20º COLÓQUIO BRASILEIRO DE MATEMÁTICA

PONTOS RACIONAIS EM CURVAS SOBRE CORPOS FINITOS

ARNALDO GARCIA

IMPA 24 - 28 JULHO, 1995

impa

ARNALDO GARCIA (IMPA, RJ)

ISBN 85-244-0099-4

Conselho Nacional de Desenvolvimento Científico e Tecnológico

INSTITUTO DE MATEMÁTICA PURA E APLICADA

Estrada Dona Castorina, 110 - Jardim Botânico

22460-320 - Rio de Janeiro, RJ, Brasil

Moinho

(Ronaldo Garcia)

Sei mesmo ser da vida
Essa eterna despedida
Água ida, água ida
Água sempre de partida

E o vazio que não cheia
Volta sempre, me volteia
Meia volta, volta e meia
Como trama, como teia

A água que passa
É, sem engano, passado
Moinho girou
Mas como moinho é humano
Passou e marcou

Do pai a saudade e o caminho
É pó e o pó vento levou
Da mãe a coragem, carinho
E gira girou.

A Maria, Maria Clara e Julia
Aos irmãos Luis Carlos, Anibal,
Ivan, Ricardo, Ronaldo e Osvaldo.

A Otto Endler e Ricardo Mañé.
(in memoriam)

Conteúdo

Prefácio.

O objetivo destas notas é apresentar, de maneira elementar, alguns resultados fundamentais da teoria de curvas algébricas sobre corpos finitos. Estaremos essencialmente interessados aqui na contagem do número de soluções de equações algébricas sobre corpos finitos. Devido ao enfoque elementar a que nos propomos, evitaremos definições precisas de certos conceitos e enunciados rigorosos de alguns teoremas. Também, apesar de certas imprecisões nos resultados, abordaremos esta teoria utilizando somente o conceito de curva plana, ao invés do modelo não-singular ou do corpo de funções associados. Para completar as lacunas matemáticas de nossa abordagem, sugerimos as referências [4] e [15].

É necessário ressaltar que o material aqui exposto é de grande profundidade matemática; sua apresentação elementar devendo-se ao fato de utilizarmos (sem demonstração), em suas diversas formas, o Teorema de Weil sobre o número de pontos racionais em curvas sobre corpos finitos.

Por serem notas de um curso do 20º Colóquio Brasileiro de Matemática, o conteúdo deste livro é necessariamente pequeno em relação ao universo matemático dos corpos finitos. Para uma exploração profunda deste universo, sugerimos a referência [8].

§0. Introdução

O estudo das soluções (raízes) de equações algébricas é, sem dúvida, um problema central da Matemática. Pertencem a esta linha de problemas, os seguintes resultados fundamentais.

1. O corpo dos números complexos $\mathbf{C}$ é um corpo algebricamente fechado. Isto é, qualquer polinômio não-constante $f(X) \in \mathbf{C}[X]$ possui raízes em $\mathbf{C}$. A primeira prova completa deste resultado, conhecido como "Teorema Fundamental da Álgebra", é devida a Gauss (1799). Provas anteriores de d'Alembert, Euler e Lagrange assumiram a existência de raízes em alguma extensão de $\mathbf{R}$.

2. Um polígono regular com n lados, n sendo primo, pode ser construido com apenas régua e compasso se e somente se $(n-1)$ é uma potência de 2. Este resultado é também devido a Gauss, que provou o caso particular $n = 17$ quando tinha apenas 18 anos de idade.

3. Um polinômio $f(X) \in \mathbf{Q}[X]$ de grau maior que 4 não é, em geral, solúvel por radicais; isto é, as suas raízes não podem ser expressas apenas adjuntando "radicais" às operações do corpo $\mathbf{Q}$. Este resultado é devido aos matemáticos Ruffini (1798) e Abel (1824). A solubilidade por radicais, no caso de polinômios de grau 3, é devida a Scipione del Ferro, Cardano e Tartaglia. No caso de grau 4, a solubilidade por radicais foi demonstrada por Lodovico Ferrari. Estes resultados foram obtidos na primeira metade do século XVI.

4. Caracterização dos polinômios $f(X) \in \mathbf{Q}[X]$ que são solúveis por radicais. Esta caracterização, devida a Evariste Galois (1831), é feita em termos do grupo de Galois de $f(X)$ sobre $\mathbf{Q}$. Um caso particular desta caracterização, obtido por Abel em 1829, afirma que polinômios $f(X) \in \mathbf{Q}[X]$, com grupo de Galois comutativo, são solúveis por radicais. Tanto Galois como Abel morreram muito jovens: Galois com 20 anos e Abel aos 27 anos.

5. O famoso "Último Teorema de Fermat", que foi finalmente provado em 1994 por A. Wiles. Este resultado afirma que

$$X^n + Y^n = Z^n, \quad \text{onde} \quad n \geq 3,$$

não possui solução $(x, y, z) \in \mathbf{Z}^3$ com $xyz \neq 0$. Foram mais de 300 anos de pesquisas matemáticas, entre a formulação do problema e a sua resolução.

Todos os cinco resultados listados acima envolvem corpos de característica zero; i.e., extensões do corpo $\mathbf{Q}$ dos números racionais. Numa outra contribuição fundamental, em junho de 1830 sob o título "Sur la théorie des nombres", Galois introduziu e determinou a estrutura dos Corpos Finitos. O ponto de partida para Galois nesta publicação foi o cálculo de congruências, módulo um primo, realizado por Gauss. Anteriormente, Lagrange (1770) considera a congruência:

$$X^2 + bY^2 \equiv c \ \text{(módulo } p); \quad b, c \in \mathbf{Z}.$$

O estudo desta congruência é um passo necessário na prova do famoso Teorema de Lagrange que afirma ser todo número inteiro positivo uma soma de quatro quadrados de inteiros.

Deixamos de considerar acima vários resultados fundamentais, tais como: Lei de Reciprocidade Quadrática de Gauss, Teorema dos Zeros de Hilbert, Teorema de Deligne resolvendo as Conjeturas de Weil, Teorema de Faltings resolvendo a Conjetura de Mordell, etc.... No seu sentido mais amplo, o estudo de equações algébricas é o objetivo central da Teoria de Números e da Geometria Algébrica.

Seja K um corpo finito de cardinalidade q e seja $f(X,Y) \in K[X,Y]$ um polinômio (absolutamente) irredutível. Associamos então o conjunto $C_a(K)$ abaixo:

$$C_a(K) = \{(\mathbf{x},\mathbf{y}) \in K \times K \mid f(\mathbf{x},\mathbf{y}) = 0\}.$$

Os elementos de $C_a(K)$ são chamados de pontos racionais sobre o corpo finito K. Para uma curva (projetiva e não-singular) C definida sobre o corpo finito K, um celebrado Teorema de Weil [18] estabelece a seguinte cota para o número de seus pontos racionais:

$$\#C(K) \quad \leq \quad q + 1 + 2g\sqrt{q}, \qquad (*)$$

onde $g = g(C)$ denota o gênero da curva C. A origem deste teorema remonta a E. Artin [1], que considerou a congruência

$$\mathbf{y}^2 \equiv f(\mathbf{x}) \pmod{p},$$

onde $f(X) \in \mathbf{Z}[X]$ é um polinômio com coeficiente do termo de mais alto grau não-divisível pelo primo p. Quando o grau de $f(X)$ é igual a 3 ou a 4 (supondo que $f(X)$ tenha raízes distintas ou seja, que $f(X)$ é separável),

então o gênero da curva C associada satisfaz $g = g(C) = 1$. Artin então formulou uma conjetura (a validade de (*) no caso particular da curva acima; i.e., no caso particular em que $g(C) = 1$) que foi posteriormente verificada por Hasse [6]. Outras demonstrações deste famoso Teorema de Weil foram obtidas por Mattuck-Tate [9], Stepanov-Bombieri [11], Stöhr-Voloch [16], etc...

