RATIONAL POINTS ON CUBIC, QUARTIC AND SEXTIC CURVES OVER FINITE FIELDS

JOSÉ ALVES OLIVEIRA

Abstract. Let \( \mathbb{F}_q \) denote the finite field with \( q \) elements. In this work, we use characters to give the number of rational points on suitable curves of low degree over \( \mathbb{F}_q \) in terms of the number of rational points on elliptic curves. In the case where \( q \) is a prime number, we give a way to calculate these numbers. As a consequence of these results, we characterize maximal and minimal curves given by equations of the forms \( ax^3 + by^3 + cz^3 = 0 \) and \( ax^4 + by^4 + cz^4 = 0 \).

1. Introduction

Let \( \mathbb{F}_q \) be a finite field with \( q = p^k \) elements. For a curve \( C \) over \( \mathbb{F}_q \), we denote by \( N_n(C) \) the number of rational points of \( C \) over \( \mathbb{F}_{q^n} \). For an irreducible non-singular curve \( C \) over \( \mathbb{F}_q \), the well-known Riemann Hypothesis [17, Theorem 3.3] states that the number of rational points on a curve \( C \) over \( \mathbb{F}_{q^n} \) satisfies

\[
N_n(C) = q^n + 1 - 2g \sum_{i=1}^{2g} \omega_i^n,
\]

where \( g \) denotes the genus of \( C \) and \( |\omega_i| = \sqrt{q} \) for all \( i \). Also by this result, we have the well-known Hasse-Weil bound for the number of rational points on an irreducible non-singular curve over \( \mathbb{F}_q \) of genus \( g \), given by

\[
|N_n(C) - q^n - 1| \leq 2g \sqrt{q^n}.
\]  

(1)

In general, calculating the exact value \( N_n(C) \) is a difficult task. Many authors have studied curves whose number of rational points attains the upper Hasse-Weil bound, called maximal curves. The number of points on some special curves was studied in [4, 6, 9, 10, 11, 13, 19]. From Riemann Hypothesis, it is possible to deduce another bounds for irreducible singular plane curves. In fact, Aubry and Perret [1] generalized this result to irreducible curves.

Date: January 31, 2020.

2010 Mathematics Subject Classification. 12E20 (primary) and 14H52 (secondary).

Key words and phrases. Algebraic curves, Hasse-Weil’s bound, Caracter sums, Ferrmat curves, Finite fields.
Theorem 1.1. [1, Corollary 2.4] The number of points on an irreducible curve \( C \) over \( \mathbb{F}_q \) is given by

\[
N_n(C) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n \sum_{i=1}^{g} \beta_i^n - \Delta_X \sum_{i=1}^{\Delta_X} \beta_i^n,
\]

where \( \Delta_X \) is a constant depending on \( C \) and \( \omega_i, \beta_i \) are complex numbers. Furthermore, \( |\omega_i| = \sqrt{q} \), for all \( 1 \leq i \leq 2g \), and \( |\beta_i| = 1 \), for all \( 1 \leq i \leq \Delta_X \). In addition, \( \Delta_X \leq \pi - g \), where \( \pi \) is the arithmetic genus of \( C \).

For \( q \) an odd prime power, elliptic curves over \( \mathbb{F}_q \) are curves given by equations of the form

\[
y^2 = ax^3 + bx^2 + cx + d,
\]

with \( 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 \neq 0 \), where \( a \neq 0, b, c, d \) are elements of \( \mathbb{F}_q \). Results involving points on elliptic curves can be found in [14, 20, 21]. Since the elliptic curve \( C : y^2 = ax^3 + bx^2 + cx + d \) has genus 1, Theorem 1.1 states that there is a complex number \( \omega_q(a, b, c, d) \) satisfying

\[
N_n(C) = q^n + 1 - \omega_q(a, b, c, d)^n - \overline{\omega_q(a, b, c, d)}^n,
\]

where \( |\omega_q(a, b, c, d)| = \sqrt{q} \). In Section 3, we show a way to calculate \( \omega_q(a, b, c, d) \) computationally faster than direct computation.

In this work, we use sums of characters to give the number of rational points on suitable curves of degree 3, 4 and 6 over \( \mathbb{F}_q \) in terms of the complex numbers \( \omega_q(a, b, c, d) \). Although the clear connection between sums of characters and number of rational points on curves, there exists few articles in literature exploring this relation. The connection between sums of characters and elliptic curves have already been studied by Williams [26]. We use techniques similar to those used by Williams in addition to character properties, associating different forms to count the number of points on the same curve in order to get the exact number of points. In this work, we are interested in affine curves with equation \( y^i = f(x) \), where \( i = 2, 3 \) or 4 and \( f(x) \) has suitable form. For \( n \) a positive integer, let \( i \) be a divisor of \( q^n - 1 \) and \( \chi_i \) denotes a multiplicative character of order \( i \) on \( \mathbb{F}_q^* \). To reduce the notation, we leave implicit the dependence on \( n \). It is convenient to extend the domain of the definition of \( \chi_i \) from \( \mathbb{F}_q^* \) to \( \mathbb{F}_{q^n}^* \) by setting \( \chi_i(0) = 1 \) if \( i = 1 \) and \( \chi_i(0) = 0 \) if \( i \geq 2 \). Some of the main results of this paper are the following.
Theorem 1.2. Let $a, b \in \mathbb{F}_q^*$. The number of rational points on the curve $C : y^3 = ax^6 + b$ over $\mathbb{F}_{q^n}$ satisfies

$$N_n(C) = q^n + 1 - \omega_1^n - \omega_2^n - \omega_3^n - \omega_4^n - \omega_5^n - \omega_6^n - \chi_3(a) - \chi_3^2(a),$$

where $\omega_1 := \omega_q(a^{-1}, 0, 0, -ba^{-1})$, $\omega_2 := \omega_q(b^{-1}, 0, 0, -ab^{-1})$, $\omega_3 := \omega_q(1, 0, 0, -4ab)$ and $\omega_4 := \omega_q(-4ab, 0, 0, 1)$.

Despite the following Theorem does not express the number of rational points on the curves in terms of $\omega_q(a, b, c, d)$, this general result will be useful to calculate the number of points on special curves of low degree.

Theorem 1.3. Let $A, B, C, a, b, c$ be elements in $\mathbb{F}_q$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}$ be the roots of the polynomial $f(x) = ax^2 + bx + c$. Let $C_1 : y^2 = (Ax^2 + Bx + C)(ax^2 + bx + c)^{-1}$ and $C_2 : y^3(ax^2 + bx + c) = Ax^2 + Bx + C$ be two curves over $\mathbb{F}_q$. The number of rational points on the curves $C_1$ and $C_2$ over $\mathbb{F}_{q^n}$ satisfies

$$N_n(C_1) = N_n(C) - \sum_{j=1}^{i-1} \chi_j^i \left(\frac{A}{a}\right) - \delta + \gamma$$

and

$$N_n(C_2) = N_n(C) + 1 - \sum_{j=1}^{i-1} \chi_j^i \left(\frac{A}{a}\right) - \delta,$$

where $C$ is the curve over $\overline{\mathbb{F}}_q$ given by the equation $z^2 = (B - by^i)^2 - 4(A - ay^i)(C - cy^i)$, $\gamma := \mathbb{1}_{\{\alpha_1 \in \mathbb{F}_{q^n}\}} + \mathbb{1}_{\{\alpha_1 \in \mathbb{F}_{q^n}, \alpha_1 \neq \alpha_2\}}$ and $\delta$ is given by

$$\delta := \begin{cases} 1 + \chi_2(b^2 - 4ac), & \text{if } i = 1; \\ 1 + \chi_2(4Ac + 4Ca - 2Bb), & \text{if } i = 2 \text{ and } b^2 - 4ac = 0; \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 1.4. For $a, b, c \in \mathbb{F}_q$ with $a \neq 0$, let $C : y^4 = ax^4 + bx^2 + c$ be a curve over $\mathbb{F}_q$, with $q \equiv 1 \pmod{4}$. The number of rational points on $C$ over $\mathbb{F}_{q^n}$ satisfies

$$N_n(C) = \begin{cases} q^n + 1 - \omega_1^n + \omega_2^n + \omega_3^n + \omega_4^n, & \text{if } b^2 - 4ac \neq 0 \text{ and } c \neq 0; \\ q^n + 1 - \omega_1^n + \omega_2^n + \omega_3^n + \omega_4^n, & \text{if } b^2 - 4ac \neq 0 \text{ and } c = 0; \\ q^n + 1 - \omega_1^n + \omega_2^n + \omega_3^n + \omega_4^n, & \text{if } b^2 - 4ac = 0 \text{ and } c \neq 0; \\ q^n + 1 - \omega_1^n + \omega_2^n + \omega_3^n + \omega_4^n, & \text{if } b^2 - 4ac = 0 \text{ and } c = 0, \end{cases}$$

where $\omega_1 := \omega_q(a^{-1}, 0, d_1, 0)$, $d_1 := \frac{b^2 - 4ac}{4a^2}$, $\omega_2 := \omega_q(c^{-1}, 0, d_2, 0)$, $d_2 := \frac{b^2 - 4ac}{4c}$ and $\omega_3 := \omega_q(a, b, c, 0)$.
In order to prove these main results, we calculate the number of points on many others curves. For all the curves, we give explicitly the complex numbers from Theorem 1.1, as we can see in Theorems 1.2 and 1.4.

As a consequence of the results presented throughout the paper, in Section 7 we discuss about the maximality and minimality of curves with equations of the form

$$ax^n + by^n + cz^n = 0$$

in the cases $n = 3$ and $n = 4$, where $a, b, c$ are elements in a prime field $\mathbb{F}_p$, generalizing the conditions presented by Garcia and Tafazolian [7] in these cases. The case where $a = b = c = 1$, the well-known Fermat curve, was discussed in [7]. More generally, the techniques presented here give a new way to state when an irreducible curve attains the upper bound given in Theorem 1.1.

The reason why we can not generalize this results to curves given by equations of the form $y^i = f(x)$ of any degree is due to the fact that we do not know how to relate any sum of characters with a elliptic curves. For low degree, there is a natural way to find this relation, as we use in the results in this article.

