UNIVERSITY OF LUXEMBOURG
Department of Mathematics

Experimental Mathematics

COUNTING POINTS ON CURVES OVER FINITE FIELDS $\mathbb{F}_q$

Selma Jusufovic and Irma Skrijelj

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

Winter semester 2020 – 2021

Abstract

The purpose of this paper is to find out the number of solutions of polynomial equations in two variables over a finite field, by doing experimentations. We used the properties of finite fields to find the solutions. Moreover we tried to find algebraic numbers in $\mathbb{C}$, which we used for the formulas of the number of solutions.

We are grateful to dear Prof. Dr. Gerard van der Geer and dear Bryan Advocaat for all their support and help through this mathematical experimental project.

Contents

1 Introduction

Finite Fields were first introduced by Evariste Galois in his paper "sur la théorie des nombres" in 1830. This paper is considered to be the founding article of the general theory of finite fields. In honor of Evariste Galois, finite fields are also named Galois fields.
Moreover, finite fields are fundamental in many areas of mathematics including number theory, Galois theory, cryptography and many more.

Our main goal is to examine the solutions of the polynomial equations
$f(x, y) = 0$ over finite fields. The number of solutions of these equations is finite. That makes it possible to count them, in contrast to the solutions of polynomial equations over the real numbers.
An equation $f(x, y) = 0$ over the real numbers usually defines a curve. So the solutions of polynomial equations $f(x, y) = 0$ over finite fields are analogous to those of the real numbers.

2 Finite fields

In this chapter we will only discuss finite fields. First we will see what finite fields are by giving a definition, showing some properties and examples. After that we will show some multiplication and addition tables with the elements of a finite field.

2.1 Definition and properties

Definition 2.1. A field is a set F with two binary operations $+$ and $\times$ such that:

- $(F, +)$ is a commutative group with identity element 0
- $(F \setminus \{0\}, \times)$ is a commutative group with identity element 1.
- $\forall a, b, c \in F$: $a(b + c) = ab + ac$.

A field is called finite when its number of elements is finite.

More precisely, for each field F there is always a homomorphism $\mathbb{Z} \longrightarrow F$ sending $1 \in \mathbb{Z}$ to $1 \in F$. This means that the homomorphism is either injective or the kernel is a prime ideal $\neq (0)$ in $\mathbb{Z}$, hence of the form (p) for a prime p. In that case F contains $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.
If F is a finite field it cannot contain $\mathbb{Z}$, hence it contains a finite field $\mathbb{F}_p$.

Definition 2.2. By definition, the prime field of a field F is the smallest subfield of F, the intersection of all subfields of F. For a finite field F the prime field is a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for a prime p.

Properties. Any two finite fields with the same number of elements are isomorphic and they can't have two different subfields with the same number of elements. So, every finite field contains a unique prime field $\mathbb{F}_p$ with characteristic p.

The order of a finite field is always a power of a prime number.

Proof. Let $\mathbb{F}_q$ be a finite field of cardinality q. Then it contains a unique prime field $\mathbb{F}_p$ with characteristic p. Thus $\mathbb{F}_q$ is an extension of $\mathbb{F}_p$ and $\mathbb{F}_q$ is a $\mathbb{F}_p-$ vector space. The dimension of the vector space is the degree of the extension ($[\mathbb{F}_q\colon \mathbb{F}_p]$).
Let $[\mathbb{F}_q\colon \mathbb{F}_p] = n$.
$\Rightarrow$ the dimension of the vector space is n.
Hence $|\mathbb{F}_q| = p^n$.

■

Another useful fact is that any finite subgroup of the multiplicative group of a field is cyclic. In particular, for a finite field $\mathbb{F}_q$ the group $\mathbb{F}_q^*$ is cyclic.

Examples

a) $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ and $\alpha^3 = 1$ so $\mathbb{F}_4 = \{\ 0, \alpha^0, \alpha^1, \alpha^2\}$

b) $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ with $\alpha^{15} = 1$ so $\mathbb{F}_{16} = \{\ 0,\ \alpha^i \quad i = 0, \cdots, 14\}$.