O objetivo destas notas é apresentar alguns melhoramentos da cota de Weil. O caráter elementar só sendo possível pois, exceto na seção 4 (Método de Stöhr-Voloch), assumimos aqui sem demonstração o Teorema de Weil, em suas diversas formas de apresentação.

§1. Curvas Algébricas

Seja K um corpo. Vamos sempre denotar por $\overline{K}$ um fêcho algébrico de K. Se $f(X,Y)$ é um polinômio em $K[X,Y]$, então a *curva algébrica afim* associada $C_a = C_a(\overline{K})$ é definida por

$$C_a = \{(\mathbf{x},\mathbf{y}) \in \overline{K} \times \overline{K} \mid f(\mathbf{x},\mathbf{y}) = 0\}.$$

Mais geralmente, para um corpo L tal que $K \subseteq L \subseteq \overline{K}$, denotamos

$$C_a(L) = \{(\mathbf{x},\mathbf{y}) \in L \times L \mid f(\mathbf{x},\mathbf{y}) = 0\}.$$

Estaremos sempre assumindo aqui que o polinômio $f(X,Y)$ é *absolutamente irredutível*, isto é, que $f(X,Y)$ é irredutível em $\overline{K}[X,Y]$. Denotaremos por $d = \deg(f)$ o grau (total) do polinômio $f(X,Y)$. O monômio X^iY^j tendo grau total $(i+j)$, temos que o grau de f é igual ao máximo dos graus dos monômios que aparecem no polinômio $f(X,Y)$.

Ao polinômio $f(X,Y)$ associamos também um polinômio $F(X,Y,Z)$ em três variáveis, como abaixo:

$$F(X,Y,Z) = Z^d \cdot f(\frac{X}{Z}, \frac{Y}{Z}).$$

O polinômio $F(X,Y,Z)$ assim construído é um *polinômio homogêneo*, isto é, todos os monômios de $F(X,Y,Z)$ têm o mesmo grau. Por ser polinômio homogêneo de grau d, temos que:

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d \cdot F(X,Y,Z), \quad \forall\, \lambda \in \overline{K}.$$

Dados (x_1, y_1, z_1) e (x_2, y_2, z_2) dois elementos de $\overline{K}^3$, ambos distintos de $(0,0,0)$, dizemos que eles são equivalentes se existe $\lambda \in \overline{K}$ tal que

$$(x_1, y_1, z_1) = \lambda \cdot (x_2, y_2, z_2).$$

A classe de equivalência de um tal elemento (x_1, y_1, z_1), isto é a reta ligando $(0,0,0)$ ao elemento (x_1, y_1, z_1), será denotada por $(x_1 : y_1 : z_1)$.

Definimos a *curva projetiva* associada C como abaixo:

$$C = C(\overline{K}) = \{(x_1 : y_1 : z_1) \in \overline{K}^3 \mid F(x_1, y_1, z_1) = 0\}.$$

Observamos que a curva afim C_a é mergulhada em C pela aplicação

$$(x, y) \mapsto (x : y : 1)$$

Os pontos de C da forma $(x_1 : y_1 : 0)$ são chamados *pontos do infinito* com relação a curva afim C_a.

De maneira análoga, denotamos (para $K \subseteq L \subseteq \overline{K}$)

$$C(L) = \{(x_1 : y_1 : z_1) \in L^3 \mid F(x_1, y_1, z_1) = 0\}.$$

A cardinalidade de tal conjunto $C(L)$, quando L é um corpo finito, é essencialmente o objetivo central destas notas.

Um invariante básico da curva plana C é o seu gênero $g = g(C)$ e este invariante satisfaz:

$$g \leq \frac{(d-1)(d-2)}{2}, \quad \text{com} \quad d = \deg(f(X, Y)).$$

A desigualdade acima é uma igualdade se e só se a curva plana C não possui *pontos singulares*; equivalentemente, é uma igualdade se e só se temos que, para $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \overline{K}^3$, vale a implicação **(1)** seguinte:

$$F(\mathbf{x}, \mathbf{y}, \mathbf{z}) = F_X(\mathbf{x}, \mathbf{y}, \mathbf{z}) = F_Y(\mathbf{x}, \mathbf{y}, \mathbf{z}) = F_Z(\mathbf{x}, \mathbf{y}, \mathbf{z}) = 0$$
$$\Rightarrow (\mathbf{x}, \mathbf{y}, \mathbf{z}) = (0, 0, 0). \qquad (1)$$

Acima, o símbolo F_X denota a derivada parcial de F em relação a variável X e, similarmente, para F_Y e F_Z. A definição de gênero e o seu cálculo, quando existem pontos singulares, fogem do escopo destas notas.

Apresentamos agora um teorema, que não será explicitamente utilizado no decorrer destas notas, que nos diz que certos polinômios são absolutamente irredutíveis. Este teorema trata de polinômios $f(X, Y) \in K[X, Y]$, K sendo um corpo qualquer, do tipo especial seguinte:

$$f(X, Y) = a_0 Y^n + a_1(X) Y^{n-1} + \cdots + a_n(X);\ a_i(X) \in K[X].$$

Supomos sempre que $a_0 \in K$ é não-nulo; i.e., temos

$$\deg_Y f(X, Y) = n,$$

onde $\deg_Y$ denota o grau na variável Y.

Para polinômios $f(X, Y)$ da forma acima, definimos

$$\varphi(f) = \max \left\{ \frac{\deg a_i(X)}{i} \;\middle|\; i = 1, 2, \ldots, n \right\}.$$

Provamos inicialmente a afirmação:

Afirmação. Seja $f(X,Y) \in K[X,Y]$ um polinômio como acima. Se este polinômio $f(X,Y)$ é redutível; i.e., se existem polinômios $g(X,Y)$ e $h(X,Y)$ em $K[X,Y]$ tais que

$$f(X,Y) = g(X,Y) \cdot h(X,Y),$$

então

$$\varphi(f) = \max\{\varphi(g), \varphi(h)\}.$$

Demonstração. Primeiramente, observamos que $g(X,Y)$ e $h(X,Y)$ são ainda polinômios do tipo especial aqui considerado. Escrevemos $g(X,Y)$ e $h(X,Y)$ da seguinte maneira:

$$g(X,Y) = b_0 Y^r + b_1(X)Y^{r-1} + \cdots + b_r(X)$$

e

$$h(X,Y) = c_0 Y^s + c_1(X)Y^{s-1} + \cdots + c_s(X),$$

onde $b_j(X)$, $c_k(X) \in K[X]$ e as constantes $b_0, c_0 \in K$ satisfazem $b_0 \cdot c_0 \neq 0$. Claramente, devemos ter que

$$r + s = n, \quad r < n \quad \text{e} \quad s < n.$$

Obtemos então a expressão

$$a_i(X) = \sum_{j+k=i} b_j(X) \cdot c_k(X); \quad 0 \leq i \leq n.$$

Pela própria definição da função φ, temos

$$\begin{aligned} \deg(b_j(X) \cdot c_k(X)) &\leq j\varphi(g) + k\varphi(h) \\ &\leq (j+k) \cdot \max\{\varphi(g), \varphi(h)\}. \end{aligned}$$

