UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

**On $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$
and the Hasse-Witt invariant for a class of Kummer extension**

Cirilo Gonçalves Júnior

Tese de Doutorado do Programa de Pós-Graduação em
Matemática (PPG-Mat)

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Cirilo Gonçalves Júnior

On $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$
and the Hasse-Witt invariant for a class of Kummer
extension

Doctoral dissertation submitted to the Institute of
Mathematics and Computer Sciences – ICMC-USP,
in partial fulfillment of the requirements for the
degree of the Doctorate Program in Mathematics.
EXAMINATION BOARD PRESENTATION COPY

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
January 2020

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

G643o Gonçalves Júnior, Cirilo
 On F_q^3 -Frobenius nonclassical curves of type
 $Yq^2+q+1=f(X)$ and the Hasse-Witt invariant for a
 class of Kummer extension / Cirilo Gonçalves
 Júnior; orientador Herivelto Martins Borges Filho.
 -- São Carlos, 2020.
 113 p.

 Tese (Doutorado - Programa de Pós-Graduação em
 Matemática) -- Instituto de Ciências Matemáticas e
 de Computação, Universidade de São Paulo, 2020.

 1. Frobenius nonclassical curves. 2.
 Hyperelliptic curves. 3. Automorphism group. 4. a-
 number. 5. Hasse-Witt invariant. I. Martins Borges
 Filho, Herivelto , orient. II. Título.

Cirilo Gonçalves Júnior

**Sobre curvas $\mathbb{F}_{q^3}$ -Frobenius não-clássicas do tipo
 $Y^{q^2+q+1} = f(X)$ e o invariante de Hasse-Witt para uma
classe de extensões de Kummer**

Tese apresentada ao Instituto de Ciências
Matemáticas e de Computação – ICMC-USP,
como parte dos requisitos para obtenção do título
de Doutor em Ciências – Matemática. *EXEMPLAR
DE DEFESA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Janeiro de 2020

Para Priscila, Cecília e Letícia.

ACKNOWLEDGEMENTS

Primeiramente, agradeço a Deus, por ter me dado força e perseverança para chegar até aqui.

Agradeço ao meu orientador, Prof. Herivelto, pela paciência, direcionamentos e sugestões valiosas que contribuíram grandemente para a melhoria deste texto.

Agradeço aos professores por aceitarem participar da banca examinadora.

Agradeço também a todos os professores que me acompanharam durante a graduação, mestrado e doutorado. Em especial, ao meu mestre e orientador de graduação e mestrado, professor Cícero Fernandes De Carvalho, da Universidade Federal de Uberlândia.

Um agradecimento especial a minha esposa, Priscila, pelo apoio e companheirismo durante o doutorado.

Agradeço também os meus amigos do ICMC-USP, sala 3-252, por terem me ajudado passar por este período em São Carlos. Desejo a todos sucesso!

Por fim, agradeço ao CEFET-MG pelo apoio financeiro.

*“Fides et Ratio binae quasi pennae videntur quibus
veritatis ad contemplationem hominis attollitur animus.”*

São João Paulo II

ABSTRACT

GONÇALVES, C. **On $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$ and the Hasse-Witt invariant for a class of Kummer extension.** 2020. ?? p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

Inserted in the context of algebraic curves defined over finite fields, this work presents several results in two different topics. First, it gives a complete characterization of the $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$, and it provides an explicit computation of the following birational invariants: genus, automorphism group, Hasse-Witt invariant and a -number. The number of $\mathbb{F}_{q^3}$ -rational points is computed as well. Second, this work provides an extensive study of the Hasse-Witt invariant of the curves $Y^m + X^n + 1 = 0$ and $Y^m + X^n + X = 0$. A combinatorial formula for this invariant is presented in the general case, and explicit closed formulas are provided for special values of m and n .

Keywords: Frobenius nonclassical curves, hyperelliptic curves, automorphism group, a -number, Hasse-Witt invariant.

RESUMO

GONÇALVES, C. **Sobre curvas $\mathbb{F}_{q^3}$ -Frobenius não-clássicas do tipo $Y^{q^2+q+1} = f(X)$ e o invariante de Hasse-Witt para uma classe de extensões de Kummer.** 2020. ?? p. Tese (Doutorado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2020.

Inserido no contexto de curvas algébricas definidas sobre corpos finitos, este trabalho apresenta vários resultados em dois tópicos diferentes. Primeiro, ele apresenta uma caracterização completa das curvas $\mathbb{F}_{q^3}$ -Frobenius não-clássicas do tipo $Y^{q^2+q+1} = f(X)$ e fornece um cálculo explícito dos seguintes invariantes birracionais: gênero, grupo automorfismo, invariante de Hasse-Witt e a -number. O número de pontos $\mathbb{F}_{q^3}$ -racionais também é calculado. Segundo, este trabalho fornece um extensivo estudo do invariante de Hasse-Witt das curvas $Y^m + X^n + 1 = 0$ e $Y^m + X^n + X = 0$. Uma fórmula combinatória para esse invariante é apresentada no caso geral, e fórmulas fechadas explícitas são fornecidas para valores especiais de m e n .

Palavras-chave: Curvas Frobenius não-classicas, curvas hiperelípticas, grupo de automorfismo, a -number, invariante de Hasse-Witt.

LIST OF TABLES

CONTENTS

INTRODUCTION

Let $\mathbb{F}_q$ be the field with q elements, where q is a power of a prime number p , and let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$. A topic of great interest in the theory of algebraic curves over finite fields is the study of $\mathbb{F}_q$ -Frobenius nonclassical curves, that is, irreducible plane curves $\mathcal{C}$ of degree d and genus g defined over $\mathbb{F}_q$, such that the q -Frobenius map takes each simple point $P \in \mathcal{C}$ to a point on the tangent line to $\mathcal{C}$ at P . In this case, there is an exponent h with $p \leq p^h \leq d$ such that the intersection multiplicity of $\mathcal{C}$ and the tangent line to $\mathcal{C}$ at a simple point $P \in \mathcal{C}$ is at least p^h , and it is exactly p^h for a general point $P \in \mathcal{C}$.

Frobenius nonclassical curves were introduced in the work of Stöhr and Voloch (??), and one reason for highlighting this special class of curves $\mathcal{C}$ comes from fact that

$$\frac{v(2g-2) + (q+2)d}{2}$$

is an upper bound on the number of $\mathbb{F}_q$ -rational points on $\mathcal{C}$ (??), where

$$v = \begin{cases} p^h, & \text{if } \mathcal{C} \text{ is } \mathbb{F}_q\text{-Frobenius nonclassical} \\ 1, & \text{otherwise} \end{cases}.$$

Thus, the $\mathbb{F}_q$ -Frobenius nonclassical curves potentially have many rational points. In fact, $d(q-d+2)$ is a lower bound on the number of $\mathbb{F}_q$ -rational points on such curves of degree d (??), moreover, the equality holds when the curve is nonsingular (??).

Another interesting fact (which will be much explored in this work) is that the $\mathbb{F}_q$ -Frobenius nonclassical curves are related to minimal value set polynomial (MVSP), that is, polynomials $f(X) \in \mathbb{F}_q[X]$ for which the value set $V_f := \{f(\alpha) : \alpha \in \mathbb{F}_q\}$ has minimal size $\lfloor (q-1)/\deg(f) \rfloor + 1$ (??). In particular, the irreducible components of the curve $Y^{\frac{q^k-1}{q-1}} = f(X)$ are $\mathbb{F}_{q^k}$ -Frobenius nonclassical if and only if f is an MVSP with $V_f = \mathbb{F}_q$ (??).

Let $\mathcal{C}$ be a projective, nonsingular, geometrically irreducible algebraic curve of genus g defined over $\mathbb{F}_q$. Another topic of great interest is the study of the Hasse-Witt invariant $\gamma(\mathcal{C})$ of $\mathcal{C}$, which is given by the dimension of the space spanned by the logarithmic differentials on $\mathcal{C}$. It is well known that $\gamma(\mathcal{C})$ is a number between 0 and g , and it is equal to the p -rank of $\mathcal{C}$ (??), that is, the number of copies of $\mathbb{Z}/p\mathbb{Z}$ in the Jacobian of $\mathcal{C}$ (??).

An important result concerning the Hasse-Witt invariant is the Deuring-Shafarevich's formula (??, Theorem 11.62), which relates the Hasse-Witt invariants of two curves $\mathcal{C}$ and $\mathcal{D}$, when the function field $\mathbb{K}(\mathcal{C})$ of $\mathcal{C}$ is a p -power Galois extension of the function field $\mathbb{K}(\mathcal{D})$ of

$\mathcal{D}$. More precisely, if the curve $\mathcal{C}$ has an automorphism group G of order power of p , then

$$\gamma(\mathcal{C}) - 1 = |G|(\gamma(\mathcal{D}) - 1) + \sum_{i=1}^s (|G| - l_i),$$

where $\mathcal{D}$ is the quotient curve $\mathcal{C}/G$, and $l_1, \dots, l_s$ are the sizes of the short orbits of G on the points of $\mathcal{C}$.

Moreover, it is well known that $\gamma(\mathcal{C})$ may affect the size of the automorphism group $\text{Aut}(\mathcal{C})$ of $\mathcal{C}$. In particular, curves with large automorphism group often have Hasse-Witt invariant zero (??) and (??). In this sense, Nakajima uses the Hasse-Witt invariant to give an upper bound for the size of the Sylow p -subgroup of $\text{Aut}(\mathcal{C})$, when $g \geq 2$ (??). Another problem of great interest in the study of the automorphism groups is to find a function $f(g)$ such that if $|\text{Aut}(\mathcal{C})| > f(g)$ then $\gamma(\mathcal{C}) = 0$. For instance, in 2019, Giulietti and Korchmáros proved that for $p > 2$ and $g \geq 2$, if

$$f(g) = \begin{cases} \frac{p}{p-2} 84g^2, & \text{if } G \text{ is a solvable subgroup of } \text{Aut}(\mathcal{C}) \\ 900g^2, & \text{if } G \text{ is non-solvable subgroup of } \text{Aut}(\mathcal{C}) \text{ and } g \text{ is even} \end{cases}$$

and $|G| > f(g)$ then the Hasse-Witt invariant of $\mathcal{C}$ is zero (??, Theorem 1.1 and 1.2).

Algebraic curves over finite fields are often used in the construction of error correcting codes. In general, when the number $N_q(\mathcal{C})$ of $\mathbb{F}_q$ -rational points of a projective nonsingular curve $\mathcal{C}$ is large compared to its genus g , the associated codes are expected to have good parameters. In this sense, a problem of great interest in the theory of algebraic curves is to determine $N_q(\mathcal{C})$.

A remarkable result related to $N_q(\mathcal{C})$ is the Hasse-Weil bound, which states that

$$|N_q(\mathcal{C}) - (q + 1)| \leq 2g\sqrt{q}, \quad (1)$$

see (??, Theorem 9.18), (??, Theorem 5.2.3). The curve $\mathcal{C}$ is called $\mathbb{F}_q$ -maximal if the upper bound in (??) is attained and $\mathbb{F}_q$ -minimal if the lower bound in (??) is attained. To some extent, the problem of finding maximal/minimal curves motivates the study of the Hasse-Witt invariant, since these curves have Hasse-Witt invariant zero (??, Proposition 1).

Let n and m be positive integers coprime to p , with $n \geq m \geq 2$. Consider the curve $\mathcal{F}_{m,n} : Y^m + X^n + 1 = 0$ defined over $\mathbb{F}_q$. In 2013, S. Tafazolian and F. Torres (??, Theorem 5), provided a characterization of the maximality of these curves. More precisely, they proved that the curve $\mathcal{F}_{m,n}$ is $\mathbb{F}_{q^2}$ -maximal if and only if both n and m divides $q + 1$. In this case, $\mathcal{F}_{m,n}$ is $\mathbb{F}_{q^2}$ -covered by the Hermitian curve. See also (??, Proposition 3.1). In 2014, these same authors provided a characterization of the maximality of curves of type $\mathcal{D}_{m,n} : Y^m + X^n + X = 0$ when $n - 1$ and m are positive integers coprime to p , and n divides m (??, Theorem 4.1). More precisely, they proved that the curve $\mathcal{D}_{m,n}$ is $\mathbb{F}_{q^2}$ -maximal if and only if $q \equiv -1 \pmod{m(n-1)}$. In this case, $\mathcal{F}_{m,n}$ is $\mathbb{F}_{q^2}$ -covered by the Hermitian curve. Here they use the fact that $\mathcal{D}_{m,n}$ is $\mathbb{F}_{q^2}$ -isomorphic to the curve $\mathcal{F}_{m,n-1}$, when m divides n . Thus, in these cases we have that the Hasse-Witt invariant of these curves are zero.

We now give an outline of the content of the thesis.

In Chapter 1, the basic theoretical foundations in algebraic function fields and algebraic curves over finite fields are laid. The content of this chapter will be used throughout the entire work. The results quoted in it are all very well-known, and most of the time the reader is referred to standard text books for their proofs.

In Chapter 2, we discuss the problem of classifying all $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of the type $Y^{q^2+q+1} = f(X)$, where $f \in \mathbb{F}_{q^3}[X]$. This discussion is motivated by the well known fact that any $\mathbb{F}_{q^2}$ -Frobenius nonclassical curve of the type $Y^{q+1} = f(X)$ is projectively equivalent to the Hermitian curve $Y^{q+1} = X^q + X$. The main result of the Section ?? states that an $\mathbb{F}_{q^3}$ -Frobenius nonclassical curve of the type $Y^{q^2+q+1} = f(X)$ is projectively equivalent to one the following curves: the Fermat curve of degree $q^2 + q + 1$, Norm-Trace curve of degree $q^2 + q + 1$, or the curve $Y^{q^2+q+1} = X^{q^2+1} + X^q$. Moreover, we compute the genus and the number of $\mathbb{F}_{q^3}$ -rational points for these curves. Finally, in Section ??, we use a canonical series to prove that the automorphism group of the curve $Y^{q^2+q+1} = X^{q^2+1} + X^q$ is a subgroup of order $2(q^4 + q^2 + 1)$ of the group $\text{PGL}(3, \mathbb{F}_{q^6})$ isomorphic to $C_{q^4+q^2+1} \rtimes C_2$.

In Chapter 3, for a suitable number h , we perform an analysis of the behaviour of the h -th iterate of the Cartier operator applied in the elements of a certain basis of the space of holomorphic differentials on $\mathcal{F}_{m,n}$ and $\mathcal{D}_{m,n}$. We then reduce the problem of computing the Hasse-Witt invariant of these curves to the problem of counting the cardinality of a certain finite subset of $\mathbb{N} \times \mathbb{N}$. In section ??, we use the results of section ?? to compute the Hasse-Witt invariant of some curves of the type $Y^m + X^{p^h-1} + 1 = 0$, when m divides $p^h - 1$.

Finally, we consider the hyperelliptic curves $\mathcal{C}_n = \mathcal{F}_{2,n}$ and $\mathcal{D}_n = \mathcal{D}_{2,n}$, and from the results obtained in the section ?? and by Lucas's Theorem, we reduce the problem of computing the Hasse-Witt invariant of these curves into the problem of counting the number of solutions to $x_1 + x_2p + \dots + x_hp^{h-1} \equiv 0 \pmod{(p^h - 1)/n}$ with $x_i \in \{0, \dots, (p-1)/2\}$, where h is the order of p modulo n . We apply this result to compute the Hasse-Witt invariant of some hyperelliptic curves of this type (Sections ?? and ??).

In Chapter 4, we compute the a -number of the curve given by $Y^{q^2+q+1} = X^{q^2+1} + X^q$, that is, the dimension of the space of exact holomorphic differentials on this curve. We also compute the Hasse-Witt invariant of this curve (when $q = p$) and the Fermat curve of degree $p^2 + p + 1$.

PRELIMINARIES

In this opening chapter, we shall collect most of the needed background in algebraic function field theory and algebraic curves. For a more comprehensive account we refer the reader to (??), (??) and (??).

1.1 Algebraic function fields

1.1.1 Places and divisors

Throughout this section we denote by k an arbitrary field.

Definition 1.1.1. *An algebraic function field F/k of one variable over k is an extension field $k \subseteq F$ such that F is a finite extension of $k(x)$ for some element $x \in F$ which is transcendental over k .*

Any function field F/k can be represented as a simple algebraic field extension of a rational function field $k(x)$, that is, $F = k(x, y)$ where $\varphi(y) = 0$ for some irreducible polynomial $\varphi(T) \in k(x)[T]$.

Definition 1.1.2. *A valuation ring of the function field F/k is a ring $\mathcal{O} \subseteq F$ with the following properties:*

1. $k \subsetneq \mathcal{O} \subsetneq F$,
2. for every $z \in F$ we have that $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Proposition 1.1.3 ((??), Proposition 1.1.5). *Let $\mathcal{O}$ be a valuation ring of the function field F/k . Then the following hold:*

1. $\mathcal{O}$ is a local ring, that is, $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^\times$, where $\mathcal{O}^\times$ is the group of units of $\mathcal{O}$.

2. Let $0 \neq x \in F$ then $x \in P$ if and only if $x^{-1} \notin \mathcal{O}$.
3. $\tilde{k} \subseteq \mathcal{O}$ and $\tilde{k} \cap P = \{0\}$, where $\tilde{k}$ is the field of constants of F/k , that is,

$$\tilde{k} = \{z \in F : z \text{ is algebraic over } k\}.$$

Theorem 1.1.4 ((??), Theorem 1.1.6). *Let $\mathcal{O}$ be a valuation ring of the function field F/k and let P be its unique maximal ideal. Then the following hold:*

1. P is a principal ideal.
2. if $P = t\mathcal{O}$ then each $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}^\times$.
3. $\mathcal{O}$ is a principal ideal domain. More precisely, if $P = t\mathcal{O}$ and $\{0\} \neq I \subseteq \mathcal{O}$ is an ideal then $I = t^n \mathcal{O}$ for some $n \in \mathbb{N}$.

Definition 1.1.5. 1. A place P of the function field F/k is the maximal ideal of some valuation ring $\mathcal{O}$ of F/k . Every $t \in P$ such that $P = t\mathcal{O}$ is called a local parameter for P (other notations are prime element or uniformizing variable).

2. $\mathbb{P}_F := \{P : P \text{ is a place of } F/k\}$.

Let P be the maximal ideal of the valuation ring $\mathcal{O}$ of F/k . It follows from Proposition ?? that $\mathcal{O}$ is uniquely determined by P , namely $\mathcal{O} = \{z \in F : z^{-1} \notin P\}$. Thus $\mathcal{O}_P := \mathcal{O}$ is called the valuation ring of the place P .

Definition 1.1.6. A discrete valuation of F/k is a function $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ with the following properties:

1. $v(x) = \infty$ if and only if $x = 0$.
2. $v(xy) = v(x) + v(y)$ for all $x, y \in F$.
3. $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in F$.
4. There exists an element $z \in F$ with $v(z) = 1$.
5. $v(a) = 0$ for all $0 \neq a \in k$.

Lemma 1.1.7 ((??), Lemma 1.1.11 (Strict Triangle Inequality)). *Let v be a discrete valuation of F/k and $x, y \in F$ with $v(x) \neq v(y)$. Then $v(x+y) = \min\{v(x), v(y)\}$.*

Definition 1.1.8. Let $P \in \mathbb{P}_F$ be a place of F/k and t be a local parameter for P . An element $0 \neq z \in F$ has a unique representation $z = t^n u$ with $u \in \mathcal{O}_P^\times$ and $n \in \mathbb{Z}$. Define the function $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ such that $v_P(z) := n$ and $v_P(0) := \infty$.

Theorem 1.1.9 ((??), Theorem 1.1.6). *Let F/k be a function field.*

1. *For a place $P \in \mathbb{P}_F$, the function v_P defined above is a discrete valuation of F/k . Moreover we have*

$$\begin{aligned}\mathcal{O}_P &= \{z \in F : v_P(z) \geq 0\}, \\ \mathcal{O}_P^\times &= \{z \in F : v_P(z) = 0\}, \\ P &= \{z \in F : v_P(z) > 0\}.\end{aligned}$$

2. *An element $x \in F$ is a local parameter for P if and only if $v_P(x) = 1$.*
3. *Conversely, suppose that v is a discrete valuation of F/k . Then the set $P := \{z \in F : v(z) > 0\}$ is a place of F/k , and $\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$ is the corresponding valuation ring.*
4. *Every valuation ring $\mathcal{O}$ of F/k is a maximal proper subring of F .*

Definition 1.1.10. *Let $P \in \mathbb{P}_F$.*

1. *$F_P := \mathcal{O}_P/P$ is the residue class field of P . The map $x \mapsto x(P)$ from F to $F_P \cup \{\infty\}$ is called the residue class map with respect to P .*
2. *$\deg P := [F_P : k]$ is called the degree of P . A place of degree one is also called a rational place of F/k .*

Proposition 1.1.11 ((??), Proposition 1.1.15). *If P is a place of F/k and $0 \neq x \in P$ then $\deg P \leq [F : k(x)] < \infty$.*

Definition 1.1.12. *Let $z \in F$ and $P \in \mathbb{P}_F$. We say that P is a zero of z if $v_P(z) > 0$; P is a pole of z if $v_P(z) < 0$. If $v_P(z) = m > 0$, P is a zero of z of order m ; if $v_P(z) = -m < 0$, P is a pole of z of order m .*

Proposition 1.1.13 ((??), Corollary 1.1.20). *Let F/k be a function field and $z \in F$ be an element transcendental over k . Then z has at least one zero and one pole. In particular $\mathbb{P}_F \neq \emptyset$.*

Proposition 1.1.14 ((??), Corollary 1.3.4). *In a function field F/k every element $0 \neq x \in F$ has only finitely many zeros and poles.*

From here on, F/k will always denote an algebraic function field of one variable such that k is the full constant field of F/k .

Definition 1.1.15. *The divisor group of F/k is defined as the (additively written) free abelian group which is generated by the places of F/k ; it is denoted by $\text{Div}(F)$. The elements of $\text{Div}(F)$ are called divisors of F/k . In other words a divisor is a formal sum*

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ with } n_P \in \mathbb{Z}, \text{ almost all } n_P = 0.$$

The support of D is defined as

$$\text{Supp}D := \{P \in \mathbb{P}_F : n_P \neq 0\}.$$

Two divisors $D = \sum n_P P$ and $D' = \sum n'_P P$ are added coefficientwise,

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

The zero element of the divisor group $\text{Div}(F)$ is the divisor

$$0 = \sum_{P \in \mathbb{P}_F} r_P P, \text{ with all } r_P = 0.$$

For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \text{Div}(F)$ we define $v_Q(D) := n_Q$, therefore

$$\text{Supp}D = \{P \in \mathbb{P}_F : v_P(D) \neq 0\} \text{ and } D = \sum_{P \in \text{Supp}(D)} v_P(D) \cdot P.$$

A partial ordering on $\text{Div}(F)$ is defined by

$$D_1 \leq D_2 \text{ if and only if } v_P(D_1) \leq v_P(D_2) \text{ for all } P \in \mathbb{P}_F.$$

If $D_1 \leq D_2$ and $D_1 \neq D_2$ we will also write $D_1 < D_2$. A divisor $D \geq 0$ is called effective (or positive). The degree of a divisor is defined as

$$\deg D := \sum_{P \in \text{Supp}(D)} v_P(D) \cdot \deg P,$$

and this yields a homomorphism $\deg : \text{div}(F) \longrightarrow \mathbb{Z}$.

Definition 1.1.16. Let $0 \neq x \in F$ and denote by Z (resp. N) the set of zeros (resp. poles) of x in $\mathbb{P}_F$. Then we define

$$\begin{aligned} \text{div}(x)_0 &:= \sum_{P \in Z} v_P(x) P, \text{ the zero divisor of } x, \\ \text{div}(x)_\infty &:= \sum_{P \in N} (-v_P(x)) P, \text{ the pole divisor of } x, \\ \text{div}(x) &:= \text{div}(x)_0 - \text{div}(x)_\infty. \end{aligned}$$

Clearly $\text{div}(x)_0 \geq 0$, $\text{div}(x)_\infty \geq 0$ and $\text{div}(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P$. The elements $0 \neq x \in F$ which are constant are characterized by

$$x \in k \Leftrightarrow \text{div}(x) = 0.$$

Definition 1.1.17. The set of divisors

$$\text{Prin}(F) := \{\text{div}(x) : 0 \neq x \in F\}$$

is called the group of principal divisors of F/k . This is a subgroup of $\text{Div}(F)$. The factor group

$$\text{Pic}(F) = \text{Div}(F)/\text{Prin}(F)$$

is called the divisor class group (or Picard group) of F/k . For a divisor $D \in \text{Div}(F)$, the corresponding element in the factor group $\text{Pic}(F)$ is denoted by $[D]$, the divisor class of D . Two divisors $D, D' \in \text{Div}(F)$ are said to be equivalent, written

$$D \sim D'$$

if $[D] = [D']$, that is, $D = D' + \text{div}(x)$ for some $x \in F \setminus \{0\}$. Note that $\sim$ is an equivalence relation.

1.1.2 Riemann-Roch spaces

Definition 1.1.18. For a divisor $A \in \text{Div}(F)$ we define the Riemann-Roch space associated to A by

$$\mathcal{L}(A) := \{x \in F : \text{div}(x) \geq -A\} \cup \{0\}.$$

Lemma 1.1.19 ((??), Lemma 1.4.6). Let $A \in \text{Div}(F)$. Then we have:

1. $\mathcal{L}(A)$ is a vector space over k .
2. If A' is a divisor equivalent to A , then $\mathcal{L}(A) \cong \mathcal{L}(A')$ (isomorphic as vector spaces over k).

Lemma 1.1.20 ((??), Lemma 1.4.7). 1. $\mathcal{L}(0) = k$.

2. If $A < 0$ then $\mathcal{L}(A) = \{0\}$.

Proposition 1.1.21 ((??), Proposition 1.4.9). For each divisor $A \in \text{Div}(F)$ the space $\mathcal{L}(A)$ is a finite-dimensional vector space over k .

Definition 1.1.22. For $A \in \text{Div}(F)$ the integer $\ell(A) := \dim \mathcal{L}(A)$ is called the dimension of the divisor A .

Theorem 1.1.23 ((??), Theorem 1.4.11). All principal divisors have degree zero. More precisely, if $x \in F/k$ then

$$\deg \text{div}(x)_0 = \deg \text{div}(x)_\infty = [F : k(x)].$$

Corollary 1.1.24 ((??), Corollary 1.4.12). 1. Let A, A' be divisors with $A \sim A'$. Then we have

$$\ell(A) = \ell(A') \text{ and } \deg A = \deg A'.$$

2. If $\deg A < 0$ then $\ell(A) = 0$.
3. For a divisor A of degree zero the following assertions are equivalent:
 - (a) A is principal.

$$(b) \ell(A) \geq 1.$$

$$(c) \ell(A) = 1.$$

Proposition 1.1.25 ((??), Proposition 1.4.14). *There exists a constant $\gamma \in \mathbb{Z}$ such that for all divisors $A \in \text{Div}(F)$ the following hold:*

$$\deg A - \ell(A) \leq \gamma.$$

Definition 1.1.26. *The genus g of F/k is defined by*

$$g := \max\{\deg A - \ell(A) + 1 : A \in \text{Div}(F)\}.$$

Note that this definition makes sense by Proposition ?? . Moreover, if $A = 0$ then $\deg 0 - \ell(0) + 1 = 0$, hence $g \geq 0$.

Theorem 1.1.27 ((??), Theorem 1.4.17 (Riemann's Theorem)). *Let F/k be a function field of genus g . Then we have:*

1. *For all divisors $A \in \text{Div}(F)$,*

$$\ell(A) \geq \deg A + 1 - g.$$

2. *There exists an integer c , depending only on the function field F/k , such that*

$$\ell(A) = \deg A + 1 - g,$$

whenever $\deg A \geq c$.

1.1.3 The Riemann-Roch theorem

In this section F/k denotes an algebraic function field of genus g .

Definition 1.1.28. *For $A \in \text{Div}(F)$ the integer*

$$i(A) := \ell(A) - \deg A + g - 1$$

is called the index of specialty of A .

Definition 1.1.29. *An adele (or repartition) of F/k is a mapping*

$$\begin{aligned} \alpha : \mathbb{P}_F &\longrightarrow F \\ P &\longmapsto \alpha_P \end{aligned}$$

such that $\alpha_P \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$. We regard an adele as an element of the direct product $\prod_{P \in \mathbb{P}_F} F$ and therefore use the notation $\alpha = (\alpha_P)$. The set

$$\mathcal{A}_F = \{\alpha : \alpha \text{ is an adele of } F/k\}$$

is called the *adele space* of F/k . Note that $\mathcal{A}_F$ is a vector space over k .

The *principal adele* of an element $x \in F$ is the adele with all components α_P satisfying $\alpha_P = x$ (note that this definition makes sense because any element $0 \neq x \in F$ has only finitely many zeros and poles). This gives an embedding $F \hookrightarrow \mathcal{A}_F$. The valuations v_P of F/k extend naturally to $\mathcal{A}_F$ by setting $v_P(\alpha) = v_P(\alpha_P)$. By definition we have that $v_P(\alpha) \geq 0$ for almost all $P \in \mathbb{P}_F$.

Definition 1.1.30. For $A \in \text{Div}(F)$ we define

$$\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F : v_P(\alpha) \geq -v_P(A) \text{ for all } P \in \mathbb{P}_F\}.$$

Obviously this is a k -subspace of $\mathcal{A}_F$.

Theorem 1.1.31 ((??), Theorem 1.5.4; Corollary 1.5.5). *The following assertions hold:*

1. $i(A) = \dim(\mathcal{A}_F / (\mathcal{A}_F(A) + F))$ for all $A \in \text{Div}(F)$.
2. $g = \dim(\mathcal{A}_F / (\mathcal{A}_F(0) + F))$.

Definition 1.1.32. A *Weil differential* of F/k is a k -linear map $\omega : \mathcal{A}_F \rightarrow k$ vanishing on $\mathcal{A}_F(A) + F$ for some divisor $A \in \text{Div}(F)$. We call

$$\Omega_F = \{\omega : \omega \text{ is a Weil differential of } F/k\}$$

the *module of Weil differentials* of F/k . For $A \in \text{Div}(F)$ let

$$\Omega_F(A) = \{\omega \in \Omega_F : \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

Note that Ω_F is a k -vector space and $\Omega_F(A)$ is a subspace of Ω_F .

Lemma 1.1.33 ((??), Lemma 1.5.7). For $A \in \text{div}(F)$ we have $\dim \Omega_F(A) = i(A)$.

Definition 1.1.34. For $x \in F$ and $\omega \in \Omega_F$ we define

$$\begin{aligned} x\omega : \mathcal{A}_F &\longrightarrow k \\ \alpha &\longmapsto \omega(x\alpha) \end{aligned}$$

Note that $x\omega$ is again a Weil differential of F/k . Hence Ω_F is a vector space over F .

Proposition 1.1.35 ((??), Proposition 1.5.9). Ω_F is a one-dimensional vector space over F .

Consider for a fixed $0 \neq \omega \in \Omega_F$ the set of divisors

$$M(\omega) = \{A \in \text{div}(F) : \omega \text{ vanishes on } \mathcal{A}_F(A) + F\}.$$

Lemma 1.1.36 ((?), Lemma 1.5.10). *Let $0 \neq \omega \in \Omega_F$. Then there exists a uniquely determined divisor $W \in M(\omega)$ such that $A \leq W$ for all $A \in M(\omega)$.*

Definition 1.1.37. *i) The divisor $\text{div}(\omega)$ of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of F/k satisfying*

- 1) ω vanishes on $\mathcal{A}_F(\text{div}(\omega)) + F$, and
- 2) if ω vanishes on $\mathcal{A}_F(A) + F$ then $A \leq \text{div}(\omega)$.

ii) For $0 \neq \omega \in \Omega_F$ and $P \in \mathbb{P}_F$ we define $v_P(\omega) = v_P(\text{div}(\omega))$.

iii) A place P is said to be a zero (resp. pole) of ω if $v_P(\omega) > 0$ (resp. $v_P(\omega) < 0$). The Weil differential ω is called regular at P if $v_P(\omega) \geq 0$, and ω is said to be holomorphic (or regular) if it is regular at all places $P \in \mathbb{P}_F$.

iv) A divisor W is called a canonical divisor of F/k if $W = \text{div}(\omega)$ for some $\omega \in \Omega_F$.

It follows from the definitions that

$$\Omega_F(A) = \{\omega \in \Omega_F : \omega = 0 \text{ or } \text{div}(\omega) \geq A\} \text{ and } \Omega_F(0) = \{\omega \in \Omega_F : \omega \text{ is holomorphic}\}.$$

Moreover, as a consequence of Lemma ?? we obtain $\dim \Omega_F(0) = g$.

Proposition 1.1.38 ((?), Proposition 1.5.13). *i) For $0 \neq x \in F$ and $0 \neq \omega \in \Omega_F$ we have*

$$\text{div}(x\omega) = \text{div}(x) + \text{div}(\omega).$$

ii) Any two canonical divisors of F/k are equivalent.

Note that the canonical divisors of F/k form a whole class $[W]$ in the divisor class group $\text{Pic}(F)$; this divisor class is called the *canonical class* of F/k .

Theorem 1.1.39 ((?), Theorem 1.5.14 (Duality Theorem)). *Let A be an arbitrary divisor and $W = \text{div}(\omega)$ be a canonical divisor of F/k . Then the mapping*

$$\begin{array}{ccc} \mu : \mathcal{L}(W - A) & \longrightarrow & \Omega_F(A) \\ x & \longmapsto & x\omega \end{array}$$

is an isomorphism of k -vector spaces. In particular, $i(A) = \ell(W - A)$.

Theorem 1.1.40 ((?), Theorem 1.5.15 (Riemann-Roch Theorem)). *Let W be a canonical divisor of F/k . Then for each divisor $A \in \text{Div}(F)$,*

$$\ell(A) = \deg A + 1 - g + \ell(W - A).$$

Corollary 1.1.41 ((?), Corollary 1.5.16). *For a canonical divisor W we have $\deg W = 2g - 2$ and $\ell(W) = g$.*

Theorem 1.1.42 ((??), Theorem 1.5.17). *If A is a divisor of F/k of degree $\deg A \geq 2g - 1$ then $\ell(A) = \deg A + 1 - g$.*

Proposition 1.1.43 ((??), Proposition 1.6.1). *Suppose that $g_0 \in \mathbb{Z}$ and $W_0 \in \text{Div}(F)$ satisfy*

$$\ell(A) = \deg A + 1 - g_0 + \ell(W_0 - A)$$

for all $A \in \text{Div}(F)$. Then $g_0 = g$, and W_0 is a canonical divisor.

Proposition 1.1.44 ((??), Proposition 1.6.2). *A divisor B is canonical if and only if $\deg B = 2g - 2$ and $\ell(B) \geq g$.*

Proposition 1.1.45 ((??), Proposition 1.6.3). *For a function field F/k the following conditions are equivalent:*

1. *F/k is rational, that is, $F = k(x)$ for some x which is transcendental over the field k .*
2. *F/k has genus 0, and there exists some divisor $A \in \text{Div}(F)$ with $\deg A = 1$.*

Proposition 1.1.46 ((??), Proposition 1.6.6). *Let $P \in \mathbb{P}_F$. Then for each $n \geq 2g$ there exists an element $x \in F$ with pole divisor $\text{div}(x)_\infty = nP$.*

Definition 1.1.47. *For any place P , a non-negative integer n is a non-gap (or pole number) at P if there exists a function $x \in F$ such that $\text{div}(x)_\infty = nP$; otherwise, n is a gap number at P .*

Lemma 1.1.48 ((??), Chapter 6, Lemma 6.87). *The set of non-gaps at P is a sub-semigroup $\mathcal{H}(P)$ of the additive semigroup of the non-negative integers.*

Definition 1.1.49. *The set $\mathcal{H}(P)$ is the Weierstrass semigroup at P .*

Clearly n is a non-gap at P if and only if $\ell(nP) > \ell((n-1)P)$.

Theorem 1.1.50 ((??), Theorem 1.6.8 (Weierstrass Gap Theorem)). *Suppose that F/k has genus $g > 0$ and P is a place of degree one. Then there exist exactly g gap numbers $n_1 < \dots < n_g$ at P . We have $n_1 = 1$ and $n_g \leq 2g - 1$.*

1.1.4 Extension of algebraic function fields

Let us first fix some notation to be maintained throughout the entire section. F/k denotes an algebraic function field of one variable with full constant field k . The field k is assumed to be perfect, that is, there does not exist a purely inseparable extension L/k with $1 < [L:k] < \infty$. We consider function fields F'/k' (where k' is the full constant field of F') such that $F \subseteq F'$ is an algebraic extension and $k \subseteq k'$.

Definition 1.1.51. 1. *An algebraic function field F'/k' is called an algebraic extension of F/k if $F \subseteq F'$ is an algebraic field extension and $k \subseteq k'$.*

2. The algebraic extension F'/k' of F/k is called a constant field extension if $F' = Fk'$, the composite field of F and k' .
3. The algebraic extension F'/k' of F/k is called a finite extension if $[F' : F] < \infty$.

Definition 1.1.52. Consider an algebraic extension F'/k' of F/k . A place $P' \in \mathbb{P}_{F'}$ is said to lie over $P \in \mathbb{P}_F$ if $P \subseteq P'$. We also say that P' is an extension of P or that P lies under P' , and we write $P'|P$.

Proposition 1.1.53 ((??), Proposition 3.1.4). Let F'/k' be an algebraic extension of F/k . Suppose that P (resp. P') is a place of F/k (resp. F'/k'), and let $\mathcal{O}_P \subseteq F$ (resp. $\mathcal{O}_{P'} \subseteq F'$) denote the corresponding valuation ring, v_P (resp. $v_{P'}$) the corresponding discrete valuation. Then the following assertions are equivalent:

1. $P'|P$.
2. $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.
3. There exists an integer $e \geq 1$ such that $v_{P'}(x) = e \cdot v_P(x)$ for all $x \in F$. Moreover, if $P'|P$ then

$$P = P' \cap F \text{ and } \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

For this reason, P is also called the restriction of P' to F .

Definition 1.1.54. Let F'/k' be an algebraic extension of F/k , and let $P' \in \mathbb{P}_{F'}$ be a place of F'/k' lying over $P \in \mathbb{P}_F$.

1. The integer $e(P'|P) := e$ with

$$v_{P'}(x) = e \cdot v_P(x) \text{ for all } x \in F$$

is called the ramification index of P' over P . We say that $P'|P$ is ramified if $e(P'|P) > 1$, and $P'|P$ is unramified if $e(P'|P) = 1$.

2. $f(P'|P) := [F'_{P'} : F_P]$ is called the relative degree of P' over P .