Moreover, the finite field $\mathbb{F}_{p^n}$ is a subfield of $\mathbb{F}_{p^m} \Leftrightarrow n$ divides m.
Now, let us move on to the description of $\mathbb{F}_q = \mathbb{F}_{p^n}$.
$\mathbb{F}_{p^n}$ can be constructed in the following way. One can choose an irreducible polynomial f in $\mathbb{F}_p[x]$ of degree n, then $(\mathbb{F}_q =)\ \mathbb{F}_{p^n} \ \cong\ \mathbb{F}_p[x]/(f)$.
$\mathbb{F}_p[x]/(f)$ is an extension field of $\mathbb{F}_p$ and the irreducible polynomial f is not always unique.
So in other words, $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ with $f(\alpha) = 0$.

Examples

a) For $\mathbb{F}_4$ we have that $\alpha^3 = 1$ (because $\mathbb{F}_4^*$ is cyclic), but then $\alpha \neq 1$ satisfies $\alpha^2 + \alpha + 1 = 0$, since $X^3 - 1 = (X^2 + X + 1)(X - 1)$ and $\alpha \neq 1$.

b) For $\mathbb{F}_8$ we have that $\beta^7 = 1$ ($\mathbb{F}_8^*$ is cyclic), hence $\beta \neq 1$ satisfies $\beta^3 + \beta + 1 = 0$ or $\beta^3 + \beta^2 + 1 = 0$ since $X^7 - 1 = (X - 1)(X^3 + X^2 + 1)(X^3 + X + 1)$ in $\mathbb{F}_2[x]$.

c) $\mathbb{F}_9 \ \cong\ \mathbb{F}_3[x]/(x^2 + 1)$ or $\mathbb{F}_9 \ \cong\ \mathbb{F}_3[x]/(x^2 + x + 2)$.

Furthermore, by FERMAT'S little theorem, if p is a prime number and $x \in \mathbb{F}_p$, then $x^p = x$.

$$\Rightarrow x^p - x = \prod_{a \in \mathbb{F}_p} (x - a)$$

More generally every element of $\mathbb{F}_{p^n}$ satisfies the polynomial equation $x^{p^n} - x = 0$.

2.2 Addition and multiplication table

◇ addition and multiplication table on $\mathbb{F}_4$:

$\mathbb{F}_4$=$\{0, 1, \alpha, \alpha+1\}$ and $\mathbb{F}_4 \cong \mathbb{F}_2[\mathrm{x}]\backslash(x^2+x+1)$, $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$. So we have that $\alpha^2 = \alpha + 1$ and $\alpha^3 = \alpha \cdot \alpha^2 = \alpha(\alpha+1) = \alpha^2 + 1 = 1$.

We get the following multiplication and addition table.

$+$	0	1	α	α+1
0	0	1	α	α+1
1	1	0	α+1	α
α	α	α+1	0	1
α+1	α+1	α	1	0

$\cdot$	0	1	α	α+1
0	0	0	0	0
1	0	1	α	α+1
α	0	α	α+1	1
α+1	0	α+1	1	α

◇ addition and multiplication table on $\mathbb{F}_8$:

$\mathbb{F}_8$=$\{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$ and $\mathbb{F}_8 \cong \mathbb{F}_2[\mathrm{x}]\backslash(x^3+x+1)$, so $\alpha^3 = \alpha+1$, $\alpha^4 = \alpha^2+\alpha$, $\alpha^5 = \alpha^2+\alpha+1$, $\alpha^6 = \alpha^2+1$, $\alpha^7 = 1$.

$+$	0	1	α	α^2	α+1	α^2+α	α^2+α+1	α^2+1
0	0	1	α	α^2	α+1	α^2+α	α^2+α+1	α^2+1
1	1	0	α+1	α^2+1	α	α^2+α+1	α^2+α	α^2
α	α	α+1	0	α^2+α	1	α^2	α^2+1	α^2+α+1
α^2	α^2	α^2+1	α^2+α	0	α^2+α+1	α	α+1	1
α+1	α+1	α	1	α^2+α+1	0	α^2+1	α^2	$\alpha^2+\alpha$
$\alpha^2+\alpha$	$\alpha^2+\alpha$	α^2+α+1	α^2	α	α^2+1	0	1	α+1
α^2+α+1	α^2+α+1	α^2+α	α^2+1	α+1	α^2	1	0	α
α^2+1	α^2+1	α^2	α^2+α+1	1	α^2+α	α+1	α	0

$\cdot$	0	1	α	α^2	α+1	α^2+α	α^2+α+1	α^2+1
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α+1	α^2+α	α^2+α+1	α^2+1
α	0	α	α^2	α+1	α^2+α	α^2+α+1	α^2+1	1
α^2	0	α^2	α+1	α^2+α	α^2+α+1	α^2+1	1	α
α+1	0	α+1	α^2+α	α^2+α+1	α^2+1	1	α	α^2
$\alpha^2+\alpha$	0	α^2+α	α^2+α+1	α^2+1	1	α	α^2	α+1
α^2+α+1	0	α^2+α+1	α^2+1	1	α	α^2	α+1	α^2+α
α^2+1	0	α^2+1	1	α	α^2	α+1	α^2+α	α^2+α+1

Now let us move on to the next chapter COUNTING POINTS ON CURVES OVER FINITE FIELDS.