Pela expressão para $a_i(X)$ acima, concluimos

$$\deg a_i(X) \leq i \cdot \max\{\varphi(g), \varphi(h)\},$$

ou seja,

$$\varphi(f) \leq \max\{\varphi(g), \varphi(h)\}.$$

Vamos provar abaixo que:

$$\varphi(f) \geq \max\{\varphi(g), \varphi(h)\}.$$

Denotando $\varphi = \varphi(f)$, temos

$$f(X, Y^{\varphi}) = g(X, Y^{\varphi}) \cdot h(X, Y^{\varphi}).$$

Observamos que $\varphi \in \mathbf{Q}$ e que φ não é um número inteiro em geral; assim na igualdade acima estão possivelmente envolvidos *polinômios com expoentes racionais*. Denotando por $\deg(\dots)$ o grau total, temos

$$\deg f(X, Y^{\varphi}) = n \cdot \varphi.$$

De fato, a igualdade acima segue de

$$f(X, Y^{\varphi}) = a_0 Y^{n\varphi} + a_1(X) Y^{(n-1)\varphi} + \cdots + a_n(X),$$

e de que, para $1 \leq i \leq n$, vale

$$\begin{aligned} \deg(a_i(X) Y^{(n-i)\varphi}) &= \deg a_i(X) + (n-i)\varphi \\ &\leq i\varphi + (n-i)\varphi = n\varphi. \end{aligned}$$

Agora, claramente, temos

$$\deg g(X, Y^{\varphi}) \geq r\varphi \quad \text{e} \quad \deg h(X, Y^{\varphi}) \geq s\varphi.$$

Assim,

$$\deg(g(X, Y^{\varphi}) \cdot h(X, Y^{\varphi})) \geq r\varphi + s\varphi = n\varphi.$$

Por outro lado, devemos ter

$$\deg(f(X, Y^{\varphi})) = \deg(g(X, Y^{\varphi}) \cdot h(X, Y^{\varphi})).$$

Concluimos então que valem as igualdades:

$$\deg g(X, Y^{\varphi}) = r\varphi \quad \text{e} \quad \deg h(X, Y^{\varphi}) = s\varphi.$$

Da expressão

$$g(X, Y^{\varphi}) = b_0 Y^{r\varphi} + b_1(X) Y^{(r-1)\varphi} + \cdots + b_r(X),$$

e da igualdade $\deg g(X, Y^{\varphi}) = r\varphi$, obtemos então

$$\deg(b_j(X) Y^{(r-j)\varphi}) = \deg b_j(X) + (r-j)\varphi \leq r\varphi.$$

Assim, obtemos $\deg b_j(X) \leq j\varphi$, para $j = 1, 2, \ldots, r$, e, portanto, temos $\varphi(g) \leq \varphi$. Analogamente, temos $\varphi(h) \leq \varphi$. Isto prova que

$$\varphi(f) \geq \max\{\varphi(g), \varphi(h)\}. \qquad \square$$

Teorema 0. *Seja $f(X, Y) \in K[X, Y]$ um polinômio do tipo especial:*

$$f(X, Y) = a_0 Y^n + a_1(X) Y^{n-1} + \cdots + a_n(X);\ a_i(X) \in K[X] \quad \text{e} \quad a_0 \in K \setminus \{0\}.$$

Suponha que $\deg a_n(X) = m$ *é relativamente primo com* n *e ainda que*

$$\frac{m}{n} > \frac{\deg a_i(X)}{i}, \quad \text{para} \quad i = 1, 2, \ldots, n-1.$$

Então, o polinômio $f(X,Y)$ *é absolutamente irredutível.*

Demonstração: Suponha que

$$f(X,Y) = g(X,Y) \cdot h(X,Y); \quad g, h \in \overline{K}[X,Y].$$

Com as notações já introduzidas, temos

$$\varphi(g) = \max\left\{ \frac{\deg b_j(X)}{j} \;\middle|\; j = 1, 2, \ldots, r \right\} = \frac{\alpha}{\beta}; \;\; \beta \leq r < n$$

$$\varphi(h) = \max\left\{ \frac{\deg c_k(X)}{k} \;\middle|\; k = 1, 2, \ldots, s \right\} = \frac{\gamma}{\delta}; \;\; \delta \leq s < n,$$

onde $\alpha, \beta, \gamma, \delta \in \mathbf{N}$.

Como m e n são relativamente primos e das hipóteses feitas no enunciado do teorema, concluimos (utilize que $\beta < n$ e que $\delta < n$)

$$\varphi(f) = \frac{m}{n} \neq \max\left\{ \frac{\alpha}{\beta}, \; \frac{\gamma}{\delta} \right\} = \max\{\varphi(g), \varphi(h)\}.$$

Isto contradiz a afirmação provada acima. □

Exercício. Seja $f(X,Y) \in K[X,Y]$ um polinômio do tipo especial como acima ($\deg_Y f(X,Y) = n$). Suponha que

$$MDC(\deg a_{n-1}(X), \; n-1) = 1 \quad \text{e} \quad \varphi(f) = \frac{\deg a_{n-1}(X)}{n-1}.$$

Mostre que se $f(X,Y) \in K[X][Y]$ não tem raiz em $K[X]$, então $f(X,Y)$ é irredutível em $K[X,Y]$.

Recordamos agora algumas propriedades básicas dos corpos finitos. Denotaremos por $\mathbf{F}_q$ o corpo finito com q elementos, onde q é (necessariamente) uma potência de um primo p. O corpo $\mathbf{F}_q$ é o *corpo de raízes* (sobre $\mathbf{F}_p$) do polinômio $X^q - X$, assim temos que:

$$\mathbf{x}^{q-1} = 1, \quad \forall\, \mathbf{x} \in \mathbf{F}_q \setminus \{0\}.$$

Denotaremos por $\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$ o *grupo multiplicativo* do corpo $\mathbf{F}_q$. O grupo $\mathbf{F}_q^*$ é cíclico de ordem $(q-1)$, e então possui exatamente um subgrupo de ordem m, para cada divisor m de $(q-1)$.

