Jamil Ferreira

Sobre corpos de funções algébricas e algumas relações com a criptografia

CAMPINAS

2013

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

JAMIL FERREIRA

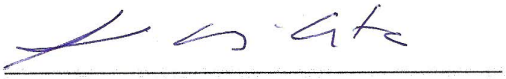
SOBRE CORPOS DE FUNÇÕES ALGÉBRICAS E ALGUMAS RELAÇÕES COM A CRIPTOGRAFIA

Orientadora: Profa. Dra. Sueli Irene Rodrigues Costa

Tese de doutorado apresentada ao Instituto de Matemática, Estatística e Computação Científica da Unicamp para obtenção do título de Doutor em Matemática.

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO JAMIL FERREIRA E ORIENTADA PELA PROFA. DRA. SUELI IRENE RODRIGUES COSTA.

Assinatura da Orientadora



CAMPINAS

2013

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

F413s

Ferreira, Jamil, 1956-
Sobre corpos de funções algébricas e algumas relações com a criptografia / Jamil Ferreira. – Campinas, SP : [s.n.], 2013.

Orientador: Sueli Irene Rodrigues Costa.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

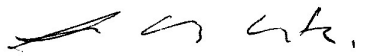
1. Corpos de funções algébricas. 2. Número de classes de divisores. 3. Corpos de funções hiperelípticos. 4. Criptografia. I. Costa, Sueli Irene Rodrigues,1949-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: On algebraic function fields and some relations with cryptography
Palavras-chave em inglês:
Algebraic function fields
Divisor class number
Hyperellyptic function fields
Cryptography
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Sueli Irene Rodrigues Costa [Orientador]
Cícero Fernandes de Carvalho
Jeroen Antonius Maria van de Graaf
Paulo Roberto Brumatti
Valmecir Antônio dos Santos Bayer
Data de defesa: 02-07-2013
Programa de Pós-Graduação: Matemática

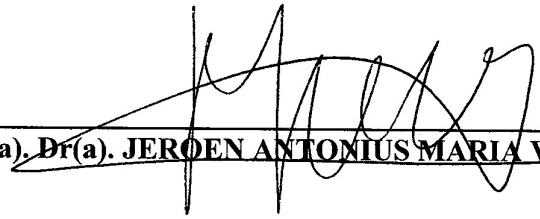
Tese de Doutorado defendida em 02 de julho de 2013 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

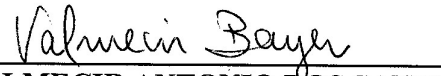


Prof(a). Dr(a). SUELI IRENE RODRIGUES COSTA

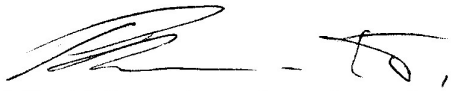
Prof(a). Dr(a). CÍCERO FERNANDES DE CARVALHO



Prof(a). Dr(a). JEROEN ANTONIUS MARIA VAN DE GRAAF



Prof(a). Dr(a). VALMECIR ANTONIO DOS SANTOS BAYER



Prof(a). Dr(a). PAULO ROBERTO BRUMATTI

Ao Bloco Carnavalesco *"Custa Mas Vai"*, da minha cidade natal, São João del-Rei.

Agradecimentos

A jornada que resultou nesta tese teve a participação positiva de pessoas e entidades, sem as quais ela não lograria êxito. Aquelas que mais diretamente participaram desta longa aventura foram, em primeiro lugar, minha orientadora Sueli Costa, que aceitou orientar-me na sua área atual de pesquisa, teoria da informação, ainda como estudante especial e, dessa forma, permitiu que eu compatibilizasse minhas atividades docentes com os estudos e pesquisas de doutorado. Sueli manteve-se, durante todo o período após meu retorno ao IMECC, depois de vinte anos, orientadora, colega e exemplo de pesquisadora. Com ela, tive a liberdade de estudar e pesquisar, sem qualquer tipo de pressão, tópicos que me atraíram, mesmo que não diretamente ligados às especificidades de sua pesquisa.

De grande importância para minha formação matemática foram também: meu orientador no Programa de Doutorado em Matemática da *S.U.N.Y. at Binghamton*, Alex Feingold, com quem estudei teoria de representação de álgebras de Kac-Moody, embora, infelizmente, após cumprir todos os créditos do Programa e o exame de qualificação nessa área, em 1997, encontrei uma obstrução na tese que, por erros estratégicos meus, acabou por não ser concluída; meu orientador de mestrado no IMECC e primeiro orientador de doutorado, Richard Pfister, com quem comecei a estudar álgebras de Kac-Moody, cujo programa interrompi em 1989, com o início das minhas atividades docentes no Departamento de Matemática da UFES, onde, em 1994, obtive o incentivo dos colegas para retomar meu doutorado no Exterior.

Do lado institucional, foram decisivos os apoios: da Coordenação de Pós-Graduação do IMECC

por ter aceito minha readmissão ao programa de doutorado como aluno regular; de vários professores do IMECC, especialmente, Rodney Bassanezzi; dos funcionários da Secretaria de Pós-Graduação, Tânia, Lívia e Ednaldo, pela paciente assistência nos itens burocráticos; dos professores que gentilmente aceitaram compor a banca; da Pró-Reitoria de Pesquisa da UFOP, pelo auxílio financeiro para deslocamento durante meus estudos na UNICAMP; daqueles colegas do DEMAT-UFOP que manifestaram em atitudes profissionais seu entendimento de que a dedicação ao doutorado é um trabalho de pesquisa.

Finalmente, as bolsas do CNPq e CAPES em meu primeiro ingresso no Doutorado na UNICAMP foram de extrema valia, bem como a bolsa da CAPES para meus estudos no Exterior, conforme manifestei expontaneamente em meus relatórios de estudos na ocasião. É de fundamental importância para o árduo trabalho de pesquisa do doutorando que, apesar de seu esforço, não concluir seu programa durante a vigência da bolsa, a continuidade do apoio da CAPES, não mais em termos financeiros, mas na demonstração de confiança e solidariedade para com a iniciativa de cunho científico do pesquisador, itens fundamentais para o equilíbrio emocional e consequente sucesso num projeto de risco como é um programa de doutorado em matemática.

Agradeço ainda ao meu amigo Otacílio Ricardo pela fundamental assistência no LaTeX.

Todo esse apoio técnico foi fundamentalmente fortalecido nesses longos anos pelo convívio com amigos, parentes ou não, cuja extensa lista de nomes omito, sem receio de ressentimentos. Foram eles que me ajudaram a não deixar a peteca cair.

Ninguém é mais do que aprendiz

de tudo quanto a vida apronta

eu não acredito em quem diz

que encara esta vida e não se amedronta

...

Vive sem defesa a criatura

À mercê da loucura

E à procura de paz

Porém eu não reclamo dessa aventura

Sinceramente me satisfaz

*(`Aventura` - **Mauro Duarte e Paulo César Pinheiro**)*

Resumo

O número de classes de divisores de grau zero, h, de corpos de funções algébricas elípticos e hiperelípticos desempenha papel importante nos esquemas criptográficos baseados em curvas elípticas e hiperelípticas. Nesse contexto, h é um número grande e é usualmente procurado por meio de algoritmos (*baby step - giant step*, por exemplo) em um intervalo de números reais obtido após um truncamento no produto infinito de Euler da função zeta do corpo de funções. Tendo a desigualdade de Hasse-Weil como motivação, encontramos identidades finitas para h que são também explícitas no sentido de que seus custos computacionais são diretamente deduzíveis dessas identidades. Como consequência, obtivemos também identidades finitas e explícitas para os coeficientes a_i do L-polinômio da função zeta. Ferramentas fundamentais nesta pesquisa foram as L-séries de Artin e outros resultados envolvendo os símbolos polinomiais de Legendre.

Abstract

The divisor class number of degree zero, h, of elliptic and hyperelliptic function fields plays an important role in cryptographic schemes based on elliptic and hyperelliptic curves. In this context, h is a large number and it is usually searched by means of algorithms (baby step - giant step, for example) in an interval of real numbers obtained after truncating the infinit Euler product coming from the zeta function of the function field. Taking the Hasse-Weil inequality as motivation, we derived finite identities for h which are also explicit in the sense that their computational costs are straightforwardly derivable from these identities. We also obtained finite and explicit identities for the coefficients a_i of the L-polynomialof the zeta function. Fundamental tools for this research were the Artin L-series and other results involving the Legendre polynomial symbols.

Sumário

Capítulo 1

Introdução e motivação

1.1 Motivação

O tema deste trabalho foi gerado principalmente durante os seminários de Teoria da Informação, coordenado pela minha orientadora Professora Sueli I. R. Costa, a partir do qual pude identificar a álgebra e outras áreas da matemática pura como ferramentas fundamentais na Teoria dos Códigos Corretores de Erros e em Criptografia. Envolvi-me, em particular, no estudo da teoria dos corpos de funções algébricas, motivado pelo potencial de aplicabilidade dessa teoria, tanto quanto pela curiosidade em estudá-la. Vale ressaltar a correspondência entre corpos de funções algébricas F e curvas projetivas não singulares C, de modo que os *lugares* de F (veja Capítulo 2) estão em bijeção com os pontos de C. Assim, todo o tratamento algébrico pelo qual optamos neste trabalho possui sua contrapartida geométrica, conforme [19], [24] ou [16].

De importância fundamental para este trabalho, foram os resultados contidos nos artigos de Stein, Teske e Scheidler ([23] e [21]) e de Michael Rosen [9], nos quais percebemos a viabilidade de uma *identidade finita e explícita* - (IFE) para h, o *número de classes de divisores de grau zero* de certos corpos de funções algébricas. O termo "*explícita*" refere-se ao fato de que o custo computacional da identidade é deduzível imediatamente da própria expressão da identidade através

da contagem dos polinômios nela envolvidos.

A ordem h do grupo de classes de divisores de grau 0 em corpos elípticos e hiperelípticos de funções algébricas desempenha importante papel nos sistemas criptográficos baseados nesses corpos ([16], [19], [23]), conforme comentaremos no Capítulo 3. Uma identidade infinita de h dada pela produtória de Euler vem sendo utilizada desde 1999 por pesquisadores como, por exemplo, Stein, Teske, Scheidler ([21], [23], [22]). Seu método consiste em aplicar um truncamento num certo nível da produtória infinita de Euler, produzir um intervalo real que contém h e aplicar métodos algorítmicos (*baby-step giant-step* ou *Pollard's kangaroo*) para identificar h nesse intervalo ([23]).

Por outro lado, a desigualdade de Hasse-Weil,

$$(q^{\frac{1}{2}} - 1)^{2g} \leq h(F) \leq (q^{\frac{1}{2}} + 1)^{2g},$$

fornece a ordem de grandeza q^g para h de corpos de funções algébricas $F/\mathbb{F}_q$ de gênero g, q potência de um primo ímpar, bem como uma estimativa para h, em termos de uma expansão quase $q-$ária com coeficientes da ordem de grandeza $q^{1/2}$, como se vê facilmente expandindo-se os extremos dessa desigualdade. Tendo essas observações como motivação, buscamos uma Identidade Finita e Explícita (IFE) para h, em termos de uma expansão quase q-ária da ordem de q^g.

O L-polinômio calculado em 1 fornece h como soma de seus coeficientes, $a_0 + a_1 + \cdots + a_{2g}$, mas os cálculos dos a_i's dependem dos lugares N_j, $j \leq i$ (veja [19]), que dependem dos inversos das raízes do L-polinômio, que dependem dos a_i, fechando-se um círculo em que as expressões para esses invariantes não apresentam complexidade explícita. Estamos em busca de uma expressão finita e explícita para os a_i, portanto para h, independente de N_j ou das raízes do L-polinômio e que seja efetivamente computável. Nessa busca, percebemos, no artigo de Michael Rosen ([9]), a possibilidade de adaptar a L-série de Artin - que envolve originalmente a ordem h_B do grupo de Picard da ordem maximal B de extensões quadráticas de $F_q(t)$ - para expressões que fornecem uma identidade finita e explícita para o número de classes h da extensão.

Essa L-série adaptada não apenas oferece uma identidade finita e explícita para h, mas, ana-

lisada em conjunto com o L-polinômio obtido da função zeta da extensão e um teorema de Stein, Teske e Scheidler ([23], [21]), permite obter relações entre os coeficientes do L-polinômio e as somas M_i dos símbolos de Legendre polinomiais sobre os polinômios mônicos. O custo desses cálculos é imediato das expressões encontradas, o que permite avaliar sua viabilidade em sistemas criptográficos.

Para compreender e relacionar essas informações, foi necessário estudar a teoria básica de corpos de funções algébricas e obter uma noção de como ela se relaciona com a criptografia. As referências principais para essa teoria são [16], [19] e [24].

Esta tese tem, portanto, como um dos objetivos estudar a obstrução envolvida na substituição da estimativa dada pela desigualdade de Hasse-Weil acima por uma igualdade. Em outras palavras, perguntamos qual a obstrução para que $log_q h = g$. Respondemos com uma IFE para h, na forma de uma soma $h = q^g + c_{g-1}q^{g-1} + ... + c_1 q^1 + c_0$, com os respectivos custos das parcelas explícitos nas mesmas.

Uma palavra sobre notação assintótica e complexidade computacional antes de prosseguir. O *custo* da IFE de h, que definiremos oportunamente no Capítulo 4 como sendo o número de polinômios requisitados para o cálculo de h através dessa IFE, será denotado por $\mathrm{Cpx}(h)$. A razão é que esse número de polinômios se mostrará claramente fundamental para a avaliação da complexidade computacional envolvida.

Estamos adotando aqui a usual notação assintótica segundo a qual uma função positiva de variável natural $g(n)$ se diz da ordem de $f(n)$, também positiva, o que se denota por $g(n) = \mathcal{O}(f(n))$ ou $g(n) \in \mathcal{O}(f(n))$ ou ainda $\mathrm{Grz}(g(n)) = \mathcal{O}(f(n))$, se existe $c > 0$ tal que $g(n) \leq cf(n)$, para todo n suficientemente grande. Em contextos de análise de algoritmos, considera-se f como a função "ótima" satisfazendo a desigualdade anterior, no sentido de ser o limite superior menor possível para g, ou seja, comete-se um certo abuso de linguagem ao utilizar-se a notação $\mathcal{O}(f)$ para o que deveria ser denotado mais precisamente por $\Theta(f)$, que significa existirem constantes

positivas c e d tais que $c \cdot f(n) \leq g(n) \leq d \cdot f(n)$, para todo n suficientemente grande.

Dessa forma, o custo da IFE de h acima mencionada mostrou-se como $\mathrm{Cpx}(h) = \mathcal{O}(q^g)$, que é igual à sua ordem de grandeza $\mathrm{Grz}(h)$.

Outras expressões finitas e explícitas poderão ter custo maior ou menor. Fica aberta a questão de saber qual é a obstrução mínima, ou o custo mínimo, para se expressar h finitamente e explicitamente. Para a criptografia interessa saber qual a complexidade de uma IFE, uma vez que já utiliza rotineiramente uma identidade infinita, portanto, com obstrução ou custo infinito, truncada em um certo nível com complexidade $\mathrm{Cpx}(h)$ menor do que q^g, conforme comentaremos na próxima seção, tendo como base o artigo de A. Stein e E. Teske [23].

O método que utilizamos para o cálculo da IFE de h utiliza a L-série de Artin, diferentemente do método usualmente utilizado, principalmente por A. Stein, R. Scheidler e E. Teske ([23], [21]), entre outros, como mencionamos acima.

Obtivemos também IFE´s para os coeficientes a_i do $L-$polinômio da função zeta de K, bem como para o número N_1 de *lugares* (tradução para o português do termo "place") de grau 1, todas em função das somas dos símbolos polinomiais de Legendre de ordem 2. O custo $\mathrm{Cpx}(h) = q^g$ obtido para a IFE de h em nosso método é maior do que a complexidade obtida na criptografia atual, mas não depende de truncamento de produtória infinita e de algoritmos de busca de um inteiro em um intervalo. Esse custo relativamente alto de nossa IFE em relação ao obtido na criptografia atual sugere que seja esta a razão pela qual a criptografia vem utilizando identidade infinita, sem mencionar, em geral, a impraticabilidade das IFE´s de h e sem utilizá-las sistematicamente. Embora a determinação de h por aproximações algorítmicas possa ser, em geral, mais econômica para a critptografia, há situações em que IFE´s são úteis ([10]), além de interessantes por si mesmas. Essa conjectura implica que, nas situações em que $\mathrm{Cpx}(h) = q^g$ for computacionalmente impraticável, truncamentos e algoritmos serão necessários para custos menores de obtenção de h e poderão ser comparados com os advindos dos algoritmos atuais que partem de identidades

infinitas.

A desigualdade de Hasse-Weil

$$\left(1-\frac{2}{\sqrt{q}}+\frac{1}{q}\right)^{g} \leq \frac{h}{q^{g}} \leq \left(1+\frac{2}{\sqrt{q}}+\frac{1}{q}\right)^{g}$$

decorre da Hipótese de Riemann para Corpos de Funções, ou Teorema de Hasse-Weil, conforme estudaremos no Capítulo 2. Ela fornece as estimativas

$$q^{g}\left(1-\frac{2}{\sqrt{q}}+\frac{1}{q}\right)^{g} \leq h \leq q^{g}\left(1+\frac{2}{\sqrt{q}}+\frac{1}{q}\right)^{g}$$

ou

$$(q-2\sqrt{q}+1)^{g} \leq h \leq (q+2\sqrt{q}+1)^{g}$$

para o número h de classes dos divisores de extensões finitas de

$$K=\mathbb{F}_{q}(x),$$

onde $q=p^{n}$, p primo ímpar em todo este trabalho.

Por outro lado, ela implica, é claro, que $h \approx q^{g}$, isto é, h é assintoticamente da ordem $O(q^{g})$. Entretanto, como se trata de um número muito grande, que tende ao infinito conforme q tende ao infinito, não é fácil determinar precisamente uma IFE de h. As IFE´s que apresentaremos no Capítulo 4 exibem parcelas de ordem menor do tipo, $c_{j}q^{j}$, $j=0,\cdots,g-1$, como sugerido pela desigualdade de Hasse-Weil, conforme veremos adiante.

Definição 1.1.1. Uma expressão para h do tipo $h=q^{g}+c_{g-1}q^{g-1}+...+c_{1}q^{1}+c_{0}$ será chamada de **expansão quase q-ária de h.**

Observamos que expansões *quase* q-árias não são únicas como se pode ver facilmente por analogia com o sistema decimal ou pela desigualdade de Hasse-Weil, onde há duas expansões *quase* q-árias próximas de h.

O inteiro h pertence ao intervalo

$$\left[(q-2\sqrt{q}+1)^g, (q+2\sqrt{q}+1)^g\right],$$

para todo q e g, e, conforme $q \to \infty$, h "se aproxima assintoticamente" de q^g no sentido de que $\left(1-\sqrt{q}\right)^{2g} = \mathcal{O}(q^g) = \left(1+\sqrt{q}\right)^{2g}$. Assim, dizemos que o inteiro h é assintoticamente próximo de

$$(q-2\sqrt{q}+1)^g \text{ e de } (q+2\sqrt{q}+1)^g,$$

conforme $q \to \infty$. Portanto, duas expansões *quase* q-árias se aproximam de h assintoticamente.

Por exemplo, para $g = 1$, temos:

$$q^1 - (2\sqrt{q}+1) \approx h \approx q^1 + (2\sqrt{q}+1),$$

$$= q^1 + c_0 = q + \mathcal{O}\left(q^{\frac{1}{2}}\right)$$

com $c_i = \mathcal{O}\left(q^{\frac{1}{2}}\right)$, $i = 0 = g-1$.

Para $g = 2$, temos:

$$q^2 - 4q\sqrt{q} + 6q - 4\sqrt{q} + 1 \approx h \approx q^2 + 4q\sqrt{q} + 6q + 4\sqrt{q} + 1 =$$

$$= q^2 + (4\sqrt{q}+6)\, q + (4\sqrt{q}+1)$$

$$\approx q^2 + \mathcal{O}\left(\sqrt{q}\right) q^1 + \mathcal{O}\left(\sqrt{q}\right)$$

$$= q^2 + c_1 q^1 + c_0,$$

onde $c_i = \mathcal{O}\left(q^{\frac{1}{2}}\right)$, $i = 0, 1 = g-1$.

Para $g = 3$, cálculos análogos mostram que

$$h \approx q^3 + c_2 q^2 + c_1 q^1 + c_0,$$

onde $c_i = \mathcal{O}\left(q^{\frac{1}{2}}\right)$, $i = 0, 1, 2 = g-1$.

Assim, vemos que, assintoticamente, e de um modo geral, os invariantes que formam os coeficientes *quase* q-ários de h para gênero g são c_i de ordem $\mathcal{O}\left(q^{\frac{1}{2}}\right)$. Ou seja,

$$h \approx q^g + c_{g-1}q^{g-1} + ... + c_1q^1 + c_0,$$

com

$$c_i = \mathcal{O}\left(q^{\frac{1}{2}}\right), 0 \leq i \leq g-1.$$

Essa aproximação assintótica para h motivou a busca por uma expressão quase $q-$ária para h nos termos da definição anterior e satisfazendo a mesma relação de ordem de grandeza sobre os coeficientes c_j, $j = 0, 1, \cdots, g-1$, isto é, $\mathrm{Grz}\,(c_j) = \mathcal{O}\left(q^{\frac{1}{2}}\right)$. Encontramos ainda $\mathrm{Cpx}(c_j) \leq \mathcal{O}(q^g)$.

Essa análise foi feita para extensões de $K = \mathbb{F}_q(x)$ do tipo $K(\sqrt{D})$, onde D é um polinômio mônico irredutível de grau d sobre K, em que $3 \leq d \leq 8$, ou seja, para os casos de extensões elípticas ($g = 1$) e hiperelípticas de gênero $g = 2$ e $g = 3$ que interessam para a criptografia [16].

1.2 Identidade infinita do número h de classes de divisores

Uma identidade infinita de h dada pela produtória de Euler vem sendo utilizada desde 1999 por pesquisadores como, por exemplo, Stein-Teske [23]. Seu método consiste em aplicar um truncamento num certo nível λ da produtória infinita, majorar o produto infinito recortado, produzir um intervalo real do tipo $(E - L^2, E + L^2)$ que contém h, com L tão pequeno quanto possível, e aplicar um algoritmo para a identificação de h nesse intervalo. A complexidade computacional desse método é $\mathcal{O}\left(q^{1/4}\right)$ e $\mathcal{O}\left(q^{3/4}\right)$, para $g = 1$ e $g = 2$, respectivamente. Para $g \geq 3$, obtem-se complexidade $\mathcal{O}\left(q^{\left(\frac{2g-1}{5}\right)}\right)$, de onde se segue, por exemplo, que para $g = 3$, obtem-se $\mathcal{O}\,(q)$. Notemos que h não é identificado nesse caso por uma IFE.

Nossos cálculos para os casos citados sugerem a conjectura de que, em geral, tem-se

$$\mathrm{Grz}\,(c_i) = \mathcal{O}\left(q^{\frac{1}{2}}\right) \text{ e } \mathrm{Cpx}\,(c_i) \leq \mathcal{O}(q^g),$$

onde os coeficientes c_i´s são IFE´s e $h = q^g + c_{g-1}q^{g-1} + ... + c_1 q^1 + c_0$. De passagem, conjecturamos que $\mathrm{Cpx}(h) \geq \mathcal{O}(q^g)$, para qualquer que seja a IFE que o represente, com base nas evidências de nossos cálculos para $g = 1, 2, 3$ e $3 \leq d \leq 8$. Esta conjectura explicaria por que a criptografia vem recorrendo até o presente momento a algoritmos para a obtenção de h com $\mathrm{Cpx}(h) < \mathcal{O}(q^g)$.

1.3 IFE do número h de classes de divisores pela L-série de Artin

Se o gênero de uma extensão finita de $\mathbb{F}_q(x)$ é g, então a desigualdade de Hasse-Weil implica que a ordem de grandeza de h é $\mathcal{O}(q^g)$. Entretanto, qual é, precisamente, a identificação desse inteiro h?

Uma IFE de h poderia revelar propriedades úteis, por exemplo, a paridade de h, antes de qualquer cálculo, pelo mero exame dessa IFE, o que não é possível no procedimento de Stein-Teske que precisa esperar o fim do algoritmo de busca.

O *handbook* de criptografia com curvas elípticas e hiperelípticas ([2], página 135, ver também [19], página 230) exibe a fórmula

$$N_k = q^k + 1 - \sum_{i=1}^{2g} {\omega_i}^k$$

para o número de pontos da curva projetiva não singular associada à curva afim $Y^2 = D(x)$ sobre $\mathbb{F}_{q^k}$. Os ω_i´s são as inversos das raízes do $L-$polinômio. Notemos que $N_1 = q^1 + 1 - \sum_{i=1}^{2g} {\omega_i}^1$ constitui uma IFE para o primeiro coeficiente $a_1 = -\sum_{i=1}^{2g} {\omega_i}^1$ do $L-$polinômio. Em [19], página 230, encontramos uma IFE para a_j, por indução dependente de $N_k, 1 \leq k \leq j$, e $a_i, 1 \leq i \leq j-1$. A complexidade de a_j nessa IFE é dada por $\mathrm{Cpx}(a_j) = \mathrm{Cpx}(N_j) = O(q^j)$, porque há q^j pontos para a determinação dos pontos da curva projetiva associada à curva afim $Y^2 = D(x)$ sobre $\mathbb{F}_{q^j}$. Logo, tal IFE não traz vantagens em termos computacionais sobre a nossa. Existem algoritmos eficientes que diminuem tal complexidade ([2]) para o cálculo de a_j, mas não afetam a complexidade de suas

IFE´s.

