisfies

$$N_n = p^n + 1 - \alpha^n - \overline{\alpha}^n$$

for $p = 7$ and $p = 13$. We first begin with $p = 7$. Below follows a table, where we assemble the first six values of N_n.

n	1	2	3	4	5	6
N_n	9	63	324	2331	17019	117936

Table 7: The first 6 values of N_n computed with Algorithm 6.

In order to check that α satisfies $N_n = 7^n + 1 - \alpha^n - \overline{\alpha}^n$, let us first find a and b. Since $\alpha\overline{\alpha} = 7$ and $N_1 = 9$, we obtain after some computations

$$\alpha = \frac{-1 + i\sqrt{27}}{2}.$$

After some calculations, we notice that the formula

$$N_n = 7^n + 1 - \alpha^n - \overline{\alpha}^n, \qquad \text{where } \alpha = \frac{-1 + i\sqrt{27}}{2},$$

holds for every $n \in \{0, \dots, 6\}$. Therefore, it seems reasonable that it holds for all n.

Let us now look at the case, where $p = 13$. First, we give a table of the first six values of N_n with the help of SAGE.

n	1	2	3	4	5	6
N_n	9	171	2268	28899	372069	4826304

Table 8: The first 6 values of N_n computed with Algorithm 6.

If we proceed with the same calculations as for $p = 7$, we find that α satisfies $N_n = 13^n + 1 - \alpha^n - \overline{\alpha}^n$ with $\alpha\overline{\alpha} = 13$ if $a = 5$ and $b = 1$.

After computations for $n \in \{0, \dots, 6\}$ of

$$N_n = 13^n + 1 - \alpha^n - \overline{\alpha}^n, \qquad \text{where } \alpha = \frac{5 + i\sqrt{27}}{2},$$

we can see that it holds, so we can suppose that the formula holds for every n.

Let us now examine the case, where $p = 2$ and $p = 5$. We begin with the case $p = 2$. In the above table, the first six values of N_n are represented.

n	1	2	3	4	5	6
N_n	3	9	9	9	33	81

Table 9: The first 6 values of N_n computed with Algorithm 6.

Then, α satisfies $N_n = 2^n + 1 - \alpha^n - \overline{\alpha}^n$ with $\alpha\overline{\alpha} = 2$ if $a = 0$ and $b = \dfrac{2\sqrt{6}}{9}$. Therefore, we get $\alpha = \sqrt{2}i$ and we easily check that the formula

$$N_n = 2^n + 1 - \alpha^n - \overline{\alpha}^n, \qquad \text{where } \alpha = \sqrt{2}i,$$

holds for every $n \in \{0, \dots, 6\}$. Thus, we can assume that it holds for every n.

Let us now look at the case, where $p = 5$. As for the previous cases, we first give a table of the first six values of N_n.

n	1	2	3	4	5	6
N_n	6	36	126	576	3126	15876

Table 10: The first 6 values of N_n computed with Algorithm 6.

Again, α satisfies $N_n = 5^n + 1 - \alpha^n - \overline{\alpha}^n$ with $\alpha\overline{\alpha} = 5$ if $a = 0$ and $b = \dfrac{2\sqrt{15}}{9}$. Therefore, we obtain $\alpha = \sqrt{5}i$ and with some computations, we see that the formula

$$N_n = 5^n + 1 - \alpha^n - \overline{\alpha}^n, \qquad \text{where } \alpha = \sqrt{5}i,$$

holds for every $n \in \{0, \dots, 6\}$. Hence, we can assume that it holds for all n.

In general, we can assume that for $p \equiv 2 \mod 3$, a closed formula for N_n is

$$N_n = p^n + 1 - \alpha^n - \overline{\alpha}^n, \qquad \text{where } \alpha = \sqrt{p}i,$$

with $\alpha\overline{\alpha} = p$.

For the case, where $p \equiv 1 \mod 3$, we can assume that a closed formula for N_n is

$$N_n = p^n + 1 - \alpha^n - \overline{\alpha}^n, \qquad \text{where } \alpha = \frac{a + i\sqrt{27}b}{2},$$

with $\alpha\overline{\alpha} = p$ and $a \equiv 2 \mod 3$.

Example 2.7. Consider the equation $y^2 + y = x^7$ over $\mathbb{F}_2$ and the number of solutions of this equation over $\mathbb{F}_{2^n}$ is given by

$$N_n = \#\left\{(x, y) : x, y \in \mathbb{F}_{2^n},\ y^2 + y = x^7\right\} + 1.$$

In order to find a formula for N_n, let us first compute N_1 and N_2.