Dada uma extensão de grau r de corpos finitos $\mathbf{F}_{q^r}|\mathbf{F}_q$, seu grupo de Galois é cíclico de ordem r. Um gerador deste grupo de Galois é o *automorfismo σ de Frobenius*

$$\sigma: \mathbf{F}_{q^r} \to \mathbf{F}_{q^r}, \quad \sigma(\mathbf{x}) = \mathbf{x}^q.$$

Em particular, para a extensão quadrática $\mathbf{F}_{p^{2n}}|\mathbf{F}_{p^n}$, temos que o *traço* (denotado $\mathcal{T}$) e a *norma* (denotada $\mathcal{N}$) são dados por

$$\mathcal{T}(\mathbf{y}) = \mathbf{y} + \mathbf{y}^{p^n}, \quad \forall\, \mathbf{y} \in \mathbf{F}_{p^{2n}}$$

e

$$\mathcal{N}(\mathbf{x}) = \mathbf{x}^{1+p^n}, \quad \forall\, \mathbf{x} \in \mathbf{F}_{p^{2n}}.$$

Observação: Para um polinômio absolutamente irredutível $f(X,Y) \in K[X,Y]$, definimos seu *corpo de funções* como sendo o corpo de frações do domínio $K[X,Y]/(f(X,Y))$, onde $(f(X,Y))$ denota o ideal principal de $K[X,Y]$ gerado pelo polinômio $f(X,Y)$. Estamos aqui interessados em determinar cotas para $\#C(L)$, quando L é um corpo finito tal que $K \subseteq L \subseteq \overline{K}$. Na verdade, as cotas determinadas neste livro são cotas para o número de *lugares racionais* (sobre o corpo finito L) do corpo de funções associado.

O conceito de curva algébrica é bem mais abrangente que o de curva plana introduzido nesta seção. Por exemplo, considere dois polinômios $f_1(X,Y,Z)$ e $f_2(X,Y,Z) \in K[X,Y,Z]$ sem fator comum de grau estritamente positivo. Associamos então a tais polinômios $f_1(X,Y,Z)$ e $f_2(X,Y,Z)$, o conjunto:

$$C = C(\overline{K}) = \{(\mathbf{x},\mathbf{y},\mathbf{z}) \in \overline{K}^3 \mid f_1(\mathbf{x},\mathbf{y},\mathbf{z}) = f_2(\mathbf{x},\mathbf{y},\mathbf{z}) = 0\}.$$

Tal conjunto C é uma *curva algébrica*. Para escolhas genéricas de f_1 e f_2, tal curva é irredutível e não-singular. Analogamente, para $n \in \mathbf{N}$, considere $(n-1)$ polinômios em n variáveis $f_1, f_2, \ldots, f_{n-1} \in K[X_1, X_2, \ldots, X_n]$ que sejam dois a dois relativamente primos. Novamente, para escolhas genéricas de $f_1, f_2, \ldots, f_{n-1}$, associamos a *curva algébrica* C (irredutível e não-singular) como abaixo:

$$\begin{aligned} C &= C(\overline{K}) \\ &= \{(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) \in \overline{K}^n \mid \forall\, i, 1 \leq i \leq n-1,\ f_i(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n) = 0\}. \end{aligned}$$

As cotas determinadas neste livro para $\#C(L)$, onde L denota um corpo finito, são válidas para as curvas algébricas (mais gerais) definidas acima.

§2. Curvas Maximais

Seja C uma curva algébrica projetiva não-singular definida sobre um corpo finito $K = \mathbf{F}_q$. É um resultado profundo devido a Weil [18] *que vale a desigualdade seguinte:*

$$\#C(\mathbf{F}_q) \leq 1 + q + 2g\sqrt{q} \ , \qquad (*)$$

onde g denota o gênero da curva C.

Curvas para as quais a desigualdade em (*) é uma igualdade (neste caso, a cardinalidade q é um quadrado; i.e., $q = p^{2n}$, $n \in \mathbf{N}$) são chamadas *curvas maximais* (sobre $\mathbf{F}_q$). Por um resultado devido a Ihara [7], temos que o gênero g de uma curva maximal sobre $\mathbf{F}_q$ (q um quadrado) satisfaz a desigualdade

$$g \leq \frac{\sqrt{q} \cdot (\sqrt{q} - 1)}{2}. \qquad (**)$$

Equivalentemente, o resultado de Ihara afirma que:

$$\text{Se} \quad g > \frac{q - q^{1/2}}{2}, \quad \text{então} \quad \#C(\mathbf{F}_q) < 1 + q + 2g\sqrt{q}.$$

O exemplo abaixo nos fornece uma situação onde ambas desigualdades (*) e (**) são de fato igualdades. Em outras palavras, é um exemplo de curva maximal com gênero maior possível (segundo (**)).

Exemplo 1. (Curva de Hermite) Considere a curva projetiva C associada ao polinômio $f(X, Y)$ abaixo:

$$f(X, Y) = Y^{p^n} + Y - X^{1+p^n} \quad \in \quad \mathbf{F}_q[X, Y],$$

onde $\mathbf{F}_q$ é o corpo finito de cardinalidade $q = p^{2n}$, com $n \in \mathbf{N}$.

O polinômio homogêneo associado $F(X, Y, Z)$ é dado por (grau $F = d = 1 + p^n$)

$$F(X, Y, Z) = Z \cdot Y^{p^n} + Z^{p^n} \cdot Y - X^{1+p^n}.$$

Um cálculo direto mostra que C é não-singular; i.e., a implicação em **(1)** é satisfeita. Assim o gênero g da curva C é dado por

$$g = \frac{(d-1)(d-2)}{2} = \frac{p^n \cdot (p^n - 1)}{2} = \frac{\sqrt{q}(\sqrt{q} - 1)}{2}.$$

Para a contagem dos pontos do conjunto $C(\mathbf{F}_q)$, olhamos primeiramente para sua parte afim $C_a(\mathbf{F}_q)$:

$$\begin{aligned} C_a(\mathbf{F}_q) &= \{(\mathbf{x}, \mathbf{y}) \in \mathbf{F}_q \times \mathbf{F}_q \mid f(\mathbf{x}, \mathbf{y}) = 0\} \\ &= \{(\mathbf{x}, \mathbf{y}) \in \mathbf{F}_q \times \mathbf{F}_q \mid \mathcal{T}(\mathbf{y}) = \mathcal{N}(\mathbf{x})\}, \end{aligned}$$

onde $\mathcal{T}$ e $\mathcal{N}$ denotam o traço e a norma da extensão $\mathbf{F}_q \mid \mathbf{F}_{p^n}$. Usando que o traço e a norma têm como imagem o corpo $\mathbf{F}_{p^n}$; i.e., são aplicações como abaixo:

$$\mathcal{T}: \mathbf{F}_{p^{2n}} \to \mathbf{F}_{p^n} \quad \text{e} \quad \mathcal{N}: \mathbf{F}_{p^{2n}} \to \mathbf{F}_{p^n},$$

e que o traço é uma aplicação sobrejetora $\mathbf{F}_{p^n}$-linear (em particular, $\#\mathcal{T}^{-1}(\mathbf{y}) = p^n$, $\forall \mathbf{y} \in \mathbf{F}_{p^n}$), obtemos

$$\begin{aligned} \#C_a(\mathbf{F}_q) &= \sum_{\mathbf{x} \in \mathbf{F}_q} \#\{\mathbf{y} \in \mathbf{F}_q \mid \mathcal{T}(\mathbf{y}) = \mathbf{x}^{1+p^n}\} \\ &= \sum_{\mathbf{x} \in \mathbf{F}_q} \#\mathcal{T}^{-1}(\mathbf{x}^{1+p^n}) \\ &= \sum_{\mathbf{x} \in \mathbf{F}_q} p^n = p^{2n} \cdot p^n = p^{3n}. \end{aligned}$$

Notando que $(0:1:0)$ é o único ponto do infinito de C com relação a curva afim C_a, temos então que:

$$\#C(\mathbf{F}_q) = 1 + p^{3n}.$$

Um cálculo direto mostra que também

$$1 + q + 2g\sqrt{q} \ = 1 + p^{3n}.$$

Assim a curva C é maximal sobre $\mathbf{F}_q (q = p^{2n})$ ou seja, obtemos uma igualdade em (*) para a curva C deste Exemplo 1.