Proposition 1.1.55 ((??), Proposition 3.1.7). Let F'/k' be an algebraic extension of F/k .

1. For each place $P' \in \mathbb{P}_{F'}$ there exists exactly one place $P \in \mathbb{P}_F$ such that $P'|P$, namely $P = P' \cap F$.
2. Conversely, every place $P \in \mathbb{P}_F$ has at least one, but only finitely many extensions $P' \in \mathbb{P}_{F'}$.

Proposition 1.1.56 ((??), Proposition 3.1.11 (Fundamental Equality)). Let F'/k' be an finite extension of F/k , let P be a place of F/k . If $P_1, \dots, P_m$ are all the places of F'/k' lying over P , then

$$\sum_{i=1}^m e(P_i|P) f(P_i|P) = [F' : F].$$

Definition 1.1.57. Let F'/k' be an extension of F/k of degree $[F' : F] = n$, and let $P \in \mathbb{P}_F$.

1. P splits completely in F'/F if there exist exactly n distinct places $P' \in \mathbb{P}_{F'}$ with $P'|P$.
2. P is totally ramified in F'/F if there exists a place $P' \in \mathbb{P}_{F'}$ with $P'|P$ and $e(P'|P) = n$.

By the Fundamental Equality it is clear that a place $P \in \mathbb{P}_F$ splits completely in F'/F if and only if $e(P'|P) = f(P'|P) = 1$ for all places $P'|P$ in F' . If P is totally ramified in F'/F then there exists exactly one place $P' \in \mathbb{P}_{F'}$ with $P'|P$.

Theorem 1.1.58 ((??), Proposition 3.7.3 (Kummer Extensions)). Let F/k be an algebraic function field where k contains a primitive n -th root of unity (with $n > 1$ and n relatively prime to the characteristic of k). Suppose that $u \in F$ is an element satisfying

$$u \neq w^d \text{ for all } w \in F \text{ and } d \mid n, d > 1. \quad (1.1)$$

Let

$$F' = F(y) \text{ with } y^n = u.$$

Such an extension F'/F is said to be a Kummer extension of F . We have:

1. The polynomial $\Phi(T) = T^n - u$ is the minimal polynomial of y over F (in particular, it is irreducible over F). The extension F'/F is Galois of degree $[F' : F] = n$; its Galois group is cyclic, and the automorphisms of F'/F are given by $\sigma(y) = \zeta y$, where $\zeta \in k$ is an n -th root of unity.
2. Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ be an extension of P . Then $e(P'|P) = n/\gcd(n, v_P(u))$.
3. If k' denotes the constant field of F' and $\mathfrak{g}$ (resp. $\mathfrak{g}'$) the genus of F/k (resp. F'/k'), then

$$\mathfrak{g}' = 1 + \frac{n}{[k' : k]} \left(\mathfrak{g} - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{\gcd(n, v_P(u))}{n} \right) \deg P \right).$$

Theorem 1.1.59 ((??), Proposition 6.3.1). Suppose that $F = k(x, y)$ is defined by the equation

$$y^n = a \prod_{i=1}^s p_i(x)^{n_i}$$

with $s > 0$ pairwise distinct irreducible monic polynomials $p_i(x) \in k[x]$, $0 \neq a \in k$, $0 \neq n_i \in \mathbb{Z}$, $\text{char}(k) \nmid n$ and $\gcd(n, n_i) = 1$ for $1 \leq i \leq s$. Then we have:

1. k is the full constant field of F , and $[F : k(x)] = n$. If k contains a primitive n -th root of unity, $F/k(x)$ is a cyclic field extension.

2. Let P_i (resp. P_∞) denote the zero of $p_i(x)$ (resp. the pole of x) in $k(x)$. The places $P_1, \dots, P_s$ are totally ramified in $F/k(x)$. All places $Q_\infty \in \mathbb{P}_F$ with $Q_\infty | P_\infty$ have ramification index $e(Q_\infty | P_\infty) = n/d$ where

$$d = \gcd\left(n, \sum_{i=1}^s n_i \deg(p_i(x))\right). \quad (1.2)$$

No places $P \in \mathbb{P}_{k(x)}$ other than $P_1, \dots, P_s, P_\infty$ ramify in $F/k(x)$.

3. The genus of F/k is

$$g = \frac{n-1}{2} \left(-1 + \sum_{i=1}^s \deg(p_i(x)) \right) - \frac{d-1}{2}, \quad (1.3)$$

with d as in (??).

Lemma 1.1.60. Let $\mathcal{C} : Y^n = f(X)$ be a curve, where $f(X) = a \prod_{i=1}^s (X - r_i)^{d_i} \in \mathbb{F}_q[X]$, $a \neq 0$, $n = \sum_{i=1}^s d_i$ and $\gcd(n, p) = \gcd(n, d_i) = 1$ for $1 \leq i \leq s$. Then the genus of $\mathcal{C}$ is $g(\mathcal{C}) = \frac{(n-1)(s-2)}{2}$.

Proof. Since $d = \gcd(n, \sum_{i=1}^s d_i) = n$, it follows from Proposition ?? that $g(\mathcal{C}) = \frac{(n-1)(s-2)}{2}$. $\square$

1.1.5 The Zeta function and the Hasse-Weil Bound

Throughout this section, F denotes an algebraic function field of genus g whose constant field is the finite field $\mathbb{F}_q$. As before, $\text{Div}(F)$ denotes the divisor group of the function field $F/\mathbb{F}_q$. A divisor $A = \sum_{P \in \mathbb{P}_F} a_P P$ is effective if all $a_P \geq 0$; we write $A \geq 0$.

Lemma 1.1.61 ((??), Lemma 5.1.1). For every $n \geq 0$ there exists only finitely many effective divisors of degree n .

Definition 1.1.62 ((??), Definition 5.1.2 and Proposition 5.1.3). 1. The set $\text{Div}^0(F) := \{A \in \text{Div}(F) : \deg A = 0\}$ is a subgroup of $\text{Div}(F)$ called the group of divisors of degree zero.

2. The set $\text{Pic}^0(F) := \{[A] \in \text{Pic}(F) : \deg[A] = 0\}$ is a finite group called the group of divisors classes of degree zero.

3. The order of $\text{Pic}^0(F)$ is called the class number of $F/\mathbb{F}_q$.

Thus, let A_n be the cardinality of

$$\{A \in \text{Div}(F) : A \geq 0 \text{ and } \deg A = n\}.$$

For instance, $A_0 = 1$ and A_1 is the number of places $P \in \mathbb{P}_F$ of degree one.

Definition 1.1.63. The power series

$$Z(T) := Z_F(T) := \sum_{n=0}^{\infty} A_n T^n \in \mathbb{C}[[T]]$$

is called the Zeta function of $F/\mathbb{F}_q$.

Proposition 1.1.64 ((?), Proposition 5.1.8 (Euler Product)). *For $|T| < q^{-1}$ the Zeta function can be represented as an absolutely convergent product*

$$Z(T) = \prod_{P \in \mathbb{P}_F} (1 - T^{\deg P})^{-1}.$$

In Particular, $Z(T) \neq 0$ for $|T| < q^{-1}$.

Proposition 1.1.65 ((?), Proposition 5.1.13 (Functional Equation of the Zeta Function)). *The Zeta function of $F/\mathbb{F}_q$ satisfies the functional equation*

$$Z(T) = q^{g-1} T^{2g-2} Z\left(\frac{1}{qT}\right).$$

Definition 1.1.66. *The polynomial $L(T) := (1 - T)(1 - qT)Z(T)$ is called the L -polynomial of $F/\mathbb{F}_q$.*

Theorem 1.1.67 ((?), Theorem 5.1.15). (a) $L(T) \in \mathbb{Z}[T]$ and $\deg(L(T)) = 2g$.

(b) (functional Equation) $L(T) = q^g T^{2g} L(1/qT)$.

(c) $L(1) = |\text{Pic}^0(F)|$, the class number of $F/\mathbb{F}_q$.

(d) We write $L(T) = a_0 + a_1 T + \cdots + a_{2g} T^{2g}$. Then the following hold:

a) $a_0 = 1$ and $a_{2g} = q^g$.

b) $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$.

c) $a_1 = N - (q + 1)$ where N is the number of places $P \in \mathbb{P}_F$ of degree one.

(e) $L(T)$ factors in $\mathbb{C}[T]$ in the form

$$L(T) = \prod_{i=1}^{2g} (1 - \alpha_i T) \tag{1.4}$$

The complex numbers $\alpha_1, \dots, \alpha_{2g}$ are algebraic integers, and they can be arranged in such a way that $\alpha_i \alpha_{g+i} = q$ hold for $i = 1, \dots, g$.

(f) If $L_r(T) := (1 - T)(1 - q^r T)Z_r(T)$ denotes the L -polynomial of the constant field extension $F_r = F\mathbb{F}_{q^r}$, then

$$L_r(T) = \prod_{i=1}^{2g} (1 - \alpha_i^r T),$$

where the α_i are given by (??).

The above theorem shows that the cardinality $N(F)$ of $\{P \in \mathbb{P}_F : \deg P = 1\}$ can easily be calculated if the L -polynomial $L(T)$ of $F/\mathbb{F}_q$ is known. More generally we consider for $r \geq 1$ the cardinality N_r of $\{P \in \mathbb{P}_{F_r} : \deg P = 1\}$, where $F_r = F\mathbb{F}_{q^r}$ is the constant field extension of $F/\mathbb{F}_q$ of degree r .

Corollary 1.1.68 ((??), Corollary 5.1.16). *For all $r \geq 1$*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r,$$

where $\alpha_1, \dots, \alpha_{2g} \in \mathbb{C}$ are the reciprocals of the roots of $L(T)$. In particular,

$$N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Theorem 1.1.69 ((??), Theorem 5.2.1 (Hasse-Weil)). *The reciprocals of the roots of $L(T)$ satisfy*

$$|\alpha_i| = q^{1/2} \text{ for } i = 1, \dots, 2g.$$

Theorem 1.1.70 ((??), Theorem 5.2.3 (Hasse-Weil Bound)). *The number $N = N(F)$ of places of $F/\mathbb{F}_q$ of degree one satisfies the inequality*

$$|N - (q + 1)| \leq 2gq^{1/2}.$$

Theorem 1.1.71 ((??), Theorem 5.3.1 (Serre Bound)). *For a function field $F/\mathbb{F}_q$ of genus g the number of places of degree one is bounded by*

$$|N - (q + 1)| \leq g[2q^{1/2}],$$

where $[a]$ denotes the integer part of the real number a .

Definition 1.1.72. A function field $F/\mathbb{F}_q$ of genus g is said to be maximal if $N = q + 1 + 2gq^{1/2}$.

Proposition 1.1.73 ((??), Proposition 5.3.3 (Ihara)). *Suppose that $F/\mathbb{F}_q$ is a maximal function field. Then $g \leq (q - q^{1/2})/2$.*

1.2 Algebraic function fields of a curve

Throughout this section we denote by $\mathbb{K}$ the algebraic closure of a field of characteristic $p > 0$.

1.2.1 Algebraic function fields

Definition 1.2.1. Let $\mathcal{C} : f(x, y) = 0$ be an affine irreducible algebraic curve defined over $\mathbb{K}$. The function field of $\mathcal{C}$, written $\mathbb{K}(\mathcal{C})$ is the quotient field of the domain $\mathbb{K}[x, y]/(f)$.

Definition 1.2.2. Let $\mathcal{C} : F(x, y, z) = 0$ be a projective and irreducible algebraic curve defined over $\mathbb{K}$. The function field of $\mathcal{C}$ is

$$\mathbb{K}(\mathcal{C}) = \left\{ \frac{G}{H} : \begin{array}{l} G, H \in \mathbb{K}[x, y, z] \text{ are homogeneous polynomials} \\ \text{of the same degree, where } F \text{ does not divide } H \end{array} \right\} / \sim,$$

where $\sim$ is an equivalence relation, such that $\frac{G}{H} \sim \frac{G'}{H'}$ if and only if F divides $(GH' - G'H)$.

Let $\mathcal{C} : F(x, y, z) = 0$ be a projective and geometrically irreducible algebraic curve and $\mathcal{C}' : f(x, y) = 0$ where $f(x, y) = F(x, y, 1) \in \mathbb{K}[x, y]$. Note that $\alpha : \mathbb{K}(\mathcal{C}') \rightarrow \mathbb{K}(\mathcal{C})$, with

$$\alpha\left(\frac{g(x, y)}{h(x, y)}\right) = \frac{g\left(\frac{x}{z}, \frac{y}{z}\right)}{h\left(\frac{x}{z}, \frac{y}{z}\right)} \text{ and } \alpha^{-1}\left(\frac{G(x, y, z)}{H(x, y, z)}\right) = \frac{G(x, y, 1)}{H(x, y, 1)},$$

is a $\mathbb{K}$ -isomorphism. Thus, $\mathbb{K}(\mathcal{C})$ is a finite extension of $\mathbb{K}(x)$, where x is transcendental over $\mathbb{K}$. Moreover, $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ where the irreducible polynomial $f(x, T) \in \mathbb{K}(x)[T]$ is such that $f(x, y) = 0$.

Definition 1.2.3. Let $\mathcal{C}$ be an irreducible algebraic curve. The genus $\mathfrak{g}(\mathcal{C})$ of $\mathcal{C}$ is the genus of $\mathbb{K}(\mathcal{C})$.

Theorem 1.2.4 ((?), Theorem 5.57). The genus of a nonsingular, irreducible plane curve of degree n is $\mathfrak{g} = \frac{(n-1)(n-2)}{2}$.

Proposition 1.2.5 ((?), Theorems 4.31, 4.32, 4.46 and 5.28). Each point of C is associated to at least one and at most a finite number of places of $\mathbb{K}(\mathcal{C})$. Moreover, each simple point of C is associated to exactly one place of $\mathbb{K}(\mathcal{C})$.

Definition 1.2.6. Let $P \in \mathcal{C}$ and $\varphi \in \mathbb{K}(\mathcal{C})$. We say that φ is defined at P if φ has a representation of the form $\varphi = G/H$ such that $H(P) \neq 0$. In this case, $\varphi(P) = G(P)/H(P)$ is the value φ in P .

Observe that for each $P \in \mathcal{C}$ we have

$$\mathcal{O}_P(\mathcal{C}) := \{\varphi \in \mathbb{K}(\mathcal{C}) : \varphi \text{ is defined at } P\}$$

is a subring of $\mathbb{K}(\mathcal{C})$. Moreover $\mathcal{O}_P(\mathcal{C})$ is a local ring, with maximal ideal

$$\mathfrak{m}_P(\mathcal{C}) = \{\varphi = G/H \in \mathbb{K}(\mathcal{C}) : H(P) \neq 0 \text{ and } G(P) = 0\}.$$

The ring $\mathcal{O}_P(\mathcal{C})$ is called the *local ring* of $\mathcal{C}$ at P . Note that the value $\varphi(P)$ of a function $\varphi \in \mathcal{O}_P(\mathcal{C})$ is well-defined (cf. (?, Comments on Page 47)).

1.2.2 Rational transformations and morphisms

Definition 1.2.7. Let $\mathcal{C} : f(x, y) = 0$ be an affine irreducible algebraic curve defined over $\mathbb{K}$. A rational transformation of $\mathcal{C}$ is a mapping

$$\begin{aligned} \varphi : \quad \mathcal{C} &\dashrightarrow \mathbb{A}^2 \\ (x, y) &\longmapsto \left(\frac{g(x, y)}{l(x, y)}, \frac{h(x, y)}{l(x, y)} \right) \end{aligned}$$

where $g, h, l \in \mathbb{K}[x, y]$ and $l(x, y)$ not vanishing identically on $\mathcal{C}$. From this, for each $P(a, b) \in \mathcal{C}$ such that $l(a, b) \neq 0$ we have

$$\varphi(a, b) = \left(\frac{g(a, b)}{l(a, b)}, \frac{h(a, b)}{l(a, b)} \right).$$

The expression for φ is not uniquely determined, but $\varphi(a, b)$ does not depend on the particular chosen functions. The mapping φ is *defined* at $P = (a, b)$ if φ has a representation of the form

$$\varphi(x, y) = \left(\frac{g(x, y)}{l(x, y)}, \frac{h(x, y)}{l(x, y)} \right)$$

such that $l(a, b) \neq 0$. If there exists no such expression, then φ is not defined at $P = (a, b)$.

In terms of homogeneous coordinates, a *rational transformation* is a mapping $\varphi : \mathcal{C} \dashrightarrow \mathbb{P}^2$ with

$$\varphi(x : y : z) = (G_1(x, y, z) : G_2(x, y, z) : G_3(x, y, z))$$

with G_1, G_2, G_3 homogeneous polynomials of the same degree. The mapping φ is *defined* at $Q = (a : b : c)$ if φ has a representation of the form

$$\varphi(x : y : z) = (G_1(x, y, z) : G_2(x, y, z) : G_3(x, y, z))$$

with $G_i(a, b, c) \neq 0$ for some $i \in \{1, 2, 3\}$. In this case, $\varphi(Q)$ is defined to be $(G_1(Q) : G_2(Q) : G_3(Q))$. The triple (G_1, G_2, G_3) is not unique. But, if

$$(G_1(x, y, z) : G_2(x, y, z) : G_3(x, y, z)) = (H_1(x, y, z) : H_2(x, y, z) : H_3(x, y, z))$$

where H_1, H_2, H_3 are also homogeneous polynomials of the same degree, and H_1, H_2, H_3 do not all vanish at Q , then $(G_1(Q) : G_2(Q) : G_3(Q))$ and $(H_1(Q) : H_2(Q) : H_3(Q))$ define the same point $\varphi(Q)$. In this way, φ is defined at all but a finite number of points of $\mathcal{C}$ (cf. (??, Comments on Page 114)).

Definition 1.2.8. Let $\mathcal{C}$ and $\mathcal{D}$ be projective and irreducible algebraic curves defined over $\mathbb{K}$.

1. A morphism $\varphi : \mathcal{C} \rightarrow \mathbb{P}^2$ is a rational transformation defined at all points of $\mathcal{C}$.
2. An isomorphism of $\mathcal{C}$ with $\mathcal{D}$ is a one-to-one morphism φ from $\mathcal{C}$ onto $\mathcal{D}$ such that φ^{-1} is a morphism.
3. A birational transformation of $\mathcal{C}$ with $\mathcal{D}$ is a rational transformation φ from $\mathcal{C}$ into $\mathcal{D}$ such that there exists a rational transformation $\varphi^{-1} : \mathcal{D} \dashrightarrow \mathcal{C}$ with $\varphi^{-1} \circ \varphi = \text{Id}_{\mathcal{C}}$ and $\varphi \circ \varphi^{-1} = \text{Id}_{\mathcal{D}}$, where $\varphi^{-1} \circ \varphi = \text{Id}_{\mathcal{C}}$ means that, for each $Q \in \mathcal{C}$ such that φ is defined at Q and φ^{-1} is defined at $\varphi(Q)$, the equality $\varphi^{-1}(\varphi(Q)) = Q$ holds, and similarly for $\varphi \circ \varphi^{-1} = \text{Id}_{\mathcal{D}}$.
4. We say that $\mathcal{C}$ and $\mathcal{D}$ are birationally equivalent if there exists a birational transformation from $\mathcal{C}$ to $\mathcal{D}$.

Definition 1.2.9. Let k be a field of characteristic $p > 0$.

1. A projectivity (or projective transformation) $\varphi_A : \mathbb{P}^2 \longrightarrow \mathbb{P}^2$ is given by

$$\varphi_A(x : y : z) = (\alpha_{11}x + \alpha_{12}y + \alpha_{13}z : \alpha_{21}x + \alpha_{22}y + \alpha_{23}z : \alpha_{31}x + \alpha_{32}y + \alpha_{33}z)$$

where $\alpha_{ij} \in k$ and $A = (\alpha_{ij})$ is a suitable nonsingular matrix. The projectivities of $\mathbb{P}^2$ constitute its projective general linear group $\mathrm{PGL}(3, k)$.

2. Two projective curves $\mathcal{C} : F(x, y, z) = 0$ and $\mathcal{D} : G(x, y, z) = 0$, defined over k , are said to be k -projectively equivalent if there exists a projectivity φ_A such that $F(x, y, z) = G(\varphi_A(x : y : z))$. In this case, since A is a nonsingular matrix, it follows that $\mathcal{C}$ and $\mathcal{D}$ are birationally equivalent.

Theorem 1.2.10 ((??), Section 6.6; Proposition 12). *Two projective and irreducible algebraic curves are birationally equivalent if and only if their function fields are isomorphic.*

Corollary 1.2.11 ((??), Section 6.6). *Every curve is birationally equivalent to a plane curve.*

An irreducible algebraic curve is said to be *rational* if it is birationally equivalent to $\mathbb{A}^1$ (or $\mathbb{P}^1$).

Theorem 1.2.12 ((??), Section 3.2, Theorem 1). *Let $\mathcal{C}$ be an irreducible algebraic curve and $P \in \mathcal{C}$. The point P is nonsingular if and only if $\mathcal{O}_P(\mathcal{C})$ is a discrete valuation ring. In this case, if $L = ax + by + c$ is any line through P that is not tangent to $\mathcal{C}$ at P , then the image l of L in $\mathcal{O}_P(\mathcal{C})$ is a local parameter for $\mathcal{O}_P(\mathcal{C})$.*

Proposition 1.2.13 ((??), Section 7.1, Corollary 3). *Two nonsingular projective curves are isomorphic if and only if their function fields are isomorphic.*

Proposition 1.2.14 ((??), Section 7.1, Corollary 4). *Let $\mathcal{C}$ be a nonsingular projective curve. Then there exists a natural one-to-one correspondence between the points of $\mathcal{C}$ and the discrete valuation rings of $\mathbb{K}(\mathcal{C})$. If $P \in \mathcal{C}$ then $\mathcal{O}_P(\mathcal{C})$ is the corresponding discrete valuation ring.*

Theorem 1.2.15 ((??), Section 7.5, Theorem 3). *Let $\mathcal{C}$ be a projective curve. Then $\mathcal{C}$ is birationally equivalent to a nonsingular projective curve $\mathcal{X}$.*

We say that $\mathcal{X}$ is a *nonsingular model* of $\mathcal{C}$, or of $\mathbb{K}(\mathcal{C})$.

Corollary 1.2.16 ((??), Section 7.5). *There exists a natural one-to-one correspondence between nonsingular projective curves over $\mathbb{K}$ and algebraic function fields in one variable over $\mathbb{K}$.*

1.2.3 Divisors and canonical divisors of a curve

Let $\mathcal{X}$ be a projective, nonsingular and geometrically irreducible algebraic curve of genus $g > 0$ defined over $\mathbb{K}$, the algebraic closure of a field of characteristic $p > 0$. It follows from Proposition ?? that there exists a natural one-to-one correspondence between the points of

$\mathcal{X}$ and the places of $\mathbb{K}(\mathcal{X})$. Moreover, if $P \in \mathcal{X}$ then $\mathfrak{m}_P(\mathcal{X})$ is a principal ideal of $\mathcal{O}_P(\mathcal{X})$, namely $\mathfrak{m}_P(\mathcal{X}) = t\mathcal{O}_P(\mathcal{X})$, where t is a local parameter for $\mathcal{X}$ at P . In this case, an element $0 \neq \varphi \in \mathbb{K}(\mathcal{X})$ has a unique representation $\varphi = t^n \psi$ with $\psi \in \mathcal{O}_P(\mathcal{X})^\times$ and $n \in \mathbb{Z}$ (cf. Theorem ??). Thus, we define the discrete valuation $\text{Ord}_P : \mathbb{K}(\mathcal{X}) \longrightarrow \mathbb{Z} \cup \{\infty\}$ by $\text{Ord}_P(\varphi) := n$ and $\text{Ord}_P(0) := \infty$. The value $\text{Ord}_P(\varphi)$ is called the *order* of φ at P (cf. Theorem ??). Thus, if $0 \neq \varphi \in \mathbb{K}(\mathcal{X})$, the *principal divisor* of φ is

$$\text{div}(\varphi) = \sum_{P \in \mathcal{X}} \text{Ord}_P(\varphi)P.$$

Note that $\text{div}(\varphi)$ is a well-defined divisor (cf. Proposition ??). In general, since there exists a one-to-one correspondence between places of $\mathbb{K}(\mathcal{X})$ and points of $\mathcal{X}$ (cf. Proposition ??), a divisor D of $\mathbb{K}(\mathcal{X})$ can be written as $D = \sum_{P \in \mathcal{X}} n_P P$, with $n_P \in \mathbb{Z}$, almost all $n_P = 0$. Thus, a divisor of $\mathbb{K}(\mathcal{X})$ is also called a divisor on $\mathcal{X}$ (or $\mathcal{C}$, when $\mathcal{X}$ is a nonsingular model of $\mathcal{C}$).

Let x be a separating variable of $\mathbb{K}(\mathcal{X})$, that is, x is not a p -th power of an element in $\mathbb{K}(\mathcal{X})$ (cf. (??, Lemma 5.38)). We denote by $\Delta_{\mathcal{X}} = \{\varphi dx : \varphi \in \mathbb{K}(\mathcal{X})\}$ the differential module of $\mathbb{K}(\mathcal{X})$. Note that if $\Omega_{\mathbb{K}(\mathcal{X})}$ is the module of Weil differential of $\mathbb{K}(\mathcal{X})/\mathbb{K}$, then we can identify $\Delta_{\mathcal{X}}$ with $\Omega_{\mathbb{K}(\mathcal{X})}$ (cf. (??, Remark 4.3.7)).

Proposition 1.2.17 ((??), Section 8.4, Proposition 6). (i) *Let $\mathbb{K}(\mathcal{X})$ be an algebraic function field in one variable over $\mathbb{K}$. Then $\Delta_{\mathcal{X}}$ is a one-dimensional vector space over $\mathbb{K}(\mathcal{X})$.*

(ii) *($\text{char}(\mathbb{K}) = 0$) If $x \in \mathbb{K}(\mathcal{X})$, with $x \notin \mathbb{K}$, then dx is a basis for $\Delta_{\mathcal{X}}$ over $\mathbb{K}(\mathcal{X})$.*

Proposition 1.2.18 ((??), Section 8.4, Proposition 7). *With $\mathbb{K}(\mathcal{X})$ as in Proposition ??, let $\mathcal{O}$ be a discrete valuation ring of $\mathbb{K}(\mathcal{X})$, and let t be a local parameter in $\mathcal{O}$. If $\varphi \in \mathcal{O}$, then $\frac{d\varphi}{dt} \in \mathcal{O}$.*

Definition 1.2.19. *Let $\mathcal{C}$ be a projective curve and $\mathcal{X}$ its nonsingular model. A differential $\omega \in \Delta_{\mathcal{C}}$ is called a differential on $\mathcal{C}$ (or on $\mathcal{X}$).*

Let $\omega \neq 0$ be a differential on $\mathcal{X}$ and $P \in \mathcal{X}$. We define the *order* of ω at P , $\text{Ord}_P(\omega)$, as follows: Choose a local parameter $t \in \mathcal{O}_P(\mathcal{X})$, write $\omega = \varphi dt$, with $\varphi \in \mathbb{K}(\mathcal{X})$, and set $\text{Ord}_P(\omega) = \text{Ord}_P(\varphi)$. This definition does not depend on the chosen local parameter, indeed, if u is another local parameter, and $\varphi dt = \psi du$, then $\varphi/\psi = du/dt$ and $\psi/\varphi = dt/du$ belongs to $\mathcal{O}_P(\mathcal{X})$ (cf. Proposition ??). It follows that $\text{Ord}_P(\omega) = \text{Ord}_P(\psi)$.

Thus, the *canonical divisor* $\text{div}(\omega)$ is

$$\text{div}(\omega) = \sum_{P \in \mathcal{X}} \text{Ord}_P(\omega)P.$$

As before, $\text{div}(\omega)$ is a well-defined divisor. As a consequence of this definition, we have the following result.

Lemma 1.2.20. *If t is a local parameter for P , then $P \notin \text{Supp}(\text{div}(dt))$.*

Remark 1.2.21. *Let $\mathbb{K}(\mathcal{X}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{X}$, where x is a separating variable of $\mathbb{K}(\mathcal{X})$. If p does not divide $\text{Ord}_P(\text{div}(x))$ then $\text{Ord}_P(\text{div}(dx)) = \text{Ord}_P(\text{div}(x)) - 1$ (cf. (??, Section 5.8)).*

1.3 Linear series

Throughout this section we denote by $\mathcal{X}$ a projective, nonsingular and geometrically irreducible algebraic curve of genus $g > 0$ defined over $\mathbb{K}$, the algebraic closure of a field of characteristic $p > 0$.

Let $x_0, x_1, \dots, x_r$ be elements of $\mathbb{K}(\mathcal{X})$ linearly independent over $\mathbb{K}$, and let B be a fixed divisor of $\mathbb{K}(\mathcal{X})$. An ordered $(r+1)$ -tuple $c = (c_0, c_1, \dots, c_r)$ of elements in $\mathbb{K}(\mathcal{X})$ is *permissible* when $c \neq 0$. For such an $(r+1)$ -tuple c , consider the divisor

$$A_c = \text{div}(c_0x_0 + c_1x_1 + \dots + c_rx_r) + B.$$

Definition 1.3.1. *The set $\mathcal{L}$ of divisors A_c for all permissible $(r+1)$ -tuple c is a virtual linear series.*

Note that there may be a finite number of places occurring in every divisor of $\mathcal{L}$. Such places are the *fixed places* of $\mathcal{L}$. A sum of fixed places is a *fixed divisor* of $\mathcal{L}$.

Theorem 1.3.2 ((??), Theorem 6.13; Corollary 6.15 and 6.18). *Let $\mathcal{L}$ be a virtual linear series.*

1. *All divisors of $\mathcal{L}$ are equivalent to B and hence are equivalent to each other.*
2. *If $B \sim B'$, then divisors in $\mathcal{L}$ can be represented in the form*

$$\text{div}(c_0x_0 + c_1x_1 + \dots + c_rx_r) + B'$$

for some $x_0, x_1, \dots, x_r \in \mathbb{K}(\mathcal{X})$ linearly independent over $\mathbb{K}$.

3. *The integer r depends only on the series $\mathcal{L}$ and not on its representations.*

Definition 1.3.3. *Let $\mathcal{L}$ be a virtual linear series.*

1. *The common degree of the divisors of a virtual linear series is the order (or degree) of the virtual linear series.*
2. *The integer r is the dimension of the virtual linear series $\mathcal{L}$.*

Note that the virtual linear series $\mathcal{L}$ is a projective space over $\mathbb{K}$ whose points are the divisors of $\mathcal{L}$. The dimension of $\mathcal{L}$ is equal to the dimension of the projective space. Hence $\mathbb{P}^r(\mathbb{K})$ can be regarded as a *representative* of $\mathcal{L}$.

Definition 1.3.4. A subseries of a virtual linear series $\mathcal{L}$ is the set of all divisors corresponding to a projective subspace of $\mathbb{P}^r(\mathbb{K})$, the projective space representative of $\mathcal{L}$.

Theorem 1.3.5 ((??), Theorems 6.21 and 6.30). The following assertions hold:

1. Every subseries of a virtual linear series is a virtual linear series.
2. The effective divisors of a virtual linear series $\mathcal{L}$ constitute a subseries.

Definition 1.3.6. A linear series is a virtual linear series consisting of effective divisors; it is denoted by g_n^r , where n is its order and r is its dimension.

Theorem 1.3.7 ((??), Theorem 6.35). The effective divisors equivalent to a divisor C constitute a linear series.

Definition 1.3.8. The linear series consisting of all effective divisors equivalent to a divisor C is a complete linear series and is denoted by $|C|$.

Definition 1.3.9. Let x be a separating variable of $\mathbb{K}(\mathcal{X})$. The complete linear series $|dx|$ is the canonical series.

It follows from Corollary ?? that the canonical series has order $2g - 2$. Moreover, its dimension is $g - 1$ (see (??, Theorem 6.61)).

1.4 Automorphism group of a curve

Throughout this section we denote by $\mathbb{K}$ the algebraic closure of $\mathbb{F}_q$, where q is a power of a prime p , and let $\mathcal{C}$ be a geometrically irreducible algebraic curve defined over $\mathbb{F}_q$. Let $\text{Aut}_{\mathbb{K}}(\mathcal{C}) := \text{Aut}_{\mathbb{K}}(\mathbb{K}(\mathcal{C}))$ be the $\mathbb{K}$ -automorphism group of $\mathbb{K}(\mathcal{C})$, that is, the group of automorphisms of $\mathbb{K}(\mathcal{C})$ which fix every element of $\mathbb{K}$.

An element $\alpha \in \text{Aut}_{\mathbb{K}}(\mathcal{C})$ is called a $\mathbb{K}$ -automorphism of $\mathcal{C}$. Since α acts on the set of places of $\mathbb{K}(\mathcal{C})$ (cf. (??, Chapter 11)), this action can be extended to $\text{div}(\mathbb{K}(\mathcal{C}))$ in a natural way. If $D = \sum n_P P$ is a divisor of $\mathbb{K}(\mathcal{C})$ then

$$D^\alpha = \sum n_P P^\alpha,$$

where P^α is the action of α on P called the *image* of P by α .

Lemma 1.4.1 ((??), Lemma 11.3 and Equation 11.2). Let α be a $\mathbb{K}$ -automorphism of $\mathcal{C}$ and P a place of $\mathbb{K}(\mathcal{C})$. If $\varphi \in \mathbb{K}(\mathcal{C})$, then

$$\text{Ord}_P(\alpha(\varphi)) = \text{Ord}_{P^\alpha}(\varphi).$$

Lemma 1.4.2 ((??), Lemma 11.1 and 11.2). *If α is a $\mathbb{K}$ -automorphism of $\mathbb{K}(\mathcal{C})$, then the birational transformation β given by*

$$(x, y) \mapsto (\alpha(x), \alpha(y))$$

preserves the curve $\mathcal{C}$. Reciprocally, if a birational transformation β of $\mathbb{K}(\mathcal{C})$, defined by

$$(x, y) \mapsto (x', y')$$

preserves the curve $\mathcal{C}$, then there exists a $\mathbb{K}$ -automorphism α of $\mathbb{K}(\mathcal{C})$ such that $x' = \alpha(x)$ and $y' = \alpha(y)$.

Since $\mathcal{C}$ is birationally equivalent to an irreducible nonsingular curve $\mathcal{X}$ embedded in a projective space $\mathbb{P}^{g-1}(\mathbb{K})$ such that every $\mathbb{K}$ -automorphism of $\mathbb{K}(\mathcal{C})$ can be represented as a linear collineation of $\mathbb{P}^{g-1}(\mathbb{K})$ preserving $\mathcal{X}$ (cf. (??, Chapter 11)), then a $\mathbb{K}$ -automorphism can be viewed as a truly geometric concept.

Lemma 1.4.3 ((??), Lemma 11.4). *If α is a $\mathbb{K}$ -automorphism of $\mathbb{K}(\mathcal{C})$, and $\varphi \in \mathbb{K}(\mathcal{C})$, then $\text{div}(\varphi)^\alpha = \text{div}(\alpha^{-1}(\varphi))$; more particularly,*

$$(\text{div}(\varphi)_0)^\alpha = \text{div}(\alpha^{-1}(\varphi))_0 \text{ and } (\text{div}(\varphi)_\infty)^\alpha = \text{div}(\alpha^{-1}(\varphi))_\infty.$$

Remark 1.4.4. *If n is a gap number at P , and n is a non-gap at Q , then $Q^\alpha \neq P$, for all $\mathbb{K}$ -automorphism α of $\mathcal{C}$. Indeed, suppose that there exists an automorphism α , such that $Q^\alpha = P$. Let φ be a function such that $\text{div}(\varphi)_\infty = nQ$ (cf. Definition ??). Thus,*

$$\text{div}(\alpha^{-1}(\varphi))_\infty = (\text{div}(\varphi)_\infty)^\alpha = nP$$

(cf. Lemma ??), it follows that n is a non-gap at P , which is a contradiction.

Lemma 1.4.5. *Let α be a $\mathbb{K}$ -automorphism of $\mathcal{C}$ and let n be a positive integer. If P and Q are places of $\mathbb{K}(\mathcal{C})$ such that $P^\alpha = Q$, then $\alpha(\mathcal{L}(nQ)) = \mathcal{L}(nP)$.*

Proof. If $\varphi \in \mathcal{L}(nQ)$ then $\text{Ord}_Q(\varphi) \geq -n$ and $\text{Ord}_{\bar{Q}}(\varphi) \geq 0$, for all $\bar{Q} \neq Q$. It follows from Lemma ?? that $\text{Ord}_P(\alpha(\varphi)) = \text{Ord}_Q(\varphi) \geq -n$ and $\text{Ord}_{\bar{P}}(\alpha(\varphi)) = \text{Ord}_{\bar{P}^\alpha}(\varphi) \geq 0$, for all $\bar{P} \neq P$. Therefore, $\alpha(\varphi) \in \mathcal{L}(nP)$. On the other hand, if $\varphi \in \mathcal{L}(nP)$ then $\text{Ord}_P(\varphi) \geq -n$ and $\text{Ord}_{\bar{P}}(\varphi) \geq 0$, for all $\bar{P} \neq P$. It follows from Lemma ?? that $\text{Ord}_Q(\alpha^{-1}(\varphi)) = \text{Ord}_P(\varphi) \geq -n$ and $\text{Ord}_{\bar{Q}}(\alpha^{-1}(\varphi)) = \text{Ord}_{\bar{Q}^{\alpha^{-1}}}(\varphi) \geq 0$, for all $\bar{Q} \neq Q$. Therefore, $\alpha^{-1}(\varphi) \in \mathcal{L}(nQ)$ and consequently $\varphi = \alpha(\alpha^{-1}(\varphi)) \in \alpha(\mathcal{L}(nQ))$. $\square$

Theorem 1.4.6 ((??), Theorem 11.18). *Let $\alpha \in \text{Aut}_{\mathbb{K}}(\mathcal{C})$ and let*

$$L = \left\{ \text{div} \left(\sum_{i=0}^r c_i x_i \right) + B : c = (c_0 : \dots : c_r) \in \mathbb{P}^r(\mathbb{K}) \right\}, \text{ with } B \in \text{Div}(\mathbb{K}(\mathcal{C}))$$

be a linear series of $\mathbb{K}(\mathcal{C})$. Then the divisors D^α with D ranging over L are the divisors of a linear series L^α of $\mathbb{K}(\mathcal{C})$, where

$$L^\alpha = \left\{ \operatorname{div} \left(\sum_{i=0}^r c_i \alpha(x_i) \right) + B^\alpha : c = (c_0 : \dots : c_r) \in \mathbb{P}^r(\mathbb{K}) \right\}.$$

Lemma 1.4.7 ((??), Chapter 11, Lemma 11.19). *Every $\mathbb{K}$ -automorphism of $\mathbb{K}(\mathcal{C})$ preserves the canonical series of $\mathbb{K}(\mathcal{C})$.*

Now, let G be a finite subgroup of $\operatorname{Aut}_{\mathbb{K}}(\mathcal{C})$. We define the subfield $\mathbb{K}(\mathcal{C})^G$ consisting of all elements of $\mathbb{K}(\mathcal{C})$ which are fixed by every element in G . Thus, $\mathbb{K}(\mathcal{C})^G$ also has transcendence degree one over $\mathbb{K}$. Let $\mathcal{Y}$ be a nonsingular model of $\mathbb{K}(\mathcal{C})^G$, that is, a projective, nonsingular, geometrically irreducible, algebraic curve with function field $\mathbb{K}(\mathcal{C})^G$. We call $\mathcal{Y}$ the *quotient curve* of $\mathcal{C}$ by G and it is denoted by $\mathcal{C}/G$.