- We have $N_1 = \#\left\{(x,y) : x, y \in \mathbb{F}_2,\ y^2 + y = x^7\right\} + 1$. The solutions of the equation $y^2 + y = x^7$ over $\mathbb{F}_2$ are given by

$$\mathcal{S} = \{(0,0), (0,1)\}.$$

Therefore, $N_1 = 2 + 1 = 3$.

- We have $N_2 = \#\left\{(x,y) : x, y \in \mathbb{F}_4,\ y^2 + y = x^7\right\} + 1$. We proceed as for N_1 and solve the equation $y^2 + y = x^7$ over $\mathbb{F}_4$ and we obtain $N_2 = 5$.

However, two values are not enough to make an experimental conclusion, that is why we calculate the first eight values of N_n and assemble them in the table below.

n	1	2	3	4	5	6	7	8
N_n	3	5	3	17	33	101	129	257

Table 11: The first 8 values of N_n computed with Algorithm 7.

We observe the following pattern

$$\begin{array}{ll} N_1 = 3 = 2^1 + 1, & N_6 = 101 = 2^6 + 1 + 36, \\ N_2 = 5 = 2^2 + 1, & N_7 = 129 = 2^7 + 1, \\ N_3 = 3 = 2^3 + 1 - 6, & N_8 = 257 = 2^8 + 1, \\ N_4 = 17 = 2^4 + 1, & N_9 = 633 = 2^9 + 1 + 120, \\ N_5 = 33 = 2^5 + 1, & N_{10} = 1025 = 2^{10} + 1. \end{array}$$

From similar calculations as in Example 2.3 we get that

$$N_n = 2^n + 1 - \alpha_1^n - \overline{\alpha_1}^n - \alpha_2^n - \overline{\alpha_2}^n - \alpha_3^n - \overline{\alpha_3}^n,$$

where α_1, α_2 and α_3 are given by

$$\alpha_1 = \sqrt[3]{1 + i\sqrt{7}}, \quad \alpha_2 = \zeta\sqrt[3]{1 + i\sqrt{7}}, \quad \alpha_3 = \zeta^2\sqrt[3]{1 + i\sqrt{7}}.$$

2.2 Generalisations

In the previous Subsection 2.1, we looked at some examples of equations over finite fields and tried to find a general formula for the number of solutions. Since the formulas were all of the same type, it seems reasonable to assume that the number of solutions of an equation over a finite field $\mathbb{F}_{p^n}$ is of the form

$$N_n = p^n + 1 - \sum_{k=1}^{g} \alpha_k^n + \overline{\alpha}_k^n,$$

where $\alpha_k \overline{\alpha}_k = p$ and g is a measure for the complexity of the equation, called the genus. In fact, this formula only holds for complete or projective curves that are smooth, that is without singular or multiple points.

Having found the general formula above, means that, if we are given a complete, smooth curve over some finite field, then we only need g and the α_k's to find the number of solutions of this equation over a finite field $\mathbb{F}_{p^n}$.

Now, we consider the polynomial P of the form

$$P(t) = \prod_{k=1}^{g} (1 - \alpha_k t)\,(1 - \overline{\alpha}_k t)\,.$$

Let us calculate P for the following equations.

a) Consider the equation $y^2+y = x^3$ over $\mathbb{F}_2$. Note that the number of solutions of this equation over $\mathbb{F}_{2^n}$ is the same as the number of solutions of $y^2+y = x^3+1$ over $\mathbb{F}_{2^n}$. So from Example 2.1, we have that $g = 1$ and $\alpha = i\sqrt{2}$. Hence,

$$P(t) = (1 - i\sqrt{2}t)(1 + i\sqrt{2}t) = 2t^2 + 1.$$

b) Consider the equation $y^2+y = x^5$ over $\mathbb{F}_2$. As in the previous case, the number of solutions of this equation over $\mathbb{F}_{2^n}$ is the same as the number of solutions of $y^2 + y = x^5 + 1$ over $\mathbb{F}_{2^n}$. Therefore, Example 2.4 gives us $g = 2$, $\alpha_1 = 1 + i$ and $\alpha_2 = -1 + i$. Thus, we obtain

$$P(t) = (1 - (1 + i)t)(1 - (1 - i)t)(1 - (-1 + i)t)(1 - (-1 - i)t) = 4t^4 + 1.$$

c) Consider the equation $x^3y + y^3z + z^3x = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_2$. Going back to Example 2.3, we get $g = 3$ and

$$\alpha_1 = \sqrt[3]{\frac{-5 + i\sqrt{7}}{2}}, \quad \alpha_2 = \zeta\sqrt[3]{\frac{-5 + i\sqrt{7}}{2}}, \quad \alpha_3 = \zeta^2\sqrt[3]{\frac{-5 + i\sqrt{7}}{2}}.$$

