UNIVERSIDADE FEDERAL DO ABC
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Leandro Albino Mosca Rodrigues

Frobenius não classicalidade de algumas famílias de curvas de Fermat generalizadas

Santo André, 2024

Universidade Federal do ABC

Centro de Matemática, Computação e Cognição

Leandro Albino Mosca Rodrigues

Frobenius não classicalidade de algumas famílias de curvas de Fermat generalizadas

Orientador: Prof. Dr. Nazar Arakelian

Tese de doutorado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Doutor em Matemática

Este exemplar corresponde à versão final da tese
defendida pelo aluno Leandro Albino Mosca Rodrigues,
e orientada pelo Prof. Dr. Nazar Arakelian.

Santo André, 2024

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Albino Mosca Rodrigues, Leandro
Frobenius não classicalidade de algumas famílias de curvas de Fermat generalizadas / Leandro Albino Mosca Rodrigues. — 2024.

84 fls.

Orientação de: Nazar Arakelian

Tese (Doutorado) — Universidade Federal do ABC, Programa de Pós Graduação em Matemática, Santo André, 2024.

1. Curvas Algébricas. 2. Frobenius Classicalidade. 3. Stöhr-Voloch. 4. Pontos Racionais. I. Arakelian, Nazar. II. Programa de Pós-Graduação em Matemática, 2024. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca examinadora no dia da defesa, sob responsabilidade única do(a) autor(a) e com a anuência do(a) (co)orientador(a)

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Avenida dos Estados, 5001 - Bairro Santa Terezinha - Santo André - SP
CEP 09210-580 · Fone: (11) 4996-0017

Ata de Defesa de Tese de Doutorado e Folha de Assinaturas

No dia 20 de Junho de 2024 às 10:00, no local: meet.google.com/cwq-jhjg-ngp, realizou-se a Defesa da Tese de Doutorado, que constou da apresentação do trabalho intitulado **"Frobenius não classicalidade de algumas famílias de curvas de Fermat generalizadas"** de autoria do candidato, **LEANDRO ALBINO MOSCA RODRIGUES**, RA nº 23202010165, discente do Programa de Pós-Graduação em MATEMÁTICA da UFABC, sob orientação do Profº NAZAR ARAKELIAN. Concluídos os trabalhos de apresentação e arguição, o candidato foi considerado aprovado pela Banca Examinadora.

E, para constar, foi lavrada a presente ata e folha de assinaturas assinada pelos membros da Banca.

gov.br Documento assinado digitalmente
NAZAR ARAKELIAN
Data: 21/06/2024 12:07:41-0300
Verifique em https://validar.iti.gov.br

Dr. NAZAR ARAKELIAN, UFABC
Presidente - Interno ao Programa

gov.br Documento assinado digitalmente
CICERO FERNANDES DE CARVALHO
Data: 20/06/2024 14:45:02-0300
Verifique em https://validar.iti.gov.br

Dr. CÍCERO FERNANDES DE CARVALHO, UFU
Membro Titular - Examinador(a) Externo à Instituição

gov.br Documento assinado digitalmente
GREGORY DURAN CUNHA
Data: 20/06/2024 13:21:41-0300
Verifique em https://validar.iti.gov.br

Dr. GREGORY DURAN CUNHA, UFG
Membro Titular - Examinador(a) Externo à Instituição

gov.br Documento assinado digitalmente
HERIVELTO MARTINS BORGES FILHO
Data: 21/06/2024 08:12:18-0300
Verifique em https://validar.iti.gov.br

Dr. HERIVELTO MARTINS BORGES FILHO, USP
Membro Titular - Examinador(a) Externo à Instituição

Documento assinado digitalmente
gov.br
PIETRO SPEZIALI
Data: 20/06/2024 12:55:03-0300
Verifique em https://validar.iti.gov.br

Dr. PIETRO SPEZIALI, UNICAMP
Membro Titular - Examinador(a) Externo à Instituição

Dr. WANDERSON TENÓRIO, UFMT
Membro Suplente - Examinador(a) Externo à Instituição

Dr. MATHEUS BERNARDINI DE SOUZA, UNB
Membro Suplente - Examinador(a) Externo à Instituição

"O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001"

DEDICATÓRIA

Dedico essa tese a todos os professores que resolveram dedicar sua vida a ensinar e acreditar em um futuro melhor pra esse país.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais: os valores e ensinamentos aprendidos desde criança me ajudaram a trilhar esse caminho e concluir mais uma fase da minha vida.

Obrigado ao meu cachorro Manhoso, ao meu gato Miu e a minha gata negra que passaram longas tardes dentro do quarto comigo enquanto eu ficava sentado em frente ao computador.

Não posso deixar de agradecer ao meu orientador Nazar, que me acompanhou nesse processo complicado e iniciado em meio a uma pandemia. Mesmo nas condições que eram disponíveis ele nunca desistiu de mim.

Queria agradecer às sessões de terapia com a Dani, que me ajudaram e superar uma parte bem complicada desse processo.

Emanoel, Gabriela e Oertes obrigado por terem iniciado essa jornada junto comigo e pelas caronas no nosso único mês de aula presencial.

Também queria agradecer aos demais colegas que cursaram disciplina comigo de modo virtual. Em especial Tiago, Wanessa e Maria Clara.

Queria agradecer ainda ao João Paulo, um amigo que nunca vi pessoalmente, mas sempre me auxiliou nas enormes e muitas dúvidas que apareceram.

Somente aqueles que sofreram por muito tempo conseguem ver luz através das sombras.
(Roronoa Zoro)

RESUMO

Neste trabalho determinamos condições necessárias e suficientes para que algumas famílias de curvas algébricas planas de Fermat generalizadas estudadas por [4] sejam Frobenius não clássicas em relação ao sistema linear de retas e ao sistema linear de cônicas. Tendo como base abordagens desenvolvidas em trabalhos posteriores ao surgimento da teoria de Stöhr-Voloch, usamos métodos que podem facilmente ser realizados sem a necessidade de recursos computacionais.

Palavras-chave: Stöhr-Voloch, Curvas Algébricas, Frobenius Classicalidade

ABSTRACT

In this paper we give necessary and sufficient conditions for some families of generalized Fermat algebraic plane curves introduced in [4] to be Frobenius non-classical with respect to the linear system of lines and the linear system of conics. Based on approaches developed in papers after the emergence of the Stöhr-Voloch theory, we use methods that can easily be performed without the need for computational resources.

Keywords: Stöhr-Voloch, Algebraic Curves, Frobenius Classicality

CONTEÚDO

INTRODUÇÃO

Considere $\mathbb{F}_q$ um corpo finito com $q = p^h$ elementos e $\mathcal{F}$ uma curva algébrica irredutível de gênero g e grau n definida sobre $\mathbb{F}_q$ com $N(\mathcal{F})$ pontos racionais. Em [17, Theorem 5.2.3] temos que:

$$|N(\mathcal{F}) - (q-1)| \leq 2gq^{\frac{1}{2}}. \tag{1}$$

No caso em que $\mathcal{F}$ é uma curva algébrica plana não-singular de grau n, (1) pode ser rescrita como:

$$|N(\mathcal{F}) - (q-1)| \leq (n-1)(n-2)q^{\frac{1}{2}}. \tag{2}$$

A expressão (1) é comunente chamada de cota de Hasse-Weil e, desde o seu surgimento, muitos matemáticos vêm descobrindo novas maneiras para aprimorá-la quando possível. Podemos citar os trabalhos de Serre, Stark e Ihara dentro deste campo [15, 16, 17].

É justificável tais esforços em determinar cotas cada vez melhores para $N(\mathcal{F})$, pois podemos encontrar algumas aplicações envolvendo a quantidade de pontos racionais de uma curva algébrica em outras áreas, tais como o problema de Waring sobre corpos finitos [9], somas exponenciais [7], entre outros.

Em 1985, Stöhr e Voloch [18] introduziram o conceito de curvas Frobenius não-clássicas que não só corroboram os resultados obtidos por Hasse-Weil, Serre e Stark, mas abrem novos caminhos para melhorar a cota (1).

Dado um inteiro $s \in \{1, \ldots, n-1\}$ considere $\sum_s$ o sistema linear das curvas de grau s em $\mathbb{P}^2(\overline{\mathbb{F}}_q)$. Considerando $M = \binom{s+2}{2} - 1$, é demonstrado em [18, Proposition 2.1] que existe uma sequência de inteiros $0 = \nu_0 < \ldots < \nu_{M-1}$ chamada de sequência de $\mathbb{F}_q$-Frobenius de ordem de $\mathcal{F}$ em relação à $\sum_s$. No caso em que $\nu_i = i$, $i = 0, 1, \ldots, M-1$. a curva é dita $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_s$, caso contrário é chamada de $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_s$.

Nas condições de [18, Theorem 2.13] temos o Teorema de Stöhr-Voloch:

$$N(\mathcal{F}) \leq ((\nu_1 + \ldots + \nu_{M-1})(2g-2) + (q+M)d)/M \tag{3}$$

Observe que no caso em que $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_s$, (3) pode ser rescrita como:

$$N(\mathcal{F}) \leq (M(M-1)(g-1) + (q+M)d)/M$$

Há muitas outras variações equivalentes para escrevermos o Teorema de Stöhr-Voloch que podem ser usadas dependendo da abordagem que iremos usar [3, 5, 9].

Um refinamento da cota, dado por [6, Theorem 2.2] com base em [18] é:

$$N(\mathcal{F}) \leq \frac{(\nu_1 + \cdots + \nu_{M-1})(2g-2) + (q+M)d - \sum A(Q)}{M}, \tag{4}$$

sendo

$$A(Q) = \begin{cases} \sum_{i=1}^{M}(j_i(Q) - \nu_{i-1}) - M, \text{ para } Q \in \mathcal{F}(\mathbb{F}_q) \\ \sum_{i=0}^{M-1}(j_i(Q) - \nu_i), \text{ nos demais casos.} \end{cases}$$

De acordo com [11] determinar quando uma curva é não clássica pode ser um trabalho difícil, por isso muitos matemáticos têm buscado condições para determinar quando uma certa família de curvas é clássica [2, 3, 5, 8, 9]. Ao caracterizar tais curvas, temos uma outra família de curvas que seriam então as curvas Frobenius não clássicas. Essa classificação nos permite obter um resultado que serve a dois própositos importantes como é explicado por [3, 5]. As curvas $\mathbb{F}_q$-Frobenius clássicas são aquelas que possuem uma melhor cota para a quantidade de pontos racionais. Por outro lado, as curvas $\mathbb{F}_q$-Frobenius não clássicas são aquelas para as quais potencialmente existem muitos pontos racionais.

Considerando a curva de Fermat $\mathcal{F} : ax^n + by^n = 1$, em [9, Theorem 2, Theorem 3] temos um estudo sobre as condições para as quais essa curva é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_1$ e à $\sum_2$. Em [3, Theorem 1.2] temos as condições para os quais essa curva é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_3$. É importante ainda mencionar que em [3, Appendix B] é demonstrado um caso omitido por [9] considerando $\sum_2$.

Tomando como base as generalizações das curvas de Fermat sobre corpos finitos feitas por [4, Theorem 5.1], neste trabalho iremos estudar as condições para as quais as curvas $ax^n + by^m = 1$, $a, b \in \mathbb{F}_q^*$, m, n inteiros positivos e $ax^n y^m + bx^n + cy^m = 1$, $a, b, c \in \mathbb{F}_q$, $c \neq -\frac{a}{b}$, $a \neq 0$, m, n inteiros positivos são $\mathbb{F}_q$-Frobenius não clássicas em relação à $\sum_1$ e à $\sum_2$.

Inicialmente, no capítulo 1, enunciaremos os conceitos necessários para que tenhamos todos os pré-requisitos para realizar as demontrações. Grande parte deste capítulo estará baseado no artigo de Stöhr-Voloch [18] e na classificação das curvas planas de Fermat $\mathbb{F}_q$-Frobenius não clássicas em relação à $\sum_1$ e $\sum_2$ feitas por [3, 8, 9, 10, 14].

No capítulo 2 faremos um estudo completo sobre a curva $ax^n + by^m = 1$, $a, b \in \mathbb{F}_q^*$, $m, n \in \mathbb{Z}_+^*$ determinando condições para que a mesma seja $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_1$ ou $\sum_2$. Neste capítulo ainda determinamos a quantidade de pontos $\mathbb{F}_q$-racionais

para os casos da $\mathbb{F}_q$-Frobenius não classicalidade. Obtemos ainda uma cota melhor para os casos em que $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius clássica.

No capítulo 3 faremos um estudo completo sobre a curva $ax^n y^m + bx^n + cy^m = 1$, $a, b, c \in \mathbb{F}_q$, $c \neq -\frac{a}{b}$, $a \neq 0$ e $m, n \in \mathbb{Z}_+^*$ determinando condições para que a mesma seja $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_1$ ou $\sum_2$. Neste capítulo também determinamos a quantidade de pontos $\mathbb{F}_q$-racionais para o os casos de $\mathbb{F}_q$-Frobenius não classicalidade. Obtemos ainda uma cota melhor para os casos em que $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius clássica.

Ao longo deste trabalho usaremos as seguintes notações:

- $\mathbb{F}_q$ é o corpo finito de $q = p^h$ elementos, sendo $h \geq 1$, p primo (característica do corpo $\mathbb{F}_q$);
- $\overline{\mathbb{F}}_q$ é o fecho algébrico de $\mathbb{F}_q$;
- $N(\mathcal{F})$ é quantidade de pontos $\mathbb{F}_q$-racionais da curva $\mathcal{F}$;
- $\mathbb{H}(\mathcal{F})$ é o corpo de funções de $\mathcal{F}$ sobre $\mathbb{H}$, sendo $\mathcal{F}$ uma curva irredutível sobre $\mathbb{F}_q$ e $\mathbb{H}$ uma extensão algébrica de $\mathbb{F}_q$;
- $\sum_s$ é o sistema linear de todas as curvas de grau s em $\mathbb{P}^2(\overline{\mathbb{F}}_q)$;
- v_P é a valoração discreta em P para um ponto não singular $P \in \mathcal{F}$;
- $I(P, C \cap D)$ é a multiplicidade de intersecção das curvas planas C e D em um ponto P;
- $D_t^{(r)} f$ é a r-ésima derivada de Hasse de $f \in \overline{\mathbb{F}}_q(\mathcal{F})$ em relação à variável separante t de $\overline{\mathbb{F}}_q(\mathcal{F})$;
- $A_{\mathbb{K}}^n$ é o espaço afim de dimensão n sobre um corpo algebricamente fechado $\mathbb{K}$;
- $\mathbb{P}^n(\mathbb{K})$ é o espaço projetivo de dimensão n sobre um corpo algebricamente fechado $\mathbb{K}$.

1 PRELIMINARES

Neste capítulo iremos relembrar alguns conceitos básicos de curvas algébricas planas, faremos um apanhado geral sobre a teoria de Stöhr-Voloch e os principais resultados sobre a $\mathbb{F}_q$-classicalidade e $\mathbb{F}_q$-Frobenius classicalidade de uma curva algébrica plana de Fermat em relação ao sistema linear de retas e em relação ao sistema linear de cônicas.

1.1 CURVAS ALGÉBRICAS PLANAS

A maior parte dos resultados desta seção estão baseados em [11], [12] e [19]. As demonstrações aqui serão omitidas, visto que podem não só serem encontradas nas referências citadas, bem como na maioria de outros materiais deste assunto.

Sendo $\mathbb{K}$ um corpo algebricamente fechado e $f \in \mathbb{K}[x,y]$ um polinômio não constante, uma **curva algébrica plana afim** é o conjunto dado por:

$$\mathcal{F} = V(f) = \{(x,y) \in A^2_{\mathbb{K}} \mid f(x,y) = 0\}.$$

Dizemos que o **grau** da curva $\mathcal{F}$ é o grau do polinômio f, indicado por $deg(\mathcal{F})$.

As *componentes irredutíveis* da curva $\mathcal{F} = V(f)$ são $V(f_1), \ldots, V(f_r)$ tais que $f = f_1^{m_1} \cdot \ldots \cdot f_r^{m_r}$ é a decomposição de f em fatores irredutíveis ($f_i \in \mathbb{K}[x,y]$ e $m_i \in \mathbb{Z}_+$). No caso particular em que f é irredutível dizemos que a curva é **irredutível**.

Sejam $\mathcal{F}$ uma curva plana afim de grau n e $\ell : ax + by + c = 0$ uma reta contendo o ponto $P = (x_0, y_0) \in \mathcal{F}$. Temos que para algum $t \in \mathbb{K}$:

$$f(x_0 + bt, y_0 - at) = g(t) = g_0 + g_1 t + \ldots + g_n t^n = g_m t^m + \ldots + g_n t^n. \tag{5}$$

tal que $g_m \neq 0$ e $g_n \neq 0$.

Sendo ℓ uma reta que não é componente de $\mathcal{F}$, o inteiro m de (5) é a **multiplicidade de intersecção de ℓ e $\mathcal{F}$ em P** e é indicada por $I(P, \ell \cap \mathcal{F})$.

Dado ainda um ponto $P \in \mathcal{F}$, definimos a **multiplicidade de $\mathcal{F}$ em P** por:

$$m_P(\mathcal{F}) = min\{(I(P, \ell \cap \mathcal{F})\}, \forall \ell \text{ tal que } P \in \ell. \tag{6}$$

No caso em que $m_P(\mathcal{F}) = 1$ dizemos que P é um **ponto simples** ou um **ponto não singular**, caso contrário dizemos que P é um **ponto múltiplo** ou um **ponto singular**.

Uma curva é dita **não singular** se possui apenas pontos não singulares, caso contrário é chamada de **singular**.

Dizemos ainda que uma reta ℓ é **tangente a** $\mathcal{F}$ **em** P quando $I(P, \ell \cap \mathcal{F}) > m_P(\mathcal{F})$. Sendo P um ponto não singular de $\mathcal{F}$ e ℓ_P a reta tangente à $\mathcal{F}$ por P, se P é um ponto de inflexão então $I(P, \ell_P \cap \mathcal{F}) \geq 3$.

Sendo $f \in \mathbb{K}[x, y]$ um polinômio não constante de grau n, associamos o polinômio homogêneo dado por $F(X, Y, Z) = Z^n f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$. Analogamente para todo polinômio homogêneo $F(X, Y, Z)$ associamos o polinômio $f \in \mathbb{K}[x, y]$ dado por $F(x, y, 1) = f(x, y)$.

Sendo $F(X, Y, Z) \in \mathbb{K}[X, Y, Z]$ um polinômio homogêneo não constante, uma **curva algébrica plana projetiva** é o conjunto dado por:

$$\mathcal{F} = V(F) = \{(X_0 : Y_0 : Z_0) \in \mathbb{P}^2(\mathbb{K}) \mid F(X_0, Y_0, Z_0) = 0\}.$$

Dizemos que um ponto no infinito é um ponto da forma $P_\infty = (X : Y : 0)$, e assim podemos dizer que uma curva algébrica plana projetiva é o união do conjunto dos pontos afins com os pontos no infinitos pertecentes a esta curva.

As definições já feitas para o caso afim se estendem de modo natural ao caso projetivo.

Como iremos tratar apenas de curvas planas neste trabalho, para simplificar a linguagem, muitas vezes usaremos apenas o termo curva ao invés de curva algébrica plana afim. Analogamente charemos a curva algébrica plana projetiva simplesmente de curva projetiva.

Iremos ainda, por abuso de linguagem, nos referir a uma curva $\mathcal{F}$ definida pelo polinômio f por $\mathcal{F} : f = 0$.

Teorema 1.1.1. *(Bézout) Dadas as curvas planas projetivas $\mathcal{F}$ e $\mathcal{G}$ sem componentes em comum, temos que*

$$\sum_{P \in \mathcal{F} \cap \mathcal{G}} I(P, \mathcal{F} \cap \mathcal{G}) = deg(\mathcal{F}) \cdot deg(\mathcal{G}).$$

Considerando $F_{x_i x_j} = \frac{\partial^2 F}{\partial F_{x_i} \partial F_{x_j}}$, se o determinante

$$H(X, Y, Z) = \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{vmatrix}$$

é não nulo, então a curva projetiva dada por $\mathcal{H} : H(X,Y,Z) = 0$ é a **curva Hessiana** de $\mathcal{F}$.

Teorema 1.1.2. *Se $n \equiv 1(mod p)$, então a curva Hessiana é nula.*

Teorema 1.1.3. *Supondo que $\mathcal{H}$ é não nula.*

- *Seja $p \neq 2$. Um ponto não singular de $\mathcal{F}$ é de inflexão se, e somente se, é um ponto comum de $\mathcal{F}$ e $\mathcal{H}$.*
- *Todo ponto singular de $\mathcal{F}$ pertence a $\mathcal{H}$.*

1.2 TEORIA DE STÖHR-VOLOCH

Nesta seção iremos resumir alguns resultados que são explanados em [3], [9] e [18]. Assim como na seção anterior, não iremos realizar as demonstrações, visto que as mesmas podem ser encontradas detalhadamente nas referências citadas.

Dada uma curva projetiva irredutível e não singular $\mathcal{F} : f = 0$ de grau n sobre $\mathbb{F}_q$, considere o sistema linear $\sum_s$ de todas as curvas projetivas de grau s, tal que $s \in \{1, \ldots, n-1\}$.