Observação: Uma outra maneira de verificar que a curva C considerada no Exemplo 1 satisfaz (sendo $q = p^{2n}$, $n \in \mathbf{N}$)

$$\#C(\mathbf{F}_q) = 1 + p^{3n},$$

é a seguinte: Seja $(\mathbf{x}, \mathbf{y}) \in \overline{K} \times \overline{K}$, onde $K = \mathbf{F}_q$, um ponto da curva afim; isto é,

$$\mathbf{y}^{p^n} + \mathbf{y} = \mathbf{x}^{1+p^n}.$$

Suponha que $\mathbf{x} \in K$; i.e., temos $\mathbf{x}^{p^{2n}} = \mathbf{x}$. Assim,

$$\mathbf{y}^{p^{2n}} + \mathbf{y}^{p^n} = (\mathbf{y}^{p^n} + \mathbf{y})^{p^n} = (\mathbf{x}^{1+p^n})^{p^n} = \mathbf{x}^{p^{2n}+p^n} = \mathbf{x}^{1+p^n} = \mathbf{y}^{p^n} + \mathbf{y}.$$

Vemos então que $\mathbf{y}^{p^{2n}} = \mathbf{y}$, ou seja, que $\mathbf{y} \in \mathbf{F}_q$.

Para cada $\mathbf{x} \in \mathbf{F}_q$, existem exatamente p^n soluções no fêcho algébrico $\overline{\mathbf{F}}_q$ para a equação polinomial

$$Y^{p^n} + Y = \mathbf{x}^{1+p^n},$$

pois o polinômio $Y^{p^n} + Y - \mathbf{x}^{1+p^n}$ é *separável* (i.e., tem raízes distintas). Os argumentos acima mostram que qualquer solução $\mathbf{y} \in \overline{\mathbf{F}}_q$ é racional sobre $\mathbf{F}_q$; isto é, temos que $\mathbf{y} \in \mathbf{F}_q$. Para cada $\mathbf{x} \in \mathbf{F}_q$ ($\mathbf{x}$ percorre aqui um conjunto de cardinalidade p^{2n}), existem p^n elementos $\mathbf{y}$ em $\mathbf{F}_q$ tais que o par $(\mathbf{x}, \mathbf{y})$ pertence a curva. Somando o ponto do infinito a estes p^{3n} pares $(\mathbf{x}, \mathbf{y})$, concluimos

$$\#C(\mathbf{F}_q) = 1 + p^{3n}.$$

Exercício. Considere a curva projetiva C associada ao polinômio $f(X, Y)$ abaixo:

$$f(X, Y) = Y^{p^n} + Y - X^m \quad \in \quad \mathbf{F}_q[X, Y],$$

onde $q = p^{2n}$ e onde m é um divisor próprio de $(p^n + 1)$.

a) Mostre que $P = (1 : 0 : 0)$ é o único ponto no infinito da curva projetiva associada C. Mostre que o ponto P é a única singularidade da curva C; i.e., mostre que para $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \overline{\mathbf{F}}_q^3$ vale a implicação seguinte (onde F denota o polinômio homogêneo associado):

$$F(\mathbf{x}, \mathbf{y}, \mathbf{z}) = F_X(\mathbf{x}, \mathbf{y}, \mathbf{z}) = F_Y(\mathbf{x}, \mathbf{y}, \mathbf{z}) = F_Z(\mathbf{x}, \mathbf{y}, \mathbf{z}) = 0$$

$$\Rightarrow (\mathbf{x}, \mathbf{y}, \mathbf{z}) = (0, 0, 0) \quad \text{ou} \quad (\mathbf{x} : \mathbf{y} : \mathbf{z}) = (1 : 0 : 0).$$

b) Seja H o (único) subgrupo do grupo multiplicativo $\mathbf{F}_q^*$ com ordem satisfazendo $|H| = m \cdot (p^n - 1)$. Mostre que:

$$\mathbf{x}^{mp^n} = \mathbf{x}^m, \quad \forall\, \mathbf{x} \in H \cup \{0\}.$$

c) Copiando argumentos utilizados na observação anterior, mostre que:

$$\mathbf{x} \in H \cup \{0\} \quad \text{e} \quad f(\mathbf{x}, \mathbf{y}) = 0 \quad \Rightarrow \quad \mathbf{y} \in \mathbf{F}_q.$$

d) Conclua que a curva C é maximal sobre $\mathbf{F}_q$. Para isto, utilize que o gênero g da curva C é dado por

$$g = g(C) = \frac{(p^n - 1)(m-1)}{2}.$$

Observação: A curva de Hermite é única no seguinte sentido. Se uma curva algébrica é maximal sobre $\mathbf{F}_q (q = p^{2n},\ n \in \mathbf{N})$ e de gênero g satisfazendo

$$g = \frac{p^n(p^n - 1)}{2},$$

então esta curva é isomorfa a curva considerada no Exemplo 1. Isto é o resultado central de [10].

§3. A Cota de Serre

Vamos precisar aqui do conceito de inteiro algébrico. Um número complexo $\alpha \in \mathbf{C}$ é dito um *inteiro algébrico* se ele é raiz de um polinômio mônico de $\mathbf{Z}[t]$; i.e., o elemento α satisfaz:

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \text{ com } a_i \in \mathbf{Z} \text{ e } n \in \mathbf{N}.$$

A soma e o produto de inteiros algébricos são ainda inteiros algébricos. Um inteiro algébrico pertencente ao corpo dos números racionais $\mathbf{Q}$ está necessariamente em $\mathbf{Z}$.

Vamos precisar também da seguinte forma do teorema de Weil (equivalente à desigualdade em (*)). *Para uma curva C de gênero g definida sobre o corpo finito $\mathbf{F}_q$, existem números complexos α_i, i=1,2, ... ,2g, tais que:*

$$\#C(\mathbf{F}_q) = 1 + q - \sum_{i=1}^{2g} \alpha_i \ , \qquad (*_1)$$

onde α_i é inteiro algébrico satisfazendo $|\alpha_i| = \sqrt{q}$. Mais ainda,

$$\prod_{i=1}^{2g}(1 - \alpha_i t) \quad \in \quad \mathbf{Z}[t].$$

Note que o lado direito da desigualdade (*) é obtido a partir de $(*_1)$ tomando $\alpha_1 = \cdots = \alpha_{2g} = -\sqrt{q}$.

Embora não será usado explicitamente nestas notas, enfatizamos que os inteiros algébricos α_i, $i = 1, 2, \ldots, 2g$, são os inversos das raízes da *Função Zeta* associada à curva C.

Podemos agora provar o seguinte teorema, devido a J.-P. Serre [12]. Ele representa um melhoramento da cota (*) quando a cardinalidade q do corpo finito não é um quadrado.