Nesta tese oferecemos uma nova IFE para h, baseada na comparação de duas outras identidades finitas (IF) de h, sendo uma delas explícita, aquela que será adaptada da L-série de Artin de 1924, que se referia ao grupo de Picard de ordens, e aplicada ao grupo de divisores de grau zero em extensões quadráticas de corpos de funções racionais do tipo $K = F_q(x)\left(D^{1/2}\right)$. Mais precisamente, no Capítulo 4 mostraremos que:

Se D é um polinômio de grau d, indicado por $\deg(D) = d$, *livre de quadrados em* $F_q[x]$, *uma identificação finita e explícita de h em extensões quadráticas* $F_q(x)\left(D^{1/2}\right)$ *de corpos de funções é dada pela L-série de Artin de 1924 adaptada ao número h de classes de divisores.*

A outra IF é dada pelo polinômio L da função *zeta* de K. Comparando as duas IF´s de h e utilizando as fórmulas de Stein-Teske-Scheidler para gênero $g \geq 1$, estaremos aptos a obter IFE´s para os coeficientes a_i de L como funções de q e das somas M_i de símbolos de Legendre polinomiais. Esses símbolos também determinam a L-série de Artin adaptada. Ao mesmo tempo, mostraremos que metade destes coeficientes, $M_{g+i}, 1 \leq i \leq g$, cujas IFE´s teriam custo em princípio da ordem de q^{g+i}, possuem, na verdade, custo menor ou igual a $\mathcal{O}(q^g)$.

Observamos que não há na literatura (p. ex., [2], [19], [16], [18], [24]) IFE´s para a_i em função de invariantes elementares e computáveis. Portanto, as IFE´s que apresentaremos no Capítulo 4 parecem ser inéditas.

Mais precisamente, investigamos aqui as parcelas de h da forma $\mathcal{O}\left(\sqrt{q}\right) q^{g-i}$, que dão uma expansão *quase* q-ária de h que se aproxima de q^g no intervalo

$$[\left(q - 2q^{1/2} + 1\right)^g, \left(q + 2q^{1/2} + 1\right)^g].$$

Os coeficientes de uma certa expansão *quase* q-ária de h são invariantes determinados pelas somas de símbolos de Legendre polinomiais, mas suas expressões explícitas estão em aberto, exceto para

certos i's com $3 \leq d \leq 8$, que abordamos aqui.

Em outras palavras, esta tese se preocupa com a pergunta: o que se pode dizer dos coeficientes de uma expansão *quase* q-ária de h, invariantes de $K = F_q(x)\left(D^{1/2}\right)$, além do fato de que eles fornecem uma alternativa ao truncamento da produtória infinita de Euler? IFE´s não carregam, em princípio, o custo de terem de se aliar a algoritmos de busca de um inteiro em um intervalo, procedimento dominante até o presente em criptografia sobre corpos de funções algébricas. Por outro lado, apresentam complexidade maior para determinar h.

Em vista do fato de que existe uma IF para h, dada pelo L-polinômio, cujos coeficientes inteiros não possuem IFE´s na literatura disponível com complexidade menor do que q^i, como já observamos, esta tese também tem como objetivo responder à pergunta: que propriedades possuem as somas M_i de símbolos de Legendre polinomiais, além de fornecerem uma IFE para h, revelando-se assim importantes invariantes do corpo de funções subjacente, e que relação há entre as duas IFE´s?

A questão de saber se é necessário um algoritmo, análogo aos algoritmos Schank´s baby-step giant-step e Pollard´s kangoroo, de busca em um certo intervalo real previamente determinado por truncamento de uma IFE de h, se quisermos diminuir a complexidade de determinação de h por meio de uma IFE, não é tratada aqui por limitação de tempo e de espaço. Nossa conjectura é que IFE´s podem ser truncadas e os algoritmos usuais podem ser aplicados para se obter h com complexidade menor do que $\mathcal{O}(q^g)$, analogamente ao truncamento que a criptografia contemporânea realiza na produtória infinita de Euler. Se a eficiência obtida será melhor do que a de Stein-Teske só a pesquisa poderá responder.

No Capítulo 4, nossa tarefa será, portanto, investigar os invariantes c_i que aparecem como coeficientes *quase q-ários* de h e qual a complexidade com que a L-série de Artin fornece uma IFE para h.

Os coeficientes quase q-ários c_i de h são determinados por somas M_i de símbolos $\chi(M)$ de

Legendre polinomiais, a serem definidos no Capítulo 4.

Demonstraremos no Capítulo 4 o teorema seguinte:

TEOREMA 1.3.1 (Decomposição *quase* q-ária de h). *Se* $F = \mathbb{F}_q(t)\sqrt{D}$, *onde* D *é um polinômio irredutível em* $\mathbb{F}_q[t]$ *de grau* d, *então* h *admite uma decomposição quase* q*-ária*

$$h = q^g + c_{g-1}q^{g-1} + ... + c_1q^1 + c_0 = L(1),$$

tal que $c_i = \mathcal{O}\left(q^{\frac{1}{2}}\right)$ *e* $Cpx(c_i) \leq \mathcal{O}(q^g)$, *para todo* $0 \leq i \leq g-1$, $3 \leq d \leq 8$.

A demonstração deste teorema será por meio de um cálculo direto comparando-se a L-série de Artin adaptada e o polinômio L, não ficando claro se existe um argumento geral para qualquer $d > 8$. Entretanto, é plausível que sempre exista um tal cálculo análogo para cada grau d, nos termos da conjectura seguinte.

CONJECTURA 1.3.2. h *admite uma decomposição quase* q*-ária*

$$h = q^g + c_{g-1}q^{g-1} + ... + c_1q^1 + c_0,$$

tal que $c_i = \mathcal{O}\left(q^{\frac{1}{2}}\right)$ *e* $\mathcal{O}(q^g) \geq Cpx(c_i)$ *para todo* $0 \leq i \leq g-1$.

Uma observação crucial é que, enquanto a identificação de Stein-Teske é uma identidade infinita de somas I_i sobre polinômios mônicos irredutíveis, a soma finita de Artin oferece uma IFE por meio de somas M_i de símbolos de Legendre polinomiais sobre polinômios mônicos.

A comparação da IF de h dada pelo $L-$polinômio com a IFE de h da nossa adaptação da L-série de Artin fornecerá uma IFE de h envolvendo apenas as somas M_i de símbolos de Legendre polinomiais.

Portanto, as partições $d_1 + ... + d_k = i$ do grau i em graus d_j de polinômios m_j mônicos irredutíveis que fatoram os mônicos M_i de grau i compensam, digamos assim, as infinitas parcelas truncadas na série infinita, de somas de símbolos de Legendre polinomiais sobre polinômios

irredutíveis, derivadas da produtória infinita de Euler. Assim, temos a IFE de h nos teoremas acima.

Fórmulas para $M_i := \sum_{\deg(M)=i} \chi(M)$, dos símbolos de Legendre polinomiais, com M mônico, em função de q, g e D são um problema em aberto. Para gênero $g \geq 1$ teremos as fórmulas de Stein-Teske-Scheidler para

$$I_i = \sum_{\deg(M)=i} \chi(M),$$

com M mônico irredutível de grau i, que fornecerão no Capítulo 4, juntamente com outros resultados, boas estimativas de M_i.

Devemos enfatizar que estamos mencionando uma IFE e não uma *aproximação* de h. Para uma aproximação de h, não encontramos uma complexidade menor do que a de Stein-Teske, cujo método, entretanto, não fornece uma expressão explícita para h que o identifique por meio de um número finito de termos computáveis exatamente.

Portanto, essa tese focaliza o problema de uma IFE de h até então inexplorada na literatura disponível, e o problema de saber se tal IFE pode oferecer uma alternativa para o procedimento por truncamento da produtória infinita de Euler obtida por Stein-Teske que exige um algoritmo de busca do inteiro h em um certo intervalo. Neste sentido, ela é também dedicada a motivar e iniciar uma pesquisa mais aprofundada das propriedades das somas invariantes elementares de símbolos de Legendre polinomiais M_i.

A infinita maioria desses invariantes M_i continuará em aberto, porque a dificuldade do problema foge ao escopo de uma única tese, mas alguns dos casos mais importantes para a criptografia são justamente esses em gênero $1, 2$ e 3 [16].

Nosso trabalho foi organizado da seguinte forma:

No Capítulo 2, apresentamos os objetos e resultados clássicos básicos sobre a teoria de corpos de funções algébricas que serão utilizados nos capítulos seguintes.

No Capítulo 3, apresentamos os pilares sobre os quais se apóiam nossos teoremas sobre as IFE's

para h e outros invariantes de certos corpos de funções. Descreveremos a relevância dos corpos de funções elípticos e hiperelípticos em sistemas criptográficos, em particular, o papel do grupo dos divisores de grau 0 e de sua ordem h; construiremos uma identificação finita e explícita de h através de uma adaptação da $L-$ série de Artin de sua tese de 1924 e apresentaremos o teorema de Stein-Teske-Scheidler.

No Capítulo 4, relacionaremos vários dos resultados anteriores para apresentar outra IFE de h e obter expressões efetivamente computáveis para os coeficientes do $L-$ polinômio, envolvendo as somas dos símbolos de Legendre polinomiais.

Finalmente, no último capítulo, faremos os comentários sobre as limitações do nosso trabalho e as perspectivas futuras por ele propiciadas.

Capítulo 2

Preliminares

Neste capítulo, apresentaremos as definições e os resultados básicos sobre corpos de funções algébricas que são de relevância para este trabalho. As referências principais para os tópicos aqui tratados são [24], [19] e [16].

2.1 Corpos de funções algébricas

Definição 2.1.1. Seja k um corpo arbitrário e $k[x]$ o anel de polinômios sobre k na variável x. O corpo de frações $k(x)$ de $k[x]$ se chama **corpo de funções racionais de uma variável** x, abreviado por **CFR**. Qualquer extensão finita K de $k(x)$ se diz um **corpo de funções algébricas de uma variável sobre** k ou simplesmente **corpo de funções**, denotado por K/k e abreviado por **CFA**. O corpo k se chama **corpo de constantes de** K. Consideraremos que o corpo k_a constituído pelos elementos de K que são algébricos sobre k é o próprio k, em cujo caso dizemos que k é o **corpo total de constantes de** K. Nesse caso, se $y \in K \setminus k$, então y é transcendente sobre k.

Exemplo 2.1.1. Seja $k = F_3$ o corpo com três elementos e consideremos $F_3(t)$ e o polinômio $p(y) = y^2 - t \in F_3(t)[y]$. Tomemos a extensão algébrica K de $F_3(t)$ adjuntando a esse corpo uma raiz

$\alpha = \sqrt{t}$ de $p(y)$. Essa extensão é isomorfa a $\frac{F_3(t)[y]}{(p(y))}$ e seus elementos são do tipo $f(t) = a(t)+b(t)\sqrt{t}$, com $a(t)$, $b(t) \in F_3(t)$. Notemos a analogia com o corpo de números $\mathbb{Q}(\sqrt{2})$, extensão quadrática de $\mathbb{Q}$. Notemos ainda que todo elemento de $K \setminus k$ é transcendente sobre k.

Exemplo 2.1.2. Seja $k = \mathbb{Q}$ e consideremos $\mathbb{Q}(t)$ e o polinômio $p(y) = y^2 - 2 \in \mathbb{Q}(t)[y]$. Tomemos a extensão algébrica K de $\mathbb{Q}(t)$ adjuntando a esse corpo uma raiz $\alpha = \sqrt{2}$ de $p(y)$. Essa extensão K não tem k como corpo total de constantes porque $\sqrt{2}$ é algébrico sobre k, pertence a K, mas não a k.

De modo geral, se k_a não for igual a k, um argumento usual da teoria de extensões de corpos mostra que K/k_a é um corpo de funções algébricas (veja [16], pág. 12, Lema 1.5.1.), no qual os elementos de K que são transcendentes sobre sobre k o serão sobre k_a e este será o corpo total de constantes de K/k_a.

2.2 Valorações, anéis de valoração e lugares

Definição 2.2.1. Uma valoração de K/k é uma aplicação $\nu : K \to \mathbb{R} \cup \{\infty\}$ tal que:

1. $\nu(z) = \infty$ se, e somente se, $z = 0$;
2. $\nu(yz) = \nu(y) + \nu(z)$, para todo $y, z \in K$;
3. $\nu(y + z) \geq \min(\nu(y), \nu(z))$, para todo $y, z \in K$;
4. $\nu(K^*) \neq 0$;
5. $\nu(\alpha) = 0$, para todo $\alpha \in k^*$.

Se o conjunto $\nu\{K^*\}$ for discreto, então a valoração ν se diz **discreta**; se $\nu\{K^*\} = \mathbb{Z}$, então ν se diz **normalizada**, abreviada por **VDN**.

Verifica-se que a *desigualdade triangular* formulada em 3. acima é uma igualdade (*desigualdade triangular estrita*) sempre que $\nu(y) \neq \nu(z)$. Além disso, se $k = \mathbb{F}_q$, como $k \setminus \{0\} = k^*$ é um grupo cíclico, segue-se facilmente a validade automática de 5..

Exemplo 2.2.1. No corpo de funções racionais $k(x)$, para um polinômio mônico irredutível $p(x) \in k[x]$, a função $\nu_{p(x)} : k(x) \to \mathbb{Z} \cup \infty$ definida abaixo é uma valoração discreta e normalizada de $k(x)$: se $0 \neq \frac{f(x)}{g(x)} = p(x)^m \frac{f_1(x)}{g_1(x)}$, onde foram retirados os fatores $p(x)$ de $f(x)$ e de $g(x)$, pomos $\nu_{p(x)}(\frac{f(x)}{g(x)}) = m$ e $\nu_{p(x)}(0) = \infty$. Além dessa valoração, temos uma outra VDN de $k(x)$ definida por $\nu_\infty(\frac{f(x)}{g(x)}) = \deg(g(x)) - \deg(f(x))$, se esses polinômios são não nulos, e $\nu_\infty(0) = \infty$.

Provaremos mais adiante que "qualquer valoração do corpo de funções racionais $k(x)$ é discreta e é **equivalente** (veja definição a seguir) a $\nu_{p(x)}$, para algum polinômio mônico irredutível $p(x) \in k(x)$, ou a ν_∞".

Definição 2.2.2. Duas valorações discretas, ν e λ, de K/k se dizem **equivalentes** se existe uma constante $c > 0$ tal que

$$\nu(z) = c\lambda(z), \text{ para todo } z \in K^*.$$

A definição acima produz uma relação de equivalência no conjunto das valorações discretas de K/k. Cada classe de equivalência de valorações discretas se chama um **lugar** de K/k. Se ν é uma valoração discreta de K/k, então $\nu(K^*)$ é um subgrupo discreto de $(\mathbb{R}, +)$, logo, da forma $\nu(K^*) = b\mathbb{Z}$, para algum $b > 0$. Fazendo $c = b^{-1} > 0$, vemos que cada lugar de K/k se identifica com sua única valoração (discreta) normalizada ν_P de K/k, para a qual $\nu_P(K^*) = \mathbb{Z}$.

Observação 2.2.1. O termo "*lugar*", que vem sendo utilizado nos trabalhos da área em português, como em [25], é a tradução do termo em inglês "*place*".

Definição 2.2.3. Dado um lugar P de K/k e um elemento $z \in K^*$, diz-se que P é um **zero** de z se $\nu_P(z) > 0$ e P é um **polo** de z se $\nu_P(z) < 0$. Um elemento $t \in K$ tal que $\nu_P(t) = 1$ se diz **parâmetro local** (ou **uniformizador**) de K no lugar P.

Pomos ainda $\mathcal{O}_P = \{z \in K \,|\nu_P(z) \geq 0\}$ e $M_P = \{z \in K \,|\nu_P(z) > 0\}$. Usando as propriedades de valoração, verifica-se que $\mathcal{O}_P$ é um anel, chamado de **anel de valoração** e que M_P é seu único ideal maximal, denominado o **ideal maximal do lugar** P, que é principal e gerado por qualquer

parâmetro local t, isto é, $M_P = t\mathcal{O}_P$. Além disso, $\mathcal{O}_P$ é principal e seus ideais são do tipo $t^m\mathcal{O}_P$, para $m \in \mathbb{N}$.

Exemplo 2.2.2. Consideremos o CFR $k(x)$ e o lugar $P = p(x) = x + 1$. Os elementos de $k(x)$ que têm P como zero são precisamente as frações irredutíveis $\frac{f(x)}{g(x)}$ tais que $p(x) \mid f(x)$, isto é, $x + 1$ é fator de $f(x)$, mas não o é de $g(x)$. Assim, $f(-1) = 0$, mas $g(-1) \neq 0$. Analogamente, P é polo das frações irredutíveis $\frac{f(x)}{g(x)}$ tais que $p(x) \mid g(x)$, isto é, daquelas que têm $x + 1$ como fator do denominador. Por outro lado, o lugar ∞ é zero das frações irredutíveis $\frac{f(x)}{g(x)}$ tais que $\deg(g(x)) > \deg(f(x))$ e é polo das frações irredutíveis $\frac{f(x)}{g(x)}$ tais que $\deg(g(x)) < \deg(f(x))$.

O caminho descrito acima pode ser revertido de modo que um lugar de K/k pode ser definido como o ideal maximal de algum anel de valoração (caracterizado de forma puramente algébrica) de K/k.

Teorema 2.2.1. *([16], Teorema 1.5.8) Qualquer valoração do corpo de funções racionais $k(x)$ é discreta e é* ***equivalente*** *(veja definição a seguir) a $\nu_{p(x)}$, para algum polinômio mônico irredutível $p(x) \in k(x)$, ou a ν_∞.*

A demonstração do teorema acima, em linhas gerais, consiste do seguinte: seja ν uma valoração discreta de $k(x)$ e P seu lugar correspondente. Consideramos dois casos.

1. $\nu(x) \geq 0$. Neste caso, mostra-se que o ideal $J = k[x] \cap M_P$ de $k[x]$ é primo. Seja então $p(x)$ o polinômio mônico irredutível gerador de J. Como $p(x) \in M_P$, então $c := \nu(p(x)) > 0$. Se $h(x) \in k[x]$ não é divisível por $p(x)$, então $\nu(h(x)) = 0$ e, daí, se escrevermos $r(x) \in k[x]$ arbitrário na forma $r(x) = p(x)^m \frac{f(x)}{g(x)}$, com $m \in \mathbb{Z}$ e $f(x), g(x) \in k[x]$ não divisíveis por $p(x)$, obtemos

$$\nu(r(x)) = m\nu(p(x)^m) + \nu(f(x)) + m\nu(g(x)^{-1}) = m\nu(p(x)) = \nu_{p(x)}(r(x)) \cdot c,$$

one $c = \nu(p(x)$, ou seja, ν é equivalente a $\nu_{p(x)}$.

2. $\nu(x) < 0$. Neste caso, $c := \nu(x^{-1}) > 0$ e $x^{-1} \in M_P$. Tomemos qualquer polinômio não nulo $f(x) \in k[x]$ de grau d, digamos. Temos:

$$f(x) = \sum_{i=0}^{d} \alpha_i x^i = x^d \sum_{i=0}^{d} \alpha_i x^{i-d} = x^d \sum_{i=0}^{d} \alpha_{d-i} x^{-i},$$

com $\alpha_i \in k$. Além disso,

$$\sum_{i=0}^{d} \alpha_{d-i} x^{-i} = \alpha_d + \sum_{i=0}^{d} \alpha_{d-i} x^{-i} = \alpha_d + s(x),$$

onde $s(x) \in M_P$. Como $\alpha_d \neq 0$, temos $\nu(\alpha_d) = 0$ e, daí, usando a desigualdade triangular estrita, segue que

$$\nu\left(\sum_{i=0}^{d} \alpha_{d-i} x^{-i}\right) = \min\{\nu(\alpha_d), \nu(s(x))\} = 0.$$

Portanto,

$$\begin{aligned}\nu(f(x)) = \nu(x^d \sum_{i=0}^{d} \alpha_{d-i} x^{-i}) &= \nu(x^d) + \nu\left(\sum_{i=0}^{d} \alpha_{d-i} x^{-i}\right) \\ &= \nu(x^d) = -d\nu(x^{-1}) = c\nu_\infty(f(x)),\end{aligned}$$

ou seja, ν é equivalente a ν_∞.

Assim, há exatamente dois tipos de lugares do CFR $k(x)$: os **lugares finitos**, contendo alguma valoração $\nu_{p(x)}$ e os **lugares infinitos**, contento a valoração ν_∞. Dado dois polinômios mônicos irredutíveis $p(x)$ e $q(x) \in k[x]$, temos $\nu_{p(x)}(q(x)) = 0$, $\nu_{q(x)}(q(x)) = 1$ e $\nu_\infty(q(x)) < 0$, logo tais valorações são duas a duas inequivalentes. Assim, o conjunto dos lugares de $k(x)$ pode ser também identificado com o conjunto

$$\left\{p(x) \in k[x] \mid p(x)\text{mônicoirredutível}\right\} \cup \{\infty\}.$$

Definição 2.2.4. Seja P um lugar de um corpo de funções algébricas K/k de uma variável sobre k. O corpo $K_P = \frac{\mathcal{O}_P}{M_P}$ é chamado **de corpo de classes residuais de** P. O homomorfismo canônico

$$z \in \mathcal{O}_P \mapsto z(P) := z + M_P \in K_P$$

é chamado **aplicação de classes residuais de** P.

Exemplo 2.2.3. Considerando novamente o CFR $k(x)$, verifica-se que, para $p(x) \in k(x)$ mônico irredutível, tem-se:

$$K_{p(x)} = \frac{\mathcal{O}_{p(x)}}{M_{p(x)}} \cong \frac{k[x]}{(p(x))} \text{ e que } K_\infty = \frac{\mathcal{O}_\infty}{M_\infty} \cong k.$$

A verificação desse fato se dá através de um homomorfismo sobrejetor de $\mathcal{O}_{p(x)}$ sobre $\frac{k[x]}{(p(x))}$ de núcleo $M_{p(x)}$, no caso do lugar finito $p(x)$ e do homomorfismo sobrejetor de $\mathcal{O}_\infty$ sobre k com núcleo M_∞. O argumento dessa demonstração serve para provar também que *"toda valoração de $k(x)$ é automaticamente discreta."*

Pode-se provar ainda que *"toda valoração de um CFA F/k é discreta"* ([16], Teorema 1.5.12). Para isso, toma-se um elemento transcendente $x \in F$ sobre k tal que F é uma extensão finita de $K = k(x)$. Seja ν uma valoração arbitrária sobre F e ξ sua restrição a K. É suficiente provar que o índice $[\nu(F^*) : \xi(K^*)]$ é finito, pois, nesse caso, sendo $\nu(F^*)$ um subgrupo infinito de $(\mathbb{R}, +)$, não se poderia ter $\xi(K^*) = 0$. Daí, ξ é uma valoração de K, logo discreta, pela observação anterior, logo ν é também discreta. Mais uma vez, usa-se nos detalhes da prova, a desigualdade triangular estrita.

Assim, a restrição de uma valoração de K/k a $k(x)$ produz uma valoração de $k(x)$. Valorações equivalentes de K produzem restrições equivalentes. Um lugar Q de K corresponde, por restrição, a um único lugar P de $k(x)$, em cujo caso se diz: Q **está sobre** P ou P **está sob** Q. Assim, *qualquer lugar de K está sobre um lugar de $k(x)$ correspondente a um polinômio mônico irredutível $p(x) \in k[x]$ ou sobre o lugar infinito de $k(x)$.*

Teorema 2.2.2. *O corpo de classes residuais de qualquer lugar de F/k é uma extensão finita de (uma cópia isomórfica de) k.*

Para a demonstração, toma-se um lugar Q que está acima do lugar P de $K := k(x)$, com x transcendente sobre k.

Imergimos, de forma natural, $R_P := \frac{\mathcal{O}_P}{M_P}$ em $R_Q := \frac{\mathcal{O}_Q}{M_Q}$ e mostramos que essa imersão, digamos, ρ, satisfaz $[R_Q : \rho(R_P)] \leq [F : K] \leq \infty$. Como R_P é uma extensão finita de (uma cópia isomórfica de) k, o resultado segue. Esse teorema dá consistência à definição seguinte.

Definição 2.2.5. O **grau** $\deg(P)$ de um lugar P de K/k é definido como o grau da extensão do corpo de classes residuais de P sobre k. Um lugar de K/k de grau 1 é também chamado de **lugar racional de** K/k.

Exemplo 2.2.4. Pelo exemplo anterior, se $K = k(x)$ é o CFR sobre k, então o grau do lugar finito $p(x)$ é o grau do polinômio $p(x)$ e o grau do lugar infinito de K é 1. Se $k = F_q$, então o CFR $k(x)$ possui exatamente $q+1$ lugares racionais: os correspondentes aos q polinômios mônicos irredutíveis de grau 1 e o lugar infinito.

2.3 Extensões de valorações

Sejam F/k e E/k' CFA de uma variável tais que $F \subset E$, $k \subset k'$, $[E : F] < \infty$, logo, $[k' : k] < \infty$. Se ν é uma valoração de E/k', então sua restrição a F/k é uma valoração. Além disso, valorações equivalentes de E produzem valorações equivalentes em F. Assim, um lugar Q de E corresponde por restrição a um único lugar P de F. Com argumentos análogos àqueles que provam que valorações em CFA são discretas, demonstra-se o teorema seguinte.

Teorema 2.3.1. *([16], Lema 1.6.1.) Para toda valoração ν de E/k', tem-se*

$$[\nu(E^*) : \nu(F^*)] \leq [E : F] < \infty$$

.

Nas condições do teorema acima, diz-se que Q **está sobre (acima de)** P ou que P **está sob (abaixo de)** Q. Denotamos por ν_Q a valoração normalizada pertencente ao lugar Q.

Definição 2.3.1. Se o lugar Q de E está sobre o lugar P de F, o **índice de ramificação** $e(Q|P)$ **de** Q **sobre** P é o inteiro positivo

$$e(Q|P) = [\nu_Q(E^*) : \nu_Q(F^*)] = [\mathbb{Z} : \nu_Q(F^*)], \text{ que é} \leq [E : F], \text{ pelo teorema acima.}$$

Diz-se que Q é **não ramificado** na extensão E/F se $e(Q|P) = 1$, que Q é **ramificado** na extensão E/F se $e(Q|P) > 1$, e que Q é **totalmente ramificado** na extensão E/F se $e(Q|P) = [E : F]$.