Definition 1.4.8. *Let G be a subgroup of $\operatorname{Aut}_{\mathbb{K}}(\mathcal{C})$. If P is a place of $\mathbb{K}(\mathcal{C})$, the stabiliser G_P of P in G is the subgroup of G consisting of all elements fixing P . The orbit*

$$P^G := \{P^\alpha : \alpha \in G\}$$

is long if $|P^G| = |G|$, otherwise P^G is short. In the latter case G is said to ramify at P .

Theorem 1.4.9 ((??), Theorem 11.57 (Riemann-Hurwitz)). *Let G be a finite $\mathbb{K}$ -automorphism group of an irreducible curve $\mathcal{C}$. If $|G_P|$ is prime to p for every place P of $\mathbb{K}(\mathcal{C})$, then*

$$2g - 2 = n(2g' - 2) + \sum_{i=1}^s (n - l_i),$$

where $n = |G|$, g and g' are the genus of $\mathcal{C}$ and its quotient curve $\mathcal{C}/G$, respectively, while $l_1, \dots, l_s$ denote the sizes of the short orbits of G .

1.5 p -Rank and Hasse-Witt invariant

1.5.1 p -Rank

Throughout this section we denote by $\mathcal{X}$ a projective, nonsingular and geometrically irreducible algebraic curve of genus $g > 0$ defined over $\mathbb{K}$, the algebraic closure of a field of characteristic $p > 0$.

Definition 1.5.1. 1. *The subgroup $\operatorname{Div}_0(\mathbb{K}(\mathcal{X}))$ of divisors of degree zero of $\operatorname{Div}(\mathbb{K}(\mathcal{X}))$ consists of all divisors of $\mathbb{K}(\mathcal{X})$ of degree zero.*

2. $\operatorname{Pic}_0(\mathbb{K}(\mathcal{X})) = \{[A] \in \operatorname{Pic}(\mathbb{K}(\mathcal{X})) : \deg A = 0\}.$

Note that the group $\text{Pic}(\mathbb{K}(\mathcal{X}))$ is written additively, that is, $[A + B] = [A] + [B]$ for $[A], [B] \in \text{Pic}(\mathbb{K}(\mathcal{X}))$. Thus, for a positive integer m and a divisor A of $\mathbb{K}(\mathcal{X})$ we define $m[A] = [mA]$. Now, we define the subgroup of $\text{Pic}(\mathbb{K}(\mathcal{X}))$ given by

$$\text{Pic}(\mathbb{K}(\mathcal{X}), m) = \{[A] \in \text{Pic}(\mathbb{K}(\mathcal{X})) : m[A] = 0\}$$

and the subgroup of $\text{Pic}_0(\mathbb{K}(\mathcal{X}))$ given by

$$\text{Pic}_0(\mathbb{K}(\mathcal{X}), m) = \text{Pic}(\mathbb{K}(\mathcal{X}), m) \cap \text{Pic}_0(\mathbb{K}(\mathcal{X})).$$

Theorem 1.5.2 ((??), Theorem 6.94). *For any positive integer m not divisible by p ,*

$$\text{Pic}_0(\mathbb{K}(\mathcal{X}), m) \cong (\mathbb{Z}_m)^{2g}$$

where g is the genus of $\mathbb{K}(\mathcal{X})$ and $(\mathbb{Z}_m)^{2g}$ is the direct product of $2g$ copies of the additive group of integers modulo m .

It is important to note that the hypothesis p does not divide m cannot be omitted in the previous theorem, even though the group $\text{Pic}_0(\mathbb{K}(\mathcal{X}), m)$ is finite, in fact, we have the following definition:

Definition 1.5.3. *There exists a non-negative integer γ such that*

$$\text{Pic}_0(\mathbb{K}(\mathcal{X}), p) \cong (\mathbb{Z}_p)^\gamma$$

(cf. (??, Comments on Page 191 and Section 9.7)), this integer γ is called the p -rank of $\mathbb{K}(\mathcal{X})$ (or $\mathcal{X}$).

Theorem 1.5.4 ((??), Theorem 6.96). *The p -rank γ of $\mathbb{K}(\mathcal{X})$ is less than or equal to the genus g of $\mathbb{K}(\mathcal{X})$.*

Theorem 1.5.5 ((??), Theorem 11.62 (Deuring-Shafarevich)). *Let G be a $\mathbb{K}$ -automorphism group of an irreducible curve $\mathcal{C}$ whose order n is a power of p . Then*

$$\gamma - 1 = n(\gamma' - 1) + \sum_{i=1}^s (n - l_i),$$

where γ and γ' are the p -ranks of $\mathcal{C}$ and its quotient curve $\mathcal{C}/G$, respectively, while $l_1, \dots, l_s$ denote the sizes of the short orbits of G on the places of $\mathbb{K}(\mathcal{C})$.

Proposition 1.5.6 ((??), Theorem 9.76). *Let F be a function field with constant field $\mathbb{F}_q$ of characteristic $p > 0$, and denote its L -polynomial by $L(T) \in \mathbb{Z}[T]$. Then the p -rank of F is $\gamma(F) = \deg(L(T) \pmod{p})$.*

Lemma 1.5.7 ((??), Lemma 6). *Let F_2/F_1 be a finite extension of function fields with constant field $\mathbb{F}_q$. If $g(F_i)$ (resp. $\gamma(F_i)$) denotes the genus (resp. p -rank) of F_i , for $i = 1, 2$. Then the following hold:*

1. $\gamma(F_2) \geq \gamma(F_1)$.
2. $\mathfrak{g}(F_2) - \gamma(F_2) \geq \mathfrak{g}(F_1) - \gamma(F_1)$.
3. If $\gamma(F_2) = 0$ then $\gamma(F_1) = 0$.
4. If F_2 is ordinary, then F_1 is ordinary.

Definition 1.5.8. For $n \geq 1$, we will call $\mathcal{X}$ minimal (respectively maximal) over $\mathbb{F}_{q^n}$ if the number N_n of $\mathbb{F}_{q^n}$ -rational points on $\mathcal{X}$ satisfies the lower (respectively upper) bound of Weil, i.e.,

$$N_n = 1 + q^n - 2\mathfrak{g}q^{n/2} \quad (\text{respectively } N_n = 1 + q^n + 2\mathfrak{g}q^{n/2}).$$

Proposition 1.5.9 ((??), Comments on Page 142 and Proposition 1). If $\mathcal{X}$ is minimal over some extension $\mathbb{F}_{q^n}$, then the p -rank of $\mathcal{X}$ is zero.

Now, note that if $\mathcal{X}$ is $\mathbb{F}_{q^2}$ -maximal then $N_{2n} = 1 + q^{2n} + (-1)^{n-1}2\mathfrak{g}q^n$, for $n \geq 1$ (??, Comments on Page 396). Thus, the following criterion hold:

Proposition 1.5.10. If $\mathcal{X}$ is maximal or minimal over some extension $\mathbb{F}_{q^n}$, then the p -rank of $\mathcal{X}$ is zero.

1.5.2 The Hasse-Witt invariant

Let $\mathcal{X}$ be a projective, nonsingular and geometrically irreducible algebraic curve of genus $\mathfrak{g} > 0$ defined over $\mathbb{F}_q$, where q is a power of p , and let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$. Let $\mathbb{K}(\mathcal{X}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{X}$, where $x \in \mathbb{K}(\mathcal{X})$ be a separating variable. We refer the reader to (??), (??) and (??, §10 and §11) for more detail on the following definitions and results. Let $\Delta_{\mathcal{X}} = \{\varphi dx : \varphi \in \mathbb{K}(\mathcal{X})\}$ be the differential module of $\mathbb{K}(\mathcal{X})$. For any $w \in \Delta_{\mathcal{X}}$ we say that

- (i) ω is holomorphic if $\text{div}(\omega)$ is effective,
- (ii) ω is exact if $\omega = df$ for some $f \in \mathbb{K}(\mathcal{X})$,
- (iii) ω is logarithmic if $\omega = df/f$ for some $f \neq 0$ in $\mathbb{K}(\mathcal{X})$.

Now, For each $\omega \in \Delta_{\mathcal{X}}$ there exists $f_0, \dots, f_{p-1} \in \mathbb{K}(\mathcal{X})$ such that

$$\omega = (f_0^p + f_1^p x + \dots + f_{p-1}^p x^{p-1})dx.$$

The Cartier operator $C : \Delta_{\mathcal{X}} \rightarrow \Delta_{\mathcal{X}}$ is defined by

$$C(\omega) := f_{p-1}dx. \tag{1.5}$$

Let $\omega \in \Delta_{\mathcal{X}}$ and $f \in \mathbb{K}(\mathcal{X})$. The Cartier operator has the following properties:

- (i) The value of $C(\omega)$ does not depend on the choice of x ,
- (ii) C is $1/p$ -linear, i.e., C is additive and $C(f^p \omega) = fC(\omega)$,
- (iii) $C(f^{p-1} df) = df$,
- (iv) $C(\omega) = 0$ if and only if ω is exact,
- (v) $C(\omega) = \omega$ if and only if ω is logarithmic,
- (vi) If ω is holomorphic, then $C(\omega)$ is also holomorphic.

As a consequence of the previous properties, we have the following results.

Lemma 1.5.11. *If $x \in \mathbb{K}(\mathcal{X})$ is a separating variable and n is a positive integer, then*

$$C^n(x^i dx) = \begin{cases} 0 & \text{if } i \not\equiv -1 \pmod{p^n}, \\ x^{s-1} dx & \text{if } i+1 = sp^n. \end{cases}$$

Proof. By induction on n . First suppose that $n = 1$. Note that if $i = (s-1)p + l$, with $l \in \{0, \dots, p-1\}$, then

$$C^n(x^i dx) = \begin{cases} x^{s-1} C(x^l dx) & \text{if } l \leq p-2, \\ x^{s-1} C(x^{p-1} dx) & \text{if } l = p-1, \end{cases} = \begin{cases} 0 & \text{if } l \leq p-2, \\ x^{s-1} dx & \text{if } l = p-1. \end{cases}$$

Now, let $n \geq 2$ and suppose that the result is true for $n-1$. If $i = (s-1)p^n + t$, with $t = (m-1)p^{n-1} + l \in \{0, \dots, p^n - 2\}$ and $l \in \{0, \dots, p^{n-1}\}$, then by induction hypothesis we can suppose that $l = p^{n-1} - 1$ and $m \in \{1, \dots, p-1\}$. Thus,

$$C^n(x^i dx) = C(C^{n-1}(x^{((s-1)p+m)p^{n-1}-1} dx)) = C(x^{(s-1)p+m-1} dx) = 0.$$

Finally, if $i = sp^n - 1$ then $C^n(x^i dx) = C(C^{n-1}(x^{sp^{n-1}-1} dx)) = C(x^{sp-1} dx) = x^{s-1} dx$. $\square$

Theorem 1.5.12. *Let $x \in \mathbb{K}(\mathcal{X})$ be a separating variable and n be a positive integer. If $q = p^n$ and*

$$f = f_0^q + f_1^q x + \dots + f_{q-1}^q x^{q-1},$$

where $f_i \in \mathbb{K}(\mathcal{X})$, for $i = 0, \dots, q-1$, then

$$C^n(f dx) = f_{q-1} dx.$$

Proof. Note that

$$C^n(f dx) = f_0 C^n(1 dx) + f_1 C^n(x dx) + \dots + f_{q-1} C^n(x^{q-1} dx).$$

By Lemma ??, $C^n(x^i dx) = 0$, for $0 \leq i \leq q-2$, and $C^n(x^{q-1} dx) = x^0 dx = dx$. Hence, $C^n(f dx) = f_{q-1} dx$. $\square$

Now, Let $\Delta_{\mathcal{X}}^{(1)}$ be the g -dimensional $\mathbb{K}$ -vector space of the holomorphic differentials on $\mathcal{X}$. The Cartier operator induces a $1/p$ -linear map $C : \Delta_{\mathcal{X}}^{(1)} \rightarrow \Delta_{\mathcal{X}}^{(1)}$.

Let $\Delta_{\mathcal{X}}^{\log}$ be the subspace of $\Delta_{\mathcal{X}}^{(1)}$ spanned by the logarithmic differentials. Let $\Delta_{\mathcal{X}}^0$ be the subspace of $\Delta_{\mathcal{X}}^{(1)}$ formed by the differentials $\omega \in \Delta_{\mathcal{X}}^{(1)}$ such that there exists a positive integer n such that $C^n(\omega) = 0$. Then

$$\Delta_{\mathcal{X}}^{(1)} = \Delta_{\mathcal{X}}^{\log} \oplus \Delta_{\mathcal{X}}^0, \quad (1.6)$$

see (??).

Definition 1.5.13. *The dimension of $\Delta_{\mathcal{X}}^{\log}$ is the Hasse-Witt invariant of $\mathcal{X}$.*

A matrix (h_{ij}) associated to C and a choice of basis for $\Delta_{\mathcal{X}}^{(1)}$ is called a *Cartier*, or *Cartier-Manin*, matrix for $\mathcal{X}$. The rank of the matrix

$$M = (h_{ij})(h_{ij}^p) \cdots (h_{ij}^{p^{g-1}})$$

coincides with Hasse-Witt invariant of $\mathcal{X}$.

Proposition 1.5.14. *Let h be a positive integer, and let $B = \{\omega_1, \dots, \omega_g\}$ be a basis for the vector space of holomorphic differentials of $\mathcal{X}$. The following assertions hold:*

1. *Suppose that there exists $\alpha \in \mathbb{F}_p$ such that $C^h(\omega) = \alpha\omega$, where $\omega \in B$. Then $\alpha \neq 0$ if and only if $\omega \in \Delta_{\mathcal{X}}^{\log}$.*
2. *Suppose that there exist $\alpha_1, \dots, \alpha_g \in \mathbb{F}_p$ such that*

$$C^h(\omega_i) = \alpha_i \omega_i, \text{ for all } i = 1, \dots, g,$$

then the Hasse-Witt invariant of $\mathcal{X}$ is given by the cardinality of the set

$$T = \{i \in \{1, \dots, g\} : \alpha_i \neq 0\}.$$

Proof. Suppose that $\alpha \neq 0$. Since $\omega \in \Delta_{\mathcal{X}}^{(1)} = \Delta_{\mathcal{X}}^{\log} \oplus \Delta_{\mathcal{X}}^0$ (cf. (??)), we have $\omega = u + v$, with $u \in \Delta_{\mathcal{X}}^{\log}$ and $v \in \Delta_{\mathcal{X}}^0$. Thus, there exists a positive integer t such that $C^{ht}(v) = 0$. Now, since $C^{ht}(w) = \beta w$, for some $\beta \neq 0$, and $C^{ht}(u) \in \Delta_{\mathcal{X}}^{\log}$, we have $C^{ht}(u) = C^{ht}(v + u) = \beta(v + u)$, that is, $\beta v = C^{ht}(u) - \beta u \in \Delta_{\mathcal{X}}^{\log}$ and consequently $v = 0$ (cf. (??)). Therefore, $\omega = u \in \Delta_{\mathcal{X}}^{\log}$. Reciprocally, if $\alpha = 0$, then $C^h(\omega) = 0$. Therefore, $\omega \notin \Delta_{\mathcal{X}}^{\log}$ (cf. (??)).

Finally, note that B is a basis of $\Delta_{\mathcal{X}}^{(1)} = \Delta_{\mathcal{X}}^{\log} \oplus \Delta_{\mathcal{X}}^0$ and $B_1 = \{\omega_i \in B : i \in T\} \subset B$. Since $B_1 \subset \Delta_{\mathcal{X}}^{\log}$ and $B \setminus B_1 \subset \Delta_{\mathcal{X}}^0$, we have that B_1 is a basis of $\Delta_{\mathcal{X}}^{\log}$. Thus, the Hasse-Witt invariant of $\mathcal{X}$ is the cardinality of T . $\square$

Theorem 1.5.15 ((??), Theorem 6.98). *The p -rank of a curve is equal to its Hasse-Witt invariant.*

Since the p -rank of a curve $\mathcal{X}$ is equal to the p -rank of its Jacobian $J_{\mathcal{X}}$, the following result can be used to compute the Hasse-Witt invariant of $\mathcal{X}$.

Theorem 1.5.16 ((??), Theorem B). *Let $G \leq \text{Aut}(\mathcal{C})$ be a (finite) subgroup such that $G = H_1 \cup \dots \cup H_t$, where the subgroup $H_i \leq G$ satisfy $H_i \cap H_j = \{1\}$ for $i \neq j$. Then we have the isogeny relation*

$$J_{\mathcal{C}}^{t-1} \times J_{\mathcal{C}/G}^g \sim J_{\mathcal{C}/H_1}^{h_1} \times \dots \times J_{\mathcal{C}/H_t}^{h_t}$$

where $g = |G|$, $h_i = |H_i|$ and, as usual, $J^n = J \times \dots \times J$ (n times).

ON $\mathbb{F}_{q^3}$ -FROBENIUS NONCLASSICAL CURVES OF TYPE $Y^{q^2+q+1} = f(X)$

2.1 Notations and preliminaries

Let q be a power of a prime p , and let $\mathbb{F}_q$ the field with q elements. We begin by establishing some notations:

- $Tr(X) = X^{q^2} + X^q + X$ will denote the trace polynomial in $\mathbb{F}_{q^3}[X]$.
- $f'(X)$ will denote the formal derivative of a polynomial $f(X) \in \overline{\mathbb{F}_q}[X]$.
- $\mathbb{N} := \{1, 2, 3, \dots\}$ and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.
- $\#A$ will denote the cardinality of a set A .
- η will denote the quadratic character of $\mathbb{F}_q$, that is

$$\eta(x) = \begin{cases} 1 & \text{if } x \text{ is a nonzero square in } \mathbb{F}_q, \\ 0 & \text{if } x = 0, \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_q. \end{cases}$$

- The floor, ceiling and fractional part functions will be denoted by $\lfloor \cdot \rfloor$, $\lceil \cdot \rceil$, and $\{ \cdot \}$ respectively.

An irreducible plane curve $\mathcal{C} : F(X, Y) = 0$ defined over $\mathbb{F}_q$ is called $\mathbb{F}_q$ -Frobenius nonclassical if

$$F(X, Y) \text{ divides } (X^q - X) \frac{\partial F}{\partial X} + (Y^q - Y) \frac{\partial F}{\partial Y}.$$

Otherwise, $\mathcal{C}$ is called $\mathbb{F}_q$ -Frobenius classical. Geometrically, $\mathcal{C}$ is $\mathbb{F}_q$ -Frobenius nonclassical if the image of each simple point $P \in C$ under the $\mathbb{F}_q$ -Frobenius map lies on the tangent line at P in

$\mathcal{C}$. Let $f(X) \in \mathbb{F}_q[X]$ be a nonconstant polynomial, and let $V_f := \{f(\alpha) : \alpha \in \mathbb{F}_q\}$ be its value set. Since f has no more than $\deg(f)$ zeros, one can easily show that V_f satisfies

$$\left\lfloor \frac{q-1}{\deg(f)} \right\rfloor + 1 \leq \#V_f \leq q.$$

If V_f attains the lower bound in the previous inequality, then f is called a minimal value set polynomial (MVSP).

The goal of this section is to establish some preliminary results which will be used in the course of the text. First, we present the following results, due to Borges, which relate $\mathbb{F}_q$ -Frobenius nonclassical curves with MVSP's.

Theorem 2.1.1 ((??), Theorem 2.5). *Let $f \in \mathbb{F}_{q^r}[X]$ be a nonconstant polynomial. Then f is an MVSP with $V_f = \mathbb{F}_q$ if and only if there exists a nonconstant polynomial $h \in \mathbb{F}_{q^r}[X]$ such that*

1. *the monomials of h are of the form $cX^{\alpha_0 + \alpha_1 q + \dots + \alpha_{r-1} q^{r-1}} \in \mathbb{F}_{q^r}[X]$, where $\alpha_i \in \{0, 1\}$.*
2. *$f = T(h) \pmod{X^{q^r} - X}$, that is, f is the unique polynomial for which $f \equiv T(h) \pmod{X^{q^r} - X}$ with $\deg(f) < q^i$, where $T(X) = \sum_{i=0}^{r-1} X^{q^i}$ is the trace polynomial.*

Theorem 2.1.2 ((??), Theorem 5.6). *Let $f(X) \in \mathbb{F}_{q^r}[X]$ be a nonconstant polynomial. The components of the curve $Y^{\frac{q^r-1}{q-1}} = f(X)$ are $\mathbb{F}_{q^r}$ -Frobenius nonclassical if and only if f is an MVSP with $V_f = \mathbb{F}_q$.*

As a consequence of these results we have the following theorem:

Theorem 2.1.3. *Let $\mathcal{C} : Y^{q+1} = f(X)$ be an $\mathbb{F}_{q^2}$ -Frobenius nonclassical curve. Then the projective closure of $\mathcal{C}$ is $\mathbb{F}_{q^2}$ -projectively equivalent to the Hermitian curve $\mathcal{H} : Y^{q+1} = X^q Z + XZ^q$.*

Proof. It follows from Theorems ?? and ?? that there exist $a, b, c, d \in \mathbb{F}_{q^2}$ such that $f(X) = T(aX^{q+1} + bX^q + cX + d) \pmod{(X^{q^2} - X)}$, where $T(X) = X^q + X$. Then, we can write $f(X) = \alpha X^{q+1} + \beta X^q + \beta^q X + \delta$, for some $\alpha, \delta \in \mathbb{F}_q$ and $\beta = b + c^q$. Now, note that the projective closure of $\mathcal{C}$ is projectively equivalent to the Hermitian curve, by means of the projectivity

$$(X : Y : Z) \mapsto \begin{cases} (\beta(tuX + sZ) : \beta uY : uX + Z) & \text{if } \alpha\beta \neq 0, \\ (\beta(X + vZ) : \beta Y : Z) & \text{if } \alpha = 0 \text{ and } \beta \neq 0, \\ (\varepsilon(X - Z) : \lambda Y : \sigma(X + Z)) & \text{if } \beta = 0, \end{cases}$$

where $v, \varepsilon, \sigma, \lambda \in \mathbb{F}_{q^2}$ are nonzero roots of $X^q + X + \delta/\beta^{q+1}$, $X^{q+1} + 1/\alpha$, $X^{q+1} - 1/\delta$, $X^{q+1} - 2$, respectively, and $u = \alpha t^q s + (t^q + s) + \delta/\beta^{q+1}$, where t, s are distinct roots of $\alpha X^{q+1} + (X^q + X) + \delta/\beta^{q+1}$ (cf. Lemma ??). Since $\mathcal{C}$ is an irreducible curve, we have $u \neq 0$, when $\alpha\beta \neq 0$, and $p \neq 2$ when $\beta = 0$. $\square$

Motivated by the previous theorems, our first objective is to classify $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$. In this sense, the next result provides a first description for such curves.

Theorem 2.1.4. *Let $\mathcal{C} : Y^{q^2+q+1} = f(X)$ be an $\mathbb{F}_{q^3}$ -Frobenius nonclassical curve. Then the projective closure of $\mathcal{C}$ is $\mathbb{F}_{q^3}$ -projectively equivalent to the projective closure of the curve given by*

$$Y^{q^2+q+1} = aX^{q^2+q+1} + b(X^{q^2} + X^q + X) + c,$$

for some $a, b, c \in \mathbb{F}_q$.

Proof. It follows from Theorem ?? and ?? that there exist $a, b_i, c_i, d \in \mathbb{F}_{q^3}$ with $1 \leq i \leq 3$ such that

$$f(X) = T(aX^{q^2+q+1} + b_1X^{q^2+q} + b_2X^{q^2+1} + b_3X^{q+1} + c_1X^{q^2} + c_2X^q + c_3X + d) \pmod{X^{q^3} - X},$$

where $T(X) = X^{q^2} + X^q + X$. Then, we can write

$$f(X) = \alpha X^{q^2+q+1} + \beta X^{q^2+q} + \beta^q X^{q^2+1} + \beta^{q^2} X^{q+1} + \gamma^{q^2} X^{q^2} + \gamma^q X^q + \gamma X + \delta,$$

with $\beta = b_1 + b_2^q + b_3^{q^2}$ and $\gamma = c_1^q + c_2^{q^2} + c_3$ elements of $\mathbb{F}_{q^3}$ and $\alpha, \delta \in \mathbb{F}_q$. We can suppose that $\beta \neq 0$ or $\gamma \neq 0$. Thus, we have some cases to consider:

- (i) If $\beta\gamma = 0$, then the projective closure of $\mathcal{C}$ is projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = aX^{q^2+q+1} + bTr(X) + c$, for some $a, b, c \in \mathbb{F}_q$, by means of the projectivity

$$(X : Y : Z) \mapsto \begin{cases} (\gamma^{q^2+q} X : Y : Z) & \text{if } \gamma \neq 0, \\ (\beta Z : Y : X) & \text{if } \gamma = 0. \end{cases}$$

- (ii) If $\beta\gamma \neq 0$ and $\alpha \neq 0$ or $\delta \neq 0$, namely $\alpha \neq 0$. Then the projective closure of $\mathcal{C}$ is projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = aX^{q^2+q+1} + bTr(X) + c$, for some $a, b, c \in \mathbb{F}_q$, by means of the projectivity

$$(X : Y : Z) \mapsto \begin{cases} (\beta(X - \frac{1}{\alpha}Z) : Y : Z) & \text{if } \beta^{q^2+q} = \alpha\gamma, \\ \left(\beta \left(\frac{\beta}{\alpha}(\alpha\gamma - \beta^{q^2+q}) \right)^{q^2+q} X - \frac{\beta}{\alpha}Z : Y : Z \right) & \text{if } \beta^{q^2+q} \neq \alpha\gamma. \end{cases}$$

- (iii) If $\beta\gamma \neq 0$ and $\alpha = \delta = 0$. Then the projective closure of $\mathcal{C}$ is projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = aX^{q^2+q+1} + bTr(X)$, for some $a, b \in \mathbb{F}_q$, by means of the projectivity

$$(X : Y : Z) \mapsto \left(\beta \left(\left(\frac{\gamma\beta}{\beta^{q^2+q+1}} - \frac{Tr(s)}{2} \right) X + Z \right) : \beta Y : X \right).$$

□

Theorem 2.1.5. *Let $\mathcal{C} : Y^{q^2+q+1} = f(X)$ be an $\mathbb{F}_{q^3}$ -Frobenius nonclassical curve. Then the projective closure of $\mathcal{C}$ is $\mathbb{F}_{q^3}$ -projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = g(X)$, where*

$$g(X) = \begin{cases} X^{q^2+q+1} + b\text{Tr}(X) + c, & \text{or} \\ X^{q^2} + X^q + X, \end{cases}$$

with $b, c \in \mathbb{F}_q$ such that $(b, c) \neq (0, 0)$.

Proof. It follows from Theorem ?? that the projective closure of $\mathcal{C}$ is $\mathbb{F}_{q^3}$ -projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = \alpha X^{q^2+q+1} + \beta \text{Tr}(X) + \gamma$, for some $\alpha, \beta, \gamma \in \mathbb{F}_q$. Thus, the projective closure of $\mathcal{C}$ is projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = g(X)$, by means of the projectively

$$(X : Y : Z) \mapsto \begin{cases} (X : \varepsilon Y : Z) & \text{if } \alpha \neq 0, \\ (X : \lambda Y : Z) & \text{if } \alpha = \gamma = 0, \\ (X + tZ : \lambda Y : Z) & \text{if } \alpha = 0 \text{ and } \gamma \neq 0, \end{cases}$$

where $\varepsilon^{q^2+q+1} = \alpha$, $\lambda^{q^2+q+1} = \beta$ and $\text{Tr}(t) = -\gamma/\beta$. □

2.2 Classification of $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$

Throughout this section we denote by q the power of an odd prime p . The goal of this section is to classify all $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$. It follows from Theorem ?? that we can consider only curves, defined over $\mathbb{F}_{q^3}$, of the type

$$\mathcal{C}_{b,c} : Y^{q^2+q+1} = X^{q^2+q+1} + b\text{Tr}(X) + c, \quad (2.1)$$

where $b, c \in \mathbb{F}_q$ such that $(b, c) \neq (0, 0)$. The following result will be used to describe the roots of $f(X) = X^{q^2+q+1} + b\text{Tr}(X) + c \in \mathbb{F}_q[X]$.

Proposition 2.2.1 ((?), Corollary 5.4). *Let $f(X) \in \mathbb{F}_q[X]$ be a nonconstant polynomial and $n \geq 1$ be an integer such that $Y^n - f(X) \notin \mathbb{F}_q[X^p, Y^p]$. If the irreducible components of $Y^n = f(X)$ are $\mathbb{F}_q$ -Frobenius nonclassical then*

1. *if an $\mathbb{F}_q$ -root of $f(X)$ has multiplicity k , where $0 < k < \deg(f)$, then $k \leq \frac{n-1}{|V_f|}$ and $k \equiv n \pmod{p}$.*
2. *if α is a root of $f(X)$ of multiplicity k , then $\alpha \in \mathbb{F}_q$ if and only if $p \nmid k$. In Particular, all simple roots of f lies in $\mathbb{F}_q$.*

Proposition 2.2.2. *Let $b, c \in \mathbb{F}_q$, with $b \neq 0$, and $f(X) = X^{q^2+q+1} + b\text{Tr}(X) + c \in \mathbb{F}_q[X]$.*

1. *If $\eta(c^2 + 4b^3) = 0$, then $f(X) = (X - r)^{q+1} \prod_{i=1}^{q^2} (X - r_i)$, where $r \in \mathbb{F}_q$ and $r_i \in \mathbb{F}_{q^3} \setminus \{r\}$ are pairwise distinct.*
2. *If $\eta(c^2 + 4b^3) = -1$, then $f(X) = (X - t)^q (X - t^q)^q \prod_{i=1}^{q^2-q+1} (X - r_i)$ where $t \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $r_i \in \mathbb{F}_{q^3}$ are pairwise distinct.*

Proof. Let x be a multiple root of f , that is, x is a common root of $f(X)$ and $f'(X)$. Thus x is a solution to

$$\begin{cases} x^q + x &= -c/b, \\ x^{q+1} &= -b. \end{cases} \quad (2.2)$$

Equivalently, x and x^q are roots of $g(X) = X^2 + \frac{c}{b}X - b$.

1. If $\eta(c^2 + 4b^3) = 0$, then g has an unique root $r \in \mathbb{F}_q$, and consequently r is the unique root of $f(X)$ of multiplicity k , for some integer $k > 1$. Since r is a root of $f(X) = X(X^{q+1} + b)^q + b(X^q + X + c/b)^q$, we have that (??) yields $k \geq q$. Finally, since $Y^{q^2+q+1} = f(X)$ is an $\mathbb{F}_{q^3}$ -Frobenius nonclassical curve (cf. Proposition ??), it follows from Proposition ?? that $k \leq q + 1$ and $k \equiv 1 \pmod{p}$. Therefore $k = q + 1$. Finally, by Proposition ?? we have that the single roots of $f(X)$ belong to $\mathbb{F}_{q^3}$.
2. If $\eta(c^2 + 4b^3) = -1$, then g has two roots $t, t^q \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and consequently t and t^q are roots of $f(X)$ of multiplicity k_1 and k_2 , respectively, for some integers $k_1 > 1$ and $k_2 > 1$. Note that, as before, $k_i \geq q$ for $i = 1, 2$. Finally, since $Y^{q^2+q+1} = f(X)$ is an $\mathbb{F}_{q^3}$ -Frobenius nonclassical curve (cf. Proposition ??), it follows from Proposition ?? that p divides k_1 and k_2 , and consequently we can write $f'(X) = (X - t)^{k_1} (X - t^q)^{k_2} h(X)$, for some polynomial h . Now, since $f'(X) = (X^{q+1} + b)^q$, it follows that t and t^q are roots of $f'(X)$ of multiplicity q . Therefore, $k_1 = k_2 = q$. Finally, by Proposition ?? we have that the single roots of $f(X)$ belong to $\mathbb{F}_{q^3}$.

□

The following remark is useful in the proof of the next lemma.

Remark 2.2.3. *Let γ be an element of a finite field $\mathbb{F}_q$, then the roots of the polynomial $X^{q+1} - \gamma$ are elements of $\mathbb{F}_{q^2}$, indeed if s is one of its roots, then $s^{q^2-1} = 1$. Moreover, $s \in \mathbb{F}_q$ is a root of $X^{q+1} - \gamma$ if and only if s is a root of $X^2 - \gamma$.*

Lemma 2.2.4. *Let $b, c, \lambda \in \mathbb{F}_q$ be such that $(b, c) \neq (0, 0)$ and $\eta(\lambda) = \eta(c^2 + 4b^3) = -1$. Let $G(X, Y) = X^{q^2}Y^{q+1} + X^qY^{q^2+1} + XY^{q^2+q}$ and $H(X, Y) = G(Y, X)$. Consider the curves $\mathcal{C}_1 : X^{q^2+q+1} - G(X, Y) + 2Y^{q^2+q+1} = 0$,*

$$\begin{aligned}
\mathcal{C}_2 : X^{q+1} - X^q Y - X Y^q + Y^{q+1} &= 1, \\
\mathcal{C}_3 : X^{q^2+q+1} + bG(X, Y) + cY^{q^2+q+1} &= 1, \\
\mathcal{C}_4 : -cX^{q^2+q+1} + bcG(X, Y) + 2b^2H(X, Y) + (2b^3 + c^2)Y^{q^2+q+1} &= 0, \\
\mathcal{C}_5 : X^{q^2+q+1} + \lambda G(X, Y) &= 1, \\
\mathcal{C}_6 : \lambda Y^{q^2+q+1} + H(X, Y) &= 0,
\end{aligned}$$

Let $A_{i,j}$ be the set of affine points in the intersection $\mathcal{C}_i \cap \mathcal{C}_j$ over $\mathbb{F}_{q^3}$. The following assertions hold:

1. $\#A_{1,2} = 2q^2$;
2. $\#A_{3,4} = q^4 + q^2 + 1$;
3. $\#A_{5,6} = q^4 + q^2 + 1$.

Proof. 1. It follows from Proposition ?? that $\mathcal{C}_1$ is given by

$$(X - Y)^{q+1} \prod_{i=1}^{q^2} (X - \alpha_i Y) = 0,$$

where $\alpha_i \in \mathbb{F}_{q^3}$, with $\alpha_i \neq 1$ and $\alpha_i \neq \alpha_j$ for all $i \neq j$. Let $l : X - Y = 0$ and $l_i : X - \alpha_i Y = 0$ be lines defined over $\mathbb{F}_{q^3}$. Note that, $l_i \cap \mathcal{C}_2$ has an affine point defined over $\mathbb{F}_{q^3}$, if and only if the polynomial $Y^{q+1} - 1/(\alpha_i - 1)^{q+1}$ has a root in $\mathbb{F}_{q^3}$, or equivalently $Y^{q^3+1} - 1/(\alpha_i - 1)^2$ has a root in $\mathbb{F}_{q^3}$, that is, a root of $Y^2 - 1/(\alpha_i - 1)^2$ (cf. Remark ??). Therefore $l_i \cap \mathcal{C}_2$ has two points defined over $\mathbb{F}_{q^3}$. Now, since these sets are pairwise disjoint, and $l \cap \mathcal{C}_2$ has exactly one point at infinite, we have $\#A_{1,2} = 2q^2$.

2. Firstly, note that if $\mathcal{C}_3 : f_1(X, Y) = 1$ and $\mathcal{C}_4 : f_2(X, Y) = 0$, then $\gcd(f_1(X, 1), f_2(X, 1)) = (X^2 + \frac{c}{b}X - b)^q = (X - t)^q(X - t^q)^q$. Thus, as before, $\mathcal{C}_3$ and $\mathcal{C}_4$ are given by

$$(X - tY)^q(X - t^qY)^q \prod_{i=1}^{q^2-q+1} (X - \alpha_i Y) = 1 \quad \text{and} \quad (X - tY)^q(X - t^qY)^q \prod_{i=1}^{q^2-q+1} (X - \beta_i Y) = 0,$$

respectively, where $\alpha_i, \beta_i \in \mathbb{F}_{q^3}$, with $\alpha_i, \beta_i \notin \{t, t^q\}$, $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for all $i \neq j$. Let $r_1 : X - tY = 0$, $r_2 : X - t^qY = 0$ and $l_i : X - \beta_i Y = 0$ be lines defined over $\mathbb{F}_{q^3}$. Note that, $l_i \cap \mathcal{C}_3$ has an affine point defined over $\mathbb{F}_{q^3}$, if and only if the polynomial $Y^{q^2+q+1} - 1/(f_1(\beta_i, 1))$ has a root in $\mathbb{F}_{q^3}$. Therefore $l_i \cap \mathcal{C}_3$ has $q^2 + q + 1$ points defined over $\mathbb{F}_{q^3}$. Now, since these sets are pairwise disjoint, and $r_j \cap \mathcal{C}_2$ has exactly one point at infinite, for $j = 1, 2$, we have $\#A_{1,2} = q^4 + q^2 + 1$.

3. If $b = \lambda$ and $c = 0$, then the result is analogous to the previous case.

□

Theorem 2.2.5. *If $(b, c) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0, 0)\}$, then the projective closure of the curve*

$$\mathcal{C}_{b,c} : Y^{q^2+q+1} = X^{q^2+q+1} + b\text{Tr}(X) + c$$

is $\mathbb{F}_{q^3}$ -projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = f(X)$, with

$$f(X) = \begin{cases} X^{q^2+q+1} + 1 & \text{if } \eta(c^2 + 4b^3) = 1, \\ X^{q^2} + X^q + X & \text{if } \eta(c^2 + 4b^3) = 0, \\ X^{q^2+q+1} + \lambda(X^{q^2} + X^q + X) & \text{if } \eta(c^2 + 4b^3) = -1, \end{cases}$$

where $\lambda \in \mathbb{F}_q$ with $\eta(\lambda) = -1$.