Sendo $P \in \mathcal{F}$, um inteiro $j(P)$ é chamado de um $(\sum_s, P)$**-ordem** se existe uma curva $\mathcal{C}$ de grau s, tal que $I(P, \mathcal{F} \cap \mathcal{C}) = j(P)$. Indicando $j_i := j_i(P)$, em [18, section 1] vemos que existem exatamente $M+1$ $(\sum_s, P)$-ordens tais que $j_0 < j_1 < \ldots < J_M$. Pelos resultados encontrados em [11, Chapter 6] e [12, Aula 10] e nas condições da curva $\mathcal{F}$, temos que $M = \binom{s+2}{2} - 1$, $j_0 = 0$ e $j_1 = 1$. A sequência de inteiros $(j_0, j_1, \ldots, j_M)$ é chamada de **sequência de** $(\sum_s, P)$**-ordens**.

Temos ainda dos resultados obtidos em [18, Theorem 1] que existe uma única curva $\mathcal{H}_P$ de grau s, chamada de curva s**-osculante de** $\mathcal{F}$ **em** P, tal que $I(P, \mathcal{F} \cap \mathcal{H}_P) = j_M$.

Seja $\varphi : \mathcal{F} \to \mathbb{P}^M(\mathbb{F}_q)$ o morfismo associado a $\sum_s$ dado por $\varphi = (\varphi_0, \ldots, \varphi_M)$, tal que $\varphi_i \in \mathbb{F}_q(\mathcal{F})$ e t uma variável separante de $\overline{\mathbb{F}}_q(\mathcal{F})$. Temos por [18, Corollary 1.3] que:

$$\mathcal{H}_P : det \begin{pmatrix} X_0 & \cdots & X_n \\ (D_t^{(j_0)}\varphi_0)(P) & \cdots & (D_t^{(j_0)}\varphi_n)(P) \\ \vdots & \ddots & \vdots \\ (D_t^{(j_{n-1})}\varphi_0)(P) & \cdots & (D_t^{(j_{n-1})}\varphi_n)(P) \end{pmatrix} = 0 \tag{7}$$

De acordo com [18, Proposition 1.4 e Theorem 1.1] existe uma sequência de inteiros $\varepsilon_0 < \varepsilon_1 < \ldots < \varepsilon_M$ escolhida minimamente na ordem lexicográfica tal que o wronskiano

$$det\left(D_t^{(\varepsilon_i)}\varphi_j\right)_{i,j=0,\ldots,M} \tag{8}$$

é não nulo.

Um inteiro nas condições de (8) é chamado de $\sum_s$**- ordem de** $\mathcal{F}$ e a sequência de inteiros $(\varepsilon_0,\ldots,\varepsilon_M)$ é a **sequência de ordem de** $\mathcal{F}$ **em relação à** $\sum_s$.

Para quase todo ponto P temos que $(j_0,\ldots,j_M) = (\varepsilon_0,\ldots,\varepsilon_M)$ e tais pontos são chamados de $\sum_s$-ordinários. Os pontos para os quais $(j_0,\ldots,j_M) \neq (\varepsilon_0,\ldots,\varepsilon_M)$ são chamados de $\sum_s$-Weierstrass.

Se $\varepsilon_i = i$ para todo $i = 0,1,\ldots,M$ a curva $\mathcal{F}$ é chamada de **clássica**. Caso contrário é chamada de **não-clássica**.

De [18, Corollary 1.7] temos um resultado importante que nos ajuda a encontrar condições para os quais uma curva é clásica.

Proposição 1.2.1. Seja $P \in \mathcal{F}$ e $j_0,\ldots,j_M$ a sequência de $(\sum_s, P)$-ordens. Se o inteiro:

$$\prod_{i>k}\frac{j_i - j_k}{i-k}$$

não é divisível por p então $\mathcal{F}$ é clássica em relação à $\sum_s$.

Temos ainda de [18, Corollary 1.9] o seguinte resultado:

Proposição 1.2.2. Seja ε um $\sum_s$-ordem e μ um inteiro tal que

$$\binom{\varepsilon}{\mu} \not\equiv 0\,(mod.p)$$

então μ é também um $\sum_s$-ordem. Em particular se $\varepsilon < p$, então $\varepsilon_i = i$, para $i = 0,1,\ldots,\varepsilon-1$.

Usando as mesmas notações já utilizadas, vamos agora definir uma nova sequência de inteiros $(\nu_0,\nu_1,\ldots,\nu_{M-1})$ que será de extrema importância para este trabalho.

Considere o determinante:

$$det\begin{pmatrix} \varphi_0^q & \cdots & \varphi_n^q \\ (D_t^{(\nu_0)}\varphi_0) & \cdots & (D_t^{(\nu_0)}\varphi_n) \\ \vdots & \ddots & \vdots \\ (D_t^{(\nu_{n-1})}\varphi_0) & \cdots & (D_t^{(\nu_{n-1})}\varphi_n) \end{pmatrix}, \tag{9}$$

Por [18, Proposition 2.1] existem inteiros $\nu_0, \ldots, \nu_{M-1}$, com $\nu_0 < \ldots < \nu_{M-1}$ escolhidos minimamente na ordem lexicográfica tal que (9) é não nulo. Temos ainda que $(\nu_0, \ldots, \nu_{M-1}) = (\varepsilon_0, \ldots, \varepsilon_M) \setminus \{\varepsilon_I\}$, para algum $I \in \{1 \ldots, M\}$.

A sequência de inteiros $(\nu_0, \ldots, \nu_{M-1})$ é chamada de **sequência $\mathbb{F}_q$-Frobenius de ordem de $\mathcal{F}$ em relação à $\sum_s$**. Se $\nu_i = i$, para todo $i = 0, \ldots, M-1$ dizemos que a curva $\mathcal{F}$ é **$\mathbb{F}_q$-Frobenius clássica em relação à $\sum_s$** e caso contrário chamamos $\mathcal{F}$ de **$\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_s$**.

Vamos definir $\varphi_q : \mathcal{F} \to \mathcal{F}$, dado por $\varphi_q = (x^q, y^q, z^q)$ como o **morfismo de Frobenius**.

Por fim, é importante ressaltar que por [11] temos:

Proposição 1.2.3. Seja $p > M$. Supondo que $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_s$, então $\mathcal{F}$ é não clássica em relação à $\sum_s$.

1.3 CURVAS DE FERMAT E CLASSICALIDADE

Sendo n um inteiro que não é divisível por p, a curva $\mathcal{F} : ax^n + by^n = 1$ é a **curva de Fermat** de grau n.

Nesta seção iremos enunciar primeiramente os principais resultados da não classicalidade e $\mathbb{F}_q$-Frobenius não classicalidade de $\mathcal{F}$ em relação à $\sum_1$ e $\sum_2$.

Inicialmente vamos enunciar o caso da não classicalidade de $\mathcal{F}$ em relação à $\sum_1$, desenvolvido por [14] .

Proposição 1.3.1. Sendo $p \neq 2$, $\mathcal{F}$ é não clássica em relação à $\sum_1$ se, e somente se,

$$n \equiv 1 \, (mod.p).$$

E de acordo com [9, Theorem 2] e [5], temos o seguinte resultado em relação à $\mathbb{F}_q$-Frobenius não classicalidade de $\mathcal{F}$ em relação à $\sum_1$.

Teorema 1.3.2. *$\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_1$, se e somente se,*

$$n = \frac{q-1}{p^r - 1}$$

para algum inteiro $r < h$, $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$.

Em [8, section 1] e por [5], temos ainda que dada uma curva $\mathcal{F} : ax^n + by^r = 1$, $(p \nmid rn)$, obtemos o seguinte resultado:

Teorema 1.3.3. *$\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_1$ se, e somente se,*

$$n = r = \frac{q-1}{p^s-1}$$

para algum inteiro $s < h$, $s \mid h$ e $a, b \in \mathbb{F}_{p^s}^*$.

Agora vamos relembrar os resultados para o sistema linear das cônicas ($\sum_2$).
Por [10, Theorem 3] temos:

Proposição 1.3.4. Sendo $p \geq 7$, $\mathcal{F}$ é não clássica em relação à $\sum_2$ se, e somente se,

$$p \mid (n-1)(n-2)(n+1)(2n-1).$$

E em relação a $\mathbb{F}_q$-Frobenius não classicalidade temos por [9, Theorem 3] e por [3, Appendix B]:

Teorema 1.3.5. *Sendo $p \geq 7$, $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ exatamente em um dos casos a seguir:*

(1) Se $p \mid (n-1)$;

(2) Se $p \mid (n-2)$ e $n = \frac{2(q-1)}{p^r-1}$ com $r < h$, $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$;

(3) Se $p \mid (2n-1)$ e $n = \frac{q-1}{2(p^r-1)}$ com $r < h$, $r \mid h$ e $a^2, b^2 \in \mathbb{F}_{p^r}$;

(4) Se $q = n+1$ e $a + b = 1$.

Para finalizar vamos usar o principal resultado de [4] para introduzir duas famílias de curvas que serão estudadas nos capítulos 2 e 3.

Inicialmente vamos considerar uma curva $\mathcal{F}$ irredutível definida sobre $\mathbb{F}_q$ de característica $p > 2$ satisfazendo a seguinte propriedade (P):

(P) O grupo de $\mathbb{F}_q$-automorfismos de $\mathcal{F}$ contém um subgrupo $G = C_n \times C_m$, sendo C_i um grupo cíclico de ordem i primo com p, tal que $max\{n, m\} > 2$ e ambas as curvas quocientes $\mathcal{F}/C_n$ e $\mathcal{F}/C_m$ são racionais.

Dizemos que uma curva $\mathcal{F}$ é uma **curva de Fermat generalizada** quando $m = n$ e as G-órbitas curtas são $\mathbb{F}_q$-racionais.

De [4, Theorem 5.1] podemos extrair o seguinte resultado:

Proposição 1.3.6. Seja $\mathcal{F}$ uma curva definida sobre $\mathbb{F}_q$ satisfazendo a propriedade (P). Suponha que cada órbita curta de G é preservada pela aplicação de Frobenius e m e n dividem $q-1$, então $\mathcal{F}$ é $\mathbb{F}_q$-birracionalmente equivalente a uma das seguintes curvas:

(a) $ax^n + by^m = 1$ com $a, b \in \mathbb{F}_q^*$;

(b) $ax^n y^m + bx^n + cy^m = 1$ com $a, b, c \in \mathbb{F}_q$ e $c \neq -\frac{a}{b}$ e $a \neq 0$.

2 CURVA $\mathcal{F} : ax^n + by^m = 1$

Considere a curva $\mathcal{F} : ax^n + by^m = 1$ definida sobre o corpo finito $\mathbb{F}_q$ tal que $a, b \in \mathbb{F}_q^*$ e $m, n \in \mathbb{Z}_+^*$. Vamos supor ainda que $p > 2$ daqui em diante e que $n \geq m$, sem perda de generalidade. Como a classicalidade da curva é uma propriedade geométrica, para as seções 2.1 e 2.3 vamos considerar que $a = b = 1$.

2.1 CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_1$

Apesar dos resultados da proposição e do teorema seguinte serem já conhecidos (Teorema 1.3.3), vamos desenvolver uma outra demonstração para o caso específico que estamos trabalhando.

Inicialmente iremos determinar sobre quais condições a curva $\mathcal{F}$ é não clássica em relação à $\sum_1$.

Proposição 2.1.1. A curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é não clássica em relação à $\sum_1$ se, e somente se, $m \equiv 1 \, (mod\ p)$ e $n \equiv 1 (mod\ p)$.

Demonstração. Temos que $p \nmid n$, logo x é uma variável separante. De acordo com [18] a não classicalidade de $\mathcal{F}$ é equivalente a $D_x^{(2)} y = 0$.

Temos que $D_x^{(1)}(x^n + y^m) = 0 \iff nx^{n-1} + my^{m-1} D_x^{(1)} y = 0$ e assim

$$D_x^{(1)} y = -\frac{nx^{n-1}}{my^{m-1}} \tag{10}$$

Derivando novamente em relação à x temos que

$$\begin{aligned} & D_x^{(1)} \left(nx^{n-1} + my^{m-1} D_x^{(1)} y \right) = 0 \iff \\ & n(n-1)x^{n-2} + D_x^{(1)}(my^{m-1}) D_x^{(1)} y + my^{m-1} D_x^{(1)} \left(D_x^{(1)} y \right) = 0 \iff \\ & n(n-1)x^{n-2} + m(m-1)y^{m-2} \left(D_x^{(1)} y \right)^2 + 2my^{m-1} D_x^{(2)} y = 0. \end{aligned} \tag{11}$$

Usando o fato que $D_x^{(2)} y = 0$ e substituindo a equação (10) em (11) obtemos:
$n(n-1)x^{n-2} + m(m-1)y^{m-2}\frac{n^2x^{2n-2}}{m^2y^{2m-2}} = 0$.
Nas condições dadas temos que $p \nmid n$ e $p \nmid m$, portanto:
$m(n-1)x^{n-2} + n(m-1)x^{2n-2}y^{-m} = 0 \iff m(n-1)y^m + n(m-1)x^n = 0 \iff$
$mn(y^m + x^n) - my^m - nx^n = 0$.

Relembrando que a equação da curva é dada por $\mathcal{F} : x^n + y^m = 1$ e substituindo na expressão acima, temos:

$$mn - m(1-x^n) - nx^n = 0 \iff m(n-1) + (m-n)x^n = 0. \tag{12}$$

Como x é transcendente, em (12) temos $m(n-1) = 0$ e $m - n = 0$. Da nossa hipótese inicial, vem que $p \nmid m$, assim $p|(n-1)$ e $p|(m-n)$ e, portanto, $p \mid (n-1)$ e $p \mid (m-1)$, ou seja, $m \equiv 1 \,(mod\, p)$ e $n \equiv 1 \,(mod\, p)$.

Se $n = m$ temos o caso já estudado por [14] e obtemos $n \equiv m \equiv 1 (mod\, p)$.

A nossa demonstração é uma simplificação do caso geral apresentado por [8, Theorem 1].

Podemos escrever a curva como $\mathcal{F} : y^m = f(x)$ com $f(x) = 1 - x^n$ e, usando [8, Theorem 1] vem que $m \equiv 1 (mod\, p)$ e $f''(x) = 0 \iff n(n-1)x^{n-2} = 0 \iff n \equiv 1 (mod\, p)$.

Note ainda que se assumirmos $m \equiv 1 \,(mod\, p)$ e $n \equiv 1 \,(mod\, p)$, em (11) obtemos $2my^{m-1}D_x^{(2)} y = 0$ e como $p \nmid m$ vem que $D_x^{(2)} y = 0$ e , consequentemente a curva $\mathcal{F}$ é não clássica em relação à $\sum_1$. □

2.2 $\mathbb{F}_q$-FROBENIUS CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_1$

É fácil verificar que a sequência de ordem de $\mathcal{F}$ em relação à $\sum_1$ é dada por $(0, 1, \varepsilon)$. Para a curva ser não clássica temos que $\varepsilon \neq 2$ e, pela proposição 2.1.1, temos que $m \equiv 1 (mod\, p)$ e $n \equiv 1 (mod\, p)$.

Vamos inicialmente enunciar um lema conhecido sobre polinômios que será de grande utilidade pra simplificar alguns cálculos.

Lema 2.2.1. [2, Lemma 4.2] Seja K um corpo arbitrário. Considere dois polinômios não constantes $b_1(x), b_2(x) \in K[x]$ e sejam l e m inteiros positivos. Então:

$$y^l - b_1(x) \text{ divide } y^m - b_2(x)$$

se, e somente se:

$$l \mid m \text{ e } b_2(x) = b_1(x)^{\frac{m}{l}}.$$

Teorema 2.2.2. *A curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica se, e somente se, $m = n = \frac{q-1}{p^r-1}$ para algum inteiro $r < h$, $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$*

Demonstração. De acordo com [18], para a curva ser $\mathbb{F}_q$-Frobenius não clássica devemos ter necessariamente

$$\begin{vmatrix} 1 & x^q & y^q \\ 1 & x & y \\ 0 & 1 & D_x^{(1)}y \end{vmatrix} = 0 \iff \begin{vmatrix} x^q - x & y^q - y \\ 1 & D_x^{(1)}y \end{vmatrix} = 0 \iff (x^q - x)D_x^{(1)}y - (y^q - y) = 0 \tag{13}$$

Temos ainda que derivando a equação da curva em relação à x, obtemos:

$$D_x^{(1)}y = -\frac{anx^{n-1}}{bmy^{m-1}} \tag{14}$$

De acordo com 2.1.1 temos que $m \equiv 1 (mod\ p)$ e $n \equiv 1 (mod\ p)$ e assim susbtituindo em (14) temos que tal expressão pode ser reescrita como

$$D_x^{(1)}y = -\frac{ax^{n-1}}{by^{m-1}} \tag{15}$$

Substituindo (15) em (13) temos:

$$(x^q - x)(-ax^{n-1}) - (y^q - y)by^{m-1} = 0 \iff -ax^{n+q-1} - by^{m+q-1} + ax^n + by^m = 0 \iff$$
$$ax^{n+q-1} + by^{m+q-1} = 1. \tag{16}$$

Observe que podemos reescrever (16) como:

$$y^{m+q-1} - \left(\frac{1}{b} - \frac{a}{b}x^{n+q-1}\right) = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Por [3, Proposition 2.6] temos que $y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right)$ divide $y^{m+q-1} - \left(\frac{1}{b} - \frac{a}{b}x^{n+q-1}\right)$ e por 2.2.1 vem que $m \mid m + q - 1$ e, portanto, $m|q - 1$, ou seja, $q - 1 = mt$, para algum inteiro t.

Usando (16) obtemos:

$$by^{m+q-1} = 1 - ax^{n+q-1}. \tag{17}$$

Por outro lado, pela equação de $\mathcal{F}$:

$$by^{m+q-1} = by^{m+mt} = by^{m(1+t)} = (1 - ax^n)^{1+t}/b^t. \tag{18}$$

Assim de (17) e (18) vem que

$$1 - ax^{n+q-1} = (1 - ax^n)^{1+t}/b^t. \tag{19}$$

Comparando os graus de ambos os termos de (19) obtemos:

$$n + q - 1 = n(1 + t) \iff nt = q - 1 \iff nt = mt \iff n = m.$$

Agora basta usar o Teorema 1.3.2 para concluir o resultado. A recíproca é imediata não necessitando de cálculos mais detalhados. □

2.3 CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_2$

Proposição 2.3.1. Se $p > 5$ e a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é não clássica em relação à $\sum_2$, então

$$p \mid (2n-1)(n+1)(n-2)(n-1) \text{ e } p \mid (2m-1)(m+1)(m-2)(m-1).$$

Demonstração. Por motivos que ficarão claros ao longo desta demonstração, dividiremos esse resultado em dois casos:

(1) Supor $p \nmid (n-1)$

Recordando que $n \geq m$ e homogeinizando a equação de $\mathcal{F}$ obtemos $X^n + Z^{n-m}Y^m - Z^n = 0$.

Vamos determinar os pontos de inflexão de $\mathcal{F}$!

A Hessiana de $\mathcal{F}$ é dada por:

$$\mathcal{H} : H(X,Y,Z) = \begin{vmatrix} F_{XX} & F_{XY} & F_{XZ} \\ F_{YX} & F_{YY} & F_{YZ} \\ F_{ZX} & F_{ZY} & F_{ZZ} \end{vmatrix} = 0.$$

E temos que $F_{XY} = F_{YX} = F_{XZ} = F_{ZX} = 0$, $F_{XX} = n(n-1)X^{n-2}$, $F_{YY} = m(m-1)Y^{m-2}Z^{n-m}$, $F_{YZ} = m(n-m)Z^{n-m-1}Y^{m-1}$ e $F_{ZZ} = (n-m)(n-m-1)y^mZ^{n-m-2} - n(n-1)Z^{n-2}$.

Assim, desomogeinizando a equação da Hessiana, obtemos

$$\mathcal{H} : H(X,Y,1) = \begin{vmatrix} n(n-1)x^{n-2} & 0 & 0 \\ 0 & m(m-1)y^{m-2} & m(n-m)y^{m-1} \\ 0 & m(n-m)y^{m-1} & y^m(n-m)(n-m-1) - n(n-1) \end{vmatrix} = 0 \iff$$

$$\mathcal{H} : H(x,y) = mn(n-1)\begin{vmatrix} x^{n-2} & 0 & 0 \\ 0 & (m-1)y^{m-2} & (n-m)y^{m-1} \\ 0 & m(n-m)y^{m-1} & y^m(n-m)(n-m-1) - n(n-1) \end{vmatrix} = 0 \iff$$

$$\mathcal{H} : mn(n-1)[(m-1)x^{n-2}y^{m-2}(y^m(n-m)(n-m-1) - n(n-1)) - m(n-m)^2x^{n-2}y^{2m-2}] = 0 \iff$$

$$\mathcal{H} : mn(n-1)x^{n-2}y^{m-2}[y^m(n-m)((m-1)(n-m-1) - m(n-m)) - n(n-1)(m-1)] = 0 \iff$$

$$\mathcal{H} : mn(n-1)x^{n-2}y^{m-2}[y^m(n-m)(1-n) - n(n-1)(m-1)] = 0 \iff$$
$$\mathcal{H} : mn(n-1)^2x^{n-2}y^{m-2}(y^m(m-n) - n(m-1)) = 0.$$

Usando o fato que $p \nmid (n-1)$, podemos escrever a equação da Hessiana por:

$$\mathcal{H} : x^{n-2}y^{m-2}(y^m(m-n) - n(m-1)) = 0. \tag{20}$$

De acordo com o Teorema 1.1.3, como o único ponto singular de $\mathcal{F}$ é $(0:1:0)$, temos que os pontos de inflexão são dados pela solução do sistema:

$$\begin{cases} x^{n-2}y^{m-2}(y^m(m-n) - n(m-1)) = 0 \\ x^n + y^m = 1 \end{cases}$$

Resolvendo o sistema, obtemos os pontos de inflexão $P_\xi = (0,\xi)$, sendo ξ uma raiz m-ésima da unidade; $P_\rho = (\rho,0)$, sendo ρ uma raiz n-ésima da unidade e $P_{\alpha,\beta} = (\alpha,\beta)$, sendo β a raíz m-ésima de $\frac{n(m-1)}{m-n}$ e α a raiz n-ésima de $\frac{m(1-n)}{m-n}$ tal que $p \nmid (m-n)$.