Observemos que da definição acima decorre que

$$\nu_Q(z) = e(Q|P)\nu_P(z), \text{ para todo } z \in F^*.$$

Se P e Q são como acima, então seus corpos de classes residuais, E_Q e F_P satisfazem $[E_Q : k'] < \infty$ e $[F_P : k] < \infty$. Além disso, a aplicação bem definida (pois $M_P \subset M_Q$) $z(P) = z + M_P \mapsto z(Q) = z + M_Q$, para $z \in \mathcal{O}_P$, é uma imersão de F_P em E_Q, de modo que E_Q pode ser visto como uma extensão finita de F_P.

Definição 2.3.2. Se o lugar Q de E está acima do lugar P de F, então o grau relativo $f(Q|P)$ de Q sobre P é o inteiro positivo $f(Q|P) = [E_Q : F_P]$.

Segue de um princípio geral relativo a extensões de valorações o resultado seguinte.

Teorema 2.3.2. *([26], Teorema 1.6.5.) Se o lugar P de F é dado e $Q_1, \cdots, Q_r$ são lugares distintos de E que estão sobre P, então*

$$\sum_{i=1}^{r} e(Q_i|P)f(Q_i|P) \leq [E : F].$$

Assim, há, no máximo, $[E : F]$ lugares de E acima de P. Quando esse máximo for atingido, diz-se que o lugar P de F **decompõe-se totalmente** na extensão $E|F$. Nesse caso, pelo teorema acima, tem-se $e(Q|P) = f(Q|P) = 1$, para cada lugar Q de E acima de P. Em particular, Q é não ramificado.

Por outro lado, se um dos lugares de E acima de P for totalmente ramificado em $E|F$, então não pode haver outro lugar de E acima de P.

Se o corpo de constantes k de um CFA F/k é perfeito e se $Q_1, \cdots, Q_r$ são todos os lugares distintos de E que estão sobre P, então o Teorema 3.1.11 de [24] mostra que

$$\sum_{i=1}^{r} e(Q_i|P)f(Q_i|P) = [E : F].$$

Como todo corpo finito é perfeito, a relação acima se aplica a eles. A este ponto, pode-se perguntar sobre a existência de um lugar Q acima de um dado lugar P de F. A resposta é afirmativa, conforme o Teorema 1 do Capítulo 4 de [17], um texto de Paulo Ribenboim sobre Teoria Clássica de Valorações.

Observação 2.3.1. Os corpos k de constantes considerados neste trabalho serão sempre totais e finitos, logo, perfeitos. Estaremos interessados em extensões K/k de grau 2, isto é, $[K : k(x)] = 2$. Nesse sentido, vale o teorema anterior com $r = 1$ ou $r = 2$,conforme exemplo adiante.

Seja $F/\mathbb{F}_q$ um CFA com corpo total de constantes $\mathbb{F}_q$. Para cada inteiro positivo n, o corpo $F_n := F \cdot \mathbb{F}_{q^n}$ chama-se **extensão do corpo de constantes de** F (contido em um fecho algébrico fixado de F). Se $\mathbb{F}_{q^n} = \mathbb{F}_q(\beta)$, então $F_n = F(\beta)$, cujo corpo de constantes é $\mathbb{F}_{q^n}$. Além disso, temos o seguinte:

Teorema 2.3.3. *([16], Teorema 1.7.2) Para todo lugar P de F e todo lugar Q de F_n acima de P, tem-se:*

(i) $e(Q|P) = 1$*, isto é, Q é não ramificado;*

(ii) $\deg(Q) = d/\mathrm{mdc}(d, n)$*, onde* $d = \deg(P)$*;*

(iii) $f(Q|P) = n/\mathrm{mdc}(d, n)$*;*

(iv) Há exatamente $\mathrm{mdc}(d, n)$ *lugares de F_n sobre P.*

Trabalharemos agora num exemplo simples, mas fundamental para o que vem posteriormente.

Exemplo 2.3.1. Seja F/k um CFA com $k = F_q$ da forma $F = \sqrt{m(x)}$, onde $m(x) \in k[x]$ é livre de quadrados, logo $[F : k(x)] = 2$. Seja P um lugar qualquer de $k(x)$ e Q_i os lugares acima de P em F. A igualdade fundamental neste caso dá

$$\sum_{i=1}^{r} e(Q_i|P)f(Q_i|P) = 2$$

de onde seguem as seguintes possibilidades:

1. $r = 2$, em cujo caso temos $e(Q_1|P) = e(Q_2|P) = 1$, $f(Q_1|P) = f(Q_2|P) = 1$. Dizemos que P se **decompõe** (totalmente) em F;

2. $r = 1$, caso em que podem ocorrer duas situações:

   (a) $e(Q_1|P) = 1$ e $f(Q_1|P) = 2$. Aqui, dizemos que P é **inerte** em F;

   (b) $e(Q_1|P) = 2$ e $f(Q_1|P) = 1$, quando se diz que P se **ramifica** em F.

2.4 Divisores e Espaços de Riemann-Roch

Seja F/k um CFA de uma variável com corpo total de constantes k. Denotamos por $\mathbf{P}_F$ o conjunto dos lugares de F. O **grupo de divisores de** F/k denotado por $\mathrm{Div}(F/k)$ ou $\mathrm{Div}(F)$, é o grupo abeliano livre gerado pelos lugares de F, isto é, um **divisor de** F é uma soma formal do tipo

$$\sum_{P \in \mathbf{P}_F} n_P P,$$

com coeficientes $n_P \in \mathbb{Z}$, quase todos nulos, isto é, apenas um número finito de coeficientes n_P é diferente de zero. Um divisor $D = \sum_{P \in \mathbf{P}_F} n_P P$ se diz **positivo**, com a notação $D \geq 0$, se $n_P \geq 0$, para todo $P \in \mathbf{P}_F$. Se os divisores D e G satisfazem $D - G \geq 0$, escrevemos $D \geq G$ ou $G \leq D$, o que define uma ordem parcial em $\mathrm{Div}(F)$.

Para $D = \sum_{P \in \mathbf{P}_F} n_P P \in \mathrm{Div}(F)$, denotamos n_P por $\nu_P(D)$, para $P \in \mathbf{P}_F$. Observemos que, para $D = P \in \mathbf{P}_F$, temos $\nu_P(D) = \nu_P(P) = 1$, em concordância com a definição da valoração ν_P. O **suporte de** D é o conjunto

$$\mathrm{supp}(D) := \{P \in \mathbf{P}_F \mid \nu_P(D) \neq 0\}.$$

O **grau de** D, $\deg(D)$, se define por $\deg(D) = \sum_{P \in \mathbf{P}_F} n_P \deg(P)$.
A aplicação $\deg : \mathrm{Div}(F^*) \to \mathbb{Z}$ é um homomorfismo de grupos, cujo núcleo é o subgrupo de $\mathrm{Div}(F)$ denotado por $\mathrm{Div}^0(F)$, e denominado **subgrupo dos divisores de grau** 0.

Teorema 2.4.1. *([16], Proposição 3.3.1.) Para todo $x \in F \setminus k$, temos*

$$\sum_{\substack{P \in \boldsymbol{P}_F, \\ \nu_P(x) > 0}} \nu_P(x) \deg(P) \leq [F : k(x)].$$

A demonstração desse teorema usa um teorema de aproximação para lugares ([16], Teorema 1.5.18).

Corolário 2.4.2. *([16], Corolário 3.3.2.) Todo elemento de F^* possui apenas um número finito de polos e de zeros.*

Em vista desse corolário, faz sentido definir os divisores de F associados aos elementos de $x \in F^*$ do seguinte modo: sejam $\mathcal{N}(x)$ o conjunto dos zeros de x e $\mathcal{P}(x)$ o conjunto dos polos de x. Definimos o **divisor dos zeros de** x por

$$(x)_0 = \sum_{P \in \mathcal{N}(x)} \nu_P(x) P$$

e o **divisor dos polos de** x por

$$(x)_\infty = \sum_{P \in \mathcal{P}(x)} (-\nu_P(x)) P.$$

Notemos que ambos os divisores são positivos. Finalmente, definimos o **divisor principal de** x, $\mathrm{div}(x)$, por

$$\mathrm{div}(x) = (x)_0 - (x)_\infty = \sum_{P \in \mathbf{P}_F} \nu_P(x) P.$$

A aplicação $\mathrm{div} : x \in F^* \mapsto \mathrm{div}(x) \in \mathrm{Div}(F)$ é um homomorfismo de grupos, cuja imagem é o subgrupo de $\mathrm{Div}(F)$ chamado subgrupo dos divisores principais de F, denotado por $\mathrm{Princ}(F)$.

Teorema 2.4.3. *([16], Proposição 3.3.3.) Todo elemento de $F \setminus k$ possui no mínimo um zero e no mínimo um polo. Em particular,* $\ker(\mathrm{div}) = k^*$. *(Lembremos que qualquer valoração se anula em k^*.)*

A demonstração desse teorema, dada em [16], utiliza a identificação de lugares P de F com os pontos da curva projetiva não singular correspondente a F.

Definição 2.4.1. Para um divisor D de F/k, definimos o **espaço de Riemann-Roch** por

$$\mathcal{L}(D) := \{x \in F^* \mid \mathrm{div}(x) + D \geq 0\} \cup \{0\}.$$

Observamos que $\mathcal{L}(D)$ é um espaço vetorial sobre k, cuja dimensão se denota por $l(D)$, que é finita, conforme mostra o teorema seguinte.

Teorema 2.4.4. *([16], Teorema 3.4.1.) Sejam D e G divisores de F/k. Então:*

1. *se $D \leq G$, então $\mathcal{L}(D)$ é um subespaço de $\mathcal{L}(G)$ e*

$$\dim(\tfrac{\mathcal{L}(G)}{\mathcal{L}(D)}) \leq \deg(G) - \deg(D);$$

2. $\mathcal{L}(0) = k$;

3. $\mathcal{L}(D) \geq 1$ *se* $D \geq 0$;

4. $l(D)$ *é finita, para todo divisor* D *e* $l(D) \leq \deg(D) + 1$;

5. se $D = G + \mathrm{div}(x)$*, para algum* $x \neq 0$ *em* F^**, então* $l(D) = l(G)$*.*

Como ilustração de aplicação desse teorema, demonstremos os próximos resultados.

TEOREMA 2.4.5. *Para todo divisor* $x \in F \setminus k$*, temos* $\deg((x)_0) = [F : k(x)]$*.*

Demonstração. Consideremos $n = [F : k(x)]$. Pelo Teorema 2.4.1, sabemos que $\deg((x)_0) \leq n$. Para provar a desigualdade oposta, escolhemos uma base $y_1, \cdots, y_n$ da extensão $F/k(x)$ e introduzimos o divisor positivo $C := \sum_{j=1}^{n} (y_j)_\infty$ de F. Para todo inteiro $m \geq 1$, cálculos rotineiros mostram que os elementos $x^{-i}y_j \in \mathcal{L}(m(x)_0 + C)$, para todo $0 \leq i \leq m$, $1 \leq j \leq n$, além de serem linearmente independentes sobre k. Por isso, $l(m(x)_0 + C) \geq n(m+1)$, para todo $m \geq 1$. Por outro lado, a desigualdade em 4. do teorema anterior diz que

$$l(m(x)_0 + C) \leq \deg(m(x)_0 + C) + 1 = m\deg((x)_0) + \deg C + 1.$$

Essas duas últimas desigualdades acarretam $m(\deg((x)_0) - n) \geq n - \deg(C) - 1$, para todo $m \geq 1$. Como o lado direito é independente de m, obtemos $\deg((x)_0) \geq n$. □

COROLÁRIO 2.4.6. *Para todo divisor* $x \in F \setminus k$*, temos* $\deg((x)_0) = \deg((x)_\infty) (= [F : k(x)])$*. Em consequência,* $\deg(\mathrm{div}(x)) = 0$*.*

Demonstração. O resultado é claro para $x \in k^*$. Para $x \in F \setminus k$, como $\deg((1/x)_0) = \deg((x)_\infty)$, o teorema anterior dá

$$\deg(x)_0 = [F : k(x)] = [F : k(1/x)] = \deg((1/x)_0) = \deg(x)_\infty.$$

□

COROLÁRIO 2.4.7. *Se* $\deg(D) < 0$*, então* $l(D) = 0$*.*

Demonstração. Se $l(D)$ fosse > 0, existiria $x \in l(D)$, isto é, existiria x satisfazendo $\mathrm{div}(x) + D \geq 0$, o que acarreta $0 \leq \deg(\mathrm{div}(x) + D) = \deg(D)$ (pois, pelo corolário acima, $\deg(\mathrm{div}(x)) = 0$), o que contraria a hipótese. □

Como vimos, o conjunto dos divisores principais forma um subgrupo de $\mathrm{Div}(F)$, denotado por $\mathrm{Princ}(F)$. O grupo quociente, $\frac{\mathrm{Div}(F)}{\mathrm{Princ}(F)}$, chama-se **grupo de classes de divisores de** F. Dois divisores D e G na mesma classe residual se dizem **equivalentes**, o que se denota por $D \equiv G$. Neste caso, os resultados acima têm as seguintes consequências:

1. $l(D) = l(G)$ e $\deg(D) = \deg(G)$;

2. $\mathrm{Princ}(F)$ é também um subgrupo de $\mathrm{Div}^0(F)$, o subgrupo dos divisores de grau 0.

O teorema seguinte caracteriza corpos de funções racionais e é consequência dos últimos resultados.

Teorema 2.4.8. *([16], Teorema 3.4.5.) São equivalentes:*

1. *F é o corpo de funções racionais sobre k;*

2. *Existe um elemento $x \in F^*$ tal que $\deg((x)_0) = 1$;*

3. *Existe um lugar racional P de F com $l(P) = 2$.*

Demonstração. Mostremos apenas que 3. implica em 1. e 2. De fato, 3. diz que existe um elemento $x \in \mathcal{L}(P) \setminus k$ tal que $\mathrm{div}(x) + P \geq 0$. Segue daí e do fato de x possuir ao menos 1 polo, que $(x)_\infty = P$. Então, $1 = \deg((x)_\infty) = [F : k(x)]$, logo, $F = k(x)$. □

2.5 Teorema de Riemann e Gênero

Os resultados desta e das próximas seções têm como objetivo obter a desigualdade de Hasse-Weil, que motivou a investigação contida neste trabalho. Eles são provados usando-se as propriedades dos espaços de Riemann-Roch e do grau de um divisor (portanto de valorações) e encontram-se nos textos sobre CFA, por exemplo, em [24] e [16]. Tais teoremas são usados para verificar as propriedades da função zeta de um CFA, que resultam na desejada desigualdade. Apresentaremos,

como temos feito, apenas os resultados e demonstrações que julgarmos oportunas para perceber como essas propriedades se aplicam.

TEOREMA 2.5.1. *([16], Teorema 3.5.1.) (**Riemann**) Para todo corpo de funções F/k, existe um inteiro não negativo g, dependendo apenas de F, tal que, para todo divisor D de F tem-se*

$$l(D) \geq \deg(D) + 1 - g.$$

COROLÁRIO 2.5.2. *Se $l(D) = \deg(D) + 1 - g$ e $G \geq D$, então $l(G) = \deg(G) + 1 - g$.*

Demonstração. Temos, pelo Teorema de Riemann, $l(G) \geq \deg(G) + 1 - g$. Para a desigualdade oposta, se $G \geq D$, a primeira propriedade apresentada sobre os espaços de Riemann-Roch (Teorema 2.4.4), acarreta o seguinte:

$$l(G) - l(D) = \dim_k \frac{\mathcal{L}(G)}{\mathcal{L}(D)} \leq \deg(G) - \deg(D),$$

de onde se segue que

$$l(G) \leq l(D) + \deg(G) - \deg(D) = \deg(D) + 1 - g + \deg(G) - \deg(D) = 1 - g + \deg(G).$$

□

COROLÁRIO 2.5.3. *([16], Corolário 3.5.3.) Existe um inteiro r, dependente apenas de F, tal que*

$$l(D) = \deg(D) + 1 - g$$

para todo divisor D de F com $\deg(D) \geq r$.

Definição 2.5.1. O inteiro não negativo g, determinado pelo corolário anterior, e que só depende de F, chama-se **gênero** do CFA F.

Observação 2.5.1. O Teorema de Riemann-Roch, que enunciaremos após o exemplo abaixo, mostra que o inteiro do corolário anterior é $2g - 1$.

Exemplo 2.5.1. Sejam $F = k(x)$ o CFR sobre k e P_∞ o lugar infinito de F. Para cada inteiro $n \geq 0$, consideremos o divisor nP_∞. Temos que $\mathcal{L}(nP_\infty) = \{z \in F^* \mid \text{div}(z) + nP_\infty \geq 0\} \cup \{0\}$. Assim, devemos ter $\sum_{P \in \mathbf{P}_F} \nu_P(z) + nP_\infty \geq 0$, o que equivale a $\nu_{p(x)}(z) \geq 0$, para todo irredutível mônico $p(x) \in k[x]$, e $\nu_\infty(z) \geq -n$. Das definições dessas valorações, é simples verificar que a primeira condição acima acarreta $z = \frac{f(x)}{g(x)}$, com $g(x) = 1$, e a segunda acarreta $deg(f(x)) \leq n$. Logo, $z = f(x) \in k[x]$ e deve ter grau $\leq n$, isto é, $l(\mathcal{L}(nP_\infty)) = n + 1$, para todo $n \geq 0$. Como $\deg(nP_\infty) = n$, o último corolário diz que $n + 1 = n + 1 - g$, isto é, $g = 0$.

Reciprocamente, se um CFA possui gênero 0 e no mínimo um lugar racional P, então, pelo Teorema 2.4.4, $l(P) \leq \deg(P) + 1 = 1 + 1 = 2$ e, pelo Teorema de Riemann, $l(P) \geq 2$, logo, $l(P) = 2$, o que caracteriza CFR, como já vimos.

TEOREMA 2.5.4. ***(Riemann-Roch)*** *([24], Teorema 1.5.15) Para cada CFA F/k, existe um único divisor W, chamado* ***divisor canônico de*** *F, para o qual vale: se F/k tem gênero g, então, para qualquer divisor D de F, tem-se*

$$l(D) = \deg(D) + 1 - g + l(W - D).$$

Além disso, $l(D) = \deg(D) + 1 - g$, sempre que $\deg(D) \geq 2g - 1$.

2.6 A função zeta de Riemann para corpos de funções, o $L-$ polinômio, o número de classes de divisores h e a desigualdade de Hasse-Weil

Lembremos que os CFA F/k com os quais lidamos neste trabalho são tais que o corpo total de constantes k é finito, $k = \mathbb{F}_q$, q é potência de um primo ímpar p.

TEOREMA 2.6.1. *([24], Lema 5.1.1.). Para todo $n \geq 0$, definindo $A_n(F)$ como sendo a cardinalidade do conjunto $\{D \in Div(F) \mid D \geq 0$ e $\deg(D) = n\}$, obtém-se que $A_n(F)$ é finita.*

Um lugar de $F/\mathbb{F}_q$ de grau 1 se chama, como vimos, lugar racional. Os lugares racionais de $F/\mathbb{F}_q$ estão em correspondência biunívuca com os pontos $\mathbb{F}_q$-racionais da correspondente curva projetiva não singular sobre $\mathbb{F}_q$. O resultado seguinte é consequência imediata do teorema anterior.

COROLÁRIO 2.6.2. *Um CFA sobre $\mathbb{F}_q$ possui apenas um número finito de lugares racionais.*

Denotemos por $N(F)$ o número de pontos racionais de $F/\mathbb{F}_q$. Mais geralmente, para cada inteiro $n \geq 1$, consideremos o CFA $F_n/\mathbb{F}_{q^n}$, em que F_n é a composição de corpos $F \cdot \mathbb{F}_{q^n}$. Seja $N_n(F)$ o número de lugares racionais de $F_n/\mathbb{F}_{q^n}$. Assim, $N(F) = N_1(F)$. A função zeta de $F/\mathbb{F}_q$, definida a seguir, incorpora todos esses dados.

Definição 2.6.1. A **função zeta** $Z(F,t)$ **de** $F/\mathbb{F}_q$ é a seguinte série de potências formal sobre os números complexos:

$$Z(F,t) := exp\left(\sum_{n=1}^{\infty} \frac{N_n(F)}{n} t^n\right) \in \mathbb{C}[[t]].$$

Exemplo 2.6.1. Computemos a função zeta do CFR $F = \mathbb{F}_q(x)$ sobre $\mathbb{F}_q$. Como $F_n = \mathbb{F}_{q^n}(x)$, então $N_n(F) = q^n + 1$, como vimos no exemplo 2.2.4. Obtemos:

$$\log Z(F,t) = \sum_{n=1}^{\infty} \frac{q^n+1}{n} t^n = \sum_{n=1}^{\infty} \frac{(qt)^n}{n} + \sum_{n=1}^{\infty} \frac{t^n}{n} = -\log(1-qt) - \log(1-t) = \log \frac{1}{(1-t)(1-qt)},$$

isto é,

$$Z(F,t) = \tfrac{1}{(1-t)(1-qt)}.$$

TEOREMA 2.6.3. *([16], Teorema 4.1.6) A função zeta pode também ser representada pelas seguintes expressões:*

(i) $Z(F,t) = \sum_{n=0}^{\infty} N_n(F) t^n$;

*(ii) (**Produto de Euler**)* $Z(F,t) = \prod_{P \in \boldsymbol{P}_F} (1 - t^{degP})^{-1}$.

Observação 2.6.1. Utilizando a fórmula (i) como definição, [24] prova, na Proposição 5.1.6., que $Z(F,t)$ é convergente para $|t| < \frac{1}{q}$. O produto de Euler em (ii) decorre facilmente de (i).

Recordemos que dois divisores D e G se dizem equivalentes quando $D = G + \mathrm{div}(x)$, para algum $x \in F^*$, logo, possuem o mesmo grau, pois $\deg(x) = 0$. Assim, pode-se falar de **grau da classe de divisores** $[D] = D + \mathrm{Princ}(F) \in \frac{\mathrm{Div}(F)}{\mathrm{Princ}(F)}$. O subconjunto $\mathrm{Div}^0(F)$ de $\mathrm{Div}(F)$, que consiste de todos os divisores de F de grau 0, é um subgrupo de $\mathrm{Div}(F)$ que contém seu outro subgrupo $\mathrm{Princ}(F)$. Podemos, então, considerar o grupo quociente

$$Cl(F) = \frac{\mathrm{Div}^0(F)}{\mathrm{Princ}(F)},$$

que se chama **grupo de classes de divisores de grau** 0 **de** F. Assim, $Cl(F)$ consiste de todas as classes de divisores $[D]$ com $D \in \mathrm{Div}^0(F)$.

TEOREMA 2.6.4. *$Cl(F)$ é um grupo abeliano finito.*

Demonstração. Basta mostrar que $Cl(F)$ é finito. Escolhamos $D \in \mathrm{Div}(F)$ com $d := \deg(D) \geq g =$ gênero de F. Pelo Teorema de Riemann, temos $l(D) \geq d+1-g \geq 1$, logo há um elemento não nulo $G = D + \mathrm{Div}(x) \geq 0$ em $\mathcal{L}(D)$. Logo, $[D] = [G]$ em $\mathrm{Div}(F)/\mathrm{Princ}(F)$. Como $A_d(F)$ é finito, assim o será o número de classes de divisores de grau d. Mostremos agora que as classes de divisores de grau 0 de F são dadas exatamente pelas expressões do tipo $[D]-[B]$, com $B \in \mathrm{Div}(F)$ de grau d, de onde decorrerá que elas são em número finito. De fato, seja $E \in \mathrm{Div}(F)$ com $\deg(E) = \deg([E]) = 0$. Como $\deg(D - E) = d$, segue-se novamente pelo Teorema de Riemann que $l(D - E) > 0$. Seja $B := D - E + \mathrm{div}(y)$ um elemento não nulo em $D - E$. Temos: $\deg(B) = d$ e $E = D - B + \mathrm{div}(y)$, isto é, $[E] = [D] - [B]$. □

Definição 2.6.2. A ordem do grupo finito $Cl(F)$ é denotada por $h(F)$ e se chama **o número de classes de divisores (de grau** 0**) de** F.

PROPOSIÇÃO 2.6.5. *Em um CFR F/k, todo divisor de grau* 0 *é principal. Em consequência, $h(F) = 1$.*

Demonstração. Seja A um divisor de grau 0. Como o gênero de um CFR é 0 (2.5.1), temos $0 > 2g-2$, de onde obtemos, pelo Teorema de Rieman-Roch, que $l(A) = \deg A + 1 - g = 1$. Assim,

existe $x \in F \setminus 0$ com $\mathrm{div}(x) \geq -A$. Como $\mathrm{div}(x)$ e A possuem, ambos, grau 0, a desigualdade anterior é uma igualdade, logo, $A = -\mathrm{div}(x) = \mathrm{div}(x^{-1})$. □

LEMA 2.6.6. *Para todo divisor $D \in \mathrm{Div}(F)$, o número de divisores positivos na classe de de divisores $[D]$ é $\frac{q^{l(D)}-1}{q-1}$.*

Demonstração. Um divisor $G \in [D]$ é positivo se, e somente se, $G = D + \mathrm{div}(x)$, para algum $x \in \mathcal{L}(D) \setminus 0$. Há exatamente $q^{l(D)} - 1$ elementos $x \in \mathcal{L}(D) \setminus 0$ e, como x, $y \in \mathcal{L}(D) \setminus 0$ produzem o mesmo divisor G se, e somente se, $y = cx$, para algum $c \in \mathbb{F}_q^*$, obtemos o resultado. □

LEMA 2.6.7. *([16], Lema 4.1.10) Todo CFA sobre um corpo finito $\mathbb{F}_q$, possui um divisor de grau 1.*

COROLÁRIO 2.6.8. *Todo CFA sobre um corpo finito de gênero 0 é um CFR.*

Demonstração. Suponhamos $F/\mathbb{F}_q$ de gênero 0. Pelo lema anterior, existe um divisor D de F de grau 1. Pelo Teorema de Riemann-Roch, $l(D) = 2$. Assim, pelo Lema 2.6.6, podemos escolher um divisor positivo $G \in [D]$. Um tal G satisfaz $G \geq 0$, $deg(G) = 1$ e $l(G) = 2$, o que acarreta, pelo Teorema 2.4.8, que F é um CFR.