Proof. 1. If $\eta(c^2 + 4b^3) = 1$, then we can suppose that $b \neq 0$ and

$$\phi(\mathcal{C}_{b,c}) : \begin{cases} Y^{q^2+q+1} + X^{q^2+q+1} + \frac{\alpha}{d^2} Z^{q^2+q+1} = 0 & \text{if } c \neq 0, \\ Y^{q^2+q+1} + X^{q^2+q+1} + \frac{1}{r^3} Z^{q^2+q+1} = 0 & \text{if } c = 0, \end{cases}$$

is the image of the projective closure of $\mathcal{C}_{b,c}$ under the isomorphism

$$\phi(X : Y : Z) = \begin{cases} \left(\frac{-\alpha b}{cd} X - Z : \frac{b\lambda}{c} Y : -\frac{b}{c} X + \alpha Z \right) & \text{if } c \neq 0, \\ \left(-\frac{1}{r} X - Z : \gamma Y : -X + rZ \right) & \text{if } c = 0, \end{cases}$$

where $\alpha \in \mathbb{F}_q$, $\lambda \in \mathbb{F}_{q^3}$, $r \in \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^3}$ are nonzero roots of $X^2 + X - d$, $X^{q^2+q+1} - \frac{\alpha(\alpha^2+d)}{d^3}$, $X^2 - b$ and $X^{q^2+q+1} - \frac{2}{r^2}$, respectively, with $d = \frac{b^3}{c^2}$ when $c \neq 0$. In both cases, the curve $\phi(\mathcal{C}_{b,c})$ is $\mathbb{F}_{q^3}$ -projectively equivalent to the Fermat curve given by $Y^{q^2+q+1} = X^{q^2+q+1} + Z^{q^2+q+1}$.

2. If $\eta(c^2 + 4b^3) = 0$, then $(b, c) = (-t^2, 2t^3)$, where $t \in \mathbb{F}_q \setminus \{0\}$, is a parametrization of the points on $c^2 + 4b^3 = 0$ in $\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0, 0)\}$, and consequently the curve $\mathcal{C}_{b,c}$ is given by

$$Y^{q^2+q+1} = X^{q^2+q+1} - t^2(X^{q^2} + X^q + X) + 2t^3,$$

for some $t \in \mathbb{F}_q \setminus \{0\}$. Thus, the projective closure of $\mathcal{C}_{b,c}$ is projectively equivalent to the curve given by $Y^{q^2+q+1} = X^{q^2} Z^{q+1} + X^q Z^{q^2+1} + XZ^{q^2+q}$, by means of the projectivity

$$(X : Y : Z) \mapsto (t(X + \alpha Z) : tY : X + \beta Z),$$

where $(\alpha, \beta) \in A_{1,2}$, with $\alpha \neq \beta$ (cf. Lemma ??).

3. If $\eta(c^2 + 4b^3) = -1$, then $\frac{4\lambda b^2}{c^2+4b^3}$ is a nonzero square in $\mathbb{F}_q$, as $\eta(\lambda) = -1$. Thus, given a root $v \in \mathbb{F}_q$ of $X^2 - \frac{4\lambda b^2}{c^2+4b^3}$, it follows that the projective closure of $\mathcal{C}_{b,c}$ is projectively equivalent to the curve given by $Y^{q^2+q+1} = X^{q^2+q+1} + \lambda(X^{q^2} Z^{q+1} + X^q Z^{q^2+1} + XZ^{q^2+q})$, by means of the projectivity

$$(X : Y : Z) \mapsto \left(\alpha X + v \left(-\frac{c}{2b} \alpha + b\beta \right) Z : Y : \beta X + v \left(\alpha + \frac{c}{2b} \beta \right) Z \right),$$

where $(\alpha, \beta) \in A_{3,4}$, with $\alpha \neq \beta$ (cf. Lemma ??).

□

So, by Corollary ?? and Theorem ?? we have a complete classification of the $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of the type $Y^{q^2+q+1} = f(X)$, where $f \in \mathbb{F}_{q^3}[X]$.

Corollary 2.2.6. *Let $\mathcal{C} : Y^{q^2+q+1} = f(X)$ be an $\mathbb{F}_{q^3}$ -Frobenius nonclassical curve, and $\lambda \in \mathbb{F}_q$ where $\eta(\lambda) = -1$. Then the projective closure of $\mathcal{C}$ is $\mathbb{F}_{q^3}$ -projectively equivalent to the projective closure of the curve given by $Y^{q^2+q+1} = g(X)$ where*

$$g(X) \in \{X^{q^2+q+1} + 1, X^{q^2} + X^q + X, X^{q^2+q+1} + \lambda(X^{q^2} + X^q + X)\}.$$

Let $b, c \in \mathbb{F}_q$ be such that $\eta(c^2 + 4b^3) = -1$. The next result gives us another model for the curve $\mathcal{C}_{b,c}$ over $\mathbb{F}_{q^6}$. More precisely, we have the following result:

Proposition 2.2.7. *If $b, c \in \mathbb{F}_q$, with $\eta(c^2 + 4b^3) = -1$, then the projective closure of $\mathcal{C}_{b,c}$ is $\mathbb{F}_{q^6}$ -projectively equivalent to the projective closure of*

$$\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q.$$

Proof. By Theorem ?? we may assume that

$$\mathcal{C}_{b,c} : Y^{q^2+q+1} = X^{q^2+q+1} + \lambda(X^{q^2} + X^q + X), \text{ where } \lambda \in \mathbb{F}_q \text{ with } \eta(\lambda) = -1.$$

Note that $\phi(\mathcal{C}_{b,c}) : Y^{q^2+q+1} + X^{q^2+1}Z^q - \frac{1}{r}X^qZ^{q^2+1} = 0$ is the image of the projective closure of $\mathcal{C}_{b,c}$ under the isomorphism

$$\phi(X : Y : Z) = \left(-\frac{1}{r}X - Z : \gamma Y : -X + rZ \right),$$

where $r \in \mathbb{F}_{q^2}$ and $\gamma \in \mathbb{F}_{q^3}$ are roots of $X^2 - \lambda$ and $X^{q^2+q+1} - (2/\lambda)$, respectively. Finally, $\phi(\mathcal{C}_{b,c})$ is isomorphic to the curve given by $Y^{q^2+q+1} = X^{q^2+1}Z^q + X^qZ^{q^2+1}$, by means of the projectivity $(X : Y : Z) \mapsto (\alpha X : Y : -\alpha^q r Z)$, where $\alpha \in \mathbb{F}_{q^6}$ is a root of $X^{q^4+q^2+1} + (1/r^q)$. $\square$

Now, let h be a positive integer and $T_{2h}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{h-1}}$ be the trace polynomial. The following result gives a classification for the roots of the quadratic polynomial $h(X) = X^2 + bX + c$.

Lemma 2.2.8 ((??), First Section). *If $h(X) = X^2 + bX + c$, with $b, c \in \mathbb{F}_{2^h}$, is a quadratic polynomial, then*

1. *h has a double root in $\mathbb{F}_{2^h}$ if and only if $b = 0$.*
2. *h has two roots in $\mathbb{F}_{2^h}$ if and only if $b \neq 0$ and $T_{2h}(c/b^2) = 0$.*
3. *h has no roots in $\mathbb{F}_{2^h}$ if and only if $b \neq 0$ and $T_{2h}(c/b^2) \neq 0$.*

Note that the projective closure of the curve $\mathcal{C}_{b,c} : Y^{2^{2h}+2^h+1} = X^{2^{2h}+2^h+1} + b(X^{2^{2h}} + X^{2^h} + X) + c$, where $b, c \in \mathbb{F}_{2^h}$ with $(b, c) \neq (0, 0)$, is $\mathbb{F}_{2^{3h}}$ -projectively equivalent to the Fermat curve of degree $2^{2h} + 2^h + 1$, when $b = 0$. On the other hand, if $bc \neq 0$, the projective closure of $\mathcal{C}_{b,c}$ is $\mathbb{F}_{2^h}$ -projectively equivalent to the projective closure of $\mathcal{C}_{d,d}$, where $d = b^3/c^2$, by means of the projectivity $(X : Y : Z) \mapsto (\frac{c}{b}X : \frac{c}{b}Y : Z)$.

Theorem 2.2.9. *If $b, c \in \mathbb{F}_q$, with $b \neq 0$, then the projective closure of the curve*

$$\mathcal{C}_{b,c} : Y^{2^{2h}+2^h+1} = X^{2^{2h}+2^h+1} + b(X^{2^{2h}} + X^{2^h} + X) + c$$

is projectively equivalent to the projective closure of the curve given by $Y^{2^{2h}+2^h+1} = f(X)$, with

$$f(X) = \begin{cases} X^{2^{2h}+2^h+1} + 1 & \text{if } T_{2^h}(b^3/c^2) = 0, \\ X^{2^{2h}} + X^{2^h} + X & \text{if } c = 0, \\ X^{2^{2h}+1} + X^{2^h} & \text{if } T_{2^h}(b^3/c^2) \neq 0. \end{cases}$$

Proof. 1. If $T_{2^h}(b^3/c^2) = 0$, then the result is analogous to Theorem ??(1).

2. For $c = 0$, let $\lambda \in \mathbb{F}_{2^h}$ be the root of $X^2 - 1/b$ (cf. Lemma ??). It follows that the projective closure of $\mathcal{C}_{b,c}$ is $\mathbb{F}_{2^h}$ -projectively equivalent to the Norm-Trace curve, by means of the projectivity $(X : Y : Z) \mapsto (X : Y : \lambda(X + Z))$.

3. If $T_{2^h}(b^3/c^2) \neq 0$, then $bc \neq 0$, and as mentioned before, the projective closure of $\mathcal{C}_{b,c}$ is $\mathbb{F}_{2^h}$ -projectively equivalent to the projective closure of

$$\mathcal{C}_{d,d} : Y^{2^{2h}+2^h+1} = X^{2^{2h}+2^h+1} + d(X^{2^{2h}} + X^{2^h} + X) + d, \text{ where } d = b^3/c^2.$$

Note that $\phi(\mathcal{C}_{b,c}) : Y^{2^{2h}+2^h+1} + X^{2^{2h}+1}Z^{2^h} - \frac{\alpha}{d}X^{2^h}Z^{2^{2h}+1} = 0$ is the image of the projective closure of $\mathcal{C}_{b,c}$ under the isomorphism

$$\phi(X : Y : Z) = \left(-\frac{\alpha}{d}X - Z : \lambda Y : -X + \alpha Z \right),$$

where $\alpha \in \mathbb{F}_{2^{2h}}$ and $\lambda \in \mathbb{F}_{2^{3h}}$ are roots of $X^2 + X - d$ and $X^{2^{2h}+2^h+1} - (\alpha^2 + d)/d^2$, respectively. Finally, $\phi(\mathcal{C}_{b,c})$ is isomorphic to the curve given by

$$Y^{2^{2h}+2^h+1} = X^{2^{2h}+1}Z^{2^h} + X^{2^h}Z^{2^{2h}+1},$$

by means of the projectivity $(X : Y : Z) \mapsto (rX : Y : -\frac{r^{2^{3h}}d}{\alpha}Z)$, where $r \in \mathbb{F}_{2^{6h}}$ is a root of $X^{2^{4h}+2^{2h}+1} + (\alpha/d)^{2^h}$.

□

Proposition 2.2.10. *Let $b, c \in \mathbb{F}_{2^h}$, with $b \neq 0$, and $f(X) = X^{2^{2h}+2^h+1} + b(X^{2^{2h}} + X^{2^h} + X) + c \in \mathbb{F}_{2^h}[X]$.*

1. If $c = 0$, then $f(X) = (X - r)^{2^h+1} \prod_{i=1}^{2^h} (X - r_i)$, where $r \in \mathbb{F}_{2^h}$ and $r_i \in \mathbb{F}_{2^{3h}} \setminus \{r\}$ are pairwise distinct.
2. If $T_{2^h}(b^3/c^2) \neq 0$, then $f(X) = (X - t)^{2^h} (X - t^{2^h})^{2^h} \prod_{i=1}^{2^{2h}-2^h+1} (X - r_i)$ where $t \in \mathbb{F}_{2^{2h}} \setminus \mathbb{F}_{2^h}$ and $r_i \in \mathbb{F}_{2^{3h}}$ are pairwise distinct.

Proof. By Lemma ??, the result is analogous to Proposition ??. □

The next goal is to compute the number of $\mathbb{F}_{q^3}$ -rational points on $\mathcal{C}_{b,c}$. Note that by $\mathbb{F}_{q^3}$ -rational points on $\mathcal{C}_{b,c}$, we mean the $\mathbb{F}_{q^3}$ -rational points on the nonsingular model of $\mathcal{C}_{b,c}$.

Proposition 2.2.11. *The number of $\mathbb{F}_{q^3}$ -rational points of $\mathcal{C}_{b,c}$ is*

$$\#\mathcal{C}_{b,c}(\mathbb{F}_{q^3}) = \begin{cases} q^5 - q^3 - q^2 + 1 & \text{if } \eta(c^2 + 4b^3) = 1, \\ q^5 + 1 & \text{if } \eta(c^2 + 4b^3) = 0, \\ q^5 + q^3 + q^2 + 1 & \text{if } \eta(c^2 + 4b^3) = -1, \end{cases} \quad \text{for } p > 2$$

and

$$\#\mathcal{C}_{b,c}(\mathbb{F}_{2^{3h}}) = \begin{cases} 2^{5h} - 2^{3h} - 2^{2h} + 1 & \text{if } T_{2^h}(b^3/c^2) = 0, \\ 2^{5h} + 1 & \text{if } c = 0, \\ 2^{5h} + 2^{3h} + 2^{2h} + 1 & \text{if } T_{2^h}(b^3/c^2) \neq 0, \end{cases} \quad \text{for } p = 2.$$

Proof. 1. If p is an odd prime, we have the following cases.

- (i) If $\eta(c^2 + 4b^3) = 1$, then the projective closure of $\mathcal{C}_{b,c}$ is $\mathbb{F}_{q^3}$ -projectively equivalent to the Fermat curve of degree $q^2 + q + 1$ (cf. Theorems ?? and ??).
- (ii) If $\eta(c^2 + 4b^3) = 0$, then the projective closure of $\mathcal{C}_{b,c}$ is $\mathbb{F}_{q^3}$ -projectively equivalent to the Norm-Trace curve of degree $q^2 + q + 1$ (cf. Theorems ?? and ??).
- (iii) If $\eta(c^2 + 4b^3) = -1$, then by Proposition ??, $\mathcal{C}_{b,c}$ is given by $Y^{q^2+q+1} = f(X)$, where

$$f(X) = (X - t)^q (X - t^q)^q \prod_{i=1}^{q^2-q+1} (X - r_i),$$

with $t, t^q \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $r_i \in \mathbb{F}_{q^3}$. Note that $\mathcal{C}_{b,c}$ has $q^2 - q + 1$ affine points of type $(r_i, 0)$, with $i \in \{0, \dots, q^2 - q + 1\}$. Moreover, for each of the $q^3 - q^2 + q - 1$ values of $\alpha \in \mathbb{F}_{q^3}$, with $\alpha \neq r_i$ for all $i \in \{0, \dots, q^2 - q + 1\}$, we have $q^2 + q + 1$ affine points of type (α, β) , where β is a root of $Y^{q^2+q+1} - f(\alpha)$. Finally, $\mathcal{C}_{b,c}$ has $q^2 + q + 1$ points at infinity of type $(1 : \lambda : 0)$, where λ is a root of $Y^{q^2+q+1} - 1$. Now, since the singularities of $\mathcal{C}_{b,c}$ are not defined in $\mathbb{F}_{q^3}$, the curve $\mathcal{C}_{b,c}$ has $q^5 + q^3 + q^2 + 1$ $\mathbb{F}_{q^3}$ -rational points.

2. If $p = 2$ then the result is analogous to the previous case. □

Proposition 2.2.12. *The genus of $\mathcal{C}_{b,c}$ is given by*

$$g(\mathcal{C}_{b,c}) = \begin{cases} \frac{q^4+2q^3-q}{2} & \text{if } \eta(c^2+4b^3) = 1, \\ \frac{q^4+q^3-q^2-q}{2} & \text{if } \eta(c^2+4b^3) = 0, \\ \frac{q^4+q}{2} & \text{if } \eta(c^2+4b^3) = -1, \end{cases} \quad \text{for } p > 2$$

and

$$g(\mathcal{C}_{b,c}) = \begin{cases} \frac{2^{4h}+2^{3h+1}-2^h}{2} & \text{if } T_{2^h}(b^3/c^2) = 0, \\ \frac{2^{4h}+2^{3h}-2^{2h}-2^h}{2} & \text{if } c = 0, \\ \frac{2^{4h}+2^{2h}}{2} & \text{if } T_{2^h}(b^3/c^2) \neq 0, \end{cases} \quad \text{for } p = 2.$$

Proof. Suppose that p is an odd prime. If $\eta(c^2+4b^3) = 1$, then the curve $\mathcal{C}_{b,c}$ is nonsingular. Thus, by Theorem ?? we have the result. Otherwise, the result follows from Proposition ?? and Lemma ??.

If $p = 2$ then the result is analogous to the previous case. $\square$

2.3 The automorphism group

Throughout this section, we denote by $\mathbb{K}$ the algebraic closure of $\mathbb{F}_q$, where q is a power of a prime p . Let $b, c \in \mathbb{F}_q$ be such that $(b, c) \neq (0, 0)$. Observe that the curve $\mathcal{C}_{b,c}$ is equivalent to the Fermat curve or Norm-trace curve, when $\eta(c^2+4b^3) = 1$ (or $T_q(b^3/c^2) = 0$, when $p = 2$) or $\eta(c^2+4b^3) = 0$ (or $b \neq 0$ and $c = 0$, when $p = 2$), respectively. The following results provide the automorphism groups of these curves.

Theorem 2.3.1 (??, Theorem 1 and Comments on Page 257). *If $p \nmid n$ and $n \neq q + 1$, then the $\mathbb{K}$ -automorphism group of the Fermat curve $\mathcal{F}_n : Y^n + X^n + 1 = 0$ is $\text{Aut}_{\mathbb{K}}(\mathcal{F}_n) \cong (C_n \times C_n) \rtimes S_3$.*

Theorem 2.3.2 (??, Theorem 3.1). *If $r \geq 3$ and $\mathcal{N}_{q,r} : X^{\frac{q^r-1}{q-1}} = Y^{q^{r-1}} + Y^{q^{r-2}} + \dots + Y$ is the norm-trace curve, then $\text{Aut}_{\mathbb{K}}(\mathcal{N}_{q,r})$ has order $q^{r-1}(q^r - 1)$ and is a semidirect product $G \rtimes C$, where*

$$G = \{(x, y) \mapsto (x, y + a) : T_{q^r}(a) = 0\}, \quad C = \{(x, y) \mapsto (bx, b^{\frac{q^r-1}{q-1}} y) : b \in \mathbb{F}_{q^r}^*\}.$$

In this sense, the objective of this section is to compute the automorphism group of the curve $\mathcal{C}_{b,c}$, when $\eta(c^2+4b^3) = -1$ (or $T_q(b^3/c^2) \neq 0$, when $p = 2$). For this, we begin by investigating the canonical series $|dy|$ and the dimension of the Riemann-Roch spaces associated to the divisors $(q^2 + q + 1)P_1$ and $(q^2 + q + 1)P_2$, where P_1 and P_2 are suitable points on the nonsingular model of $\mathcal{C}_{b,c}$.

2.3.1 Riemann-Roch space and canonical series

Consider the following curve

$$\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q, \quad (2.3)$$

defined over $\mathbb{F}_{q^6}$ and let $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{C}$, where $y^{q^2+q+1} = x^{q^2+1} + x^q$. Note that $(0 : 0 : 1)$ and $(1 : 0 : 0)$ are the unique singular points on the projective closure of $\mathcal{C}$. From Kummer extension theory it follows that each point on $\mathcal{C}$ is associated to a unique place on $\mathbb{K}(\mathcal{C})$ (cf. Theorem ??). Thus we denote by Q_0 and Q_∞ the unique places associated to $(0 : 0 : 1)$ and $(1 : 0 : 0)$, respectively. Let $Q_i = (\beta_i, 0)$ be points on $\mathcal{C}$, where β_i , for $i = 1, \dots, q^2 - q + 1$, are the nonzero roots of $f(X) = X^{q^2+1} + X^q$. If D is a divisor on $\mathcal{C}$, then the *Riemann-Roch space* associated to D , defined by $\mathcal{L}(D) = \{\varphi \in \mathbb{K}(\mathcal{C}) : \text{div}(\varphi) \geq -D\} \cup \{0\}$, is a vector space over $\mathbb{K}$ of finite dimension denoted by $\ell(D)$.

Lemma 2.3.3. *If $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ is the function field of $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$, then the following assertions hold:*

1. $\text{div}(x) = (q^2 + q + 1)(Q_0 - Q_\infty)$;
2. $\text{div}(y) = \sum_{i=1}^{q^2-q+1} Q_i + qQ_0 - (q^2 + 1)Q_\infty$;
3. $\text{div}(dx) = (q^2 + q) \sum_{i=1}^{q^2-q+1} Q_i + (q^2 + q)Q_0 - (q^2 + q + 2)Q_\infty$;
4. $\text{div}(dy) = (q^4 + q^2 + q)Q_0 - (q^2 + 2)Q_\infty$.

Proof. Let $P = (a, b)$ be a nonsingular point on $\mathcal{C}$. Note that the line $Y - b = 0$ is not tangent to $\mathcal{C}$ at P . Thus it follows from Theorem ?? and Lemma ?? that $t = y - b$ is a local parameter for $\mathcal{C}$ at P , and $P \notin \text{Supp}(\text{div}(dy))$. Thus, we can write $\text{div}(dy) = nQ_0 + mQ_\infty$, for some integers n and m . Since $\text{div}(dy)$ is a canonical divisor of degree $n + m = 2g(\mathcal{C}) - 2$ (Corollary ??) and $p \nmid (q^2 + 1)$, we have $m = -(q^2 + 2)$ (cf. Remark ??), consequently $\text{div}(dy) = (q^4 + q^2 + q)Q_0 - (q^2 + 2)Q_\infty$. Finally, from $f_x dx + f_y dy = 0$, we have $\text{div}(dx) = (q^2 + q) \sum_{i=1}^{q^2-q+1} Q_i + (q^2 + q)Q_0 - (q^2 + q + 2)Q_\infty$. $\square$

Theorem 2.3.4. *Let $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$. Consider the subset $B \subset \mathbb{K}(\mathcal{C})$ given by $B = \cup_{s=0}^{q-1} B_s$, where*

$$B_0 = \left\{ \frac{x^j}{y^{i+1}} : 1 \leq i \leq q \text{ and } 0 \leq j \leq i-1 \right\}, \text{ and}$$

$$B_s = \left\{ \frac{x^j}{y^{i+s+1}} : sq \leq i \leq (s+1)q \text{ and } s \leq j \leq i-1 \right\} \text{ for each } 1 \leq s \leq q-1.$$

Then B is a basis of the Riemann-Roch space $\mathcal{L}(\text{div}(dx))$ associated to $\text{div}(dx)$ of $\mathcal{C}$.

Proof. It follows directly from the that $B \subset \mathcal{L}(\operatorname{div}(dx))$ is a linearly independent set with $\mathfrak{g}(\mathcal{C})$ elements. $\square$

Since $dx = \frac{y^{q^2+q}}{x^{q^2}} dy$, as a consequence of the previous result we have the following result.

Corollary 2.3.5. *Let $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$. Consider the subset $B' \subset \mathbb{K}(\mathcal{C})$ given by $B' = \cup_{s=0}^{q-1} B'_s$, where*

$$B'_0 = \left\{ \frac{y^{q^2+q-i-1}}{x^{q^2-j}} : 1 \leq i \leq q \text{ and } 0 \leq j \leq i-1 \right\}, \text{ and}$$

$$B'_s = \left\{ \frac{y^{q^2+q-i-s-1}}{x^{q^2-j}} : sq \leq i \leq (s+1)q \text{ and } s \leq j \leq i-1 \right\} \text{ for } 1 \leq s \leq q-1.$$

Then B' is a basis of the Riemann-Roch space $\mathcal{L}(\operatorname{div}(dy))$ associated to $\operatorname{div}(dy)$ of $\mathcal{C}$.

Note that B' gives an explicit to the canonical series

$$|dy| = \{\operatorname{div}(\varphi dy) : \varphi \in \mathcal{L}(\operatorname{div}(dy)) \setminus \{0\}\} \text{ of } \mathbb{K}(\mathcal{C})$$

(cf. Definitions ?? and ??). One can easily check that for $g = \frac{y^{q^2+q-i-s-1}}{x^{q^2-j}} \in B'$, we have

$$\operatorname{div}(gdy) = (q^2 + q - i - s - 1) \sum_{i=1}^{q^2-q+1} Q_i + \alpha Q_0 + \beta Q_\infty \quad (2.4)$$

where $\alpha = q^2 + j(q^2 + q + 1) - q(i + s)$ and $\beta = (i + s)(q^2 + 1) - j(q^2 + q + 1) - q - 1$.

Lemma 2.3.6. *Let $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ and B' be the basis of the Riemann-Roch space $\mathcal{L}(\operatorname{div}(dy))$, as in Corollary ??. If g and h are elements of B' , with $g \neq h$, then the following assertions hold:*

1. $\operatorname{Ord}_{Q_0}(gdy) \neq \operatorname{Ord}_{Q_0}(hdy)$.
2. $\operatorname{Ord}_{Q_\infty}(gdy) \neq \operatorname{Ord}_{Q_\infty}(hdy)$.

Proof. Let

$$g = \frac{y^{q^2+q-i_1-s_1-1}}{x^{q^2-j_1}} \text{ and } h = \frac{y^{q^2+q-i_2-s_2-1}}{x^{q^2-j_2}},$$

where $i_l = s_l q + m_l$, for $l = 1, 2$, with $1 \leq m_l \leq q$, when $s_l = 0$, and otherwise $0 \leq m_l \leq q$.

1. If $\operatorname{Ord}_{Q_0}(gdy) = \operatorname{Ord}_{Q_0}(hdy)$, then by (??) we have $(j_1 - j_2)(q^2 + q + 1) = q(i_1 + s_1 - i_2 - s_2)$. Consequently $(q^2 + q + 1)$ divides $(i_1 + s_1 - i_2 - s_2)$. Since $-(q^2 + q + 1) < i_1 + s_1 - i_2 - s_2 < q^2 + q + 1$, we have $j_1 = j_2$ and $i_1 + s_1 = i_2 + s_2$. Thus $(s_1 - s_2)(q + 1) = m_2 - m_1$, and hence $(q + 1)$ divides $(m_2 - m_1)$. Since $-q \leq m_2 - m_1 \leq q$, we have $g = h$.
2. The proof is analogous.

$\square$

2.3.2 Weierstrass semigroup

Let $b, c \in \mathbb{F}_q$ be such that $\eta(c^2 + 4b^3) = -1$ (or $T_q(b^3/c^2) \neq 0$, when $p = 2$). By Propositions ?? and ??, we can suppose that

$$\mathcal{C}_{b,c} : Y^{q^2+q+1} = (X - \alpha_1)^q (X - \alpha_2)^q \prod_{i=1}^{q^2-q+1} (X - r_i), \quad (2.5)$$

where α_1 and α_2 are roots of $g(X) = X^2 + \frac{c}{b}X - b$. Note that $(\alpha_1 : 0 : 1)$ and $(\alpha_2 : 0 : 1)$ are the unique singular points on the projective closure of $\mathcal{C}$. From Kummer extension theory it follows that each point on $\mathcal{C}$ is associated to a unique place on $\mathbb{K}(\mathcal{C})$ (cf. Theorem ??). Thus we denote by P_1 and P_2 the unique places associated to $(\alpha_1 : 0 : 1)$ and $(\alpha_2 : 0 : 1)$, respectively. In this section we will use the Weierstrass semigroup to compute the dimension of the Riemann-Roch spaces associated to the divisors $(q^2 + q + 1)P_1$ and $(q^2 + q + 1)P_2$. Throughout this section, the floor, ceiling and fractional part functions will be denoted by $\lfloor \cdot \rfloor$, $\lceil \cdot \rceil$ and $\{ \cdot \}$, respectively.

Theorem 2.3.7 (??), Theorem 3.5). *Let $F/K(x)$ be a Kummer extension given by*

$$Y^m = \prod_{i=1}^r (X - \alpha_i)^{\lambda_i}, \text{ with } 0 < \lambda_i < m.$$

Fix an element $\alpha_0 \in K \setminus \{\alpha_1, \dots, \alpha_r\}$, and set $\alpha_{r+1} = \infty$, $\lambda_0 = 0$ and $\lambda_{r+1} = -\sum_{i=0}^r \lambda_i$. For each $u = 0, \dots, r+1$, consider the usual place $P_u \in \mathbb{P}_{K(x)}$ corresponding to $\alpha_u \in K \cup \{\infty\}$, and the divisor $D_u = \sum_{Q_{u,v} | P_u} Q_{u,v} \in \text{Div}(F)$. If $s \geq 1$ is an integer, then $\ell(sD_u) - \ell((s-1)D_u)$ is the number of elements $j \in \{0, \dots, (m, \lambda_u) - 1\}$ such that

$$\sum_{i=0}^r \left\{ \frac{(t_u + jm_u)\lambda_i}{m} \right\} \leq 1 + \left\lfloor \frac{s-1}{m} \right\rfloor$$

where $m_u = \frac{m}{(m, \lambda_u)}$ and $t_u \in \{0, \dots, m_u - 1\}$ is the unique element for which $s + \frac{\lambda_u}{(m, \lambda_u)}t_u \equiv 0 \pmod{m_u}$.

For each $s \in \mathbb{N}$, let $t_j(s) \in \{0, 1, \dots, q^2 + q\}$ be the unique element for which $s + qt_j(s) \equiv 0 \pmod{(q^2 + q + 1)}$. Note that if $l \in \{1, \dots, q^2 + q\}$, then l can be written uniquely in the form $l = \alpha q + \beta$ where $0 \leq \alpha \leq q$ and $1 \leq \beta \leq q$.

Proposition 2.3.8. *Let $n \in \mathbb{N}$ and $s = n(q^2 + q + 1) + \alpha q + \beta$ where $0 \leq \alpha \leq q$ and $1 \leq \beta \leq q$, then*

$$\sigma_j(s) := \sum_{i=1}^{q^2-q+3} \left\{ \frac{t_j(s)\lambda_i}{q^2+q+1} \right\} = 2 - \alpha + \beta(q+1), \text{ for } j = 1, 2,$$

where $t_j(s) \in \{0, 1, \dots, q^2 + q\}$ is the unique element for which $s + qt_j(s) \equiv 0 \pmod{(q^2 + q + 1)}$ and $\lambda_i = q$ if $i \in \{1, 2\}$, or $\lambda_i = 1$ otherwise.

Proof. Note that $t_j(s) = \beta(q+1) - \alpha$ and $\left\{ \frac{qt_j(s)}{q^2+q+1} \right\} = \frac{q^2+q+1-\alpha q-\beta}{q^2+q+1}$. Therefore

$$\sigma_j(s) = 2 \left\{ \frac{qt_j(s)}{q^2+q+1} \right\} + (q^2 - q + 1) \left\{ \frac{t_j(s)}{q^2+q+1} \right\} = 2 - \alpha + \beta(q+1).$$

□

For $n \in \mathbb{N}$, let $s \in \mathbb{N}$ be such that $s \in \{n(q^2 + q + 1), \dots, (n+1)(q^2 + q + 1)\}$. If $s = n(q^2 + q + 1)$ then $\sigma_j(s) = 0$ and consequently $\ell(sP_j) - \ell((s-1)P_j) = 1$. Therefore s is a non-gap at P_j . If $s = n(q^2 + q + 1) + l$, where $1 < l \leq q^2 + q + 1$, then

$$\left\lfloor \frac{s-1}{q^2 + q + 1} \right\rfloor = \left\lfloor n + \frac{l-1}{q^2 + q + 1} \right\rfloor = n.$$

Thus, it follows from Theorem ?? that

$$\ell(sP_j) - \ell((s-1)P_j) = \begin{cases} 1 & \text{if } \sigma_j(s) \leq n+1, \\ 0 & \text{if } \sigma_j(s) > n+1, \end{cases} \quad \text{for } j = 1, 2.$$

Finally, note that s is a gap number at P_j if and only if $\ell(sP_j) - \ell((s-1)P_j) = 0$, that is, $\sigma_j(s) > n+1$.

Corollary 2.3.9. *The set of all gaps at P_j is given by*

$$G(P_j) = \{n(q^2 + q + 1) + \alpha q + \beta : 0 \leq n \leq q(q-1), 0 \leq \alpha \leq q, 1 \leq \beta \leq q, \beta(q-1) - \alpha > n-1\}, \text{ for } j = 1, 2.$$

Proof. If $s = n(q^2 + q + 1) + \alpha q + \beta$ with $0 \leq n \leq q(q-1)$, $0 \leq \alpha \leq q$ and $1 \leq \beta \leq q$, then

$$\sigma_j(s) > n+1 \Leftrightarrow 2 - \alpha + \beta(q+1) > n+1 \Leftrightarrow \beta(q+1) - \alpha > n-1,$$

hence s is a gap number at P_j . Now, If $n \geq q(q-1) + 1$ then $\beta(q-1) - \alpha \leq q(q-1) \leq n-1$, hence s is a non-gap at P_j .

□

Corollary 2.3.10. *For each $j = 1, 2$, the dimension of the Riemann-Roch space associated to divisor $(q^2 + q + 1)P_j$ is given by $\ell((q^2 + q + 1)P_j) = 3$.*

Proof. It is enough to observe that $q^2 + 1$ and $q^2 + q + 1$ are the smallest nonzero elements of the Weierstrass semigroup at P_j .

□

2.3.3 The automorphism group of $\mathcal{C}_{b,c}$, with $\eta(c^2 + 4b^3) = -1$

Let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$. If $b, c \in \mathbb{F}_q$ are such that $\eta(c^2 + 4b^3) = -1$ (or $T_q(b^3/c^2) \neq 0$, if $p = 2$), then it follows from Proposition ?? and Theorem ?? that the projective closure of $\mathcal{C}_{b,c}$ is $\mathbb{F}_{q^6}$ -projectively equivalent to the projective closure of the curve

$$\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q, \quad (2.6)$$

defined over $\mathbb{F}_{q^6}$. Let $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{C}$, where $y^{q^2+q+1} = x^{q^2+1} + x^q$. As before, let Q_0 and Q_∞ be the unique places associated to the singularities $(0 : 0 : 1)$ and $(1 : 0 : 0)$ on the projective closure of $\mathcal{C}$, respectively. Let $Q_i = (\beta_i, 0)$ be points on $\mathcal{C}$, where β_i , for $i = 1, \dots, q^2 - q + 1$, are the nonzero roots of $f(X) = X^{q^2+1} + X^q$.

Lemma 2.3.11. *The integer $q^2 + 1$ is a gap number at $Q_i = (\beta_i, 0)$, for all $i = 1, \dots, q^2 - q + 1$,*

Proof. Since

$$\mathcal{C} : Y^{q^2+q+1} = X^q \prod_{i=1}^{q^2-q+1} (X - \beta_i),$$

using the same notations as in Theorem ??, we have $j \in \{0\}$, $t_u = q$, $\lambda_1 = q$, and $\lambda_2 = \dots = \lambda_{q^2-q+2} = 1$. Since

$$\sum_{l=1}^{q^2-q+2} \left\{ \frac{q\lambda_l}{q^2+q+1} \right\} = \frac{q^3+q}{q^2+q+1} > 1 = 1 + \left\lfloor \frac{q^2}{q^2+q+1} \right\rfloor,$$

it follows from Theorem ?? that $\ell((q^2+1)Q_i) - \ell(q^2Q_i) = 0$, for all $j = 1, \dots, q^2 - q + 1$. Therefore, $q^2 + 1$ is a gap number at Q_i , for all $i = 1, \dots, q^2 - q + 1$. $\square$

Theorem 2.3.12. *The set $\{Q_0, Q_\infty\}$ is fixed by the automorphism group of $\mathcal{C}$.*

Proof. Consider the divisor

$$D = \operatorname{div} \left(\frac{1}{x} dy \right) = (q^4 - 1)Q_0 + (q - 1)Q_\infty \in |dy|,$$

and let α be a $\mathbb{K}$ -automorphism of $\mathcal{C}$. It follows from Lemma ?? that

$$D^\alpha = (q^4 - 1)Q_0^\alpha + (q - 1)Q_\infty^\alpha \in |dy|.$$

Since $q^2 + 1$ is a gap number at Q_i , for $i = 1, \dots, q^2 - q + 1$ (cf. Lemma ??), and $q^2 + 1$ is a non-gap at Q_0 and Q_∞ (cf. Corollary ??), we have $Q_0^\alpha, Q_\infty^\alpha \notin \{Q_i, \dots, Q_{q^2-q+1}\}$ (cf. Remark ??). Let B' be the basis of $\mathcal{L}(\operatorname{div}(dy))$, as in Corollary ?. Since $D^\alpha \in |dy|$, we have $D^\alpha = \operatorname{div}(f dy) \in |dy|$, where

$$f = \sum_{s,i,j} c_{s,i,j} \frac{y^{q^2+q-i-s-1}}{x^{q^2-j}} = \frac{h(x,y)}{x^{q^2}},$$

for some polynomial $h(x,y)$ (cf. Corollary ??). One can easily check that

$$\operatorname{div}(h(x,y)) = (q^4 - 1)Q_0^\alpha + (q - 1)Q_\infty^\alpha + (q^3 - q)Q_0 - (q^4 + q^3 - 2)Q_\infty$$

(cf. Lemma ??). Thus, $h(x,y) = x^t y^r g(x,y)$, where t and r are integers, and $g(x,y)$ is a polynomial, with $g(0,0) \neq 0$. Since $Q_0^\alpha, Q_\infty^\alpha \notin \{Q_i, \dots, Q_{q^2-q+1}\}$, we have $r = 0$, consequently $h(x,y) = x^t g(x,y)$.