Teorema 1. (Cota de Serre). *Para uma curva algébrica não-singular C de gênero g definida sobre o corpo finito $\mathbf{F}_q$, vale a desigualdade*

$$\#C(\mathbf{F}_q) \leq 1 + q + g \cdot [2\sqrt{q}],$$

onde $[\gamma]$ denota a parte inteira de $\gamma \in \mathbf{R}$.

Demonstração: Como

$$\prod_{i=1}^{2g}(1 - \alpha_i t) \quad \in \quad \mathbf{Z}[t],$$

podemos reordenar os números complexos $\alpha_1, \ldots, \alpha_g$, $\alpha_{g+1}, \ldots, \alpha_{2g}$ de tal forma que:

$$\alpha_{g+i} = \overline{\alpha}_i \ , \text{ para } i = 1, 2, \ldots, g,$$

onde $\overline{\alpha}_i$ denota o *complexo-conjugado* de α_i. Com esta reordenação dos inteiros algébricos α_i e de $|\alpha_i| = \sqrt{q}$, obtemos

$$\alpha_{g+i} = \overline{\alpha}_i = q/\alpha_i \ .$$

Seja $\beta_i = \alpha_i + \overline{\alpha}_i + [2\sqrt{q}] + 1$, para $i = 1, 2, \ldots, g$. Como β_i é um número real e como $|\alpha_i + \overline{\alpha}_i| \leq |\alpha_i| + |\overline{\alpha}_i| = 2\sqrt{q}$, temos $\beta_i > 0$. Observamos também que β_i, para $i = 1, 2, \ldots, g$, é um inteiro algébrico.

Seja agora $E = \mathbf{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{2g})$. Então $E|\mathbf{Q}$ é *extensão galoisiana*, pois E é o corpo de raízes sobre $\mathbf{Q}$ do polinômio $\prod_{i=1}^{2g}(1 - \alpha_i t) \in \mathbf{Z}[t]$. Qualquer automorfismo σ desta extensão $E|\mathbf{Q}$ induz então uma permutação no conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_{2g}\}$. Se $\sigma(\alpha_i) = \alpha_j$, então temos

$$\sigma(\overline{\alpha}_i) = \sigma(q/\alpha_i) = q/\sigma(\alpha_i) = q/\alpha_j = \overline{\alpha}_j.$$

Assim, um automorfismo σ induz também uma permutação no conjunto $\{\beta_1, \beta_2, \ldots, \beta_g\}$. Logo, o elemento $\prod_{i=1}^{g}\beta_i$ fica fixo por todos os automorfismos da extensão $E|\mathbf{Q}$, e consequentemente

$$\prod_{i=1}^{g}\beta_i \quad \in \quad \mathbf{Q}.$$

Sendo um número racional e ao mesmo tempo um inteiro algébrico, concluimos que

$$\prod_{i=1}^{g}\beta_i \quad \in \quad \mathbf{Z}.$$

Agora, de $\beta_i > 0$, obtemos

$$\prod_{i=1}^{g}\beta_i \quad \geq \quad 1.$$

Utilizando a desigualdade abaixo entre a *média aritmética* e a *geométrica*

$$\frac{1}{g}\sum_{i=1}^{g}\beta_i \quad \geq \quad \left(\prod_{i=1}^{g}\beta_i\right)^{1/g},$$

concluimos

$$g \leq \sum_{i=1}^{g} \beta_i = \sum_{i=1}^{g} (\alpha_i + \overline{\alpha}_i) + g[2\sqrt{q}] + g$$

$$= (\sum_{i=1}^{2g} \alpha_i) + g[2\sqrt{q}] + g.$$

Utilizando agora a igualdade $(*_1)$, obtemos finalmente

$$\#C(\mathbf{F}_q) \leq 1 + q + g[2\sqrt{q}]. \quad \square$$

Exercício. Utilizando os mesmos argumentos da demonstração do Teorema 1 e substituindo β_i (para $i = 1, 2, \ldots, g$) por

$$\beta_i' = -(\alpha_i + \overline{\alpha}_i) + [2\sqrt{q}] + 1,$$

mostre que:

$$\#C(\mathbf{F}_q) \geq 1 + q - g[2\sqrt{q}].$$

Tomemos, por exemplo, o caso $q = 8$ e $g = 3$. Neste caso,

$$2g\sqrt{q} \simeq 16,97 \quad \text{e} \quad g[2\sqrt{q}\,] = 15.$$

Assim, a cota do Teorema 1 é efetivamente menor que a cota na desigualdade (*) e, para uma curva C de gênero 3, temos

$$\#C(\mathbf{F}_8) \leq 1 + 8 + 15 = 24.$$

O exemplo seguinte mostra que a cota acima é atingida.

Exemplo 2. (Quártica de Klein). Considere a curva C associada ao polinômio

$$f(X,Y) = Y^3 + X^3Y + X \quad \in \quad \mathbf{F}_8[X,Y].$$

O polinômio $F(X,Y,Z)$ homogêneo associado de grau 4 é

$$F(X,Y,Z) = ZY^3 + X^3Y + XZ^3 \quad \in \quad \mathbf{F}_8[X,Y,Z].$$

Vemos então que são dois os pontos no infinito, a saber: os pontos $(0:1:0)$ e $(1:0:0)$. É fácil verificar que a implicação **(1)** está satisfeita neste caso e, portanto, temos $g = g(C) = 3$.

Note que um ponto $(\mathbf{x},\mathbf{y})$ da curva afim associada C_a satisfaz:

$$\mathbf{x} = 0 \quad \Leftrightarrow \quad \mathbf{y} = 0.$$

Chamaremos este ponto $(0,0)$ de origem. Multiplicando $f(X,Y)$ por X^6, obtemos

$$W^3 + X^7 \cdot W + X^7, \text{ onde } W = X^2 \cdot Y.$$

Retirando a origem da curva afim C_a, podemos agora ver que:

$$\begin{aligned} \#C_a(\mathbf{F}_8) - 1 &= \#\{(\mathbf{x},\mathbf{w}) \in \mathbf{F}_8^* \times \mathbf{F}_8 \mid \mathbf{x}^7 = \frac{\mathbf{w}^3}{\mathbf{w}+1}\} \\ &= \#\{(\mathbf{x},\mathbf{w}) \in \mathbf{F}_8^* \times \mathbf{F}_8 \mid \mathbf{w}^3 + \mathbf{w} + 1 = 0\}. \end{aligned}$$

A última igualdade acima decorre de que $\mathbf{x}^7 = 1$, $\forall\, \mathbf{x} \in \mathbf{F}_8^*$. Observando que o polinômio $W^3 + W + 1$ tem três raízes no corpo $\mathbf{F}_8$, pois é irredutível em $\mathbf{F}_2[W]$, concluimos

$$\#\{(\mathbf{x},\mathbf{w}) \in \mathbf{F}_8^* \times \mathbf{F}_8 \mid \mathbf{w}^3 + \mathbf{w} + 1 = 0\} = 7 \times 3 = 21.$$

Somando a estas 21 soluções, a origem e os dois pontos no infinito, obtemos

$$\#C(\mathbf{F}_8) = 21 + 1 + 2 = 24.$$

Apresentamos agora uma prova do resultado de Ihara (desigualdade (**)). Ele nos diz que se o gênero da curva é "grande" com relação a cardinalidade do corpo finito, então a curva não é maximal.