2. Preliminaries

In this section, we recall some general results involving rational points on curves over finite fields. Throughout the paper, we use the notation bellow.

**Notation**

- $\mathbb{F}_q$ is a finite fields with $q = p^k$ elements.
- $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$.
- For a curve $C$ over $\mathbb{F}_q$ and $n \geq 1$, the set of $\mathbb{F}_q^n$-rational points is denoted by $C(\mathbb{F}_q^n)$.
- $N_n(C)$ is the number of rational points of a curve $C$ over $\mathbb{F}_q^n$.
- The genus of a curve $C$ over $\mathbb{F}_q$ is denoted by $g$.
- For $D$ a divisor of a curve $C$, $N(D) = q^{\deg(D)}$ is the norm of $D$.
- $\overline{\omega}$ denotes the complex conjugate of a complex number $\omega$.
- The indicator function of an event $A$ is denoted by $1_A$.
- For $n$ a positive integer, let $i$ be a divisor of $q^n - 1$ and $\chi_i$ denotes a multiplicative character of order $i$ on $\mathbb{F}_q^n$. 


Remark 2.1. The algebraic curves theory is developed in the projective space, then points at the infinity may be on the curve. For example, the point \((x_0, y_0, z_0) = (0, 1, 0)\) is on the homogenization of the elliptic curve \(y^2 = x^3 + 1\). Therefore, Theorem 1.1 is considering those points at the infinity. In the results that we present in this paper, we follow that convention, considering those rational points.

Definition 2.2. Let \(a \neq 0, b, c, d\) be elements in \(F_q\). The curve \(C: y^2 = ax^3 + bx^2 + cx + d\) is called elliptic curve over \(F_q\) if the roots of the polynomial \(f(x) := ax^3 + bx^2 + cx + d\) are distinct.

As a direct consequence from Riemann Hypothesis, we have the following result.

Theorem 2.3. Let \(C: x^2 = ay^3 + by^2 + cy + d\) be an elliptic curve over a finite field \(F_q\). There exists a complex number \(\omega\), with \(|\omega| = \sqrt{q}\), that satisfies

\[N_n(C) = q^n + 1 - \omega^n - \overline{\omega}^n.\]

The number \(\omega\) is unique unless conjugation. As \(\omega\) depends on \(a, b, c, d\) and \(q\), we denote \(\omega\) by \(\omega_q(a, b, c, d)\).

As \(\omega_q(a, b, c, d)\) is unique unless conjugation, we let

\[\omega_q: F_q^* \times F_q^3 \longrightarrow \{z \in \mathbb{C} : |z| = \sqrt{q}, \Im(\omega) \geq 0\}\]  

be the function defined by \((a, b, c, d) \mapsto \omega_q(a, b, c, d)\), where \(\Im(\omega)\) denotes the imaginary part of \(\omega_q\). In Section 3, we present a way to compute \(\omega_q(a, b, c, d)\) computationally faster.

Remark 2.4. By definition of \(\omega_q\) and Theorem 2.3, we have \(\omega_q^n(a, b, c, d) = \omega_q(a, b, c, d)^n\) for all \(a, b, c, d \in F_q\) and for all positive integer \(n\).

3. Rational Points On Elliptic Curves

From now, we consider \(q\) odd.

Lemma 3.1. [15, Theorem 5.48] If \(a, b, c \in F_q\), with \(a \neq 0\) and \(\Delta := b^2 - 4ac\), then

\[
\sum_{x \in F_q^n} \chi_2(ax^2 + bx + c) = \begin{cases} 
-\chi_2(a), & \text{if } \Delta \neq 0; \\
(q^n - 1)\chi_2(a), & \text{if } \Delta = 0.
\end{cases}
\]

Lemma 3.2. [15, Theorem 5.4] If \(\chi\) is a nontrivial multiplicative character of \(F_q^*\), then

\[
\sum_{g \in F_q} \chi(g) = 0.
\]
Remark 3.3. The discriminant of a cubic polynomial \( f(x) = ax^3 + bx^2 + cx + d \) is given by
\[
\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2,
\] (3)
where \( \Delta \neq 0 \) if and only if the roots of \( f(x) \) are distinct. In addition, every root of \( f(x) \) is an element of \( \mathbb{F}_q \) if \( \Delta = 0 \).

From here, let \( \Delta(a, b, c, d) \) denote the discriminant of the polynomial \( f(x) = ax^3 + bx^2 + cx + d \).

Lemma 3.4. Let \( a, b, c, d \in \mathbb{F}_q \) be elements in \( \mathbb{F}_q \), with \( a \neq 0 \). If \( \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q^* \) are the roots of the polynomial \( f(x) := ax^3 + bx^2 + cx + d \), then
\[
\sum_{x \in \mathbb{F}_q^n} \chi_2(f(x)) = \begin{cases} 
-\omega_q(n) - \omega_q(n), & \text{if } \Delta \neq 0; \\
-\chi_2(\alpha), & \text{if } f(x) = a(x - \alpha)^2(x - \beta); \\
0, & \text{if } f(x) = a(x - \alpha)^3,
\end{cases}
\]
where \( \Delta := \Delta(a, b, c, d) \) as defined in Equation (3) and the complex number \( \omega_q(a, b, c, d) \) is defined as in Theorem 2.3.

Proof: Let \( C \) be the curve \( y^2 = ax^3 + cx^2 + cx + d \). We observe that
\[
N_n(C) = 1 + \sum_{x \in \mathbb{F}_q^n} [1 + \chi_2(ax^3 + bx^2 + cx + d)].
\]
By Theorem 2.3, if \( \Delta \neq 0 \), we have
\[
N_n(C) = 1 + \sum_{x \in \mathbb{F}_q^n} [1 + \chi_2(ax^3 + bx^2 + cx + d)] = q^n + 1 - \omega_q(a, b, c, d)n - \omega_q(a, b, c, d)n,
\]
As \( \sum_{x \in \mathbb{F}_q^n} 1 = q^n \), the result follows. If \( \Delta = 0 \), then there exists a root \( \alpha \in \mathbb{F}_q \) of the polynomial \( ax^3 + bx^2 + cx + d \) with multiplicity \( \geq 2 \). Hence, \( ax^3 + bx^2 + cx + d = a(x - \alpha)^2(x - \beta) \), with \( \alpha, \beta \in \mathbb{F}_q \). Thus, from the relation
\[
\chi_2(ax^3 + bx^2 + cx + d) = \chi_2((x - \alpha)^2(x - \beta)) = \begin{cases} 
\chi_2(a(x - \beta)), & \text{if } x \neq \alpha; \\
0, & \text{if } x = \alpha,
\end{cases}
\]
and Lemma 3.2, we have
\[
\sum_{x \in \mathbb{F}_q^n} \chi_2(ax^3 + bx^2 + cx + d) = \sum_{x \in \mathbb{F}_q^n \setminus \{\alpha\}} \chi_2(a(x - \alpha)^2(x - \beta)) = \sum_{x \in \mathbb{F}_q^n \setminus \{\alpha\}} \chi_2(ax - a\beta) = -\chi_2(a\alpha - a\beta).
\]
This complete the proof. \( \square \)
As we use Lemma 3.4 in most results in this paper, it is convenient to introduce the following notation. We define the function $\Delta^\prime : \mathbb{F}_q^4 \to \{1, 2, 3\}$ by letting

$$\Delta^\prime(a, b, c, d) = \begin{cases} 1, & \text{if } \alpha_i \neq \alpha_j \text{ for all } 1 \leq i < j \leq 3; \\ 2, & \text{if } \alpha_i = \alpha_j \neq \alpha_k \text{ for some } \{i, j, k\} = \{1, 2, 3\}; \\ 3, & \text{if } \alpha_1 = \alpha_2 = \alpha_3, \end{cases}$$

where $\alpha_1, \alpha_2, \alpha_3$ are the roots of the polynomial $f(x) := ax^3 + bx^2 + cx + d$. From this definition, it follows that $\Delta(a, b, c, d) \neq 0$ if and only if $\Delta^\prime(a, b, c, d) = 1$. We also define the function $\alpha : \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_q^4 : \Delta^\prime(a, b, c, d) = 2\} \to \mathbb{F}_q$ by

$$\alpha(a, b, c, d) = a\alpha_1 - a\alpha_2,$$

where $f(x) = a(x - \alpha_1)^2(x - \alpha_2)$.

**Lemma 3.5.** [15, Lemma 7.3] Let $m$ be a positive integer. We have

$$\sum_{a \in \mathbb{F}_q} a^m = \begin{cases} 0, & \text{if } (q - 1) \nmid m \text{ or } m = 0; \\ -1, & \text{if } (q - 1) \mid m \text{ and } m \neq 0, \end{cases}$$

where $0^0 := 1$.

**Remark 3.6.** It is known that $\chi_2(a) = (-1)^n \in \mathbb{C}$ if and only if $a^{\frac{q - 1}{2}} = (-1)^n \in \mathbb{F}_q$. Indeed, by definition, $\chi_2(b) = -1$ if and only if $b$ is not a square in $\mathbb{F}_q^*$, so $b = \theta^i$, where $\theta$ is a generator of the group $\mathbb{F}_q^*$ and $i$ is odd. It follows that $b^{\frac{q - 1}{2}} = (\theta^{\frac{q - 1}{2}})^i = (-1)^i = -1$.

In similar way, we have that $\chi_2(b) = -1$ if and only if $b^{\frac{q - 1}{2}} = 1$.

The following lemma characterizes, modulo $p$, the trace of Frobenius

$$\tau_q(a, b, c, d) := \omega_q(a, b, c, d) + \omega_q(a, b, c, d)$$

of an elliptic curve given by equation $g^2 = ax^3 + bx^2 + cx + d$ over $\mathbb{F}_p$. As we are interested in odd characteristic, we suppose $b = 0$. This lemma enables us to calculate the number of points on elliptic curves whose coefficients are in a prime field $\mathbb{F}_p$.