Em seguida vamos calcular a multiplicidade de cada um destes pontos em relação à $\mathcal{F}$ com as respectivas retas tangentes em tais pontos

- $P_\xi = (0,\xi)$

  Uma equação da reta tangente é dada por $\ell_\xi : m\xi^{m-1}(y-\xi) = 0 \iff$
  $\ell_\xi : y - \xi = 0$. Uma parametrização é dada por $y = \xi$ e $x = t$ e assim temos que $f(t,\xi) = t^n + \xi^m - 1 \iff f(t,\xi) = t^n$ e portanto $I(P_\xi, \ell_\xi \cap \mathcal{F}) = n$.

- $P_\rho = (\rho, 0)$

  Uma equação da reta tangente é dada por $\ell_\rho : n\rho^{n-1}(x-\rho) = 0 \iff \ell_\rho : x - \rho = 0$. Uma parametrização é dada por $y = t$ e $x = \rho$ e assim temos que $f(\rho, t) = \rho^m + t^m - 1 \iff f(\rho, t) = t^m$ e portanto $I(P_\rho, \ell_\rho \cap \mathcal{F}) = m$.

- $P_{\alpha,\beta} = (\alpha, \beta)$

  Uma equação da reta tangente é dada por $\ell_{\alpha,\beta} : n\alpha^{n-1}(x-\alpha) + m\beta^{m-1}(y-\beta) = 0 \iff \ell_{\alpha,\beta} : n\alpha^{n-1}x - n\alpha^n + m\beta^{m-1}y - m\beta^m = 0 \iff \ell_{\alpha,\beta} : n\alpha^{n-1}x + \beta^{m-1}y - mn = 0$. Uma parametrização é dada por $y = \beta - n\alpha^{n-1}t$ e $x = \alpha + m\beta^{m-1}t$ e assim temos que $f(\alpha + m\beta^{m-1}t, \beta - n\alpha^{n-1}t) = (\alpha + m\beta^{m-1}t)^n + (\beta - n\alpha^{n-1}t)^m - 1 = \alpha^n + \beta^m - 1 + t^m(n^m\alpha^{m(n-1)} + f(t)) \iff f(\alpha + m\beta^{m-1}t, \beta - n\alpha^{n-1}t) = t^m(n^m\alpha^{m(n-1)} + f(t))$, e portanto $I(P_{\alpha,\beta}, \ell_{\alpha,\beta} \cap \mathcal{F}) = m$.

Olhando apenas para os casos de ponto de inflexão, temos que a sequência de $(\sum_1, P_{\tilde{\xi}})$-ordem é dada por $(0, 1, n), n \geq 3$ e consequentemente a sequência de $(\sum_2, P_{\tilde{\xi}})$-ordem é dada por $(0, 1, 2, n, n+1, 2n)$. Analogamente usando P_ρ obtemos que a sequência de $(\sum_2, P_\rho)$-ordem é dada por $(0, 1, 2, m, m+1, 2m)$. O mesmo resultado se aplica ao calcularmos a sequência de $(\sum_2, P_{\alpha,\beta})$-ordem.

Usando a proposição 1.2.1 segue que se $\mathcal{F}$ é não clássica em relação à $\sum_2$, então

$$p \mid (2n-1)(n-2)(n+1) \text{ e } p \mid (2m-1)(m-2)(m+1)(m-1).$$

(2) Supor $p \mid (n-1)$.

Note que supondo $p \mid n-1$, a Hessiana se anula. Para este caso, vamos usar as ideias apresentadas no capítulo 1 e a equação (8).

Temos que $p \nmid n$, logo x é uma variável separante. Um morfismo associado ao sistema linear dado por $\sum_2$ é $\varphi = (1 : x : y : xy : x^2 : y^2)$.

Analisaremos o determinante

$$A = det \begin{pmatrix} 1 & x & y & xy & x^2 & y^2 \\ 0 & 1 & D_x^{(1)}y & xD_x^{(1)}y + y & 2x & 2yD_x^{(1)}y \\ 0 & 0 & D_x^{(2)}y & xD_x^{(2)}y + D_x^{(1)}y & 2 & (D_x^{(1)}y)^2 + 2yD_x^{(2)}y \\ 0 & 0 & D_x^{(3)}y & xD_x^{(3)}y + D_x^{(2)}y & 0 & 2D_x^{(1)}yD_x^{(2)}y + 2yD_x^{(3)}y \\ 0 & 0 & D_x^{(4)}y & xD_x^{(4)}y + D_x^{(3)}y & 0 & 2D_x^{(1)}yD_x^{(3)}y + (D_x^{(2)}y)^2 + 2yD_x^{(4)}y \\ 0 & 0 & D_x^{(5)}y & xD_x^{(5)} + D_x^{(4)}y & 0 & 2D_x^{(2)}yD_x^{(3)}y + 2D_x^{(4)}yD_x^{(1)}y + 2yD_x^{(5)}y \end{pmatrix}$$

Note que tal determinante, após operações elementares sobre as colunas, pode ser reescrito como:

$$A = det\begin{pmatrix} 1 & x & y & 0 & 0 & y^2 \\ 0 & 1 & D_x^{(1)}y & y & x & 0 \\ 0 & 0 & D_x^{(2)}y & D_x^{(1)}y & 2 & (D_x^{(1)}y)^2 \\ 0 & 0 & D_x^{(3)}y & D_x^{(2)}y & 0 & 2D_x^{(1)}yD_x^{(2)}y \\ 0 & 0 & D_x^{(4)}y & D_x^{(3)}y & 0 & 2D_x^{(1)}yD_x^{(3)}y + (D_x^{(2)}y)^2 \\ 0 & 0 & D_x^{(5)}y & D_x^{(4)}y & 0 & 2D_x^{(2)}yD_x^{(3)}y + 2D_x^{(4)}yD_x^{(1)}y \end{pmatrix}$$

Desenvolvendo o determinante por Chió temos

$$A = det\begin{pmatrix} 1 & D_x^{(1)}y & y & x & 0 \\ 0 & D_x^{(2)}y & D_x^{(1)}y & 2 & (D_x^{(1)}y)^2 \\ 0 & D_x^{(3)}y & D_x^{(2)}y & 0 & 2D_x^{(1)}yD_x^{(2)}y \\ 0 & D_x^{(4)}y & D_x^{(3)}y & 0 & 2D_x^{(1)}yD_x^{(3)}y + (D_x^{(2)}y)^2 \\ 0 & D_x^{(5)}y & D_x^{(4)}y & 0 & 2D_x^{(2)}yD_x^{(3)}y + 2D_x^{(4)}yD_x^{(1)}y \end{pmatrix}$$

Desenvolvendo novamente por Chió, obtemos:

$$A = det\begin{pmatrix} D_x^{(2)}y & D_x^{(1)}y & 2 & (D_x^{(1)}y)^2 \\ D_x^{(3)}y & D_x^{(2)}y & 0 & 2D_x^{(1)}yD_x^{(2)}y \\ D_x^{(4)}y & D_x^{(3)}y & 0 & 2D_x^{(1)}yD_x^{(3)}y + (D_x^{(2)}y)^2 \\ D_x^{(5)}y & D_x^{(4)}y & 0 & 2D_x^{(2)}yD_x^{(3)}y + 2D_x^{(4)}yD_x^{(1)}y \end{pmatrix}$$

E aplicando Laplace na terceira coluna obtemos

$$A = 2det\begin{pmatrix} D_x^{(3)}y & D_x^{(2)}y & 2D_x^{(1)}yD_x^{(2)}y \\ D_x^{(4)}y & D_x^{(3)}y & 2D_x^{(1)}yD_x^{(3)}y + (D_x^{(2)}y)^2 \\ D_x^{(5)}y & D_x^{(4)}y & 2D_x^{(2)}yD_x^{(3)}y + 2D_x^{(4)}yD_x^{(1)}y \end{pmatrix}$$

Aplicando mais uma operação elementar na coluna obtemos:

$$A = 2det\begin{pmatrix} D_x^{(3)}y & D_x^{(2)}y & 0 \\ D_x^{(4)}y & D_x^{(3)}y & (D_x^{(2)}y)^2 \\ D_x^{(5)}y & D_x^{(4)}y & 2D_x^{(2)}yD_x^{(3)}y \end{pmatrix}$$

Por fim, desenvolvendo tal determinante de ordem 3 obtemos:

$$A = 2D_x^{(2)}y\left(D_x^{(3)}y\right)^3 + D_x^{(5)}y\left(D_x^{(2)}y\right)^3 - 3D_x^{(4)}yD_x^{(3)}y\left(D_x^{(2)}y\right)^2 \iff$$
$$A = D_x^{(2)}y\left(2\left(D_x^{(3)}y\right)^3 + D_x^{(5)}y\left(D_x^{(2)}y\right)^2 - 3D_x^{(4)}yD_x^{(3)}yD_x^{(2)}y\right) \tag{21}$$

Usando o fato que $p|n-1$ vem que:

$D_x^{(1)}y = -\frac{x^{n-1}}{my^{m-1}}$, $D_x^{(2)}y = -\frac{(m-1)x^{2n-2}}{2m^2y^{2m-1}}$, $D_x^{(3)}y = -\frac{(2m-1)(m-1)x^{3n-3}}{6m^3y^{3m-1}}$, $D_x^{(4)}y = -\frac{(3m-1)(2m-1)(m-1)x^{4n-4}}{24m^4y^{4m-1}}$ e $D_x^{(5)}y = -\frac{(4m-1)(3m-1)(2m-1)(m-1)x^{5n-5}}{120m^5y^{5m-1}}$.

Substituindo as expressões acima em (21), temos que $A = 0 \iff m-1 = 0$ ou $2m-1 = 0$ ou $m-2 = 0$ ou $m+1 = 0$.

É importante notar que se $p|(n-1)$ e $p|(m-1)$, $\mathcal{F}$ é não-clássica em relação à $\sum_1$ e, portanto, será não clássica em relação à $\sum_2$.

De fato, suponha que $(0,1,\varepsilon)$, $\varepsilon \geq 3$ seja a sequência de ordem de $\mathcal{F}$ em relação à $\sum_1$. Considerando todas as cônicas geradas pela união de duas dessas retas obtemos a sequência de ordem $(0,1,2,\varepsilon,\varepsilon+1,2\varepsilon)$ e como $\varepsilon > 3$ ela é formada de 6 elementos distintos e será então a sequência de ordem de $\mathcal{F}$ em relação à $\sum_2$ e, portanto não clássica.

Pela Proposição 2.1.1, segue que $\mathcal{F}$ é não clássica em relação à $\sum_1$, e portanto não clássica em relação à $\sum_2$.

Assim, juntando os casos (1) e (2), concluímos que se $p > 5$ e a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é não clássica em relação à $\sum_2$, então $p \mid (2n-1)(n+1)(n-2)(n-1)$ e $p \mid (2m-1)(m+1)(m-2)(m-1)$. □

Para concluir o caso da não classicalidade de $\mathcal{F}$ em relação à $\sum_2$, iremos demonstrar o lema abaixo que é uma adaptação de [3, Lemma 3.4] para o nosso caso de cônicas.

Lema 2.3.2. Assuma $p > 5$. Seja $\overline{\mathbb{F}}_q(x,y)$ o corpo de funções de $\mathcal{F}$, e $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico. Suponha que exista um polinômio $G(X,Y) = \sum a_{ij}(x,y)^p X^i Y^j \in \overline{\mathbb{F}}_q[x,y][X,Y]$ de grau $d \geq 2$ tal que $G(x,y) = 0$. Para $G_P(X,Y) := \sum a_{ij}(u,v)^p X^i Y^j \in \overline{\mathbb{F}}_q[X,Y]$, é válido o seguinte:

(a) Se $G_P(X,Y)$ é irredutível de grau $d = 2$, então $\mathcal{F}$ é não clássica em relação à $\sum_2$ e a curva $\mathcal{G}_P : G_P(X,Y) = 0$ é a cônica osculante de $\mathcal{F}$ em P.

(b) Se a curva $\mathcal{G}_P : G_P(X,Y) = 0$ é tal que $I(P, \mathcal{G}_P \cap \mathcal{C}) < p$ para toda cônica $\mathcal{C}$, então $\mathcal{F}$ é clássica em relação à $\sum_2$.

Demonstração. Nas condições de um ponto genérico e supondo que $\mathcal{F}$ é clássica em relação à $\sum_1$, podemos afirmar que a sequência de ordem de $\mathcal{F}$ em relação à $\sum_2$ é dada por $(0,1,2,3,4,\varepsilon)$.

Seja $\mathcal{G}_P$ a curva definida por $\mathcal{G}_P : G_P(X,Y) = 0$, temos:

$$G_P(x,y) = G_P(x,y) - G(x,y) = \sum (a_{ij}(u,v) - a_{ij}(x,y))^p x^i y^j,$$

Como a quantidade de pólos e zeros é finita, para um ponto genérico segue que $v_P(G_P(x,y)) \geq p$, ou seja,

$$I(P, \mathcal{F} \cap \mathcal{G}_P) \geq p > 5. \tag{22}$$

Como $\mathcal{G}_p$ é uma cônica concluímos que $\varepsilon > 5$ e portanto $\mathcal{F}$ é não clássica em relação à $\sum_2$.

Seja $\mathcal{H}_P$ a cônica osculante de $\mathcal{F}$ em P. Pelo hipótese de (a) temos que $deg(\mathcal{G}_P) = 2$ e a desigualdade (22) implica que $I(P, \mathcal{F} \cap \mathcal{H}_P) \geq p$, e por [3, Lemma 3.3] temos:

$$I(P, \mathcal{H}_p \cap \mathcal{G}_P) \geq p > 4 = deg(\mathcal{H}_P) \cdot deg(\mathcal{G}_P)$$

Como $\mathcal{G}_P$ é irredutível, pelo Teorema de Bézout 1.1.1 , $\mathcal{G}_P$ e $\mathcal{H}_P$ devem ser a mesma curva, e como P é um ponto genérico o resultado segue. Afirmação (b) segue diretamente de [3, Lemma 3.3] e do fato que a não classicalidade de $\mathcal{F}$ em relação à $\sum_2$ implica que $I(P, \mathcal{F} \cap \mathcal{H}_P) \geq p$ conforme a proposição 1.2.2. □

Observação 2.3.3. Note que se $\mathcal{G}_p$ é irredutível de grau d, com $2 < d < p/2$, então, pelo Teorema de Bézout 1.1.1, as condições do Lema 2.3.2(b) são satisfeitas, isto é, $\mathcal{F}$ é clássica em relação à $\sum_2$.

Lema 2.3.4. Considerando $p > 2$, são irredutíveis sobre $\overline{\mathbb{F}}_q$ as seguintes curvas projetivas:

(a) $\mathcal{F}_1 : X^2 + Y^2 - Z^2 = 0$;

(b) $\mathcal{F}_2 : XZ + YZ - XY = 0$;

(c) $\mathcal{F}_3 : X^2 + Y^2 + Z^2 - 2XY - 2XZ - 2YZ = 0$;

(d) $\mathcal{F}_4 : ZY - X^2 + 2XZ - Z^2 = 0$;

(e) $\mathcal{F}_5 : XZ + Y^2 - Z^2 = 0$;

(f) $\mathcal{F}_6 : XY - YZ + Z^2 = 0$;

(g) $\mathcal{F}_7 : XY^2 - Z^3 + 2YZ^2 - Y^2Z = 0$;

(h) $\mathcal{F}_8 : X^2Y - YZ^2 + Z^3 = 0$;

(i) $\mathcal{F}_9 : XZ^3 - Y^4 + 2Y^2Z^2 - Z^4 = 0$.

Demonstração. Para os itens (a) a (f) basta observar que as cônicas são não singulares e portanto irredutíveis.

De acordo com [19] se uma cúbica tem uma única singularidade que é um nó, então ela é irredutível. Para os itens (g) e (h) basta verificar que isto ocorre. Por exemplo, para o item (g) o único ponto singular de $\mathcal{F}_1$ é $(1:0:0)$ e é fácil verificar que tal ponto é um nó. Para a outra curva, o cálculo é análogo.

Para o item (i) basta observar que a quártica possui um único ponto singular de multiplicidade 3 e portanto é irredutível. □

Proposição 2.3.5. Supondo $p > 5$, a curva $\mathcal{F}$ é clássica em relação à $\sum_2$, nos casos:

(a) $p|(2n-1)$ e $p|(m+1)$;

(b) $p|(2m-1)$ e $p|(n+1)$;

(c) $p|(2n-1)$ e $p|(m-2)$;

(d) $p|(2m-1)$ e $p|(n-2)$;

(e) $p|(m+1)$ e $p|(n-2)$;

(f) $p|(n+1)$ e $p|(m-2)$;

Demonstração. (a) Considere inteiros r, s, k, l tais que $2n = p^r k + 1$ e $m = p^s l - 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $2n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$(x^n + y^m - 1)(x^n - y^m + 1) = 0 \iff x^{2n} - y^{2m} + 2y^m - 1 = 0$$

$$\iff (x^w)^{p^s} x - ((y^l)^2)^{p^s} y^{-2} + 2(y^l)^{p^s} y^{-1} - 1 = 0. \tag{23}$$

Considerando $P = (u:v:1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (23) obtemos a cúbica projetiva $\mathcal{G}_7 : \alpha XY^2 - \beta^2 Z^3 + 2\beta YZ^2 - Y^2 Z = 0$. Como $\mathcal{G}_7$ é projetivamente equivalente a $\mathcal{F}_7 : XY^2 - Z^3 + 2YZ^2 - Y^2 Z = 0$, que é irredutível, segue do Lema 2.3.2 e da observação 2.3.3 que $\mathcal{F}$ é clássica em relação à $\sum_2$.

(b) Com um raciocínio análogo ao item anterior e fazendo a transformação projetiva $(X:Y:Z) \mapsto (Y:X:Z)$, obtemos a cúbica projetiva irredutível $\mathcal{F}_7 : XY^2 - Z^3 + 2YZ^2 - Y^2 Z = 0$ e, portanto $\mathcal{F}$ é clássica em relação à $\sum_2$.

(c) Considere inteiros r, s, k, l tais que $2n = p^r k + 1$ e $m = p^s l + 2$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $2n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$(x^n + y^m - 1)(x^n - y^m + 1) = 0 \iff x^{2n} - y^{2m} + 2y^m - 1 = 0$$

$$\iff (x^w)^{p^s} x - ((y^l)^2)^{p^s} y^4 + 2(y^l)^{p^s} y^2 - 1 = 0. \tag{24}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (24) obtemos a quártica projetiva $\mathcal{G}_9 : \alpha X Z^3 - \beta^2 Y^4 + 2\beta Y^2 Z^2 - Z^4 = 0$. Como $\mathcal{G}_9$ é projetivamente equivalente a $\mathcal{F}_9 : XZ^3 - Y^4 + 2Y^2Z^2 - Z^4 = 0$, que é irredutível, segue do Lema 2.3.2 e da observação 2.3.3 que $\mathcal{F}$ é clássica em relação à $\sum_2$ para $p > 7$.

Vamos analisar separadamente o caso $p = 7$.

Temos que o ponto $Q = (2 : s : 1)$, $s^2 = -2$ é um ponto de inflexão da curva $\mathcal{F}_9$ e sendo ℓ_Q a reta tangente à $\mathcal{F}_9$ pelo ponto Q, temos que $\ell_Q : X - 2sY + Z = 0$. É fácil provar ainda que $I(Q, \mathcal{F}_9 \cap \ell_Q) = 3$.

Considerando a cônica $\mathcal{C}_1 := (\ell_Q)^2$ e como ℓ_Q não é componente de $\mathcal{F}_9$, temos que $I(Q, \mathcal{F}_9 \cap \mathcal{C}_1) = 6$.

Considerando uma cônica $\mathcal{C} \neq \mathcal{C}_1$ que contenha ℓ_Q como componente, temos que $\mathcal{C} := \ell_Q \cdot \ell$ e, portanto, $I(Q, \mathcal{F}_9 \cap \mathcal{C}) = I(Q, \mathcal{F}_9 \cap \ell_Q) + I(Q, \mathcal{F}_9 \cap \ell) \leq 3 + 3 < 7$.

Já no caso das cônicas que não possuem ℓ_Q como componente, usando [3, Lema 3.3] e o Teorema de Bézout 1.1.1 temos $I(Q, \mathcal{F}_9 \cap \mathcal{C}) < 7$.

Portanto, $I(Q, \mathcal{F}_9 \cap \mathcal{C}) < 7$ para todas as cônicas e, consequentemente, $\mathcal{F}$ é clássica em relação à $\sum_2$.

(d) Com um raciocínio análogo ao item anterior e fazendo a transformação projetiva $(X : Y : Z) \mapsto (Y : X : Z)$, obtemos $\mathcal{F}_9 : XZ^3 - Y^4 + 2Y^2Z^2 - Z^4 = 0$ e concluímos que $\mathcal{F}$ é clássica em relação à $\sum_2$.

(e) Considere inteiros r, s, k, l tais que $n = p^r k + 2$ e $m = p^s l - 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s + 2 = wp^s + 2$. Temos que:

$$x^n + y^m - 1 = 0 \iff (x^w)^{p^s} x^2 + (y^l) p^s y^{-1} - 1 = 0. \tag{25}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (25) obtemos a cúbica projetiva $\mathcal{G}_8 : \alpha X^2Y - YZ^2 + \beta Z^3 = 0$. Como $\mathcal{G}_8$ é projetivamente equivalente a $\mathcal{F}_8 : X^2Y - YZ^2 + Z^3 = 0$, que é irredutível, segue do Lema 2.3.2 e da observação 2.3.3 que $\mathcal{F}$ é clássica em relação à $\sum_2$.