□

TEOREMA 2.6.9. *([16], Teorema 4.1.11) Seja $F/\mathbb{F}_q$ um CFR sobre $\mathbb{F}_q$ de gênero g. Então, a função zeta de F é racional da forma*

$$Z(F,t) = \frac{L(F,t)}{(1-t)(1-qt)},$$

onde $L(F,t) \in \mathbb{Z}[t]$ é um polinômio de grau no máximo $2g$ e $L(F,0) = 1$. Além disso, $L(F,1) = h(F)$. (No próximo teorema, veremos que $degL(F,t) = 2g$.)

Definição 2.6.3. O polinômio $L(F,t)$ do teorema acima se chama $L-$ **polinômio de** $F/\mathbb{F}_q$.

Esse polinômio possui importantes propriedades que listamos a seguir (veja Teorema V.1.15 em [24]), culminando com o Teorema de Hasse-Weil e um corolário que fornece uma desigualdade fundamental envolvendo $h(F)$.

Teorema 2.6.10. *([24], Teorema 5.1.15.)*

1. *O $L-$ polinômio $L(F,t)$ do CFA $F/\mathbb{F}_q$ de gênero g satisfaz a equação funcional*

$$L(F,t) = q^g t^{2g} L\left(F, \tfrac{1}{qt}\right);$$

2. *Escrevendo $L(F,t) = \sum_{i=0}^{2g} a_i t^i$, com $a_i \in \mathbb{Z}$, então:*

   (a) *$a_0 = 1$ e $a_{2g} = q^g$;*

   (b) *$a_{2g-i} = q^{g-i} a_i$, para $0 \leq i \leq g$;*

   (c) *$a_1 = N - (q+1)$, onde N é o número de lugares de grau um;*

3. *$L(F,t)$ se fatora em $\mathbb{C}[t]$ na forma*

$$L(t,F) = \prod_{i=1}^{2g} (1 - \alpha_i t),$$

   onde os complexos α_i são inteiros algébricos, inversos das raízes de $L(F,t)$, e podem ser arranjados de forma que $\alpha_i \alpha_{g+i} = q$, para $i = 1, \cdots, g$;

4. *Se $L_r(t) := \frac{L(F,t)}{(1-t)(1-q^r t)} Z_r(t)$ denota o $L-$polinômio da extensão do corpo de constantes $F_r = F\mathbb{F}_{q^r}$, então,*

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

   onde os α_i são como no item anterior.

Corolário 2.6.11. *([24], Corolário 5.1.16) Para todo $r \geq 1$,*

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

onde $\alpha_1, \cdots, \alpha_{2g} \in \mathbb{C}$ são os inversos das raízes de $L(t)$.Em particular, temos

$$N = N_1 = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

TEOREMA 2.6.12. *([24], Teorema 5.2.1.)* ***[Hasse-Weil]*** *Seja* $L(F,t) = \prod_{i=1}^{2g}(1-w_i t)$*, o L-polinômio do CFA* $F/\mathbb{F}_q$ *de gênero* g*. Aqui,* w_i*,* $1 \leq i \leq 2g$*, são os inversos das raízes de* $L(F,t)$*. Então* $|w_i| = q^{\frac{1}{2}}$*, para todo* i*.*

TEOREMA 2.6.13. ***[Desigualdade de Hasse-Weil]*** *O número de classes de divisores* $h(F)$ *de um CFA* $F/\mathbb{F}_q$ *de gênero* g *satisfaz* $(q^{\frac{1}{2}}-1)^{2g} \leq h(F) \leq (q^{\frac{1}{2}}+1)^{2g}$*.*

Demonstração. $|h(F)| = |L(F,1)| = \prod_{i=1}^{2g}|1-w_i|$. Agora, $1-|w_i| \leq |1-w_i| \leq 1+|w_i|$ que, pelo Teorema de Hasse-Weil, equivale a $1-q^{\frac{1}{2}} \leq |1-w_i| \leq 1+q^{\frac{1}{2}}$, de onde seguem as desigualdades desejadas. □

2.7 Corpos elípticos e hiperelípticos de funções

Descreveremos nesta seção, com base na referência [24], os corpos de funções que interessam para os sistemas criptográficos e com os quais lidamos neste trabalho, os elípticos e os hiperelípticos em característica ímpar.

Definição 2.7.1. Um CFA F/K se diz **elíptico** se são satisfeitas as seguintes condições:

1. o gênero de F/K é 1;
2. existe um divisor A de F com $\deg(A) = 1$.

As proposição 6.1.2. e 6.1.3. de [24] descrevem CFA F/K elípticos para *car* $K \neq 2$, nos termos do teorema seguinte:

TEOREMA 2.7.1. *Suponhamos car* $K \neq 2$*.*

1. *Seja* F/K *CFA elíptico. Então existem* $x, y \in F$ *tais que* $F = K(x,y)$ *e* $y^2 = f(x) \in K[x]$*, onde* $f(x) \in K[x]$ *é um polinômio de grau* 3 *livre de quadrados.*

2. *Reciprocamente, se* $F = K(x, y)$ *e* $y^2 = f(x) \in K(x)$ *é livre de quadrados, com* $deg(f(x)) = 3$*, então* F/K *é elíptico.*

Neste caso, o lugar P_∞ *de* $K(x)$ *ramifica em* $F/K(x)$ *e, se* Q_∞ *é sua extensão, então* $e(Q_\infty/P_\infty) = 2$ *e* $f(Q_\infty/P_\infty) = 1$.

Definição 2.7.2. Um CFA F/K se diz **hiperelíptico** se tiver gênero $g \geq 2$ e contiver um subcorpo racional $K(x) \subset F$ tal que $[F : K(x)] = 2$.

As Proposições 6.2.2. e 6.2.3. de [24] descrevem CFA F/K hiperelípticos:

TEOREMA 2.7.2. *1. Um CFA* F/K *é hiperelíptico se, e somente se, existe um divisor* A *de* F *tal que* $\deg(A) = 2$ *e* $l(A) \geq 2$*. Todo CFA de gênero 2 é hiperelíptico.*

2. *Suponhamos car* $K \neq 2$.

   (a) *Seja* F/K *um CFA hiperelíptico de gênero* g*. Então existem* $x, y \in F$ *tais que* $F = K(x, y)$ *e* $y^2 = f(x) \in K[x]$*, onde* $f(x) \in K[x]$ *é um polinômio de grau* $2g+1$ *ou* $2g+2$ *livre de quadrados.*

   (b) *Reciprocamente, se* $F = K(x, y)$ *e* $y^2 = f(x) \in K[x]$*, onde* $f(x)$ *é um polinômio de grau* $m > 4$ *livre de quadrados, então* F/K *é hiperelíptico de gênero* $g = \frac{m-1}{2}$*, se* m *é ímpar, ou* $g = \frac{m-2}{2}$*, se* m *é par. No primeiro caso, o lugar* P_∞ *de* $K(x)$ *ramifica e, no segundo caso,* P_∞ *decompõe se o coeficiente dominante de* $f(x)$ *é quadrado em* K^* *e é inerte em caso contrário.*

Capítulo 3

Sobre criptografia e o número de classes

3.1 Criptografia e corpos de funções algébricas

Apresentamos aqui o papel desempenhado pelos corpos de funções algébricas, especialmente o seu grupo de classes de divisores de grau zero e sua ordem h, em sistemas criptográficos. As referências principais para os temas aqui tratados são [19] e [16].

3.1.1 Criptografia

A criptografia - do grego, *kryptós* (escondido, secreto) e *gráphein* (escrever) - pode ser entendida como a arte de transformar informação escrita de sua forma original em uma que não pode ser compreendida, a menos que se saiba como decifrá-la, isto é, a menos que se tenha uma chave secreta que a decifre.

Criptografia consiste de dois processos: o primeiro, chamado *encriptação* é uma forma de codificar a informação, de modo a torná-la ininteligível a quem não é autorizado a lê-la; o segundo, chamado *decriptação*, é o processo inverso, de decodificar a mensagem encriptada, sendo necessário para tal um conhecimento especial.

Suponhamos que uma pessoa, de agora em diante denominada Alice, deseja enviar uma infor-

mação a outra pessoa, que chamaremos de Bob, de tal forma que ninguém além de Bob seja capaz de entendê-la. Para tanto, Alice codificará a mensagem, obtendo uma nova mensagem, chamada texto cifrado. Quando Bob o recebe, ele o decodifica, obtém o texto original e o lê.

Para esse processo funcionar, Alice precisa de usar uma chave de encriptação para obter o texto cifrado, e Bob precisa de uma chave de decriptação para decodificá-la e obter o texto original. A chave de decriptação precisa ser mantida em segredo.

Há duas maneiras básicas de codificar uma mensagem: *simétrica* e *assimétrica*. Chamando de a e b as chaves de encriptação e decriptação, respectivamente, diz-se que a codificação é simétrica se $a = b$ ou se b pode ser facilmente obtida de a. Neste caso, Alice e Bob precisam combinar a chave secreta antes de começarem a enviar informações entre si, caso contrário, qualquer pessoa deduziria b de a e poderia decifrar a mensagem.

No caso de sistemas assimétricos, a e b são distintos e a computação de b a partir de a não é possível. A vantagem desse sistema é que a pode ser tornada **pública** sem perigo. Esse sistema funciona assim: se Bob quer receber uma mensagem encriptada, ele publica a chave a e mantém b em segredo. Quando Alice envia a Bob uma mensagem, ela usa a para obter o texto cifrado. Apenas Bob poderá decifrar a mensagem pois ele é o único que conhece a chave b. Nem mesmo Alice poderia obter a mensagem original da encriptada.

Por essa razão, sitemas assimétricos também são chamados de *sistemas criptográficos de chave pública*. Eles hoje são utilizados em vários setores de atividade, como bancos, companhias de cartões de crédito, troca de artigos científicos entre colaboradores, de modo a evitar plágios, etc. A razão disso é que a troca de chaves secretas passa a ser desnecessária, possibilitando uma gama muito maior de comunicações seguras. Descreveremos brevemente na próxima seção dois importantes sistemas de chave pública, o *RSA* e o *ElGamal*.

3.1.2 Sistemas criptográficos

O sistema criptográfico mais simples que existe, utilizado por César nas guerras que promovia, consiste basicamente em transladar cada letra do alfabeto para a seguinte (ou para um número fixo de letras adiante,módulo 26, no nosso caso). Esse número fixo é a chave de codificação e decodificação (sistema simétrico). O sistema de César é, portanto, de fácil decodificação.

O problema principal em sistemas simétricos é a distribuição e administração da chave. Se Alice e Bob usam um tal sistema, eles precisam combinar a chave antes de começarem a trocar informação.

Em sistemas de chave pública, a troca de chaves não é mais um problema. Bob torna pública a chave de encriptação a para ser utilizada por qualquer pessoa que queira enviar-lhe uma mensagem. Quando Bob recebe a mensagem encriptada com sua chave pública a, ele utiliza sua chave secreta de decriptação b para decodificar a mensagem.

O sistema criptográfico de chave pública mais popular é o sistema *RSA*, criado em 1978 por Ron **R**ivest, Adi **S**hamir e Len **A**dleman. Ele foi um dos primeiros sistemas criptográficos a serem inventados e ainda se mantém o mais importante. Sua segurança reside na dificuldade de se encontrar a fatoração de um número inteiro que é produto de dois primos grandes. Vejamos como funciona.

Bob encontra dois primos grandes, p e q e computa $n = pq$. Agora, ele escolhe qualquer inteiro a tal que $1 < a < \varphi(n) = (p-1)(q-1)$ ($\varphi(n) =$ número de inteiros positivos menores do que n e relativamente primos com n), com $\text{mdc}(a, \varphi(n)) = 1$. Devido a essa escolha, existe $b \in \{1, \cdots, \varphi(n) - 1\}$ tal que $ab \equiv 1 \bmod \varphi(n)$. O número b pode ser computado através do algoritmo extendido de Euclides (ver [19]).

Bob publica a chave (n, a) e sua chave privada é b. Como comentado acima, b pode ser computado conhecendo-se p e q, ou seja, fatorando-se n, o que é impossível se p e q são suficientemente grandes.

O processo funciona assim: suponhamos que uma certa mensagem seja escrita em um alfabeto de N letras. Para transformarmos a mensagem em um número, atribuiremos a cada letra do alfabeto um número de 0 a $N-1$. Ponhamos $t = \log_N n$ e assumamos que Alice tem um texto $m_1 m_2 \cdots m_k$, onde cada m_i é um número correspondente a uma letra do alfabeto. Então ela define $m = \sum_{i=1}^{t} m_i N^{t-i}$. Obtemos $0 \leq m \leq (N-1)\sum_{i=1}^{t} N^{t-i} = N^t - 1 < n$. Seja $c = m^a \bmod n$ o texto cifrado e escrevamos c na base N. Como $0 \leq c < n < N^{t+1}$, a expressão de c na base N possui comprimento máximo igual a $t+1$, isto é,

$$c = \sum_{i=0}^{t} c_i N^{t-i}, \text{ com } c_i \in \{0, 1, \cdots N-1\}, \text{ para } 0 \leq i \leq t.$$

Portanto, a mensagem encriptada consiste do inteiro $c = c_1 c_2 \cdots c_t$. O fato crucial que faz o sistema *RSA* funcionar, e que se baseia no teorema a seguir, é que $c^b \bmod n = m$. Assim, Bob usa sua chave secreta b para obter m, depois ele o expressa na base N, usa as letras correspondentes e obtém a mensagem de Alice.

TEOREMA 3.1.1. *([19], Teorema 10.2.3) Se p e q são primos distintos, $n = pq$, $\varphi(n) = (p-1)(q-1)$, a é primo com $\varphi(n)$, $0 \leq m \leq n$ e b satisfaz $ab \equiv 1 \bmod n$, então $(m^a)^b \bmod n = m$.*

3.1.3 Criptografia com corpos finitos e o criptossistema de ElGamal

O conceito de chave pública foi introduzido por Diffie e Hellman em 1976 [5]. A diferença em relação a sistemas simétricos está na utilização de uma função unidirecional, ou seja, uma função que é fácil de usá-la, mas difícil de invertê-la. No exemplo do *RSA*, tal função é a que multiplica dois primos grandes. Neste caso, a função inversa é a fatoração de um dado inteiro como produto de dois primos, o que, dependendo dos primos, pode ser muito difícil.

Os sistemas criptográficos que utilizam corpos finitos baseiam-se na dificuldade computacional de resolução do *problema do logaritmo discreto* (PLD), que consiste do seguinte: seja $\mathbb{F}_q^*$ o grupo multiplicativo do corpo finito de q elementos. Escolhemos $g \in \mathbb{F}_q^*$ a que chamamos *base*. Dado

$y \in \mathbb{F}_q^*$, determinar um inteiro x tal que $y = g^x$, isto é, "$x = \log_g y$". O PLD pode ser definido para qualquer grupo finito. A dificuldade computacional de resolução deste problema para grupos de ordem alta está na base do método de troca de chaves de Diffie-Hellman [16].

Do mesmo modo, o a inviabilidade computacional do PDL é a base do sistema criptográfico de ElGamal, que descrevemos brevemente a seguir.

Exemplo 3.1.1. [***Criptossistema de ElGamal***] Seja A um grupo abeliano finito de ordem alta e $a \in A$ um elemento de A também de ordem alta. O par A e a são tornados públicos.
Alice quer enviar uma mensagem para Bob. Como no RSA, ela transforma a mensagem em um elemento m de A.
Bob escolhe $h \in \mathbb{Z}$ como sua chave privada e publica $b := a^h$.
Alice escolhe $k \in \mathbb{Z}$ e computa $c_1 = a^k$ e $c_2 = mb^k$ em A. O par (c_1, c_2) é enviado a Bob.
Bob, então, desvenda o texto m computando $c_2 c_1^{-h}$, pois

$$c_2 c_1^{-h} = mb^k \left(a^h\right)^k \left(a^k\right)^{-h} = m.$$

A condição necessária para a segurança do criptossistema de ElGamal é a inviabilidade do PLD em A, pois a chave privada h de Bob,que abre a mensagem m de Alice só é descoberta se se puder calcular $\log_a b$ em A, o que é inviável. Além disso, caso a mensagem (c_1, c_2) de Alice seja interceptada, m continua em segurança pois sua descoberta depende de $k = \log_a c_1$, também tornado inviável.

O criptossistema de ElGamal e outros sistemas criptográficos podem ser implementados utilizando-se os grupos de classes de divisores de grau 0 de corpos de funções algébricas elípticos (cf. Seção 2.7) ao invés do grupo multiplicativo de corpos finitos. Esses CFA - ou, similarmente, as curvas elípticas não singulares - foram inicialmente propostos para tais fins em 1985 por Neal Koblitz [12] e Victor Miller [14]. As razões para utilizá-los são as seguintes: primeiro, existe apenas um corpo finito de q elementos, enquanto há muitos corpos de funções elípticos sobre $\mathbb{F}_q$.

Segundo, e mais importante, é a ausência de algoritmos em tempo subexponencial hábeis para quebrar o sistema (ainda tendo o PLD como base), desde que o corpo elíptico de funções sobre $\mathbb{F}_q$ seja escolhido sendo *não-supersingular*, isto é, quando o número de lugares (ou divisores primos) de grau 1, $N_1(\mathbb{F}_q)$, for congruente a 1 módulo p.

Embora não se conheçam algorítmos em tempo subexponencial para o PLD em CFA elípticos não-supersingulares, o progresso alcançado na computação de logaritmos discretos para corpos finitos e na fatoração de inteiros requerem chaves cada vez maiores para a segurança dos sistemas criptográficos de chave pública.

Em 1989, Koblitz [13] generalizou o uso de criptossistemas elípticos para o uso de criptossistemas hiperelípticos. A razão principal pela qual os corpos hiperelípticos $F = \mathbb{F}_q(x)\left(\sqrt{f(x)}\right)$ (cf. Seção 2.7) são convenientes para propósitos criptográficos é que os elementos do grupo de classes de divisores de grau 0 possuem uma representação conveniente como pares (u, v) de elementos de $\mathbb{F}_q[x]$ (cf. [15]). Essa representação torna a adição no grupo de classes facilmente implementável.

Outra vantagem dos criptossistemas baseados em corpos de funções hiperelípticos sobre os elípticos é que os primeiros podem ser construídos com o mesmo nível de segurança que os últimos, utilizando um corpo de base menor. Mais precisamente, a ordem de h = número de classes de divisores de grau 0 de um corpo de funções hiperelíptico de gênero g sobre um corpo de q elementos é aproximadamente q^g. Isso significa que se tivermos um corpo de funções elíptico (gênero igual a 1), com um corpo de base de tamanho q da ordem de 3^{200}, então o corpo hiperlíptico de gênero 2, 3 ou 4 poderá ter corpo de base da ordem de 3^{100}, 3^{67} ou 3^{50}, respectivamente.

Os algoritmos de ataque ao PLD em corpos hiperelípticos indicam que apenas os de gênero baixo (2 e 3) devem ser usados para propósitos criptográficos, além do fato de que h deve ser divisível por um primo da ordem de $2^{160} \approx 1,47 \times 10^{50}$. Uma abordagem computacional detalhada sobre os sistemas criptográficos baseados em curvas elípticas e hiperelípticas e vários outros tópicos referentes a essas curvas e corpos de funções podem ser encontradas em [2].

3.2 A L-série de Artin adaptada a uma IFE para h

Utilizaremos aqui a linguagem e os resultados contidos em [9] e [18] para deduzir uma identidade finita e explícita para h, o número de classes de divisores de $F = \mathbb{F}_q(x)(\sqrt{D})$, onde $D(x) \in \mathbb{F}_q[x]$ é livre de quadrados e q é ímpar. Essa identidade é uma consequência direta dos resultados contidos nas referências acima sobre as L-séries de Artin. Essas L-séries dependem do *símbolo de Legendre polinomial de ordem 2* ou do *caráter de ordem 2* que definiremos na próxima subseção. Nessas referências, define-se de maneira geral o símbolo polinomial de Legendre de ordem $l \geq 2$.

3.2.1 O símbolo de Legendre polinomial de ordem 2

Sejam $A = \mathbb{F}_q[x]$ e $K = \mathbb{F}_q(x)$. O grupo multiplicativo A^* dos elementos inversíveis de A é igual a $(\mathbb{F}_q)^*$, que é cíclico de ordem $q-1$. Para $D \in A$, temos que a ordem do anel $\frac{A}{(D)}$, denotada por $\left|\frac{A}{(D)}\right|$, é $q^{\deg(D)}$. Definimos, então, $|D| := q^{\deg(D)}$ e, no caso em que se $D = 0$, pomos $|D| = 0$.

Se $P \in A$ for irredutível de grau d e P não dividir D, então o grupo multiplicativo dos elementos não nulos do corpo $\left(\frac{A}{(P)}\right)$, denotado por $\left(\frac{A}{(P)}\right)^*$, tem ordem $|P|-1$ e contém uma cópia de $(\mathbb{F}_q)^*$. Denotemos por $\overline{a}$ a classe de $a \in A$ em $\left(\frac{A}{(P)}\right)$. Suponhamos que q é ímpar, de modo que $2|q-1$. Temos:

$$\left(\overline{a}^{\frac{|p|-1}{2}}\right)^2 = \overline{a}^{|P|-1} = \overline{1},$$

de onde se segue que $\overline{a}^{\frac{|p|-1}{2}}$ é uma raiz quadrada da unidade em $\left(\frac{A}{(P)}\right)^*$, isto é, $\pm\overline{1} \in \mathbb{F}_q$. Em termos de congruências, essa igualdade equivale a $a^{\frac{|p|-1}{2}} \equiv \pm 1 \bmod P$. Finalmente, obtemos a seguinte definição:

Definição 3.2.1. Para D e P como acima, definimos o **símbolo de Legendre polinomial de ordem** 2, denotado por $\chi_D(P)$, como sendo 1 ou -1, dependendo da classe de equivalência de $D^{\frac{|p|-1}{2}}$. Estendemos a definição para o caso em que P divide D, pondo $\chi_D(P) = 0$.

Como $D^{\frac{|p|-1}{2}} \equiv \pm 1 \bmod P$, então existe $K(x) \in A$ tal que

$$P(x)K(x) = D(x)^{\frac{|P|-1}{2}} - \chi_D(P).$$

Seja α uma raiz de P em $\mathbb{F}_{q^d}$, onde, lembramos, $d = \deg(P)$. Da igualdade anterior, vem

$$P(\alpha)K(\alpha) = D(\alpha)^{\frac{|P|-1}{2}} - \chi_D(P),$$

isto é,

$$\chi_D(P) = D(\alpha)^{\frac{|P|-1}{2}} = D(\alpha)^{\frac{q^d-1}{2}}.$$

Observemos que se $P \mid A$, então $\chi_P(D) = 0$, que também é $D(\alpha)^{\frac{|P|-1}{2}}$. Assim, em qualquer caso, $\chi_D(P) = D(\alpha)^{\frac{|P|-1}{2}}$, onde α é uma raiz de P.

Notemos também que $D(\alpha)^{\frac{|P|-1}{2}}$ não depende da raiz α escolhida entre os conjugados de Frobënius $\left\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{d-1}}\right\}$. De fato, temos que

$$(\alpha + \beta)^{q^k} = (\alpha^{q^k} + \beta^{q^k}),$$

para α e β em qualquer extensão de $\mathbb{F}_q$ e $k \in \mathbb{N}$ (Cf. [16]). Além disso, para $u \in \mathbb{F}_{q^d}$, temos $u^{\frac{q^d-1}{2}} = u^{\frac{q-1}{2}\cdot\left(1+q+q^2+\cdots+q^{d-1}\right)}$. Como $N_d : u \in \mathbb{F}_{q^d} \mapsto N_d(u) = u^{1+q+\cdots+q^{d-1}} \in \mathbb{F}_q$ é a **norma de** $\mathbb{F}_{q^d}$ **sobre** $\mathbb{F}_q$, então

$$u^{\frac{q^d-1}{2}} = (N_d(u))^{\frac{q-1}{2}} \in \mathbb{F}_q.$$

Assim, temos

$$D(\alpha)^{\frac{q^d-1}{2}} = N_d\left[(D(\alpha))\right]^{\frac{q-1}{2}} = N_d\left[\left(D(\alpha^{q^j})\right)\right]^{\frac{q-1}{2}} = D(\alpha^{q^j})^{\frac{q^d-1}{2}}.$$

Essas considerações permitem expressar o símbolo polinomial de Legendre módulo 2 do seguinte modo, para P de grau d e D, como acima:

$$\chi_D(P) = \left\{\left[N_d(D(\alpha))\right]^{\frac{q-1}{2}}\right\}^*,$$

onde $N_d : u \in \mathbb{F}_{q^d} \mapsto N_d(u) = u^{1+q+\cdots+q^{d-1}} \in \mathbb{F}_q$ é a **norma de** $\mathbb{F}_{q^d}$ **sobre** $\mathbb{F}_q$ e o asterisco * da igualdade indica uma imersão do grupo das unidades de $\mathbb{F}_q^*$ no grupo das unidades complexas em $S^1 \subset \mathbb{C}$, que nospermite identificar as unidades $\pm 1 \in \mathbb{F}_q^*$ com $\pm 1 \mathbb{C}$.

O símbolo de Legendre possui as seguintes propriedades: se D é um produto de irredutíveis distintos D_k, então

$$\chi_D(I) = \prod_k \chi_{D_k}(I),$$

e se M é um produto de irredutíveis I_j, então

$$\chi_D(M) = \prod_k \prod_j \chi_{D_k}(I_j).$$

Exemplo 3.2.1. Fixemos $D(x) = x - a \in F_q[x]$ um polinômio irredutível de grau $d = 1$ e raiz a. Calculemos $M_1 := \sum_{\substack{\mathrm{Deg}(I)=1,\\ I \text{mônico}}} \chi_(D)(I)$. Temos:

$$M_1 = \sum_{\deg(I)=1} \chi(I) = \sum_{I=x-k} \left\{ \left[N(D(k)) \right]^{\frac{q-1}{2}} \right\}^* =$$

$$= \sum_{k \in F_q} \left\{ [k-a]^{\frac{q-1}{2}} \right\}^* = \frac{q-1}{2} - \frac{q-1}{2} = 0,$$

porque a expressão acima entre chaves é 1 se $k-a$ é um quadrado e -1 caso contrário (observemos que a norma de F_q^* sobre F_q^* é a identidade).