**Lemma 3.7.** Let $\mathcal{C} : y^2 = Ax^3 + Bx + C$ be an elliptic curve over $\mathbb{F}_{p^n}$, where $p$ is an odd prime. The trace of Frobenius of $\mathcal{C}$ satisfies the relation

$$\tau_{p^n}(A, 0, B, C) \equiv \sum_{l = \frac{p^n - 1}{2}}^{\lfloor \frac{p^n - 1}{2} \rfloor} \left( \begin{array}{c} p^n - 1 \\ 2l \end{array} \right) \left( \begin{array}{c} 2l \\ \frac{p^n - 1}{2} - 2l \end{array} \right) A^{\frac{p^n - 1}{2} - l} B^{\frac{p^n - 1}{2} - 2l} C^{\frac{p^n - 1}{2} - 2l} \pmod{p}.$$

**Proof:** We observe that

$$1 + \chi(Ax^3 + Bx + C) = \begin{cases} 0, & \text{if } Ax^3 + Bx + C \text{ is not a square in } \mathbb{F}_{p^n}; \\ 2, & \text{if } Ax^3 + Bx + C \text{ is a square in } \mathbb{F}_{p^n}. \end{cases}$$
Therefore, we have
\[ N_1(C) = 1 + \sum_{x \in \mathbb{F}_p} [1 + \chi(Ax^3 + Bx + C)] = p^n + 1 + \sum_{x \in \mathbb{F}_p} \chi(Ax^3 + Bx + C). \]

By Remark 3.6,
\[ \sum_{x \in \mathbb{F}_p} \chi(x^3 + Ax + B) \equiv \sum_{x \in \mathbb{F}_p} (Ax^3 + Bx + C)^{p^n - 1 \over 2} \]
\[ \equiv \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{p^n-1} \binom{p^n-1}{i} (Ax^3 + Bx)^i C^{p^n-1-i \over 2} \]
\[ \equiv \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{p^n-1} \binom{p^n-1}{i} C^{p^n-1-i \over 2} \sum_{j=0}^{i} \binom{i}{j} A^j B^{i-j} x^{2j+i} \]
\[ \equiv \sum_{x \in \mathbb{F}_p} \sum_{i=0}^{p^n-1} \sum_{j=0}^{i} \binom{p^n-1}{i} \binom{i}{j} A^j B^{i-j} C^{p^n-1-i \over 2} x^{2j+i} \pmod{p}. \]

By Lemma 3.5, the sum \( \sum_{x \in \mathbb{F}_p} x^{2j+i} \) is nonzero only if \( 2j + i \equiv 0 \pmod{p^n - 1} \) and \( 2j + i \neq 0 \), and in these cases, the sum is \( -1 \). In addition, since
\[ 2j + i \leq 2 \cdot \frac{p^n - 1}{2} + \frac{p^n - 1}{2} = \frac{3(p^n - 1)}{2} < 2(p^n - 1), \]
it follows that
\[ N_1(C) - p^n - 1 \equiv \sum_{i=0}^{p^n-1} \sum_{j=0}^{i} \binom{p^n-1}{i} \binom{i}{j} A^j B^{i-j} C^{p^n-1-i \over 2} \sum_{x \in \mathbb{F}_p} x^{2j+i} \]
\[ \equiv - \sum_{l=\left\lfloor \frac{p^n-1}{6} \right\rfloor}^{\frac{p^n-1}{2}} \binom{p^n-1}{2l} \left( \frac{2l}{p^n-1-2l} \right) A^{p^n-1-2l \over 2} B^{2l-p^{n-1-2l \over 2}} C^{p^n-1-2l \over 2} \]
\[ \equiv - \sum_{l=\left\lfloor \frac{p^n-1}{6} \right\rfloor}^{\frac{p^n-1}{2}} \binom{p^n-1}{2l} \left( \frac{2l}{p^n-1-2l} \right) A^{p^n-1-2l \over 2} B^{2l-p^{n-1-2l \over 2}} C^{p^n-1-2l \over 2} \pmod{p}. \]

Since \( N_1(C) = p^n + 1 - \tau_p(A, 0, B, C) \), the result follows. \( \square \)

In Lemma 3.7 there is an abuse of language when we write
\[ \sum_{x \in \mathbb{F}_p} \chi(x^3 + Ax + B) \equiv \sum_{x \in \mathbb{F}_p} (Ax^3 + Bx + C)^{p^n-1 \over 2} \]
since the left summation is over \( C \) and the right summation is over \( \mathbb{F}_q \). In fact, we do it many times throughout this paper.

Since \( |\tau(A, 0, B, C)| = |\omega_p(A, 0, B, C) + \omega_p(A, 0, B, C)| \leq 2 \sqrt{p} \) (by Theorem 2.3), we can use Lemma 3.7 to calculate the complex number \( \omega_p(A, 0, B, C) \) in the case where \( p \geq 17 \), as in the following example.
Example 3.8. Let $J : x^2 = y^3 + 2$ be an elliptic curve over $\mathbb{F}_{19}$. From Lemma 3.7,

$$\omega_{19}(1, 0, 0, 2) + \omega_{19}(1, 0, 0, 2) \equiv \sum_{l=3}^{4} \binom{9}{2l} \binom{2l}{9-1} 9^{2l-9} 2^{g-2l} \equiv 7 \pmod{19}.$$ 

Since $|\omega_{19}(1, 0, 0, 2) + \omega_{19}(1, 0, 0, 2)| \leq |2\sqrt{19}| = 8$, we have $\omega_{19}(1, 0, 0, 2) + \omega_{19}(1, 0, 0, 2) = 7$. Thus, using that $|\omega_{19}(1, 0, 0, 2)| = \sqrt{19}$, we must have

$$\omega_{19}(1, 0, 0, 2) = \frac{7}{2} + i\sqrt{19 - \frac{7^2}{2^2}} = \frac{7}{2} + i\sqrt{27/4}.$$ 

In addition, the number of rational points of $J$ over $\mathbb{F}_{19^n}$ is given by

$$N_n(J) = 19^n + 1 - \left(\frac{7}{2} + i\sqrt{27/4}\right)^n - \left(\frac{7}{2} - i\sqrt{27/4}\right)^n.$$ 

We will use this technique in the examples of this paper in order to calculate the number of rational points on suitable curves. In [22], the author presents congruences similar to the congruence in Lemma 3.7. In fact, some values of $\omega_q$ are well-known in the case where $p$ is a prime number, e.g. see Theorem 6.2.9 and Theorem 6.2.10 in [2].

4. Rational Points on Curves of the Form $y^2 = f(x)$

Throughout this section, for an event $A$, let

$$1_A := \begin{cases} 
1, & \text{if } A \text{ occurs;} \\
0, & \text{if } A \text{ does not occur}
\end{cases}$$

be the indicator function of the event $A$. In algebraic geometry, a hyperelliptic curve of genus $g \geq 1$ is an algebraic curve given by equation

$$y^2 + h(x)y = f(x),$$

where $f(x)$ is a polynomial of degree $2g+1$ or $2g+2$ with distinct roots and $h(x)$ is a polynomial of degree $\leq g+1$. When the characteristic of the field is not 2, we can take $h(x) = 0$ (make the change of variables, by taking $y = z - \frac{1}{2}h(x)$ and $x = w$). Hyperelliptic curves are useful in cryptography (for example, see [3]). In Ulas [25] and Nelson, Solymosi, Tom and Wong [18], the authors present results concerning the number of rational points on hyperelliptic curves. In this Section, we present the number of rational points on curves of the form $y^2 = f(x)$, where $f(x) \in \mathbb{F}_q$ is a suitable polynomial of degree 4 or 6. In particular, we give the number of points on most hyperelliptic curves of genus 1 when $q$ is odd.
**Remark 4.1.** Let $\Lambda_1, \Lambda_2 \subset \mathbb{F}_q$ be two sets with the same number of elements. Let $f$ be a bijective map from $\Lambda_1$ to $\Lambda_2$ and $g : \Lambda_2 \to \mathbb{F}_q$ an arbitrary function. Then

$$\sum_{x \in \Lambda_1} \chi_i(g(f(x))) = \sum_{z \in \Lambda_2} \chi_i(g(z)).$$

**Lemma 4.2.** If $a, b, c, d \in \mathbb{F}_q$, with $a \neq 0$ and $d \neq 0$, then

$$\sum_{x \in \mathbb{F}_q^n} \chi_2(ax^3 + bx^2 + cx + d) \chi_2(x) = \begin{cases} -\omega_q(d, c, b, a)^n - \omega_q(d, c, b, a) - \chi_2(a), & \text{if } \Delta' = 1; \\ -\chi_2(a) - \chi_2(a), & \text{if } \Delta' = 2; \\ -\chi_2(a), & \text{if } \Delta' = 3, \end{cases}$$

where $\Delta' := \Delta'(a, b, c, d)$, $\alpha := \alpha(a, b, c, d)$ and $\omega_q(d, c, b, a)$ is defined as in Theorem 2.3.