(f) Com um raciocínio análogo ao caso anterior e fazendo a transformação projetiva $(X : Y : Z) \mapsto (Y : X : Z)$, obtemos a cúbica projetiva irredutível $\mathcal{F}_8 : X^2Y - YZ^2 - Z^3 = 0$ e portanto $\mathcal{F}$ é clássica em relação à $\sum_2$.

□

Proposição 2.3.6. Supondo $p > 5$ a curva $\mathcal{F}$ é não clássica em relação à $\sum_2$, nos casos:

(a) $p|(m-2)$ e $p|(n-2)$;

(b) $p|(m+1)$ e $p|(n+1)$;

(c) $p|(2m-1)$ e $p|(2n-1)$;

(d) $p|(m-1)$ e $p|(n-1)$;

(e) $p|(2m-1)$ e $p|(n-1)$;

(f) $p|(m-1)$ e $p|(2n-1)$;

(g) $p|(m-2)$ e $p|(n-1)$;

(h) $p|(m-1)$ e $p|(n-2)$;

(i) $p|(m+1)$ e $p|(n-1)$;

(j) $p|(m-1)$ e $p|(n+1)$.

Demonstração. (a) Considere inteiros r, s, k, l tais que $n = p^r k + 2$ e $m = p^s l + 2$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s + 2 = wp^s + 2$. Temos que:

$$x^n + y^m - 1 = 0 \iff (x^w)^{p^s} x^2 + (y^l)^{p^s} y^2 - 1 = 0. \tag{26}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (26) obtemos a cônica projetiva $\mathcal{G}_1 : \alpha X^2 + \beta Y^2 - Z^2 = 0$. Como $\mathcal{G}_1$ é projetivamente equivalente a $\mathcal{F}_1 : X^2 + Y^2 - Z^2 = 0$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(b) Considere inteiros r,s,k,l tais que $n = p^r k - 1$ e $m = p^s l - 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s - 1 = wp^s - 1$. Temos que:

$$(x^n + y^m - 1)(xy) = 0 \iff (x^w)^{p^s} y + (y^l)^{p^s} x - xy = 0. \tag{27}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (27) obtemos a cônica projetiva $\mathcal{G}_2 : \alpha YZ + \beta XZ - XY = 0$. Como $\mathcal{G}_2$ é projetivamente equivalente a $\mathcal{F}_2 : XZ + YZ - XY = 0$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(c) Considere inteiros r,s,k,l tais que $2n = p^r k + 1$ e $2m = p^s l + 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $2n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$\begin{aligned}
&(x^n + y^m)^2 = 1 \implies \\
&x^{2n} + 2x^n y^m + y^{2m} = 1 \implies \\
&(x^{2n} + y^{2m} - 1)^2 = (2x^n y^m)^2 \implies \\
&x^{4n} + y^{4m} + 1 - 2x^{2n} y^{2m} - 2x^{2n} - 2y^{2m} = 0 \implies \\
&((x^w)^{p^s})^2 x^2 + ((y^l)^{p^s})^2 y^2 + 1 - 2(x^w)^{p^s} (y^l)^{p^s} xy - 2(x^w)^{p^s} x - 2(y^l)^{p^s} y = 0.
\end{aligned} \tag{28}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (28) obtemos a cônica projetiva $\mathcal{G}_3 : \alpha^2 X^2 + \beta^2 Y^2 + Z^2 - 2\alpha\beta XY - 2\alpha XZ - 2\beta YZ = 0$. Como $\mathcal{G}_3$ é projetivamente equivalente a $\mathcal{F}_3 : X^2 + Y^2 + Z^2 - 2XY - 2XZ - 2YZ = 0$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(d) Note que neste caso $\mathcal{F}$ é não clássica em relação à $\sum_1$ e, portanto, não clássica em relação à $\sum_2$.

(e) Considere inteiros r,s,k,l tais que $n = p^r k + 1$ e $2m = p^s l + 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$\begin{aligned}
(x^n + y^m - 1)(-x^n + y^m + 1) = 0 &\iff y^{2m} - x^{2n} + 2x^n - 1 - 0 \\
&\iff (y^l)^{p^s} y - (x^{2w})^{p^s} x^2 + 2(x^k)^{p^s} x - 1 = 0.
\end{aligned} \tag{29}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (29) obtemos a cônica projetiva $\mathcal{G}_4 : \beta YZ - \alpha^2 X^2 + 2\alpha XZ - Z^2 = 0$.

Como $\mathcal{G}_4$ é projetivamente equivalente a $\mathcal{F}_4 : ZY - X^2 + 2XZ - Z^2 = 0$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(f) Com um raciocínio análogo ao item anterior e fazendo a transformação projetiva $(X : Y : Z) \mapsto (Y : X : Z)$, obtemos a cônica projetiva $\mathcal{F}_4 : ZY - X^2 + 2XZ - Z^2 = 0$ e concluímos que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(g) Considere inteiros r, s, k, l tais que $n = p^r k + 1$ e $m = p^s l + 2$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$(x^n + y^m - 1) = 0 \iff (x^w)^{p^s} x^1 + (y^l)^{p^s} y^2 - 1 = 0; \tag{30}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (30) obtemos a cônica projetiva $\mathcal{G}_5 : \alpha XZ + \beta Y^2 - Z^2 = 0$.

Como $\mathcal{G}_5$ é projetivamente equivalente a $\mathcal{F}_5 : XZ + Y^2 - Z^2 = 0$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(h) Com um raciocínio análogo ao item anterior e fazendo a transformação projetiva $(X : Y : Z) \mapsto (Y : X : Z)$, obtemos a cônica projetiva $\mathcal{F}_5 : XZ + Y^2 - Z^2 = 0$ e concluímos que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(i) Considere inteiros r, s, k, l tais que $n = p^r k + 1$ e $m = p^s l - 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$(x^n + y^m - 1) = 0 \iff (x^w)^{p^s} x + (y^l)^{p^s} y^{-1} - 1 = 0 \iff (x^w)^{p^s} xy + (y^l)^{p^s} - y = 0 \tag{31}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (35) obtemos a cônica projetiva $\mathcal{G}_6 : \alpha XY + \beta Z^2 - YZ = 0$.

Como $\mathcal{G}_6$ é projetivamente equivalente a $\mathcal{F}_6 : XY - YZ + Z^2 = 0$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(j) Com um raciocínio análogo ao item anterior e fazendo a transformação projetiva $(X : Y : Z) \mapsto (Y : X : Z)$, obtemos a cônica projetiva $\mathcal{F}_6 : XY - YZ + Z^2 = 0$ e concluímos que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

□

Teorema 2.3.7. *Supondo $p > 5$, a curva $\mathcal{F}$ é não clássica em relação à $\sum_2$ se, e somente se, umas das condições é válida:*

(a) $p|(m-2)$ *e* $p|(n-2)$;

(b) $p|(m+1)$ *e* $p|(n+1)$;

(c) $p|(2m-1)$ *e* $p|(2n-1)$;

(d) $p|(m-1)$ *e* $p|(n-1)(n-2)(2n-1)(n+1)$;

(e) $p|(n-1)$ *e* $p|(m+1)(m-2)(2m-1)$.

Demonstração. A demonstração segue diretamente das proposições 2.3.1, 2.3.5 e 2.3.6. □

2.4 $\mathbb{F}_q$-FROBENIUS CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_2$

Nesta seção iremos considerar $p > 5$ e $\mathcal{H}_P$ irá denotar a cônica osculante de $\mathcal{F}$ em P.

Para a nossa demonstração vamos adaptar de [3] as próximas duas proposições para o nosso caso das cônicas.

Proposição 2.4.1. Suponha $p > 5$, $\mathcal{F}$ clássica em relação à $\sum_1$ e não clássica em relação à $\sum_2$. Para $P = (u : v : 1) \in \mathcal{F}, uv \neq 0$, a cônica osculante $\mathcal{H}_P$ de $\mathcal{F}$ em P é a curva projetiva irredutível $\mathcal{H}_P(X, Y, Z)$, tal que:

$$\mathcal{H}_P(X,Y,Z): \begin{cases} au^{n-2}X^2 + bv^{m-2}Y^2 - Z^2 = 0, \text{ se } p \mid (m-2) \text{ e } p|(n-2); \\ au^{n+1}YZ + bv^{m+1}XZ - XY = 0, \text{ se } p \mid (m+1) \text{ e } p|(n+1); \\ a^4u^{(4n-2)}X^2 + b^4v^{(4m-2)}Y^2 + Z^2 - 2a^2b^2u^{(2n-1)}v^{(2m-1)}XY - 2a^2u^{(2n-1)}XZ - \\ \qquad 2b^2v^{(2m-1)}YZ = 0, \text{se } p \mid (2m-1) \text{ e } p|(2n-1); \\ b^2v^{2m-1}YZ - a^2u^{2n-2}X^2 + 2au^{n-1}XZ - Z^2 = 0, \text{ se } p \mid (2m-1) \text{ e } p|(n-1); \\ au^{n-1}XY + bv^{m+1}Z^2 - YZ = 0, \text{ se } p|(m+1) \text{ e } p|(n-1); \\ au^{n-1}XZ + bv^{m-2}Y^2 - Z^2 = 0, \text{ se } p|(m-2) \text{ e } p|(n-1); \\ au^{n-2}X^2 + bv^{m-1}YZ - Z^2 = 0, \text{se } p|(m-1) \text{ e } p|(n-2); \\ a^2u^{2n-1}XZ - b^2v^{2m-2}Y^2 + 2bv^{m-1}YZ - Z^2 = 0, \text{ se } p|(m-1) \text{ e } p|(2n-1); \\ bv^{m-1}YX + au^{n+1}Z^2 - XZ = 0, \text{ se } p|(m-1) \text{ e } p|(n+1). \end{cases}$$

Demonstração. A demonstração é análoga a feita na proposição 2.3.6 para todos os itens. □

Proposição 2.4.2. Se $\mathcal{F}$ é clássica em relação à $\sum_1$ e não clássica em relação à $\sum_2$, então as seguintes afirmações são válidas:

(a) A sequência de ordens de $\mathcal{F}$ em relação à $\sum_2$ é $(0,1,2,3,4,p^r)$, para algum $r > 0$.

(b) A curva $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $\varphi_q(P) \in \mathcal{H}_P$ para infinitos pontos $P \in \mathcal{F}$.

Demonstração. Suponha que $(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5)$ seja a sequência de ordem de $\mathcal{F}$ em relação à $\sum_2$ e que $\varepsilon_4 > 4$. Assim temos que $\varepsilon_4 \geq p$ e portanto $\varepsilon_5 > p$. Considere $P \in \mathcal{F}$, tal que $j_i(P) = \varepsilon_i$ para todo $i \in \{0,1,2,3,4,5\}$. Considere agora uma cônica $\mathcal{C}_P$ tal que $I(P, \mathcal{F} \cap \mathcal{C}_P) = \varepsilon_4 \geq p$ e seja $\mathcal{H}_P$ a cônica osculante de $\mathcal{F}$ em P. Como $\mathcal{H}_P \neq \mathcal{C}_P$, por [3, Lemma 3.3] temos que $I(P, \mathcal{H}_P \cap \mathcal{C}_P) > p > 4 = deg(\mathcal{H}_P) \cdot deg(\mathcal{C}_P)$.

Assim pelo Teorema de Bézout $\mathcal{H}_P$ e $\mathcal{C}_P$ possuem uma componente em comum. Porém pela proposição 2.4.1 a cônica osculante é irredutível. Assim, $\mathcal{H}_P = \mathcal{C}_P$, o que é uma contradição. Portanto $\varepsilon_4 = 4$ e assim $\varepsilon_i = i$ para $0 \leq i \leq 4$. Agora segue de [10, Proposition 2] e da proposição 2.4.1 que $\varepsilon_5 = p^r$ para algum $r > 0$. A segunda afirmação segue de (a) e de (7). □

Proposição 2.4.3. Seja $p > 5$ e suponha que $p|(n-2)$ e $p|(m-2)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $m = n = \frac{2(q-1)}{p^r-1}$ com $r < h$ tal que $r|h$ e $a, b \in \mathbb{F}_{p^r}$.

Demonstração. Pelas proposições 2.4.1 e 2.4.2(b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n-2+2q} + by^{m-2+2q} - 1 = 0 \iff by^{m-2+2q} = 1 - ax^{n-2+2q}. \tag{32}$$

Observe que podemos reescrever (32) como:

$$y^{m-2+2q} - \left(\frac{1}{b} - \frac{a}{b}x^{n-2+2q}\right) = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Usando 2.4.2 (b) temos que $y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right)$ divide $y^{m-2+2q} - \left(\frac{1}{b} - \frac{a}{b}x^{n-2+2q}\right)$ e por 2.2.1 vem que $m \mid m-2+2q$ e, portanto, $m|2q-2$, ou seja, $2q-2 = mt$, para algum inteiro t.

Note agora que:

$$by^{m-2+2q} = by^{m+mt} = by^{m(1+t)}.$$

Assim, usando a equação de $\mathcal{F}$, obtemos:

$$by^{m(1+t)} = (1-ax^n)^{(1+t)}/b^t. \tag{33}$$

Portanto de (32) e (33) temos que:

$$1 - ax^{n-2+2q} = (1-ax^n)^{(1+t)}/b^t.$$

Comparando o grau de ambos os lados, obtemos:

$$n-2+2q = n(1+t) \iff -2+2q = nt \iff mt = nt \iff m = n.$$

Agora basta usar o Teorema 1.3.5 para concluir a demonstração. □

Proposição 2.4.4. Seja $p > 5$ e suponha que $p|(n+1)$ e $p|(m+1)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $m = n$, $q = n+1$ e $a+b = 1$.

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n+1}y^q + by^{m+1}x^q - x^q y^q = 0. \tag{34}$$

Vamos inicialmente supor que $n+1-q < 0$, neste caso podemos reescrever (34) como

$$ax^{n+1}y^q + by^{m+1}x^q - x^q y^q = 0 \iff ay^{q-m-1} + bx^{q-n-1} - x^{q-n-1}y^{q-m-1} = 0.$$

Usando a proposição 2.4.2 (b) temos que $ax^n + by^m - 1$ divide $ay^{q-m-1} + bx^{q-n-1} - x^{q-n-1}y^{q-m-1}$, ou seja,

$$ay^{q-m-1} + bx^{q-n-1} - x^{q-n-1}y^{q-m-1} = (ax^n + by^m - 1)h(x,y) \tag{35}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$. Substituindo $x = 0$ em (35) temos que

$$ay^{q-m-1} = (by^m - 1)h(0,y)$$

o que é contradição.

Assim podemos supor que $n+1-q \geq 0$ e podemos reescrever (34) como

$$ax^{n+1}y^q + by^{m+1}x^q - x^q y^q = 0 \iff by^{m+1-q} = 1 - ax^{n+1-q}. \tag{36}$$

Observe que podemos então reescrever (36) como:

$$y^{m+1-q} - \left(\frac{1}{b} - \frac{a}{b}x^{n+1-q}\right) = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Usando novamente a proposição 2.4.2 (b) temos que $y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right)$ divide $y^{m+1-q} - \left(\frac{1}{b} - \frac{a}{b}x^{n+1-q}\right)$ e pelo Lema 2.2.1 vem que $m \mid m+1-q$ e, portanto, $m|1-q$, ou seja, $1-q = mt$, para algum inteiro t.

Note agora que:

$$by^{m+1-q} = by^{m+mt} = by^{m(1+t)}.$$

Assim, usando a equação de $\mathcal{F}$, obtemos:

$$by^{m(1+t)} = (1-ax^n)^{(1+t)}/b^t. \tag{37}$$

Portanto de (36) e (37) temos que:

$$1 - ax^{n+1-q} = (1-ax^n)^{(1+t)}/b^t.$$

Comparando o grau de ambos os lados, obtemos:

$$n+1-q = n(1+t) \iff -1-q = nt \iff mt = nt \iff n = m.$$

Usando o Teorema 1.3.5 vamos supor que $p|(n-1)$ e usar o fato que $p|(n+1)$, logo concluímos que $p|(2n)$ e assim temos que $p|n$, o que é uma contradição com as hipóteses iniciais. Usando os casos (2) e (3) do Teorema 1.3.5 chegamos, de maneira análoga, também a uma contradição. Note porém que podemos ter o caso $t = 1$ e portanto $q = n+1$ e $a+b = 1$ que satisfaz todas as condições, e assim concluímos a demonstração. □

Proposição 2.4.5. Seja $p > 5$ e suponha que $p|(2n-1)$ e $p|(2m-1)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $m = n = \frac{q-1}{2(p^r-1)}$ com $r < h$ tal que $r \mid h$ e $a^2, b^2 \in \mathbb{F}_{p^r}$;

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$a^4x^{4n-2+2q} + b^4y^{4m-2+2q} + 1 - 2a^2b^2x^{2n-1+q}y^{2m-1+q} - 2a^2x^{2n-1+q} - 2b^2y^{2m-1+q} = 0 \iff$$

$$b^4y^{4m-2+2q} = -a^4x^{4n-2+2q} - 1 + 2a^2b^2x^{2n-1+q}y^{2m-1+q} + 2a^2x^{2n-1+q} + 2b^2y^{2m-1+q} \iff$$

$$b^4y^{4m-2+2q} = -a^4x^{4n-2+2q} - 1 + y^{2m-1+q}(2a^2b^2x^{2n-1+q} + 2b^2) + 2a^2x^{2n-1+q}. \tag{38}$$

Usando a proposição 2.4.2 (b) temos que $ax^n + by^m - 1$ divide $a^4x^{4n-2+2q} + b^4y^{4m-2+2q} + 1 - 2a^2b^2x^{2n-1+q}y^{2m-1+q} - 2a^2x^{2n-1+q} - 2b^2y^{2m-1+q}$, ou seja,

$$\left(b^2y^{2m-1+q} - 1\right)^2 + \left(a^4x^{4n-2+2q} - 2a^2b^2x^{2n-1+q}y^{2m-1+q} - 2a^2x^{2n-1+q}\right) = (ax^n + by^m - 1)h(x,y), \tag{39}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$. Subsituindo $x = 0$ em (39) temos que

$$\left(b^2y^{2m-1+q} - 1\right)^2 = (by^m - 1)h(0,y)$$

e consequentemente $m \mid 2m - 1 + q$, logo $m|q-1$, ou seja, $q - 1 = mt$, para algum inteiro t.

Utilizando a equação da curva, podemos escrever:

$$y^{2m-1+q} = (y^m)^{2+t} = (1 - ax^n)^{2+t}/b^{2+t}.$$

Substituindo a expressão anterior em (38), obtemos:

$$b^4y^{4m-2+2q} = -a^4x^{4n-2+2q} - 1 + ((1 - ax^n)^{2+t}/b^{2+t})(2a^2b^2x^{2n-1+q} + 2b^2) + 2a^2x^{2n-1+q}. \tag{40}$$

As opções para o grau no 2º membro de (40) são: $4n - 2 + 2q = 4n + 2(q-1)$ ou $n(2+t) + 2n - 1 + q = 4n + q - 1 + nt$.

Observe que na hipótese que fizemos no início do capítulo, sem perda de generalidade, obtemos $n \geq m \iff nt \geq mt \iff nt \geq q - 1 \iff 4n + q - 1 + nt \geq 4n + 2(q-1)$. Assim, o grau do 2º membro de (40) será $4n + q - 1 + nt$.

Note agora que:

$$b^4y^{4m-2+2q} = b^4y^{4m+2mt} = b^4y^{m(4+2t)}.$$

Usando a equação de $\mathcal{F}$, obtemos:

$$b^4y^{m(4+2t)} = (1 - ax^n)^{(4+2t)}/b^{2t}. \tag{41}$$

Portanto de (40) e (41) temos que:

$$-a^4x^{4n-2+2q} - 1 + ((1 - ax^n)^{2+t}/b^{2+t})(2a^2b^2x^{2n-1+q} + 2b^2) + 2a^2x^{2n-1+q} = (1 - ax^n)^{(4+2t)}/b^{2t}.$$

Comparando o grau de ambos os lados, obtemos:

$$4n + q - 1 + nt = n(4 + 2t) \iff q - 1 = nt \iff n = \frac{q-1}{t} \iff n = m.$$

Agora basta usar o Teorema 1.3.5 para concluir a demonstração. □

Proposição 2.4.6. Seja $p > 5$ e suponha que $p|(n-1)$ e $p|(m-1)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $m = n = \frac{q-1}{p^r-1}$ para algum inteiro $r < h$ e $a, b \in \mathbb{F}_{p^r}$.

Demonstração. A demonstração segue diretamente do Teorema 2.2.2 e do fato explicado na demonstração da proposição 2.3.1. □

Proposição 2.4.7. Seja $p > 5$ e suponha que $p|(n-2)$ e $p|(m-1)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $n = 2m = \frac{2(q-1)}{p^r-1}$ com $r < h$ tal que $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$.

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n-2+2q} + by^{m-1+q} - 1 = 0 \iff by^{m-1+q} = 1 - ax^{n-2+2q}. \tag{42}$$

Observe que podemos reescrever (42) como:

$$y^{m-1+q} - \left(\frac{1}{b} - \frac{a}{b}x^{n-2+2q}\right) = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Usando a proposição 2.4.2 (b) temos que $y^m - \left(\frac{1}{b} - \frac{ax^n}{b}\right)$ divide $y^{m-1+q} - \left(\frac{1}{b} - \frac{ax^{n-2+2q}}{b}\right)$ e pelo Lema 2.2.1 vem que $m \mid m - 1 + q$ e, portanto, $m|q-1$, ou seja, $q - 1 = mt$, para algum inteiro t.