3 Counting points on curves over finite fields

In this chapter we will look at the solutions of polynomial equations $f(x, y) = 0$ over finite fields. We will first show some examples and then after that, we will give a small summary on how in fact to predict easily the number of solutions of the type of equations $f(x, y) = 0$.
Let us first start with the equation $y^2 + y = x^3$ over $\mathbb{F}_{2^n}$.

3.1 Example 1

We consider the equation $y^2 + y = x^3$ over $\mathbb{F}_{2^n}$. Let $N_n = \#\{(x, y)\}: \ x, y \in \mathbb{F}_{2^n} : y^2 + y = x^3\} + 1$.
First we did some experimentations and we calculated by hand the solutions for N_1, N_2 and N_3.

For the equation over $\mathbb{F}_2$ $(n = 1)$, we get the following solution set;
$S_1 = \{(1, 0), (1, 1)\}$.
$\Rightarrow N_1 = 3$.

For $y^2 + y = x^3/\mathbb{F}_4$ $(n = 2)$ we get the solution set
$S_2 = \{(0, 0),\ (0, 1),\ (1, \alpha),\ (1, \alpha + 1),\ (\alpha, \alpha), (\alpha, \alpha + 1),\ (\alpha + 1, \alpha),\ (\alpha + 1, \alpha + 1)\}$.
$\Rightarrow N_2 = 9$.

For $y^2 + y = x^3/\mathbb{F}_8$ $(n = 3)$ the set of solutions is
$S_3 = \{(0, 0),\ (0, 1), (\alpha + 1, \alpha^2 + \alpha), (\alpha + 1, \alpha^2 + \alpha + 1), (\alpha^2 + 1, \alpha^2 + \alpha),$
$(\alpha^2 + 1, \alpha^2 + \alpha + 1), (\alpha^2 + \alpha + 1, \alpha^2), (\alpha^2 + \alpha + 1, \alpha^2 + 1)\}$.
$\Rightarrow N_3 = 9$.

$y^2 + y = x^3$ over $\mathbb{F}_{16}$ (n=4) has the following solution set,
$S_4 = \{(0,\ 0),\ (0,\ 1),\ (1,\ \alpha^2 + \alpha),\ (1,\ \alpha^2 + \alpha + 1),\ (\alpha^2 + \alpha,\ \alpha^2 + \alpha),$
$(\alpha^2 + \alpha,\ \alpha^2 + \alpha + 1),\ (\alpha^2 + \alpha + 1,\ \alpha^2 + \alpha),\ (\alpha^2 + \alpha + 1,\ \alpha^2 + \alpha + 1)\}$
$\Rightarrow N_4 = 9$.

Furthermore, $N_5 = 33$ and $N_6 = 81$.

Instead of calculating the solutions by hand, there is an easier method to find the number of solutions for n odd. It is the following.

The multiplicative group $\mathbb{F}_q^*$ is cyclic. For $q = 2^n$ we thus have a cyclic group of order $2^n - 1$. The map $f : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*,\ x \longmapsto x^3$ is a homomorphism of groups. The kernel of the map consists of solutions of $x^3 = 1$, that is, elements whose order divides 3.
Let $K := ker(f) = \{x \in \mathbb{F}_q^* : x^3 = 1\}$. Every image element of f is taken k times, with $k = \# K$.
$x^3 = 1 \Leftrightarrow ord(x)$ divides 3. Hence the kernel only consists of elements whose order divides 3, and 3 divides $2^n - 1$ if and only if n is even.

Let us now separate the case where n is even and the case where n is odd.