3.2.2 A L-série de Artin

Seja m livre de quadrados em $A = \mathbb{F}_q[x]$. A $L-$ **série** correspondente ao símbolo de Legendre χ_m se define por

$$L(s, \chi_m) = \sum_{n \text{ mônico}} \chi_m(n).|n|^{-s},$$

onde $|n| = q^{\deg(n)}$.

Escrevendo

$$L(s, \chi_m) = \sum_{d=0}^{\infty} \left(\sum_{\substack{n \text{ mônico,} \\ \deg(n)=d}} \chi_m(n) \right) q^{-ds},$$

e denotando por M_d a soma $\sum_{\substack{n \text{ mônico,} \\ \deg(n)=d}} \chi_m(n)$, podemos reescrever $L(s, \chi_m)$ na forma

$$L(s, \chi_m) = \sum_{d=0}^{\infty} M_d q^{-ds}.$$

LEMA 3.2.1. ***[Teorema de Artin para extensões quadráticas de*** $\mathbb{F}_q(x)$***]*** *([9], Teorema 0.6. para $l = 2$) Sejam $m \in A$ livre de quadrados de grau d, B fecho integral de $A = \mathbb{F}_q[x]$ em $F = \mathbb{F}_q(x)\sqrt{m}$, h_B a ordem do grupo de Picard de B (*$\mathrm{Pic}(B) = \frac{\textit{grupo dos ideais inversíveis}}{\textit{grupo dos ideais principais}}$*), R_B o regulador, d_B o discriminante de B sobre A, e g o gênero de F/K. Temos:*

1. *Se m tem grau ímpar, então o lugar ∞ ramifica em F. Neste caso, $d = 2g + 1$ e $L(1, \chi_m) = \frac{q^{1/2} h_B}{\sqrt{|d_B|}}$;*
2. *Se m tem grau par e seu coeficiente dominante não é um quadrado em $\mathbb{F}_q$, então o lugar ∞ é inerte em F. Neste caso, $d = 2g + 2$ e $L(1, \chi_m) = \frac{q+1}{2} \frac{h_B}{\sqrt{|d_B|}}$;*
3. *Se m tem grau par e seu coeficiente dominante é um quadrado em $\mathbb{F}_q$, então o lugar ∞ decompõe em F. Neste caso, $d = 2g + 2$ e $L(1, \chi_m) = \frac{(q-1) h_B R_B}{\sqrt{|d_B|}}$.*

LEMA 3.2.2. *([18], Teorema 17.8.A) Nas condições do Teorema de Artin, se $h := h(F)$ denota o número de classes de divisores de grau 0 de F, temos:*

1. *$h = h_B$, se ∞ ramifica;*
2. *$h = h_B/2$, se ∞ é inerte;*
3. *$h = h_B R_B$, se ∞ decompõe.*

Além disso, $|d_B| = q^d$.

LEMA 3.2.3. *([18], Lema 17.10.) Com a notação da L− série acima, se m é livre de quadrados, então* $M_d = 0$*, para* $d \geq \deg(m)$*.*

A relação entre os lemas acima fornece nossa primeira identificação explícita e finita para h, conforme os três teoremas seguintes.

TEOREMA 3.2.4. ***[Identidade finita e explícita de*** h ***(1)]*** *Sejam* $F = \mathbb{F}_q(x)\left(m^{1/2}\right)$ *uma extensão quadrática com gênero g, onde m é um polinômio livre de quadrados fixado sobre* $\mathbb{F}_q$ *com* $d = \deg(m)$ *ímpar. Então o lugar infinito se ramifica,* $d = 2g+1$ *e a L-série de Artin adaptada às classes de divisores dessa extensão fornece a fórmula:*

$$1 + \frac{1}{q}\sum_{\deg(n)=1}\chi_m(n) + \frac{1}{q^2}\sum_{\deg(n)=2}\chi_m(n) + ... + \frac{1}{q^{d-1}}\sum_{\deg(n)=d-1}\chi_m(n) = \frac{h}{q^g}$$

ou, equivalentemente,

$$h = q^g + q^{g-1}M_1 + ... + qM_{g-1} + M_g + \frac{1}{q}M_{g+1} + \frac{1}{q^2}M_{g+2} + ... + \frac{1}{q^g}M_{2g},$$

onde $M_i = \sum_{\deg(n)=i}\chi_m(n)$ *indica a soma dos símbolos de Legendre polinomiais para polinômios mônicos n com* $\deg(n) = i$*.*

Demonstração. $L(1,\chi_m) = \sum_{i=0}^{\infty}\left(\sum_{\substack{n \text{ mônico}\\ \deg(n)=i}}\chi_m(n)\right)q^{-i} =$

$$\sum_{i=0}^{d-1}\left(\sum_{\substack{n \text{ mônico}\\ \deg(n)=i}}\chi_m(n)\right)q^{-i} =$$

$$1 + \frac{1}{q}\sum_{\substack{n \text{ mônico}\\ \deg(n)=1}}\chi_m(n) + \frac{1}{q^2}\sum_{\substack{n \text{ mônico}\\ \deg(n)=2}}\chi_m(n) + \cdots + \frac{1}{q^{d-1}}\sum_{\substack{n \text{ mônico}\\ \deg(n)=d-1}}\chi_m(n) =$$

$$\frac{q^{1/2}h_B}{\sqrt{|d_B|}} = \frac{q^{1/2}h}{\sqrt{q^d}} = hq^{1/2-1/2\cdot(2g+1)} = \frac{h}{q^g}.$$

Como $d - 1 = 2g$, segue-se a segunda igualdade. □

TEOREMA 3.2.5. ***[Identidade finita e explícita de*** h ***(2)]*** *Sejam* $F = \mathbb{F}_q(x)\left(m^{1/2}\right)$ *uma extensão quadrática com gênero* g*, onde* m *é um polinômio livre de quadrados fixado sobre* $\mathbb{F}_q$ *com* $d = \deg(D)$ *par e coeficiente dominante não quadrado em* $\mathbb{F}_q$*. Então o lugar infinito é inerte,* $d = 2g+2$ *e a L-série de Artin adaptada às classes de divisores dessa extensão fornece a fórmula:*

$$1 + \frac{1}{q}\sum_{\deg(n)=1}\chi_m(n) + \frac{1}{q^2}\sum_{\deg(n)=2}\chi_m(n) + ... + \frac{1}{q^{d-1}}\sum_{\deg(n)=d-1}\chi_m(n) = \frac{h\left(\frac{q+1}{q}\right)}{q^g}$$

ou, equivalentemente,

$$h = \frac{q}{q+1}\left(q^g + q^{g-1}M_1 + ... + qM_{g-1} + M_g + \frac{1}{q}M_{g+1} + ... + \frac{1}{q^{g+1}}M_{2g+1}\right),$$

onde $M_i = \sum_{\deg(n)=i}\chi_m(n)$ *indica a soma dos símbolos de Legendre polinomiais para polinômios mônicos* n *com* $\deg(n) = i$*.*

Demonstração. $L(1,\chi_m) = \sum_{i=0}^{\infty}\left(\sum_{\substack{n\text{mônico}\\ \deg(n)=i}}\chi_m(n)\right)q^{-i} =$

$$\sum_{i=0}^{d-1}\left(\sum_{\substack{n\text{mônico}\\ \deg(n)=i}}\chi_m(n)\right)q^{-i} =$$

$$1 + \frac{1}{q}\sum_{\substack{n\text{mônico}\\ \deg(n)=1}}\chi_m(n) + \frac{1}{q^2}\sum_{\substack{n\text{mônico}\\ \deg(n)=2}}\chi_m(n) + \cdots + \frac{1}{q^{d-1}}\sum_{\substack{n\text{mônico}\\ \deg(n)=d-1}}\chi_m(n) =$$

$$\frac{(q+1)h_B}{2\sqrt{|d_B|}} = \frac{(q+1)2h}{2\sqrt{q^{2g+2}}} = \frac{h}{q^g}\cdot\frac{q+1}{q}.$$

Como $d-1 = 2g+1$, segue-se a segunda igualdade. □

TEOREMA 3.2.6. ***[Identidade finita e explícita de*** h ***(3)]*** *Sejam* $F = \mathbb{F}_q(x)\left(m^{1/2}\right)$ *uma extensão quadrática com gênero* g*, onde* m *é um polinômio livre de quadrados fixado sobre* $\mathbb{F}_q$ *com* $d = \deg(m)$ *par e coeficiente dominante quadrado em* $\mathbb{F}_q$*. Então o lugar infinito se*

decompõe, $d = 2g + 2$ e a L-série de Artin adaptada às classes de divisores dessa extensão fornece a fórmula:

$$1 + \frac{1}{q} \sum_{\deg(n)=1} \chi_m(n) + \frac{1}{q^2} \sum_{\deg(n)=2} \chi_m(n) + ... + \frac{1}{q^{d-1}} \sum_{\deg(n)=d-1} \chi_m(n) = \frac{h\left(\frac{q-1}{q}\right)}{q^g}$$

ou, equivalentemente,

$$h = \frac{q}{q-1}\left(q^g + q^{g-1}M_1 + ... + qM_{g-1} + M_g + \frac{1}{q}M_{g+1} + ... + \frac{1}{q^{g+1}}M_{2g+1}\right),$$

onde $M_i = \sum_{\deg(M)=i} \chi(M)$ indica a soma dos símbolos de Legendre polinomiais para polinômios mônicos M com $\deg(M) = i$.

Demonstração. $L(1, \chi_m) = \sum_{i=0}^{\infty} \left(\sum_{\substack{n\text{mônico} \\ \deg(n)=i}} \chi_m(n) \right) q^{-i} =$

$$\sum_{i=0}^{d-1} \left(\sum_{\substack{n\text{mônico} \\ \deg(n)=i}} \chi_m(n) \right) q^{-i} =$$

$$1 + \frac{1}{q} \sum_{\substack{n\text{mônico} \\ \deg(n)=1}} \chi_m(n) + \frac{1}{q^2} \sum_{\substack{n\text{mônico} \\ \deg(n)=2}} \chi_m(n) + \cdots + \frac{1}{q^{d-1}} \sum_{\substack{n\text{mônico} \\ \deg(n)=d-1}} \chi_m(n) =$$

$$\frac{(q-1)R_B h_B}{\sqrt{|d_B|}} = \frac{(q-1)h}{\sqrt{q^{2g+2}}} = \frac{h}{q^g} \cdot \frac{q-1}{q}.$$

Como $d - 1 = 2g + 1$, segue-se a segunda igualdade. □

Segue-se imediatamente dos três teoremas anteriores, o seguinte:

Teorema 3.2.7. ***[Identidade finita e explícita de h assintótica]*** *Sejam $F = \mathbb{F}_q(x)\left(m^{1/2}\right)$ uma extensão quadrática com gênero g, onde m é um polinômio livre de quadrados fixado sobre $\mathbb{F}_q$ com $d = \deg(m)$. Então a L-série de Artin adaptada às classes de divisores dessa extensão fornece a fórmula:*

$$1 + \frac{1}{q} \sum_{\deg(n)=1} \chi_m(n) + \frac{1}{q^2} \sum_{\deg(n)=2} \chi_m(n) + ... + \frac{1}{q^{d-1}} \sum_{\deg(n)=d-1} \chi_m(n) \approx \frac{h}{q^g}$$

ou, equivalentemente,

$$h \approx q^g + q^{g-1}M_1 + ... + \frac{1}{q^{g+1}}M_{2g+1},$$

se ∞ *é inerte ou se decompõe* ($d = 2g + 2$)*, ou*

$$h \approx q^g + q^{g-1}M_1 + ... + \frac{1}{q^g}M_{2g},$$

se ∞ *ramifica* ($d = 2g + 1$)*. Como usual,* $M_i = \sum_{\deg(n)=i} \chi_m(n)$ *indica a soma dos símbolos de Legendre polinomiais para polinômios mônicos* n *com* $\deg(n) = i$*.*

A seguir, vamos estudar mais alguns exemplos sobre as somas M_i que ocorrem nas L-séries de Artin adaptadas e adiantar algumas considerações que serão provadas no Capítulo 4.

Exemplo 3.2.2. Seja $D(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau $d = 2$. Calculemos M_1.

É um exercício em [18], página 43, exercícios 2 a 5, mostrar que

$$M_1 = \sum_{\deg(I)=1} \chi_D(I) = \sum_{k\in\mathbb{F}_q} \left\{ [N_1(D(k))]^{\frac{q-1}{2}} \right\}^* = \sum_{k\in\mathbb{F}_q} \left\{ [D(k)]^{\frac{q-1}{2}} \right\}^* = \pm 1$$

Observemos que, pela L-série de Artin adaptada, sendo $d = 2$ então $g = 0$, de onde segue-se imediatamente que $M_1 = -1$, para todo q, se ∞ é inerte, isto é, se o coeficiente dominante de $D(x)$ é um quadrado. Se ∞ se decompõe, isto é, se o coeficiente dominante de $D(x)$ não é um quadrado, então $M_1 = 1$, para todo q. Observamos, neste exemplo, que M_1 parece depender de D, no entanto, veremos, no Capítulo 4, que os M_i´s pertencem a intervalos cujos centros e raios dependem apenas de d (ou, equivalentemente, do gênero g) e de q.

Já para $d = 3$ esses invariantes elementares M_1 oferecem muito mais dificuldade para se deixarem revelar. Essa dificuldade faz juz à sua importância, pois, se $g = 1$, então $h = q + M_1 + 1$, valendo relações similares em gêneros 2 e 3, como veremos no próximo capítulo. Tais fatos não estão presentes na literatura disponível.

Exemplo 3.2.3. Seja $D(x) \in \mathbb{F}_3[x]$ um polinômio irredutível de grau $d = 3$. Calculemos M_1.

Os polinômios mônicos irredutíveis de grau 3 sobre F_3 fornecem

$$M_1 = \sum_{\deg(I)=1} \chi_D(I) = \sum_{k\in\mathbb{F}_3} \left\{ [D(k)]^{\frac{q-1}{2}} \right\}^* = \pm 1, \pm 3$$

que são todas as somas possíveis de três raízes quadradas de 1.

Exemplo 3.2.4. Seja $D(x) \in \mathbb{F}_q[x]$, $q = 3$ ou 5, um polinômio irredutível de grau $d = 3$. Examinemos M_2.

Cálculos rotineiros, embora tediosos (veja tabela 4.1), revelam que, para os polinômios irredutíveis de grau 3, sobre $\mathbb{F}_3$, temos $M_2 = 3 = q$. Para alguns dos quarenta polinômios irredutiveis de grau 3, sobre $\mathbb{F}_5$, temos $M_2 = 5 = q$. Veremos no próximo capítulo que no caso de gênero 1, realmente teremos $M_2 = q$.

3.3 O Teorema de Stein-Teske-Scheidler

Em [23], Stein e Teske descrevem um método de aproximação para h de corpos hiperelípticos K por meio de um truncamento da produtória infinita de Euler. A ideia básica dessa técnica é encontrar inteiros E e L tais que $|h - E| \leq L^2$. Havendo encontrado um tal intervalo de comprimento $2L^2 - 1$, pode-se procurar por h neste intervalo pelos métodos *baby step - giant step* ou *Pollard's kangaroo* em $\mathcal{O}(L)$ operações. A base teórica de seu método está no teorema que enunciaremos a seguir. O Exemplo 2.2. de [21] permite que enunciemos tal teorema para gênero $g \geq 1$, ao invés da hipótese original $g \geq 2$. A complexidade computacional desse método é $\mathcal{O}\left(q^{1/4}\right)$ e $\mathcal{O}\left(q^{3/4}\right)$, para $g = 1$ e $g = 2$, respectivamente. Para $g \geq 3$, obtém-se complexidade $\mathcal{O}\left(q^{\left(\frac{2g-1}{5}\right)}\right)$.

Curiosamente, esse teorema, juntamente com as IFEs da seçãoanterior serão a base para as IFE's e expressões quase $q-$ árias que apresentaremos no Capítulo 4.

Teorema 3.3.1. *(Stein-Teske-Scheidler) ([23], Teorema 1.1.; [21], Exemplo 2.2.) Seja* $F = \mathbb{F}_q(x)\sqrt{D}$, *q ímpar,* $D \in \mathbb{F}_q[x]$ *livre de quadrados de grau d, um CFA com gênero* $g \geq 1$.

(1) Se $d = 2g + 2$ e o coeficiente dominante de D é um quadrado em $\mathbb{F}_{||}^*$, isto é, ∞ se decompõe (veja Teorema 3.2.6), então:

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \chi(P)^{\frac{n}{\nu}} = -1 - \sum_{i=1}^{2g} w_i^n;$$

(2) Se $d = 2g + 1$, isto é, ∞ ramifica (veja Teorema 3.2.4), então:

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \chi(P)^{\frac{n}{\nu}} = -\sum_{i=1}^{2g} w_i^n;$$

(3) Se $d = 2g + 2$ e o coeficiente dominante de D não é um quadrado em F_q^*, isto é, ∞ é inerte (veja Teorema 3.2.5), então:

$$\sum_{\nu|n} \nu \sum_{\deg(P)=\nu} \chi(P)^{\frac{n}{\nu}} = (-1)^{n+1} - \sum_{i=1}^{2g} w_i^n.$$

Aqui, w_i, $i = 1, \cdots, 2g$ são os inversos das raízes do $L-$ polinômio da função zeta de F. Além disso, o símbolo de Legendre polinomial $\chi(P)(= \chi_D(P))$ ocorre nos somatórios para P percorrendo todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q[x]$ de grau ν.

Capítulo 4

Identidades finitas e explícitas para h

4.1 Exemplos preliminares

Neste capítulo, mostraremos que, para $3 \leq \deg(D) \leq 8$, $\mathrm{Cpx}(a_i) = \mathrm{Cpx}(M_i)$, onde M_i são os coeficientes da L-série de Artin, a_i os coeficientes do L-polinômio do correspondente corpo de funções e o custo Cpx será definido oportunamente. O método utilizado pode ser estendido para graus maiores do que 8, mas a complicação dos cálculos cresce rapidamente parametrizada pela complexidade das partições do inteiro i (veja a demonstração dos casos $\deg(D) = 7$ e 8). É fácil perceber quais as conjecturas que podem ser feitas sobre os M_i´s e programas computacionais podem confirmá-las para valores maiores de i em uma fase seguinte, computacional, da pesquisa. Além disso, acreditamos que uma análise mais profunda das valorações e da estrutura dos divisores da extensão $K = \mathbb{F}_q(x)\sqrt{D}$ forneça novos métodos para a determinação rigorosa dos valores de $M_i, 4 \leq i$, evitando-se a complicação exemplificada nos casos $\deg(D) = 7$ e 8.

Alternativamente, poderíamos utilizar $L(K, 1) = h$ e considerar

$$\mathrm{Cpx}\,(h) = \max\left\{\mathrm{Cpx}\,(a_i)\,, 1 \leq i \leq g\right\},$$

onde os a_i´s são os coeficientes de $L(K, t)$. Entretanto, a IF (veja [19]) que conhecemos para a_i

é função de N_j = número de divisores primos de grau j, $j \leq i$, e não há na literatura disponível IFE´s para N_j em geral (ver, entretanto, a contagem de pontos em variedades algébricas por meio de somas de Gauss e de Jacobi em [11].). A fórmula (ver [24])

$$N_j = q^j + 1 - \sum_{k=1}^{2g} (w_k)^j$$

não serve como IFE porque w_k é função dos coeficientes a_i´s de $L(K,t)$, para todo $1 \leq k \leq 2g$, os quais, por sua vez, são obtidos da função zeta de K, ou seja, da exponencial de uma série onde os coeficientes são os próprios N_j.

Exemplo 4.1.1. Consideremos o polinômio mônico irredutível $D(X) = X^3 + 2X + 1 \in \mathbb{F}_5[X]$ e a extensão $K = \mathbb{F}_5(x)(D^{1/2})$. Pela fatoração do $L-$polinômio (veja Teorema 2.6.10), $a_1 = -\sum_{i=1}^{2g} w_i$, que, pelo Teorema 3.3.1 para $n = 1$, é igual a I_1. Mas

$$M_1 = I_1 = \sum_{\mathrm{Deg}(I)=1} \chi_D(I) = \sum_{\substack{x-a \\ a\in\mathbb{F}_5}} \chi_D(x-a) = \sum_{a\in\mathbb{F}_5} \left\{ [N(D(a))]^{\frac{5-1}{2}} \right\}^* =$$

$$\sum_{a\in\mathbb{F}_5} \left\{ \left(a^3 + 2a + 1)\right)^2 \right\}^* = \left\{1^2\right\}^* + \left\{4^2\right\}^* + \left\{13^2\right\}^* + \left\{34^2\right\}^* + \left\{73^2\right\}^* = 1 + 1 - 1 + 1 - 1 = 1.$$

Cálculos análogos fornecem $M_2 = 5$, de onde também obtemos, com a L-série de Artin adaptada (Teorema 3.2.5),

$$h = q + M_1 + \frac{1}{q} M_2 = 5 + 1 + \frac{1}{5} \cdot 5 = 7.$$

Notemos que o $L-$polinômio é dado por $L(K,t) = 1 + a_1 t + qt^2$ e h também pode se obter como $h = L(K,1) = 1 + 1 + 5 = 7$.

Assim, os importantes e notáveis invariantes N_1, h e $a_1 = -\sum_{i=1}^{2g} w_i$, possuem IFE´s por meio das quais são calculados efetivamente como função de M_1 e M_2, quando $D(X)$ é irredutível em $\mathbb{F}_5[X]$, um resultado ausente, aparentemente, na literatura disponível. É plausível supor que isso se generalize para qualquer q ímpar.

Exemplo 4.1.2. Fixemos o polinômio $D(X) = X^4 + X^2 + 2 \in \mathbb{F}_3[X]$. Como os polinômios irredutíveis de grau 2 são apenas X^2+1, X^2+X+2 e X^2+2X+2, segue-se facilmente que $D(X)$

é irredutível sobre $\mathbb{F}_3$. Podemos verificar por meio de cálculos tediosos (veja a tabela 4.1 a seguir) que

$$M_3 := \sum_{\deg(M)\,=\,3} \chi_D(M(X)) = -3,$$

onde a soma se estende para todos os polinômios mônicos de grau 3. Há 27 polinômios mônicos sobre $\mathbb{F}_3$ conforme a tabela seguinte:

Tabela 4.1: Símbolos polinomiais de Legendre sobre polinômios mônicos de grau 3.

$m(X)$	χ_D		χ_D		χ_D		χ_D		χ_D	
X^3+X	-1	X^3+1	1	X^3+X^2+X	-1	X^3+2X^2+X+1	1	X^3+2X+2	-1	
X^3+2X	-1	X^3+2	1	X^3+2X^2+X	-1	X^3+2X^2+2X+1	1	X^3+X^2	1	
X^3+X+1	-1	X^3+2X^2+2X	1	X^3+X^2+2X	1	X^3+X^2+X+2	1	X^3+2X^2	1	
X^3+X+2	-1	X^3+X^2+X+1	1	X^3+X^2+2X+2	1	X^3+X^2+1	-1			
X^3+2X+1	-1	X^3+X^2+2X+1	-1	X^3+2X^2+X+2	1	X^3+X^2+2	-1			
X^3	-1	X^3+2X^2+2	-1	X^3+2X^2+2X+2	-1	X^3+2X^2+1	-1			
TOTAIS	-6		2		0		0		1	-3

Por exemplo,

$$\chi_D(X^3+X) = \chi_D(X(X^2+1)) = -\chi_D(X^2+1) = \chi_D(X)\chi_D(X^2+1) = [N_1(D(0))]^* - [N_2(D(\beta))]^*,$$

onde β é raiz de X^2+1 em $\mathbb{F}_{3^2}$. A última expressão fica, então,

$$[N_1(2)]^*[N_2(D(\beta))]^* = \left[2^{\frac{3-1}{2}}\right]\left\{\left[\beta^2\left(\beta^2+1\right)+2\right]^{(1+3)\frac{3-1}{2}}\right\}^* = (-1)^* \cdot \left\{2^4\right\}^* = (-1)\cdot 1 = -1.$$

Mostraremos (Teoremas 4.2.2 e 4.2.3) que a soma de todos os q^3 símbolos de Legendre polinomiais é $\pm q$, isto é, $M_3 = \pm q$, generalizando este exemplo em $\mathbb{F}_3$.

Vamos estudar na próxima seção algumas propriedades fundamentais das somas M_i que constituem as parcelas da L-série de Artin. De passagem, observamos que quando $g = 0$, então $\deg(D) = 1$ ou $\deg(D) = 2$. Se $\deg(D) = 2$, temos, das L-séries de Artin adaptadas (Teoremas 3.2.5 e 3.2.6, respectivamente) as seguintes fórmulas para h:

$\frac{q+1}{q}h = 1 + \frac{M_1}{q} = \frac{q+M_1}{q}$, quando ∞ é inerte e

$\frac{q-1}{q}h = 1 + \frac{M_1}{q} = \frac{q+M_1}{q}$, quando ∞ se decompõe.

Concluímos, respectivamente, que $M_1 = 1$ ou -1, uma vez que, pela desigualdade de Hasse-Weil, $h = 1$ quando $g = 0$. Quando ∞ ramifica ($\deg(D) = 1$), já havíamos demonstrado no Exemplo 3.2.1 que $M_1 = 0$.

Vale ressaltar que estamos apresentando uma IFE para h e não uma aproximação. Dessa forma, a apresentação de uma IFE para h objetiva, além de oferecer uma alternativa ao truncamento da produtória infinita de Euler, motivar e iniciar o desenvolvimento e análise das somas de símbolos de Legendre polinomiais presentes na IFE de h dos CFA $\mathbb{F}_q(x)\sqrt{D}$, de gêneros $g = 1, 2$ e 3, que são os casos mais importantes na criptografia contemporânea.