Note agora que:

$$by^{m-1+q} = by^{m+mt} = by^{m(1+t)}.$$

Assim, usando a equação de $\mathcal{F}$, obtemos:

$$by^{m(1+t)} = (1 - ax^n)^{(1+t)}/b^t. \tag{43}$$

Portanto de (42) e (43) temos que:

$$1 - ax^{n-2+2q} = (1 - ax^n)^{(1+t)}/b^t.$$

Comparando o grau de ambos os lados, obtemos:

$$n - 2 + 2q = n(1+t) \iff -2 + 2q = nt \iff 2mt = nt \iff n = 2m.$$

Sendo $n = 2m$ e usando novamente o lema 2.2.1 temos que $m|(m-1+q)$ e

$$\left(\frac{1}{b} - \frac{a}{b}x^{n-2+2q}\right) = \left(\frac{1}{b} - \frac{a}{b}x^n\right)^{\frac{m-1+q}{m}} \Longrightarrow \left(\frac{1}{b} - \frac{a}{b}x^{2m-2+2q}\right) = \left(\frac{1}{b} - \frac{a}{b}x^{2m}\right)^{1+\frac{-1+q}{m}}. \quad (44)$$

Note que (44) implica que $\frac{q-1}{m} = p^r - 1$ para algum $r > 0$ e, consequentemente $(p^r - 1)|q-1$. Nas condições dadas temos que $r < h$, $r|h$ e podemos escrever $n = 2m = \frac{2(q-1)}{p^r-1}$. Observe ainda que de (44) concluímos que $a, b \in \mathbb{F}_{p^r}$.

Observe que a recíproca pode facilmente ser observada, pois $m + q - 1 = m + mt = m(1+t)$, assim $m|(m+q-1)$. Note ainda que nas condições dadas:

$$\left(\frac{1}{b} - \frac{a}{b}x^n\right)^{1+\frac{q-1}{m}} = \left(\frac{1}{b} - \frac{a}{b}x^n\right)^{p^r} = \frac{1}{b} - \frac{a}{b}x^{np^r} = \frac{1}{b} - \frac{a}{b}x^{n+2q-2} \Longrightarrow \left(\frac{1}{b} - \frac{a}{b}x^{n+2q-2}\right) = \left(\frac{1}{b} - \frac{a}{b}x^n\right)^{\frac{m-1+q}{m}}.$$

Assim usando o Lema 2.2.1 concluímos que a recíproca também é válida. □

Proposição 2.4.8. Seja $p > 5$ e suponha que $p|(2n-1)$ e $p|(m-1)$. Então a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_2$.

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$a^2x^{2n-1+q} - b^2y^{2m-2+2q} + 2by^{m-1+q} - 1 = 0 \iff a^2x^{2n-1+q} = b^2y^{2m-2+2q} - 2by^{m-1+q} + 1. \quad (45)$$

Observe que podemos reescrever (45) como:

$$x^{2n-1+q} - \left(\frac{by^{m-1+q} - 1}{a}\right)^2 = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$x^n - \left(\frac{1}{a} - \frac{b}{a}y^m\right) = 0.$$

Usando a proposição 2.4.2 (b) temos que $x^n - \left(\frac{1}{a} - \frac{b}{a}y^m\right)$ divide $x^{2n-1+q} - \left(\frac{by^{m-1+q}-1}{a}\right)^2$ e pelo Lema 2.2.1 vem que $n \mid 2n-1+q$ e, portanto, $n|q-1$, ou seja, $q-1 = nt$, para algum inteiro t.

Assim usando a equação de $\mathcal{F}$, obtemos:

$$a^2x^{2n-1+q} = a^2x^{n(2+t)} = (1-by^m)^{2+t}/a^t. \tag{46}$$

Portanto, de (45) e (46) temos que:

$$b^2y^{2m-2+2q} - 2by^{m-1+q} + 1 = (1-by^m)^{2+t}/a^t.$$

Comparando o grau de ambos os lados, obtemos:

$$2m-2+2q = m(2+t) \iff 2(q-1) = mt \iff 2n = m.$$

Como estamos supondo que $n \geq m$, temos uma contradição. □

Proposição 2.4.9. Seja $p > 5$ e suponha ainda que $p|(n+1)$ e $p|(m-1)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_2$.

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$by^{m-1+q}x^q + ax^{n+1} - x^q = 0 \tag{47}$$

Vamos inicialmente supor que $n+1-q < 0$, neste caso podemos reescrever (47) como

$$by^{m-1+q}x^q + ax^{n+1} - x^q = 0 \iff by^{m-1+q}x^{q-n-1} + a - x^{q-n-1} = 0$$

Usando a proposição 2.4.2 (b) temos que $ax^n + by^m - 1$ divide $by^{m-1+q}x^{q-n-1} + a - x^{q-n-1}$, ou seja,

$$by^{m-1+q}x^{q-n-1} + a - x^{q-n-1} = (ax^n + by^m - 1)h(x,y) \tag{48}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$.

Substituindo $x = 0$ em (48) temos que

$$a = (by^m - 1)h(0,y)$$

o que é uma contradição.

Assim podemos supor que $n+1-q \geq 0$ e podemos reescrever (47) como

$$by^{m-1+q}x^q + ax^{n+1} - x^q = 0 \iff by^{m-1+q} = 1 - ax^{n+1-q} \tag{49}$$

Observe que podemos reescrever (49) como:

$$y^{m-1+q} - \left(\frac{1}{b} - \frac{a}{b}x^{n+1-q}\right) = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Usando a proposição 2.4.2 (b) temos que $y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right)$ divide $y^{m-1+q} - \left(\frac{1}{b} - \frac{a}{b}x^{n+q-1}\right)$ e pelo Lema 2.2.1 vem que $m \mid m-1+q$ e, portanto, $m|q-1$, ou seja, $q-1 = mt$, para algum inteiro t.

Assim usando a equação de $\mathcal{F}$, obtemos:

$$by^{m-1+q} = by^{m(1+t)} = (1-ax^n)^{1+t}/b^t. \tag{50}$$

Portanto, de (49) e (50) temos que:

$$1 - ax^{n+1-q} = (1-ax^n)^{1+t}/b^t.$$

Comparando o grau de ambos os lados, obtemos:

$$n+1-q = n(1+t) \iff 1-q = nt \iff n = -m.$$

Como estamos supondo que $n \geq m$, temos uma contradição. □

Proposição 2.4.10. Seja $p > 5$ e suponha ainda que $p|(n-1)$ e $p|(2m-1)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $2m = n = \frac{q-1}{p^r-1}$ com $r < h$ tal que $r|h$ e $a, b \in \mathbb{F}_{p^r}$.

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$b^2y^{2m-1+q} - a^2x^{2n-2+2q} + 2ax^{n-1+q} - 1 = 0 \iff b^2y^{2m-1+q} = a^2x^{2n-2+2q} - 2ax^{n-1+q} + 1. \tag{51}$$

Observe que podemos reescrever (51) como:

$$y^{2m-1+q} - \left(\frac{ax^{n-1+q} - 1}{b}\right)^2 = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Usando a proposição 2.4.2 (b) temos que $y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right)$ divide $y^{2m-1+q} - \left(\frac{ax^{n-1+q}-1}{b}\right)^2$ e pelo Lema 2.2.1 vem que $m \mid 2m-1+q$ e, portanto, $m|q-1$, ou seja, $q-1 = mt$, para algum inteiro t.

Assim usando a equação de $\mathcal{F}$, obtemos:

$$b^2y^{2m-1+q} = b^2y^{m(2+t)} = (1-ax^n)^{2+t}/b^t. \tag{52}$$

Portanto, de (51) e (52) temos que:

$$a^2x^{2n-2+2q} - 2ax^{n-1+q} + 1 = (1-ax^n)^{2+t}/b^t.$$

Comparando o grau de ambos os lados, obtemos:

$$2n-2+2q = n(2+t) \iff 2(q-1) = nt \iff n = 2m.$$

Sendo $n = 2m$ e usando novamente o Lema 2.2.1 temos que $m|(2m-1+q)$ e

$$\left(\frac{1}{b} - \frac{a}{b}x^{n-1+q}\right)^2 = \left(\frac{1}{b} - \frac{a}{b}x^n\right)^{\frac{2m-1+q}{m}} \Longrightarrow \left(\frac{1}{b} - \frac{a}{b}x^{n-1+q}\right) = \left(\frac{1}{b} - \frac{a}{b}x^n\right)^{1+\frac{-1+q}{n}}. \tag{53}$$

Note que (53) implica que $\frac{q-1}{n} = p^r - 1$ para algum $r > 0$ e, consequentemente $(p^r-1)|q-1$. Nas condições dadas temos que $r < h$, $r|h$ e podemos escrever $2m = n = \frac{q-1}{p^r-1}$. Observe ainda que de (53) concluímos que $a, b \in \mathbb{F}_{p^r}$.

Observe que a recíproca pode facilmente ser observada, pois $2m+q-1 = 2m+mt = m(2+t)$, assim $m|(2m+q-1)$. Note ainda que nas condições dadas:

$$\left(\frac{1}{b} - \frac{a}{b}x^n\right)^{1+\frac{1+q}{n}} = \left(\frac{1}{b} - \frac{a}{b}x^n\right)^{p^r} = \frac{1}{b} - \frac{a}{b}x^{np^r} = \frac{1}{b} - \frac{a}{b}x^{n-1+q} \Longrightarrow \left(\frac{1}{b} - \frac{a}{b}x^{n-1+q}\right)^2 = \left(\frac{1}{b} - \frac{a}{b}x^n\right)^{\frac{2m-1+q}{m}}.$$

Assim usando o Lema 2.2.1 concluímos que a recíproca também é válida. □

Proposição 2.4.11. Seja $p > 5$ e suponha ainda que $p|(n-1)$ e $p|(m-2)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius clássica.

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n-1+q} + by^{m-2+2q} - 1 = 0 \iff by^{m-2+2q} = 1 - ax^{n-1+q}. \tag{54}$$

Observe que podemos reescrever (54) como:

$$y^{m-2+2q} - \left(\frac{1}{b} - \frac{a}{b}x^{n-1+q}\right) = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Usando a proposição 2.4.2 (b) temos que $y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right)$ divide $y^{m-2+2q} - \left(\frac{1}{b} - \frac{a}{b}x^{n-1+q}\right)$ e pelo Lema 2.2.1 vem que $m \mid m-2+2q$ e, portanto, $m|2q-2$, ou seja, $2q-2 = mt$, para algum inteiro t.

Assim usando a equação de $\mathcal{F}$, obtemos:

$$by^{m-2+2q} = by^{m(1+t)} = (1-ax^n)^{1+t}/b^t. \tag{55}$$

Portanto, de (54) e (55) temos que:

$$1 - ax^{n-1+q} = (1-ax^n)^{1+t}/b^t.$$

Comparando o grau de ambos os lados, obtemos:

$$n - 1 + q = n(1+t) \iff m = 2n.$$

Como estamos supondo que $n \geq m$, temos uma contradição. □

Proposição 2.4.12. Seja $p > 5$ e suponha ainda que $p|(n-1)$ e $p|(m+1)$. Então, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_2$.

Demonstração. Pelas proposições 2.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n-1+q}y^q + by^{m+1} - y^q = 0. \tag{56}$$

Vamos inicialmente supor que $m+1-q < 0$, neste caso podemos reescrever (56) como

$$ax^{n-1+q}y^q + by^{m+1} - y^q = 0 \iff ax^{n-1+q}y^{q-m-1} + b - y^{q-m-1} = 0.$$

Usando a proposição 2.4.2 (b) temos que $ax^n + by^m - 1$ divide $ax^{n-1+q}y^{q-m-1} + b - y^{q-m-1}$, ou seja,

$$ax^{n-1+q}y^{q-m-1} + b - y^{q-m-1} = (ax^n + by^m - 1)h(x,y) \tag{57}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$.

Substituindo $y = 0$ em (57) temos que

$$b = (ax^n - 1)h(x, 0)$$

o que é uma contradição.

Assim podemos supor que $m + 1 - q \geq 0$ e podemos reescrever (56) como

$$ax^{n-1+q}y^q + by^{m+1} - y^q = 0 \iff by^{m+1-q} = 1 - ax^{n-1+q} \tag{58}$$

Observe que podemos assim reescrever (58) como:

$$y^{m+1-q} - \left(\frac{1}{b} - \frac{a}{b}x^{n-1+q}\right) = 0.$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right) = 0.$$

Usando a proposição 2.4.2 (b) temos que $y^m - \left(\frac{1}{b} - \frac{a}{b}x^n\right)$ divide $y^{m+1-q} - \left(\frac{1}{b} - \frac{a}{b}x^{n-1+q}\right)$ e pelo Lema 2.2.1 vem que $m \mid m + 1 - q$ e, portanto, $m|1 - q$, ou seja, $1 - q = mt$, para algum inteiro t.

Assim usando a equação de $\mathcal{F}$, obtemos:

$$by^{m+1-q} = by^{m(1+t)} = (1 - ax^n)^{1+t}/b^t. \tag{59}$$

Portanto, de (58) e (59) temos que:

$$1 - ax^{n-1+q} = (1 - ax^n)^{1+t}/b^t.$$

Comparando o grau de ambos os lados, obtemos:

$$n - 1 + q = n(1 + t) \iff n = -m.$$

Assim temos que tal condição é uma contradição e portanto concluímos a demonstração. □

Teorema 2.4.13. *Suponha $p > 5$ e $q = p^h$. A curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, uma das condições é válida:*

(a) $p|(n-1)$ *e* $m = n = \frac{q-1}{p^r-1}$ *com* $r < h$ *e* $a, b \in \mathbb{F}_{p^r}$;

(b) $p|(n-2)$ *e* $m = n = \frac{2(q-1)}{p^r-1}$ *com* $r < h$ *tal que* $r \mid h$ *e* $a, b \in \mathbb{F}_{p^r}$;

(c) $p|(2n-1)$ *e* $m = n = \frac{q-1}{2(p^r-1)}$ *com* $r < h$ *tal que* $r \mid h$ *e* $a^2, b^2 \in \mathbb{F}_{p^r}$;

(d) $p|(n+1)$ *e* $q = n+1 = m+1$ *e* $a+b = 1$;

(e) $p|(n-1)$ *e* $n = 2m = \frac{q-1}{p^r-1}$ *com* $r < h$ *tal que* $r \mid h$ *e* $a, b \in \mathbb{F}_{p^r}$;

(f) $p|(n-2)$ *e* $n = 2m = \frac{2(q-1)}{p^r-1}$ *com* $r < h$ *tal que* $r \mid h$ *e* $a, b \in \mathbb{F}_{p^r}$.

Demonstração. Segue diretamente das proposições 2.4.3, 2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8, 2.4.9, 2.4.10, 2.4.11 e 2.4.12. □

2.5 A QUANTIDADE DE PONTOS RACIONAIS

Vamos determinar $N(\mathcal{F})$ para os casos dados pelo Teorema 2.4.13. Os casos $(a), (b)$ e (c) podem ser encontrados em [9] e aqui nos limitaremos apenas a enunciá-los. Para os casos $(d), (e)$ e (f) iremos fazer a demonstração.

Teorema 2.5.1. *Seja* $n = m = \frac{q-1}{p^r-1}$ *com* $r < h$, $r \mid h$ *e* $a, b \in \mathbb{F}_{p^r}$, *então*

$$N(\mathcal{F}) = n(q-n+2).$$

Demonstração. A demonstração pode ser encontrada em [9, 2.(vi)]. □

Teorema 2.5.2. *Seja* $n = m = \frac{2(q-1)}{p^r-1}$ *com* $r < h$, *tal que* $r \mid h$ *e* $a, b \in \mathbb{F}_{p^r}$. *Considere ainda* $\psi(\alpha) = 1$ *se* α *é um quadrado e* $\psi(\alpha) = 0$ *caso contrário. Então*

$$N(\mathcal{F}) = \frac{n^2}{4}(p^r + 1 - 2(\psi(a) + \psi(b) + \psi(-ab))) + n(\psi(a) + \psi(b) + \psi(-ab)).$$

Demonstração. A demonstração pode ser encontrada em [9, 2.(viii)] □

Teorema 2.5.3. *Seja* $n = m = \frac{q-1}{2(p^r-1)}$ *com* $r < h$, *tal que* $r \mid h$ *e* $a^2, b^2 \in \mathbb{F}_{p^r}$, *então*

$$N(\mathcal{F}) = n^2(p^r - 2) + 3n.$$

Demonstração. A demonstração pode ser encontrada em [9, 2.(vii)]. □

Teorema 2.5.4. *Seja* $q = n+1 = m+1$ *e* $a+b = 1$, *então*

$$N(\mathcal{F}) = (q-1)^2.$$

Demonstração. Considere a curva de Fermat $\mathcal{F} : ax^{q-1} + (1-a)y^{q-1} = 1$. Note que tal curva não possui pontos no infinito, assim, supondo α e β racionais não nulos temos que $a\alpha^{q-1} + (1-a)\beta^{q-1} = a + (1-a) = 1$. Como há $q-1$ pontos racionais em F_q^* temos que $N(\mathcal{F}) = (q-1)^2$. □

Para a demonstração dos dois últimos casos, vamos definir o conceito de transformação geométrica e dois teoremas cuja demonstração pode ser encontrada em [11].

Definição 2.5.5. A transformação geométrica na curva $\mathcal{G} : g(x,y) = 0$ com um ponto de multiplicidade r na origem é a curva $\mathcal{G}' : g'(x,y) = 0$ tal que

$$g'(x,y) = g(x,xy)/x^r.$$

Teorema 2.5.6. *Se $O = (0,0)$ é um ponto singular ordinário na curva $\mathcal{G} : g(x,y) = 0$ de multiplicidade r, então:*

(i) O é o centro de exatamente r ramos de $\mathcal{G}$;

(ii) os r ramos são todos lineares.

Demonstração. A demonstração pode ser encontrada em [11, Theorem 4.45]. □

Teorema 2.5.7. *Seja $P \in \mathbb{P}^2(\mathbb{F}_q)$ um ponto singular de uma curva irredutível $\mathcal{G}$ definida sobre $\mathbb{F}_q$. Se γ é um ramo linear de $\mathcal{G}$ com centro P e ℓ é a reta tangente comum em P de $\mathcal{G}$ e γ, então γ é $\mathbb{F}_q$-Racional se, e somente se, ℓ está definida sobre $\mathbb{F}_q$.*

Demonstração. A demonstração pode ser encontrada em [11, Theorem 8.10]. □

Teorema 2.5.8. *Seja $n = 2m = \frac{q-1}{p^r-1}$ com $r < h$, tal que $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$. Então*

$$N(\mathcal{F}) = \frac{n^2}{2}(p^r - 2) + 2n$$

Demonstração. Considerando a curva projetiva $\mathcal{F} : aX^n + bY^{\frac{n}{2}}Z^{\frac{n}{2}} = Z^n$ o seu único ponto singular é $P = (0:1:0)$.

Como a função norma é sobrejetiva, temos que $a = \alpha^n$ para algum $\alpha \in \mathbb{F}_q$ e assim o número de pontos racionais de $\mathcal{F}$ sobre $\mathbb{F}_q$ é igual ao número de pontos racionais da curva projetiva $\mathcal{D} : X^n + bY^{\frac{n}{2}}Z^{\frac{n}{2}} = Z^n$ também sobre $\mathbb{F}_q$. Note que como $\mathcal{D}$ é singular precisamos determinar quantos pontos racionais temos para a equação de $\mathcal{D}$, e nesse caso, precisamos ainda determinar a quantidade de ramos de grau 1 de $\mathcal{D}$ centrados em P.

Inicialmente vamos analisar o caso para os pontos de $\mathcal{D}$ que são não singulares. Neste caso a curva é singular e, portanto, basta contar os pontos racionais de $\mathcal{D}$.

Considerando a situação acima, no caso em que $XYZ = 0$ a quantidade de pontos pontos racionais é $n + \frac{n}{2} = \frac{3n}{2}$.

Desomogeinizando com $Z = 1$, considere agora (x, y) com $xy \neq 0$ um ponto racional de $\mathcal{F}$, ou seja, $x^n + by^{\frac{n}{2}} = 1 \iff by^{\frac{n}{2}} = 1 - x^n$ e, portanto, $y^{\frac{n}{2}} \in \mathbb{F}_{p^r}$. Neste caso há $n \cdot \frac{n}{2}(p^r - 2) = \frac{n^2}{2}(p^r - 2)$ pontos racionais e assim, a quantidade de pontos racionais na condição dos pontos não singulares, é dada por $\frac{n^2}{2}(p^r - 2) + \frac{3n}{2}$.

Vamos agora determinar quantos ramos racionais de $\mathcal{D}$ centrados em P temos.

Desomogeinizando $\mathcal{D}$ em relação à variável Y obtemos $x^n + bz^{\frac{n}{2}} - z^n = 0$, que é equivalente a $bz^m + x^{2m} - z^{2m} = 0$. Como $m_P(\mathcal{D}) = m$, fazendo a transformação geométrica obtemos $g'(x, z) = bz^m + x^m - x^m z^{2m}$. Note que $g'_m = bz^m + x^m$ e assim $m_P(\mathcal{D}') = m$, sendo P um ponto singular ordinário. Note ainda que todas as m retas tangentes estão definidas sobre $\mathbb{F}_q$ e portanto pelos Teoremas 2.5.6 e 2.5.7 temos exatamente $m = \frac{n}{2}$ ramos centrados em P, todos eles são lineares e racionais.