If n is odd then 3 does not divide $2^n - 1$. Hence there are no elements of order 3, hence $k = 1$. Hence the map is injective for n odd. Moreover $x = 0$ goes to 0 under $x \longrightarrow x^3$. So the map f is a bijection of $\mathbb{F}_{2^n}$ odd.
On the other hand, when n is even 3 divides $2^n - 1$. Hence there are elements of order 3 and $\#K > 1$.
In a cyclic group (multiplicatively written) of order n with $n \equiv 0 \ (mod\ 3)$, the kernel of $x \longrightarrow x^3$ had order 3. This implies that $\#K = 3$. Hence, every image element of f is taken 3 times if n is even.
Further, let us find the solutions of $y^2 + y = x^3/\mathbb{F}_{2^n}$ for n odd.

We see that if x runs through $\mathbb{F}_{2^n}$ we get all the elements of $\mathbb{F}_{2^n}$ as the right hand side. As for the left hand side, let us observe the map $\varphi\colon y \longrightarrow y^2 + y$. We notice that φ is a linear map.

Proof. Let $\varphi\colon \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n},\ y \longmapsto y^2 + y$ be a map. $\mathbb{F}_{2^n}$ is a vector space over the field $\mathbb{F}_2$.
Let us show that φ is a linear map:

$\diamond$ *i)* Let $a, b \in \mathbb{F}_{2^n}$

$$\begin{aligned} \varphi(a+b) &= (a+b)^2 + (a+b) \\ &= \varphi(a) + \varphi(b). \end{aligned}$$

$\diamond$ *ii)* Let $a \in \mathbb{F}_{2^n}$.

$$\varphi(0a) = 0 \quad and \quad \varphi(1a) = \varphi(a).$$

$\Rightarrow \varphi$ is a linear map.

■

$ker(\varphi) = \{0,\ 1\}$

$\Rightarrow \varphi$ is not injective, so $|im\varphi| \neq 2^n$.

$im(\varphi) = \frac{2^n}{2} = 2^{n-1}$.

Hence the image in $\mathbb{F}_{2^n}$ consists of 2^{n-1} elements. Call this image A. For x in A we can solve the equation $y^2 + y = x$ and we get that it has 2 solutions.
In total there are $2 \times 2^{n-1} = 2^n$ solutions. Hence $N_n = 2^n + 1$, for n odd.

This technique is only useful for n odd. As for n even it is impossible to find the number of solutions with this method. Therefore we need another approach where we can find all the numbers of solutions.

We tried to find, experimentally, an algebraic number $\alpha \in \mathbb{C}$ with $\alpha\bar{\alpha} = 2$ such that $N_n = 2^n + 1 - \alpha^n - \bar{\alpha}^n$, $\forall n \geq 1$. To find this algebraic number, we look at our solutions on page 6.

We have that $N_1 = 3$, so $3 = 2 + 1 - \alpha - \bar{\alpha}$.

Moreover $\bar{\alpha} = \frac{2}{\alpha}$, so $0 = \alpha + \frac{2}{\alpha}$.
This means that α is a solution of $(X-\alpha)(X-\bar{\alpha}) = X^2+2 = 0$ and hence $\alpha = \sqrt{-2}$ and $\bar{\alpha} = -\sqrt{-2}$.

We notice that the formula $N_n = 2^n + 1 - \sqrt{-2}^n - (-\sqrt{-2})^n$ holds for n odd, as well as for $n = 2$, $n = 4$ and $n = 6$ by inspection. The formula can be checked for many n. So probably it holds for all n.
Let us proceed to the next example.

3.2 Example 2

We consider the equations $y^2 + y = x^3 + 1$ and $y^2 + y = x^3 + x$ over $\mathbb{F}_{2^n}$ and let again $N_n = \#\{(x, y)\} : \ x, y \in \mathbb{F}_{2^n} : y^2 + y = x^3 + 1\} + 1$.

To find the number of solutions of these polynomial equations we will proceed as before in 3.1.
We try to find an $\alpha \in \mathbb{C}$ such that $N_n = 2^n + 1 - \alpha^n - \bar{\alpha}^n$, $\forall n \geq 1$.

By inspection, we notice that $y^2 + y = x^3 + 1/\mathbb{F}_{2^n}$ has the same number of solutions as $y^2 + y = x^3/\mathbb{F}_{2^n}$. Let us prove that this is indeed the case.