Thus, we obtain

$$P(t) = 8t^6 + 5t^3 + 1.$$

d) Lastly, we consider the equation $y^3-y = x^4$ over $\mathbb{F}_3$. After some computations, we find $\alpha_1 = \sqrt{3}$, $\alpha_2 = -\sqrt{3}$ and $\alpha_3 = i\sqrt{3}$, so that $g = 3$. This implies that

$$P(t) = (1-\sqrt{3})(1-\sqrt{3})(1+\sqrt{3})(1+\sqrt{3})(1-i\sqrt{3})(1+i\sqrt{3}) = 27t^6-9t^4-3t^2+1.$$

From the polynomial P, we obtain the so called Zeta function of the curve, which is given by

$$Z(t) = \frac{P(t)}{(1-t)(1-pt)}.$$

Let us show that the Zeta function satisfies

$$Z\left(\frac{1}{pt}\right) = p^{1-g}t^{2-2g}Z(t).$$

This follows by simply using the definition of P and from the following computation. Thus,

$$\begin{aligned}
Z\left(\frac{1}{pt}\right) = \frac{P(\frac{1}{pt})}{(1-\frac{1}{pt})(1-\frac{1}{t})} &= \frac{\prod_{k=1}^{g}(1-\alpha_k\frac{1}{pt})(1-\overline{\alpha}_k\frac{1}{pt})}{(1-\frac{1}{pt})(1-\frac{1}{t})} \\
&= \frac{\prod_{k=1}^{g}\frac{1}{pt^2}-\alpha_k\frac{1}{pt}-\overline{\alpha}_k\frac{1}{pt}+1}{(1-\frac{1}{pt})(1-\frac{1}{t})} \\
&= \frac{\prod_{k=1}^{g}\frac{1}{pt^2}\left(1-\alpha_k t-\overline{\alpha}_k t+pt^2\right)}{\frac{1}{pt}(1-pt)\frac{1}{t}(1-t)} \\
&= \frac{(pt^2)^{-g}\prod_{k=1}^{g}(1-\alpha_k t)(1-\overline{\alpha}_k t)}{(pt^2)^{-1}(1-t)(1-pt)} \\
&= p^{1-g}t^{2-2g}Z(t).
\end{aligned}$$

In addition, we can also show that

$$\log(Z(t)) = \sum_{n=1}^{\infty} N_n \frac{t^n}{n}.$$

We prove it by simply doing some calculations and using the Taylor series expansion. Hence,

$$\begin{aligned}
\log(Z(t)) &= \log\left(\frac{P(t)}{(1-t)(1-pt)}\right) \\
&= \log(P(t)) - \log(1-t) - \log(1-pt) \\
&= \sum_{k=1}^{g}\left(\log(1-\alpha_k t)+\log(1-\overline{\alpha}_k t)\right) - \log(1-t) - \log(1-pt) \\
&= \sum_{k=1}^{g}\left(-\sum_{n=1}^{\infty}\frac{\alpha_k^n t^n}{n} - \sum_{n=1}^{\infty}\frac{\overline{\alpha}_k^n t^n}{n}\right) + \sum_{n=1}^{\infty}\frac{t^n}{n} + \sum_{n=1}^{\infty}\frac{p^n t^n}{n} \\
&= \sum_{n=1}^{\infty}\left(p^n + 1 - \sum_{k=1}^{g}\alpha_k^n + \overline{\alpha}_k^n\right)\frac{t^n}{n} \\
&= \sum_{n=1}^{\infty} N_n \frac{t^n}{n}.
\end{aligned}$$

Let us now look at some examples, where we calculate g and Z.

Example 2.8.

a) Let us consider the equation $y^2 = x^7 + 1$ over $\mathbb{F}_3$ and let

$$N_n = \#\left\{(x,y) : x, y \in \mathbb{F}_{3^n},\ y^2 = x^7 + 1\right\} + 1.$$

In order to find the genus g, we calculate the first few values of N_n with Sage.

n	1	2	3	4	5	6
N_n	4	10	28	82	244	892

Table 12: The first 6 values of N_n computed with Sage.