Now, suppose that $Q_0^\alpha, Q_\infty^\alpha \notin \{Q_0\}$. Since $g(0,0) \neq 0$ and

$$\operatorname{div}(g(x,y)) = (q^4 - 1)Q_0^\alpha + (q - 1)Q_\infty^\alpha + (q^3 - q - t(q^2 + q + 1))Q_0 + (t(q^2 + q + 1) - q^4 - q^3 + 2)Q_\infty,$$

we have $q^3 - q = t(q^2 + q + 1)$, which is a contradiction. Therefore, $Q_0^\alpha = Q_0$ or $Q_\infty^\alpha = Q_0$. Thus, we have some cases to consider:

If $Q_0^\alpha = Q_0$, then suppose that $Q_\infty^\alpha \neq Q_\infty$. One can easily check that $t = q^2 - 1$ and

$$\operatorname{div}(g(x,y)) = (q - 1)Q_\infty^\alpha - (q - 1)Q_\infty.$$

Hence, $q - 1$ is a non-gap at Q_∞ , which is a contradiction (cf. Corollary ??). Consequently, $Q_\infty^\alpha = Q_\infty$.

If $Q_\infty^\alpha = Q_0$, set $D = \operatorname{div}(dy/x^{q^2-q+1}) = (q-1)Q_0 + (q^4-1)Q_\infty \in |dy|$, then the same arguments above can be used to show that $Q_0^\alpha = Q_\infty$.

Therefore,

$$D^\alpha = (q^4-1)Q_0^\alpha + (q-1)Q_\infty^\alpha \in \{(q^4-1)Q_0 + (q-1)Q_\infty, (q-1)Q_0 + (q^4-1)Q_\infty\}.$$

Hence, the set $\{Q_0, Q_\infty\}$ is fixed by α . □

Proposition 2.3.13. *The following assertions hold:*

1. $\mathcal{L}((q^2+q+1)Q_\infty) = \langle 1, y, x \rangle$;
2. $\mathcal{L}((q^2+q+1)Q_0) = \langle 1, \frac{1}{x}, \frac{y}{x} \rangle$.

Proof. 1. It follows from Proposition ??, Theorem ?? and Corollary ?? that $\ell((q^2+q+1)Q_\infty) = 3$. Hence, it is enough to observe that $\langle 1, y, x \rangle \subset \mathcal{L}((q^2+q+1)Q_\infty)$ and that $1, x, y$ are linearly independent functions.

2. The proof is analogous. □

Theorem 2.3.14. *If $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ then $\operatorname{Aut}_{\mathbb{K}}(\mathcal{C}) \cong C_{q^4+q^2+1} \rtimes C_2$.*

Proof. Note that for any (q^4+q^2+1) -th root of unity $\lambda \in \mathbb{F}_{q^6}$, the projectivities

$$(X : Y : Z) \mapsto (\lambda^{q^2+q+1}X : \lambda^q Y : Z) \text{ and } (X : Y : Z) \mapsto (Z : Y : X).$$

preserve $\mathcal{C}$. Thus, the subgroup $G = \langle h_1, h_2 \rangle$ of $\operatorname{PGL}(3, \mathbb{F}_{q^6})$ is a subgroup of $\operatorname{Aut}_{\mathbb{K}}(\mathcal{C})$ of order $2(q^4+q^2+1)$, with

$$h_1 = \begin{pmatrix} \lambda^{q^2+q+1} & 0 & 0 \\ 0 & \lambda^q & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } h_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad (2.7)$$

where $\lambda \in \mathbb{F}_{q^6}$ is a primitive (q^4+q^2+1) -th roots of unity.

Now, by Theorem ??, the set $\{Q_0, Q_\infty\}$ is invariant under the action of $\operatorname{Aut}_{\mathbb{K}}(\mathcal{C})$. This induces a group homomorphism

$$\varphi : \operatorname{Aut}_{\mathbb{K}}(\mathcal{C}) \rightarrow \mathbb{Z}/2\mathbb{Z} \text{ with } \varphi(\alpha) = \begin{cases} 0 & \text{if } Q_0^\alpha = Q_0, \\ 1 & \text{if } Q_0^\alpha = Q_\infty. \end{cases}$$

It follows that $|\operatorname{Aut}_{\mathbb{K}}(\mathcal{C})| = 2|\ker(\varphi)|$, as there exists $\alpha \in \operatorname{Aut}_{\mathbb{K}}(\mathcal{C})$ such that $Q_0^\alpha = Q_\infty$. Now, let $\alpha \in \ker(\varphi)$, that is, α fixes Q_∞ . Since $\alpha(x), \alpha(y) \in \alpha(\mathcal{L}((q^2+q+1)Q_\infty)) \subseteq \langle 1, y, x \rangle$ (cf. Lemma

?? and Proposition ??), it follows that α is linear. Thus, we can write $\alpha(X : Y : Z) = (a_1X + a_2Y + a_3Z : b_1X + b_2Y + b_3Z : c_1X + c_2Y + c_3Z)$, for some $a_i, b_i, c_i \in \mathbb{K}$ with $i = 1, 2, 3$. Since $Q_\infty^\alpha = Q_\infty$ and $Q_0^\alpha = Q_0$, we have $\alpha(X : Y : Z) = (aX + \bar{a}Y : bY : \bar{c}Y + cZ)$ for some $a, \bar{a}, b, \bar{c}, c \in \mathbb{K}$. Moreover, $\alpha(y)^{q^2+q+1} - \alpha(x)^{q^2+1} - \alpha(x)^q = 0$ in $\mathbb{K}(x, y)$ and therefore $F(X, Y, Z) = Y^{q^2+q+1} - X^{q^2+1}Z^q - X^qZ^{q^2+1}$ divides

$$G(X, Y, Z) = \alpha(Y)^{q^2+q+1} - \alpha(X)^{q^2+1}\alpha(Z)^q - \alpha(X)^q\alpha(Z)^{q^2+1}$$

in $\mathbb{K}[X, Y, Z]$. Since $\deg(G) = \deg(F)$, we have $G(X, Y, Z) = b^{q^2+q+1}F(X, Y, Z)$. Consequently $\alpha \in \ker(\varphi)$ if and only if $\alpha(X : Y : Z) = (aX : bY : Z)$ where $(a : b : 1) \in \mathbb{P}^2(\mathbb{K})$, with $ab \neq 0$, is a solution to

$$\begin{cases} X^{q^2+1} &= Y^{q^2+q+1}, \\ X^q &= Y^{q^2+q+1}. \end{cases} \quad (2.8)$$

Hence $|\ker(\varphi)| = q^4 + q^2 + 1$ and consequently $\text{Aut}_{\mathbb{K}}(\mathcal{C}) = G$. Finally, since $\langle h_1 \rangle = \ker(\varphi) \cong C_{q^4+q^2+1}$ is normal in G , we have $\text{Aut}_{\mathbb{K}}(\mathcal{C}) \cong C_{q^4+q^2+1} \rtimes C_2$. $\square$

Corollary 2.3.15. *The automorphism group of the curve $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ admits a presentation*

$$\text{Aut}_{\mathbb{K}}(\mathcal{C}) = \langle \sigma, \tau : \sigma^{q^4+q^2+1} = 1, \tau^2 = 1 \text{ and } \tau\sigma\tau = \sigma^{q^3} \rangle,$$

where the automorphisms σ and τ are given by

$$\sigma(x) = \lambda^{q^2+q+1}x, \quad \sigma(y) = \lambda^q y \quad \tau(x) = \frac{1}{x}, \quad \tau(y) = \frac{y}{x},$$

where λ denotes a primitive $(q^4 + q^2 + 1)$ -th root of unity.

Proof. It is enough to note that

$$h_2 h_1 h_2 = \lambda^{q^2+q+1} \begin{pmatrix} \lambda^{q^3(q^2+q+1)} & 0 & 0 \\ 0 & \lambda^{q^4} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \lambda^{q^2+q+1} h_1^{q^3},$$

where h_1 and h_2 are defined by (??). $\square$

Corollary 2.3.16. *Let q be a power of an odd prime p . If $b, c \in \mathbb{F}_q$, with $\eta(c^2 + 4b^3) = -1$, then $\text{Aut}_{\mathbb{K}}(\mathcal{C}_{b,c}) \subset \text{PGL}(3, \mathbb{F}_{q^3})$ and its order is $2(q^4 + q^2 + 1)$.*

Proof. By Theorem ?? we may assume that

$$\mathcal{C}_{b,c} : Y^{q^2+q+1} = X^{q^2+q+1} + \lambda(X^{q^2} + X^q + X), \text{ where } \lambda \in \mathbb{F}_q \text{ with } \eta(\lambda) = -1.$$

Consider the following birational transformations

$$\alpha(x, y, z) = (\varepsilon x + \lambda \gamma z, y, \gamma x + \varepsilon z) \text{ and } \beta(x, y, z) = (\varepsilon x - \lambda \gamma z, y, \gamma x - \varepsilon z),$$

where $(\varepsilon, \gamma) \in A_{5,6} \subset \mathbb{F}_{q^3} \times \mathbb{F}_{q^3}$ (cf. Lemma ??). Since α and β preserve the curve $\mathcal{C}_{b,c}$, they are $\mathbb{K}$ -automorphism of this curve (cf. Lemma ??). Hence, it follows from Lemma ?? that the cardinality of the set of all $\mathbb{K}$ -automorphisms of type α and β is $2(q^4 + q^2 + 1)$. Since $\mathcal{C}_{b,c}$ is isomorphic to $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ (cf. Proposition ??), it follows from Theorem ?? that $\text{Aut}_{\mathbb{K}}(\mathcal{C}_{b,c}) \subset \text{PGL}(3, \mathbb{F}_{q^3})$ and its order is $2(q^4 + q^2 + 1)$.

□

THE HASSE-WITT INVARIANT FOR A CLASS OF KUMMER EXTENSION

3.1 The Hasse-Witt invariant of $Y^m + X^n + 1 = 0$ and $Y^m + X^n + X = 0$

Let $\mathbb{F}_q$ be the field with q elements, where q is a power of a prime p , and let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$. For positive integers n and m not divisible by p , with $n \geq m$, consider the curve

$$\mathcal{F}_{m,n} : Y^m + X^n + 1 = 0,$$

defined over $\mathbb{F}_q$. Let $\mathbb{K}(\mathcal{F}_{m,n}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{F}_{m,n}$, with $y^m + x^n + 1 = 0$. We refer the reader to (??) and (??), for more detail on the following results. The genus of $\mathcal{F}_{m,n}$ is given by

$$g = \frac{nm - n - m - \gcd(n, m)}{2} + 1 \quad (3.1)$$

and the set

$$B = \left\{ \omega_{i,j} = \frac{x^i}{y^{m-j-1}} dx : (i, j) \in I \right\}, \quad (3.2)$$

is a basis for the vector space of holomorphic differentials of $\mathcal{F}_{m,n}$, where

$$I = \{(i, j) \in \mathbb{N}^2 : im + jn \leq 2g - 2\}. \quad (3.3)$$

Remark 3.1.1. Let h_1 and h_2 be the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times$, respectively. Set

$h = \text{lcm}(h_1, h_2)$ and $q = p^h$. Note that if $(i, j) \in I$, then

$$\begin{aligned} \frac{x^i}{y^{m-j-1}} &= \frac{x^i}{y^{q(m-j-1)}} y^{m(m-j-1)(q-1)/m} \\ &= (-1)^{(m-j-1)(q-1)/m} \frac{x^i}{y^{q(m-j-1)}} (x^n + 1)^{(m-j-1)(q-1)/m} \\ &= (-1)^{(m-j-1)(q-1)/m} \sum_{r=0}^{\frac{(m-j-1)(q-1)}{m}} \binom{\frac{(m-j-1)(q-1)}{m}}{r} \frac{x^{rn+i}}{y^{q(m-j-1)}}. \end{aligned}$$

Therefore,

$$\omega_{i,j} = (-1)^{(m-j-1)(q-1)/m} \sum_{r=0}^{\frac{(m-j-1)(q-1)}{m}} \binom{\frac{(m-j-1)(q-1)}{m}}{r} \frac{x^{rn+i}}{y^{q(m-j-1)}} dx. \quad (3.4)$$

Theorem 3.1.2. Let p be a prime and m, n be positive integers coprime to p , with $n \geq m$. The Hasse-Witt invariant of the curve

$$\mathcal{F}_{m,n} : Y^m + X^n + 1 = 0,$$

is given by the cardinality of the set

$$T = \left\{ (i, j) \in I : \binom{\frac{(m-j-1)(q-1)}{m}}{\frac{(i+1)(q-1)}{n}} \not\equiv 0 \pmod{p} \right\}, \quad (3.5)$$

where $q = p^h$ and $h = \text{lcm}(h_1, h_2)$, with h_1 and h_2 the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$ and $(\mathbb{Z}/n\mathbb{Z})^\times$, respectively.

Proof. It follows from (??) that

$$\omega_{i,j} = (-1)^{(m-j-1)(q-1)/m} \sum_{r=0}^{\frac{(m-j-1)(q-1)}{m}} \binom{\frac{(m-j-1)(q-1)}{m}}{r} \frac{x^{rn+i}}{y^{q(m-j-1)}} dx.$$

Now, using the $1/p$ -linearity of the Cartier operator (cf. Section ??), we have

$$C^h(\omega_{i,j}) = \frac{(-1)^{(m-j-1)(q-1)/m}}{y^{m-j-1}} \sum_{r=0}^{\frac{(m-j-1)(q-1)}{m}} \binom{\frac{(m-j-1)(q-1)}{m}}{r} C^h(x^{rn+i} dx). \quad (3.6)$$

By Lemma ??, the term $C^h(x^{rn+i} dx)$, in equation (??), is nonzero if and only if $nr + i \equiv -1 \pmod{q}$. Since $im + nj \leq 2g - 2$ (cf. Equation (??) and (??)), we have that $i \leq n - 2$. Since $0 \leq r \leq q - 1$, it follows that $0 \leq nr + i \leq (n - 1)q + q - 2$. Thus, if $nr + i \equiv -1 \pmod{q}$, then $nr + i \in \{q - 1, 2q - 1, \dots, (n - 1)q - 1\}$ and consequently

$$r \in \left\{ \frac{q-i-1}{n}, \frac{2q-i-1}{n}, \dots, \frac{(n-1)q-i-1}{n} \right\} \cap \mathbb{Z}.$$

Moreover, one can easily check that $(i+1)(q-1)/n$ is the unique integer in

$$\left\{ \frac{q-i-1}{n}, \frac{2q-i-1}{n}, \dots, \frac{(n-1)q-i-1}{n} \right\}.$$

Thus, we can conclude from equation (??) that

$$C^h(\omega_{i,j}) = (-1)^{(m-j-1)(q-1)/m} \binom{\frac{(m-j-1)(q-1)}{m}}{\frac{(i+1)(q-1)}{n}} \omega_{i,j}.$$

It follows from Proposition ?? that the Hasse-Witt invariant of the curve $\mathcal{F}_{m,n}$ is given by the cardinality of the set

$$T = \left\{ (i, j) \in I : \binom{\frac{(m-j-1)(q-1)}{m}}{\frac{(i+1)(q-1)}{n}} \not\equiv 0 \pmod{p} \right\}.$$

□

Now, let m and n be positive integers, such that m and $n-1$ are not divisible by p , and $n \geq m$. Consider the curve

$$\mathcal{D}_{m,n} : Y^m + X^n + X = 0,$$

defined over $\mathbb{F}_q$. Let $\mathbb{K}(\mathcal{D}_{m,n}) = \mathbb{K}(x, y)$ be the function field of $\mathcal{D}_{m,n}$, with $y^m + x^n + x = 0$. It is well known that the set B , given in (??), is a basis for the vector space of holomorphic differentials of $\mathcal{D}_{m,n}$ (??, Proposition 2)¹. Thus, as in Theorem ??, an analogous proof gives the following result.

Theorem 3.1.3. *Let p be a prime, and let $m, n-1$ be positive integers coprime to p . The Hasse-Witt invariant of the curve*

$$\mathcal{D}_{m,n} : Y^m + X^n + X = 0,$$

is given by the cardinality of set

$$T = \left\{ (i, j) \in I : \binom{\frac{(m-j-1)(q-1)}{m}}{\frac{(mi+j+1)(q-1)}{m(n-1)}} \not\equiv 0 \pmod{p} \right\}, \quad (3.7)$$

where $q = p^h$, and h is the order of p in $(\mathbb{Z}/m(n-1)\mathbb{Z})^\times$.

3.2 The Hasse-Witt invariant of $Y^m + X^{p^h-1} + 1 = 0$

We have seen in Theorem ?? that the Hasse-Witt invariant of $\mathcal{F}_{m,n}$ is given in terms of certain binomial coefficients. In this section, we use Lucas' theorem (see (??) or (??, Theorem 1)) to investigate the behavior of these binomial coefficients, in order to compute closed formulas of the Hasse-Witt invariant of $\mathcal{F}_{m,n}$ for special values of m and n . The following table summarizes the cases we worked out.

¹ Towse proved this result for curves $\mathcal{D}_{m,n}$ defined over $\mathbb{C}$, with m coprime to n , but one we can check that this result is also true in this case.

q	m	n	$\gamma(\mathcal{F}_{m,n})$	
p^h	$m \mid p-1$	$q-1$	$\sum_{j=1}^{m-1} \left(\frac{j(p-1)}{m} + 1 \right)^h - 2(m-1)$	Theorem ??
p^h	$q-1$	q^l-1	$\left(\sum_{r=1}^p r^l \right)^h - q^l - 2q + 3$	Corollary ??
p^h	$q-1$	$q-1$	$q \left(\frac{p+1}{2} \right)^h - 3(q-1)$	Corollary ??
p^h	$q+1$	$q^{2l}-1$	$\left(\sum_{r=1}^p r^l (p-r+1)^l \right)^h - 2q$	Corollary ??
p^h	$\frac{q-1}{2}$	$q-1$	$(q+1) \left(\frac{1}{2} \left(\frac{p+1}{2} \right)^h - 2 \right) + 4$	Corollary ??

Table 1 – The Hasse-Witt invariant of $\mathcal{F}_{m,n}$, for special values of m and n

Theorem 3.2.1 ((?) (Lucas' Theorem)). *Let p be a prime, and let $a_0, b_0, \dots, a_r, b_r \in \{0, 1, \dots, p-1\}$. Then*

$$\binom{a_r p^r + \dots + a_1 p + a_0}{b_r p^r + \dots + b_1 p + b_0} \equiv \prod_{i=0}^r \binom{a_i}{b_i} \pmod{p}.$$

As a consequence of Theorems ?? and ??, we have the following result.

Theorem 3.2.2. *Let m and h be positive integers such that m divides $p^h - 1$. The Hasse-Witt invariant of the curve $\mathcal{F}_{m,p^h-1} : Y^m + X^{p^h-1} + 1 = 0$ is*

$$\gamma = \sum_{j=1}^{m-1} \left(\prod_{r=1}^h (a_{j,r} + 1) \right) - 2(m-1). \quad (3.8)$$

where $\frac{j(p^h-1)}{m} = a_{j,1}p^{h-1} + \dots + a_{j,h-1}p + a_{j,h}$, with $a_{j,i} \in \{0, \dots, p-1\}$ for all $1 \leq j \leq m-1$ and $1 \leq r \leq h$. In particular, if m divides $p-1$ then

$$\gamma = \sum_{j=1}^{m-1} \left(\frac{j(p-1)}{m} + 1 \right)^h - 2(m-1). \quad (3.9)$$

Proof. Let $u = \frac{p^h-1}{m}$. It follows from Theorem ?? that the Hasse-Witt invariant of $\mathcal{F}_{m,p^h-1}$ is the cardinality of the set

$$\left\{ (i, j) \in I : \binom{u(m-j-1)}{i+1} \not\equiv 0 \pmod{p} \right\}.$$

Since $mu = n = p^h - 1$, we have $(i, j) \in I = \{(i, j) \in \mathbb{N}^2 : im + jn \leq nm - n - m - \gcd(n, m)\}$ if and only if $i + ju \leq u(m-1) - 2$. This means that $0 \leq i \leq u(m-1) - 2$, and that the number $u(m-j-1)$ can vary between $i+2$ and $u(m-1)$. Moreover the number $\binom{u(m-j-1)}{i+1}$ is not zero modulo p , with $0 \leq i \leq u(m-1) - 2$ and $i+2 \leq u(m-j-1) \leq u(m-1)$, if and only if $\binom{u(j)}{i}$

is not zero modulo p , with $1 \leq i \leq u(m-1) - 1$ and $i+1 \leq uj \leq u(m-1)$. Consequently the Hasse-Witt invariant of $\mathcal{F}_{m,p^h-1}$ is the cardinality of the set

$$\left\{ (i, j) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq i \leq u(m-1) - 1 \\ i+1 \leq uj \leq u(m-1) \end{array} \text{ and } \binom{uj}{i} \not\equiv 0 \pmod{p} \right\},$$

that is, the cardinality of the set

$$\left\{ (i, j) \in \mathbb{N}^2 : 1 \leq i < uj \leq u(m-1) \text{ and } \binom{uj}{i} \not\equiv 0 \pmod{p} \right\} = \bigcup_{j=1}^{m-1} T_j \quad (3.10)$$

where

$$T_j = \left\{ (i, j) \in \mathbb{N}^2 : 1 \leq i \leq uj - 1 \text{ and } \binom{uj}{i} \not\equiv 0 \pmod{p} \right\}, \text{ for all } 1 \leq j \leq m-1.$$

Now, let us fix $uj = a_{j,1}p^{h-1} + \dots + a_{j,h-1}p + a_{j,h}$, with $a_{j,r} \in \{0, \dots, p-1\}$ for all $1 \leq j \leq m-1$ and $0 \leq r \leq h$. By Lucas' Theorem, for each $j \in \{1, \dots, m-1\}$, the integers $i \in \{1, \dots, uj-1\}$ for which $\binom{uj}{i} \not\equiv 0 \pmod{p}$ are given by

$$i = b_1p^{h-1} + \dots + b_{h-1}p + b_h$$

where $b_r \in \{0, \dots, a_{j,r}\}$ for all $1 \leq r \leq h$. Clearly, there exist $\prod_{r=1}^h (a_{j,r} + 1) - 2$ such integers, since $(0, j), (uj, j) \notin T_j$. Since $T_j \cap T_l = \emptyset$, for $j \neq l$, we have

$$\gamma = \sum_{j=1}^{m-1} \left(\prod_{r=1}^h (a_{j,r} + 1) \right) - 2(m-1).$$

In particular, note that if m divides $p-1$ then $a_{j,r} = j(p-1)/m$, for all $r \in \{1, \dots, h\}$. Thus, the equation (??) follows immediately from equation (??). $\square$

Now, we will use the previous theorem to compute closed formulas for the Hasse-Witt invariant of $\mathcal{F}_{m,p^h-1}$ in some cases.

Corollary 3.2.3. *Let t and l be positive integers. If $q = p^t$, then the Hasse-Witt invariant of the curve $\mathcal{F}_{q-1,q^l-1} : Y^{q-1} + X^{q^l-1} + 1 = 0$ is*

$$\gamma = \left(\sum_{r=1}^p r^l \right)^t - q^l - 2q + 3.$$

In particular, if $l = 1$ then

$$\gamma = q \left(\frac{p+1}{2} \right)^t - 3(q-1).$$

Proof. Let $m = p^t - 1$, $u = (p^{lt} - 1)/(p^t - 1)$ and $j = a_1p^{t-1} + \dots + a_{t-1}p + a_t$ with $a_1, \dots, a_t \in \{0, \dots, p-1\}$. Note that if $ju = a_{j,1}p^{lt-1} + \dots + a_{j,lt-1}p + a_{j,lt}$, with $a_{j,r} \in \{0, \dots, p-1\}$, then $a_{j,it+r} = a_r$, for all $i \in \{0, \dots, l-1\}$ and $r \in \{1, \dots, t\}$, as

$$ju = \sum_{i=0}^{l-1} (a_1p^{(i+1)t-1} + \dots + a_{t-1}p^{it+1} + a_t p^{it}).$$

It follows from Theorem ?? and Lemma ?? that

$$\begin{aligned}
\gamma &= \sum_{j=1}^{p^t-2} \left(\prod_{r=1}^{lt} (a_{j,r} + 1) \right) - 2(p^t - 2) \\
&= \sum_{j=0}^{p^t-1} \left(\prod_{r=1}^t (a_r + 1) \right)^l - 2(p^t - 2) - (p^{tl} + 1) \\
&= \sum_{a_1, \dots, a_t=1}^p (a_1 \cdots a_t)^l - p^{tl} - 2p^t + 3 \\
&= \left(\sum_{r=1}^p r^l \right)^t - p^{tl} - 2p^t + 3.
\end{aligned}$$

□

Note that if $l = 1$ in the previous corollary, then $\mathcal{F}_{p^t-1, p^t-1}$ is the Fermat curve. Its Hasse-Witt invariant was computed by Bassa and Beelen in (??, Theorem 19), and clearly the Corollary ?? extends their result.

Corollary 3.2.4. *Let t, n be positive integers and $q = p^t$. The Hasse-Witt invariant of the curve $\mathcal{F}_{q+1, q^{2n}-1} : Y^{q+1} + X^{q^{2n}-1} + 1 = 0$ is*

$$\gamma = \left(\sum_{r=1}^p r^n (p - r + 1)^n \right)^t - 2q.$$

Proof. Let $m = p^t + 1$, $u = (q^{2n} - 1)/(q + 1)$ and $v = (q^{2n} - 1)/(q^2 - 1)$. Note that $j \in \{1, \dots, p^t\}$ if and only if $j = a_{t-l-1}p^{t-1} + \dots + a_1p^{l+1} + a_0p^l$, where $l \in \{0, \dots, t-2\}$ and $a_0, \dots, a_{t-l-1} \in \{0, \dots, p-1\}$ with $a_0 \neq 0$, for $t \geq 2$, or $j = a_{t-1}p^{t-1}$, where $a_{t-1} \in \{1, \dots, p\}$, for $t \geq 1$.

Firstly, suppose that $t \geq 2$. For each $j = a_{t-l-1}p^{t-1} + \dots + a_1p^{l+1} + a_0p^l$, where $l \in \{0, \dots, t-2\}$ and $a_0, \dots, a_{t-l-1} \in \{0, \dots, p-1\}$, with $a_0 \neq 0$, we have

$$\begin{aligned}
ju &= p^l v(p^t - 1) \left(\sum_{i=0}^{t-l-1} a_i p^i \right) \\
&= p^l v \left(\sum_{i=1}^{t-l-1} a_i p^{t+i} + (a_0 - 1)p^t + \sum_{i=t-l}^{t-1} (p-1)p^i + \sum_{i=1}^{t-l-1} (p - a_i - 1)p^i + (p - a_0) \right) \\
&= p^l \sum_{r=0}^{n-1} p^{2rt} \left(\sum_{i=1}^{t-l-1} a_i p^{t+i} + (a_0 - 1)p^t + \sum_{i=t-l}^{t-1} (p-1)p^i + \sum_{i=1}^{t-l-1} (p - a_i - 1)p^i + (p - a_0) \right).
\end{aligned}$$

Now, suppose that $t \geq 1$. For each $j = a_{t-1}p^{t-1}$, with $a_{t-1} \in \{1, \dots, p\}$, we have

$$\begin{aligned}
ju &= p^{t-1} v(p^t - 1) a_{t-1} = p^{t-1} v \left((a_{t-1} - 1)p^t + \sum_{i=1}^{t-1} (p-1)p^i + (p - a_{t-1}) \right) \\
&= p^{t-1} \sum_{r=0}^{n-1} p^{2rt} \left((a_{t-1} - 1)p^t + \sum_{i=1}^{t-1} (p-1)p^i + (p - a_{t-1}) \right).
\end{aligned}$$

It follows from Theorem ?? and Lemma ?? that

$$\begin{aligned}\gamma &= \sum_{l=0}^{t-2} p^{nl} \left(\sum_{a_1, \dots, a_{t-l-1}=0}^{p-1} \sum_{a_0=1}^{p-1} a_0^n (p - a_0 + 1)^n \prod_{i=1}^{t-l-1} (a_i + 1)^n (p - a_i)^n \right) \\ &\quad + p^{n(t-1)} \left(\sum_{a_{t-1}=1}^p a_{t-1}^n (p - a_{t-1} + 1)^n \right) - 2p^t \\ &= \left(\sum_{r=1}^p r^n (p - r + 1)^n \right)^t - 2p^t.\end{aligned}$$

□

Lemma 3.2.5. *Let h be a positive integer and consider the following sets*

$$\begin{aligned}S^h &= \left\{ (i, j) : 0 \leq i \leq j \leq p^h - 1 \text{ and } \binom{j}{i} \not\equiv 0 \pmod{p}, \text{ with } j \text{ even} \right\} \\ R^h &= \left\{ (i, j) : 0 \leq i \leq j \leq p^h - 1 \text{ and } \binom{j}{i} \not\equiv 0 \pmod{p}, \text{ with } j \text{ odd} \right\}.\end{aligned}$$

We have

$$\#S^h = \frac{(p^h + 1)(p + 1)^h}{2^{h+1}} \text{ and } \#R^h = \frac{(p^h - 1)(p + 1)^h}{2^{h+1}}.$$

Proof. By induction on h . First suppose $h = 1$ and note that if $k_1 \in \{0, \dots, (p-1)/2\}$, and $k_2 \in \{0, \dots, (p-1)/2 - 1\}$, then $2k_1, 2k_2 + 1 \in \{0, \dots, p-1\}$. By Lucas' Theorem, the integers $0 \leq i \leq 2k_1$ are such that $\binom{2k_1}{i} \not\equiv 0 \pmod{p}$. Analogously, the integers $0 \leq i \leq 2k_2 + 1$ are such that $\binom{2k_2+1}{i} \not\equiv 0 \pmod{p}$. Therefore,

$$\#S^1 = \sum_{k_1=0}^{\frac{p-1}{2}} (2k_1 + 1) = \frac{(p+1)(p+1)}{2^2} \text{ and } \#R^1 = \sum_{k_2=0}^{\frac{p-1}{2}-1} (2k_2 + 2) = \frac{(p-1)(p+1)}{2^2}.$$

Now, let $h \geq 2$ and suppose that the result is true for $h-1$. Let $j = a_{h-1}p^{h-1} + b$, where $b = a_{h-2}p^{h-2} + \dots + a_1p + a_0$. Note that j is even if and only if a_{h-1} and b are both even or both odd. Thus

$$\#S^h = \frac{(p+1)(p+1)}{2^2} \frac{(p^{h-1}+1)(p+1)^{h-1}}{2^h} + \frac{(p-1)(p+1)}{2^2} \frac{(p^{h-1}-1)(p+1)^{h-1}}{2^h} = \frac{(p^h+1)(p+1)^h}{2^{h+1}}.$$

Moreover, j is odd if and only if a_{h-1} is even and b is odd or a_{h-1} is odd and b is even. Thus

$$\#R^h = \frac{(p+1)(p+1)}{2^2} \frac{(p^{h-1}-1)(p+1)^{h-1}}{2^h} + \frac{(p-1)(p+1)}{2^2} \frac{(p^{h-1}+1)(p+1)^{h-1}}{2^h} = \frac{(p^h-1)(p+1)^h}{2^{h+1}}.$$

□

Corollary 3.2.6. *If h is a positive integer, then the Hasse-Witt invariant of the curve*

$\mathcal{F}_{(p^h-1)/2, p^h-1} : Y^{(p^h-1)/2} + X^{p^h-1} + 1 = 0$ *is*

$$\gamma = (p^h + 1) \left(\frac{1}{2} \left(\frac{p+1}{2} \right)^h - 2 \right) + 4.$$

Proof. It follows from (??) that

$$\gamma = \# \left\{ (i, j) \in \mathbb{N}^2 : 1 \leq i < 2j \leq p^h - 3 \text{ and } \binom{2j}{i} \not\equiv 0 \pmod{p} \right\}.$$

Let S^h be as in the previous lemma. Note that it is enough to compute the cardinality of S^h and then remove the number corresponding to (i, j) in S^h occurring in the cases $j = p^h - 1$ and $j = 0$. Moreover, for each of the $(p^h + 1)/2 - 2$ values of $j \in \{1, \dots, p^h - 2\}$, with j even, we must remove the number corresponding to (i, j) in S^h occurring in the cases $i = 0$ and $i = j$. Thus, it follows from Lemma ?? that

$$\gamma = \frac{(p^h + 1)(p + 1)^h}{2^{h+1}} - p^h - 1 - 2 \left(\frac{p^h + 1}{2} - 2 \right) = (p^h + 1) \left(\frac{1}{2} \left(\frac{p + 1}{2} \right)^h - 2 \right) + 4.$$

□

3.3 The Hasse-Witt invariant of $Y^2 = X^n + 1$

Throughout this section p is an odd prime. Let $n \geq 5$ be an integer coprime to p . Consider the hyperelliptic curve

$$\mathcal{C}_n : Y^2 = X^n + 1,$$

defined over $\mathbb{F}_q$, where q is a power of p . It follows from (??) and (??) that

$$\mathfrak{g}_n = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd,} \\ \frac{n-2}{2} & \text{if } n \text{ is even,} \end{cases} \quad (3.11)$$

is the genus of $\mathcal{C}_n$, and

$$B = \left\{ \omega_r = \frac{x^{r-1}}{y} dx : r = 1, \dots, \mathfrak{g}_n \right\} \quad (3.12)$$

is a basis for the vector space of holomorphic differentials on $\mathcal{C}_n$. This section illustrates how one can use Theorem ?? to provide closed formulas for the Hasse-Witt invariant of $\mathcal{C}_n$. The following tables summarizes the cases we worked out.

q	n	$\gamma(\mathcal{C}_n)$	
p^h	$q - 1$	$\left(\frac{p+1}{2} \right)^h - 2$	Corollary ??
p^h	$2(q - 1)$	$\left(\frac{p+1}{2} \right)^h - 2$	Corollary ??
p^h	$2(q + 1)$	$\left(\frac{p+1}{2} \right)^h$	Corollary ??
p^h	$q^2 + q + 1$	$\left(\frac{(p+1)(p+3)}{8} \right)^h$	Corollary ??
p^h	$2(q^2 + q + 1)$	$2 \left(\frac{(p+1)(p+3)}{8} \right)^h$	Corollary ??

Table 2 – The Hasse-Witt invariant of $\mathcal{C}_n$, for special values of n

n	hypotheses	$\gamma(\mathcal{C}_n)$	Corollary
$\frac{q-1}{2}$	$4 \mid q-1$	$\frac{1}{2} \left(\left(\frac{p+1}{2} \right)^h + u \right) - 2$	??
$\frac{q-1}{2}$	$4 \nmid q-1$	$\frac{1}{2} \left(\frac{p+1}{2} \right)^h - 1$	??
$\frac{2t(q-1)}{p+3}$	$\begin{array}{l} 2t \mid p+3 \\ (p+3) \mid 2t(q-1) \\ \frac{2t(q-1)}{p+3} \text{ odd} \end{array}$	$\frac{2t}{p+3} \left(\left(\frac{p+1}{2} \right)^h - (-1)^h \right) + (-v)^h - 1$	??
$\frac{2t(q-1)}{p+3}$	$\begin{array}{l} 2t \mid p+3 \\ (p+3) \mid 2t(q-1) \\ \frac{2t(q-1)}{p+3} \text{ even} \end{array}$	$\frac{2t}{p+3} \left(\left(\frac{p+1}{2} \right)^h - (-1)^h \right) + (-v)^h - 2$	??
$\frac{2t(q-1)}{p+1}$	$\begin{array}{l} 2t \mid p+1 \\ (p+1) \mid 2t(q-1) \\ \frac{2t(q-1)}{p+1} \text{ odd} \end{array}$	$\frac{2t}{p+1} \left(\frac{p+1}{2} \right)^h - 1$	??
$\frac{2t(q-1)}{p+1}$	$\begin{array}{l} 2t \mid p+1 \\ (p+1) \mid 2t(q-1) \\ \frac{2t(q-1)}{p+1} \text{ even} \end{array}$	$\frac{2t}{p+1} \left(\frac{p+1}{2} \right)^h - 2$	??
$\frac{2t(q-1)}{p-1}$	$2t \mid p-1$	$\frac{2t}{p-1} \left(\left(\frac{p+1}{2} \right)^h - 1 \right) - 1$	??
$\frac{(2t+1)(q-1)}{p-1}$	$\begin{array}{l} (2t+1) \mid p-1 \\ h \text{ odd} \end{array}$	$\frac{2t+1}{p-1} \left(\left(\frac{p+1}{2} \right)^h - 1 \right) - \frac{1}{2}$	??

Table 3 – The Hasse-Witt invariant of $\mathcal{C}_n$, for special values of n , with $q = p^h$

where

$$u := \begin{cases} 1 & \text{if } 4 \mid p-1, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and } v := \begin{cases} 1 & \text{if } \frac{p+3}{2t} \mid \frac{p^h-1}{p-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Firstly, note that as a consequence of Theorem ?? we have the following result.