Portanto, $N(\mathcal{F}) = \frac{n^2}{2}(p^r - 2) + \frac{3n}{2} + \frac{n}{2} \iff N(\mathcal{F}) = \frac{n^2}{2}(p^r - 2) + 2n$. □

Teorema 2.5.9. *Seja $n = 2m = \frac{2(q-1)}{p^r-1}$ com $r < h$, tal que $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$. Então*

$$N(\mathcal{F}) = \begin{cases} m^2(p^r - 3) + 4m, \text{ se } a \text{ é quadrado} \\ m^2(p^r - 1) + 2m, \text{ se } a \text{ não é quadrado} \end{cases}.$$

Demonstração. Considerando a curva projetiva $\mathcal{F} : aX^{2m} + bY^m Z^m = Z^{2m}$ o seu único ponto singular é $P = (0 : 1 : 0)$.

Suponha que a seja um quadrado em $\mathbb{F}_{p^r}$. Como a função norma é sobrejetiva, temos que $a = \alpha^{2m}$ e $b = \beta^m$ para algum $\alpha, \beta \in \mathbb{F}_q$ e assim, o número de pontos racionais de $\mathcal{F}$ sobre $\mathbb{F}_q$ é igual ao número de pontos racionais da curva projetiva $\mathcal{D} : X^{2m} + Y^m Z^m = Z^{2m}$ também sobre $\mathbb{F}_q$.

Caso a não seja um quadrado, considere apenas $b = \beta^n$ para algum $\beta \in \mathbb{F}_q$, e assim o número de pontos racionais de $\mathcal{F}$ sobre $\mathbb{F}_q$ é igual ao número de pontos racionais da curva $\mathcal{D} : aX^{2m} + Y^m Z^m = Z^{2m}$ também sobre $\mathbb{F}_q$.

Vamos usar os mesmos argumentos do Teorema anterior neste caso.

Inicialmente vamos analisar o caso para os pontos de $\mathcal{D}$ que são não singulares, para ambos os casos acima.

Considerando esta situação e analisando o caso $XYZ = 0$, a quantidade de pontos racionais é $m + 2m = 3m$ se a é um quadrado e m se a não é quadrado.

Desomogeinizando com $Z = 1$, considere agora (x, y) com $xy \neq 0$ um ponto racional de $\mathcal{F}$, ou seja, $x^{2m} + y^m = 1$ se a é quadrado e $ax^{2m} + y^m = 1$ se a não é quadrado. Neste caso há $m \cdot m(p^r - 3) = m^2(p^r - 3)$ pontos racionais no caso em que a é quadrado e $(p^r - 1)m^2$ no caso em que a não é quadrado assim, supondo todas as condições anteriores, a quantidade de pontos racionais é dada por $\begin{cases} m^2(p^r - 3) + 3m, \text{ se } a \text{ é quadrado} \\ m^2(p^r - 1) + m, \text{ se } a \text{ não é quadrado} \end{cases}$.

Vamos agora determinar a quantidade de ramos de grau 1 de $\mathcal{D}$ centrados em P.

Desomogeinizando a curva $\mathcal{D}$ em relação a variável Y obtemos $ax^{2m} + z^m - z^2m = 0$ e note que $m_P(\mathcal{D}) = m$. Fazendo a transformação geométrica obtemos $g'(x, z) = ax^m + z^m - x^m z^2 m$ e $g'_m = ax^m + z^m$ e assim $m_P(\mathcal{D}') = m$, sendo P um ponto singular ordinário. Note ainda que todas as m retas tangentes estão definidas sobre $\mathbb{F}_q$ e portanto por 2.5.6 e 2.5.7 temos exatamente $m = \frac{n}{2}$ ramos centrados em P, todos eles são lineares e racionais.

Portanto

$$N(\mathcal{F}) = \begin{cases} m^2(p^r - 3) + 4m, \text{ se } a \text{ é quadrado} \\ m^2(p^r - 1) + 2m, \text{ se } a \text{ não é quadrado} \end{cases}.$$

□

Vamos agora determinar uma cota para $N(\mathcal{F})$ nos casos em que $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius clássica.

Com as notações anteriores e as definições feitas na introdução deste trabalho, temos as seguintes expressões:

$$A(P_\xi) = \begin{cases} 4n - 10, & \text{se } P_\xi \in \Gamma(\mathbb{F}_q) \\ 2n - 6, & \text{caso contrário} \end{cases}$$

$$A(P_\rho) = \begin{cases} 4m - 10, & \text{se } P_\rho \in \Gamma(\mathbb{F}_q) \\ 2m - 6, & \text{caso contrário} \end{cases}$$

Sendo α e β a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^n - a^{-1}$ e $T^m - b^{-1}$ e, por [4] o gênero da curva expresso por $g = \frac{mn-m-n-mdc(m,n)+2}{2}$, uma cota melhor é dada por:

$$N(\mathcal{F}) \leq \frac{2(mn - m - n - mdc(m, n)) + (q + 5)n}{5} - \frac{\alpha(4n - 10) + (n - \alpha)(2n - 6) + \beta(4m - 10)}{5} - \frac{(m - \beta)(2m - 6)}{5}.$$

Corolário 2.5.10. Dada a curva projetiva $\mathcal{F} : aX^n + bY^m Z^{n-m} = Z^n$ definida sobre $\mathbb{F}_q$ tal que $a, b, \in \mathbb{F}_q^*$ e m e n inteiros positivos. Supondo $p > 5$ e $\mathcal{F}$ clássica em relação à $\sum_1$ uma das condições a seguir é válida:

(i) Se $n = m = \frac{q-1}{p^r-1}$ com $r < h$, $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$, então

$$N(\mathcal{F}) = n(q - n + 2);$$

(ii) Se $n = m = \frac{q-1}{2(p^r-1)}$ com $r < h$, tal que $r \mid h$ e $a^2, b^2 \in \mathbb{F}_{p^r}$, então $N(\mathcal{F}) = n^2(p^r - 2) + 3n$;

(iii) Se $n = m = \frac{q-1}{2(p^r-1)}$ com $r < h$, tal que $r \mid h$ e $a^2, b^2 \in \mathbb{F}_{p^r}$, então $N(\mathcal{F}) = n^2(p^r - 2) + 3n$;

(iv) Se $q = n + 1 = m + 1$ e $a + b = 1$, então $N(\mathcal{F}) = (q-1)^2$;

(v) Se $n = 2m = \frac{q-1}{p^r-1}$ com $r < h$, tal que $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$, então $N(\mathcal{F}) = \frac{n^2}{2}(p^r - 2) + 2n$;

(vi) Se $n = 2m = \frac{2(q-1)}{p^r-1}$ com $r < h$, tal que $r \mid h$ e $a, b \in \mathbb{F}_{p^r}$, então

$$N(\mathcal{F}) = \begin{cases} m^2(p^r - 3) + 4m, \text{ se } a \text{ é quadrado} \\ m^2(p^r - 1) + 2m, \text{ se } a \text{ não é quadrado} \end{cases};$$

(vii) Em todos os demais casos, uma cota para $N(\mathcal{F})$ é dada por:

$$N(\mathcal{F}) \leq \frac{2(mn - m - n - mdc(m,n)) + (q+5)n}{5} - \frac{\alpha(4n-10) + (n-\alpha)(2n-6) + \beta(4m-10)}{5} - \frac{(m-\beta)(2m-6)}{5}.$$

Sendo α e β a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^n - a^{-1}$ e $T^m - b^{-1}$.

3 CURVA $\mathcal{F} : a x^n y^m + b x^n + c y^m = 1$

Considere a curva $\mathcal{F} : ax^n y^m + bx^n + cy^m = 1$ definida sobre o corpo finito $\mathbb{F}_q$ tal que $a, b, c \in \mathbb{F}_q$, $c \neq -\frac{a}{b}$, $a \neq 0$ e m, n inteiros positivos. Vamos supor ainda que $p > 2$ daqui em diante e que $n \geq m$, sem perda de generalidade. Como a classicalidade da curva é uma propriedade geométrica, para as seções 3.1 e 3.3 vamos considerar que $b = c = 1$. Note ainda que $a \neq -1$, pois caso contrário a curva $\mathcal{F} : -x^n y^m + x^n + y^m - 1 = (y^m - 1)(-x^n + 1) = 0$ e, portanto, redutível.

3.1 CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_1$

Vamos determinar sobre quais condições a curva $\mathcal{F}$ é não clássica em relação à $\sum_1$.

Proposição 3.1.1. Para todo m, n inteiros positivos, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é clássica em relação à $\sum_1$.

Demonstração. Temos que $p \nmid n$, logo x é uma variável separante. De acordo com [18] a não classicalidade de $\mathcal{F}$ é equivalente a $D_x^{(2)} y = 0$.

Derivando, obtemos:

$$D_x^{(1)}(ax^n y^m + x^n + y^m) = 0 \iff nx^{-1}(ax^n y^m + x^n) + my^{-1} D_x^{(1)} y(ay^m x^n + y^m) = 0 \iff$$
$$nx^{-1}(1 - y^m) + my^{-1} D_x^{(1)} y(1 - x^n) = 0 \iff ny(1 - y^m) + mx D_x^{(1)} y(1 - x^n) = 0$$

Assim, temos:

$$D_x^{(1)} y = \frac{ny(1 - y^m)}{mx(x^n - 1)}. \tag{60}$$

Derivando novamente vem que:

$$D_x^{(1)}(ny(1 - y^m) + mx D_x^{(1)} y(1 - x^n)) = 0 \iff$$
$$D_x^{(1)}(ny - ny^{m+1} + mx D_x^{(1)} y - mx^{n+1} D_x^{(1)} y) = 0 \iff$$
$$nD_x^{(1)} y - n(m+1) y^m D_x^{(1)} y + mD_x^{(1)} y + 2mx D_x^{(2)} y - m(n+1) x^n D_x^{(1)} y - 2mx^{n+1} D_x^{(2)} y = 0 \iff$$
$$D_x^{(1)} y[n - n(m+1) y^m + m - m(n+1) x^n] + 2mx D_x^{(2)} y[1 - x^n] = 0 \tag{61}$$

Usando o fato que $D_x^{(2)} y = 0$, temos:

$$D_x^{(1)} y[n - n(m+1)y^m + m - m(n+1)x^n] = 0$$

Note que $D_x^{(1)} y$ não é nulo, assim temos que ter necessariamente para todos os pontos nos quais a curva se anula que:

$$n - n(m+1)y^m + m - m(n+1)x^n = 0 \tag{62}$$

Substituindo o ponto $P = (1,0) \in \mathcal{F}$ em (62) temos que $n - mn = 0 \iff n = 0$ ou $m = 1$. Como $p \nmid n$ vem que $m \equiv 1 \, (mod\ p)$.

Substituindo agora o ponto $Q = (0,1) \in \mathcal{F}$ em (62) temos que $-nm + m = 0 \iff m = 0$ ou $n = 1$. Como $p \nmid m$ vem que $n \equiv 1 \, (mod\ p)$.

Note porém que se supormos $m \equiv 1 \, (mod\ p)$ e $n \equiv 1 \, (mod\ p)$ não garantimos que $D_x^{(2)} y = 0$.

Substituindo tal hipótese em (61) temos que:

$$\begin{aligned} &2D_x^{(1)} y[1 - x^m - y^m] + 2xD_x^{(2)} y[1 - x^n] = 0 \\ &ax^n y^m D_x^{(1)} + xD_x^{(2)} y[1 - x^n] = 0 \\ &D_x^{(2)} y = -\frac{ax^n y^m D_x^{(1)} y}{x(1 - x^n)} \end{aligned}$$

Substituindo (60) na expressão acima obtemos:

$$D_x^{(2)} y = \frac{ax^{n-2} y^{m+1}(1 - y^m)}{(x^n - 1)^2} \neq 0. \tag{63}$$

Assim, concluímos que $\mathcal{F}$ é sempre clássica em relação à $\sum_1$. □

3.2 $\mathbb{F}_q$-FROBENIUS CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_1$

De acordo com a proposição 3.1.1 a curva $\mathcal{F}$ é clássica para todo m, n inteiros. Assim podemos concluir diretamente o Teorema abaixo.

Teorema 3.2.1. *Supondo $p > 5$, a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_1$ para todo m, n inteiros.*

3.3 CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_2$

Para facilitar os cálculos desenvolvidos nessa seção iremos usar uma adaptação de [1, Proposizione 3.3].

Proposição 3.3.1. Dada a curva projetiva $\mathcal{F} : aX^nY^m + bX^nZ^m + cY^mZ^n - Z^{m+n} = 0$ definida sobre $\mathbb{F}_q$ tal que $a, b, c \in \mathbb{F}_q$, $c \neq -\frac{a}{b}$, $a \neq 0$ e m, n inteiros positivos. Supondo $p > 5$, e $\mathcal{F}$ clássica em relação à $\sum_1$, temos:

(a) $\mathcal{F}$ é geometricamente irredutível;

(b) O gênero de $\mathcal{F}$ é $(n-1)(m-1)$;

(c) Os únicos pontos singulares de $\mathcal{F}$ são $P = (1 : 0 : 0)$ e $Q = (0 : 1 : 0)$, sendo que $m_P(\mathcal{F}) = m$ e $m_Q(\mathcal{F}) = n$. Além disso, as retas tangentes a $\mathcal{F}$ em P e Q são dadas pelas equações afins $y = \alpha$ e $x = \beta$, respectivamente, sendo $\alpha^m = -ba^{-1}$ e $\beta^n = -ca^{-1}$, e essas retas tangentes interceptam $\mathcal{F}$ nos pontos correspondentes com multiplicidade $m + n$;

(d) A multiplicidade de interseção de um ramo de centrado em P ou Q com a sua reta tangente é $m + 1$ e $n + 1$, respectivamente;

(e) Os pontos $P_\xi = (0 : \xi : 1)$ e $P_\rho = (\rho : 0 : 1)$, com $\xi^m = c^{-1}$ e $\rho^n = b^{-1}$ são pontos de inflexão de $\mathcal{F}$. Além disso, as retas tangentes a $\mathcal{F}$ em P_ξ e P_ρ são dadas pelas equações $y = \xi$ e $x = \rho$, respectivamente, e estas retas interceptam $\mathcal{F}$ com multiplicidades n e m, respectivamente.

Proposição 3.3.2. Se $p > 5$ e a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é não clássica em relação à $\sum_2$, então

$$p \mid (n+1)(n-1) \text{ e } p \mid (m+1)(m-1).$$

Demonstração. Olhando apenas para os casos de ponto de inflexão, temos que a sequência de $(\sum_1, P_\xi)$-ordem é dada por $(0, 1, n)$, $n \geq 3$ e consequentemente a sequência de $(\sum_2, P_\xi)$-ordem é dada por $(0, 1, 2, n, n+1, 2n)$. Analogamente usando P_ρ obtemos que a sequência de $(\sum_2, P_\rho)$-ordem é dada por $(0, 1, 2, m, m+1, 2m)$.

Usando a proposição 1.2.1 segue que se $\mathcal{F}$ é não clássica em relação à $\sum_2$, então

$$p \mid (2n-1)(n-2)(n+1)(n-1) \text{ e } p|(2m-1)(m-2)(m+1)(m-1). \tag{64}$$

Vamos considerar agora Γ um modelo não singular de $\mathcal{F}$ e $P_\gamma \in \Gamma$ um ramo γ de $\mathcal{F}$ centrado em P. Pela proposição 3.6.1 a sequência de $(\sum_1, P)$-ordem é dada por $(0, 1, m+1)$ e consequentemente a sequência de $(\sum_2, P)$-ordem é dada por $(0, 1, 2, m+1, m+2, 2m+2)$. Analogamente para o ponto Q obtemos a sequência de $(\sum_2, Q)$-ordem dada por $(0, 1, 2, n+1, n+2, 2n+2)$.

Usando novamente a proposição 1.2.1 segue que se $\mathcal{F}$ é não clássica em relação à $\sum_2$, então

$$p \mid (n+1)(n-1)(n+2)(2n+1) \text{ e } p|(m+1)(m-1)(m+2)(2m+1). \tag{65}$$

Usando (64) e (65) concluímos que $p \mid (n+1)(n-1)$ e $p \mid (m+1)(m-1)$.

□

Para conlcluir o caso da não classicalidade de $\mathcal{F}$ em relação à $\sum_2$ vamos novamente usar o Lema 2.3.2 juntamente com a observação 2.3.3.

Lema 3.3.3. Considerando $p > 2$ e $a \neq -1$ são irredutíveis sobre $\overline{\mathbb{F}}_q$ as seguintes curvas projetivas:

(a) $\mathcal{F}_1 : aXY + XZ + YZ - Z^2 = 0$;

(b) $\mathcal{F}_2 : aXZ + XY + Z^2 - YZ = 0$;

(c) $\mathcal{F}_3 : aYZ + XY + Z^2 - XZ = 0$;

(d) $\mathcal{F}_4 : aZ^2 + YZ + XZ - XY = 0$;

Demonstração. Para todos os itens basta observar que as cônicas são não singulares e portanto irredutíveis.

□

Proposição 3.3.4. Supondo $p > 5$ e $a \neq -1$ a curva $\mathcal{F}$ é não clássica em relação à $\sum_2$, nos casos:

(a) $p \mid (n-1)$ e $p \mid (m-1)$;

(b) $p \mid (n-1)$ e $p \mid (m+1)$;

(c) $p \mid (m-1)$ e $p \mid (n+1)$;

(d) $p \mid (n+1)$ e $p \mid (m+1)$.

Demonstração. (a) Considere inteiros r,s,k,l tais que $n = p^r k + 1$ e $m = p^s l + 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$ax^n y^m + x^n + y^m - 1 = 0 \iff a(x^w)^{p^s} x (y^l)^{p^s} y + (x^w)^{p^s} x + (y^l)^{p^s} y - 1 = 0. \tag{66}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (66) obtemos a cônica projetiva $\mathcal{G}_1 : a\alpha\beta XY + \alpha XZ + \beta YZ - Z^2 = 0$.

Como $\mathcal{G}_1$ é projetivamente equivalente a $\mathcal{F}_1 : aXY + XZ + YZ - Z^2 = 0$ com $a \neq -1$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(b) Considere inteiros r,s,k,l tais que $n = p^r k + 1$ e $m = p^s l - 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s + 1 = wp^s + 1$. Temos que:

$$ax^n y^m + x^n + y^m - 1 = 0 \iff a(x^w)^{p^s} x (y^l)^{p^s} y^{-1} + (x^w)^{p^s} x + (y^l)^{p^s} y^{-1} - 1 = 0. \tag{67}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (67) obtemos a cônica projetiva $\mathcal{G}_2 : a\alpha\beta XZ + \alpha XY + \beta Z^2 - YZ = 0$.

Como $\mathcal{G}_2$ é projetivamente equivalente a $\mathcal{F}_2 : aXZ + XY + Z^2 - YZ = 0$ com $a \neq -1$, que é irredutível, segue do Lema 2.3.2 (a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(c) Com um raciocínio análogo ao caso anterior e fazendo a transformação projetiva $(X : Y : Z) \mapsto (Y : X : Z)$, obtemos a cônica projetiva irredutível $\mathcal{F}_3 : aYZ + XY + Z^2 - XZ = 0$ com $a \neq -1$ e, portanto, $\mathcal{F}$ é não clássica em relação à $\sum_2$.

(d) Considere inteiros r,s,k,l tais que $n = p^r k - 1$ e $m = p^s l - 1$, $p \nmid k$, $p \nmid l$. Sem perda de generalidade vamos supor que $r \geq s \iff r = s + d$ para algum inteiro d e assim $n = (p^d k)p^s - 1 = wp^s - 1$. Temos que:

$$ax^n y^m + x^n + y^m - 1 = 0 \iff a(x^w)^{p^s} x^{-1} (y^l)^{p^s} y^{-1} + (x^w)^{p^s} x^{-1} + (y^l)^{p^s} y^{-1} - 1 = 0. \tag{68}$$

Considerando $P = (u : v : 1) \in \mathcal{F}$ um ponto genérico e $\alpha = (u^w)^{p^s}$ e $\beta = (v^l)^{p^s}$, por (68) obtemos a cônica projetiva $\mathcal{G}_3 : a\alpha\beta Z^2 + \alpha YZ + \beta XZ - XY = 0$.

Como $\mathcal{G}_3$ é projetivamente equivalente a $\mathcal{F}_4 : aZ^2 + YZ + XZ - XY = 0$ com $a \neq -1$, que é irredutível, segue do Lema 2.3.2(a) que $\mathcal{F}$ é não clássica em relação à $\sum_2$.

□

Teorema 3.3.5. *Supondo $p > 5$ e $a \neq -1$, a curva $\mathcal{F}$ é não clássica em relação à $\sum_2$ se, e somente se, umas das condições é válida:*

(a) $p \mid (n-1)$ *e* $p \mid (m-1)$;

(b) $p \mid (n-1)$ *e* $p \mid (m+1)$;

(c) $p \mid (m-1)$ *e* $p \mid (n+1)$;

(d) $p \mid (n+1)$ *e* $p \mid (m+1)$.

Demonstração. A demonstração segue diretamente das proposições 3.3.2 e 3.3.4. □

3.4 $\mathbb{F}_q$-FROBENIUS CLASSICALIDADE DE $\mathcal{F}$ EM RELAÇÃO À $\sum_2$

Nesta seção iremos considerar $\mathcal{H}_P$ a cônica osculante de $\mathcal{F}$ em P.