After trying to find α such that $N_n = 3^n + 1 + \alpha^n + \overline{\alpha}^n$ and α_1, α_2 such that $N_n = 3^n + 1 + \alpha_1^n + \overline{\alpha}_1^n + \alpha_2^n + \overline{\alpha}_2^n$, we always get that the formula fails for a certain n. However, we are lucky to find α_1, α_2 and α_3 such that $N_n = 3^n + 1 + \alpha_1^n + \overline{\alpha}_1^n + \alpha_2^n + \overline{\alpha}_2^n + \alpha_3^n + \overline{\alpha}_3^n$ and they are given by

$$\alpha_1 = i\sqrt{3}, \quad \alpha_2 = \frac{3 + i\sqrt{3}}{2}, \quad \alpha_3 = \frac{-3 + i\sqrt{3}}{2}.$$

Hence, $g = 3$ and the polynomial P is equal to $P(t) = 27t^6 + 1$ after some calculations. Finally, the Zeta function Z of the curve is given by

$$Z(t) = \frac{27t^6 + 1}{(1-t)(1-3t)}.$$

b) Consider now the same equation $y^2 = x^7 + 1$, but this time over $\mathbb{F}_5$ and let

$$N_n = \#\left\{(x,y) : x, y \in \mathbb{F}_{5^n},\ y^2 = x^7 + 1\right\} + 1.$$

As before, we need to calculate the first few values of N_n in order to find the genus g of the curve. Hence, we obtain the following table.

n	1	2	3	4	5
N_n	4	26	126	626	3126

Table 13: The first 5 values of N_n computed with Sage.

First, we try to find α such that $N_n = 5^n + 1 + \alpha^n + \overline{\alpha}^n$, but the formula does not hold for the first values of n. The same happens if we try to find α_1 and α_2 such that $N_n = 5^n + 1 + \alpha_1^n + \overline{\alpha}_1^n + \alpha_2^n + \overline{\alpha}_2^n$. Nevertheless, for

$$\alpha_1 = i\sqrt{5}, \quad \alpha_2 = \frac{\sqrt{15} + i\sqrt{15}}{2}, \quad \alpha_3 = \frac{-\sqrt{15} + i\sqrt{15}}{2},$$

the formula $N_n = 5^n + 1 + \alpha_1^n + \overline{\alpha}_1^n + \alpha_2^n + \overline{\alpha}_2^n + \alpha_3^n + \overline{\alpha}_3^n$ holds for the first values of n. Therefore, we conclude that $g = 3$ and using α_1, α_2 and α_3 from above, we obtain $P(t) = 125t^6 + 1$, so that the Zeta function is equal to

$$Z(t) = \frac{125t^6 + 1}{(1-t)(1-5t)}.$$

3 Implementations

In this section, we will explain the algorithms we implemented on Sage and used for the calculations of the number of solutions in the examples of Section 2.

3.1 Algorithm for Example 2.1

```
1  def N(n):
2      F = GF(2**n)
3  
4      E = EllipticCurve(F, [0,0,1,0,1])
5  
6      return E.cardinality()
```

Algorithm 1: Sage code used for Table 1.

Below follows a short description of every line in Algorithm 1.

- **Lines 2 - 4:** We first define F as the finite field of size 2^n using the predefined command *GF*, which takes the prime power 2^n as a parameter and generates the finite field of size 2^n.

  Then, we define E to be the curve of equation $y^2+y=x^3+1$ over F using the predefined command *EllipticCurve*. In Sage, *EllipticCurve*$\big([a_1,a_2,a_3,a_4,a_6]\big)$ returns the elliptic curve of equation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$. That is why we use the function *EllipticCurve*, which takes F and $[0,0,1,0,1]$ as parameters to generate the curve of equation $y^2+y=x^3+1$ over F.

- **Line 6:** We finally return the number of solutions of the equation over F using the predefined command *cardinality*. Note that since the point at infinity is taken into considerations in this command, we do not add one at the end.

3.2 Algorithm for Example 2.2

```
1  def N(p):
2      F = GF(p)
3  
4      P.<x,y,z> = ProjectiveSpace(2, F)
5  
6      C = Curve(x**3 + y**3 + z**3)
7  
8      S = C.rational_points()
9  
10     return len(S)
```

Algorithm 2: Sage code used for Table 2 and Table 3.

Next follows a short description of every line in Algorithm 2.

- **Lines 2 - 8:** As before, we start by defining F as the finite field of size p and P the projective space of dimension 2 over F using the command *ProjectiveSpace*.

Moreover, we let C be the curve of equation $x^3 + y^3 + z^3 = 0$ in P over F using the predefined command *Curve*. Additionally, we define S to be a list containing the solutions of C using the predefined command *rational_points*.