Theorem 3.3.1. *Let p be an odd prime and n a positive integer coprime to p . Then the Hasse-Witt invariant of the curve $\mathcal{C}_n : Y^2 = X^n + 1$ is given by the cardinality of the set*

$$T = \left\{ r \in \{1, \dots, \mathfrak{g}_n\} : \left(\frac{\frac{q-1}{2}}{\frac{r(q-1)}{n}} \right) \not\equiv 0 \pmod{p} \right\}$$

where $q = p^h$ and h is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Corollary 3.3.2. *If r is a positive integer and $\gamma(\mathcal{C}_n)$ is the Hasse-Witt invariant of the curve $\mathcal{C}_n : Y^2 = X^n + 1$, then*

$$i) \quad \gamma(\mathcal{C}_{p^r-1}) = \left(\frac{p+1}{2} \right)^r - 2.$$

$$ii) \quad \gamma(\mathcal{C}_{2(p^r+1)}) = \left(\frac{p+1}{2} \right)^r.$$

$$iii) \quad \gamma(\mathcal{C}_{p^{2r+p^r+1}}) = \left(\frac{(p+1)(p+3)}{8} \right)^r.$$

Proof. i) This result is a consequence of Theorem ??.

ii) It follows from Theorem ?? and Lucas's Theorem that it suffices to count the values

$$u = a_1 p^{2r-1} + \cdots + a_{r-1} p^{r+1} + a_r p^r + b_1 p^{r-1} + \cdots + b_{r-1} p + b_r \geq 1$$

with $a_i, b_i \in \{0, \dots, \frac{p-1}{2}\}$, for all $1 \leq i \leq r$, such that $(p^r - 1)/2$ divides u . Note that $u \equiv (a_1 + b_1)p^{r-1} + \cdots + (a_{r-1} + b_{r-1})p + (a_r + b_r) \pmod{(p^r - 1)/2}$. If $(p^r - 1)/2$ divides $(a_1 + b_1)p^{r-1} + \cdots + (a_{r-1} + b_{r-1})p + (a_r + b_r)$, since it is a number between 0 and $p^r - 1$, we have

$$(a_1 + b_1)p^{r-1} + \cdots + (a_{r-1} + b_{r-1})p + (a_r + b_r) \in \left\{ \frac{p^r - 1}{2}, p^r - 1 \right\}$$

and consequently $b_i = \frac{p-1}{2} - a_i$, for all $1 \leq i \leq r$. Therefore, it suffices to count the values $a_i \in \{0, \dots, \frac{p-1}{2}\}$, for all $1 \leq i \leq r$.

iii) It follows from Theorem ?? and Lucas's Theorem that it suffices to count the values

$$u = a_1 p^{3r-1} + \cdots + a_r p^{2r} + b_1 p^{2r-1} + \cdots + b_r p^r + c_1 p^{r-1} + \cdots + c_r \geq 1$$

with $a_i, b_i, c_i \in \{0, \dots, \frac{p-1}{2}\}$, for all $1 \leq i \leq r$, such that $p^r - 1$ divides u . Observe that

$$u \equiv (a_1 + b_1 + c_1)p^{r-1} + \cdots + (a_{r-1} + b_{r-1} + c_{r-1})p + (a_r + b_r + c_r) \pmod{p^r - 1}.$$

If $p^r - 1$ divides $(a_1 + b_1 + c_1)p^{r-1} + \cdots + (a_{r-1} + b_{r-1} + c_{r-1})p + (a_r + b_r + c_r)$, since it is a number between 0 and $3(p^r - 1)/2$, we have

$$(a_1 + b_1 + c_1)p^{r-1} + \cdots + (a_{r-1} + b_{r-1} + c_{r-1})p + (a_r + b_r + c_r) = p^r - 1$$

and consequently $c_i = (p - 1) - (a_i + b_i)$, for all $1 \leq i \leq r$. Therefore, it suffices to count the values $a_i, b_i \in \{0, \dots, \frac{p-1}{2}\}$ such that $a_i + b_i \geq (p - 1)/2$, for all $1 \leq i \leq r$. Now, note that for each $a_i \in \{0, \dots, \frac{p-1}{2}\}$ there exist $(a_i + 1)$ values for $b_i \in \{0, \dots, \frac{p-1}{2}\}$ such that $a_i + b_i \geq (p - 1)/2$. Therefore

$$\gamma(\mathcal{C}_{p^{2r+p^r+1}}) = \left(\sum_{a_i=0}^{\frac{p-1}{2}} (a_i + 1) \right)^r = \left(\frac{(p+1)(p+3)}{8} \right)^r.$$

□

Let p be an odd prime, $n \geq 5$ be an integer, h be the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$ and $m = \frac{p^h - 1}{n}$. By Theorem ?? and Lucas' Theorem ??, to compute the Hasse-Witt invariant of $\mathcal{C}_n$, it is enough to count the values of

$$u = x_1 + x_2 p + \cdots + x_h p^{h-1},$$

with $x_i \in \{0, \dots, \frac{p-1}{2}\}$, for all $1 \leq i \leq h$, such that m divides u . More generally, if $\frac{p-1}{2} = mt + s$ with t, s positive integers, such that $0 \leq s \leq m-1$, then it is enough to count the number of solutions to

$$a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv 0 \pmod{m}$$

where $1 \leq a_i \leq m-1$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ and $x_i \in \{0, \dots, \frac{p-1}{2}\}$, with $1 \leq i \leq h$. Thus, we have the following lemma.

Lemma 3.3.3. *Let h, m and t be positive integers, and let $a_1, \dots, a_h \in \{1, \dots, m-1\}$ be such that a_i are units in $\mathbb{Z}/m\mathbb{Z}$. Then the number N of solutions to*

$$a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv 0 \pmod{m}$$

with $s \in \{0, \dots, m-1\}$ and $0 \leq x_i \leq tm + s$, is given by

$$N = \frac{(tm + s + 1)^h - (s + 1)^h}{m} + \delta$$

for some suitable number $\delta \geq 0$.

Proof. Let $N_{h,a}$ be the number of solutions to $a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv a \pmod{m}$ with $0 \leq x_i \leq tm + s$ and $a \in \{0, \dots, m-1\}$. We want to proof that

$$N_{h,a} = \frac{(tm + s + 1)^h - (s + 1)^h}{m} + \delta(a, h)$$

for some suitable number $\delta(a, h)$. By induction on h , first suppose $h = 1$. In this case

$$N_{1,a} = \begin{cases} \frac{(tm + s + 1) - (s + 1)}{m} + 1 & \text{if } b \leq s, \\ \frac{(tm + s + 1) - (s + 1)}{m} & \text{if } b > s, \end{cases}$$

is the number of solutions to $x_1 \equiv b \pmod{m}$, where $b = a_1^{-1}a \in \mathbb{Z}/m\mathbb{Z}$ and $0 \leq x_1 \leq tm + s$. Now, let $h \geq 2$ and suppose that the result is true for $h-1$. For each $j \in \{0, \dots, tm + s\}$, let $N_{h,a}^j$ be the number of solutions to

$$a_1j + a_2x_2 + \dots + a_hx_h \equiv a \pmod{m},$$

with $0 \leq x_i \leq tm + s$. In this case, $N_{h,a}^j$ is the number of solutions to $j + b_2x_2 + \dots + b_hx_h \equiv b \pmod{m}$, where $0 \leq x_i \leq tm + s$ with $b = a_1^{-1}a \in \mathbb{Z}/m\mathbb{Z}$ and $b_i = a_1^{-1}a_i \in \mathbb{Z}/m\mathbb{Z}$, for all $2 \leq i \leq h$. Note that $\sum_{j=0}^{tm-1} N_{h,a}^j = (tm + s + 1)^{h-1}$. Moreover, for each $j \in \{0, \dots, s\}$ we have $N_{h,a}^{tm+j} = N_{h-1,c_j}$, where $c_j \equiv a - j \pmod{m}$ and $c_j \in \{0, \dots, m-1\}$. By induction hypothesis, we have

$$\begin{aligned} N_{h,a} &= t(tm + s + 1)^{h-1} + \sum_{j=0}^s N_{h,a}^{tm+j} \\ &= \frac{(tm + s + 1)^h - (s + 1)^h}{m} + \sum_{j=0}^s \delta(c_j, h-1) \\ &= \frac{(tm + s + 1)^h - (s + 1)^h}{m} + \delta(a, h), \end{aligned}$$

where $\delta(a, h) = \sum_{j=0}^s \delta(c_j, h-1)$. □

Using induction as in Lemma ??, we obtain the following result.

Proposition 3.3.4. *Let h, m and t be positive integers, and let $a_1, \dots, a_h \in \{1, \dots, m-1\}$ be such that a_i are units in $\mathbb{Z}/m\mathbb{Z}$. Let N be the number of solutions to*

$$a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv a \pmod{m}$$

where $a \in \{0, \dots, m-1\}$ and $x_i \in \{0, \dots, tm+s\}$.

1. if $s = -2$, then

$$N = \begin{cases} \frac{(tm-1)^h - (-1)^h}{m} & \text{if } a_1^{-1}(a + a_2 + \dots + a_h) \not\equiv -1 \pmod{m}, \\ \frac{(tm-1)^h - (-1)^h}{m} + (-1)^h & \text{if } a_1^{-1}(a + a_2 + \dots + a_h) \equiv -1 \pmod{m}. \end{cases}$$

2. If $s = -1$, then $N = t^h m^{h-1}$;

$$3. \text{ If } s = 0, \text{ then } N = \begin{cases} \frac{(tm+1)^h - 1}{m} + 1 & \text{if } a = 0, \\ \frac{(tm+1)^h - 1}{m} & \text{if } a \neq 0. \end{cases}$$

Proposition 3.3.5. *Let h, m and t be positive integers, and let $a_1, \dots, a_h \in \{1, \dots, m-1\}$ be such that a_i are units in $\mathbb{Z}/m\mathbb{Z}$. If h is odd and m is even, then the number of solutions to $a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv 0 \pmod{m}$, where $0 \leq x_i \leq tm + \frac{m}{2}$, is*

$$N = \frac{(tm + \frac{m}{2} + 1)^h - 1}{m} + \frac{1}{2}.$$

Proof. Let $n = \frac{m}{2}$ and M be the number of solutions to $a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv n \pmod{2n}$, with $0 \leq x_i \leq (2t+1)n$. Note that $N = M$, indeed $(x_1, \dots, x_h)$ is a solution to $a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv 0 \pmod{2n}$, with $0 \leq x_i \leq (2t+1)n$, if and only if $(n - x_1, \dots, n - x_h)$ is a solution to $a_1x_1 + a_2x_2 + \dots + a_hx_h \equiv n \pmod{2n}$, with $0 \leq x_i \leq (2t+1)n$. Finally, note that $N + M$ is the number of solutions to $a_1x_1 + \dots + a_hx_h \equiv 0 \pmod{n}$, with $0 \leq x_i \leq (2t+1)n$. It follows from Proposition ?? that $2N = N + M = \frac{((2t+1)n+1)^h - 1}{n} + 1 = \frac{(tm + \frac{m}{2} + 1)^h - 1}{\frac{m}{2}} + 1$. $\square$

Now, as a consequence of Lucas' Theorem ??, we are able to compute the Hasse-Witt invariant of the curve $\mathcal{C}_n : Y^2 = X^n + 1$ in terms of number of solutions to $x_1 + x_2p + \dots + x_hp^{h-1} \equiv 0 \pmod{m}$, with $x_i \in \{0, \dots, \frac{p-1}{2}\}$, for $1 \leq i \leq h$. More precisely, we have the following theorem.

Theorem 3.3.6. *Let p be an odd prime, $n \geq 5$ be an integer, h be the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$ and $m = \frac{p^h - 1}{n}$. The Hasse-Witt invariant of the curve $\mathcal{C}_n : Y^2 = X^n + 1$ is*

$$\gamma_n = \begin{cases} N - 1 & \text{if } n \text{ is odd,} \\ N - 2 & \text{if } n \text{ is even,} \end{cases}$$

where N is the number of solutions to $x_1 + x_2p + \cdots + x_hp^{h-1} \equiv 0 \pmod{m}$, with $x_i \in \{0, \dots, \frac{p-1}{2}\}$, for $1 \leq i \leq h$.

Proof. By Theorem ??, the Hasse-Witt invariant of $\mathcal{C}_n$ is the cardinality of

$$T = \left\{ rm \in \{m, \dots, m\mathfrak{g}_n\} : \binom{\frac{p^h-1}{2}}{rm} \not\equiv 0 \pmod{p} \right\},$$

and by Lucas's Theorem the cardinality N of

$$\left\{ rm \in \left\{0, \dots, \frac{p^h-1}{2}\right\} : \binom{\frac{p^h-1}{2}}{rm} \not\equiv 0 \pmod{p} \right\}$$

is the number of solutions to

$$x_1 + x_2p + \cdots + x_hp^{h-1} \equiv 0 \pmod{m} \quad (3.13)$$

with $x_i \in \{0, \dots, \frac{p-1}{2}\}$, for $1 \leq i \leq h$. Now, note that $(0, \dots, 0)$ is a solution to (??). Moreover, if n is odd, then the equation (??) has no solutions $(x_1, \dots, x_n)$ with $x_1 + x_2p + \cdots + x_hp^{h-1} > m\mathfrak{g}_n$, otherwise we have $x_1 + x_2p + \cdots + x_hp^{h-1} \geq (p^h - 1 + m)/2 > (p^h - 1)/2$, as $m\mathfrak{g}_n = (p^h - 1 - m)/2$, which is a contradiction. Therefore, $\gamma_n = N - 1$. Now, if n is even, then m divides $(p^h - 1)/2$ and consequently $(\frac{p-1}{2}, \dots, \frac{p-1}{2})$ is the unique solution to (??) with $x_1 + x_2p + \cdots + x_hp^{h-1} > m\mathfrak{g}_n$, as $m\mathfrak{g}_n = (p^h - 1)/2 - m$. Therefore, $\gamma_n = N - 2$. $\square$

Now, using Propositions ??, ?? and Theorem ??, we are able to compute the Hasse-Witt invariant of $\mathcal{C}_n$ in the following cases:

Corollary 3.3.7. *If h is a positive integer, then the Hasse-Witt invariant of the curve $\mathcal{C} : Y^2 = X^{(p^h-1)/2} + 1$ is given by*

$$\gamma = \begin{cases} \frac{1}{2} \left(\left(\frac{p+1}{2} \right)^h + u \right) - 2 & \text{if } 4 \mid p^h - 1, \\ \frac{1}{2} \left(\frac{p+1}{2} \right)^h - 1 & \text{if } 4 \nmid p^h - 1, \end{cases}$$

where $u = 1$, when 4 divides $p - 1$, otherwise $u = 0$.

Proof. If $n = (p^h - 1)/2$, then h is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $m := (p^h - 1)/n = 2$. If 4 does not divide $p - 1$ (resp. 4 divides $p - 1$) then $(p - 1)/2 = 2t - 1$ (resp. $(p - 1)/2 = 2t$). Thus, by Proposition ?? and Theorem ??, we have

$$\gamma = \begin{cases} \frac{1}{2} \left(\left(\frac{p+1}{2} \right)^h + u \right) - 2 & \text{if } 4 \mid p^h - 1, \\ \frac{1}{2} \left(\frac{p+1}{2} \right)^h - 1 & \text{if } 4 \nmid p^h - 1. \end{cases}$$

$\square$

Corollary 3.3.8. *Let t and h be positive integers. If t is an even divisor of $p+3$, and $p+3$ divides $t(p^h-1)$, then the Hasse-Witt invariant of the curve $Y^2 = X^{t(p^h-1)/(p+3)} + 1$ is given by*

$$\gamma = \begin{cases} \frac{t}{p+3} \left(\left(\frac{p+1}{2} \right)^h - (-1)^h \right) + (-u)^h - 1 & \text{if } \frac{t(p^h-1)}{p+3} \text{ is odd,} \\ \frac{t}{p+3} \left(\left(\frac{p+1}{2} \right)^h - (-1)^h \right) + (-u)^h - 2 & \text{if } \frac{t(p^h-1)}{p+3} \text{ is even,} \end{cases}$$

where $u = 1$, when $\frac{p+3}{t}$ divides $\frac{p^h-1}{p-1}$, otherwise $u = 0$.

Proof. If $n = t(p^h-1)/(p+3)$, then h is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $m := (p^h-1)/n = (p+3)/t$. Since $(p-1)/2 = (mt/2) - 2$, by Proposition ?? and Theorem ??, we have the result. $\square$

Corollary 3.3.9. *Let t and h be positive integers. If t is an even divisor of $p+1$, and $p+1$ divides $t(p^h-1)$, then the Hasse-Witt invariant of the curve $Y^2 = X^{t(p^h-1)/(p+1)} + 1$ is given by*

$$\gamma = \begin{cases} \frac{t}{p+1} \left(\left(\frac{p+1}{2} \right)^h - 1 \right) & \text{if } \frac{t(p^h-1)}{p+1} \text{ is odd,} \\ \frac{t}{p+1} \left(\left(\frac{p+1}{2} \right)^h - 2 \right) & \text{if } \frac{t(p^h-1)}{p+1} \text{ is even.} \end{cases}$$

Proof. If $n = t(p^h-1)/(p+1)$, then h is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $m := (p^h-1)/n = (p+1)/t$. Since $(p-1)/2 = (mt/2) - 1$, by Proposition ?? and Theorem ??, we have the result. $\square$

Corollary 3.3.10. *Let t and h be positive integers. If t is an even divisor of $p-1$, then the Hasse-Witt invariant of the curve $Y^2 = X^{t(p^h-1)/(p-1)} + 1$ is given by*

$$\gamma = \frac{t}{p-1} \left(\left(\frac{p+1}{2} \right)^h - 1 \right) - 1.$$

Proof. If $n = t(p^h-1)/(p-1)$, then h is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $m := (p^h-1)/n = (p-1)/t$. Since $(p-1)/2 = mt/2$, by Proposition ?? and Theorem ??, we have the result. $\square$

Corollary 3.3.11. *Let t and h be positive integers. If t is an odd divisor of $p-1$, and h is an odd number, then the Hasse-Witt invariant of the curve $\mathcal{C} : Y^2 = X^{t(p^h-1)/(p-1)} + 1$ is given by*

$$\gamma = \frac{t}{p-1} \left(\left(\frac{p+1}{2} \right)^h - 1 \right) - \frac{1}{2}.$$

Proof. Let $t = 2r+1$. If $n = (2r+1)(p^h-1)/(p-1)$, then h is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. Let $m := (p^h-1)/n = (p-1)/(2r+1)$. Since $(p-1)/2 = mr + m/2$, by Proposition ?? and Theorem ??, we have the result. $\square$

3.4 The Hasse-Witt invariant of $Y^2 = X^n + X$

Throughout this section p is an odd prime. Let $n \geq 5$ be an integer, with $n - 1$ coprime to p . Consider the hyperelliptic curve

$$\mathcal{D}_n : Y^2 = X^n + X,$$

defined over $\mathbb{F}_q$, where q is a power of p . This section illustrates how one can use Theorem ?? to provide closed formulas for the Hasse-Witt invariant of $\mathcal{D}_n$. The following table summarizes the cases we worked out.

n	hypotheses	$\gamma(\mathcal{D}_n)$	Corollary
$q + 2$		$\left(\frac{p+1}{2}\right)^h$	??
$\frac{q+1}{2}$	$4 \mid q + 1$	$\frac{1}{2} \left(\left(\frac{p+1}{2}\right)^h - u \right)$	??
$\frac{q+1}{2}$	$4 \nmid q + 1$	$\frac{1}{2} \left(\frac{p+1}{2}\right)^h - 1$	??
$\frac{2t(q-1)}{p+3} + 1$	$4t \mid p + 3$ $(p+3) \mid 2t(q-1)$ $\frac{2t(q-1)}{p+3}$ even	$\frac{1}{2} \left(\left(\frac{p+1}{2}\right)^h - (-1)^h \right) + (-u)^h$	??
$\frac{2t(q-1)}{p+3} + 1$	$4t \mid p + 3$ $(p+3) \mid 2t(q-1)$ $\frac{2t(q-1)}{p+3}$ odd	$\frac{1}{2} \left(\left(\frac{p+1}{2}\right)^h - (-1)^h \right) + (-u)^h - 1$	??
$\frac{2t(q-1)}{p+1} + 1$	$4t \mid p + 1$ $(p+1) \mid 2t(q-1)$ $\frac{2t(q-1)}{p+1}$ even	$\frac{1}{2} \left(\frac{p+1}{2}\right)^h$	??
$\frac{2t(q-1)}{p+1} + 1$	$4t \mid p + 1$ $(p+1) \mid 2t(q-1)$ $\frac{2t(q-1)}{p+1}$ odd	$\frac{1}{2} \left(\frac{p+1}{2}\right)^h - 1$	??
$\frac{2t(q-1)}{p-1} + 1$	$4t \mid p - 1$	$\frac{2t}{p-1} \left(\left(\frac{p+1}{2}\right)^h - 1 \right)$	??
$\frac{(2t+1)(q-1)}{p-1} + 1$	$(2t+1) \mid p - 1$ h odd	$\frac{2t+1}{p-1} \left(\left(\frac{p+1}{2}\right)^h - 1 \right) - \frac{1}{2}$	??

Table 4 – The Hasse-Witt invariant of $\mathcal{D}_n$, for special values of n , with $q = p^h$

where

$$u := \begin{cases} 1 & \text{if } 4 \mid p - 1, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and } v := \begin{cases} 1 & \text{if } \frac{p+3}{4t} \mid \frac{q-1}{p-1} \text{ and } \frac{p+3}{2t} \nmid \frac{q-1}{p-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Firstly, note that as a consequence of Theorem ??, we have the following result.

Theorem 3.4.1. *Let p be an odd prime, and let $n \geq 5$ be an integer, with $n - 1$ coprime to p . The Hasse-Witt invariant of the curve $\mathcal{D}_n : Y^2 = X^n + X$ is given by the cardinality of set*

$$T = \left\{ r \in \{1, \dots, \mathfrak{g}_n\} : \left(\frac{\frac{q-1}{2}}{(2r-1)(q-1)} \right) \not\equiv 0 \pmod{p} \right\},$$

where $q = p^h$ and h is the order of p in $(\mathbb{Z}/2(n-1)\mathbb{Z})^\times$.

In the next theorem we use the Kani and Rosen method (Theorem ??) to relate the Hasse-Witt invariants of the curves $\mathcal{C}_n$ and $\mathcal{D}_n$.

Theorem 3.4.2. *Let $p > 2$ be a prime, and let $u \geq 1$ be an odd integer coprime with p . For each integer $k \geq 0$, we denote by $\mathcal{F}_k$ and $\mathcal{G}_k$ the curves*

$$\mathcal{C}_{2^k u} : Y^2 = X^{2^k u} + 1 \text{ and } \mathcal{D}_{2^k u+1} : Y^2 = X^{2^k u+1} + X,$$

respectively. Then the following hold.

- (i) $\gamma(\mathcal{F}_0) = \gamma(\mathcal{G}_0)$.
- (ii) $\gamma(\mathcal{G}_{k-1}) = \gamma(\mathcal{F}_k) - \gamma(\mathcal{F}_{k-1})$, for $k \geq 1$.
- (iii) $\gamma(\mathcal{F}_1) = 2\gamma(\mathcal{F}_0)$
- (iv) $\gamma(\mathcal{F}_k) = 2\gamma(\mathcal{F}_0) + \sum_{i=1}^{k-1} \gamma(\mathcal{G}_i)$, for $k \geq 2$.

Proof. One can check that the map $(x, y) \mapsto (\frac{1}{x}, \frac{y}{x^{(u+1)/2}})$ from $\mathcal{F}_0$ to $\mathcal{G}_0$ gives $\mathcal{F}_0 \cong \mathcal{G}_0$, and the first assertion follows. For $k \geq 1$, note that $\pi : (x, y) \mapsto (-x, y)$ and $\sigma : (x, y) \mapsto (x, -y)$ are automorphisms of $\mathcal{F}_k$, and that $G = \langle \pi, \sigma \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is a subgroup of $\text{Aut}(\mathcal{F}_k)$ with

$$G = \langle \pi \rangle \cup \langle \sigma \rangle \cup \langle \pi \circ \sigma \rangle.$$

Clearly, each pairwise intersection of the three subgroup is trivial. Moreover, one can readily check that both the quotient curves $\mathcal{F}_k/G$ and $\mathcal{F}_k/\langle \sigma \rangle$ have genus zero, and that $\mathcal{F}_k/\langle \pi \rangle \cong \mathcal{F}_{k-1}$ and $\mathcal{F}_k/\langle \pi \circ \sigma \rangle \cong \mathcal{G}_{k-1}$. Thus Theorem ?? yields

$$J_{\mathcal{F}_k}^2 \sim J_{\mathcal{F}_{k-1}}^2 \times J_{\mathcal{G}_{k-1}}^2,$$

and then

$$\gamma(\mathcal{F}_k) = \gamma(\mathcal{F}_{k-1}) + \gamma(\mathcal{G}_{k-1}), \quad (3.14)$$

which proves the second assertion. In addition, (i) and (ii) clearly imply (iii). For the last assertion, note that the process can be repeated for the curve $\mathcal{F}_{k-1}$ when $k \geq 2$, and inductively equation ?? gives

$$\gamma(\mathcal{F}_k) = \gamma(\mathcal{F}_0) + \gamma(\mathcal{G}_0) + \cdots + \gamma(\mathcal{G}_{k-1}).$$

Now $\gamma(\mathcal{F}_0) = \gamma(\mathcal{G}_0)$ finishes the proof. $\square$

Now, as a consequence of Theorem ?? we can compute the Hasse-Witt invariant of the following hyperelliptic curves. From here on, $\gamma(\mathcal{C}_n)$ will always denote the Hasse-Witt invariant of the curve $\mathcal{C}_n : Y^2 = X^n + 1$. Firstly, observe that the curve $\mathcal{D}_{2g+1} : Y^2 = X^{2g+1} + X$ is $\mathbb{F}_{q^2}$ -maximal if and only if $q \equiv -1$ or $2g+1 \pmod{4g}$ (??, Theorem 1).

Corollary 3.4.3. *Let p be an odd prime, and let $t \geq 1$ be an integer. If m is an odd divisor of $p^t - 1$, then $\mathcal{C}_{\frac{p^t-1}{m}} : Y^2 = X^{\frac{p^t-1}{m}} + 1$ and $\mathcal{C}_{\frac{2(p^t-1)}{m}} : Y^2 = X^{\frac{2(p^t-1)}{m}} + 1$ have the same Hasse-Witt invariant. In particular, the Hasse-Witt invariant of $\mathcal{C}_{2(p^t-1)}$ is $\left(\frac{p+1}{2}\right)^t - 2$.*

Proof. It follows from Corollary ?? that $\gamma(\mathcal{D}_{\frac{p^t-1}{m}+1}) = \gamma(\mathcal{C}_{\frac{2(p^t-1)}{m}}) - \gamma(\mathcal{C}_{\frac{p^t-1}{m}})$. Since $p^t = 4g\left(\frac{m-1}{2}\right) + 2g + 1$, we have $\mathcal{D}_{\frac{p^t-1}{m}+1}$ is $\mathbb{F}_{p^{2t}}$ -maximal. Therefore, $\gamma(\mathcal{D}_{\frac{p^t-1}{m}+1}) = 0$. Finally, it follows from Corollary ?? that $\gamma(\mathcal{C}_{2(p^t-1)}) = \left(\frac{p+1}{2}\right)^t - 2$. $\square$

In the next result we use the well known fact that if n divides $q + 1$, then $Y^2 = X^n + 1$ is $\mathbb{F}_{q^2}$ -maximal.

Corollary 3.4.4. *If h is a positive integer, then the Hasse-Witt invariant of the curve $\mathcal{D} : Y^2 = X^{p^h+2} + X$ is given by*

$$\gamma(\mathcal{D}) = \left(\frac{p+1}{2}\right)^h.$$

Proof. It follows from Corollary ?? that $\gamma(\mathcal{D}) = \gamma(\mathcal{C}_{2(p^h+1)}) - \gamma(\mathcal{C}_{p^h+1})$. Since $\mathcal{C}_{p^h+1}$ is $\mathbb{F}_{p^{2h}}$ -maximal, we have $\gamma(\mathcal{C}_{p^h+1}) = 0$ (cf. Proposition ??). Thus, by Corollary ??, we have the result. $\square$

Corollary 3.4.5. *If r is a positive integer, then the Hasse-Witt invariant of the curve $\mathcal{C}_{2(p^{2r}+p^r+1)} : Y^2 = X^{2(p^{2r}+p^r+1)} + 1$ is*

$$\gamma = 2 \left(\frac{(p+1)(p+3)}{8} \right)^r.$$

Proof. It follows from Corollary ?? that $\gamma = 2\gamma(\mathcal{C}_{p^{2r}+p^r+1})$. Thus, by Corollary ??, we have the result. $\square$

Corollary 3.4.6. *If h is a positive integer, then the Hasse-Witt invariant of the curve $\mathcal{D} : Y^2 = X^{(p^h+1)/2} + X$ is given by*

$$\gamma(\mathcal{D}) = \begin{cases} \frac{1}{2} \left(\left(\frac{p+1}{2} \right)^h - u \right) & \text{if } 4 \mid p^h - 1, \\ \frac{1}{2} \left(\frac{p+1}{2} \right)^h - 1 & \text{if } 4 \nmid p^h - 1, \end{cases}$$

where u is one, when 4 divides $p - 1$, otherwise u is zero.

Proof. If $4 \mid p^h - 1$ (resp. $4 \nmid p^h - 1$) then $(p^h + 1)/2$ is odd (resp. even). It follows from Corollary ?? that $\gamma(\mathcal{D}) = \gamma(\mathcal{C}_{p^h-1}) - \gamma(\mathcal{C}_{(p^h-1)/2})$ (resp. $\gamma(\mathcal{D}) = \gamma(\mathcal{C}_{(p^h-1)/2})$). Thus, by Corollaries ?? and ??, we have the result. $\square$

Corollary 3.4.7. *Let t and h be positive integers. If $4t$ divides $p+3$, and $p+3$ divides $2t(p^h-1)$, then the Hasse-Witt invariant of the curve $\mathcal{D} : Y^2 = X^{2t(p^h-1)/(p+3)+1} + X$ is given by*

$$\gamma(\mathcal{D}) = \begin{cases} \frac{1}{2} \left(\left(\frac{p+1}{2} \right)^h - (-1)^h \right) + (-u)^h & \text{if } \frac{2t(p^h-1)}{p+3} \text{ is even,} \\ \frac{1}{2} \left(\left(\frac{p+1}{2} \right)^h - (-1)^h \right) + (-u)^h - 1 & \text{if } \frac{2t(p^h-1)}{p+3} \text{ is odd,} \end{cases}$$

where $u = 1$, when $\frac{p+3}{4t}$ divides $\frac{p^h-1}{p-1}$ and $\frac{p+3}{2t}$ does not divide $\frac{p^h-1}{p-1}$, otherwise $u = 0$.

Proof. It follows from Corollary ?? that $\gamma(\mathcal{D}) = \gamma(\mathcal{C}_{4t(p^h-1)/(p+3)}) - \gamma(\mathcal{C}_{2t(p^h-1)/(p+3)})$. Thus, by Corollary ??, we have the result. $\square$

Corollary 3.4.8. *Let t and h be positive integers. If $4t$ divides $p+1$, and $p+1$ divides $2t(p^h-1)$, then the Hasse-Witt invariant of the curve $\mathcal{C} : Y^2 = X^{2t(p^h-1)/(p+1)+1} + X$ is given by*

$$\gamma = \begin{cases} \frac{1}{2} \left(\frac{p+1}{2} \right)^h & \text{if } \frac{2t(p^h-1)}{p+1} \text{ is even,} \\ \frac{1}{2} \left(\frac{p+1}{2} \right)^h - 1 & \text{if } \frac{2t(p^h-1)}{p+1} \text{ is odd.} \end{cases}$$

Proof. It follows from Corollary ?? that $\gamma(\mathcal{D}) = \gamma(\mathcal{C}_{4t(p^h-1)/(p+1)}) - \gamma(\mathcal{C}_{2t(p^h-1)/(p+1)})$. Thus, by Corollary ??, we have the result. $\square$

Corollary 3.4.9. *Let t and h be positive integers. If $4t$ divides $p-1$, then the Hasse-Witt invariant of the curve $\mathcal{C} : Y^2 = X^{2t(p^h-1)/(p-1)+1} + X$ is given by*

$$\gamma = \frac{2t}{p-1} \left(\left(\frac{p+1}{2} \right)^h - 1 \right).$$

Proof. It follows from Corollary ?? that $\gamma(\mathcal{D}) = \gamma(\mathcal{C}_{4t(p^h-1)/(p-1)}) - \gamma(\mathcal{C}_{2t(p^h-1)/(p-1)})$. Thus, by Corollary ??, we have the result. $\square$

Corollary 3.4.10. *Let t and h be positive integers. If t is an odd divisor of $p-1$, and h is an odd number, then the Hasse-Witt invariant of the curve $\mathcal{D} : Y^2 = X^{t(p^h-1)/(p-1)+1} + X$ is given by*

$$\gamma(\mathcal{D}) = \frac{t}{p-1} \left(\left(\frac{p+1}{2} \right)^h - 1 \right) - \frac{1}{2}.$$

Proof. Since $t(p^h-1)/(p-1)+1$ is even, we have by Corollary ?? that $\gamma(\mathcal{D}) = \gamma(\mathcal{C}_{t(p^h-1)/(p-1)})$. Thus, by Corollary ??, we have the result. $\square$

3.5 The Hasse-Witt invariant of $Y^2 = X^n + 1$: an alternative approach

Let p be an odd prime. Let $n \geq 5$ be an integer coprime to p . Consider the curve

$$\mathcal{C}_n : Y^2 = X^n + 1,$$

of genus g_n (cf. (??)), defined over $\mathbb{F}_q$, where q is a power of p . Consider the basis

$$B = \left\{ \omega_m = \frac{x^{m-1}}{y} dx : 1 \leq m \leq g_n \right\}$$

for the vector space of holomorphic differentials of $\mathcal{C}_n$ given in (??). Note that if $m \in \{1, \dots, g_n\}$, then

$$\frac{x^{m-1}}{y} = \frac{x^{m-1}}{y^{p^j}} (y^2)^{(p^j-1)/2} = \frac{x^{m-1}}{y^{p^j}} (x^n + 1)^{(p^j-1)/2} = \sum_{r=0}^{(p^j-1)/2} \binom{\frac{p^j-1}{2}}{r} \frac{x^{nr+m-1}}{y^{p^j}}.$$

Therefore,

$$\omega_m = \sum_{r=0}^{(p^j-1)/2} \binom{\frac{p^j-1}{2}}{r} \frac{x^{nr+m-1}}{y^{p^j}} dx \quad (3.15)$$

Lemma 3.5.1. *Let p be an odd prime. For $m \in \{1, \dots, g_n\}$ consider $\omega_m \in B$, and let j be a positive integer. If there exists $\tilde{m} \in \{1, \dots, g_n\}$ such that n divides $\tilde{m}p^j - m$, then*

$$C^j(\omega_m) = \binom{\frac{p^j-1}{2}}{\frac{\tilde{m}p^j-m}{n}} \omega_{\tilde{m}},$$

otherwise $C^j(\omega_m) = 0$.

Proof. Note that $\omega_m = \sum_{r=0}^{(p^j-1)/2} \binom{\frac{p^j-1}{2}}{r} \frac{x^{nr+m-1}}{y^{p^j}} dx$ (cf. (??)). Using the $1/p$ -linearity of the Cartier operator (cf. Section ??), we have

$$C^j(\omega_m) = \frac{1}{y} \sum_{r=0}^{(p^j-1)/2} \binom{\frac{p^j-1}{2}}{r} C^j(x^{nr+m-1} dx). \quad (3.16)$$

By Lemma ??, the term $C^j(x^{nr+m-1} dx)$ in equation (??) is nonzero if and only if $nr + m \equiv 0 \pmod{p^j}$. Since $0 < nr + m \leq \frac{np^j-1}{2} < (n-1)p^j$ (cf. (??)), we have $nr + m \in \{p^j, 2p^j, \dots, (n-1)p^j\}$, that is, $nr \in \{p^j - m, 2p^j - m, \dots, (n-1)p^j - m\}$. Now, suppose that there exists $\tilde{m} \in \{1, \dots, g_n\}$ such that n divides $\tilde{m}p^j - m$. Since r is an integer and $X \equiv mp^{-j} \pmod{n}$ has a unique solution in $\{0, \dots, n-1\}$, we have that $\tilde{m}$ is unique. Thus, if there exists such an $\tilde{m}$, then it follows from equation (??) that

$$C^j(\omega_m) = \binom{\frac{p^j-1}{2}}{\frac{\tilde{m}p^j-m}{n}} \omega_{\tilde{m}},$$

otherwise, $C^j(\omega_m) = 0$. □

Let $m \neq 0$ be an integer. Throughout this section we denote by $\text{rad}(m)$ the radical of m , that is

$$\text{rad}(m) = \prod_{\substack{p|m \\ p \text{ prime}}} p.$$

Moreover, we denote by $v_p(m)$ the p -adic valuation of m , that is, the highest n such that p^n divides m .

Let p be an odd prime, n be a positive integer, α be the order of p in $(\mathbb{Z}/2\text{rad}(n)\mathbb{Z})^\times$ and $m \in \{1, \dots, \mathfrak{g}_n\}$. Let I be a positive integer and $p_1, \dots, p_I$ be prime numbers such that

$$n = \prod_{i=1}^I p_i^{n_i}, \quad p^\alpha - 1 = s \prod_{i=1}^I p_i^{t_i} \quad \text{and} \quad m = u \prod_{i=1}^I p_i^{v_i}, \quad (3.17)$$

where $v_i \geq 0$ and n_i, s, t_i, u are positive integers with p_i coprime to s and u , for all $i \in \{1, \dots, I\}$. The following result will be used in the proof of Theorem ??.

Lemma 3.5.2. *Let p be an odd prime, n, m, γ be positive integers, and let α be the order of p in $(\mathbb{Z}/2\text{rad}(n)\mathbb{Z})^\times$. Suppose that Equation (??) holds. If $n_I \geq t_I + v_I + 1$ and $n_i \leq t_i + v_i$ for $i \in \{1, \dots, I-1\}$, then*

$$mp^{\alpha A} \equiv m + \gamma su \prod_{i=1}^{I-1} p_i^{t_i+v_i} p_I^{n_I-1} \pmod{n},$$

where $A = \gamma p_I^{n_I - t_I - v_I - 1}$.

Proof. Note that

$$mp^{\alpha A} = u \prod_{i=1}^I p_i^{v_i} \left(s \prod_{i=1}^I p_i^{t_i} + 1 \right)^A = u \sum_{\lambda=0}^A \binom{A}{\lambda} s^\lambda \prod_{i=1}^I p_i^{\lambda t_i + v_i} = m + \gamma su \prod_{i=1}^{I-1} p_i^{t_i+v_i} p_I^{n_I-1} + nz,$$

for some $z \in \mathbb{Z}$. Indeed, for each $i \in \{1, \dots, I\}$, let

$$\beta_\lambda := \binom{A}{\lambda} s^\lambda \prod_{i=1}^I p_i^{\lambda t_i + v_i} = \frac{A(A-1) \cdots (A-\lambda+1)}{\lambda!} s^\lambda \prod_{i=1}^I p_i^{\lambda t_i + v_i}, \quad \text{for all } \lambda \geq 2.$$

Write $\lambda = a_0 + a_1 p_i + \dots + a_r p_i^r$, with $0 \leq a_i \leq p-1$, and let $s_{p_i}(\lambda) = a_0 + a_1 + \dots + a_r$. It follows from Theorem ?? that

- If λ is not a power of p_i , then $s_{p_i}(\lambda) \geq 2$, it follows that $v_{p_i}(\lambda!) = \frac{\lambda - s_{p_i}(\lambda)}{p_i - 1} \leq \frac{\lambda - 2}{p_i - 1} \leq \lambda - 1 - 1 \leq (\lambda - 1)t_i - 1$.
- If λ is a power of p_i , then $s_{p_i}(\lambda) = 1$. Since $2\text{rad}(n)$ divides $p^\alpha - 1 = s \prod_{i=1}^I p_i^{t_i}$ it follows that if $p_i = 2$ then $t_i \geq 2$. So

$$v_{p_i}(\lambda!) = \frac{\lambda - 1}{p_i - 1} = \begin{cases} \frac{\lambda - 1}{p_i - 1} & \text{if } p_i = 2 \\ \frac{\lambda - 1}{p_i - 1} & \text{if } p_i \geq 3 \end{cases} < \begin{cases} (\lambda - 1)t_i & \text{if } p_i = 2 \\ (\lambda - 1)t_i & \text{if } p_i \geq 3 \end{cases}.$$

Thus $v_{p_i}(\lambda!) \leq (\lambda - 1)t_i - 1$.