**Proof:** Using the fact that $\chi_2(0) = 0$, we have

$$\sum_{x \in \mathbb{F}_q^n} \chi_2(ax^3 + bx^2 + cx + d) \chi_2(x) = \sum_{x \in \mathbb{F}_q^n} \chi_2(ax^3 + bx^2 + cx + d) \chi_2(x^{-3})$$

$$= \sum_{x \in \mathbb{F}_q^n} \chi_2(a + bx^{-1} + cx^{-2} + dx^{-3})$$

$$= \sum_{x \in \mathbb{F}_q^n} \chi_2(a + bz + cz^2 + dz^3).$$

By Lemma 3.4,

$$\sum_{x \in \mathbb{F}_q^n} \chi_2(a + bz + cz^2 + dz^3) = \begin{cases} -\omega_q(d, c, b, a)^n - \omega_q(d, c, b, a) - \chi_2(a), & \text{if } \Delta' = 1; \\ -\chi_2(a) - \chi_2(a), & \text{if } \Delta' = 2; \\ -\chi_2(a), & \text{if } \Delta' = 3, \end{cases}$$

where $\Delta' := \Delta'(a, b, c, d)$ and $\alpha := \alpha(a, b, c, d)$. \qed

**Theorem 4.3.** For $a, b, c, d, e \in \mathbb{F}_q$, with $a \neq 0$, let $C : y^2 = (ax^3 + bx^2 + cx + d)(x + e)$ be a curve over $\mathbb{F}_q$. The number of rational points on $C$ over $\mathbb{F}_q^n$ satisfies

$$N_n(C) = \begin{cases} q^n + 1 - \omega_q(d', c', b', a') - \omega_q(d', c', b', a') - \chi_2(a'), & \text{if } d' \neq 0 \text{ and } \Delta' = 1; \\ q^n + 1 - \chi_2(a') - \chi_2(a'), & \text{if } d' \neq 0 \text{ and } \Delta' = 2; \\ q^n + 1 - \chi_2(a') - \chi_2(c'), & \text{if } d' = 0 \text{ and } (b')^2 \neq 4a'c'; \\ q^n + 1 + (q^n - 1)(\chi_2(a') - \chi_2(c')), & \text{if } d' = 0 \text{ and } (b')^2 = 4a'c'; \end{cases}$$

where $a' = a$, $b' = b - 3ae$, $c' = 3ae^2 - 2eb + c$, $d' = be^2 - ae^3 + d - ec$, $\Delta' := \Delta'(a', b', c', d')$ and $\alpha := \alpha(a', b', c', d')$. 


Proof: We have

\[
N_n(C) = 1 + \sum_{x \in \mathbb{F}_q^n} [1 + \chi_2(ax^3 + bx^2 + cx + d)\chi_2(x + e)]
\]

\[
= q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \chi_2(a(z - e)^3 + b(z - e)^2 + c(z - e) + d)\chi_2(z)
\]

\[
= q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \chi_2(a(z^3 - 3z^2e + 3ze^2 - e^3) + b(z^2 - 2ze + e^2) + c(z - e) + d)\chi_2(z)
\]

\[
= q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \chi_2(a(z^3 - 3z^2e + 3ze^2 - e^3) + b(z^2 - 2ze + e^2) + c(z - e) + d)\chi_2(z).
\]

Hence, the result follows by Lemma 4.2 in the case \(be^2 - ae^3 + d - ec \neq 0\). Otherwise,

\[
N_n(C) = q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \chi_2(a(z^3 - 3z^2e + 3ze^2 - e^3) + (3ae^2 - 2eb + c)z + be^2 - ae^3 + d - ec)\chi_2(z).
\]

In this case, the result follows by Lemma 3.1.

Example 4.4. Let \(J : y^2 = (x^3 + x^2 - x + 1)(x + 1)\) be a curve over \(\mathbb{F}_{73}\). In order to calculate \(\omega_{73}(2,0,-2,1)\), we use Lemma 3.7 as in Example 3.8. We note that

\[
\omega_{73}(2,0,-2,1) + \overline{\omega_{73}(2,0,-2,1)} \equiv \sum_{l=12}^{18} \binom{36}{2l} \left( \frac{2l}{36-l} \right) z^{36-l}(-2)^{3l-36} \equiv 16 \pmod{73},
\]

then \(\omega_{73}(2,0,-2,1) = 8 + 3i\). Since \(\Delta'(2,0,-2,1) = 1\), Theorem 4.3 states that the number of rational points on \(J\) over \(\mathbb{F}_{73^n}\) is given by

\[
N_n(J) = 73^n - (8 + 3i)^n - (8 + 3i)^n.
\]

Theorem 4.5. For \(a, b, c, d \in \mathbb{F}_q\), with \(a \neq 0\), let \(C : y^2 = ax^6 + bx^4 + cx^2 + d\) be a curve over \(\mathbb{F}_q\). The number of rational points on \(C\) over \(\mathbb{F}_{q^n}\) is given by

\[
N_n(C) = \begin{cases} 
q^n + 1 - \omega_1^n - \overline{\omega_1}^n - \omega_2^n - \overline{\omega_2}^n - \chi_2(a), & \text{if } d \neq 0 \text{ and } \Delta' = 1; \\
q^n + 1 - \chi(\alpha_1) - \chi(\alpha_2) - \chi_2(a), & \text{if } d \neq 0 \text{ and } \Delta' = 2; \\
q^n + 1 - \chi_2(a), & \text{if } d \neq 0 \text{ and } \Delta' = 3; \\
q^n + 1 - \omega_1^n - \overline{\omega_1}^n - \chi_2(a) - \chi_2(c), & \text{if } d = 0 \neq c \text{ and } b^2 - 4ac \neq 0; \\
q^n + 1 - \chi(\alpha_1) + (q^n - 1)\chi(a) - \chi_2(c), & \text{if } d = 0 \text{ and } b^2 - 4ac = 0; \\
q^n + 1 - \chi(\alpha_1) - \chi_2(a) - \chi_2(c), & \text{if } c = d = 0 \text{ and } b^2 - 4ac \neq 0,
\end{cases}
\]

where \(\omega_1 := \omega_q(a,b,c,d), \omega_2 := \omega_q(d,c,b,a), \alpha_1 := \alpha(a,b,c,d), \alpha_2 := \alpha(d,c,b,a)\) and \(\Delta' := \Delta'(a,b,c,d)\).
Proof: The number of rational points on $C$ is given by

$$N_n(C) = 1 + \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_2(ax^3 + bx^2 + cx + d) \right] \left[ 1 + \chi_2(x) \right]$$

$$= q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \left[ \chi_2(ax^3 + bx^2 + cx + d) + \chi_2(x) + \chi_2(ax^3 + bx^2 + cx + d) \chi_2(x) \right].$$

The result follows by Lemma 3.4, Lemma 3.2 and Lemma 4.2 in the case $d \neq 0$. Otherwise,

$$N_n(C) = q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \chi_2(ax^3 + bx^2 + cx) + \sum_{x \in \mathbb{F}_q^n} \chi_2(ax^3 + bx^2 + cx) \chi_2(\frac{1}{x})$$

$$= q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \chi_2(ax^3 + bx^2 + cx) + \sum_{x \in \mathbb{F}_q^n} \chi_2(ax^2 + bx + c).$$

Hence, the result follows by Lemma 3.1 and Lemma 3.4. \qed

Example 4.6. Let $J : y^2 = 2x^6 + 1$ be a curve over $\mathbb{F}_{29}$. In order to calculate $\omega_{29}(2, 0, 0, 1)$ and $\omega_{29}(1, 0, 0, 2)$, we use Lemma 3.7 as in Example 3.8. We note that

$$\omega_{29}(2, 0, 0, 1) + \omega_{29}(2, 0, 0, 1) \equiv \sum_{l=5}^{7} \binom{14}{2l} \left( \frac{2l}{14 - l} \right) 2^{14 - l} - 0^{14 - l} 1^{14 - 2l} \equiv 0 \pmod{29}$$

and

$$\omega_{29}(1, 0, 0, 2) + \omega_{29}(1, 0, 0, 2) \equiv \sum_{l=5}^{7} \binom{14}{2l} \left( \frac{2l}{14 - l} \right) 1^{14 - l} - 0^{14 - l} 2^{14 - 2l} \equiv 0 \pmod{29},$$

then $\omega_{29}(2, 0, 0, 1) = \omega_{29}(1, 0, 0, 2) = i\sqrt{29}$. Since 2 is not square residue in $\mathbb{F}_{29}$ and $\Delta(2, 0, 0, 1) = 1$, Theorem 4.5 states that the number of rational points on $J$ over $\mathbb{F}_{29^n}$ is given by

$$N_n(J) = \begin{cases} 29^n + 4 \cdot 29^{2k+1}, & \text{if } n = 4k + 2 \text{ for an integer } k; \\ 29^n - 4 \cdot 29^{2k}, & \text{if } n = 4k \text{ for an integer } k; \\ 29^n + 2, & \text{if } n \equiv 1 \pmod{2}. \end{cases}$$

Theorem 4.7. For $a, b, c \in \mathbb{F}_q$, with $a \neq 0$, let $C : y^2 = ax^4 + bx^2 + c$ be a curve over $\mathbb{F}_q$.

The number of rational points on $C$ over $\mathbb{F}_{q^n}$ is given by

$$N_n(C) = \begin{cases} q^n + 1 - \omega_q(a, b, c, 0)^n - \omega_q(a, b, c, 0)^n - \chi_2(a), & \text{if } b^2 - 4ac \neq 0, \text{ with } c \neq 0; \\ q^n + 1 - \chi_2(b) - \chi_2(a), & \text{if } b^2 - 4ac \neq 0, \text{ with } c = 0; \\ q^n + 1 - \chi_2(b/2) + (q^n - 1) \chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c \neq 0; \\ q^n + 1 + (q^n - 1) \chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c = 0. \end{cases}$$

Proof: As in the last theorem,

$$N_n(C) = q^n + 1 + \sum_{x \in \mathbb{F}_q^n} \left[ \chi_2(ax^2 + bx + c) + \chi_2(x) + \chi_2(ax^3 + bx^2 + cx) \right].$$

By Lemma 3.1, Lemma 3.2 and Lemma 3.4, the result follows. \qed
Lemma 4.8. Let \( i \) be a divisor of \( q^n - 1 \) and \( A, B, C, a, b, c \in \mathbb{F}_q \), with \( A \neq 0 \) and \( a \neq 0 \). If \( \alpha_1, \alpha_2 \in \mathbb{F}_q^* \) are the roots of the polynomial \( f(x) = ax^2 + bx + c \) and the polynomials \( f(x) \) and \( g(x) = Ax^2 + Bx + C \) has no common roots, then

\[
\sum_{x \in \mathbb{F}_q^n, x \notin \{\alpha_1, \alpha_2\}} \left[ 1 + \chi_i \left( \frac{Ax^2 + Bx + C}{ax^2 + bx + c} \right) + \cdots + \chi_i^{i-1} \left( \frac{Ax^2 + Bx + C}{ax^2 + bx + c} \right) \right] = N_n(C) - \delta - \left[ 1 + \cdots + \chi_i^{i-1} \left( \frac{A}{a} \right) \right],
\]

where \( C \) is a curve given by the equation \( z^2 = (B - by^i)^2 - 4(A - ay^i)(C - cy^i) \) and \( \delta \) is a constant referent to points at the infinity given by

\[
\delta := \begin{cases} 
1 + \chi_2(b^2 - 4ac), & \text{if } i = 1; \\
1 + \chi_2(4Ac + 4Ca - 2Bb), & \text{if } i = 2 \text{ and } b^2 - 4ac = 0; \\
1, & \text{otherwise.}
\end{cases}
\]