Proposição 2. *O gênero g de uma curva maximal sobre $\mathbf{F}_q$ satisfaz:*

$$g \leq \sqrt{q} \cdot (\sqrt{q} - 1)/2.$$

Demonstração: Vamos precisar do seguinte refinamento de $(*_1)$: *Para uma curva C de gênero g definida sobre o corpo finito $\mathbf{F}_q$, vale*

$$\#C(\mathbf{F}_{q^r}) = 1 + q^r - \sum_{i=1}^{2g} \alpha_i^r \ , \quad \forall r \in \mathbf{N}. \qquad (*_r)$$

Agora, uma curva algébrica C é maximal sobre o corpo finito $\mathbf{F}_q$ se e somente se $\alpha_i = -\sqrt{q}$, $\forall i = 1, 2, \ldots, 2g$. Então, para tais curvas maximais, temos (tomando $r = 2$)

$$\#C(\mathbf{F}_{q^2}) = 1 + q^2 - \sum_{i=1}^{2g} \alpha_i^2 = 1 + q^2 - 2gq.$$

Utilizando então a desigualdade óbvia abaixo:

$$\#C(\mathbf{F}_{q^2}) \quad \geq \quad \#C(\mathbf{F}_q),$$

e a hipótese que a curva C é maximal; i.e.,

$$\#C(\mathbf{F}_q) = 1 + q + 2g\sqrt{q} \ ,$$

concluimos a desigualdade de Ihara

$$g \ \leq \ \sqrt{q}(\sqrt{q}-1)/2 \quad = \quad \frac{1}{2}(q-\sqrt{q}). \quad \square$$

Exercício. Seja C uma curva de gênero g atingindo a cota de Serre sobre o corpo finito $\mathbf{F}_q$; i.e.,

$$\#C(\mathbf{F}_q) = 1 + q + g[2\sqrt{q}].$$

a) Com a notação do Teorema 1, mostre que:

$$\beta_i = 1, \quad \forall i = 1, 2 \ldots, g.$$

Equivalentemente, vale a igualdade

$$\alpha_i + \overline{\alpha}_i = -[2\sqrt{q}], \quad \forall i = 1, 2, \ldots, g.$$

Dica: Utilize que a desigualdade entre média aritmética e geométrica é uma igualdade se e só se temos $\beta_1 = \beta_2 = \cdots = \beta_g$.

b) Seja $\gamma = [2\sqrt{q}]$. Mostre que:

$$\alpha_i^2 + \overline{\alpha}_i^2 = \gamma^2 - 2q, \quad \forall i = 1, 2, \ldots, g.$$

Dica: Utilize o item a) e que $\alpha_i \cdot \overline{\alpha}_i = q$.

c) Com argumentos análogos aos utilizados na demonstração da desigualdade de Ihara (Proposição 2), conclua

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

onde a última desigualdade acima decorre de computações simples.

d) Utilizando o item a), mostre que:

$$\prod_{i=1}^{2g}(1 - \alpha_i t) = (1 + [2\sqrt{q}]t + qt^2)^g.$$

§4. O Método de Stöhr-Voloch

Este método envolve a construção de uma *função auxiliar* (em geral, esta função é obtida da equação do *hiperplano osculante*) que tenha zero de ordem "grande" em cada ponto do conjunto $C(\mathbf{F}_q)$. Ilustraremos este método usando o caso particular de curvas planas. Neste caso, ordem "grande" vai significar ordem ≥ 2.

Vamos necessitar alguns conceitos antes de enunciar o teorema central desta seção. Num ponto $(\mathbf{x}, \mathbf{y})$ da curva afim C_a associada ao polinômio $f(X, Y)$ (i.e., $f(\mathbf{x}, \mathbf{y}) = 0$), definimos *reta tangente* da curva em $(\mathbf{x}, \mathbf{y})$ como sendo a reta dada pela equação linear

$$(X - \mathbf{x})f_X(\mathbf{x}, \mathbf{y}) + (Y - \mathbf{y})f_Y(\mathbf{x}, \mathbf{y}) = 0. \qquad (2)$$

Note que o conceito de reta tangente só faz sentido se $f_X(\mathbf{x}, \mathbf{y}) \neq 0$ ou $f_Y(\mathbf{x}, \mathbf{y}) \neq 0$; isto é, se o ponto $(\mathbf{x}, \mathbf{y})$ não é uma singularidade da curva afim associada a $f(X, Y)$.

Supomos agora que $f(X, Y) \in \mathbf{F}_q[X, Y]$ e escrevemos

$$f(X, Y) = \sum_{i,j} a_{ij} X^i Y^j, \text{ com } a_{ij} \in \mathbf{F}_q.$$

Se $(\mathbf{x}, \mathbf{y}) \in C_a$, então $(\mathbf{x}^q, \mathbf{y}^q) \in C_a$. De fato, temos que:

$$f(\mathbf{x}, \mathbf{y}) = 0 \quad \Rightarrow \quad f(\mathbf{x}^q, \mathbf{y}^q) = f(\mathbf{x}, \mathbf{y})^q = 0.$$

A igualdade $f(\mathbf{x}^q, \mathbf{y}^q) = f(\mathbf{x}, \mathbf{y})^q$ é verificada como abaixo:

$$f(\mathbf{x}^q, \mathbf{y}^q) = \sum_{i,j} a_{ij} \mathbf{x}^{iq} \mathbf{y}^{jq} = \sum_{i,j} a_{ij}^q \mathbf{x}^{iq} \mathbf{y}^{jq}$$

$$= (\sum_{i,j} a_{ij} \mathbf{x}^i \mathbf{y}^j)^q = f(\mathbf{x}, \mathbf{y})^q.$$

Utilizamos, para estabelecer as igualdades acima, que $a_{ij}^q = a_{ij}$, $\forall i, j$; e ainda que

$$(\mathbf{w} + \mathbf{z})^q = \mathbf{w}^q + \mathbf{z}^q, \quad \forall \mathbf{w}, \mathbf{z} \in \overline{\mathbf{F}}_q \ .$$

A *função auxiliar* $h(X, Y)$ do polinômio (absolutamente irredutível) $f(X, Y) \in \mathbf{F}_q[X, Y]$ é dada pela equação

$$h(X, Y) = (X - X^q) f_X(X, Y) + (Y - Y^q) f_Y(X, Y), \qquad (3)$$

onde f_X e f_Y denotam as derivadas parciais de f.
Note que o grau do polinômio $h(X, Y)$ satisfaz:

$$\deg(h) \leq \deg(f) + q - 1.$$

Dados dois polinômios $g_1(X, Y)$ e $g_2(X, Y) \in \mathbf{F}_q[X, Y]$, escrevemos aqui $g_1 \equiv g_2 \pmod{f}$ se existir polinômio $g_3 \in \mathbf{F}_q[X, Y]$ tal que:

$$g_1 - g_2 = f \cdot g_3.$$

Proposição 3. *Seja $h(X, Y)$ a função auxiliar do polinômio $f(X, Y)$ como definida pela Equação* (3).

Se $h \equiv 0 (\mathrm{mod}\, f)$, *então* $(f_{XX} f_Y^2 - 2 f_{XY} f_X f_Y + f_{YY} f_X^2) \equiv 0 (\mathrm{mod}\, f)$.