Para gênero maior ou igual a 1, o seguinte teorema, que diz respeito aos caráteres multiplicativos de $\mathbb{F}_q$, fornece informações sobre a independência de certas médias de símbolos de Legendre em relação a D e q.

TEOREMA 4.1.1. *([16] Teorema 4.4.10.) Seja Ψ um caráter multiplicativo de $\mathbb{F}_q$ de ordem $m > 1$ e seja $f(x) \in \mathbb{F}_q[x]$ um polinômio de grau positivo que não seja uma potência m-ésima de algum polinômio em $\mathbb{F}_q[x]$. Seja d o número de raízes de $f(x)$ em seu corpo de decomposição sobre $\mathbb{F}_q$. Então,*

$$\left| \sum_{c \in \mathbb{F}_q} \Psi(f(c)) \right| \leq (d-1)\sqrt{q}.$$

No que segue, utilizaremos o caráter multiplicativo módulo 2 ou símbolo de Legendre polinomial definido anteriormente, uma vez que trabalharemos em extensões quadráticas de $\mathbb{F}_q(x)$, isto é, $\chi_D(I) = \left\{ [N_i(D(\beta))]^{\frac{q-1}{2}} \right\}^* = \chi(I)$ (quando o polinômio fixado D estiver subentendido), onde $N_i : u \in \mathbb{F}_{q^i} \mapsto N_i(u) = u^{1+q+\cdots+q^{i-1}} \in \mathbb{F}_q$ é a **norma de $\mathbb{F}_{q^i}$ sobre $\mathbb{F}_q$** e o asterisco * da igualdade indica uma imersão do grupo das unidades de $\mathbb{F}_q^*$ no grupo das unidades complexas em $S^1 \subset \mathbb{C}$. Lembremos que

$$M_i = \sum_{\deg(M) = i} \chi(M)$$

indica a soma dos símbolos de Legendre polinomiais para polinômios mônicos M com $\deg(M) = i$. Similarmente,

$$I_i = \sum_{\deg(I)\,=\,i} \chi(I)$$

indica a soma dos símbolos de Legendre polinomiais para polinômios mônicos **irredutíveis** I com $\deg(I) = i$. Estabeleceremos relações entre M_i e I_i como evidências convincentes para algumas conjecturas e para as IFE´s de h em geral no contexto de extensões quadráticas $\mathbb{F}_q(x)(\sqrt{D})$.

PROPOSIÇÃO 4.1.2. *Seja I_1 a soma de símbolos de Legendre polinomiais, associados ao polinômio irredutível $D(x) \in \mathbb{F}_q[x]$, com $\deg(D) = 3$, para os polinômios mônicos irredutíveis de grau 1 sobre $\mathbb{F}_q$. Então, $\frac{I_1}{\sqrt{q}}$ pertence ao intervalo de centro 0 e raio $\deg(D) - 1 = 2$, independente de D e q.*

Demonstração. O Teorema 4.1.1 acima fornece para I_1 a seguinte estimativa:

$$|I_1| = \left|\sum_{\deg(I)=1} \chi(I)\right| = \left|\sum_{c\in F_q} \left[(D(c))^{\frac{q-1}{2}}\right]^*\right| = \left|\sum_{c\in F_q} \Psi(D(c))\right| \leq (d-1)\sqrt{q} = 2\sqrt{q}.$$

□

PROPOSIÇÃO 4.1.3. *Seja I_2 a soma de símbolos de Legendre polinomiais, associados ao polinômio irredutível $D(x) \in \mathbb{F}_q[x]$, com $\deg(D) = 3$, para os polinômios mônicos irredutíveis de grau $i = 2$ sobre $\mathbb{F}_q$. Então, $\frac{I_2}{q}$ pertence ao intervalo $\left[-\frac{3}{2}, \frac{1}{2}\right]$ independente de D e q.*

Demonstração. O teorema acima fornece para I_2 a seguinte estimativa:

$$\left|\sum_{c\in\mathbb{F}_{q^2}} \Psi(D(c))\right| =$$

$$\left|\sum_{c\in\mathbb{F}_q} \Psi(D(c)) + \sum_{c\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q} \Psi(D(c))\right| =$$

$$\left|\sum_{c\in\mathbb{F}_q} \left[(D(c))^{(1+q)\frac{q-1}{2}}\right]^* + \sum_{c\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q} \left[(D(c))^{(1+q)\frac{q-1}{2}}\right]^*\right| =$$

$$\left|\sum_{c\in\mathbb{F}_q} 1 + 2I_2\right| = |q + 2I_2| \leq (d-1)\sqrt{q^2} = 2q.$$

As justificativas para a terceira igualdade são as seguintes: quando $c \in \mathbb{F}_q$, $D(c) \in \mathbb{F}_q^*$ e $D(c)^{1+q} = D(c)^{q-1} \cdot D(c)^2 = D(c)^2$, de onde segue-se que $(D(c)^{1+q})^{\frac{q-1}{2}} = \left(D(c)^{\frac{q-1}{2}}\right)^2 = 1$, portanto

$$\sum_{c \in \mathbb{F}_q} \left[(D(c))^{(1+q)\frac{q-1}{2}}\right]^* = q.$$

Para o segundo somatório, temos: cada $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ é raiz de um polinômio irredutível de grau 2 sobre $\mathbb{F}_q$ e seu conjugado $c^q \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ também o é. Como o símbolo de Legendre polinomial não depende da raiz escolhida, temos:

$$\left(D(c)^{1+q}\right)^{\frac{q-1}{2}} = \left(D(c^q)^{1+q}\right)^{\frac{q-1}{2}} = \pm 1 \in \mathbb{F}_q$$

que corresponde a $\pm 1 \in \mathbb{C}$. Assim, o segundo somatório é igual a $2I_2$. □

Corolário 4.1.4. *Seja $D(x) \in \mathbb{F}_q[x]$ um polinômio irredutível de grau 3 e $F = \mathbb{F}_q(x)\sqrt{D}$ o CFA de gênero $g = 1 = \frac{3-1}{2}$ associado à raiz quadrada de $D(x)$. Então $h = q + M_1 + k$, onde $k \in \{-1, 1, 3\}$. Dessa expressão, obtemos $Cpx(h) = \mathcal{O}(q) = \mathcal{O}(q^g)$ e $M_1 + k = \mathcal{O}(\sqrt{q})$.*

A demonstração desse corolário está após a definição que destacamos abaixo com o objetivo de se deixar claro o que entendemos por custo da expressão de um somatório S, denotado por $\mathrm{Cpx}(S)$, pela evidente importância desse custo para o cálculo da complexidade computacional de S.

Definição 4.1.1. Seja S um somatório de termos. O custo desse somatório, denotado por $\mathrm{Cpx}(S)$, se define como sendo o número de avaliações necessárias para se calcular S. Nos casos que trataremos, S é uma soma de caráteres aplicados a polinômios, logo $\mathrm{Cpx}(S)$ dar-se-á pelo número de polinômios requisitados para a avaliação desses caráteres.

Demonstração. Observamos, inicialmente, que, pela L-série de Artin adaptada, $h = q + M_1 + M_2/q$, de onde se segue que $q|M_2$ ou $M_2/q \in \mathbb{Z}$. Obtivemos, nos teoremas anteriores, as seguintes estimativas:

$$|M_1| = |I_1| \leq 2\sqrt{q} \Rightarrow \left|\frac{M_1}{\sqrt{q}}\right| \leq 2 \Rightarrow \frac{(M_1)^2}{2q} \leq 2$$

e

$$\frac{I_2}{q} \in \left[-\frac{3}{2}, \frac{1}{2}\right].$$

Temos:

$$M_2 = I_2 + \sum_{I=(x+c)^2} \chi_D(I) + \sum_{\substack{I=(x+a)(x+b),\\ a\neq b}} \chi_D(I).$$

Denotemos, de agora em diante, a soma $\sum_{\substack{I=(x+a)(x+b),\\ a\neq b}} \chi_D(I)$ por φ_{21}. Temos:

$$M_2 = I_2 + q + \varphi_{21} \text{ e } (M_1)^2 = (I_1)^2 = q + 2\varphi_{21}.$$

Segue-se que:

$$\frac{M_2}{q} = 1 + \frac{(M_1)^2}{2q} - \frac{1}{2} + \frac{I_2}{q} = \frac{1}{2} + a + b, \text{ onde } a \in [0, 2]$$

e $b \in \left[-\frac{3}{2}, \frac{1}{2}\right]$, de onde se obtém

$$\frac{M_2}{q} \in \{-1, 0, 1, 2, 3\}.$$

Segue-se, então, que $h = q + M_1 + k$, onde $k \in \{-1, 1, 3\}$. Como q e k são constantes, então

$$\text{Cpx}h = \text{Cpx}(M_1) = \text{Cpx}\left(\sum_{\text{Deg}(n)=1} \chi_D(n)\right).$$

Como há q polinômios mônicos de grau 1 sobre $\mathbb{F}_q$, há q avaliações requisitadas para o cálculo de M_1, logo,pela Definição 4.1.1, temos $\text{Cpx}M_1 = q$.

Ainda, como há q^2 polinômios mônicos de grau 2, então ocorrem q^2 símbolos ± 1's em M_2, de onde vem que M_2 é um inteiro ímpar. Logo, $\frac{M_2}{q} \in \{-1, 1, 3\}$. □

É interessante comparar este corolário com o procedimento de Stein-Teske. Pela desigualdade de Hasse-Weil, aquele procedimento considera um intervalo de comprimento $4q^{1/2}$ para a busca de h por um algoritmo. Por outro lado, este corolário oferece uma expressão explícita e finita para

h em um conjunto com três inteiros. Assim, este corolário nos dá uma medida clara da diferença entre identificar h por uma expressão infinita e por meio de uma IFE.

Nas condições do corolário anterior, obtemos ainda:

COROLÁRIO 4.1.5. *h e a_1 = coeficiente de grau 1 de $L(K,t)$ da extensão quadrática $K = \mathbb{F}_q(x)(\sqrt{D})$ têm paridade invariante ímpar, independente de D.*

Demonstração. Da L-série de Artin adaptada, $h = q + M_1 + M_2/q$, com q, M_1 e M_2 ímpares, logo h é ímpar. Neste caso, $L(K,t) = 1 + a_1 t + a_2 t^2 = 1 + a_1 t + qt^2$ (pois $a_0 = 1$ e $a_2 = q$). Assim, $h = L(K,1) = 1 + a_1 + q$ e, como h e q são ímpares, então a_1 também o é. □

PROPOSIÇÃO 4.1.6. *Seja I_4 a soma de símbolos de Legendre polinomiais, associados ao polinômio irredutível $D(x) \in \mathbb{F}_q[x]$, com $\deg(D) = 4$, para os polinômios mônicos irredutíveis de grau 4 sobre $\mathbb{F}_q$. Então, I_4/q^2 pertence ao intervalo $\left[-1, \frac{1}{2}\right]$, independente de D e q.*

Demonstração. Seja I_4 a soma de símbolos de Legendre polinomiais, associados ao polinômio irredutível $D(x) = \mathbb{F}_q[x]$, com $\deg(D) = 4$, para os polinômios mônicos irredutíveis de grau 4 sobre $\mathbb{F}_q$. Assim, temos para I_4 a seguinte estimativa:

$$\left|\sum_{c\in\mathbb{F}_{q^4}} \Psi(D(c))\right| =$$

$$\left|\sum_{c\in\mathbb{F}_q} \Psi(D(c)) + \sum_{c\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q} \Psi(D(c)) + \sum_{c\in\mathbb{F}_{q^4}\setminus\mathbb{F}_{q^2}} \Psi(D(c))\right| =$$

$$\left|\sum_{c\in\mathbb{F}_q} \left[N_4\left(D\left(c\right)\right)^{\frac{q-1}{2}}\right]^* + \sum_{c\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q} \left[N_4\left(D\left(c\right)\right)^{\frac{q-1}{2}}\right]^* + \sum_{c\in\mathbb{F}_{q^4}\setminus\mathbb{F}_{q^2}} \left[N_4\left(D\left(c\right)\right)^{\frac{q-1}{2}}\right]^*\right| =$$

$$\left|\sum_{c\in\mathbb{F}_q} 1 + \sum_{c\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q} 1 + 4I_4\right| =$$

$$\left|q + \left(q^2 - q\right) + 4I_4\right| =$$

$$\left|q^2 + 4I_4\right| \leq (d-1)\sqrt{q^4} = 3q^2.$$

Segue-se que $-1 \leq \frac{I_4}{q^2} \leq \frac{1}{2}$.

As justificativas para a terceira igualdade acima são as seguintes: se $c \in \mathbb{F}_q$, então $D(c) \in \mathbb{F}_q$ e

$$N_4(D(c))^{\frac{q-1}{2}} = \left(D(c)^{1+q+q^2+q^3}\right)^{\frac{q-1}{2}} = D(c)^{\frac{q^4-1}{2}} = \left(D(c)^{q-1}\right)^{\frac{(q+1)(q^2+1)}{2}} = 1;$$

se $c \in \mathbb{F}_{q^2}$, então $D(c) \in \mathbb{F}_{q^2}$ e

$$N_4(D(c))^{\frac{q-1}{2}} = \left(D(c)^{1+q+q^2+q^3}\right)^{\frac{q-1}{2}} = D(c)^{\frac{q^4-1}{2}} = \left(D(c)^{q^2-1}\right)^{\frac{(q^2+1)}{2}} = 1;$$

se $c \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$, então c^q, c^{q^2}, $c^{q^3} \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$, pois são essas as raízes de um mesmo polinômio irredutível de grau 4 sobre $\mathbb{F}_q$. Os elementos de $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ se agrupam em conjuntos de raízes de polinômios irredutíveis de grau 4 sobre $\mathbb{F}_q$ do tipo $\left\{c, c^q, c^{q^2}, c^{q^3}\right\}$, logo $\sum_{c \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}} N_4 \left[(D(c))^{\frac{q-1}{2}}\right]^* = 4I_4$. □

Observamos que, aqui também, $\frac{I_4}{q^2}$ localiza-se em um intervalo que só depende de g (ou $\deg(D)$), e não de D.

Como já mencionado da seção 3.1, os corpos K de funções algébricas elípticos e hiperelípticos de gêneros $g = 1$, 2 e 3 são de grande serventia para os propósitos criptográficos. As principais razões são que h pode ser computado com esforço viável, a inviabilidade computacional para a solução do problema do logaritmo discreto é alta e a aritmética é eficiente no grupo de classes $Cl(K)$.

Apresentaremos nesta e nas próximas seções deste capítulo estimativas sobre a complexidade e ordem de grandeza de uma IFE para h, além de informações sobre IFE´s dos coeficientes a_i de $L(K,t)$ e sobre as somas I_i e M_i da L-série de Artin adaptada. O teorema seguinte corresponde às três situações estabelecidas pelo Teorema de Stein-Teske-Scheidler (Teorema 3.3.1).

TEOREMA 4.1.7. *Seja $K = \mathbb{F}_q(x)(\sqrt{D})$, com $D(x)$ irredutível em $\mathbb{F}_q[x]$.*

1. *Seja $\deg(D) = 2g+1$, com $g \geq 1$. Então, $a_i = M_i$, para $1 \leq i \leq 3$.*

2. *Seja $\deg(D) = 2g+2$, com $g \geq 1$. Então,*

(a) $a_1 = M_1 + 1$, $a_2 = M_2 + M_1 + 1$ *e* $a_3 = M_3 + M_2 + M_1 + 1$, *se* ∞ *se decompõe;*

(b) $a_1 = M_1 - 1$, $a_2 = M_2 - M_1 + 1$ *e* $a_3 = M_3 - M_2 + M_1 - 1$, *se* ∞ *é inerte.*

Demonstração.

Da parte (2) do Teorema 3.3.1, com $n = 1$, obtemos:

$$M_1 = I_1 = \sum_{\deg(P)=1} \chi(P) = -\sum_{i=1}^{2g} w_i = a_1, \tag{4.1}$$

onde a_j representa os coeficientes do $L-$polinômio. Para $n = 2$, obtemos:

$$\sum_{\deg(P)=1} \chi(P)^2 + 2 \sum_{\deg(P)=2} \chi(P) = q + 2I_2 = -\sum_{i=1}^{2g} w_i^2. \tag{4.2}$$

Segue-se que

$$(M_1)^2 = (a_1)^2 = \sum_{i=1}^{2g} (w_i)^2 + 2\sum_{i\neq j} w_i w_j = (-q - 2I_2) + 2a_2,$$

de onde obtém-se

$$2a_2 = (M_1)^2 + 2I_2 + q. \tag{4.3}$$

Mas

$$M_1^2 = \left(\sum_{\deg(P)=1} \chi(P) \right)^2 = \sum_{\deg(P)=1} \chi(P)^2 + 2 \cdot \sum_{\substack{\deg(P)=1,\ \deg(Q)=1,\\ P\neq Q}} \chi(P)\chi(Q) = q + 2\varphi_{21},$$

onde φ_{21} é a função simétrica de ordem 2 na expressão de M_1^2. Logo, (4.3) fica

$$2a_2 = q + 2\varphi_{21} + 2I_2 + q = 2(q + \varphi_{21} + I_2). \tag{4.4}$$

Mas

$$q + \varphi_{21} + I_2 = M_2 = \sum_{\substack{\deg(P)=2\\ P \text{ mônico}}} \chi(P),$$

o que se deduz particionando-se os mônicos de grau 2 em produtos de irredutíveis iguais de grau 1 (fornecendo o q), produto de irredutíveis distintos de grau 1 (fornecendo φ_{21}) e, finalmente, irredutíveis de grau 2 (fornecendo I_2). Assim, (4.4) equivale a $2a_2 = 2M_2$ ou

$$a_2 = M_2. \tag{4.5}$$

Analogamente, quando $a_1 = M_1 \pm 1$, obtemos

$$a_2 = M_2 \pm M_1 + 1, \tag{4.6}$$

pelas partes (3) e (1), respectivamente, do Teorema 3.3.1. Isso demonstra as afirmações feitas em relação a a_1 e a_2 nas duas partes do teorema. Para a_3, consideremos os três casos do enunciado. Antes, algumas igualdades importantes relacionando símbolos de Legendre.

Particionando o grau 3, obtemos para M_3 a expressão

$$M_3 = qM_1 + I_2I_1 + I_3 + \varphi_{31}. \tag{4.7}$$

De fato, temos:

$$\begin{aligned} M_3 &= \sum_{\substack{\mathrm{Deg}(p)=3 \\ p \text{ mônico}}} \chi_D(p) = \\ &\quad \sum_{\substack{\mathrm{Deg}(p_1)=1 \\ \mathrm{Deg}(p_2)=2,\ p_2 \text{ irredutivel}}} \chi_D(p_1)\chi_D(p_2) + \sum_{\substack{\mathrm{Deg}(p_i)=1 \\ p_i's \text{ distintos}}} \chi_D(p_1)\chi_D(p_2)\chi_D(p_3) \\ &+ \sum_{\substack{\mathrm{Deg}(p_i)=1 \\ p_1 \neq p_2}} \chi_D(p_1)^2\chi_D(p_2) + \sum_{\mathrm{Deg}(p)=1} \chi_D(p)^3 \\ &+ \sum_{\substack{\mathrm{Deg}(p)=3 \\ p \text{ irredutivel}}} \chi_D(p). \end{aligned} \tag{4.8}$$

O último membro da expressão acima consiste de cinco somatórios. É imediato perceber que o primeiro é I_1I_2, o segundo é φ_{31}, a expressão simétrica de ordem 3 que ocorre em M_1^3, e o quinto é I_3. Com cálculos elementares, verifica-se que o terceiro mais o quarto somatórios resultam em qM_1.

Agora, elevando-se M_1 ao cubo, obtemos:

$$(M_1)^3 = (3q-2)M_1 + 6\varphi_{31}. \tag{4.9}$$

De fato, temos, lembrando que $(\chi_D(p))^2$ é sempre igual a 1:

$$M_1^3 = \left(\sum_{c \in \mathbb{F}_q} \chi_D(x-c) \right)^3$$

$$
\begin{aligned}
&= \sum_{c\in\mathbb{F}_q} (\chi_D(x-c))^3 + 3\sum_{c\in\mathbb{F}_q} (\chi_D(x-c))^2 \left(\sum_{d\neq c} \chi_D(x-d)\right) \\
&+ 6 \sum_{\substack{a,b,c\in\mathbb{F}_q \\ a\neq b\neq c\neq a}} \chi_D(x-a)\chi_D(x-b)\chi_D(x-c) \\
&= \sum_{c\in\mathbb{F}_q} \chi_D(x-c) + 3\sum_{c\in\mathbb{F}_q} (M_1 - \chi_D(x-c)) + 6\varphi_{31} \\
&= \sum_{c\in\mathbb{F}_q} \chi_D(x-c) + 3\left(qM_1 - \sum_{c\in\mathbb{F}_q} \chi_D(x-c)\right) + 6\varphi_{31} \\
&= M_1 + 3qM_1 - 3M_1 + 6\varphi_{31}. \qquad (4.10)
\end{aligned}
$$

Eliminando φ_{31} de (4.7) e (4.11), obtemos:

$$6M_3 = (M_1)^3 + (3q+2)M_1 + 6I_2I_1 + 6I_3 = (I_1)^3 + (3q+2)I_1 + 6I_2I_1 + 6I_3. \qquad (4.11)$$

Agora, vamos às especificidades dos casos apresentados no teorema.

1. Denotando por ρ_n a soma dos inversos das raízes de $L(K,t)$ no Teorema 3.3.1, isto é, $\rho_n = \sum_{i=1}^{2g} w_i^n$, temos que:

$$-\rho_2 = q + 2I_2, \qquad (4.12)$$

pois, para $n = 2$ no Teorema 3.3.1(2), temos

$$-\rho_2 = -\sum_{i=1}^{2g} w_i^2 = \sum_{\mathrm{Deg}(p)=1} \chi(P)^2 + \sum_{\mathrm{Deg}(p)=2} \chi(P) = q + 2I_2.$$

Analogamente, obtemos

$$-\rho_3 = M_1 + 3I_3. \qquad (4.13)$$

Agora, pelo Binômio de Newton, obtemos, onde os a_i's são os coeficientes do $L-$ polinômio:

$$-(a_1)^3 = \left(\sum_{i=1}^{2g} w_i\right)^3 = -2\rho_3 + 3\rho_2\rho_1 - 6a_3. \qquad (4.14)$$

Substituindo (4.1), (4.12) e (4.13) em (4.14), obtém-se

$$-M_1^3 = 2(M_1 + 3I_3) + 3(q + 2I_2)M_1 - 6a_3 \qquad (4.15)$$

e, portanto,

$$6a_3 = M_1^3 + (2+3q)M_1 + 6I_2M_1 + 6I_3. \tag{4.16}$$

Da igualdade dos segundos membros de (4.11) e de (4.16), vem que:

$$a_3 = M_3. \tag{4.17}$$

2. (a) Agora, suponhamos que $a_1 = M_1 + 1$. Da parte (3) do Teorema 3.3.1, temos:

$$-1 - \rho_2 = q + 2I_2 \tag{4.18}$$

e

$$-1 - \rho_3 = M_1 + 3I_3. \tag{4.19}$$

Pelo Binômio de Newton:

$$-(a_1)^3 = -2\rho_3 + 3\rho_2\rho_1 - 6a_3. \tag{4.20}$$

Substituindo (4.18) e (4.19) em (4.20), obtemos:

$$-(M_1+1)^3 = 2(1 + M_1 + 3I_3) + 3(q + 2I_2)(M_1 + 1) - 6a_3$$

e, portanto, $6a_3 =$

$$(M_1)^3 + 3(M_1)^2 + 3M_1 + 1 + 2 + 2M_1 + 6I_3 + 3M_1 + 3 + 3qM_1 + 3q + 6I_2M_1 + 6I_2,$$

ou ainda,

$$6a_3 = (M_1)^3 + 3(M_1)^2 + (8+3q)M_1 + 6I_2M_1 + 6I_2 + 6I_3 + 3q + 6. \tag{4.21}$$

De (4.11) e (4.21), vem que:

$$6a_3 - 6M_3 = 3(M_1)^2 + 6M_1 + 6I_2 + 3q + 6, \text{ ou}$$

$$6a_3 - 6M_3 = \left(6q + 3(M_1)^2 - 3q + 6I_2\right) + 6M_1 + 6. \tag{4.22}$$

Como a expressão entre parênteses em (4.22) é M_2 (ver a decomposição feita anteriormente para M_3), obtemos

$$6a_3 - 6M_3 = 6M_2 + 6M_1 + 6,$$

ou ainda,

$$a_3 = M_3 + M_2 + M_1 + 1. \tag{4.23}$$

(b) Analogamente, quando $a_1 = M_1 - 1$, obtemos

$$a_3 = M_3 - M_2 + M_1 - 1. \tag{4.24}$$

□

4.2 Identidades finitas e explícitas em gênero 1

Em todos os teoremas a partir de agora, estamos considerando extensões elípticas (nesta seção) ou hiperelípticas (nas seções seguintes) na forma $K = \mathbb{F}_q(x)\left(\sqrt{D(x)}\right)$, onde $D(x) \in \mathbb{F}_q[x]$ é um polinômio irredutível. Além disso, o símbolo de Legendre polinomial $\chi(P)$ refere-se a $\chi_D(P)$ na notação que se segue.