Proof: We observe that the summation

\[
\sum_{x \in \mathbb{F}_q^n, x \notin \{\alpha_1, \alpha_2\}} \left[ 1 + \chi_i \left( \frac{Ax^2 + Bx + C}{ax^2 + bx + c} \right) + \cdots + \chi_i^{i-1} \left( \frac{Ax^2 + Bx + C}{ax^2 + bx + c} \right) \right]
\]

count the number of rational points on the curve \( C' : y^i(ax^2 + bx + c) = Ax^2 + Bx + C \) over \( \mathbb{F}_q^n \). Let \( y_0^i \in \mathbb{F}_q^n \), if there exists \( x_0 \in \mathbb{F}_q^n \) such that \((x_0, y_0^i)\) is on the curve, then it is given by one of the following

\[
by^i - B \pm \sqrt{(B - by^i)^2 - 4(A - ay^i)(C - cy^i)}
\]

\[2(A - ay^i).\]

Hence, fixing \( y_0^i \in \mathbb{F}_q^n \), there exists \( x_0 \in \mathbb{F}_q^n \) such that \((x_0, y_0^i)\) is on the curve \( C' \) only if \((B - by_0^i)^2 - 4(A - ay_0^i)(C - cy_0^i)\) is a square in \( \mathbb{F}_q^n \) or if \( y_0^i = Aa^{-1} \). Let \( C \) be the curve given by equation \( z^2 = (B - by^i)^2 - 4(A - ay^i)(C - cy^i) \). In the case where \( Aa^{-1} \) is a \( i \)-th power in \( \mathbb{F}_q^n \) and \( Aa^{-1}b \neq B \), there are \( i \) rational points of the form \((\frac{cA-Ca}{Ba-bA}, \gamma^i)\) on the curve \( C' \), where \( \gamma \) is a \( i \)-th primitive root of \( Aa^{-1} \). Since there are \( 2i \) rational points in \( C \) where \( y^i = Aa^{-1} \) (namely \((\pm \frac{Ba-bA}{a}, \gamma^i)\)), the result is proved in this case. In the case where \( Aa^{-1}b = B \), there are no rational points with \( y^i = Aa^{-1} \) on the curve \( C' \) and only \( i \) on \( C \), then, in the same way, the result follows. \( \square \)

Remark 4.9. Let \( b, c, A, B, C \in \mathbb{F}_q \), with \( A \neq 0 \), \( b \neq 0 \) and \( A\left(\frac{b}{a}\right)^2 + B\left(\frac{b}{a}\right) + C \neq 0 \). For \( i \) a divisor of \( q^n - 1 \), in the same way of the proof of Lemma 4.8, we have

\[
\sum_{x \in \mathbb{F}_q^n, x \notin \{-c/b\}} \left[ 1 + \chi_i \left( \frac{Ax^2 + Bx + C}{bx + c} \right) + \cdots + \chi_i^{i-1} \left( \frac{Ax^2 + Bx + C}{bx + c} \right) \right] = \begin{cases} 
N_n(C) - 2, & \text{if } i = 1; \\
N_n(C) - 1, & \text{otherwise.}
\end{cases}
\]

where \( C \) is a curve given by the equation \( z^2 = (B - by^i)^2 - 4A(C - cy^i) \).
Proof: (proof of 1.3) By Lemma 4.8,

\[ N_n(C_1) = 1 + \sum_{x \in \mathbb{F}_q^n} [1 + \cdots + \chi_i^{i-1}(Ax^2 + Bx + C)(ax^2 + bx + c)^{i-1}] \]

\[ = 1 + \mathbb{I}_{\{a_1 \in \mathbb{F}_q^n\}} + \mathbb{I}_{\{a_1 \in \mathbb{F}_q^n, a_1 \neq a_2\}} + \sum_{x \in \mathbb{F}_q^n \backslash \{a_1, a_2\}} [1 + \cdots + \chi_i^{i-1}\left(\frac{Ax^2 + Bx + C}{ax^2 + bx + c}\right)] \]

\[ = 1 + \mathbb{I}_{\{a_1 \in \mathbb{F}_q^n\}} + \mathbb{I}_{\{a_1 \in \mathbb{F}_q^n, a_1 \neq a_2\}} + N_n(C) - \left[1 + \chi_i\left(\frac{A}{a}\right) + \cdots + \chi_i^{i-1}\left(\frac{A}{a}\right)\right] - \delta, \]

where \( C \) is the curve given by the equation \( z^2 = (B - by)^2 - 4(A - ay)(C - cy) \). In the same way,

\[ N_n(C_2) = 2 + \sum_{x \in \mathbb{F}_q^n \backslash \{a_1, a_2\}} [1 + \chi_i\left(\frac{Ax^2 + Bx + C}{ax^2 + bx + c}\right) + \cdots + \chi_i^{i-1}\left(\frac{Ax^2 + Bx + C}{ax^2 + bx + c}\right)] \]

\[ = 2 + N_n(C) - \left[1 + \chi_i\left(\frac{A}{a}\right) + \cdots + \chi_i^{i-1}\left(\frac{A}{a}\right)\right] - \delta. \]

\[ \square \]

We have the necessary tools to calculate \( N_n(C) \) in some cases, as we will see in the following results.

Corollary 4.10. Let \( A, B, C, a, b, c \) be elements in \( \mathbb{F}_q \) that satisfy the hypothesis of the Lemma 4.8. Assuming \( b^2 - 4ac \neq 0 \) and \( B^2 - 4AC \neq 0 \), the number of rational points on the curve \( C : y^2(ax^2 + bx + c) = Ax^2 + Bx + C \) over \( \mathbb{F}_q^n \) is given by

\[ N_n(C) = \begin{cases} 
q^n + 1 - \omega_q(a', b', c', 0)^n - \overline{\omega_q(a', b', c', 0)}^n - \chi_2(a') - \chi_2\left(\frac{A}{a}\right), & \text{if } \Delta \neq 0; \\
q^n + 1 - \chi_2(\alpha) + (q^n - 1)\chi_2(a') - \chi_2\left(\frac{A}{a}\right), & \text{if } \Delta = 0,
\end{cases} \]

where \( a' := b^2 - 4ac, b' := 4Ac + 4Ca - 2Bb, c' := B^2 - 4AC, \Delta := \Delta(a', b', c', 0) \) and \( \alpha = \alpha(a', b', c', 0) \).

Proof: It follows from Theorem 1.3 and Theorem 4.7. \[ \square \]

Corollary 4.11. Let \( A, B, C, a, b, c \) be elements in \( \mathbb{F}_q \) that satisfy the hypothesis of the Lemma 4.8. Assuming \( b^2 - 4ac \neq 0 \) and \( B^2 - 4AC \neq 0 \), the number of rational points on the curve \( C : y^2 = (ax^2 + bx + c)(Ax^2 + Bx + C) \) over \( \mathbb{F}_q^n \) is given by

\[ N_n(C) = \begin{cases} 
q^n + 2 \cdot \mathbb{I}_{\{a_1 \in \mathbb{F}_q^n\}} - \omega_q(a', b', c', 0)^n - \overline{\omega_q(a', b', c', 0)}^n - \chi_2(a') - \chi_2\left(\frac{A}{a}\right), & \text{if } \Delta \neq 0; \\
q^n + 2 \cdot \mathbb{I}_{\{a_1 \in \mathbb{F}_q^n\}} - \chi_2(\alpha) + (q^n - 1)\chi_2(a'), & \text{if } \Delta = 0,
\end{cases} \]

where \( a' := b^2 - 4ac, b' := 4Ac + 4Ca - 2Bb, c' := B^2 - 4AC, \Delta := \Delta(a', b', c', 0) \) and \( \alpha = \alpha(a', b', c', 0) \).

Proof: It follows from Theorem 1.3 and Theorem 4.7. \[ \square \]
The result in Corollary 4.11 generalize the sums of quadratic characters studied by Williams in [26], where the author calculate the sum
\[ \sum_{x \in \mathbb{F}_p} \chi_2 \left( (ax^2 + bx + c)(Ax^2 + Bx + C) \right) \]
over a prime field \( \mathbb{F}_p \).

**Example 4.12.** Let \( \mathcal{J} : y^2 = (x^2 + 3x + 2)(x^2 - 2x - 5) \) be a curve over \( \mathbb{F}_{67} \). In order to calculate \( \omega_{67}(1, 0, 24, 0) \), we use Lemma 3.7 as in Example 3.8. We note that
\[ \omega_{67}(1, 0, 24, 0) + \omega_{67}(1, 0, 24, 0) \equiv \sum_{l=11}^{16} \binom{33}{2l} \left( \frac{2l}{33-l} \right) l^{33-l}(24)^{3l-33}0^{33-2l} \equiv 0 \pmod{67}, \]
then \( \omega_{67}(1, 0, 24, 0) = i\sqrt{67} \). Since \( \Delta(1, 0, 24, 0) = -55296 \neq 0 \), Corollary 4.11 states that the number of rational points on \( \mathcal{J} \) over \( \mathbb{F}_{67^n} \) is given by
\[ N_n(\mathcal{J}) = \begin{cases} 67^n - 2 \left( i\sqrt{67} \right)^n, & \text{if } n \text{ is even;} \\ 67^n, & \text{if } n \text{ is odd.} \end{cases} \]

In Theorem 4.3 and Corollary 4.11, we give the number of rational points on \( y^2 = f(x) \), where \( f(x) \) is a polynomial of degree 4 that is reducible over \( \mathbb{F}_q \). In Theorem 4.7 we give this number in the case where \( f(x) = ax^4 + bx^2 + c \). Hence, we presented the number of rational points on most hyperelliptic curves of degree 4 over finite fields of odd characteristic. The missing case is the curve given by the equation \( y^2 = ax^4 + bx^2 + cx + d \), with \( c \neq 0 \), where \( f(x) = ax^4 + bx^2 + cx + d \) is an irreducible polynomial over \( \mathbb{F}_q \). In fact, we do not know how to calculate the number of rational points in this specific case.