Proof. We consider $y^2 + y = x^3$ over $\mathbb{F}_{2^n}$. Moreover, we suppose that we replace x by $x + 1$. Then we have the following.
$x^3 = x^2 \cdot x \to (x^2 + 1)(x + 1) = x^3 + x^2 + x + 1$.
So the number of solutions of the polynomial equation $y^2 + y = x^3 + 1$ is the same as the same number of solutions as for $y^2 + y = x^3 + x^2 + x + 1$.
Further, we have that $x^3 + x^2 + x + 1 = x^3 + (x^2 + 1) + (1 + x) + 1$.
Now if we replace y by $y + x + 1$, we get $(y + x + 1)^2 + y + x + 1 = x^3 + 1$.

So via $(x, y) \to (x + 1, y + x + 1)$ we see that the equation $y^2 + y = x^3$ changes into $y^2 + y = x^3 + 1$ and thus has the same number of solutions over $\mathbb{F}_{2^n}$ for all n.
■

Hence α is the same as in Example 1, so the number of solutions for $y^2+y = x^3+1$ over $\mathbb{F}_{2^n}$ is $N_n = 2^n + 1 - \sqrt{-2}^n - (-\sqrt{-2})^n$, $\forall n \geq 1$.

For the equation $y^2 + y = x^3 + x$, we calculated $N_1 = 1,\ N_2 = 5,\ N_3 = 13,\ N_4 = 25$ and we observed that with $\alpha = 1 + i$ these numbers, $N_1,\ N_2,\ N_3$ and N_4, agree with $2^n + 1 - \alpha^n - \bar{\alpha}^n$ for $n = 1,\ 2,\ 3,\ 4$.
The formula can be checked for many n, so probably it holds for all n.

3.3 Example 3

Consider the polynomial equation $y^2 + y = x^5 + x^3$ over $\mathbb{F}_{2^n}$. Again define
$N_n = \#\{(x,y)\}\colon\ x, y \in \mathbb{F}_{2^n} : y^2 + y = x^5 + x^3\} + 1$.

Experimentally, we find that $N_1 = 5$ and $N_2 = 5$.
To find the numbers of solutions for this equation, one α does not suffice. But instead we have to find α and β such that $N_n = 2^n + 1 - \alpha^n - \bar{\alpha}^n - \beta^n - \bar{\beta}^n$, $\forall n \geq 1$.

Since $N_1 = 5$ and $N_2 = 5$, we have

$$\underline{for\ n = 1}, \quad 5 = 2 + 1 - \alpha - \bar{\alpha} - \beta - \bar{\beta}. \tag{1}$$

$$\underline{for\ n = 2}, \quad 5 = 2^2 + 1 - \alpha^2 - \bar{\alpha}^2 - \beta^2 - \bar{\beta}^2. \tag{2}$$

$\alpha\bar{\alpha} = 2$ and $\beta\bar{\beta} = 2$. Let $a = \alpha + \bar{\alpha}$ and $b = \beta + \bar{\beta}$.
Moreover, $a^2 = \alpha^2 + 2\alpha\bar{\alpha} + \bar{\alpha}^2 = \alpha^2 + \bar{\alpha}^2 + 4$ and $b^2 = \beta^2 + \bar{\beta}^2 + 4$.
From equations (1) and (2) we get

$$a + b = -2, \ \ a^2 + b^2 = 8.$$

THIS GIVES US THE SOLUTIONS FOR a AND b:

We have $\{a, b\} = \{-1 + \sqrt{3}, -1 - \sqrt{3}\}$.
So α is a solution of $X^2 - aX + 2$ and β of $X^2 - bX + 2$.
Experimentally we verified $N_n = 2^n + 1 - \sum \alpha_i^n + \bar{\alpha_i}^n$, $i = 1, 2$ for five n. The formula can be verified for many n, so probably it holds for all n.

3.4 Example 4

Consider the equation $y^3 - y = x^4$ / $\mathbb{F}_{3^n}$ and let

$$N_n = \#\{(x,y)\}\colon x, y \in \mathbb{F}_{3^n} : y^3 - y = x^4\} + 1.$$

For this equation we have

$$N_1 = 4, \qquad N_2 = 4, \qquad N_3 = 28, \qquad N_4 = 28.$$

We notice that for this equation one α does not suffice to find the number of solutions.
If we had one α, we would have that α (with $\alpha\bar{\alpha} = 3$) is a solution of $X^2 + 3 = 0$.
This would imply that $\alpha = \sqrt{-3}$ and $\bar{\alpha} = -\sqrt{-3}$.
Now, when we check in the formula we get $13 \neq N_2$. So one α is not enough.