É importante relembrar a proposição 2.4.2, além da seguinte proposição de fácil demonstração:

Proposição 3.4.1. Suponha $p > 5$, $\mathcal{F}$ clássica em relação à $\sum_1$ e não clássica em relação à $\sum_2$. Temos que para $P = (u : v : 1) \in \mathcal{F}, uv \neq 0$, a cônica osculante $\mathcal{H}_P$ de $\mathcal{F}$ em P é a curva projetiva irredutível $\mathcal{H}_P(X, Y, Z)$, tal que:

$$\mathcal{H}_P(X,Y,Z) : \begin{cases} au^{n-1}v^{m-1}XY + bu^{n-1}XZ + cv^{m-1}YZ - Z^2 = 0, \text{ se } p \mid (n-1) \text{ e } p|(m-1); \\ au^{n-1}v^{m+1}XZ + bu^{n-1}XY + cv^{m+1}Z^2 - YZ = 0, \text{ se } p \mid (n-1) \text{ e } p|(m+1); \\ au^{n+1}v^{m-1}YZ + bu^{n+1}Z^2 + cv^{m-1}XY - XZ = 0, \text{se } p \mid (n+1) \text{ e } p|(m-1); \\ au^{n+1}v^{m+1}Z^2 + bu^{n+1}YZ + cv^{m+1}XZ - XY = 0, \text{ se } p \mid (n+1) \text{ e } p|(m+1). \end{cases}$$

Demonstração. A demonstração é análoga a feita na proposição 3.3.4 para todos os itens. □

Proposição 3.4.2. Seja $p > 5$ e suponha que $p \mid (n-1)$ e $p \mid (m-1)$. Então a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, $m = n = \frac{q-1}{p^r-1}$ com $r < h$ tal que $r \mid h$ e $a, b, c \in \mathbb{F}_{p^r}$.

Demonstração. Pelas proposições 3.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n-1+q}y^{m-1+q} + bx^{n-1+q} + cy^{m-1+q} - 1 = 0. \tag{69}$$

Note que a condição acima é equivalente a dizer que:

$$ax^{n-1+q}y^{m-1+q} + bx^{n-1+q} + cy^{m-1+q} - 1 = (ax^n y^m + bx^n + cy^m - 1)h(x,y). \tag{70}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$. Analisando (70) em $x = 0$ obtemos:

$$cy^{m-1+q} - 1 = (cy^m - 1)h(0,y).$$

e portanto $cy^m - 1 \mid cy^{m-1+q} - 1$. Usando o Lema 2.2.1 vem que $m \mid m - 1 + q$ e, portanto, $m \mid q - 1$, ou seja, $q - 1 = mt$ para algum inteiro t.

Observe que podemos reescrever (69) como:

$$y^{m-1+q}(ax^{n-1+q} + c) = 1 - bx^{n-1+q} \iff y^{m(1+t)} = \frac{1 - bx^{n-1+q}}{c + ax^{n-1+q}}. \tag{71}$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m(ax^n + c) = 1 - bx^n \iff y^{m(1+t)} = \frac{(1 - bx^n)^{1+t}}{(c + ax^n)^{1+t}}. \tag{72}$$

Portanto de (71) e (72) temos que:

$$\frac{1 - bx^{n-1+q}}{c + ax^{n-1+q}} = \frac{(1 - bx^n)^{1+t}}{(c + ax^n)^{1+t}}. \tag{73}$$

Note que a condição acima ocorre se, e somente se, $1 + t = p^r$.

Como $mt = q - 1$, vem que $m = \frac{q-1}{p^r-1}$ para algum $r > 0$ e, como $p^r - 1 \mid p^h - 1$, podemos concluir que $r < h, \quad r \mid h$.

Note ainda que de (73) obtemos $n - 1 + q = n + nt \iff nt = q - 1 \iff n = m$.

Por (73) concluímos ainda que $a, b, c \in \mathbb{F}_{p^r}$.

Observe ainda que a recíproca é facilmente observada substituindo as condições dadas em (73). □

Proposição 3.4.3. Seja $p > 5$ e suponha que $p \mid (n - 1)$ e $p \mid (m + 1)$. Então a curva $\mathcal{F}$ definida sobra $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobnenius clássica em relação à $\sum_2$.

Demonstração. Pelas proposições 3.4.1 e 2.4.2 (b) e, supondo que $m + 1 - q > 0$, temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n-1}y^{m+1}x^q + bx^{n-1}x^q y^q + cy^{m+1} - y^q = 0 \iff ax^{n-1+q}y^{m+1-q} + bx^{n-1+q} + cy^{m+1-q} - 1 = 0. \tag{74}$$

Note que a condição acima é equivalente a dizer que:

$$ax^{n-1+q}y^{m+1-q} + bx^{n-1+q} + cy^{m+1-q} - 1 = (ax^n y^m + bx^n + cy^m - 1)h(x,y). \tag{75}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$. Analisando (75) em $x = 0$ obtemos:

$$cy^{m+1-q} - 1 = (cy^m - 1)h(0,y).$$

e portanto $cy^m - 1 \mid cy^{m+1-q} - 1$. Usando o Lema 2.2.1 vem que $m \mid m + 1 - q$ e, portanto, $m \mid 1 - q$, ou seja, $1 - q = mt$ para algum inteiro t.

Observe que podemos reescrever (74) como:

$$y^{m+1-q}(c + ax^{n-1+q}) = 1 - bx^{n-1+q} \iff y^{m(1+t)} = \frac{1 - bx^{n-1+q}}{c + ax^{n-1+q}}. \tag{76}$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m(c + ax^n) = 1 - bx^n \iff y^{m(1+t)} = \frac{(1 - bx^n)^{(1+t)}}{(c + ax^n)^{(1+t)}}. \tag{77}$$

Portanto de (76) e (77) temos que:

$$\frac{1 - bx^{n-1+q}}{c + ax^{n-1+q}} = \frac{(1 - bx^n)^{(1+t)}}{(c + ax^n)^{(1+t)}}.$$

Note que a condição acima ocorre se, e somente se, $1 + t = p^r$.

Como $mt = 1 - q$, vem que $m = \frac{1-q}{p^r-1}$ para algum $r > 0$ e, como $p^r - 1 \mid p^h - 1$, podemos concluir que $r < h$, $r \mid h$.

Observe que neste caso obtemos $m < 0$ e, portanto, uma contradição. Supondo agora que $m + 1 - q < 0$ e com um raciocínio análogo obtemos a mesma condição e, assim, concluímos a demonstração. □

Proposição 3.4.4. Seja $p > 5$ e suponha que $p \mid (n + 1)$ e $p \mid (m - 1)$. Então a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_2$.

Demonstração. Pelas proposições 3.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n+1}y^{m-1}y^q + bx^{n+1} + cy^{m-1}x^q y^q - x^q = 0 \tag{78}$$

Vamos inicialmente supor que $n + 1 - q < 0$, neste caso podemos reescrever (78) como

$$ax^{n+1}y^{m-1}y^q + bx^{n+1} + cy^{m-1}x^q y^q - x^q = 0 \iff ay^{m-1+q} + b + cy^{m-1+q}x^{q-n-1} - x^{q-n-1} = 0. \tag{79}$$

Note que a condição acima é equivalente a dizer que:

$$ay^{m-1+q} + b + cy^{m-1+q}x^{q-n-1} - x^{q-n-1} = (ax^n y^m + bx^n + cy^m - 1)h(x,y). \tag{80}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$. Analisando (80) em $y = 0$ obtemos:

$$b - x^{q-n-1} = (bx^n - 1)h(x,0).$$

e, portanto, $bx^n - 1 \mid b - x^{q-n-1}$. Usando o Lema 2.2.1 vem que $n \mid q-n-1$ e, portanto, $n \mid q-1$, ou seja, $q-1 = nt$ para algum inteiro t.

Observe que podemos reescrever (79) como

$$x^{q-n-1}(1 - cy^{m-1+q}) = b + ay^{m-1+q} \iff x^{n(t-1)} = \frac{b + ay^{m-1+q}}{1 - c^{m-1+q}}. \tag{81}$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$x^n(b + ay^m) = 1 - cy^m \iff x^{n(t-1)} = \frac{(1 - cy^m)^{(t-1)}}{(b + ay^m)^{(t-1)}}. \tag{82}$$

Portanto de (81) e (82) temos que:

$$\frac{b + ay^{m-1+q}}{1 - cy^{m-1+q}} = \frac{(1 - cy^m)^{(t-1)}}{(b + ay^m)^{(t-1)}}. \tag{83}$$

Note que a condição acima ocorre se, e somente se, $t - 1 = -p^r$.

Como $nt = q - 1$, vem que $n = \frac{q-1}{1-p^r}$, e consequentemente, $n < 0$, o que é uma contradição.

Assim podemos supor que $n + 1 - q \geq 0$.

Com um raciocínio análogo ao anterior, concluímos novamente que $n < 0$ e como temos uma contradição também para este caso , concluímos a demonstração. □

Proposição 3.4.5. Seja $p > 5$ e suponha que $p \mid (n+1)$ e $p \mid (m+1)$. Então a curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não-clássica em relação à $\sum_2$ se, e somente se $m = n = \frac{q-1}{p^r+1}$ para algum $r > 0$, $r < h$ tal que $2r \mid h$ com $n + 1 - q < 0$, $ac^{p^r} = -b$, $a^{p^r+1} = 1$, $ab^{p^r} = -c$ e a, b e $c \in \mathbb{F}_{p^{2r}}$.

Demonstração. (i) Vamos inicialmente supor o caso $n + 1 - q \geq 0$ e $m + 1 - q \geq 0$.

Pelas proposições 3.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n+1}y^{m+1} + bx^{n+1}y^q + cy^{m+1}x^q - x^q y^q = 0 \iff ax^{n+1-q}y^{m+1-q} + bx^{n+1-q} + cy^{m+1-q} - 1 = 0. \tag{84}$$

Note que a condição acima é equivalente a dizer que:

$$ax^{n+1-q}y^{m+1-q} + bx^{n+1-q} + cy^{m+1-q} - 1 = (ax^n y^m + bx^n + cy^m - 1)h(x,y). \tag{85}$$

para algum $h(x,y) \in \mathbb{F}_q[x,y] \setminus \{0\}$.

Analisando (85) em $x = 0$ obtemos:

$$cy^{m+1-q} - 1 = (cy^m - 1)h(0,y).$$

e portanto $cy^m - 1 \mid cy^{m+1-q} - 1$. Usando o Lema 2.2.1 vem que $m \mid m+1-q$ e, portanto, $m \mid 1-q$, ou seja, $1-q = mt$ para algum inteiro t.

Observe que podemos reescrever (84) como:

$$y^{m+1-q}(c + ax^{n+1-q}) = 1 - bx^{n+1-q} \iff y^{m(1+t)} = \frac{1 - bx^{n+1-q}}{c + ax^{n+1-q}}. \tag{86}$$

E podemos ainda reescrever a equação de $\mathcal{F}$ como:

$$y^m(c + ax^n) = 1 - bx^n \iff y^{m(1+t)} = \frac{(1 - bx^n)^{(1+t)}}{(c + ax^n)^{(1+t)}}. \tag{87}$$

Portanto de (86) e (87) temos que:

$$\frac{1 - bx^{n+1-q}}{c + ax^{n+1-q}} = \frac{(1 - bx^n)^{(1+t)}}{(c + ax^n)^{(1+t)}}. \tag{88}$$

Note que a condição acima ocorre se, e somente se, $1 + t = p^r$.

Como $mt = 1 - q$, vem que $m = \frac{1-q}{p^r-1}$ para algum $r > 0$ e, como $p^r - 1 \mid p^h - 1$, podemos concluir que $r < h$.

Observe que neste caso obtemos $m < 0$ e portanto, uma contradição. Podemos complementar ainda e observar que neste caso teríamos

$$n + 1 - q = n(1 + t) \iff n = \frac{1-q}{p^r - 1}$$

e, consequentemente, $n < 0$.

(ii) Vamos supor agora o caso $n + 1 - q \geq 0$ e $m + 1 - q < 0$.

Pelas proposições 3.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n+1}y^{m+1} + bx^{n+1}y^q + cy^{m+1}x^q - x^q y^q = 0 \iff ax^{n+1-q} + bx^{n+1-q}y^{q-m-1} + c - y^{q-m-1} = 0.$$

Usando um raciocínio análogo ao caso (i) concluímos que $m < 0$ e $n > 0$, o que é uma contradição.

(iii) Vamos supor o caso $n+1-q<0$ e $m+1-q\geq 0$ Pelas proposições 3.4.1 e 2.4.2 (b) temos que se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica então

$$ax^{n+1}y^{m+1}+bx^{n+1}y^q+cy^{m+1}x^q-x^qy^q=0 \iff ay^{m+1-q}+b+cy^{m+1-q}x^{q-n-1}-x^{q-n-1}=0.$$

Usando um raciocínio análogo ao caso (i) concluímos que $m>0$ e $n<0$, o que é uma contradição.

(iv) Por fim, vamos supor o caso $n+1-q<0$ e $m+1-q<0$.

$$ax^{n+1}y^{m+1}+bx^{n+1}y^q+cy^{m+1}x^q-x^qy^q=0 \iff a+by^{q-m-1}+cx^{q-n-1}-x^{q-n-1}y^{q-m-1}=0.$$

Usando um raciocínio análogo ao caso (i) obtemos as expressões

$$\frac{a+by^{q-m-1}}{y^{q-m-1}-c}=\frac{(1-cy^m)^{t-1}}{(b+ay^m)^{t-1}} \iff (a+by^{q-m-1})(b+ay^m)^{t-1}=(1-cy^m)^{t-1}(y^{q-m-1}-c). \tag{89}$$

e

$$\frac{a+cx^{q-n-1}}{x^{q-n-1}-b}=\frac{(1-bx^n)^{t'-1}}{(ax^n+c)^{t'-1}} \iff (a+cx^{q-n-1})(ax^n+c)^{t'-1}=(1-bx^n)^{t'-1}(x^{q-n-1}-b). \tag{90}$$

Observe que de (89) podemos concluir que $t-1=p^r$ e como $nt=q-1$, vem que $n=\frac{q-1}{p^r+1}$ para algum $r>0$ e como $p^r+1 \mid p^h-1$, podemos concluir que $r<h$ e ainda que $2r \mid h$.

Temos ainda que $q-m-1=m(t-1) \iff nt=mt \iff m=n$.

Note agora que por (89) e (90) concluímos que $ac^{p^r}=-b$, $ab^{p^r}=-c$ e $a^{p^r+1}=1$.

Podemos ainda concluir que $a^{p^r+1}=1 \iff a^{p^{2r}-1}=1 \iff a^{p^{2r}}=a$ e, portanto, $a\in\mathbb{F}_{p^{2r}}$.

Observe ainda que das condições obtidas vem que $a(ac^{p^r})^{(p^r}=b \iff c^{p^{2r}}=c$, logo $c\in\mathbb{F}_{p^{2r}}$.

Analogamente podemos concluir que $b\in\mathbb{F}p^{2r}$.

□

O resultado obtido complementa a Proposição [1, Proposiozione 5.4] que os autores deixaram passar na demonstração.

Teorema 3.4.6. *Suponha $p>5$ e $q=p^h$. A curva $\mathcal{F}$ definida sobre $\mathbb{F}_q$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, uma das condições é válida:*

(i) $p \mid (n-1)$ *e* $m = n = \frac{q-1}{p^r-1}$ *com* $r < h$ *tal que* $r \mid h$ *e* a, b *e* $c \in \mathbb{F}_{p^r}$;

(ii) $p \mid (n+1)$ *e* $m = n = \frac{q-1}{p^r+1}$ *com* $r < h$ *tal que* $2r \mid h$, $n+1-q < 0$, $ac^{p^r} = -b$, $a^{p^r+1} = 1$, $ab^{p^r} = -c$ *e* a, b *e* $c \in \mathbb{F}_{p^{2r}}$.

Demonstração. A demonstração segue diretamente das proposições 3.4.2, 3.4.3, 3.4.4 e 3.4.5. □

3.5 A QUANTIDADE DE PONTOS RACIONAIS

Vamos determinar $N(\mathcal{F})$ para o caso dado pelo Teorema 3.4.6. Para simplificar os cálculos no item (i) vamos considerar $b = c = 1$ e, no caso, (ii) vamos considerar $a = 1$, $b = -c = t^{p^r+1}$ sendo $< t >= \mathbb{F}_{p^{2r}}$. No caso geral, podemos aplicar o mesmo raciocínio.

Teorema 3.5.1. *Seja* $n = m = \frac{q-1}{p^r-1}$ *com* $r < h$, $r \mid h$ *e* $a, b, c \in \mathbb{F}_{p^r}$, *então:*

$$N(\mathcal{F}) = n^2(p^r - 3) + 4n.$$

Demonstração. Considerando a curva projetiva $\mathcal{F} : aX^nY^n + X^nZ^n + Y^nZ^n = Z^{2n}$ os únicos pontos singulares são $P = (0:1:0)$ e $Q = (1:0:0)$.

Inicialmente vamos determinar quantos ramos racionais de $\mathcal{F}$ centrados em P temos.

Desomogeinizando $\mathcal{F}$ em relação a variável Y obtemos $\mathcal{G} : ax^n + x^nz^n + z^n - z^{2n} = 0$. Observe que $O = (0,0)$ é um ponto singular ordinário de multiplicidade n e que todas as n retas tangentes estão definidas sobre $\mathbb{F}_q$ e, portanto, pelos Teoremas 2.5.6 e 2.5.7 temos exatamente n ramos centrados em P, todos eles sendo lineares e racionais.

Usando um argumento análogo, concluímos que temos exatamente n ramos centrados em Q, todos eles sendo lineares e racionais.

Vamos agora analisar o caso para os pontos da curva $\mathcal{F}$ que são não singulares. Nesta caso a curva é singular e, portanto, basta contar os pontos racionais de $\mathcal{F}$. Considerando a situação acima, no caso em que $XYZ = 0$ a quantidade de pontos racionais é $n + n = 2n$.

Desomogeinizando com $Z = 1$, considere agora (x, y) com $xy \neq 0$ um ponto racional de $\mathcal{F}$, ou seja, $ax^ny^n + x^n + y^n = 1 \iff x^n(ay^n + 1) = 1 - y^n$. Neste caso há $n \cdot n(p^r - 3)$ pontos racionais e assim, a quantidade de pontos racionais na condição dos pontos não singulares, é dada por $n^2(p^r - 3) + 2n$.

Portanto, $N(\mathcal{F}) = n^2(p^r - 3) + 2n + 2n \iff N(\mathcal{F}) = n^2(p^r - 3) + 4n$. □

Teorema 3.5.2. *Seja* $m = n = \frac{q-1}{p^r+1}$ *com* $r < h$ *tal que* $2r \mid h$, $n+1-q < 0$, $ac^{p^r} = -b$, $a^{p^r+1} = 1$, $ab^{p^r} = -c$ *e* a, b *e* $c \in \mathbb{F}_{p^{2r}}$, *então:*

$$N(\mathcal{F}) = \left(\frac{q-1}{p^{2r}-1}\right)^2 \{N_{p^{2r}}(\mathcal{C}) - 2\} + 2n,$$

sendo $\mathcal{C} : x^{p^r-1}y^{p^r-1} + t^{p^r+1}x^{p^r-1} - t^{p^r+1}y^{p^r-1} - 1 = 0$ *a curva definida sobre* $\mathbb{F}_{p^{2r}}$.

Demonstração. Considerando a curva projetiva $\mathcal{F} : X^nY^n + t^{p^r+1}X^nZ^n - t^{p^r+1}Y^nZ^n = Z^{2n}$ os únicos pontos singulares são $P = (0:1:0)$ e $Q = (1:0:0)$.

Inicialmente vamos determinar quantos ramos racionais de $\mathcal{F}$ centrados em P temos.

Desomogeinizando $\mathcal{F}$ em relação a variável Y obtemos $\mathcal{G} : x^n + t^{p^r+1}x^nz^n - t^{p^r+1}z^n - z^{2n} = 0$. Observe que $O = (0,0)$ é um ponto singular ordinário de multiplicidade n e que todas as n retas tangentes estão definidas sobre $\mathbb{F}_q$ e, portanto, pelos Teoremas 2.5.6 e 2.5.7 temos exatamente n ramos centrados em P, todos eles sendo lineares e racionais.

Usando um argumento análogo, concluímos que temos exatamente n ramos centrados em Q, todos eles sendo lineares e racionais.

Vamos agora analisar o caso para os pontos da curva $\mathcal{F}$ que são não singulares. Nesta caso a curva é singular e, portanto, basta contar os pontos racionais de $\mathcal{F}$. Considerando a situação acima, no caso em que $XYZ = 0$ não há pontos racionais.

Desomogeinizando com $Z = 1$, considere agora (x, y) com $xy \neq 0$ um ponto racional de $\mathcal{F}$, ou seja, $x^ny^n + t^{p^r+1}x^n - t^{p^r+1}y^n = 1$.

Sendo $e = \frac{q-1}{p^{2r}-1}$, temos que a aplicação norma $\mathbb{F}_q \to \mathbb{F}_{p^{2r}}$ é dada por $x \mapsto x^e$, que é sobrejetiva.

Note ainda que nas condições temos $n = e(p^r-1)$ e, portanto, temos a curva $x^{e(p^r-1)}y^{e(p^r-1)} + t^{p^r+1}x^{e(p^r-1)} - t^{p^r+1}y^{e(p^r-1)} = 1$.

Assim $N(\mathcal{F}) = e^2\{N_{p^{2r}}(\mathcal{C}) - 2\} + 2n$, sendo $\mathcal{C} : x^{p^r-1}y^{p^r-1} + t^{p^r+1}x^{p^r-1} - t^{p^r+1}y^{p^r-1} - 1 = 0$ a curva definida sobre $\mathbb{F}_{p^{2r}}$. □

Assim como no capítulo anterior, vamos determinar uma cota para $N(\mathcal{F})$ levando em consideração apenas as inflexões.