5. **Rational Points on Curves of the Form \( y^3 = f(x) \)**

In this section, we assume \( q \equiv 1 \pmod{3} \). The case \( q \not\equiv 1 \pmod{3} \) is not interesting, since the function \( y \mapsto y^3 \) permutes the elements of \( \mathbb{F}_q \).

**Theorem 5.1.** Let \( a, A, B, C \in \mathbb{F}_q \) with \( A \neq 0 \). Let \( \mathcal{C}_1 : y^3 = (x + a)(Ax^2 + Bx + C) \) and \( \mathcal{C}_2 : y^3 = (x + a)^2(Ax^2 + Bx + C)^2 \) be curves over \( \overline{\mathbb{F}_q} \). If \( Aa^2 - Ba + C \neq 0 \), then the number of rational points on \( \mathcal{C}_1 \) and \( \mathcal{C}_2 \) over \( \mathbb{F}_q \) satisfies
\[ N_n(\mathcal{C}_2) + \chi_3(A) + \chi_3^2(A) = N_n(\mathcal{C}_1) = q^n + 1 - \omega_q(a', 0, 0, c')^n - \omega_q(a', 0, 0, c')^n, \]
where \( a' := 4Aa^2 + 4C - 4Ba \) and \( c' := B^2 - 4AC \).

**Proof:** Since the number of rational points on the \( \mathcal{C}_1 : y^3 = (x + a)(Ax^2 + Bx + C) \) is equal to the number of rational points on the curve \( \mathcal{C}' : y^3 = (x + a)^3(Ax^2 + Bx + C) \),
unless 3 possible points at the infinity, the value \( N_n(C_1) \) follows from Theorem 1.3 and Lemma 3.4. In order to calculate \( N_n(C_2) \), we note that
\[
N_n(C_2) = 1 + \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3 ((x + a)^2(Ax^2 + Bx + C)^2) \right] \\
= 1 + \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3^2 ((x + a)^4(Ax^2 + Bx + C)^4) \right] \\
= 1 + \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3 ((x + a)(Ax^2 + Bx + C)) \right] \\
= N_n(C_1) - \chi_3(A) - \chi_3^2(A).
\]

Example 5.2. Let \( J_1 : y^3 = (x+3)(-x^2+2x+2) \) be a curve over \( \mathbb{F}_{37} \). In order to calculate \( \omega_{37}(-52,0,0,12) \), we use Lemma 3.7 as in Example 3.8. We note that
\[
\omega_{37}(-52,0,0,12) + \omega_{37}(-52,0,0,12) \equiv \sum_{l=6}^{9} \binom{18}{2l} \binom{2l}{18-l} (-52)^{18-l}0^{3l-18}12^{18-2l} \equiv 27 \pmod{37},
\]
then \( \omega_{37}(-52,0,0,12) = -5 + i\sqrt{12} \). Theorem 5.1 states that the number of rational points on \( J_1 \) over \( \mathbb{F}_{37^n} \) is given by
\[
N_n(J_1) = 37^n + 1 - \left( -5 + i\sqrt{12} \right)^n - \left( -5 - i\sqrt{12} \right)^n.
\]
In addition, the number of rational points on the curve \( J_2 : y^3 = (x+3)^2(-x^2+2x+2)^2 \) over \( \mathbb{F}_{37^n} \) is given by
\[
N_n(J_2) = 37^n - 1 - \left( -5 + i\sqrt{12} \right)^n - \left( -5 - i\sqrt{12} \right)^n.
\]

Theorem 5.3. Let \( a, b \in \mathbb{F}_q^* \). The number of rational points on \( C : y^3 = ax^3 + b \) over \( \mathbb{F}_{q^n} \) satisfies
\[
N_n(C) = q^n + 1 - \omega_q(a^{-1},0,0,(b/2a)^2)^n - \omega_q(a^{-1},0,0,(b/2a)^2)^n.
\]

Proof: We have
\[
N_n(C) = 1 + \chi_3(a) + \chi_3^2(a) + \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3(ax + b) + \chi_3^2(ax + b) \right] [1 + \chi_3(x) + \chi_3^2(x)] \\
= 1 + \chi_3(a) + \chi_3^2(a) + S_1 + S_2,
\]
where
\[
S_1 : = \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3(ax^2 + bx) + \chi_3^2(ax^2 + bx) \right] \\
= \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3 \left( a \left( z - \frac{b}{2a} \right)^2 + b \left( z - \frac{b}{2a} \right) \right) + \chi_3^2 \left( a \left( z - \frac{b}{2a} \right)^2 + b \left( z - \frac{b}{2a} \right) \right) \right] \\
= \sum_{z \in \mathbb{F}_q^n} \left[ 1 + \chi_3 \left( az^2 - \frac{b^2}{4a} \right) + \chi_3^2 \left( az^2 - \frac{b^2}{4a} \right) \right].
\]
and
\[ S_1 = \sum_{x \in \mathbb{F}_q^n} \left[ \chi_3(ax + b) + \chi_3^2(ax + b) + \chi_3^3(ax + b) \right] \]
\[ = \sum_{x \in \mathbb{F}_q^n} \left[ \frac{a}{x} + \frac{b}{x^2} \right] \]
\[ = \sum_{x \in \mathbb{F}_q^n} \left[ \chi_3(a + b) + \chi_3^2(a + b) \right] \]
\[ = -\chi_3(a) - \chi_3^2(a). \]

Since \( S_1 \) count the number of rational points in the curve with equation
\[ z^2 = \frac{y^3}{a} + \frac{b^2}{4a^2}, \]
the result follows from Lemma 3.4.

\[ \square \]

**Proof:** (proof of Theorem 1.2) We note that
\[ N_n(C) = 1 + \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3(ax^2 + b) + \chi_3^2(ax^2 + b) \right] \left[ 1 + \chi_3(x) + \chi_3^2(x) \right] \]
\[ = 1 + S_1 + S_2 + S_3, \]
where
\[ S_1 := \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3(ax^2 + b) + \chi_3^2(ax^2 + b) + \chi_3(x) + \chi_3^2(x) \right] \]
\[ = \sum_{x \in \mathbb{F}_q^n} \left[ 1 + \chi_3(ax^2 + b) + \chi_3^2(ax^2 + b) \right] \]
\[ = \sum_{w \in \mathbb{F}_q^n} \left[ 1 + \chi_2(a^{-1}w^3 - ba^{-1}) \right], \]
\[ S_2 := \sum_{x \in \mathbb{F}_q^n} \left[ \chi_3(ax^2 + b) + \chi_3^2(ax^2 + b) - \chi_3(x) - \chi_3^2(x) \right] \]
\[ = \sum_{x \in \mathbb{F}_q^n} \left[ \frac{a}{x} + \frac{b}{x^2} \right] \]
\[ = \sum_{x \in \mathbb{F}_q^n} \left[ \chi_3(a + b) + \chi_3^2(a + b) \right] \]
\[ = \sum_{w \in \mathbb{F}_q^n} \chi_2(b^{-1}w^3 - ab^{-1}) - \chi_3(a) - \chi_3^2(a) \]
and
\[ S_3 := \sum_{x \in \mathbb{F}_q^n} \left[ \chi_3(ax^2 + b) + \chi_3^2(ax^2 + b) + \chi_3(x) \right] \]
\[ = \sum_{x \in \mathbb{F}_q^n} \left[ \chi_3 \left( \frac{ax^2 + b}{x} \right) + \chi_3^2 \left( \frac{ax^2 + b}{x} \right) \right]. \]

By Lemma 3.4,
\[ S_1 = q^n - \omega_1^n - \overline{\omega}_1^n, \]
where $\omega_1 := \omega_q(a^{-1}, 0, 0, -ba^{-1})$ and

$$S_2 = -\omega_2^n - \overline{\omega_2^n} - \chi_3(a) - \chi_2^2(a),$$

where $\omega_2 := \omega_q(b^{-1}, 0, 0, -ab^{-1})$. By Remark 4.9 and Theorem 4.5,

$$S_3 = -\omega_3^n - \overline{\omega_3^n} - \omega_2^n - \overline{\omega_2^n},$$

where $\omega_3 := \omega_q(1, 0, 0, -4ab)$ and $\omega_4 := \omega_q(-4ab, 0, 0, 1)$.

Example 5.4. Let $\mathcal{J} : y^3 = x^6 + 1$ be a curve over $\mathbb{F}_{103}$. We use Lemma 3.7 as in Example 3.8 to calculate the complex numbers $\omega_i$ in Theorem 1.2. We have

$\omega_{103}(1, 0, 0, -1) = -10 + i\sqrt{3}$, $\omega_{103}(1, 0, 0, -4) = \frac{7 + i\sqrt{363}}{2}$ and $\omega_{103}(-4, 0, 0, 1) = \frac{-13 + i\sqrt{243}}{2}$.

Then, by Theorem 1.2,

$$N_n(\mathcal{J}) = 103^n - 1 - 2 \cdot \omega_1^n - 2 \cdot \overline{\omega_1^n} - \omega_2^n - \overline{\omega_2^n} - \omega_3^n - \overline{\omega_3^n},$$

where $\omega_1 := -10 + i\sqrt{3}$, $\omega_2 := \frac{7 + i\sqrt{363}}{2}$ and $\omega_3 := \frac{-13 + i\sqrt{243}}{2}$.

6. Rational Points on Curves of the Form $y^4 = f(x)$

In this section, we calculate the number of rational points on curves of the form $y^4 = ax^4 + bx^2 + c$. The case $q \equiv 3 \pmod{4}$ must be considered separately, since every square is a fourth power, as we show in the following lemma.

Lemma 6.1. Let $\mathbb{F}_q$ be a finite field with $q \equiv 3 \pmod{4}$ elements and $k$ a positive integer. An element $\alpha \in \mathbb{F}_q$ is a square if and only if it is a $2^k$ power.