Now, if $i \in \{1, \dots, I-1\}$ then

$$v_{p_i}(\beta_\lambda) \geq \lambda t_i + v_i - v_{p_i}(\lambda!) \geq \lambda t_i + v_i - (\lambda - 1)t_i + 1 = t_i + v_i + 1 > n_i$$

and

$$v_{p_I}(\beta_\lambda) \geq n_I - t_I - v_I - 1 + \lambda t_I + v_I - v_{p_I}(\lambda!) \geq n_I - 1 + (\lambda - 1)t_I - (\lambda - 1)t_I + 1 = n_I.$$

Therefore

$$mp^{\alpha A} \equiv m + \gamma su \prod_{i=1}^{I-1} p_i^{t_i+v_i} p_I^{n_I-1} \pmod{n}.$$

□

In the next result we use the fact that $\Delta_{\mathcal{C}_n}^{(1)} = \Delta_{\mathcal{C}_n}^{\log} \oplus \Delta_{\mathcal{C}_n}^0$ (cf (??)).

Theorem 3.5.3. *Let p be an odd prime, n be a positive integer, α be the order of p in $(\mathbb{Z}/2\text{rad}(n)\mathbb{Z})^\times$ and $m \in \{1, \dots, \mathfrak{g}_n\}$. The differential $\omega_m \in \Delta_{\mathcal{C}_n}^{\log}$ if and only if n divides $mp^\alpha - m$ and $\left(\frac{p^\alpha - 1}{m(p^{\frac{\alpha-1}{2}})}\right) \not\equiv 0 \pmod{p}$*

Proof. Let I be a positive integer and $p_1, \dots, p_I$ be prime numbers such that

$$n = \prod_{i=1}^I p_i^{n_i}, \quad p^\alpha - 1 = s \prod_{i=1}^I p_i^{t_i} \quad \text{and} \quad m = u \prod_{i=1}^I p_i^{v_i},$$

where $v_i \geq 0$ and n_i, s, t_i, u are positive integers with p_i coprime to s and u , for all $i \in \{1, \dots, I\}$. Suppose that n does not divide

$$mp^\alpha - m = m(p^\alpha - 1) = us \prod_{i=1}^I p_i^{t_i+v_i},$$

that is, there exists $i \in \{1, \dots, I\}$ such that $n_i \geq t_i + v_i + 1$. For simplicity we suppose that $n_I \geq t_I + v_I + 1$ and $n_i \leq t_i + v_i$ for $i \in \{1, \dots, I-1\}$ (the general case following the same reasoning). Since p_I does not divide s, u and p_i , for all $1 \leq i \leq I-1$, we have that there exists $\delta \in \{1, \dots, p_I - 1\}$ such that

$$su \prod_{i=1}^{I-1} p_i^{t_i+v_i-n_i} = \lambda p_I + \delta, \text{ for some integer } \lambda.$$

Thus, we can choose positive integers γ and β such that $\gamma\delta = \beta p_I + b$, where b is a positive integer such that $\mathfrak{g}_n < m + bn/p_I \leq n-1$ (cf. Lemma ??). Finally, let $A = \gamma p_I^{n_I-t_I-v_I-1}$, and let η be a positive integer such that $j = \eta h - \alpha A > 0$. Then it follows from Lemma ?? that

$$m_j \equiv mp^{-j} \equiv mp^{\alpha A} \equiv m + bn/p_I \pmod{n}.$$

Since $\mathfrak{g}_n < m + bn/p_I \leq n-1$ we have $m_j = m + bn/p_I$. Thus there exists no $m_j \in \{1, \dots, \mathfrak{g}_n\}$ such that n divides $m_j p^j - m$, consequently $C^j(\omega_m) = 0$ (cf. Lemma ??). Therefore, $\omega_m \notin \Delta_{\mathcal{C}_n}^{\log}$ (cf

(??)), which is a contradiction. Thus n divides $mp^\alpha - m$. Now, since $\omega_m \in \Delta_{\mathcal{C}_n}^{\log}$, it follows from Lemma ?? that $C^\alpha(\omega_m) = \left(\frac{p^\alpha-1}{m(p^\alpha-1)}\right)\omega_m \neq 0$. Conversely, if n divides $mp^\alpha - m$ and $\left(\frac{p^\alpha-1}{m(p^\alpha-1)}\right) \not\equiv 0 \pmod{p}$, then it follows from Proposition ?? that $\omega_m \in \Delta_{\mathcal{C}_n}^{\log}$. $\square$

Corollary 3.5.4. *Let p be an odd prime, n be a positive integer, and α be the order of p in $(\mathbb{Z}/2\text{rad}(n)\mathbb{Z})^\times$. If $d = \gcd(n, p^\alpha - 1)$, then the Hasse-Witt invariant of $\mathcal{C}_n : Y^2 = X^n + 1$ is given by the cardinality of the set*

$$L = \left\{ i \in \left\{ 1, \dots, \left\lfloor \frac{d-1}{2} \right\rfloor \right\} : \left(\frac{\frac{p^\alpha-1}{2}}{i(p^\alpha-1)} \right) \not\equiv 0 \pmod{p} \right\}.$$

In particular, $\left\lfloor \frac{d-1}{2} \right\rfloor$ is an upper bound on the Hasse-Witt invariant of $\mathcal{C}_n$.

Proof. Let

$$L = \left\{ m \in \{1, \dots, \mathfrak{g}_n\} : n \text{ divides } m(p^\alpha - 1) \text{ and } \left(\frac{\frac{p^\alpha-1}{2}}{m(p^\alpha-1)} \right) \not\equiv 0 \pmod{p} \right\}.$$

Let $B_1 = \{\omega_m \in B : m \in L\} \subset B$. Since B is a basis of $\Delta_{\mathcal{C}_n}^{(1)} = \Delta_{\mathcal{C}_n}^{\log} \oplus \Delta_{\mathcal{C}_n}^0$ (cf (??)), $B_1 \subset \Delta_{\mathcal{C}_n}^{\log}$ and $B \setminus B_1 \subset \Delta_{\mathcal{C}_n}^0$, we have that B_1 is a basis of $\Delta_{\mathcal{C}_n}^{\log}$. Thus, the Hasse-Witt invariant of $\mathcal{C}_n$ is the cardinality of L (cf. Definition ??). Finally, It follows from Lemma ?? that

$$L = \left\{ i \in \left\{ 1, \dots, \left\lfloor \frac{d-1}{2} \right\rfloor \right\} : \left(\frac{\frac{p^\alpha-1}{2}}{i(p^\alpha-1)} \right) \not\equiv 0 \pmod{p} \right\}.$$

$\square$

Now, using Lemma ??, Theorem ?? and Corollary ??, we are able to compute the Hasse-Witt invariant of $\mathcal{C}_n$ when $2\text{rad}(n)$ divides $p-1$ or $p+1$.

Theorem 3.5.5. *Let p be an odd prime, and let n be a positive integer such that $2\text{rad}(n)$ divides $p-1$. Then the Hasse-Witt invariant of the curve $\mathcal{C}_n : Y^2 = X^n + 1$ is*

$$\gamma = \begin{cases} \frac{\gcd(n, p-1) - 1}{2} & \text{if } n \text{ is odd,} \\ \frac{\gcd(n, p-1) - 2}{2} & \text{if } n \text{ is even.} \end{cases}$$

Proof. Since the order of p in $(\mathbb{Z}/2\text{rad}(n)\mathbb{Z})^\times$ is one, it follows from Corollary ?? that γ is the cardinality of

$$L = \left\{ i \in \left\{ 1, \dots, \left\lfloor \frac{d-1}{2} \right\rfloor \right\} : \left(\frac{\frac{p-1}{2}}{i(p-1)} \right) \not\equiv 0 \pmod{p} \right\} = \left\{ 1, \dots, \left\lfloor \frac{d-1}{2} \right\rfloor \right\},$$

where $d = \gcd(n, p-1)$. Therefore, $\gamma = \left\lfloor \frac{d-1}{2} \right\rfloor$. $\square$

Proposition 3.5.6. *Let p be an odd prime, and let n be a positive integer such that $\text{rad}(n)$ divides $p + 1$. If $L = \frac{n}{\gcd(n, p+1)}$ is odd, then the curve $\mathcal{C}_n : Y^2 = X^n + 1$ has Hasse-Witt invariant zero.*

Proof. Consider the prime decomposition $n = \prod_{i=1}^l p_i^{n_i}$. Since $\text{rad}(n)$ divides $p + 1$, we have $p + 1 = s \prod_{i=1}^l p_i^{t_i}$, where $p_i \nmid s$ and $t_i \geq 1$. Now applying LTE Lemma (cf. Lemma ??) for each p_i yields

$$v_{p_i}(p^L + 1) = t_i + n_i - \min\{t_i, n_i\} \geq n_i.$$

Therefore, n divides $p^L + 1$. Hence, $\mathcal{C}_n$ is $\mathbb{F}_{p^{2L}}$ -maximal. In particular, $\gamma(\mathcal{C}_n) = 0$ (cf. Proposition ??). $\square$

Lemma 3.5.7. *Let p be an odd prime, and let n be a positive integer such that $2\text{rad}(n)$ divides $p + 1$. If $\frac{n}{\gcd(n, p+1)}$ is even and $m \in \{1, \dots, \mathfrak{g}_n\}$, then $\omega_m \in \Delta_{\mathcal{C}_n}^{\log}$ if and only if n divides $((n/2 - m)p - m)$. In particular, the Hasse-Witt invariant of $\mathcal{C}_n : Y^2 = X^n + 1$ is given by the cardinality of the set*

$$L = \{m \in \{1, \dots, \mathfrak{g}_n\} : n \text{ divides } ((n/2 - m)p - m)\}.$$

Proof. Let $t = v_2(p + 1)$. Since $2\text{rad}(n)$ divides $p + 1$, it follows that $t \geq 2$ and the order of p in $(\mathbb{Z}/2\text{rad}(n)\mathbb{Z})^\times$ is two. Let $\omega_m \in B$. If $\omega_m \in \Delta_{\mathcal{C}_n}^{\log}$, then it follows from Theorem ?? that

$$C^2(\omega_m) = \left(\frac{\frac{p^2-1}{2}}{\frac{mp^2-m}{n}} \right) \omega_m \neq 0.$$

Moreover, it follows from Lemma ?? that there exists $m_1, m_2 \in \{1, \dots, \mathfrak{g}_n\}$ such that

$$C(\omega_m) = \left(\frac{\frac{p-1}{2}}{\frac{m_1 p - m}{n}} \right) \omega_{m_1} \quad \text{and} \quad C(\omega_{m_1}) = \left(\frac{\frac{p-1}{2}}{\frac{m_2 p - m_1}{n}} \right) \omega_{m_2}.$$

Thus, $m_2 = m$, that is, n divides $m_1 p - m$ and $mp - m_1$. Hence n divides $2(m + m_1)(p - 1)/2$. Since $t \geq 2$ we have $p \equiv -1 \pmod{4}$ and so $\gcd(n, (p - 1)/2) = 1$, consequently n divides $2(m + m_1)$. Since $4 \leq 2(m + m_1) \leq 2n - 4$ we have $n = 2(m + m_1)$, consequently $m_1 = n/2 - m$. Reciprocally, if n divides $((n/2 - m)p - m)$ then $2m(p + 1) = \beta n$ for some odd integer $\beta \in \{1, \dots, p\}$. Therefore n divides $(mp - (n/2 - m))$ and consequently

$$C(\omega_m) = \left(\frac{\frac{p-1}{2}}{\frac{m_1 p - m}{n}} \right) \omega_{m_1} \neq 0 \quad \text{and} \quad C(\omega_{m_1}) = \left(\frac{\frac{p-1}{2}}{\frac{mp - m_1}{n}} \right) \omega_m \neq 0,$$

where $m_1 = n/2 - m$ (cf. Lemma ??). Therefore, it follows from Proposition ?? that $\omega_m \in \Delta_{\mathcal{C}_n}^{\log}$. In particular, the Hasse-Witt invariant of $\mathcal{C}_n$ is given by the cardinality of the set

$$L = \{m \in \{1, \dots, \mathfrak{g}_n\} : n \text{ divides } ((n/2 - m)p - m)\}$$

(this result is analogous to Corollary ??). $\square$

Theorem 3.5.8. *Let p be an odd prime, and let n be a positive integer such that $2\text{rad}(n)$ divides $p+1$. The Hasse-Witt invariant of $\mathcal{C}_n : Y^2 = X^n + 1$ is*

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

Proof. If $\frac{n}{\gcd(n, p+1)}$ is even, then it follows from Lemma ?? that the Hasse-Witt invariant of $\mathcal{C}_n$ is the cardinality of the set $\{m \in \{1, \dots, g_n\} : n \text{ divides } ((n/2 - m)p - m)\}$. Now, let $m \in \{1, \dots, g_n\}$ and note that n divides $((n/2 - m)p - m)$ if and only if

$$\frac{((n/2 - m)p - m)}{n} = \frac{1}{2} \left(p - \frac{2m(p+1)}{n} \right)$$

is an integer, that is, $2m(p+1) = n\beta$ for some odd integer β . Since there exist

$$\left\lfloor \frac{g_n \gcd(n, 2(p+1))}{n} \right\rfloor = \gcd(n, p+1) - 1$$

integers $m \in \{1, \dots, g_n\}$ for which n divides $2m(p+1)$ (cf. Lemma ??), we have $\gamma = \frac{\gcd(n, p+1)}{2}$. If $\frac{n}{\gcd(n, p+1)}$ is odd, then it follows from Lemma ?? that $\gamma = 0$. $\square$

Finally, as a consequence of Theorems ?? and ?? we have the following result.

Corollary 3.5.9. *Let p be an odd prime, n be a positive integer, and let $\gamma(\mathcal{C}_{2^n})$ be the Hasse-Witt invariant of the curve $\mathcal{C}_{2^n} : Y^2 = X^{2^n} + 1$.*

1. *If $t = v_2(p-1) \geq 2$, then*

$$\gamma(\mathcal{C}_{2^n}) = \begin{cases} 2^{n-1} - 1 & \text{if } n \leq t, \\ 2^{t-1} - 1 & \text{if } n \geq t. \end{cases}$$

2. *If $t = v_2(p+1) \geq 2$, then*

$$\gamma(\mathcal{C}_{2^n}) = \begin{cases} 0 & \text{if } n \leq t, \\ 2^{t-1} & \text{if } n > t. \end{cases}$$

Since $2\text{rad}(3^n) = 6$ divides $p-1$ or $p+1$, we have as a consequence of Theorems ?? and ?? we have the following result.

Corollary 3.5.10. *Let $p > 3$ be an odd prime and n be a positive integer, and let $\gamma(\mathcal{C}_n)$ be the Hasse-Witt invariant of the curve $\mathcal{C}_n : Y^2 = X^n + 1$. If $t = v_3(p-1) \geq 1$, then*

$$\gamma(\mathcal{C}_{3^n}) = \begin{cases} \frac{3^n-1}{2} & \text{if } n \leq t, \\ \frac{3^t-1}{2} & \text{if } n \geq t, \end{cases} \quad \text{and} \quad \gamma(\mathcal{C}_{2 \cdot 3^n}) = 2\gamma(\mathcal{C}_{3^n}).$$

Otherwise, $\gamma(\mathcal{C}_{2 \cdot 3^n}) = \gamma(\mathcal{C}_{3^n}) = 0$.

Proof. It follows from Corollary ?? that $\gamma(\mathcal{C}_{2 \cdot 3^n}) = 2\gamma(\mathcal{C}_{3^n})$. $\square$

THE HASSE-WITT INVARIANT OF THE $\mathbb{F}_{q^3}$ -FROBENIUS NONCLASSICAL CURVES OF TYPE $Y^{q^2+q+1} = f(X)$

4.1 The a -number of $\mathcal{C}_{b,c}$

Let p be a prime number, h be a positive integer and $q = p^h$. The objective of this section is to compute the a -number of the $\mathbb{F}_{q^3}$ -Frobenius nonclassical curves of type $Y^{q^2+q+1} = f(X)$, defined over $\mathbb{F}_{q^3}$. It follows from Theorem ?? that it suffices to consider curves defined over $\mathbb{F}_{q^3}$ of the type

$$\mathcal{C}_{b,c} : Y^{q^2+q+1} = X^{q^2+q+1} + b\text{Tr}(X) + c, \quad (4.1)$$

where $b, c \in \mathbb{F}_q$ are such that $(b, c) \neq (0, 0)$, defined over $\mathbb{F}_{q^3}$.

Definition 4.1.1. Let $\mathcal{X}$ be an algebraic curve defined over an algebraically closed field of characteristic $p > 0$. The a -number $a(\mathcal{X})$ of $\mathcal{X}$ is the dimension of the space of exact holomorphic differentials on $\mathcal{X}$.

If $\eta(c^2 + 4b^3) = 1$ (or $T_q(b^3/c^2) = 0$, when $p = 2$), then the a -number of $\mathcal{C}_{b,c}$ is given by the following theorem.

Theorem 4.1.2 (??, Theorem 3.2). If s is a positive integer, then the a -number of the Fermat curve $X^{sp+1} + Y^{sp+1} + 1 = 0$ is

$$a = \frac{s(s+1)p(p-1)}{4}.$$

Now, suppose that $\eta(c^2 + 4b^3) = -1$ (or $T_q(b^3/c^2) \neq 0$, when $p = 2$). By Proposition ??, the curve $\mathcal{C}_{b,c}$ is isomorphic to the curve

$$\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q.$$

Note that if ω is a holomorphic differential on $\mathcal{C}$, then ω is exact if and only if $C(\omega) = 0$, where C is the Cartier operator (cf. (??)). Thus the a -number of $\mathcal{C}$ is the rank of a Cartier-Manin matrix for $\mathcal{C}$ (cf. Section ??). Now, it follows from Theorem ?? that $B = \cup_{s=0}^{q-1} B_s$, where

$$B_0 = \left\{ \frac{x^j}{y^{i+1}} : (0, i, j) \in I_0 \right\} \text{ and } B_s = \left\{ \frac{x^j}{y^{i+s+1}} : (s, i, j) \in I_s \right\} \text{ for each } 1 \leq s \leq q-1,$$

is a basis of the Riemann-Roch space $\mathcal{L}(\text{div}(dx))$ of the curve $\mathcal{C}$, where $I = \cup_{s=0}^{q-1} I_s$, with

$$I_0 = \left\{ (0, i, j) \in \mathbb{N}_0^3 : \begin{array}{l} 1 \leq i \leq q \\ 0 \leq j \leq i-1 \end{array} \right\} \text{ and } I_s = \left\{ (s, i, j) \in \mathbb{N}_0^3 : \begin{array}{l} sq \leq i \leq (s+1)q \\ s \leq j \leq i-1 \end{array} \right\},$$

for each $1 \leq s \leq q-1$. Therefore

$$\bar{B} = \left\{ \omega_{s,i,j} = \frac{x^j}{y^{i+s+1}} dx : (s, i, j) \in I \right\} \quad (4.2)$$

is a basis for the vector space of holomorphic differentials on $\mathcal{C}$.

Lemma 4.1.3. *Let $(s, i, j) \in I$, write $i + s = mp + l$, $j = np + t$ and $s = \varepsilon p + \theta$, where $0 \leq l, t, \theta \leq p-1$. The following assertions hold:*

1. $0 \leq \varepsilon \leq p^{h-1} - 1$;
2. $sp^{h-1} + \varepsilon \leq m \leq (s+1)p^{h-1} + \varepsilon$;
3. $\varepsilon \leq n \leq m - \varepsilon - 1$.

Proof. This result follows from the definition of I . □

Theorem 4.1.4. *Let $(s, i, j) \in I$, write $i + s = mp + l$, $j = np + t$ and $s = \varepsilon p + \theta$, where $0 \leq l, t, \theta \leq p-1$. The following assertions hold:*

1. $C(\omega_{s,i,j}) = \binom{p-l-1}{p-t-1} \frac{x^{((p-t-1)q^2+q(t-l)+np)/p}}{y^{((p-l-1)(q^2+q)+mp)/p+1}} dx$. In particular, $C(\omega_{s,i,j}) = 0$ if and only if $l > t$.
2. If $l \leq t$, then $C(\omega_{s,i,j}) = \binom{p-l-1}{p-t-1} \omega_{s_1, i_1, j_1}$ with $\omega_{s_1, i_1, j_1} \in B_{s_1}$, where $s_1 = q - (l+1)p^{h-1} + \varepsilon$, $i_1 = ((p-l-1)q^2 + mp - \varepsilon p)/p$ and $j_1 = ((p-t-1)q^2 + q(t-l) + np)/p$.

Proof. 1. Note that if $0 \leq l \leq p-1$ then

$$\frac{1}{y^{l+1}} = \frac{(y^{q^2+q+1})^{p-l-1}}{y^{(p-l-1)(q^2+q)+p}} = \sum_{r=0}^{p-l-1} \binom{p-l-1}{r} \left(\frac{x^{(q^2r+q(p-l-1-r))/p}}{y^{((p-l-1)(q^2+q))/p+1}} \right)^p x^r$$

and therefore

$$\omega_{s,i,j} = \frac{x^j}{y^{i+s+1}} = \frac{x^{np+t}}{y^{mp}} \cdot \frac{1}{y^{l+1}} = \sum_{r=0}^{p-l-1} \binom{p-l-1}{r} \left(\frac{x^{(q^2r+q(p-l-1-r)+np)/p+c_r}}{y^{((p-l-1)(q^2+q)+mp)/p+1}} \right)^p x^{d_r},$$

where $r+t = c_r p + d_r$, with $0 \leq d_r \leq p-1$. Now, using the $1/p$ -linearity of the Cartier operator, we have

$$C(\omega_{s,i,j}) = \sum_{r=0}^{p-l-1} \binom{p-l-1}{r} \left(\frac{x^{(q^2 r + q(p-l-1-r) + np)/p + c_r}}{y^{((p-l-1)(q^2+q) + mp)/p+1}} \right) C(x^{d_r} dx).$$

Now, since $0 \leq r+t \leq 2p-2$ we have $d_r \equiv -1 \pmod{p}$ if and only if $r+t = p-1$, that is, $r = p-t-1$, and consequently $c_{p-t-1} = 0$ and $d_{p-t-1} = p-1$. Thus, $C(x^{d_r} dx) = dx$ for $r = p-t-1$ and $C(x^{d_r} dx) = 0$ otherwise (cf. Lemma ??). Therefore

$$C(\omega_{s,i,j}) = \binom{p-l-1}{p-t-1} \frac{x^{(q^2 r + q(p-l-1-r) + np)/p + c_r}}{y^{((p-l-1)(q^2+q) + mp)/p+1}} dx,$$

consequently $C(\omega_{s,i,j}) = 0$ if and only if $l > t$.

2. It is enough to observe that $i_1 + s_1 + 1 = ((p-l-1)(q^2+q) + mp)/p+1$ and $(s_1, i_1, j_1) \in I_{s_1}$.

□

Proposition 4.1.5. *The nonzero elements of $\{C(\omega) : \omega \in \overline{B}\}$ are all distinct.*

Proof. Let $\omega_{s_1, i_1, j_1}, \omega_{s_2, i_2, j_2} \in \overline{B}$, and let $\alpha_n \in \mathbb{F}_p$ be such that $C(\omega_{s_n, i_n, j_n}) = \alpha_n \omega_{\overline{s_n}, \overline{i_n}, \overline{j_n}}$, for some $\omega_{\overline{s_n}, \overline{i_n}, \overline{j_n}} \in \overline{B}$, for $n = 1, 2$. If $\omega_{\overline{s_1}, \overline{i_1}, \overline{j_1}} = \omega_{\overline{s_2}, \overline{i_2}, \overline{j_2}}$, then $\overline{s_1} = \overline{s_2}$ and $x^{\overline{j_1}}/y^{\overline{i_1}} = x^{\overline{j_2}}/y^{\overline{i_2}}$. Without loss of generality, suppose that $\overline{i_1} \geq \overline{i_2}$. If $\overline{j_1} \leq \overline{j_2}$, then $1 = x^{\overline{j_2} - \overline{j_1}} y^{\overline{i_1} - \overline{i_2}} \in \mathbb{K}(\mathcal{C})$ and consequently $f(x, y) = y^{q^2+q+1} - x^{q^2+1} - x^q$ divides $h(x, y) = 1 - x^{\overline{j_2} - \overline{j_1}} y^{\overline{i_1} - \overline{i_2}}$ (cf. Definition ??). Since $\deg(h) < \deg(f)$, we have $h = 0$, that is, $\overline{i_1} = \overline{i_2}$ and $\overline{j_1} = \overline{j_2}$. If $\overline{j_1} \geq \overline{j_2}$, then the result is analogous to the previous case. Finally, it follows from Lemma ?? that $\omega_{s_1, i_1, j_1} = \omega_{s_2, i_2, j_2}$. □

Note that if $\omega \in \overline{B}$, then $C(\omega)$ is either zero or belongs to the space spanned by $\overline{\omega}$, for some $\overline{\omega} \in \overline{B}$ (cf. Theorem ??). Thus, by Proposition ?? the rank of the Cartier-Manin matrix, with respect to the basis $\overline{B}$, is the cardinality of the set $\{\omega \in \overline{B} : C(\omega) = 0\}$.

Theorem 4.1.6. *The a -number of the curve $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ is*

$$\frac{q(p-1)}{12} (3p^{h-1} q^2 + q + p^{h-1} - 3).$$

Proof. Let $s \in \{0, \dots, q-1\}$ and $i \in \{sq, \dots, (s+1)q\}$. Write $i+s = mp+l$ and $s = \varepsilon p + \theta$, with $0 \leq l, \theta \leq p-1$. We want to count the values of $j \in \{s, \dots, i-1\}$ such that $C(\omega_{s,i,j}) = 0$, where $j = np+t$ with $0 \leq t \leq p-1$. For this, we define the sets $T_{0,0} = \emptyset$ and

$$T_{s,i} = \{np+t \in \mathbb{N}_0 : s \leq np+t \leq i-1 \text{ and } 0 \leq t < l\}$$

(cf. Lemma ??). It follows from Theorem ?? and Proposition ?? that the a -number is the cardinality of the set $\{\omega_{s,i,j} \in \overline{B} : C(\omega_{s,i,j}) = 0\}$, that is, the cardinality of the set

$$\bigcup_{s=0}^{q-1} \bigcup_{i=sq}^{(s+1)q} T_{s,i}.$$

Write $i = sq + a$ with $0 \leq a \leq q$. Note that $a = 0$ or $a \in \{\alpha p + 1, \dots, (\alpha + 1)p\}$ with $\alpha \in \{0, \dots, p^{h-1} - 1\}$. Thus, we have some cases to consider:

- i) If $a = 0$, then $i + s = (sp^{h-1} + \varepsilon)p + \theta$, $l = \theta$ and $i - 1 = (sp^{h-1} - 1)p + p - 1$ and therefore

$$T_{s,i} = \{np + t : 0 \leq t \leq \theta - 1, \varepsilon + 1 \leq n < sp^{h-1} - 1\}.$$

Since $T_{s,i}$ has $\theta(sp^{h-1} - \varepsilon - 1)$ elements, the cardinality of the set $\bigcup_{s=0}^{q-1} T_{s,sq}$ is

$$a_1 = \sum_{\varepsilon=0}^{p^{h-1}-1} \sum_{\theta=0}^{p-1} \theta(sp^{h-1} - \varepsilon - 1) = \frac{q(p-1)}{12} (3qp^{h-1} + q - 5p^{h-1} - 3).$$

- ii) Suppose that $a \in \{\alpha p + 1, \dots, (\alpha + 1)p - \theta - 1\}$, for some $\alpha \in \{0, \dots, p^{h-1} - 1\}$. Write $a = \alpha p + 1 + b$, where $0 \leq b \leq p - \theta - 2$. Thus $i + s = (sp^{h-1} + \alpha + \varepsilon)p + \theta + b + 1$, consequently $l = \theta + b + 1$ and $i - 1 = (sp^{h-1} + \alpha)p + b$. Therefore $T_{s,i} = T_{s,i,1} \cup T_{s,i,2} \cup T_{s,i,3}$ where

$$T_{s,i,r} = \begin{cases} \{\varepsilon p + t : \theta \leq t \leq \theta + b\} & \text{if } r = 1, \\ \{np + t : 0 \leq t \leq \theta + b, \varepsilon + 1 \leq n < sp^{h-1} + \alpha - 1\} & \text{if } r = 2, \\ \{(sp^{h-1} + \alpha)p + t : 0 \leq t \leq b\} & \text{if } r = 3. \end{cases}$$

Since $T_{s,i}$ has $(2(b+1) + (b+1+\theta)(sp^{h-1} + \alpha - \varepsilon - 1))$ elements, the cardinality of the set $\bigcup_{s=0}^{q-1} \bigcup_{\alpha=0}^{p^{h-1}-1} \bigcup_{a=\alpha p+1}^{(\alpha+1)p-\theta-1} T_{s,sq+a}$ is

$$\begin{aligned} a_2 &= \sum_{\alpha=0}^{p^{h-1}-1} \sum_{\varepsilon=0}^{p^{h-1}-1} \sum_{\theta=0}^{p-1} \sum_{b=0}^{p-\theta-2} (2(b+1) + (b+1+\theta)(sp^{h-1} + \alpha - \varepsilon - 1)) \\ &= \frac{qp^{h-1}(p-1)}{24} (4q^2 - pq - 2p^{h-1}q - 5q + 2p^{h-1} + 12). \end{aligned}$$

- iii) if $a = (\alpha + 1)p - \theta$, then $i + s = (sp^{h-1} + \alpha + \varepsilon + 1)p$ and $l = 0 < t$, for all $0 \leq t \leq p - 1$. Therefore $T_{s,i} = \emptyset$ and consequently the cardinality of $\bigcup_{s=0}^{q-1} T_{s,sq+a}$ is zero.

- iv) Suppose that $a \in \{(\alpha + 1)p - \theta + 1, \dots, (\alpha + 1)p\}$, for some $\alpha \in \{0, \dots, p^{h-1} - 1\}$. Write $a = (\alpha + 1)p - \theta + 1 + b$, where $0 \leq b \leq \theta - 1$. Thus $i + s = (sp^{h-1} + \alpha + \varepsilon + 1)p + b + 1$, consequently $l = b + 1$ and $i - 1 = (sp^{h-1} + \alpha)p + p - \theta + b$. Therefore

$$T_{s,i} = \{np + t : 0 \leq t \leq b, \varepsilon + 1 \leq n < sp^{h-1} + \alpha\}.$$

Since $T_{s,i}$ has $(b+1)(sp^{h-1} + \alpha - \varepsilon)$ elements, the cardinality of the set $\bigcup_{s=0}^{q-1} \bigcup_{\alpha=0}^{p^{h-1}-1} \bigcup_{a=(\alpha+1)p-\theta+1}^{(\alpha+1)p} T_{s,sq+a}$ is

$$\begin{aligned} a_3 &= \sum_{\alpha=0}^{p^{h-1}-1} \sum_{\varepsilon=0}^{p^{h-1}-1} \sum_{\theta=0}^{p-1} \sum_{b=0}^{p-\theta-2} (b+1)(sp^{h-1} + \alpha - \varepsilon) \\ &= \frac{qp^{h-1}(p-1)}{24} (2q^2 + pq + 2p^{h-1}q - q - 2p^{h-1}). \end{aligned}$$

Therefore, the a -number of $\mathcal{C}$ is $a_1 + a_2 + a_3 = \frac{q(p-1)}{12}(3p^{h-1}q^2 + q + p^{h-1} - 3)$. $\square$

Now, as a consequence of Theorems ?? and ?? we can to compute the a -number of $\mathcal{C}_{b,c}$.

Corollary 4.1.7. *The a -number of $\mathcal{C}_{b,c}$ is*

$$a(\mathcal{C}_{b,c}) = \begin{cases} \frac{q(q+1)}{4}((p-1)((q+1)p^{h-1} + 1)) & \text{if } \eta(c^2 + 4b^3) = 1, \\ \frac{q(p-1)}{12}(3p^{h-1}q^2 + q + p^{h-1} - 3) & \text{if } \eta(c^2 + 4b^3) = -1, \end{cases} \quad \text{for } p > 2$$

and

$$a(\mathcal{C}_{b,c}) = \begin{cases} \frac{q(q+1)}{4}((p-1)((q+1)p^{h-1} + 1)) & \text{if } T_q(b^3/c^2) = 0, \\ \frac{q(p-1)}{12}(3p^{h-1}q^2 + q + p^{h-1} - 3) & \text{if } T_q(b^3/c^2) \neq 0, \end{cases} \quad \text{for } p = 2 \text{ and } c \neq 0.$$

4.2 The Hasse-Witt invariant of $\mathcal{C}_{b,c}$, for q prime

Throughout this section q is a prime number. The objective of this section is to compute the Hasse-Witt invariant of the curve $\mathcal{C}_{b,c}$, with $b, c \in \mathbb{F}_q$ and $(b, c) \neq (0, 0)$ (cf. (??)). If $\eta(c^2 + 4b^3) = 0$ (or $b \neq 0$ and $c = 0$, when $p = 2$), then the Hasse-Witt invariant of the curve $\mathcal{C}_{b,c}$ is given by the following theorem.

Theorem 4.2.1 ((?), Lemma 2.1 (iv)). *Let p be a prime number, r be a positive integer and q be a power of p . If $r \geq 3$ and $\mathcal{N}_{q,r} : X^{\frac{q^r-1}{q-1}} = Y^{q^{r-1}} + Y^{q^{r-2}} + \dots + Y$ is the norm-trace curve, then the Hasse-Witt invariant of $\mathcal{N}_{q,r}$ is zero.*

Now, suppose that $\eta(c^2 + 4b^3) = -1$ (or $T_q(b^3/c^2) \neq 0$, when $p = 2$). By Proposition ?? and Theorem ?? the curve $\mathcal{C}_{b,c}$ is isomorphic to the curve $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ and $\overline{B} = \cup_{s=0}^{q-1} \overline{B}_s$ is a basis for the vector space of holomorphic differentials, where

$$\begin{aligned} \overline{B}_s &= \left\{ \omega_{s,i,j} = \frac{x^j}{y^{i+s+1}} dx : (s, i, j) \in I_s \right\} \\ &= \left\{ \omega_{s,i,j} = \frac{x^{nq+t}}{y^{mq+l+1}} dx : j = nq + t, i + s = mq + l, 0 \leq l, t \leq q-1, \text{ where } (s, i, j) \in I_s \right\}, \end{aligned}$$

for all $0 \leq s \leq q-1$ (cf. (??)). Note that if $(s, i, j) \in I$ is such that $j = nq + t$ and $i + s = mq + l$, with $0 \leq l, t \leq q-1$, then $0 \leq n \leq m-1$, $0 \leq n \leq s$ and $0 \leq m \leq s+1 \leq q$.

Proposition 4.2.2. *Let q be a prime number and r be a positive integer. If*

$$L_r = \{\omega \in \overline{B} : C^{r-1}(\omega) \neq 0 \text{ and } C^r(\omega) = 0\}$$

then the following assertions hold:

1. $L_1 = \left\{ \frac{x^{nq+t}}{y^{mq+l+1}} dx \in \bar{B} : t < l \right\}$ has $\frac{q(q-1)}{12}(3q^2+q-2)$ elements.

2. $L_2 = M_1 \cup M_2 \cup M_3$, where $M_k = \begin{cases} \left\{ \frac{x^{nq+t}}{y^{mq+l+1}} dx \in \bar{B} : l \leq t < m-n-1 \right\} & \text{if } k=1, \\ \left\{ \frac{x^{nq+t}}{y^{mq+l+1}} dx \in \bar{B} : m \leq l \leq t \right\} & \text{if } k=2, \\ \left\{ \frac{x^{nq+t}}{y^{mq+l+1}} dx \in \bar{B} : l \leq t, l+1 \leq m, q \leq t-l+n \right\} & \text{if } k=3, \end{cases}$

and this union is disjoint. Moreover, L_2 has $\frac{q(q-1)}{24}(3q^2+q-2)$ elements.

3. $L_k = \emptyset$ for all $k \geq 3$.

Proof. Let $\omega_{s,i,j} = \frac{x^{nq+t}}{y^{mq+l+1}} dx \in \bar{B}$, where $j = nq+t$ and $i+s = mq+l$, with $0 \leq l, t \leq q-1$. It follows from Theorems ?? and ?? that $C(\omega_{s,i,j}) = 0$ if and only if $t < l$ and that L_1 has $q(q-1)(3q^2+q-2)/12$ elements. Now, suppose that $l \leq t$ and $C(\omega_{s,i,j}) = \omega_{s_1,i_1,j_1}$. Since $-q \leq m-l-1 \leq q-1$ and $0 \leq t-l-n \leq 2q-2$ we have

$$i_1+s_1 = \begin{cases} q(q-l)+m-l-1 & \text{if } l+1 \leq m, \\ q(q-l-1)+q+m-l-1 & \text{if } m \leq l, \end{cases} \quad j_1 = \begin{cases} q(q-t-1)+t-l+n & \text{if } t-l+n \leq q-1, \\ q(q-t)+t-l+n-q & \text{if } q \leq t-l+n. \end{cases}$$

Write $j_1 = n_1q+t_1$ and $i_1+s_1 = m_1q+l_1$, with $0 \leq l_1, t_1 \leq q-1$. Thus, we have some cases to consider:

1. If $l+1 \leq m$ and $t-l+n \leq q-1$, then $\omega_{s,i,j} \in L_2$ if and only if $t_1 < l_1$ if and only if $t < m-n-1$, that is $\omega_{s,i,j} \in M_1$.
2. If $m \leq l$, then $t-l+n \leq q-1$. Since $t < q$, we have $t_1 < l_1$, that is $\omega_{s,i,j} \in M_2$.
3. Suppose that $l+1 \leq m$ and $q \leq t-l+n$. Since $t < q$, we have $t_1 < l_1$, that is $\omega_{s,i,j} \in M_3$.

Therefore $L_2 = M_1 \cup M_2 \cup M_3$. It follows from Lemma ?? that L_2 has $\frac{q(q-1)}{24}(3q^2+q-2)$ elements.