Com as notações anteriores e as definições feitas na introdução deste trabalho, temos as seguintes expressões:

$$A(P_\xi) = \begin{cases} 4n-10, & \text{se } P_\xi \in \Gamma(\mathbb{F}_q) \\ 2n-6, & \text{caso contrário} \end{cases}$$

$$A(P_\rho) = \begin{cases} 4m - 10, & \text{se } P_\rho \in \Gamma(\mathbb{F}_q) \\ 2m - 6, & \text{caso contrário} \end{cases}$$

Sendo α e β a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^m - c^{-1}$ e $T^n - b^{-1}$ e, por [4] o gênero da curva expresso por $g = (n-1)(m-1)$, uma cota melhor é dada por:

$$N(\mathcal{F}) \leq \frac{2(n-1)(m-1) + (q+5)n}{5} - \frac{\alpha(4n-10) + (n-\alpha)(2n-6) + \beta(4m-10) - (m-\beta)(2m-6)}{5}.$$

Corolário 3.5.3. Dada a curva projetiva $\mathcal{F} : aX^nY^m + bX^nZ^m + cY^mZ^n - Z^{m+n} = 0$ definida sobre $\mathbb{F}_q$ tal que $a, b, c \in \mathbb{F}_q$, $c \neq -\frac{a}{b}$, $a \neq 0$ e m, n inteiros positivos. Supondo $p > 5$, m e n dividem $q-1$ e $\mathcal{F}$ clássica em relação à $\sum_1$, uma das condições é válida:

(i) Se $n = m = \frac{q-1}{p^r-1}$ com $r < h$, $r \mid h$ e $a, b, c \in \mathbb{F}_{p^r}$, então:

$$N(\mathcal{F}) = n^2(p^r - 3) + 4n;$$

(ii) Se $m = n = \frac{q-1}{p^r+1}$ com $r < h$ tal que $2r \mid h$, $n + 1 - q < 0$, $ac^{p^r} = -b$, $a^{p^r+1} = 1$, $ab^{p^r} = -c$ e a, b e $c \in \mathbb{F}_{p^{2r}}$, então:

$$N(\mathcal{F}) = \left(\frac{q-1}{p^{2r}-1}\right)^2 \{N_{p^{2r}}(\mathcal{C}) - 2\} + 2n,$$

sendo $\mathcal{C} : x^{p^r-1}y^{p^r-1} + t^{p^r+1}x^{p^r-1} - t^{p^r+1}y^{p^r-1} - 1 = 0$ a curva definida sobre $\mathbb{F}_{p^{2r}}$;

(iii) Em todos os demais casos, uma cota para $N(\mathcal{F})$ é dada por:

$$N(\mathcal{F}) \leq \frac{2(n-1)(m-1) + (q+5)n}{5} - \frac{\alpha(4n-10) + (n-\alpha)(2n-6) + \beta(4m-10) - (m-\beta)(2m-6)}{5}.$$

Sendo α e β a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^m - c^{-1}$ e $T^n - b^{-1}$.

3.6 $\sum_2$ PASSANDO PELOS PONTOS SINGULARES DE $\mathcal{F}$

Para esta seção vamos supor que $\mathcal{F}$ é clássica em relação à $\sum_1$ e $p > 5$. Iremos ainda nos referir ao sistema de cônicas passando pelo pontos singulares de $\mathcal{F}$ por $\sum_2'$. Relembrando que os pontos singulares de $\mathcal{F}$ são dados por $(0:1:0)$ e $(1:0:0)$, tais cônicas projetivas possuem uma expressão da forma $aXY + bXZ + cYZ + dZ^2 = 0$.

Inicialmente vamos provar que a $\mathbb{F}_q$-Frobenius classicalidade de $\mathcal{F}$ em relação à $\sum_2$ é equivalente à $\mathbb{F}_q$-Frobenius não classicalidade de $\mathcal{F}$ em relação à $\sum_2'$. Para isto, vamos primeiramente demonstrar a proposição seguinte.

Proposição 3.6.1. A curva projetiva $\mathcal{F}$ é não clássica em relação à $\sum_2$ se, e somente se, é não clássica em relação à $\sum_2'$.

Demonstração. Se $\mathcal{F}$ é não clássica em relação à $\sum_2'$, dado um ponto genérico $P \in \mathcal{F}$, existe uma cônica $\mathcal{C} \in \sum_2'$ tal que $I(P, \mathcal{F} \cap \mathcal{C}) > p$ e consequentemente $\mathcal{F}$ é não clássica em relação à $\sum_2$.

Se $\mathcal{F}$ é não clássica em relação à $\sum_2$, pela proposição 3.4.1 todas as possíveis cônicas osculantes estão em $\sum_2'$ e, consequentemente, $\mathcal{F}$ é não clássica em relação à $\sum_2'$. □

Teorema 3.6.2. *A curva projetiva $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ se, e somente se, é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2'$.*

Demonstração. Se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2'$, temos que a cônica osculante $\mathcal{H}_p'$ satisfaz a propriedade $\varphi_q(P) \in \mathcal{H}_p'$ para infinitos pontos $P \in \mathcal{F}$ e, consequentemente, $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$.

Se $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica com relação à $\sum_2$, pelo Teorema 3.4.6 temos que $n = \frac{q-1}{p^r-1}$ com $r < h$ tal que $r \mid h$ e $\frac{a}{b} \in \mathbb{F}_{p^r}$. Temos ainda que $\phi_q(P) \in \mathcal{H}_P$ para infinitos pontos $P \in \mathcal{F}$. Como $\mathcal{H}_p \in \sum_2'$, vem que $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2'$. □

De acordo com o Teorema 3.4.6 temos que se $m = n = \frac{q-1}{p^r-1}$ com $r < h$ e $\frac{a}{b} \in \mathbb{F}_{p^r}$ ou $m = n = \frac{q-1}{p^r+1}$ com $r < h$ tal que $2r \mid h$, $n+1-q < 0$, $ac^{p^r} = -b$, $a^{p^r+1} = 1$, $ab^{p^r} = -c$ e a, b e $c \in \mathbb{F}_{p^{2r}}$, $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2$ e, consequentemente, pelo Teorema 3.5.2, $\mathcal{F}$ é $\mathbb{F}_q$-Frobenius não clássica em relação à $\sum_2'$. Neste caso a quantidade de pontos racionais é dada por 3.5.1 e 3.5.2.

Para todos os demais casos, $\mathcal{F}$ é sempre $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_2$ (consequentemente $\mathbb{F}_q$-Frobenius clássica em relação à $\sum_2'$) e iremos determinar uma cota para $N(\mathcal{F})$.

Por [4] temos que $g = mn - m - n + 1$ e por [11] $d = (m+n)$. Temos ainda que em relação à $\sum_2'$, por [6] $M = 3$ e, portanto, usando (3) vem que:

$$N(\mathcal{F}) \leq 2(mn - m - n) + \frac{(m+n)(q+3)}{3}. \tag{91}$$

Usando as ideias presentes ainda em [18] podemos melhorar essa cota.

A demonstração a seguir é uma generalização da demonstração feita por [6] usando a curva $\mathcal{F}$ nas condições já enunciadas.

Inicialmente vamos reunir algumas informações já obtidas ao longo deste capítulo que irão auxiliar a demonstração.

Proposição 3.6.3. Denotando por $\mathcal{D}_2'$ a série linear livre de ponto base obtida a partir de $\sum_2'$ da curva $\mathcal{F}$ e Γ um modelo não singular de $\mathcal{F}$ são válidas as afirmações:

(a) $\mathcal{D}_2'$ tem grau $m+n$;

(b) A sequência de $(\sum_2', P_{\tilde{\xi}})$-ordem é dada por $(0,1,n,n+1)$ e a sequência de $(\sum_2', P_\rho)$-ordem é dada por $(0,1,m,m+1)$.

(c) Para $P_\gamma \in \Gamma$ correspondendo a um ramo γ de $\mathcal{F}$ centrado em P a sequência de $(\sum_2', P)$-ordem é dada por $(0,1,m,m+1)$ e para $Q_\gamma \in \Gamma$ correspondendo a um ramo γ de $\mathcal{F}$ centrado em Q a sequência de $(\sum_2', Q)$-ordem é dada por $(0,1,n,n+1)$.

Demonstração. (a) Considere $\mathcal{D}_2 = \{\mathcal{C}\cdot\mathcal{F} : \mathcal{C} \in \sum_2\}$ a série linear gerada pela intersecção de $\mathcal{F}$ pelo sistema linear $\sum_2$. Pelo Teorema 1.1.1, vem que $\mathcal{D}_2$ tem grau $2(m+n)$. A base Locus de $\mathcal{D}_2$ (que é a soma de todos os divisores da série linear que aparecem no suporte com seu respectivo peso) é o divisor

$$\ell_\infty \cdot \mathcal{F} = P_1 + \cdots + P_n + Q_1 + \cdots + Q_m$$

de grau $m+n$ e sendo P_i $(i = 1,\cdots,n)$ todos os pontos distintos de Γ para os quais os correspondentes ramos estão centrados em P. Analogamente para Q_j $(j = 1,\cdots,m)$. Assim, para obtermos a nossa série linear $\mathcal{D}_2'$, livre de ponto base nas condições de [18] temos, $\mathcal{D}_2' = \mathcal{D}_2 - \ell_\infty\cdot\mathcal{F} := \{D - \ell_\infty\cdot\mathcal{F} | D \in \mathcal{D}_2\}$, que possui grau $2(m+n)-(m+n) = m+n$.

(b) Considere as retas $\ell_P = \overline{PP_{\tilde{\xi}}}$ e $\ell_Q = \overline{QP_{\tilde{\xi}}}$ e note que nenhuma destas retas é igual a ℓ_∞. Observe ainda que uma destas retas é a reta tangente a $\mathcal{F}$ em $P_{\tilde{\xi}}$. Portanto, pela proposição 3.6.1, a sequência de $(\sum_1, P_{\tilde{\xi}})$-ordem é dada por $(0,1,n)$. Assim, considerando as cônicas redutíveis dadas pela união de 2 retas escolhidas do conjunto $\{\ell_P, \ell_Q, \ell_\infty\}$, a sequência de $(\sum_2', P_{\tilde{\xi}})$-ordem é dada por $(0,1,n,n+1)$. Analogamente, considerando o ponto P_ρ obtemos a sequência de $(\sum_2', P_\rho)$-ordem dada por $(0,1,m,m+1)$.

(c) Considere $P_\gamma \in \Gamma$ um ramo γ de $\mathcal{F}$ centrado em P. Pela proposição 3.6.1 a sequência de $(\sum_1, P)$-ordem é dada por $(0, 1, m+1)$. Assim, considerando as cônicas redutíveis passando por P e Q e dadas pela união de 2 retas, vem que a sequência de $(\sum_2', P)$-ordem é dada por $(0, 1, m, m+1)$. Analogamente para o ponto Q obtemos a sequência de $(\sum_2', Q)$-ordem dada por $(0, 1, n, n+1)$.

□

Teorema 3.6.4. *Nas condições dadas temos que a cota pode ser dada por:*

$$N(\mathcal{F}) \leq 2(mn - m - n) + \frac{(m+n)(q+3)}{3} - \frac{(n-2)(2m + m_1 + n_1)}{3} - \frac{(m-2)(2n + m_2 + n_2)}{3}, \tag{92}$$

sendo m_1, n_1, m_2 e n_2 a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^m - c^{-1}$, $T^m + ba^{-1}$, $T^n - b^{-1}$ e $T^n + ca^{-1}$, respectivamente.

Demonstração. Com as notações anteriores e as definições feitas na introdução deste trabalho, temos as seguintes expressões:

$$A(P_{\tilde{\xi}}) = \begin{cases} 2n-4, & \text{se } P_{\tilde{\xi}} \in \Gamma(\mathbb{F}_q) \\ n-2, & \text{caso contrário} \end{cases}$$

$$A(P_\rho) = \begin{cases} 2m-4, & \text{se } P_\rho \in \Gamma(\mathbb{F}_q) \\ m-2, & \text{caso contrário} \end{cases}$$

$$A(P_\gamma) = \begin{cases} 2n-4, & \text{se } P_\gamma \in \Gamma(\mathbb{F}_q) \\ n-2, & \text{caso contrário} \end{cases}$$

$$A(Q_\gamma) = \begin{cases} 2m-4, & \text{se } Q_\gamma \in \Gamma(\mathbb{F}_q) \\ m-2, & \text{caso contrário} \end{cases}.$$

Sendo m_1, n_1, m_2 e n_2 a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^m - c^{-1}$, $T^m + ba^{-1}$, $T^n - b^{-1}$ e $T^n + ca^{-1}$, respectivamente, temos que:

$$\begin{aligned} N(\mathcal{F}) \leq & 2(mn - m - n) + \frac{(m+n)(q+3)}{3} - \frac{m_1(2n-4) + (m-m_1)(n-2) + m_2(2m-4)}{3} - \\ & - \frac{(n-m_2)(m-2) + n_1(2n-4) + (m-n_1)(n-2) + n_2(2m-4) + (n-n_2)(m-2)}{3}, \end{aligned}$$

Assim, concluímos que:

$$N(\mathcal{F}) \leq 2(mn - m - n) + \frac{(m+n)(q+3)}{3} - \frac{(n-2)(2m + m_1 + n_1)}{3} - \frac{(m-2)(2n + m_2 + n_2)}{3}.$$

□

Podemos assim enunciar o seguinte corolário:

Corolário 3.6.5. Dada a curva projetiva $\mathcal{F} : aX^nY^m + bX^nZ^m + cY^mZ^n - Z^{m+n} = 0$ definida sobre $\mathbb{F}_q$ tal que $a, b, c \in \mathbb{F}_q$, $c \neq -\frac{a}{b}$, $a \neq 0$ e m, n inteiros positivos. Supondo $p > 5$, m e n dividem $q-1$ e $\mathcal{F}$ clássica em relação à $\sum_1$ umas das condições a seguir é válida:

(i) Se $m = n = \frac{q-1}{p^r-1}$ com $r < h$ e $\frac{a}{b} \in \mathbb{F}_{p^r}$,temos que $N(\mathcal{F})$ é dada por:

$$N(\mathcal{F}) = n^2(p^r - 3) + 4n.$$

(ii) Se $m = n = \frac{q-1}{p^r+1}$ com $r < h$ tal que $2r \mid h$, $n + 1 - q < 0$, $ac^{p^r} = -b$, $a^{p^r+1} = 1$, $ab^{p^r} = -c$ e a, b e $c \in \mathbb{F}_{p^{2r}}$, então:

$$N(\mathcal{F}) = \left(\frac{q-1}{p^{2r}-1}\right)^2 \{N_{p^{2r}}(\mathcal{C}) - 2\} + 2n,$$

sendo $\mathcal{C} : x^{p^r-1}y^{p^r-1} + t^{p^r+1}x^{p^r-1} - t^{p^r+1}y^{p^r-1} - 1 = 0$ a curva definida sobre $\mathbb{F}_{p^{2r}}$.

(iii) Para os demais caso, uma cota para $N(\mathcal{F})$ é dada por:

$$N(\mathcal{F}) \leq 2(mn - m - n) + \frac{(m+n)(q+3)}{3} - \frac{(n-2)(2m + m_1 + n_1)}{3} - \frac{(m-2)(2n + m_2 + n_2)}{3}.$$

Considere agora o caso particular da curva projetiva plana $\mathcal{G} : a'X^nY^n - X^nZ^n - Y^nZ^n + b'Z^{2n} = 0$ com $a'b' \notin \{0, 1\}$ que foi objeto de estudo por [6].

Note que se considerarmos a nossa curva projetiva $\mathcal{F}$ e supormos $m = n$ e $b = c$ temos $\mathcal{F} : aX^nY^n + bX^nZ^n + cy^nZ^n - Z^{2n} = 0 \iff \mathcal{F} : -\frac{a}{b}X^nY^n - X^nZ^n - Y^nZ^n + \frac{1}{b}Z^{2n} = 0$.

Assim basta considerar $a' = -\frac{a}{b}$ e $b' = \frac{1}{b}$ e obtemos uma curva equivalente à curva projetiva $\mathcal{G}$.

Note que nas condições do Teorema 3.6.4 temos $n_1 = n_2 = r$ é a quantidade de raízes em $\mathbb{F}_q$ do polinômio $T^n - b^{-1} = T^n - b'$ e $m_1 = m_2 = s$ é a quantidade de raízes em $\mathbb{F}_q$ do polinômio $T^n - ba^{-1} = T^n - a'^{-1}$.

Usando o Corolário 3.6.5, nas condições atuais, obtemos o resultado demonstrado por [6, Corollary 3.3] para o nosso caso das cônicas, que é dado por:

$$N(\mathcal{G}) \leq 2(n^2 - 2n) + \frac{2n(q+3)}{3} - \frac{2(n-2)(2n + r + s)}{3}.$$

sendo r e s a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^n - b'$ e $T^n - a'^{-1}$, respectivamente.

Podemos reescrever o Corolário 3.6.5, neste caso particular, da seguinte forma:

Corolário 3.6.6. Dada a curva projetiva $\mathcal{G} : a'X^nY^n - X^nZ^n - Y^nZ^n + b'Z^{2n} = 0$ com $a'b' \notin \{0,1\}$. Supondo $p > 5$, n divide $q-1$ e $\mathcal{G}$ é clássica em relação à $\sum_1$ uma das condições a seguir é válida:

(i) Se $n = \frac{q-1}{p^r-1}$ com $r < h$ e $\frac{a}{b} \in \mathbb{F}_{p^r}$, temos que $N(\mathcal{G})$ é dada por:

$$N(\mathcal{G}) = n^2(p^r - 3) + 4n.$$

(ii) Se $m = n = \frac{q-1}{p^r+1}$ com $r < h$ tal que $2r \mid h$, $n + 1 - q < 0$, $ac^{p^r} = -b$, $a^{p^r+1} = 1$, $ab^{p^r} = -c$ e a, b e $c \in \mathbb{F}_{p^{2r}}$, temos que $N(\mathcal{G})$ é dada por:

$$N(\mathcal{G}) = \left(\frac{q-1}{p^{2r}-1}\right)^2 \{N_{p^{2r}}(\mathcal{C}) - 2\} + 2n,$$

(iii) Se $n \neq \frac{q-1}{p^r-1}$ com $r < h$ e $\frac{a}{b} \in \mathbb{F}_{p^r}$, uma cota para $N(\mathcal{G})$ é dada por:

$$N(\mathcal{G}) \leq 2(n^2 - 2n) + \frac{2n(q+3)}{3} - \frac{2(n-2)(2n+r+s)}{3}.$$

Sendo r e s a quantidade de raízes em $\mathbb{F}_q$ dos polinômios $T^n - b'$ e $T^n - a'^{-1}$, respectivamente.

BIBLIOGRAFIA

[1] ABATANGELO, V.; KORCHMÁROS, G.; *Una generalizzazione di um teorema d B. Segre sui punti regolari rispetto ad una ellisse di um piano affine di Galois*, Ann Mat. Pura Appl 172, 87-102, 1997.

[2] ARAKELIAN, N.; BORGES, H.; *Bounds for the number of points on curves over finite fields*, Israel Journal of Mathematics 228(1), 177-199, 2018.

[3] ARAKELIAN, N.; BORGES, H.; *Frobenius nonclassicality of Fermat curves with respect to cubics*, Israel Journal of Mathematics 218(1), 273–297, 2017.

[4] ARAKELIAN, N.; SPEZIALI, P.; *On generalizitions of Fermat Curves over finite fields and their automorphisms*, Communications in Algebra 45:11, 4926-4938, 2017.

[5] BORGES, H.; *Frobenius nonclassical components of curves with separable variables*, Journal of Number Theory 159, 402-425, 2016.

[6] BORGES, H.; COUTINHO, M.; *On some generalized Fermat curves and chords of an affinely regular polygon inscribed in a hyperbola*, Journal of Pure and Applied Algebra 224, 239-249, 2020.

[7] COCHRANE, T.; PINNER C.; *Explicit bounds on monomial and binomial exponential sums*, Q.J. Math. 62, 323-349, 2011.

[8] GARCIA, A.; *The Curve $y^n = f(x)$ over finite fields*, Arch-Mat, Vol 54, 36-44, 1990.

[9] GARCIA, A.; VOLOCH, J. F.; *Fermat curves over finite fields*, Journal Number Theory 30,345–356, 1988.

[10] GARCIA, A.; VOLOCH, J. F.; *Wronskians and linear independence in fields of prime characteristic*, Manuscripta Math., 59, 457-469, 1987.

[11] HIRSCHFELD, J.W.P.; KORCHMÁROS, G.; TORRES, F.; *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, 2008.

[12] IMPA-PROGRAMA DE MESTRADO: INTRODUÇÃO ÀS CURVAS ALGÉBRICAS; YOUTUBE, 2011. Dísponível em $https://www.youtube.com/playlist?list=PLo4jXE-LdDTSvn9evqkXf8mii9Q_w1nyX$ >. Acesso em 05 de setembro de 2022.

[13] LIDL,R.; NIEDERREITER, H.; *Finite fields*, Cambridge University Press, 1988.

[14] PARDINI, R.; *Some remarks on plane curves over fields of finite characteristic* , Compositio Math. 60, 3-17, 1986.

[15] SERRE, J.P.; *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C.R. Acad. Sci. Paris Sér. I Math 296, 397-402, 1983.

[16] STARK, H.; *On the Riemann hyphotesis in hyperelliptic function fields*, Symposia in Pure Mathematics 24, 285-302, 1973.

[17] STICHTENOTH, H.; *Algebraic function fields and codes*, Springer, Berlin, 1993.

[18] STÖHR, K.O.; VOLOCH, J. F.; *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) 52, 1-19, 1986.

[19] VAISENCHER, I.; *Introdução às curvas algébricas planas*, IMPA, 2009.