Proof: Since $\gcd(2^{k-1}, \frac{q-1}{2}) = 1$, there are integers $a, b$ such that $2^{k-1} \cdot a + \frac{q-1}{2} \cdot b = 1$. Then

$$\alpha^2 = a^{2^{k-1} \cdot (q-1) \cdot b} = (\alpha^a)^{2^k}$$

for all $\alpha \in \mathbb{F}_q$. Conversely,

$$\alpha^{2^k} = \alpha^{2^{k-1}a + 2^{k-1}(q-1)b} = \left(\alpha^{2^{k-2}a} \right)^2.$$

Therefore, in the case $q \equiv 3 \pmod{4}$, the number of rational points on $\mathcal{L} : y^4 = ax^4 + bx^2 + c$ is the same as the number of rational points on $y^2 = ax^4 + bx^2 + c$ unless points at the infinity. We have already presented the number of points on $y^2 = ax^4 + bx^2 + c$ in Theorem 4.7. In order to calculate $N_n(\mathcal{L})$ for any positive integer $n$ in the case where
the $a, b, c$ are elements in a prime field, we have to calculate the number of points on these curves in the case $q \equiv 1 \pmod{4}$.

**Lemma 6.2.** Let $a, b, c \in \mathbb{F}_q$, with $a \neq 0$ and $q \equiv 1 \pmod{4}$. For $f(x) := ax^2 + bx + c$, we have

$$
\sum_{x \in \mathbb{F}_q^n} [\chi_4(f(x)) + \chi_4^3(f(x))] = \begin{cases} 
-\omega_q(a^{-1},0,d,0)^n - \omega_q(b^{-1},0,d,0)^n, & \text{if } b^2 - 4ac \neq 0; \\
0, & \text{if } b^2 - 4ac = 0,
\end{cases}
$$

where $d := \frac{b^2 - 4ac}{4a}$.

**Proof:** We observe that

$$
1 + \sum_{x \in \mathbb{F}_q^n} [1 + \chi_4(ax^2 + bx + c) + \chi_4^2(ax^2 + bx + c) + \chi_4^3(ax^2 + bx + c)]
= 1 + \sum_{(z-b/2a) \in \mathbb{F}_q^n} [1 + \chi_4(az^2 - \frac{b^2-4ac}{4a}) + \chi_4^2(az^2 - \frac{b^2-4ac}{4a}) + \chi_4^3(az^2 - \frac{b^2-4ac}{4a})]
$$

calculate the number of rational points on the curve $C : z^2 = \frac{y^2}{a} + \frac{b^2-4ac}{4a^2}$. Therefore, letting $L := \sum_{x \in \mathbb{F}_q^n} [\chi_4(f(x)) + \chi_4^3(f(x))]$, by Theorem 4.7, we have

$$
L = -\sum_{x \in \mathbb{F}_q^n} \chi_4^2(ax^2 + bx + c) + \begin{cases} 
-\omega_q(a^{-1},0,d,0)^n - \omega_q(b^{-1},0,d,0)^n - \chi_2(a), & \text{if } b^2 - 4ac \neq 0; \\
(q^n - 1)\chi_2(a), & \text{if } b^2 - 4ac = 0,
\end{cases}
$$

where $d := \frac{b^2 - 4ac}{4a}$. The result follows by Lemma 3.1. 

**Proof:** (proof of Theorem 1.4) We have

$$
N_n(C) = \delta + \sum_{x \in \mathbb{F}_q^n} [1 + \chi_4(ax^2 + bx + c) + \chi_4^2(ax^2 + bx + c) + \chi_4^3(ax^2 + bx + c)] [1 + \chi_4^3(x)]
= \delta + S_1 + S_2,
$$

where $\delta := 1 + \chi_4(a) + \chi_4^3(a) + \chi_4(a)$.

$$
S_1 := \sum_{x \in \mathbb{F}_q^n} 1 + \chi_4(ax^2 + bx + c) + \chi_4^2(ax^2 + bx + c) + \chi_4^3(ax^2 + bx + c)
$$

and

$$
S_2 := \sum_{x \in \mathbb{F}_q^n} [1 + \chi_4(ax^2 + bx + c) + \chi_4^2(ax^2 + bx + c) + \chi_4^3(ax^2 + bx + c)] \chi_4^2(x).
$$

By Remark 4.1,

$$
S_2 = \sum_{x \in \mathbb{F}_q^n} \left[ \chi_4^2(x) + \chi_4 \left( \frac{ax^2 + bx + c}{x^2} \right) + \chi_4^2(\frac{ax^3 + bx^2 + cx}{x^2}) + \chi_4^3(\frac{ax^2 + bx + c}{x^2}) \right]
= \sum_{x \in \mathbb{F}_q^n} \chi_4^2(ax^3 + bx^2 + cx) + \sum_{x \in \mathbb{F}_q^n} [\chi_4(a + bz + cz^2) + \chi_4^3(a + bz + cz^2)].
$$
Using Lemma 3.1 and Lemma 6.2 in \( S_1 \) and Lemma 3.2 (in the case where \( c = 0 \)), Lemma 3.4 and Lemma 6.2 in \( S_2 \), the result follows.

\[ \square \]

**Example 6.3.** Let \( J : y^4 = x^4 + 4x^2 - 1 \) be a curve over \( \mathbb{F}_{41} \). We use Lemma 3.7 as in Example 3.8 to calculate the complex numbers \( \omega_i \) in Theorem 1.4. We have

\[
\omega_{41}(1, 0, 5, 0) = \omega_{41}(-1, 0, 5, 0) = \omega_{41}(1, 4, -1, 0) = -5 + 4i.
\]

Then, by Theorem 1.4, the number of rational points on \( J \) over \( \mathbb{F}_{41^n} \) is given by

\[
N_n(J) = 41^n + 1 - 3 \cdot (-5 + 4i)^n - 3 \cdot (-5 - 4i)^n.
\]

In the following result, we use that the number of rational points on \( \mathcal{L} : y^4 = ax^4 + bx^2 + c \) is essentially the number of points on \( \mathcal{L}' : y^2 = ax^4 + bx^2 + c \), as we have seen in Lemma 6.1.

**Corollary 6.4.** For \( a, b, c \in \mathbb{F}_p \), where \( p \equiv 3 \pmod{4} \) is a prime number and \( a \neq 0 \). The number of rational points on the curve \( \mathcal{C} : y^4 = ax^4 + bx^2 + c \) over \( \mathbb{F}_{p^n} \) satisfies

\[
N_n(\mathcal{C}) = \begin{cases} 
\rho^n + 1 - 2(i\sqrt{p})^n - 2(-i\sqrt{p})^n - \omega^n - \overline{\omega}^n, & \text{if } b^2 - 4ac \neq 0 \text{ and } c \neq 0; \\
\rho^n + 1 - (i\sqrt{p})^n - (-i\sqrt{p})^n - \chi_2(b), & \text{if } b^2 - 4ac \neq 0 \text{ and } c = 0; \\
\rho^n + 1 - \chi_2(-b/2) + p^n \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c \neq 0; \\
\rho^n + 1 - \chi_2(b) + p^n \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c = 0,
\end{cases}
\]

where \( \omega := \omega_p(a, b, c, 0) \).

**Proof:** By Theorem 1.4 and Remark 2.4,

\[
N_{2n}(\mathcal{C}) = \begin{cases} 
p^{2n} + 1 - \omega_1^{2n} - \overline{\omega_1}^{2n} - \omega_2^{2n} - \overline{\omega_2}^{2n} - \omega_3^{2n} - \overline{\omega_3}^{2n}, & \text{if } b^2 - 4ac \neq 0 \text{ and } c \neq 0; \\
p^{2n} + 1 - \omega_1^{2n} - \overline{\omega_1}^{2n} - \chi_2(b), & \text{if } b^2 - 4ac \neq 0 \text{ and } c = 0; \\
p^{2n} + 1 - \chi_2(-b/2) + p^{2n} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c \neq 0; \\
p^{2n} + 1 - \chi_2(b) + p^{2n} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0 \text{ and } c = 0,
\end{cases}
\]

where \( \omega_1 := \omega_p(a^{-1}, 0, d_1, 0), \omega_2 := \omega_p(c^{-1}, 0, d_2, 0), \omega_3 := \omega_p(a, b, c, 0) \). Lemma 3.7 states that

\[
\omega_1 + \overline{\omega_1} \equiv \omega_2 + \overline{\omega_2} \equiv 0 \pmod{p}.
\]

Since \( |\omega_1 + \overline{\omega_1}| \leq 2\sqrt{p} \) and \( |\omega_2 + \overline{\omega_2}| \leq 2\sqrt{p} \), we must have

\[
\omega_1 = \omega_2 = 0
\]

for \( p > 4 \). A straightforward calculation shows that \( \omega_3(a^{-1}, 0, d_1, 0) = \omega_3(c^{-1}, 0, d_2, 0) = 0 \). In addition, since there are \( 1 + \chi_2(a) \) points at the infinity on \( \mathcal{C} \) (by Lemma 6.1, each
element \(a \in \mathbb{F}_p\) has exactly 0 or 2 fourth roots), by Theorem 4.7, we have

\[
N_{2n-1}(C) = \begin{cases} 
  p^{2n-1} + 1 - \omega_3^{2n-1} - \overline{\omega}_3^{2n-1}, & \text{if } b^2 - 4ac \neq 0, \text{ with } c \neq 0; \\
  p^{2n-1} + 1 - \chi_2(b), & \text{if } b^2 - 4ac \neq 0, \text{ with } c = 0; \\
  p^{2n-1} + 1 - \chi_2(-b/2) + p^{2n-1} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c \neq 0; \\
  p^{2n-1} + 1 + p^{2n-1} \cdot \chi_2(a), & \text{if } b^2 - 4ac = 0, \text{ with } c = 0
\end{cases}
\]

for all positive integer \(n\). The result follows by gathering the expressions for \(N_{2n}\) and \(N_{2n-1}\). \(\square\)

7. Maximal and Minimal Curves

Let \(\mathbb{F}_{q^2}\) be a fields with \(q^2\) elements. Let \(C\) be a projective, geometrically irreducible and non-singular algebraic curve defined over \(\mathbb{F}_{q^2}\). The curve \(C\) is called maximal over \(\mathbb{F}_{q^2}\) if it attains the Hasse-Weil upper bound, that is,

\[
N_1(C) = q^2 + 1 + 2gq,
\]

where \(g\) is the genus of \(C\). Similarly, a curve is called minimal over \(\mathbb{F}_{q^2}\) if it attains the Hasse-Weil lower bound. Many researchers have studied maximal and minimal curves, e.g. see [5, 8, 12, 24]. In this section, we use the theorems presented in the previous sections in order to produce families of maximal and minimal curves. We will consider the curves with equation

\[
ax^n + by^n + cz^n = 0
\]

in the cases \(n = 3\) and \(n = 4\), where \(a, b, c\) are elements in a prime field. The special case where \(a = b = c = 1\), that is, the projective curves with equation

\[
x^n + y^n + z^n = 0,
\]

are well-known as Fermat curves. A general criteria to decide when a Fermat curve \(C : x^n + y^n + z^n = 0\) is maximal or minimal was presented by Garcia and Tafazolian [7]. A shorter proof for the same result was presented by Tafazolian [23].