TEOREMA 4.2.1. *Se* $\deg(D) = 2g + 1 = 3$*, então são verdadeiras as afirmações seguintes:*

1. $M_2 = M_{2g} = q^g = q^1$, $a_i = M_i$ *é ímpar,* $1 \leq i \leq 2g = 2$*; portanto, os coeficientes de* $L(K, t)$ *têm paridade constante ímpar invariante, isto é, não depende de* D *e de* q*, e* h *é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1 + 1$ *de lugares de grau* 1 *(cf. 2.6.10) admite uma IFE tal que* $N_1 = \mathcal{O}(q) = Cpx(N_1)$*;*

3. *$h = q + M_1 + 1$ é uma IFE com uma expansão quase $q-$ária de h da forma $h = q + \mathcal{O}(\sqrt{q})$, com $Cpx\,(h) = \mathcal{O}(q) = \mathcal{O}(q^g) = Grz(h)$;*

4. *I_2 se expressa em termos de q e I_1; M_2 se expressa em termos de M_1 e q.*

Demonstração. Da fatoração de $L(K,t)$ (Teorema 2.6.10), sabemos que $a_1 = -\sum_{i=1}^{2g} w_i$. Da segunda parte do Teorema de Stein-Teske-Scheidler (Teorema 3.3.1), obtemos, para $n = 1$ e $n = 2$, respectivamente:

$$\sum_{\deg(P)=1} \chi\,(P) = -\sum_{i=1}^{2g} w_i$$

e

$$\sum_{\deg(P)=1} \chi\,(P)^2 + 2 \sum_{\deg(P)=2} \chi\,(P) = -\sum_{i=1}^{2g} (w_i)^2.$$

Como D é irredutível e P possui grau 1, logo não divide D, então $\chi(P) = \chi_D(P) = \pm 1$, obtemos:

$$M_1 = I_1 = a_1; \tag{4.25}$$

$$q + 2I_2 = -\sum_{i=1}^{2g} (w_i)^2. \tag{4.26}$$

Entretanto,

$$(a_1)^2 = \sum_{i=1}^{2g} (w_i)^2 + 2a_2. \tag{4.27}$$

Segue-se de (4.26) e (4.27) que

$$q + 2I_2 = -(a_1)^2 + 2a_2. \tag{4.28}$$

Temos ainda:

$$(a_1)^2 = (M_1)^2 \Leftrightarrow \sum_{i=1}^{2g} (w_i)^2 + 2a_2 = q + 2\varphi_{21}, \tag{4.29}$$

onde φ_{21} é a função simétrica de ordem 2 na expressão quadrática de $(M_1)^2$. Substituindo (4.28) em (4.29), obtemos $q + 2\varphi_{21} = -q - 2I_2 + 2a_2$, que pode ser reescrita como

$$q + \varphi_{21} + I_2 = -q - \varphi_{21} - I_2 + 2a_2. \tag{4.30}$$

Lembrando que

$$q + \varphi_{21} + I_2 = M_2, \tag{4.31}$$

(4.30) fornece $2M_2 = 2a_2$ ou $M_2 = a_2$. Do Teorema 2.6.10, temos $a_0 = 1$ e $a_2 = q^g = q$. Assim,

$$L(K,t) = a_0 + a_1 t + a_2 t^2 = 1 + M_1 t + M_2 t^2,$$

o que fornece

$$L(K,1) = h = q + M_1 + 1,$$

com decomposição *quase q-ária*

$$h = q + \mathcal{O}(\sqrt{q}).$$

Como há q polinômios mônicos de grau 1 em $\mathbb{F}_q$ que entram na computação de M_1, obtemos $\mathrm{Cpx}\,(h) = \mathcal{O}(q) = \mathcal{O}(q^g) = \mathrm{Grz}(h)$, pois $\mathrm{Grz}(M_1) = \mathrm{Grz}(a_1) = \mathrm{Grz}(w_i) = q^{\frac{1}{2}}$, pelo Teorema 2.6.12. Estão assim provadas as três primeiras afirmações do teorema.

Agora, de (4.28), (4.25) e de $a_2 = q$, segue-se que

$$I_2 = \frac{-I_1^2 + q}{2}.$$

Isso, juntamente com a equação $M_2 = a_2 = q$, demonstram a afirmação (4) do teorema. Observamos que a irredutibilidade de D foi fundamental para obtermos (4.26). Isso ocorrerá em todos os teoremas que se seguem. □

Teorema 4.2.2. *Se* $\deg(D) = 2g + 2 = 4$, *e* ∞ *se decompõe, então:*

1. $M_3 = M_{2g+1} = -q^g = -q$, $a_i = M_i + M_{i-1} + \cdots + M_1 + 1$, *para* $1 \leq i \leq 2g = 2$, *é par quando* i *é ímpar e ímpar quando* i *é par; portanto, os coeficientes de* $L(K,t)$ *têm paridade alternada invariante, isto é, não depende de* D *e de* q, *e* h *é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1 + 2$ *de divisores primos de grau* 1 *admite uma IFE tal que* $Grz\,(N_1) = Cpx\,(N_1) = \mathcal{O}(q)$;

3. *$h = q + M_1 + 2$ é uma IFE com expansão quase $q-$ária da forma $h = q + \mathcal{O}(\sqrt{q})$ e tal que $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$;*

4. *I_2 se expressa em termos de q e I_1; M_2 se expressa em termos de M_1 e q.*

Demonstração. Da fatoração de $L(K,t)$, sabemos que $a_1 = -\sum_{i=1}^{2g} w_i$. Da primeira parte do Teorema de Stein-Teske, obtemos, para $n = 1$ e $n = 2$, respectivamente:

$$\sum_{\deg(P)=1} \chi(P) = -1 - \sum_{i=1}^{2g} w_i$$

e

$$\sum_{\deg(P)=1} \chi(P)^2 + 2 \sum_{\deg(P)=2} \chi(P) = -1 - \sum_{i=1}^{2g} (w_i)^2$$

Obtemos, então:

$$M_1 = I_1 = -1 + a_1; \tag{4.32}$$

$$q + 2I_2 = -1 - \sum_{i=1}^{2g} (w_i)^2 \Rightarrow q + 2I_2 + 1 = -\sum_{i=1}^{2g} (w_i)^2. \tag{4.33}$$

Entretanto,

$$(a_1)^2 = \left(-\sum_{i=1}^{2g} (w_i) \right)^2 = \sum_{i=1}^{2g} (w_i)^2 + 2a_2. \tag{4.34}$$

Segue-se, então, de (4.33) e (4.34), que

$$q + 2I_2 + 1 = -(a_1)^2 + 2a_2. \tag{4.35}$$

Também temos, de (4.32), que

$$(a_1)^2 = (1 + M_1)^2. \tag{4.36}$$

De (4.34) e (4.36) segue-se que

$$\sum_{i=1}^{2g} (w_i)^2 + 2a_2 = (M_1)^2 + 2M_1 + 1 = q + 2\varphi_{21} + 2M_1 + 1, \tag{4.37}$$

onde φ_{21} é a função simétrica de ordem 2 na expressão quadrática de $(M_1)^2$.

De (4.37), (4.33) e (4.34), obtemos:

$$q + 2\varphi_{21} + 2M_1 + 1 = -q - 2I_2 - 1 + 2a_2$$

ou

$$a_2 = q + \varphi_{21} + I_2 + M_1 + 1. \tag{4.38}$$

Observemos que, na última expressão, $q + \varphi_{21} + I_2$ é exatamente M_2. Concluímos que $a_2 = M_2 + M_1 + 1$. Como $a_2 = q$, temos que:

$$M_2 = q - M_1 - 1. \tag{4.39}$$

Em particular, M_2 se expressa em função de M_1 e q. Além disso, M_j é ímpar como soma de q^j ± 1's. Segue-se de suas expressões que a_1 é par e a_2 ímpar.

Sendo $\varphi_{21} = \frac{(I_1)^2 - q}{2}$, obtemos, de (4.38):

$$a_2 = q + \frac{(I_1)^2 - q}{2} + I_2 + I_1 + 1$$

ou

$$q = q + \frac{(I_1)^2 - q}{2} + I_2 + I_1 + 1$$

e, portanto,

$$0 = \frac{(I_1)^2 - q}{2} + I_2 + I_1 + 1.$$

Ou seja, I_2 se expressa em função de q e I_1.

Agora, comparando $L(K, 1) = h$ com h na L-série de Artin adaptada, temos:

$$h = a_0 + a_1 + a_2 = 1 + (M_1 + 1) + q =$$

$$= \frac{q}{q-1}\left(q^1 + M_1 + \frac{M_2}{q} + \frac{M_3}{q^2}\right) \Rightarrow$$

$$(q-1)(1 + (M_1 + 1) + q) = q^2 + qM_1 + M_2 + \frac{M_3}{q} \Rightarrow$$

$$q - 2 - M_1 = M_2 + \frac{M_3}{q}.$$

Portanto, por (4.39), temos:

$$M_3 = -q.$$

Assim, $h = q + M_1 + 2$ é uma IFE com expansão *quase $q-$ária* da forma $h = q + \mathcal{O}(\sqrt{q})$ e tal que $\mathrm{Cpx}(h) = \mathcal{O}(q) = \mathcal{O}(q^g) = \mathrm{Grz}(h)$, pois $\mathrm{Grz}(M_1) = \mathrm{Grz}(a_1) = \mathrm{Grz}(w_i) = q^{\frac{1}{2}}$, pelo Teorema 2.6.12. □

Teorema 4.2.3. *Se* $\deg(D) = 2g + 2 = 4$, *e* ∞ *é inerte, então:*

1. $M_3 = M_{2g+1} = q^g = q$, $a_i = M_i - M_{i-1} + \cdots \pm M_1 + (-1)^i$, *para* $1 \leq i \leq 2g = 2$, *é par quando* i *é ímpar e ímpar quando* i *é par; portanto, os coeficientes de* $L(K,t)$ *têm paridade alternada invariante, isto é, não depende de* D *e de* q, *e* h *é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1$ *de lugares de grau* 1 *admite uma IFE tal que* $Grz\,(N_1) = Cpx\,(N_1) = \mathcal{O}(q)$;

3. $h = q + M_1$ *é uma IFE com expansão quase $q-$ária da forma* $h = q + \mathcal{O}(\sqrt{q})$ *e tal que* $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$;

4. I_2 *se expressa em função de* q *e* I_1; M_2 *se expressa em função de* q *e* M_1.

Demonstração. Como nos dois casos anteriores, da fatoração de $L\,(K,t)$, sabemos que $a_1 = -\sum_{i=1}^{2g} w_i$. Da primeira parte do Teorema de Stein-Teske-Scheidler (Teorema 3.3.1), obtemos, para $n = 1$ e $n = 2$, respectivamente:

$$\sum_{\deg(P)=1} \chi\,(P) = 1 - \sum_{i=1}^{2g} w_i$$

e

$$\sum_{\deg(P)=1} \chi\,(P)^2 + 2 \sum_{\deg(P)=2} \chi\,(P) = -1 - \sum_{i=1}^{2g} (w_i)^2$$

Obtemos, então:

$$M_1 = I_1 = 1 + a_1;$$

$$q + 2I_2 = -1 - \sum_{i=1}^{2g} (w_i)^2 \Rightarrow q + 2I_2 + 1 = -\sum_{i=1}^{2g} (w_i)^2.$$

Entretanto,

$$(a_1)^2 = \sum_{i=1}^{2g}(w_i)^2 + 2a_2.$$

Segue-se das duas últimas igualdades que $q + 2I_2 + 1 = -(a_1)^2 + 2a_2$.

Temos ainda $(a_1)^2 = (-1 + M_1)^2$, de onde vem que

$$\sum_{i=1}^{2g}(w_i)^2 + 2a_2 = (M_1)^2 - 2M_1 + 1 = q + 2\varphi_{21} - 2M_1 + 1,$$

onde φ_{21} é a função simétrica de ordem 2 na expressão quadrática de $(M_1)^2$. Desse modo, obtemos:

$$q + 2\varphi_{21} - 2M_1 + 1 = -q - 2I_2 - 1 + 2a_2$$

ou

$$a_2 = q + \varphi_{21} + I_2 - M_1 + 1.$$

Observemos que, na última expressão, $q + \varphi_{21} + I_2$ é exatamente M_2. Concluímos que $a_2 = M_2 - M_1 + 1$. Como $a_2 = q$, temos que:

$$M_2 = q + M_1 - 1. \tag{4.40}$$

Sendo $\varphi_{21} = \frac{(I_1)^2 - q}{2}$, obtemos:

$$a_2 = q + \frac{(I_1)^2 - q}{2} + I_2 - I_1 + 1$$

ou

$$q = q + \frac{(I_1)^2 - q}{2} + I_2 - I_1 + 1$$

e, portanto,

$$0 = \frac{(I_1)^2 - q}{2} + I_2 - I_1 + 1.$$

Ou seja, I_2 se expressa em função de q e I_1.

Agora, comparando $L(K, 1) = h$ com h na L-série de Artin adaptada, temos:

$$h = a_0 + a_1 + a_2 = 1 + a_1 + q = 1 + (M_1 - 1) + q =$$

$$= \frac{q}{q+1}\left(q^1 + M_1 + \frac{M_2}{q} + \frac{M_3}{q^2}\right) \Rightarrow$$

$$(q+1)(M_1+q) = q^2 + qM_1 + M_2 + \frac{M_3}{q} \Rightarrow$$

$$q + M_1 = M_2 + \frac{M_3}{q}.$$

Portanto, por (4.40), temos:

$$M_3 = q.$$

Assim, $h = q + M_1$ é uma IFE com expansão *quase* $q-$*ária* da forma $h = q + \mathcal{O}(\sqrt{q})$ e tal que $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$. □

4.3 Identidades finitas e explícitas em gênero 2

TEOREMA 4.3.1. *Se* $\deg(D) = 2g+1 = 5$*, então:*

1. $M_4 = M_{2g} = q^g = q^2$*,* $a_i = M_i$*, para* $1 \leq i \leq 2g = 4$*, é ímpar; portanto, os coeficientes de* $L(K,t)$ *têm paridade constante ímpar invariante, isto é, não depende de* D *e de* q*, e* h *é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1 + 1$ *de divisores primos de grau* 1 *admite uma IFE tal que* $Grz\,(N_1) = Cpx\,(N_1) = \mathcal{O}(q)$*;*

3. $h = q^2 + \left(M_1 + \frac{M_2}{q}\right) q + M_1 + 1$ *tem expansão quase* $q-$*ária da forma* $h = q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q})$ *e* $Cpx\,(h) = \mathcal{O}(q^g) = Grz\,(h)$*;*

4. I_3 *e* I_4 *se expressam em função de* q, I_1, I_2*;* M_3 *e* M_4 *se expressam em função de* q, M_1, M_2*.*

Demonstração. Pelo Teorema 4.1.7, obtemos: $a_1 = M_1$, $a_2 = M_2$ e $a_3 = M_3$. Pelas relações entre os coeficientes de $L(K,t)$, temos $M_3 = qM_1 = qI_1$.

Da igualdade $M_3 = qM_1$ e comparando $h = L(K,1)$ com h na L-série de Artin adaptada (Teorema 3.2.4), deduzimos que

$$h = a_0 + a_1 + a_2 + a_3 + a_4 = 1 + a_1 + a_2 + a_1q + q^2 = q^2 + a_1(q+1) + a_2 + 1 =$$

$$q^2 + qM_1 + M_2 + \frac{M_3}{q} + \frac{M_4}{q^2} \Rightarrow$$

$$q^2 + M_1(q+1) + M_2 + 1 = q^2 + qM_1 + M_2 + M_1 + \frac{M_4}{q^2}$$

e, portanto, $M_4 = q^2$. De (4.11) e de $M_3 + qI_1$, obtemos $6qI_1 + 6M_3 = I_1^3 + (3q+2)I_1 + 6I_1I_2 + 6I_3$,de onde se segue que I_3 se expressa em termos de q, I_1 e I_2. Agora, comparando-se M_4 com M_1^4 de modo análogo à comparação de M_3 com M_1^3 que fizemos na demonstração do Teorema 4.1.7., chegamos a uma expressão para $M_4 = q^2$ em termos de q, I_1, I_2, I_3 e I_4, de onde I_4 se expressa em termos de q, I_1 e I_2, pois I_3 já se expressa em termos de q, I_1 e I_2.
Vemos que $\mathrm{Cpx}(M_2) = \mathcal{O}(q^2)$ de onde resulta que $\mathrm{Cpx}(h) = \mathcal{O}(q^2) = \mathcal{O}(q^g)$. Além disso, M_3 e M_4 são expressos em função de M_1, M_2 e q, logo, com complexidade $\mathcal{O}(q)$ e $\mathcal{O}(q^2)$, respectivamente. Uma decomposição *quase q-ária* de h pode ser ser escrita como

$$h = q^2 + (\frac{M_2}{q} + M_1)q + M_1 + 1 = q^2 + c_1q + c_0,$$

satisfazendo $\mathrm{Grz}(c_i) = \sqrt{q}$ para $i = 0, 1$, pois $M_1 = a_1 = -\sum_{i=0}^{2g} w_i$, $M_2 = a_2 = \sum_{\substack{i,j=0 \\ i<j}}^{2g} w_iw_j$ e, pelo Teorema 2.6.12, $|w_i| = q^{\frac{1}{2}}$. □

Teorema 4.3.2. *Se* $\deg(D) = 2g + 2 = 6$, *e* ∞ *se decompõe, então:*

1. $a_i = M_i + M_{i-1} + \cdots + M_1 + 1$, *para* $1 \leq i \leq 3$, *é par quando i é ímpar e ímpar quando i é par; portanto, para* $1 \leq i \leq 3$, *os coeficientes de* $L(K,t)$ *têm paridade alternada invariante, isto é, não depende de D e q, e h é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1 + 2$ *de divisores primos de grau* 1 *admite uma IFE tal que* $Grz(N_1) = Cpx(N_1) = \mathcal{O}(q)$;

3. $h = q^2 + \left(1 + M_1 + \frac{M_2}{q}\right) q + 2M_1 + 3$ *tem expansão quase* $q-$*ária da forma* $h = q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q})$ *e* $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$*;*

4. I_3 *se expressa em função de* q, I_1 *e* I_2*;* M_3 *se expressa em função de* q, M_1 *e* M_2*.*

Demonstração. Pelo Teorema 4.1.7, temos: $a_1 = M_1+1$, $a_2 = M_2+M_1+1$ e $a_3 = M_3+M_2+M_1+1$.

Aplicando essas igualdades em $L(K, 1) = h$, temos:

$$h = 1 + (M_1 + 1) + (M_2 + M_1 + 1) + q(M_1 + 1) + q^2.$$

Pela fórmula de N_1 e pelo Teorema 3.3.1(1), vem que:

$$N_1 = q + 1 - \sum_{i=1}^{2g}(w_i) = q + 1 + M_1 + 1 = q + M_1 + 2.$$

Como $qa_1 = a_3$, podemos escrever que:

$$q(M_1 + 1) = M_3 + M_2 + M_1 + 1,$$

de onde se segue que:

$$M_3 = (q - 1)(M_1 + 1) - M_2,$$

ou seja, M_3 se expressa em função de M_1, M_2 e q.". Essa última igualdade, juntamente com (4.11), mostram que I_3 se expressa em termos de q, I_1 e I_2.

Uma decomposição *quase q-ária* pode ser escrita como $h = q^2 + \left(1 + M_1 + \frac{M_2}{q}\right) q + 2M_1 + 3$ com *expansão quase* $q-$*ária* da forma $h = q^2+\mathcal{O}(\sqrt{q})q+\mathcal{O}(\sqrt{q})$ satisfazendo $\mathrm{Grz}(c_i) = \sqrt{q}$ para $i = 0, 1$ e $Cpx\,(h) = \mathcal{O}(q^g) = \mathrm{Grz}\,(h)$. □

Conjectura 4.3.3. *Se* $\deg(D) = 2g + 2 = 6$*, e* ∞ *se decompõe, então:*

1. $M_5 = M_{2g+1} = -q^g = -q^2$*,* $a_i = M_i + M_{i-1} + \cdots + M_1 + 1$*, para* $1 \leq i \leq 2g = 4$*, é par quando* i *é ímpar e ímpar quando* i *é par; portanto, os coeficientes de* $L\,(K, t)$ *têm paridade alternada invariante, isto é, não depende de* D *e* q*, e* h *é ímpar;*

2. I_4, I_5 se expressam em função de q, I_1, I_2; M_4, M_5 se expressam em função de M_1, M_2 e q.

Justificação da conjectura. Pelo Teorema 4.1.7, temos: $a_1 = M_1 + 1$, $a_2 = M_2 + M_1 + 1$ e $a_3 = M_3 + M_2 + M_1 + 1$.

Como $qa_1 = a_3$, podemos escrever que:

$$q(M_1 + 1) = M_3 + M_2 + M_1 + 1, \tag{4.41}$$

de onde deduzimos que:

$$M_3 = (q - 1)(M_1 + 1) - M_2. \tag{4.42}$$

É plausível repetir a sequência de raciocínio na argumentação do Teorema 4.1.7 e conjecturar que:

$$a_4 = M_4 + M_3 + M_2 + M_1 + 1. \tag{4.43}$$

Seguir-se-ia que:

$$M_4 = q^2 - q(M_1 + 1). \tag{4.44}$$

Agora, comparando $L(K, 1) = h$ com h na L-série de Artin adaptada, teríamos:

$$(q-1)\left[1 + (M_1+1) + (M_2 + M_1 + 1) + q(M_1+1) + q^2\right] =$$

$$= q^3\left[1 + \frac{M_1}{q} + \frac{M_2}{q^2} + \frac{M_3}{q^3} + \frac{M_4}{q^4} + \frac{M_5}{q^5}\right].$$

$$(q-1)\left[1 + (q+1)(M_1+1) + M_2 + (M_1+1) + q^2\right] =$$

$$= q^3 + q^2M_1 + qM_2 + M_3 + \frac{M_4}{q} + \frac{M_5}{q^2} \Rightarrow$$

$$(q-1) + (q^2-1)(M_1+1) + (q-1)M_2 + (q-1)(M_1+1) + q^3 - q^2 =$$

$$= q^3 + q^2M_1 + qM_2 + (q-1)(M_1+1) - M_2 + q - (M_1+1) + \frac{M_5}{q^2} \Rightarrow$$

$$q - 1 + q^2 M_1 + q^2 - M_1 - 1 - q^2 = q^2 M_1 + q - (M_1 + 1) + \frac{M_5}{q^2} \Rightarrow$$

$$-1 = \frac{M_5}{q^2}$$

Usando as relações (4.42) e (**??**), para simplificar a igualdade acima, chegamos a

$$M_5 = -q^2.$$

Assim, M_4 e M_5 se expressam em termos de q, M_1 e M_2. De (4.11) e (4.44), segue-se, como no Teorema 3.3.1. que I_3 se expressa em função de q, I_1 e I_2. O argumento para I_4 e I_5 seguiria a mesma linha dada no Teorema 4.1.7. partindo-se de (4.46) e de $M_5 = -q^2$, respectivamente. No entanto, a complexidade dos cálculos cresce rapidamente, parametrizado pelo número de possibilidades para se decompor um polinômio mônico como produto de irredutíveis, ou seja, pelas partições possíveis para seu grau, como verificado com o grau 3 na demonstração do Teorema 4.1.7. □

De modo análogo, utilizando os Teoremas 3.3.1(3), 4.1.7 e 3.2.5, apresentamos o teorema e a conjectura seguintes.

TEOREMA 4.3.4. *Se* $\deg(D) = 2g + 2 = 6$*, e* ∞ *é inerte, então:*

1. $a_i = M_i - M_{i-1} + \cdots \pm M_1 + (-1)^i$*, para* $1 \leq i \leq 3$*, é par quando i é ímpar e ímpar quando i é par; portanto, para* $1 \leq i \leq 3$*, os coeficientes de* $L(K, t)$ *têm paridade alternada invariante, isto é, não depende de D e q, e h é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1 + 2$ *de divisores primos de grau* 1 *admite uma IFE tal que* $Grz(N_1) = Cpx(N_1) = \mathcal{O}(q)$*;*

3. $h = q^2 + \left(-1 + M_1 + \frac{M_2}{q}\right) q + 1$ *tem expansão quase* $q-$*ária da forma* $h = q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q})$ *e* $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$*;*

4. I_3 se expressa em função de q, I_1 e I_2; M_3 se expressa em função de q, M_1 e M_2.

Demonstração. Pelo Teorema 4.1.7, temos: $a_1 = M_1 - 1$, $a_2 = M_2 - M_1 + 1$ e $a_3 = M_3 - M_2 + M_1 - 1$.

Aplicando essas igualdades em $L(K, 1) = h$, temos:

$$h = 1 + (M_1 - 1) + (M_2 - M_1 + 1) + q(M_1 - 1) + q^2.$$

Pela fórmula de N_1 e pelo Teorema 3.3.1(3), vem que:

$$N_1 = q + 1 - \sum_{i=1}^{2g}(w_i) = q + 1 + (M_1 - 1) = q + M_1.$$

Do L- polinômio, como $qa_1 = a_3$, podemos escrever que:

$$q(M_1 - 1) = M_3 - M_2 + M_1 - 1,$$

de onde deduzimos que:

$$M_3 = (q - 1)(M_1 - 1) + M_2.$$

Decorre então, como nos teorema anteriores, que I_3 se expressa em função de q, I_1, I_2 e a soma M_3 em função de M_1, M_2 e q.

Uma decomposição *quase q-ária* de h pode ser escrita como

$$h = q^2 + \left(-1 + M_1 + \frac{M_2}{q}\right) q + 1,$$

que é da forma $h = q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q})$ satisfazendo $\mathrm{Grz}(c_i) = \sqrt{q}$ para $i = 0, 1$ e $\mathrm{Cpx}\,(h) = \mathcal{O}(q^g) = \mathrm{Grz}\,(h)$.