Finally, suppose that $C^2(\omega_{s,i,j}) \neq 0$. In this case, $t \geq l$, $l+1 \leq m$, $t-l+n \leq q-1$ and $t \geq m-n+1$. Moreover, $C^r(\omega_{s,i,j}) \neq 0$ for all $r \geq 3$ and

$$C^r(\omega_{s,i,j}) = \begin{cases} \alpha_2 \frac{x^{q(q+l-t+n-1)+q+n-m}}{y^{q(q-m+l+1)+q-m+1}} & \text{if } r=2, \\ \alpha_3 \frac{x^{q(q-n-1)+q-1-t+l}}{y^{mq+l+1}} & \text{if } r=3, \\ \alpha_4 \frac{x^{q(t-l)+q-t+m-n-2}}{y^{q(q-l)+m-l}} & \text{if } r=4, \\ \alpha_5 \frac{x^{q(t-m+n+1)+q-1-n}}{y^{q(q-m+l+1)+q-m+1}} & \text{if } r=5, \\ \alpha_6 \omega_{s,i,j} & \text{if } r=6, \end{cases}$$

for some $\alpha_1, \dots, \alpha_6 \in \mathbb{F}_p$. Thus, if $C^2(\omega_{s,i,j}) \neq 0$, then $\omega_{s,i,j} \in \Delta_{\mathcal{C}}^{\log}$. Therefore $L_r = \emptyset$, for all $r \geq 3$. $\square$

In the next result we use the fact that $\Delta_{\mathcal{C}}^{(1)} = \Delta_{\mathcal{C}}^{\log} \oplus \Delta_{\mathcal{C}}^0$ (cf. (??)).

Corollary 4.2.3. *Using the same notations as in Proposition ??, Let $\omega_{s,i,j} \in \bar{B}$. Then $\omega_{s,i,j} \in \Delta_{\mathcal{C}}^{\log}$ if and only if $C^2(\omega_{s,i,j}) \neq 0$. In particular, the Hasse-Witt invariant of the curve $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ is given by the cardinality of the set*

$$L = \{\omega \in \bar{B} : C^2(\omega_{s,i,j}) \neq 0\}.$$

Proof. It follows from Proposition ?? that $\omega_{s,i,j} \in \Delta_{\mathcal{C}}^{\log}$ if and only if $C^2(\omega_{s,i,j}) \neq 0$. Finally, Since $\bar{B}$ is a basis of $\Delta_{\mathcal{C}}^{(1)} = \Delta_{\mathcal{C}}^{\log} \oplus \Delta_{\mathcal{C}}^0$ (cf. (??)), $L \subset \Delta_{\mathcal{C}}^{\log}$ and $B \setminus L \subset \Delta_{\mathcal{C}}^0$, we have that L is a basis of $\Delta_{\mathcal{C}}^{\log}$. Thus, the Hasse-Witt invariant of $\mathcal{C}$ is the cardinality of L (cf. Definition ??). $\square$

Theorem 4.2.4. *If q is a prime number, then the Hasse-Witt invariant of the curve $\mathcal{C} : Y^{q^2+q+1} = X^{q^2+1} + X^q$ is*

$$\gamma = \frac{q(q+1)(q^2+q+2)}{8}.$$

Proof. Let a_i be the cardinality of the set L_i , for $i = 1, 2$, (cf. Proposition ??). Since γ is the cardinality of $\{\omega \in \bar{B} : C^2(\omega_{s,i,j}) \neq 0\}$ (cf. Corollary ??), we have $\gamma = g - (a_1 + a_2)$, where $g = \frac{q^4+q}{2}$ is the genus of $\mathcal{C}$ (cf. Proposition ??). Thus, it follows from Proposition ?? that

$$\gamma = \frac{q(q+1)(q^2+q+2)}{8}.$$

$\square$

Corollary 4.2.5. *Let q be a prime number. If $b, c \in \mathbb{F}_q$ and $(b, c) \neq (0, 0)$, then the Hasse-Witt invariant of the curve $\mathcal{C}_{b,c} : Y^{q^2+q+1} = X^{q^2+q+1} + b\text{Tr}(X) + c$ is*

$$\gamma = \begin{cases} 0 & \text{if } \eta(c^2 + 4b^3) = 0, \\ \frac{q(q+1)(q^2+q+2)}{8} & \text{if } \eta(c^2 + 4b^3) \neq 0, \end{cases} \quad \text{for } p > 2$$

and

$$\gamma = \begin{cases} 0 & \text{if } b \neq 0 \text{ and } c = 0, \\ \frac{q(q+1)(q^2+q+2)}{8} & \text{otherwise,} \end{cases} \quad \text{for } p = 2.$$

Proof. If $\eta(c^2 + 4b^3) = 0$ (or $b \neq 0$ and $c = 0$, when $p = 2$) or -1 (or $T_q(b^3/c^2) \neq 0$, when $p = 2$), then the result follows from Theorems ?? and ?? (cf. Proposition ?? and Theorem ??), respectively. Thus, suppose that $\eta(c^2 + 4b^3) = 1$ (or $T_q(b^3/c^2) = 0$, when $p = 2$), then we may assume that

$$\mathcal{C}_{b,c} : Y^{q^2+q+1} + X^{q^2+q+1} + 1 = 0$$

(cf. Theorem ?? and ??). Now, it follows from Theorem ?? that the Hasse-Witt invariant of $\mathcal{C}$ is the cardinality of the set

$$\left\{ (i, j) \in J : \binom{(q^2 + q - j)(q - 1)}{(i + 1)(q - 1)} \not\equiv 0 \pmod{q} \right\},$$

where $J = \{(i, j) \in \mathbb{N}^2 : i + j \leq q^2 + q - 2\}$. Note that if $(i, j) \in J$, then $0 \leq i \leq q^2 + q - 2$ and that the number $q^2 + q - j$ can vary between $i + 2$ and $q^2 + q$. Moreover the number $\binom{(q^2 + q - j)(q - 1)}{(i + 1)(q - 1)}$ is not zero modulo q , with $0 \leq i \leq q^2 + q - 2$ and $i + 2 \leq q^2 + q - j \leq q^2 + q$, if and only if $\binom{j(q - 1)}{i(q - 1)}$ is not zero modulo q , with $1 \leq i \leq q^2 + q - 1$ and $i + 1 \leq j \leq q^2 + q$. Consequently the Hasse-Witt invariant of $\mathcal{C}_{b,c}$ is the cardinality of the set

$$\left\{ (i, j) \in \mathbb{N}^2 : 1 \leq i < j \leq q^2 + q \text{ and } \binom{j(q - 1)}{i(q - 1)} \not\equiv 0 \pmod{q} \right\}.$$

It follows from Lemma ?? that the Hasse-Witt invariant of $\mathcal{C}_{b,c}$ is $\gamma = \frac{q(q+1)(q^2+q+2)}{8}$. □

BIBLIOGRAPHY

ABDÓN, M.; BORGES, H.; QUOOS, L. Weierstrass points on kummer extensions. **Advances in Geometry**, v. 19, n. 3, p. 323–333, 2018. Citation on page [64](#).

BASSA, A.; BEELEN, P. The hasse-witt invariant in some towers of function fields over finite fields. **Bull Braz Math Soc**, New Series 41, n. 4, p. 567–582, 2010. Citations on pages [46](#) and [76](#).

BERLEKAMP, E. R.; RUMSEY, H.; SOLOMON, G. On the solution of algebraic equations over finite fields. **Information and Control** 10, v. 10, n. 6, p. 553–564, 1967. Citation on page [58](#).

BONINI, M.; MONTANUCCI, M.; ZINI, G. On plane curves given by separated polynomials and their automorphisms. **Advances in Geometry**, 2019. Citations on pages [61](#) and [99](#).

BORGES, H. Frobenius nonclassical components of curves with separated variables. **Journal of Number Theory**, v. 159, p. 402–425, 2016. Citations on pages [19](#), [52](#), and [54](#).

BORGES, H.; HOMMA, M. Points on singular frobenius nonclassical curves. **Bull Braz Math Soc**, New Series 48, p. 93–101, 2017. Citation on page [19](#).

FINE, N. J. Binomial coefficients modulo a prime. **American Math. Monthly**, v. 54, n. 10, p. 589–592, 1947. Citation on page [73](#).

FULTON, W. **Algebraic Curves: An Introduction to Algebraic Geometry**. [S.l.]: The Benjamin/Cummings Publishing Company, Inc., 1969. Citations on pages [23](#), [38](#), [39](#), [40](#), and [41](#).

GARCIA, A.; TAFAZOLIAN, S. Certain maximal curves and cartier operators. **Acta Arithmetica**, v. 135, n. 3, p. 199–218, 2008. Citation on page [47](#).

GIULIETTI, M.; KORCHMÁROS, G. Algebraic curves with many automorphisms. **Advances in Mathematics**, v. 349, p. 162–211, 2019. Citation on page [20](#).

HASSE, H. **Number Theory**. [S.l.]: Springer-Verlag Berlin Heidelberg New York, 1898. Citation on page [107](#).

HASSE, H.; WITT, E. Zyklische unverzweigte erweiterungskörper vom primzahlgrade p über einen algebraischen funktionenkörper der charakteristik p . **Monatsh. Math. Phys.**, v. 43, p. 477–492, 1936. Citation on page [48](#).

HEFEZ, A.; VOLOCH, J. F. Frobenius nonclassical curves. **J.F. Arch. Math**, v. 54, n. 3, p. 263–273, 1990. Citation on page [19](#).

HIRSCHFELD, J.; KORCHMÁROS, G.; TORRES, F. **Algebraic Curves Over a Finite Field**. [S.l.]: Princeton Univ. Press, Princeton and Oxford, 2008. Citations on pages [19](#), [20](#), [23](#), [31](#), [37](#), [38](#), [40](#), [41](#), [42](#), [43](#), [44](#), [45](#), [46](#), [47](#), and [49](#).

J-P.SERRE. Sur la topologie des variétés algébriques en caractéristique p . **Universidad Nacional Autónoma de México - Unesco**, p. 24–53, 1958. Citation on page [47](#).

KANI, E.; ROSEN, M. Idempotent relations and factors of jacobians. **Mathematische Annalen**, v. 284, p. 307–327, 1989. Citation on page [49](#).

KONTOGEORGIS, A. I. The group of automorphisms of the function field of the curve $x^n + y^m + 1 = 0$. **Journal of Number Theory**, v. 72, p. 110–136, 1998. Citation on page [71](#).

LEOPOLDT, H. W. über die automorphismengruppe des fermatkörpers. **Journal of Number Theory**, v. 56, p. 256–282, 1996. Citation on page [61](#).

LUCAS, E. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier. **Bull. Soc. Math. France**, v. 6, p. 49–54, 1878. Citations on pages [73](#) and [74](#).

MONTANUCCI, M.; SPEZIALI, P. The a -numbers of fermat and hurwitz curves. **Journal of Pure and Applied Algebra**, v. 222, n. 2, p. 477–488, 2018. Citation on page [95](#).

NAKAJIMA, S. p -ranks and automorphism groups of algebraic curves. **Trans. of the American Mathematical Society**, v. 303, n. 2, p. 595–607, 1987. Citation on page [20](#).

PARVARDI, A. Lifting the exponent lemma (lte). 2011. Citation on page [107](#).

STICHTENOTH, H. **Algebraic Function Fields and Codes**. 2. ed. [S.l.]: Springer-Verlag, 2009. Citations on pages [20](#), [23](#), [24](#), [25](#), [27](#), [28](#), [29](#), [30](#), [31](#), [32](#), [33](#), [34](#), [35](#), [36](#), and [40](#).

STICHTENOTH, H.; XING, C. On the structure of the divisor class group of a class of curves over finite fields. **Arch. Math.**, v. 65, n. 2, p. 141–150, 1995. Citations on pages [20](#) and [46](#).

STÖHR, K. O.; VOLOCH, J. F. Weierstrass points and curves over finite fields. **Proc. London Math.**, s3-52, p. 1–19, 1986. Citation on page [19](#).

SUBRAO, D. The p -rank of artin-schreier curves. **manuscripta math.**, v. 16, n. 2, p. 169 – 193, 1975. Citation on page [19](#).

TAFAZOLIAN, S. A note on certain maximal hyperelliptic curves. **Finite Fields and Their Applications**, v. 18, p. 1013–1016, 2012. Citation on page [86](#).

TAFAZOLIAN, S.; TORRES, F. On maximal curves of fermat type. **Adv. Geom.**, v. 13, n. 4, p. 613 – 617, 2013. Citation on page [20](#).

_____. On the curve $y^n = x^m + x$ over finite fields. **Journal of Number Theory**, v. 145, p. 51–66, 2014. Citation on page [21](#).

TOWSE, C. Weierstrass points on cyclic covers of the projective line. **Transactions of the American Mathematical Society**, v. 348, n. 8, p. 3355–337, 1996. Citations on pages [71](#) and [73](#).

COMPLEMENTARY RESULTS

A.1

Lemma A.1.1. *Let $\alpha, \beta \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_{q^2}$ such that $\alpha\beta \neq 0$. If $\mathcal{C} : Y^{q+1} = \alpha X^{q+1} + \beta X^q + \beta^q X + \delta$ is an irreducible curve, then the polynomial $g(X) = \alpha X^{q+1} + X^q + X + \delta/\beta^{q+1}$ has two roots.*

Proof. Firstly, note that $\mathcal{C}$ is projectively equivalent to $\mathcal{C}_1 : Y^{q+1} = g(X)$, by means of the projectivity $(X : Y : Z) \mapsto (\beta X : \beta Y : Z)$. Now, suppose that $g(X) = (X - r)^{q+1}$. So, $\mathcal{C}_1$ is projectively equivalent to $\mathcal{C}_2 : Y^{q+1} = Z^{q+1}$, by means of the projectivity $(X : Y : Z) \mapsto (X : Y : (X - Z)/r)$, which is a contradiction. $\square$

A.2

Lemma A.2.1. *If t and l are positive integers, then*

$$\sum_{a_1, \dots, a_t=1}^p (a_1 \cdots a_t)^l = \left(\sum_{r=1}^p r^l \right)^t.$$

Proof. By induction on t . Note that if $t = 1$, then the result is clear. Thus, let $t \geq 2$ and suppose

that the result is true for $t - 1$. Thus by induction hypothesis we have

$$\begin{aligned}
 \sum_{a_1, \dots, a_t=1}^p (a_1 \cdots a_t)^l &= \sum_{a_1, \dots, a_t=1}^p a_t^l (a_1 \cdots a_{t-1})^l \\
 &= \sum_{a_t=1}^p a_t^l \left(\sum_{a_1, \dots, a_{t-1}=1}^p (a_1 \cdots a_{t-1})^l \right) \\
 &= \left(\sum_{a_t=1}^p a_t^l \right) \left(\sum_{r=1}^p r^l \right)^{t-1} \\
 &= \left(\sum_{r=1}^p r^l \right)^t.
 \end{aligned}$$

□

Lemma A.2.2. Let n and t be positive integers. If $B(1) := \sum_{a_0=1}^p a_0^n (p - a_0 + 1)^n$ and

$$B(t) := \sum_{l=0}^{t-2} p^{nl} \left(\sum_{a_1, \dots, a_{t-l-1}=0}^{p-1} \sum_{a_0=1}^{p-1} a_0^n (p - a_0 + 1)^n \prod_{i=1}^{t-l-1} (a_i + 1)^n (p - a_i)^n \right) + p^{n(t-1)} \left(\sum_{a_{t-1}=1}^p a_{t-1}^n (p - a_{t-1} + 1)^n \right),$$

for $t \geq 2$, then

$$B(t) = \left(\sum_{r=1}^p r^n (p - r + 1)^n \right)^t, \text{ for all positive integers } t.$$

Proof. By induction on t . First suppose $t = 2$ and note that

$$\begin{aligned}
 B(2) &= \sum_{a_1=0}^{p-1} \sum_{a_0=1}^{p-1} a_0^n (p - a_0 + 1)^n (a_1 + 1)^n (p - a_1)^n + p^n \sum_{a_1=1}^p a_1^n (p - a_1 + 1)^n \\
 &= \left(\sum_{a_1=1}^p a_1^n (p - a_1 + 1)^n \right) \left(\sum_{a_0=1}^p a_0^n (p - a_0 + 1)^n - p^n \right) + p^n \sum_{a_1=1}^p a_1^n (p - a_1 + 1)^n \\
 &= \left(\sum_{r=1}^p r^n (p - r + 1)^n \right)^2.
 \end{aligned}$$

Now, let $t \geq 3$ and suppose that the result is true for $t - 1$. Thus

$$\begin{aligned}
 B(t) &= \prod_{i=1}^{t-1} \left(\sum_{a_i=1}^p a_i^n (p - a_i + 1)^n \right) \left(\sum_{a_0=1}^p a_0^n (p - a_0 + 1)^n - p^n \right) \\
 &+ p^n \left(\sum_{l=1}^{t-2} p^{n(l-1)} \left(\sum_{a_1, \dots, a_{t-l-1}=0}^{p-1} \sum_{a_0=1}^{p-1} a_0^n (p - a_0 + 1)^n \prod_{i=1}^{t-l-1} (a_i + 1)^n (p - a_i)^n \right) \right. \\
 &+ \left. p^{n(t-2)} \left(\sum_{a_{t-1}=1}^p a_{t-1}^n (p - a_{t-1} + 1)^n \right) \right) \\
 &= \left(\sum_{r=1}^p r^n (p - r + 1)^n \right)^{t-1} \left(\sum_{a_0=1}^p a_0^n (p - a_0 + 1)^n - p^n \right) + p^n B(t-1).
 \end{aligned}$$

By induction hypothesis we have

$$B(t) = \left(\sum_{r=1}^p r^n (p - r + 1)^n \right)^t.$$

□

Lemma A.2.3. *Let p be an odd prime, n be a positive integer, and let p_I be a prime such that p_I divides n . If $m \in \{1, \dots, (n-1)/2\}$, then there exists a positive integer b such that*

$$\frac{n-1}{2} < m + bn/p_I \leq n-1.$$

Proof. Note that

$$\frac{n-1}{2} < m + bn/p_I < n \Leftrightarrow 0 \leq \frac{p_I}{2n}(n-1-2m) < b < \frac{p_I}{2n}(2n-2m).$$

Since

$$\frac{p_I}{2n}(2n-2m) - \frac{p_I}{2n}(n-1-2m) = \frac{p_I}{2n}(n+1) > \frac{p_I}{2} \geq 1,$$

the result follows. $\square$

Theorem A.2.4 ((??), chapter 17 §3 (Legendre's theorem)). *Let $\lambda = a_0 + a_1p + \dots + a_rp^r$ with $0 \leq a_i \leq p-1$ be the p -adic representation of λ in the least residue system $(\text{mod } p)$, and $s_p(\lambda) = a_0 + a_1 + \dots + a_r$. If $v_p(\lambda)$ is the highest power of p that divides $\lambda \in \mathbb{Z}$, then*

$$v_p(\lambda!) = \frac{\lambda - s_p(\lambda)}{p-1}.$$

Lemma A.2.5 (Lifting The Exponent Lemma (LTE)). *Let x and y be integers, let n be a positive integer, and let p be an odd prime such that $p \mid x-y$ and none x and y is divisible by p (i.e., $p \nmid xy$). We have*

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Proof. see, e.g., (??). $\square$

Lemma A.2.6. *Let n, k and t be positive integers. The number of elements $m \in \{1, \dots, t\}$ for which n divides mk is given by*

$$\left\lfloor \frac{t \gcd(n, k)}{n} \right\rfloor.$$

Proof. Let $G = \langle g \rangle$ be a cyclic group of order n . It is well known that g^k has order $\frac{n}{\gcd(n, k)}$. That is, the smallest integer $m_0 \geq 1$ for which n divides m_0k is $m_0 = \frac{n}{\gcd(n, k)}$. By Lagrange's Theorem, n divides mk if and only if m_0 divides m . Since the number of multiples of m_0 in $\{1, \dots, t\}$ is $\left\lfloor \frac{t}{m_0} \right\rfloor$, the result follows. $\square$

A.3

Lemma A.3.1. *Let $(s_1, i_1, j_1), (s_2, i_2, j_2) \in I$. For each $k = 1, 2$ write $i_k + s_k = m_kp + l_k$, $j_k = n_kp + t_k$, $s_k = \varepsilon_kp + \theta_k$ and $i_k = s_kq + r_k$, where $0 \leq l_k, t_k, \theta_k \leq p-1$ and $0 \leq r_k \leq q-1$. Moreover,*

consider

$$\begin{aligned}\overline{s_k} &= q - (l_k + 1)p^{h-1} + \varepsilon_k \\ \overline{i_k} &= \frac{(p - l_k - 1)q^2 + m_k p - \varepsilon_k p}{p}, \text{ for } k = 1, 2. \\ \overline{j_k} &= \frac{(p - t_k - 1)q^2 + q(t_k - l_k) + n_k p}{p}\end{aligned}$$

If $\overline{s_1} = \overline{s_2}$, $\overline{i_1} = \overline{i_2}$ and $\overline{j_1} = \overline{j_2}$, then $s_1 = s_2$, $i_1 = i_2$ e $j_1 = j_2$.

Proof. Since $\overline{s_1} = \overline{s_2}$, we have $(l_2 - l_1)p^{h-1} = \varepsilon_2 - \varepsilon_1$. Thus, by Lemma ??, $\varepsilon_1 = \varepsilon_2$ and $l_1 = l_2$. Now, since $\overline{i_1} = \overline{i_2}$, we have $m_1 = m_2$, consequently $i_1 + s_1 = i_2 + s_2$ and $(s_1 - s_2)(q + 1) = r_2 - r_1$. By Lemma ??, it follows that $r_1 = r_2$ and $s_1 = s_2$, hence $i_1 = i_2$. Finally, since $\overline{j_1} = \overline{j_2}$, we have $(t_2 - t_1)q(q - 1) = (n_2 - n_1)p$, consequently $q(q - 1)$ divides $(n_2 - n_1)p$. It follows from Lemma ?? that $(n_2 - n_1)p = \alpha q(q - 1)$, for some $\alpha \in \{-1, 0, 1\}$. Suppose that $\alpha \neq 0$, namely $\alpha = 1$. Thus $t_2 = t_1 + 1$ and $j_2 = (q^2 - q + 1) + j_1$. Since, $j_1 \geq s_1 = s_2$, we have $(s_2 + 1)q - 1 \geq i_2 - 1 \geq j_2 \geq (s_2 + 1)q$. Which is a contradiction. Therefore $\alpha = 0$, that is, $j_1 = j_2$. □

Lemma A.3.2. Using the same notations as in Proposition ??, the cardinality of the set M_r is

$$\begin{cases} \frac{q(q-1)}{24}(q^2 - q - 2) & \text{if } r = 1, \\ \frac{q(q-1)}{24}(q^2 + 3q + 2) & \text{if } r = 2, \\ \frac{q(q-1)}{24}(q^2 - q - 2) & \text{if } r = 3. \end{cases}$$

Proof. Let $s \in \{0, \dots, q-1\}$ and $i \in \{sq, \dots, (s+1)q\}$. Write $i + s = mq + l$, with $0 \leq l \leq q-1$. We want to count the values of $j \in \{s, \dots, i-1\}$ such that $\frac{x^j}{y^{mq+l+1}} dx \in L_2$, where $j = nq + t$ with $0 \leq t \leq q-1$. For this, we define the sets $M_{0,0}^r = \emptyset$, with $r = 1, 2, 3$, and

$$M_{s,i}^r = \begin{cases} \{nq + t \in \{s, \dots, i-1\} : l \leq t < m - n - 1\} & \text{if } r = 1, \\ \{nq + t \in \{s, \dots, i-1\} : m \leq l \leq t\} & \text{if } r = 2, \\ \{nq + t \in \{s, \dots, i-1\} : l \leq t, l+1 \leq m, q \leq t - l + n\} & \text{if } r = 3. \end{cases}$$

Note that the cardinality of the set M_r is the cardinality of the set

$$\bigcup_{s=0}^{q-1} \bigcup_{i=sq}^{(s+1)q} M_{s,i}^r.$$

Write $i = sq + a$ with $1 \leq a \leq q$. Thus, we have two cases to consider:

- i) If $a \in \{0, \dots, q-s-1\}$, then $i + s = sq + s + a$, consequently $l = s + a$ and $m = s$. Since $m - n - 1 = s - n - 1 < l$ and $l + 1 = s + a + 1 > m$, we have $M_{s,i}^1$ and $M_{s,i}^3$ are empty.

Since $M_{s,i}^2 = \{nq + t : 0 \leq n \leq s-1 \text{ and } s+a \leq t \leq q-1\}$ has $s(q-s-a)$ elements, the cardinality of the set $\bigcup_{s=0}^{q-1} \bigcup_{a=0}^{q-s-1} M_{s,sq+a}^2$ is

$$\sum_{s=1}^{q-1} \sum_{a=0}^{q-s-1} s(q-s-a) = \frac{q(q-1)}{24}(q^2 + 3q + 2).$$

ii) If $a \in \{q-s, \dots, q\}$ write $a = q-s+b$, with $0 \leq b \leq s$. Then $i+s = (s+1)q+b$, consequently $l = b$ e $m = s+1$. Since $m > s \geq l$, we have $M_{s,i}^2$ is empty. Note that the cardinality of $M_{s,i}^1 = \{nq + t : 1 \leq n \leq s-1, b \leq t \leq s-n-1\}$ and $M_{s,i}^3 = \{nq + t : 1 \leq n \leq s-1, q+b-n \leq t \leq q-1\}$ are $(s-n-b)$ and $(n-b)$, respectively. Therefore, the cardinality of the sets $\bigcup_{s=0}^{q-1} \bigcup_{a=q-s}^q M_{s,sq+a}^1$ and $\bigcup_{s=0}^{q-1} \bigcup_{a=q-s}^q M_{s,sq+a}^3$ are

$$\sum_{s=1}^{q-1} \sum_{n=1}^{s-1} \sum_{b=0}^{s-n-1} (s-n-b) = \sum_{s=1}^{q-1} \sum_{n=1}^{s-1} \sum_{b=0}^{n-1} (n-b) = \frac{q(q-1)}{24}(q^2 - q - 2).$$

Therefore the cardinality of the set M^r is

$$\begin{cases} \frac{q(q-1)}{24}(q^2 - q - 2) & \text{if } r = 1, \\ \frac{q(q-1)}{24}(q^2 + 3q + 2) & \text{if } r = 2, \\ \frac{q(q-1)}{24}(q^2 - q - 2) & \text{if } r = 3. \end{cases}$$

□

Lemma A.3.3. *If p is a prime number, then the cardinality of the set*

$$B = \left\{ (b_1p + b_0, p^2 + a_0) \in \mathbb{N}^2 : \begin{array}{ll} 1 \leq a_0 \leq p-1 & b_1+1 \leq b_0 \leq p-1 \\ 0 \leq b_1 \leq p-1 & a_0 \leq b_0 \leq a_0 + b_1 \end{array} \right\}$$

$$\text{is } \frac{p(p-1)(p+1)}{6}.$$

Proof. It is enough to note that $B = \bigcup_{n=1}^4 B_n$, where

$$B_1 = \left\{ (b_1p + b_0, p^2 + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq (p-1)/2 \\ a_0 - 1 \leq b_1 \leq p - a_0 - 1 \end{array}, b_1 + 1 \leq b_0 \leq a_0 - b_1 \right\},$$

$$B_2 = \left\{ (b_1p + b_0, p^2 + a_0) \in \mathbb{N}^2 : \begin{array}{l} (p-1)/2 \leq b_1 \leq p-1 \\ p - b_1 \leq a_0 \leq b_1 + 1 \end{array}, a_0 \leq b_0 \leq p-1 \right\},$$

$$B_3 = \left\{ (b_1p + b_0, p^2 + a_0) \in \mathbb{N}^2 : \begin{array}{l} 0 \leq b_1 \leq (p-3)/2 \\ b_1 + 2 \leq a_0 \leq p-1-b_1 \end{array}, a_0 \leq b_0 \leq a_0 + b_1 \right\}$$

and

$$B_4 = \left\{ (b_1p + b_0, p^2 + a_0) \in \mathbb{N}^2 : \begin{array}{l} (p+1)/2 \leq a_0 \leq p-1 \\ p - a_0 \leq b_1 \leq a_0 - 2 \end{array}, a_0 \leq b_0 \leq p-1 \right\}.$$

Therefore, the cardinality of B_n is

$$\begin{cases} (p-1)(p+1)(p+3)/24 & \text{if } n = 1, \\ p(p-1)(p+1)/24 & \text{if } n = 2, \\ p(p-1)(p+1)/24 & \text{if } n = 3, \\ (p-1)(p+1)(p-3)/24 & \text{if } n = 4. \end{cases}$$

Finally, since $B_n \cap B_m = \emptyset$ for $n \neq m$, the cardinality of set B is $\frac{p(p-1)(p+1)}{6}$. $\square$

Lemma A.3.4. *If p is a prime number, then the cardinality of the set*

$$B = \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq a_1 \leq p-1 \\ 0 \leq b_1 \leq a_1 - 1 \end{array}, \begin{array}{l} a_0 \leq b_0 \leq p-1 \\ -p - a_0 + a_1 + b_0 \leq b_1 \leq b_0 - 1 \end{array} \right\}$$

is $\frac{p(p+1)(p-1)(3p-2)}{96}$.

Proof. It is enough to note that $B = \bigcup_{n=1}^{10} B_n$, where

$$\begin{aligned} B_1 &= \{ (b_1p + b_0, a_0p + a_0) \in \mathbb{N}^2 : 0 \leq b_1 < a_0 \leq p-1, a_0 \leq b_0 \leq p-1 \}, \\ B_2 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq (p-1)/2 \\ 2a_0 \leq a_1 \leq p-1 \end{array}, \begin{array}{l} 0 \leq b_1 \leq a_0 - 1 \\ a_0 \leq b_0 \leq p + a_0 - a_1 + b_1 \end{array} \right\}, \\ B_3 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq (p-1)/2 \\ a_0 + 1 \leq a_1 \leq 2a_0 - 1 \end{array}, \begin{array}{l} 0 \leq b_1 \leq a_1 - a_0 - 1 \\ a_0 \leq b_0 \leq p + a_0 - a_1 + b_1 \end{array} \right\}, \\ B_4 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} (p+1)/2 \leq a_0 \leq p-1 \\ a_0 + 1 \leq a_1 \leq p-1 \end{array}, \begin{array}{l} 0 \leq b_1 \leq a_1 - a_0 - 1 \\ a_0 \leq b_0 \leq p + a_0 - a_1 + b_1 \end{array} \right\}, \\ B_5 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq (p-3)/2 \\ 2a_0 + 1 \leq a_1 \leq p-1 \end{array}, \begin{array}{l} a_0 \leq b_1 \leq a_1 - a_0 - 1 \\ b_1 + 1 \leq b_0 \leq p + a_0 - a_1 + b_1 \end{array} \right\}, \\ B_6 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq (p-1)/2 \\ a_0 + 1 \leq a_1 \leq 2a_0 - 1 \end{array}, \begin{array}{l} a_1 - a_0 \leq b_1 \leq a_0 - 1 \\ a_0 \leq b_0 \leq p-1 \end{array} \right\}, \\ B_7 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} (p+1)/2 \leq a_0 \leq p-1 \\ a_0 + 1 \leq a_1 \leq p-1 \end{array}, \begin{array}{l} a_1 - a_0 \leq b_1 \leq a_0 - 1 \\ a_0 \leq b_0 \leq p-1 \end{array} \right\}, \\ B_8 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq (p-1)/2 \\ 2a_0 \leq a_1 \leq p-1 \end{array}, \begin{array}{l} a_1 - a_0 \leq b_1 \leq a_1 - 1 \\ b_1 + 1 \leq b_0 \leq p-1 \end{array} \right\}, \\ B_9 &= \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq (p-1)/2 \\ a_0 + 1 \leq a_1 \leq p-1 \end{array}, \begin{array}{l} a_0 \leq b_1 \leq a_1 - 1 \\ b_1 + 1 \leq b_0 \leq p-1 \end{array} \right\}, \end{aligned}$$

and

$$B_{10} = \left\{ (b_1p + b_0, a_1p + a_0) \in \mathbb{N}^2 : \begin{array}{l} (p+1)/2 \leq a_0 \leq p-1 \\ a_0 + 1 \leq a_1 \leq p-1 \end{array}, \begin{array}{l} a_0 \leq b_1 \leq a_1 - 1 \\ b_1 + 1 \leq b_0 \leq p-1 \end{array} \right\}.$$

Moreover, the cardinality of B_n is

$$\left\{ \begin{array}{ll} p(p-1)(p+1)/6 & \text{if } n = 1, \\ (p-1)(p+1)(p+3)(3p-1)/192 & \text{if } n = 2, \\ (p-1)^2(p+1)(5p+9)/192 & \text{if } n = 3, \\ (p-1)(p+1)(3p^2+2p-9)/96 & \text{if } n = 4, \\ (p-3)(p-1)(p+1)(3p-1)/96 & \text{if } n = 5, \\ (p-3)(p-1)(p+1)(5p-1)/384 & \text{if } n = 6, \\ (p-3)(p-1)(p+1)(7p-3)/384 & \text{if } n = 7, \\ (p-1)^2(p+1)^2/64 & \text{if } n = 8, \\ (p-1)^2(p+1)(p-3)/96 & \text{if } n = 9, \\ (p-1)^2(p+1)(p-3)/196 & \text{if } n = 10. \end{array} \right.$$

Finally, since $B_n \cap B_m = \emptyset$ for $n \neq m$, the cardinality of set B is $\frac{p(p+1)(p-1)(3p-2)}{96}$. $\square$

Lemma A.3.5. *If p is a prime number, then the cardinality of the set*

$$A = \left\{ (i, j) \in \mathbb{N}^2 : 1 \leq i \leq j \leq p^2 + p \text{ and } \begin{pmatrix} j(p-1) \\ i(p-1) \end{pmatrix} \not\equiv 0 \pmod{p} \right\}$$

is $\frac{p(p+1)(p^2+p+10)}{8}$.

Proof. Note that if $(i, j) \in A$ then $j = p^2 + p$, $j = p^2 + a_0$ or $j = a_1p + a_0$, where $0 \leq a_1, a_0 \leq p-1$. Moreover, we have $i = p^2 + p$, $i = p^2 + b_0$ or $i = b_1p + b_0$, where $0 \leq b_1, b_0 \leq p-1$. Thus,

$$j(p-1) = \left\{ \begin{array}{ll} \left\{ \begin{array}{ll} (a_1-1)p^2 + (p-a_1)p & \text{if } 0 = a_0 < a_1, \\ a_1p^2 + (a_0-a_1-1)p + (p-a_0) & \text{if } a_1+1 \leq a_0, \\ (a_1-1)p^2 + (p+a_0-a_1-1)p + (p-a_0) & \text{if } 1 \leq a_0 \leq a_1, \end{array} \right. & \text{if } 1 \leq j \leq p^2-1, \\ \left\{ \begin{array}{ll} (p-1)p^2 & \text{if } a_0 = 0, \\ (p-1)p^2 + (a_0-1)p + (p-a_0) & \text{if } a_0 \neq 0, \end{array} \right. & \text{if } p^2 \leq j < p^2+p, \\ \left\{ (p-1)p^2 + (p-1)p \right. & \text{if } j = p^2+p, \end{array} \right.$$

and

$$i(p-1) = \begin{cases} \begin{cases} (b_1-1)p^2 + (p-b_1)p & \text{if } b_0 = 0, \\ b_1p^2 + (b_0-b_1-1)p + (p-b_0) & \text{if } b_1+1 \leq b_0, \\ (b_1-1)p^2 + (p+b_0-b_1-1)p + (p-b_0) & \text{if } 1 \leq b_0 \leq b_1, \end{cases} & \text{if } 1 \leq j \leq p^2-1, \\ \begin{cases} (p-1)p^2 & \text{if } b_0 = 0, \\ (p-1)p^2 + (b_0-1)p + (p-b_0) & \text{if } b_0 \neq 0, \end{cases} & \text{if } p^2 \leq j < p^2+p, \\ \begin{cases} (p-1)p^2 + (p-1)p & \end{cases} & \text{if } i = p^2+p. \end{cases}$$

Now, it follows from Lucas's Theorem that $A = \bigcup_{n=1}^{11} A_n$, where

$$A_1 = \{(a_1p, a_1p) \in \mathbb{N}^2 : 1 \leq a_1 \leq p-1\},$$

$$A_2 = \{(a_1p+a_0, a_1p+a_0) \in \mathbb{N}^2 : 1 \leq a_1 < a_0 \leq p-1\},$$

$$A_3 = \{(b_1p, a_1p+a_0) \in \mathbb{N}^2 : 1 \leq a_0 \leq a_1 \leq p-1, a_1-a_0+1 \leq b_1 \leq a_1\},$$

$$A_4 = \left\{ (b_1p+b_0, a_1p+a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq a_1 \leq p-1 \\ 0 \leq b_1 \leq a_1-1 \end{array}, \begin{array}{l} a_0 \leq b_0 \leq p-1 \\ -p-a_0+a_1+b_0 \leq b_1 \leq b_0-1 \end{array} \right\},$$

$$A_5 = \{(a_1p+a_0, a_1p+a_0) \in \mathbb{N}^2 : 1 \leq a_0 \leq a_1 \leq p-1\},$$

$$A_6 = \left\{ (b_1p, p^2+a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq p-1 \\ 1 \leq b_1 \leq p-1 \end{array}, p+1 \leq a_0+b_1 \right\},$$

$$A_7 = \left\{ (b_1p+b_0, p^2+a_0) \in \mathbb{N}^2 : \begin{array}{l} 1 \leq a_0 \leq p-1 \\ 0 \leq b_1 \leq p-1 \end{array}, \begin{array}{l} b_1+1 \leq b_0 \leq p-1 \\ a_0 \leq b_0 \leq a_0+b_1 \end{array} \right\},$$

$$A_8 = \{(p^2+a_0, p^2+a_0) \in \mathbb{N}^2 : 1 \leq a_0 \leq p-1\},$$

$$A_9 = \{(p^2, p^2+a_0) \in \mathbb{N}^2 : 1 \leq a_0 \leq p-1\},$$

$$A_{10} = \{(b_1p+b_1, p^2+p) \in \mathbb{N}^2 : 1 \leq b_1 \leq p-1\},$$

$$A_{11} = \{(p^2, p^2), (p^2, p^2+p), (p^2+p, p^2+p)\}.$$

Finally, it follows from Lemmas ?? and ?? that the cardinality of B_n is

$$\left\{ \begin{array}{ll} p-1 & \text{if } n=1, \\ p(p-1)/2 & \text{if } n=2, \\ p(p-1)(p+1)/6 & \text{if } n=3, \\ p(p-1)(p+1)(3p-2)/96 & \text{if } n=4, \\ p(p-1)/2 & \text{if } n=5, \\ (p-2)(p-1)/2 & \text{if } n=6, \\ p(p-1)(p+1)/6 & \text{if } n=7, \\ p-1 & \text{if } n=8, \\ p-1 & \text{if } n=9, \\ p-1 & \text{if } n=10, \\ 3 & \text{if } n=11. \end{array} \right.$$

Therefore, since $A_n \cap A_m = \emptyset$ for $n \neq m$, the cardinality of set A is $\frac{p(p+1)(p^2+p+10)}{8}$.

□