WHEN WE TRY IT WITH α_1 AND α_2 WE SEE THAT IT WORKS:

We get that α_1, α_2 and their conjugates are the roots of the polynomial

$t^4 - 3t^2 + 9 \ = \ (t^2 + 3t + 3)(t^2 - 3t + 3)$.

Hence $N_n = 3^n + 1 - \alpha_1^n - \bar{\alpha_1}^n - \alpha_2^n - \bar{\alpha_2}^n$, $\forall n \geq 1$

with $\alpha_1,\ \alpha_2,\ \bar{\alpha}_1,\ \bar{\alpha}_2 \in \{\sqrt{\frac{3}{2} + \frac{3\sqrt{-3}}{2}},\ \sqrt{\frac{3}{2} - \frac{3\sqrt{-3}}{2}},\ -\sqrt{\frac{3}{2} + \frac{3\sqrt{-3}}{2}},\ -\sqrt{\frac{3}{2} - \frac{3\sqrt{-3}}{2}}\}$.
Experimentally we verified that $N_n = 3^n + 1 - \sum_{i=1}^{2} \alpha_i^n + \bar{\alpha}_i^n$ for four n and the formula can be verified for many n, so probably it holds for all n.

3.5 Example 5

Finally, we consider the equation $y^2 + y = x^7/\mathbb{F}_{2^n}$. Let again $N_n = \#\ \{(x,y)\}$: $x, y \in \mathbb{F}_{2^n} : y^2 + y = x^7\} + 1$.
By experimenting, we get that $N_1 = 3,\ N_2 = 5$ and $N_3 = 3$.

For this equation we find out, that we need in total $\alpha_1,\ \alpha_2$ and α_3 such that $N_n = 2^n + 1 - \alpha_1^n - \bar{\alpha_1}^n - \alpha_2^n - \bar{\alpha_2}^n - \alpha_3^n - \bar{\alpha_3}^n$, $\forall n \geq 1$.
More precisely we get that α_1, α_2, α_3 and their conjugates are solutions of the polynomial $t^6 - 2t^3 + 8$. Hence

$$\alpha_1,\ \alpha_2,\ \alpha_3,\ \bar{\alpha}_1,\ \bar{\alpha}_2,\ \bar{\alpha}_3 \in \{\sqrt[3]{1+\sqrt{-7}},\ \zeta_3\sqrt[3]{1+\sqrt{-7}},\ \zeta_3^2\sqrt[3]{1+\sqrt{-7}},\ \sqrt[3]{1-\sqrt{-7}},$$
$$\zeta_3\sqrt[3]{1-\sqrt{-7}},\ \zeta_3^2\sqrt[3]{1-\sqrt{-7}}\},\ \zeta_3 = e^{\frac{2\pi}{3}i}.$$

α_i is of the form $\sqrt[3]{1 \pm \sqrt{-7}}$.

The examples above help us to notice that if one considers certain equations $f(x,y) = 0$ defined over $\mathbb{F}_{p^n}$ then, as one finds by experimentation, one can predict the number N_n of solutions for all n if one knows N_n for $n = 1, 2, \ldots, g$ with some g.
How many N_n one needs, depends on the equation. For example for $y^2 + y = x^a$ over $\mathbb{F}_2$, we saw in example 1 that we only need N_1 if $a = 1$ and in example 5 we saw that we need $N_1,\ N_2,\ N_3$ for $a = 7$ to find the number of solutions for all n. Moreover, we also saw in example 3 that we only need N_1 and N_2 to find $N_n\ \forall n$.
So in general, the greater the exponent of x, the more N_n we need to find the number of solutions. But miraculously, once we know $N_1, \ldots, N_g$, one can predict in these cases N_n for all n.

4 Conclusion

In this project, we saw that once we found the number of solutions of $f(x, y) = 0$ for certain f over $\mathbb{F}_p$ for a few m ($m = 1, 2, \ldots, M$) we can predict the number of solutions of $f(x, y) = 0$ over $\mathbb{F}_p$ for all n. We noticed as well that, the more 'complicated' the equation was, the more α's with $\alpha\bar{\alpha} = p$ we needed.
The subject of curves over finite fields can be found in many other subjects in mathematics, like for example in coding theory, cryptography, exponential sums, etc. Curves over finite fields can even be used for a wide field of new researches that can help other areas of mathematics.