Vemos que $\mathrm{Cpx}(M_2) = \mathcal{O}(q^2)$, de onde resulta que $\mathrm{Cpx}(h) = \mathcal{O}(q^2) = \mathcal{O}(q^g)$. □

Conjectura 4.3.5. *Se* $\deg(D) = 2g + 2 = 6$, *e* ∞ *é inerte, então:*

1. $M_5 = M_{2g+1} = q^g = q^2$, $a_i = M_i - M_{i-1} + \cdots \pm M_1 + (-1)^i$, *para* $1 \leq i \leq 2g = 4$, *é par quando* i *é ímpar e ímpar quando* i *é par; portanto, para* $4 \leq i \leq 2g = 4$, *os coeficientes de* $L\,(K, t)$ *têm paridade alternada invariante, isto é, não depende de* D *e* q, *e* h *é ímpar;*

2. I_4, I_5 se expressam em função de q, I_1, I_2; M_4, M_5 se expressam em função de M_1, M_2 e q.

Justificação da conjectura. É natural conjecturar que vale a sequência de raciocínio realizada no Teorema 4.1.7, portanto, que:

$$a_4 = M_4 - M_3 + M_2 - M_1 + 1.$$

Seguir-se-ia que:

$$M_4 = q^2 + [(q-1)(M_1 - 1) + M_2] - M_2 + M_1 - 1,$$

que equivale a

$$M_4 = q^2 + q(M_1 - 1).$$

Agora, comparando $L(K, 1) = h$ com a L-série de Artin adaptada (Teorema 3.2.5), teríamos:

$$(q+1)\left[1 + (M_1 - 1) + (M_2 - M_1 + 1) + q(M_1 - 1) + q^2\right] =$$
$$= q^3\left[1 + \frac{M_1}{q} + \frac{M_2}{q^2} + \frac{M_3}{q^3} + \frac{M_4}{q^4} + \frac{M_5}{q^5}\right] \Rightarrow$$

$$(q+1)\left[(q-1)(M_1 - 1) + M_2 + M_1 + q^2\right] =$$
$$= q^3 + q^2 M_1 + qM_2 + M_3 + \frac{M_4}{q} + \frac{M_5}{q^2} \Rightarrow$$

$$(q^2 - 1)(M_1 - 1) + (q+1)M_2 + (q+1)M_1 + q^3 + q^2 =$$
$$= q^3 + q^2 M_1 + qM_2 + (q-1)(M_1 - 1) + M_2 + q + (M_1 - 1) + \frac{M_5}{q^2} \Rightarrow$$

$$1 = \frac{M_5}{q^2} \Rightarrow$$

e, portanto,

$$M_5 = q^2.$$

Logo, M_4 e M_5 se expressam em termos de q, M_1 e M_2. O fato de que I_4 e I_5 se expressam em termos de q, I_1 e I_2 é justificado como na Conjectura 4.3.3. □

4.4 Identidades finitas e explícitas em gênero 3

TEOREMA 4.4.1. *Se* $\deg(D) = 2g + 1 = 7$*, então:*

1. $a_i = M_i$*, para* $1 \leq i \leq 3$*, é ímpar; portanto, para* $1 \leq i \leq 3$*, os coeficientes de* $L(K, t)$ *têm paridade constante ímpar invariante, isto é, não depende de* D *e de* q*, e* h *é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1 + 1$ *de divisores primos de grau* 1 *admite uma IFE tal que* $Grz(N_1) = Cpx(N_1) = \mathcal{O}(q)$*;*

3. $h = q^3 + (M_1 + \frac{M_2}{q})q^2 + (\frac{M_2}{q} + \frac{M_3}{q})q + M_1 + 1$ *tem expansão quase* $q-$*ária da forma* $h = q^3 + \mathcal{O}(\sqrt{q})q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q})$ *e* $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$*.*

Demonstração. Pelo Teorema 4.1.7, temos: $a_1 = M_1$, $a_2 = M_2$ e $a_3 = M_3$.

Aplicando essas igualdades em $L(K, 1) = h$, temos:

$$h = 1 + M_1 + M_2 + M_3 + qM_2 + q^2M_1 + q^3.$$

Pela fórmula de N_1 e pelo Teorema 3.3.1(2), vem que:

$$N_1 = q + 1 - \sum_{i=1}^{2g}(w_i) = q + 1 + M_1.$$

Vemos que $\mathrm{Cpx}(M_3) = \mathcal{O}(q^3)$, de onde resulta que $\mathrm{Cpx}(h) = \mathcal{O}(q^3) = \mathcal{O}(q^g)$. □

CONJECTURA 4.4.2. *Se* $\deg(D) = 2g + 1 = 7$*, então:*

1. $M_6 = M_{2g} = q^g = q^3$*,* $a_i = M_i$*, para* $1 \leq i \leq 2g = 6$*, é ímpar; portanto, os coeficientes de* $L(K, t)$ *têm paridade constante ímpar invariante, isto é, não depende de* D *e de* q*, e* h *é ímpar;*

2. I_4, I_5, I_6 *se expressam em função de* q, I_1, I_2, I_3*;* M_4, M_5, M_6 *se expressam em função de* q, M_1, M_2, M_3*.*

Justificação da conjectura. É natural conjecturar que a sequência de raciocínio no teorema anterior é válida e, portanto, que $M_4 = a_4$ e $M_5 = a_5$. Seguir-se-ia que $M_6 = a_6 = q^3$. Além disso, nossa conjectura também implicaria, pelas relações entre os coeficientes de $L(K,t)$, que $M_4 = qM_2$ e $M_5 = q^2M_1$.

Comparando $h = L(K,1)$ com h na L-série de Artin adaptada obteremos $M_6 = a_6 = q^3$. De fato:

$$h = a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 =$$

$$= 1 + a_1 + a_2 + a_3 + a_2q + a_1q^2 + q^3 = q^3 + a_1(q^2+1) + a_2(q+1) + 1 \Rightarrow$$

$$q^3 + M_1(q^2+1) + M_2(q+1) + M_3 + 1 = q^3 + q^2M_1 + qM_2 + M_3 + \frac{M_4}{q} + \frac{M_5}{q^2} + \frac{M_6}{q^3} \Rightarrow$$

$$q^3 + M_1(q^2+1) + M_2(q+1) + M_3 + 1 = q^3 + q^2M_1 + qM_2 + M_3 + M_2 + M_1 + \frac{M_6}{q^3} \Rightarrow$$

$$1 = \frac{M_6}{q^3}$$

e, portanto, $M_6 = q^3$ e M_4, M_5, M_6 e M_7 se expressam em função de q, M_1 e M_2.

Finalmente, seguir-se-ia que:

$$h = q^3 + (\frac{M_2}{q} + M_1)q^2 + (\frac{M_3}{q} + \frac{M_2}{q})q + M_1 + 1,$$

satisfazendo a decomposição quase $q-$ária de h pelo fato de que

$$a_i = (-1)^i\sigma_i(w_1, \ldots, w_{2g}),$$

onde σ_i é a função simétrica de ordem i e $\mathcal{O}(a_i) = \mathcal{O}(q^{\frac{i}{2}})$.

Assim, pelas relações entre os coeficientes de $L(K,t)$, de $M_4 = qM_2$ deduziremos que I_4 se expressa em função de q, I_1, I_2, I_3. Analogamente, de $M_5 = q^2M_1$, deduziremos que I_5 também se expressa em função de q, I_1, I_2, I_3. O mesmo valerá para $M_6 = q^3$ e I_6. □

Teorema 4.4.3. *Se* $\deg(D) = 2g + 2 = 8$, *e* ∞ *se decompõe, então:*

1. $a_i = M_i + M_{i-1} + \cdots + M_1 + 1$, *para* $1 \leq i \leq 3$, *é par quando* i *é ímpar e ímpar quando* i *é par; portanto, para* $1 \leq i \leq 3$, *os coeficientes de* $L(K,t)$ *têm paridade alternada invariante, isto é, não depende de* D *e* q, *e* h *é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1 + 2$ *de lugares de grau* 1 *admite uma IFE tal que* $Grz(N_1) = Cpx(N_1) = \mathcal{O}(q)$;

3. $h = q^3 + (1 + M_1 + \frac{M_2}{q})q^2 + (1 + M_1 + \frac{2M_2}{q} + \frac{M_3}{q})q + 3M_1 + 4$ *tem expansão quase* $q-$*ária da forma* $h = q^3 + \mathcal{O}(\sqrt{q})q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q})$ *e* $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$.

Demonstração. Pelo Teorema 4.1.7, temos: $a_1 = M_1+1$, $a_2 = M_2+M_1+1$ e $a_3 = M_3+M_2+M_1+1$.

Aplicando essas igualdades em $L(K,1) = h$, temos:

$$h = 1 + (M_1 + 1) + (M_2 + M_1 + 1) + (M_3 + M_2 + M_1 + 1) + q\underbrace{(M_2 + M_1 + 1)}_{a_2} + q^2\underbrace{(M_1 + 1)}_{a_1} + q^3.$$

Pela fórmula de N_1 e pelo Teorema 3.3.1(1), vem que:

$$N_1 = q + 1 - \sum_{i=1}^{2g}(w_i) = q + 1 + M_1 + 1 = q + M_1 + 2.$$

Vemos que $\mathrm{Cpx}(M_3) = \mathcal{O}(q^3)$, de onde resulta que $\mathrm{Cpx}(h) = \mathcal{O}(q^3) = \mathcal{O}(q^g)$.

Uma decomposição *quase q-ária* pode ser escrita como

$$h = q^3 + (1 + M_1 + \frac{M_2}{q})q^2 + (1 + M_1 + \frac{2M_2}{q} + \frac{M_3}{q})q + 3M_1 + 4,$$

que é da forma

$$h = q^3 + \mathcal{O}(\sqrt{q})q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q}),$$

satisfazendo $\mathrm{Grz}(c_i) = \sqrt{q}$ para $i = 0, 1, 2$, e $\mathrm{Cpx}(h) = \mathcal{O}(q^g) = \mathrm{Grz}(h)$. □

Conjectura 4.4.4. *Se* $\deg(D) = 2g + 2 = 8$, *e* ∞ *se decompõe, então:*

1. $M_7 = M_{2g+1} = -q^g = -q^3$, $a_i = M_i + M_{i-1} + \cdots + M_1 + 1$, *para* $4 \leq i \leq 2g = 6$, *é par quando* i *é ímpar e ímpar quando* i *é par; portanto, para* $4 \leq i \leq 2g = 6$, *os coeficientes de* $L(K,t)$ *têm paridade alternada invariante, isto é, não depende de* D *e* q, *e* h *é ímpar;*

2. *I_4, I_5, I_6, I_7 se expressam em função de q, I_1, I_2, I_3; M_4, M_5, M_6, M_7 se expressam em função de q, M_1, M_2, M_3.*

Demonstração. É natural conjecturar que a sequência de raciocínio no teorema anterior é válida e, portanto, que:

$$a_4 = M_4 + M_3 + M_2 + M_1 + 1,$$

$$a_5 = M_5 + M_4 + M_3 + M_2 + M_1 + 1,$$

$$a_6 = M_6 + M_5 + M_4 + M_3 + M_2 + M_1 + 1.$$

Seguir-se-ia que:

$$M_4 = q(M_2 + M_1 + 1) - [M_3 + M_2 + M_1 + 1] = (q-1)(M_2 + M_1 + 1) - M_3,$$

$$M_5 = q^2(M_1 + 1) - [M_4 + M_3 + M_2 + M_1 + 1] =$$

$$q^2(M_1 + 1) - (q-1)(M_2 + M_1 + 1) + M_3 - (M_3 + M_2 + M_1 + 1) =$$

$$q^2(M_1 + 1) - q(M_2 + M_1 + 1),$$

$$M_6 = q^3 - [M_5 + M_4 + M_3 + M_2 + M_1 + 1 =$$

$$q^3 - q^2(M_1 + 1) + q(M_2 + M_1 + 1) - (q-1)(M_2 + M_1 + 1) + M_3 - M_3 - M_2 - M_1 - 1 =$$

$$q^3 - q^2(M_1 + 1).$$

Agora, comparando $L(K, 1) = h$ com a L-série de Artin adaptada (Teorema 3.2.6), teríamos:

$$(q-1)\left[2 + M_1 + (q+2)(M_2 + M_1 + 1) + M_3 + q^2(M_1 + 1) + q^3\right] =$$

$$q^4\left[1 + \frac{M_1}{q} + \frac{M_2}{q^2} + \frac{M_3}{q^3} + \frac{M_4}{q^4} + \frac{M_5}{q^5} + \frac{M_6}{q^6} + \frac{M_7}{q^7}\right] \Rightarrow$$

$$(q-1)\left[2 + M_1 + (q+2)(M_2 + M_1 + 1) + M_3 + q^2(M_1 + 1) + q^3\right] =$$

$$q^4 + q^3M_1 + q^2M_2 + qM_3 + M_4 + \frac{M_5}{q} + \frac{M_6}{q^2} + \frac{M_7}{q^3} \Rightarrow$$

$$(q-1)[2 + M_1 + (q+2)(M_2 + M_1 + 1) + M_3 + q^2(M_1+1) + q^3] =$$

$$q^4 + q^3M_1 + q^2M_2 + qM_3 + (q-1)(M_2 + M_1 + 1) - M_3 + q(M_1+1) - (M_2 + M_1 + 1) +$$
$$+q - (M_1+1) + \frac{M_7}{q^3} \Rightarrow$$

$$-1 = \frac{M_7}{q^3}$$

e, portanto,

$$M_7 = -q^3.$$

Daí, M_4, M_5, M_6 e M_7 se expressam em função de q, M_1, M_2 e M_3.

De $M_4 = (q-1)(M_2 + M_1 + 1) - M_3$ deduziremos que I_4 se expressa em função de q, I_1, I_2, I_3. Analogamente, de

$$M_5 = q^2(M_1+1) - q(M_2 + M_1 + 1)$$

deduziremos que I_5 se expressa em função de q, I_1, I_2, I_3. O mesmo valerá para $M_6 = q^3 - q^2(M_1+1)$ e I_6. □

Teorema 4.4.5. *Se* $\deg(D) = 2g + 2 = 8$, *e* ∞ *é inerte, então:*

1. $a_i = M_i - M_{i-1} + \cdots \pm M_1 + (-1)^i$, *para* $1 \leq i \leq 3$, *é par quando i é ímpar e ímpar quando i é par; portanto, para* $1 \leq i \leq 3$, *os coeficientes de* $L(K,t)$ *têm paridade alternada invariante, isto é, não depende de D e q, e h é ímpar;*

2. *o número* $N_1 = a_1 + q + 1 = q + M_1$ *de divisores primos de grau* 1 *admite uma IFE tal que* $Grz(N_1) = Cpx(N_1) = \mathcal{O}(q)$;

3. $h = q^3 + (-1 + M_1 + \frac{M_2}{q})q^2 + (1 - M_1 + \frac{M_3}{q})q + M_1$ *tem expansão quase* $q-$*ária da forma* $h = q^3 + \mathcal{O}(\sqrt{q})q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q})$ *e* $Cpx(h) = \mathcal{O}(q^g) = Grz(h)$.

Demonstração. Pelo Teorema 4.1.7, temos: $a_1 = M_1 - 1$, $a_2 = M_2 - M_1 + 1$ e $a_3 = M_3 - M_2 + M_1 - 1$. Aplicando essas igualdades em $L(K,1) = h$, temos:

$$h = 1 + (M_1 - 1) + (M_2 - M_1 + 1) + M_3 - M_2 + M_1 - 1 + q(M_2 - M_1 + 1) + q^2(M_1 - 1) + q^3.$$

Pela fórmula de N_1 e pelo Teorema 3.3.1(3), vem que:

$$N_1 = q + 1 - \sum_{i=1}^{2g}(w_i) = q + 1 + M_1 - 1 = q + M_1.$$

Vemos que $Cpx(M_3) = \mathcal{O}(q^3)$, de onde resulta que $Cpx(h) = \mathcal{O}(q^3) = \mathcal{O}(q^g)$.

Uma decomposição *quase q-ária* pode ser escrita como

$$h = q^3 + (-1 + M_1 + \frac{M_2}{q})q^2 + (1 - M_1 + \frac{M_3}{q})q + M_1$$

e é da forma

$$h = q^3 + \mathcal{O}(\sqrt{q})q^2 + \mathcal{O}(\sqrt{q})q + \mathcal{O}(\sqrt{q}),$$

satisfazendo $\mathrm{Grz}(c_i) = \sqrt{q}$ para $i = 0, 1, 2$ e $\mathrm{Cpx}(h) = \mathcal{O}(q^g) = \mathrm{Grz}(h)$. □

Conjectura 4.4.6. *Se* $\deg(D) = 2g + 2 = 8$, *e* ∞ *é inerte, então:*

1. $M_7 = M_{2g+1} = q^g = q^3$, $a_i = M_i - M_{i-1} + \cdots \pm M_1 + (-1)^i$, *para* $4 \leq i \leq 2g = 6$, *é par quando* i *é ímpar e ímpar quando* i *é par; portanto, para* $4 \leq i \leq 2g = 6$, *os coeficientes de* $L(K,t)$ *têm paridade alternada invariante, isto é, não depende de* D *e* q, *e* h *é ímpar;*

2. I_4, I_5, I_6, I_7 *se expressam em função de* q, I_1, I_2, I_3; M_4, M_5, M_6, M_7 *se expressam em função de* q, M_1, M_2, M_3.

Justificação da conjectura. É natural conjecturar que a sequência de raciocínio no teorema anterior é válida e, portanto, que:

$$a_4 = M_4 - M_3 + M_2 - M_1 + 1,$$

$$a_5 = M_5 - M_4 + M_3 - M_2 + M_1 - 1,$$

$$a_6 = M_6 - M_5 + M_4 - M_3 + M_2 - M_1 + 1.$$

Seguir-se-ia que:

$$M_4 = q(M_2 - M_1 + 1) - [M_3 - M_2 + M_1 - 1 = (q-1)(M_2 - M_1 + 1) - M_3,$$

$$M_5 = q^2(M_1 + 1) - [M_4 - M_3 + M_2 - M_1 + 1 =$$

$$= q^2(M_1 + 1) - (q-1)(M_2 - M_1 + 1) + M_3 - (M_3 - M_2 + M_1 - 1) =$$

$$= q^2(M_1 + 1) - q(M_2 - M_1 + 1),$$

$$M_6 = q^3 - [M_5 - M_4 + M_3 - M_2 + M_1 - 1 =$$

$$= q^3 - q^2(M_1 + 1) + q(M_2 - M_1 + 1) + (q-1)(M_2 - M_1 + 1) - M_3 -$$

$$-M_3 + M_2 - M_1 + 1 = q^3 - q^2(M_1 + 1).$$

Agora, comparando $L(K, 1) = h$ com a L-série de Artin adaptada (Teorema 3.2.5), teríamos:

$$(q-1)\left[M_1 + q(M_2 - M_1 + 1) + M_3 + q^2(M_1 - 1) + q^3\right] =$$

$$= q^4\left[1 + \frac{M_1}{q} + \frac{M_2}{q^2} + \frac{M_3}{q^3} + \frac{M_4}{q^4} + \frac{M_5}{q^5} + \frac{M_6}{q^6} + \frac{M_7}{q^7}\right] \Rightarrow$$

$$(q-1)\left[M_1 + q(M_2 - M_1 + 1) + M_3 + q^2(M_1 - 1) + q^3\right] =$$

$$= q^4 + q^3M_1 + q^2M_2 + qM_3 + M_4 + \frac{M_5}{q} + \frac{M_6}{q^2} + \frac{M_7}{q^3} \Rightarrow$$

$$(q-1)[1 + (M_1 - 1) + (M_2 - M_1 + 1) + M_3 - M_2 + M_1 - 1 + q(M_2 - M_1 + 1) +$$

$$= q^2(M_1 - 1) + q^3] =$$

$$= q^4 + q^3M_1 + q^2M_2 + qM_3 + (q-1)(M_2 + M_1 + 1) - M_3 + q(M_1 + 1) -$$

$$-(M_2 + M_1 + 1) + q - (M_1 + 1) + \frac{M_7}{q^3} \Rightarrow$$

$$1 = \frac{M_7}{q^3}$$

e, portanto,

$$M_7 = q^3.$$

Assim, M_4, M_5, M_6 e M_7 se expressam em função de q, M_1, M_2 e M_3."

Como nos casos anteriores, de $M_4 = (q-1)(M_2 - M_1 + 1) - M_3$ deduziremos que I_4 se expressa em função de q, I_1, I_2, I_3. Analogamente, de $M_5 = q^2(M_1 + 1) - q(M_2 - M_1 + 1)$ deduziremos que I_5 se expressa em função de q, I_1, I_2, I_3. O mesmo valerá para $M_6 = q^3 - q^2(M_1 + 1)$ e I_6. □

Capítulo 5

Conclusões, limitações e novos rumos para pesquisa

Nossa adaptação da L-série de Artin oferece uma identificação finita e explícita (IFE) para $h(F)$ do CFA $F = \mathbb{F}_q(x)(\sqrt{D})$ de gêneros 1, 2 e 3, e as evidentes generalizações dos padrões sugeridos nesses casos.

Por limitação de tempo e de espaço, não foi possível tratar da questão do truncamento da IFE de h seguido de um algoritmo para localização de h no intervalo determinado pelo truncamento. Como continuação da pesquisa, é natural perguntar se o método usualmente empregado pela criptografia contemporânea na produtória infinita de Euler produziria a mesma complexidade se aplicado à IFE de h obtida nesta tese.

A pesquisa forneceu os coeficientes a_i do $L-$polinômio em função de q e das somas M_i de símbolos de Legendre polinomiais sobre polinômios mônicos de grau i. Tais IFE´s, até onde sabemos, não estão explicitadas na literatura, portanto, devem ser inéditas.

Vê-se, portanto, que os invariantes elementares M_i e I_i, de símbolos de Legendre polinomiais sobre classes de polinômios de grau i mônicos e irredutíveis, respectivamente, são poderosos geradores de invariantes fundamentais não elementares e importantes do CFA, fato não registrado

ainda na literatura.

Ao mesmo tempo, mostramos que metade das parcelas da L-série de Artin adaptada, $M_{g+i}, 1 \leq i \leq g$, que, em princípio, teriam complexidade algorítmica maior do que $\mathcal{O}(q^g)$, podem ser obtidas com complexidade de ordem menor ou igual a essa.

Obtivemos ainda uma *expansão quase* $q-$*ária de* h, sugerida pela desigualdade de Hasse-Weil, isto é,

$$h = q^g + c_{g-1}q^{g-1} + ... + c_1 q^1 + c_g,$$

com

$$\mathrm{Grz}\left(c_i\right) = \mathcal{O}\left(q^{\frac{1}{2}}\right), 1 \leq i \leq g$$

e

$$\mathrm{Cpx}\left(c_i\right) \leq \mathcal{O}\left(q^g\right), 1 \leq i \leq g.$$

Os coeficientes dessa expansão são determinados pelas somas M_i e I_i, mas suas expressões explícitas estão em aberto, ao que nos consta, com excessão dos casos $1 \leq d \leq 8$ e das generalizações que propusemos.

Além disso, nossa análise demonstra que os coeficientes a_i do $L-$polinômio se expressam em função dos coeficientes M_i da L-série de Artin, de forma que $\mathrm{Cpx}(a_i) = \mathrm{Cpx}(M_i)$.

Nosso método pode ser empregado para gêneros maiores do que 3, embora não tenhamos ainda vislumbrado uma demonstração geral da evidente generalização decorrente de nossa análise. Numa outra direção, pode-se investigar o que ocorre se os polinômios D que originam as extensões quadráticas forem apenas livre de quadrados, não necessariamente irredutíveis.

Referências Bibliográficas

[1] Artin, E., *Quadratishe Körper im Gebiete der höheren Kongruenzen I, II*, Math. Zeit., 19, 153-246, (1924).

[2] Cohen, H. (Ed.) et al., *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman and Hall, 2006.

[3] Coutinho, S. C., *Números Inteiros e Criptografia RSA*, IMPA, 2009.

[4] Coutinho, S. C., *Primalidade em Tempo Polinomial*, SBM, 2004.

[5] Diffie, W., Hellman, M. E., *New directions in cryptography*, IEEE Trans. Inf. Theory 22, 644-654 (1976).

[6] ElGamal, T., *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inf. Theory 31, 469-472 (1985).

[7] Ferreira, J., *Almost q-ary expansion for the divisor class number of hyperelliptic function fields* $K/\mathbb{F}_q(x)$, Journal of Algebra, Number Theory and Applications - aceito para publicação em agosto de 2013.

[8] Hasse, H., *Number Theory*, Springer-Verlag - 1980.

[9] Hoffstein, J., Rosen, M., *Average values of L-series in function fields*, J. reine angew. Math. 426 117-150 (1992).

[10] Kedlaya, K. S., Sutherland, A. V., *Computing L-Series of Hyperelliptic Curves*, in ANTS-VIII, LNCS 5011, van der Poorten, A. J., Stein, A. (Eds.), pp. 312-326. Berlin: Springer-Verlag, (2008).

[11] Kenneth, I., Rosen, M., *A Classical Introduction to Modern Number Theory*, Second Edition, Springer, NY, 1993.

[12] Koblitz, N., *Elliptic curve cryptosystems*, Mathematics of Computation 48, 203-209 (1987).

[13] Koblitz, N., *Hyperelliptic cryptosystems*, Journal of Cryptology 1, 139-150 (1989).

[14] Miller, V. S., *Use of elliptic curves in cryptography*, Advances in Cryptology - CRYPTO 85, Proc. Conf., Santa Barbara/Calif. 1985, Lect. Notes Comput. Sci. 218, 417-426 (1986).

[15] Mumford, D., *Tata Lectures on Theta H*, Birkhäuser, Boston, 2007.

[16] Niederreiter, H., Xing, C. G., *Algebraic Geometry in Coding Theory and Criptography*, Princeton University Press - 2009.

[17] Ribenboim, P., *The Theory of Classical Valuations*, Springer, NY, 1999.

[18] Rosen M., *Number Theory in Function Fields*, Springer, NY, 2002

[19] Salvador G.D.V, *Topics on the theory of algebraic function fields*, Birkhäuser - 2006.

[20] Scheidler R., *Cryptography in Quadratic Function Fields*, Designs, Codes and Cryptography 22(3), 239-264 - (2001).

[21] Scheidler, R., Stein, A., *Approximating Euler products and class number computation in algebraic number fields*, Rocky Mountain Journal of Mathematics 40(5), pp. 1689-1727 (2010).

[22] Stein A., *Sharp upper bounds for arithmetics in hyperelliptic function fields*, Journal of Ramanujan Matematical Society 9, pp. 1-86, (2001).

[23] Stein A., Teske E., *Explicit bounds and heuristics on class numbers in hyperelliptic function fields*, Mathematics of Computations Vol. 71, Number 238, pp.837-861, (2001).

[24] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag - 1993.

[25] Strey, E., *A Hipótese de Riemann para Curvas Algébricas e uma Caracterização da Curva Hermitiana*, Dissertação de Mestrado - UFES - 2008.

[26] Weiss, E., *Algebraic Number Theory*, McGraw-Hill - New York - 1963.