- **Line 10:** Finally, in order the obtain the number of solutions, we return the length of S using the predefined command *len*.

3.3 Algorithm for Example 2.3

```
1  def N(n):
2      F = GF(2**n)
3
4      P.<x,y,z> = ProjectiveSpace(2, F)
5
6      C = Curve(y*x**3 + z*y**3 + x*z**3)
7
8      S = C.rational_points()
9
10     return len(S)
```

Algorithm 3: SAGE code used for Table 4.

It is easy to see that this algorithm is the same as Algorithm 2, except that we replace the fuction that describes the curve.

3.4 Algorithm for Example 2.4

```
1  def N(n):
2      F = GF(2**n)
3
4      A.<x,y> = AffineSpace(2, F)
5
6      C = Curve(y^2 + y + x^5 + 1)
7
8      S = C.rational_points()
9
10     return len(S) + 1
```

Algorithm 4: SAGE code used for Table 5.

Below follows a short description of every line in Algorithm 4.

- **Lines 2 - 8:** We start by defining F as the finite field of size 2^n and let A be the affine space of dimension 2 over F using the predefined command *AffineSpace*.

  As in the previous last two algorithms, we let C be the curve of equation $y^2 + y = x^5 + 1$ over F and S be defined as the set of solutions of C over F.

- **Line 10:** We finally return the length of S in order to obtain the number of solutions of C over F and this time, we have to add one since the command *rational_points* does not include the point at infinity.

3.5 Algorithm for Example 2.5

```
def N(n):
    F = GF(2**n)

    E = EllipticCurve(F, [0,0,1,1,1])

    return E.cardinality()
```

Algorithm 5: Sage code used for Table 6.

This is the same as Algorithm 1, we simply replace the variables of the curve.

3.6 Algorithm for Example 2.6

```
def N(n, p):
    F = GF(p**n)

    P.<x,y,z> = ProjectiveSpace(2, F)

    C = Curve(x**3 + y**3 + z**3)

    S = C.rational_points()

    return len(S)
```

Algorithm 6: SAGE code used for Table 7 and Table 8.

This is again the same algorithm as Algorithm 2 and 3, with the simple change that we use a different function.

3.7 Algorithm for Example 2.7

```
def N(n):
    F = GF(2**n)

    A.<x,y> = AffineSpace(2, F)

    C = Curve(y**2 + y + x**7)

    S = C.rational_points()

    return len(S) + 1
```

Algorithm 7: SAGE code used for Table 9.

See Algorithm 4 for explanations, it is the same, except that we replace the curve.

4 Conclusion

In conclusion, we found experimentally a measure for the complexity of an equation in two variables and it is reasonable to assume that for any complete or projective, smooth curve, the number of zeroes over a finite field $\mathbb{F}_{p^n}$ is of the form

$$N_n = p^n + 1 - \sum_{k=1}^{g} \alpha_k^n + \overline{\alpha}_k^n,$$

where $\alpha_k \overline{\alpha}_k = p$ and g is a measure of the complexity of the curve, called the genus of the curve, which is an integer. In addition, the Zeta function of the curve is given by

$$Z(t) = \frac{P(t)}{(1-t)(1-pt)},$$

where P is defined by

$$P(t) = \prod_{k=1}^{g} (1 - \alpha_k t)(1 - \overline{\alpha}_k t).$$

Moreover, the Zeta function Z satisfies

$$Z\left(\frac{1}{pt}\right) = p^{1-g} t^{2-2g} Z(t) \quad \text{and} \quad \log(Z(t)) = \sum_{n=1}^{\infty} N_n \frac{t^n}{n}.$$

We can also see that in order to determine Z, we need at least g N_n's. This is because we need to know all the g α_k's. To find them, we need to solve a system, where the N_n's are the equations, given by $N_n = p^n + 1 -$"Newton power sum in $\alpha_1, \overline{\alpha_1}, \alpha_2, \overline{\alpha}_2, ..., \alpha_g, \overline{\alpha}_g$" and the α_k's are the variables. We also know that in order to solve such a system, we need as many equations as variables, hence we require g N_n's.

Acknowledgement

The three authors would like to thank Prof. Dr. Gerard Van Der Geer and Bryan Advocaat for having supervised this project in the Experimental Mathematics Lab of University of Luxembourg.

References

[1] Lassina Dembele, Lecture notes "Théorie des nombres et applications à la cryptographie", May 2021.

[2] Karuk Andriana, "Elliptic Curves and a Theorem of Gauss", University of Barcelona, January 2019.

[3] The Sage Development Team, Sage Tutorial Release 9.2, October 2020.