**Lemma 7.1** ([16], Lucas’s Theorem). For non-negative integers \(m\) and \(n\) and a prime \(p\), the following holds:

\[
\binom{n}{m} \equiv \left( \binom{n_0}{m_0} \right) \left( \binom{n_1}{m_1} \right) \cdots \left( \binom{n_k}{m_k} \right) \pmod{p},
\]

where \(\binom{m}{m_i} := 0\) if \(m_i > n_i\) and \(m = m_k p^k + \cdots + m_1 p + m_0, n = n_k p^k + \cdots + n_1 p + n_0\) are the base \(p\) expansions of \(m\) and \(n\).
Theorem 7.2. Let \( a, b, c \) be non-null elements in a prime field \( \mathbb{F}_p \), where \( p \neq 3 \). Let \( C \) be the projective non-singular curve of genus 1 given by equation \( ax^3 + by^3 + cz^3 = 0 \). Then

i) \( C \) is maximal over \( \mathbb{F}_{p^{2n}} \) if and only if \( 3 \) divides \( p^n + 1 \);

ii) \( C \) is minimal over \( \mathbb{F}_{p^{2n}} \) if and only if \( 3 \) divides \( p^n - 1 \) and \( p \equiv 2 \pmod{3} \).

Proof: We note that the \( C \) has the same number of rational points as the affine curve \( C' \) given by equation \( y^3 = -\frac{a}{b} x^3 - \frac{c}{b} \). Since \( C' \) has genus 1, the number of rational points on \( C' \) is given by

\[
N_n(C') = p^n + 1 - \omega^n - \overline{\omega}^n,
\]

for a complex number \( \omega \), where \( |\omega| = \sqrt{p} \). In the case \( p \equiv 2 \pmod{3} \), since \( y \mapsto y^3 \) permutes the elements of \( \mathbb{F}_p \), we have \( N_1(C') = p + 1 \) and then \( \omega = i\sqrt{p} \). Hence, the result is proved in this case. For \( p \equiv 1 \pmod{3} \), Theorem 5.3 and Lemma 3.7 show that

\[
N_n(C') \equiv 1 - \left( \frac{p^{n-1}}{2} \right) \left( \frac{-b}{a} \right) \left( \frac{c^2}{4a^2} \right) \left( \frac{p^n-1}{4} \right) \pmod{p}.
\]

By Lemma 7.1, we must have

\[
\left( \frac{p^{n-1}}{2} \right) \left( \frac{p^n-1}{3} \right) \equiv \left( \frac{p-1}{2} \frac{p^n-1}{3} \right) \not\equiv 0 \pmod{p}.
\]

Thus \( N_n(C') \neq p^n + 1 \) and then \( \omega \neq i\sqrt{p^3} \). Hence, the result is shown. \( \square \)

Theorem 7.3. Let \( a, b, c \) be non-null elements in a prime field \( \mathbb{F}_p \). Let \( C \) be the projective non-singular curve of genus 3 given by equation \( ax^4 + by^4 + cz^4 = 0 \). Then

i) \( C \) is maximal over \( \mathbb{F}_{p^{2n}} \) if and only if \( 4 \) divides \( p^n + 1 \);

ii) \( C \) is minimal over \( \mathbb{F}_{p^{2n}} \) if and only if \( 4 \) divides \( p^n - 1 \) and \( p \equiv 3 \pmod{4} \).

Proof: Since the projective curve with equation \( ax^4 + by^4 + cz^4 = 0 \) has the same number of rational points as the affine curve given by equation \( y^4 = -\frac{a}{b} x^4 - \frac{c}{b} \), the result follows from Corollary 6.4 and Lemma 3.7 for the case \( p \equiv 3 \pmod{4} \). For the case \( p \equiv 1 \pmod{4} \), Lemma 3.7 states that

\[
\omega_{p^n}(-a/b, 0, -c/b, 0) \equiv \left( \frac{p^{n-1}}{2} \right) \left( \frac{-b}{a} \right) \left( \frac{c^2}{4a^2} \right) \left( \frac{p^n-1}{4} \right) \pmod{p}.
\]

Since

\[
\left( \frac{p^{n-1}}{2} \right) \left( \frac{p^n-1}{4} \right) \equiv \left( \frac{p-1}{2} \frac{p^n-1}{4} \right) \not\equiv 0 \pmod{p}
\]

by Lemma 7.1, the result follows from Theorem 1.4. \( \square \)
The results proved in 7.3 and 7.2 generalize the result of Tafazolian [23] for Fermat curves of degree 3 and 4.

**Conjecture 7.4.** The prime number $p$ in Theorems 7.3 and 7.2 can be replaced by a power of a prime.

From the results presented in this section, it emerge the following question.

**Question 7.5.** Are the conditions for the maximality and minimality of the curve $ax^n + by^n + cz^n = 0$ the same as the conditions for the Fermat curve $x^n + y^n + z^n = 0$ presented in [23] for all positive integer $n$?

In the same way of the proofs of Theorems 7.2 and 7.3, it is possible give conditions for which the singular curves presented in this paper are optimal. But, none of the singular curves presented here attains the upper bound

$$q^n + 1 + 2g\sqrt{q} + \pi - g$$

in Theorem 1.1.

8. Acknowledgments

I am grateful to Fabio Enrique Brochero Martínez for his useful comments. This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

References

[1] Y. Aubry and M. Perret, *A weil theorem for singular curves*, (1996).
[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Wiley New York, 1998.
[3] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman and Hall/CRC, 2005.
[4] A. Cossidente, J. Hirschfeld, G. Korchmáros, and F. Torres, *On plane maximal curves*, Compositio Mathematica, 121 (2000), pp. 163–181.
[5] R. Fuhrmann, A. Garcia, and F. Torres, *On maximal curves*, Journal of number theory, 67 (1997), pp. 29–51.
[6] A. Garcia, *On curves with many rational points over finite fields*, in Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, 2002, pp. 152–163.
[7] A. Garcia and S. Tafazolian, *Cartier operators and maximal curves*, Acta Arith, 135 (2008), pp. 199–218.
[8] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Mathematica Annalen, 343 (2009), p. 229.
[9] J. Hirschfeld, G. Korchmáros, et al., *On the number of rational points on an algebraic curve over a finite field*, Bulletin of the Belgian Mathematical Society-Simon Stevin, 5 (1998), pp. 313–340.
[10] J. W. P. Hirschfeld, G. Korchmáros, F. Torres, and F. E. T. Orihuela, *Algebraic curves over a finite field*, Princeton University Press, 2008.
[11] S. Hu, S. Hong, and W. Zhao, *The number of rational points of a family of hypersurfaces over finite fields*, Journal of Number Theory, 156 (2015), pp. 135–153.

[12] A. Kazemifard, A. R. Naghipour, and S. Tafazolian, *A note on superspecial and maximal curves*, Bulletin of the Iranian Mathematical Society, 39 (2013), pp. 405–413.

[13] D. B. Leep and C. C. Yeomans, *The number of points on a singular curve over a finite field*, Archiv der Mathematik, 63 (1994), pp. 420–426.

[14] R. Lercier and F. Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, in International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1995, pp. 79–94.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20, Cambridge University Press, 1997.

[16] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics, (1878), pp. 289–321.

[17] C. Moreno, *Algebraic Curves over Finite Fields*, no. 97, Cambridge University Press, 1993.

[18] K. Nelson, J. Solymosi, F. Tom, and C. Wong, *The number of rational points of hyperelliptic curves over subsets of finite fields*, Involve, a Journal of Mathematics, 12 (2019), pp. 755–765.

[19] A. Rojas-León, *On the number of rational points on curves over finite fields with many automorphisms*, Finite Fields and Their Applications, 19 (2013), pp. 1–15.

[20] R. Schoof, *Counting points on elliptic curves over finite fields*, Journal de théorie des nombres de Bordeaux, 7 (1995), pp. 219–254.

[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106, Springer Science & Business Media, 2009.

[22] Z.-H. Sun, *Congruences concerning legendre polynomials ii*, Journal of Number Theory, 133 (2013), pp. 1950–1976.

[23] S. Tafazolian, *A characterization of maximal and minimal fermat curves*, Finite Fields and Their Applications, 16 (2010), pp. 1–3.

[24] S. Tafazolian and F. Torres, *A note on certain maximal curves*, Communications in Algebra, 45 (2017), pp. 764–773.

[25] M. Ulas, *Rational points on certain hyperelliptic curves over finite fields*, Bulletin of the Polish Academy of Sciences Mathematics, 55 (2007), pp. 97–104.

[26] K. S. Williams, *Evaluation of character sums connected with elliptic curves*, Proceedings of the American Mathematical Society, 73 (1979), pp. 291–299.

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 31270-901, Brazil,

E-mail address: jose-alvesoliveira@hotmail.com