Demonstração: A hipótese $h \equiv 0 (\mathrm{mod}\, f)$ é equivalente a

$$(X - X^q) f_X(X, Y) \quad \equiv \quad -(Y - Y^q) f_Y(X, Y).$$

Multiplicando então o polinômio $(f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2)$ por $(X - X^q)^2$, obtemos

$$(X - X^q)^2 \cdot [f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2]$$
$$\equiv [(X - X^q)^2 f_{XX} + 2(X - X^q)(Y - Y^q)f_{XY} + (Y - Y^q)^2 f_{YY}] \cdot f_Y^2.$$

Logo, basta mostrar a validade da congruência seguinte:

$$(X - X^q)^2 f_{XX} + 2(X - X^q)(Y - Y^q)f_{XY} + (Y - Y^q)^2 f_{YY} \equiv 0.$$

Novamente da hipótese $h \equiv 0 \pmod f$, obtemos que existe polinômio $g = g(X, Y)$ tal que:

$$h = (X - X^q)f_X + (Y - Y^q)f_Y = f \cdot g.$$

Derivando parcialmente em relação a X, temos

$$(X - X^q)f_{XX} + f_X + (Y - Y^q)f_{XY} = f_X \cdot g + f \cdot g_X.$$

Em particular, multiplicando por $(X - X^q)$,

$$(X - X^q)^2 f_{XX} + (X - X^q)(Y - Y^q)f_{XY} \equiv (X - X^q)f_X(g - 1).$$

De maneira análoga,

$$(Y - Y^q)^2 f_{YY} + (X - X^q)(Y - Y^q)f_{XY} \equiv (Y - Y^q)f_Y(g - 1).$$

Somando as duas últimas congruências acima, obtemos finalmente

$$(X-X^q)^2 f_{XX}+2(X-X^q)(Y-Y^q)f_{XY}+(Y-Y^q)^2 f_{YY} \equiv h\cdot(g-1) \equiv 0. \quad \square$$

Observação: a) No caso em que a cardinalidade do corpo finito é uma potência de 2 (i.e., $q = 2^n$ com $n \in \mathbf{N}$), é fácil verificar que o polinômio $(f_{XX}f_Y^2 - 2f_{XY}f_Xf_Y + f_{YY}f_X^2)$ é identicamente nulo.

b) Se a função auxiliar dada pela Equação **(3)** satisfaz $h \equiv 0 (\mathrm{mod}\, f)$ então, para todo $(\mathbf{x}, \mathbf{y}) \in \overline{\mathbf{F}}_q \times \overline{\mathbf{F}}_q$ tal que $f(\mathbf{x}, \mathbf{y}) = 0$, vale que:

$$(\mathbf{x}^q - \mathbf{x})f_X(\mathbf{x}, \mathbf{y}) + (\mathbf{y}^q - \mathbf{y})f_Y(\mathbf{x}, \mathbf{y}) = 0.$$

Equivalentemente, em todo ponto $(\mathbf{x}, \mathbf{y})$ da curva afim C_a associada a $f(X, Y)$, temos

$$(\mathbf{x}^q, \mathbf{y}^q) \quad \in \quad T_{(\mathbf{x},\mathbf{y})}(C_a),$$

onde $T_{(\mathbf{x},\mathbf{y})}$ denota a reta tangente (vide Equação **(2)**) no ponto $(\mathbf{x}, \mathbf{y})$.

Dados dois polinômios $f(X, Y)$, $h(X, Y)$ e um ponto $P = (\mathbf{x}, \mathbf{y})$, denotamos por $\mathcal{I}(P; f, h)$ a *multiplicidade de interseção* em P da curva associada a $f(X, Y)$ com a curva associada a $h(X, Y)$. Estaremos sempre supondo que os polinômios $f(X, Y)$ e $h(X, Y)$ não tem fator comum de grau estritamente positivo. A multiplicidade de interseção satisfaz então as seguintes propriedades naturais:

a) $\mathcal{I}(P; f, h) \in \mathbf{N}$.

b) $\mathcal{I}(P; f, h) = 0$ se e só se $f(\mathbf{x}, \mathbf{y}) \neq 0$ ou $h(\mathbf{x}, \mathbf{y}) \neq 0$.

c) Se $f(\mathbf{x}, \mathbf{y}) = h(\mathbf{x}, \mathbf{y}) = 0$ e se as retas tangentes em $P = (\mathbf{x}, \mathbf{y})$ das curvas determinadas por $f(X, Y)$ e por $h(X, Y)$ coincidem, então

$$\mathcal{I}(P; f, h) \quad \geq \quad 2.$$

O teorema de Bezout afirma então que:

$$\sum_{P} \mathcal{I}(P; f, h) \quad \leq \quad (\deg f) \cdot (\deg h), \tag{4}$$

onde $P = (\mathbf{x}, \mathbf{y})$ *percorre os pontos do plano* $\overline{\mathbf{F}}_q \times \overline{\mathbf{F}}_q$.

Podemos agora apresentar uma prova do resultado central desta seção (vide [16, Theorem 0.1]).

Teorema 4. *Seja* $\mathbf{F}_q$ *um corpo finito cuja cardinalidade* q *não é uma potência do primo 2. Seja* $f(X, Y) \in \mathbf{F}_q[X, Y]$ *um polinômio absolutamente irredutível de grau* d. *Suponha que* $f(X, Y)$ *não divida o polinômio* $(f_{XX} f_Y^2 - 2 f_{XY} f_X f_Y + f_{YY} f_X^2)$, *então vale a desigualdade*

$$\#C(\mathbf{F}_q) \leq \frac{1}{2} d \cdot (d + q - 1),$$

onde C *é a curva (projetiva) associada a* $f(X, Y)$.

Demonstração: Por simplicidade, nos restringiremos aqui ao caso afim; i.e., não trataremos com o polinômio homogêneo associado $F(X, Y, Z)$ e nem com a forma projetiva do teorema de Bezout (nesta versão projetiva, a Equação (4) é uma igualdade).

Segue da Proposição 3 que o polinômio $f(X, Y)$ também não divide $h(X, Y) = (X - X^q) f_X + (Y - Y^q) f_Y$; i.e., $f(X, Y)$ e $h(X, Y)$ não possuem fator comum de grau estritamente positivo.

Considere um ponto $(\mathbf{x}, \mathbf{y}) \in \mathbf{F}_q \times \mathbf{F}_q$ tal que $f(\mathbf{x}, \mathbf{y}) = 0$. Pela própria definição da função auxiliar $h(X, Y)$, temos também $h(\mathbf{x}, \mathbf{y}) = 0$. A equação

da reta tangente em $(\mathbf{x}, \mathbf{y})$ da curva associada ao polinômio $h(X, Y)$ é dada por (vide Equação (2))

$$(X - \mathbf{x})h_X(\mathbf{x}, \mathbf{y}) + (Y - \mathbf{y})h_Y(\mathbf{x}, \mathbf{y}) = 0.$$

Claramente,

$$h_X(X, Y) = (X - X^q)f_{XX} + f_X + (Y - Y^q)f_{XY}$$

e

$$h_Y(X, Y) = (X - X^q)f_{XY} + (Y - Y^q)f_{YY} + f_Y.$$

Sendo $(\mathbf{x}, \mathbf{y}) \in \mathbf{F}_q \times \mathbf{F}_q$, vemos que:

$$h_X(\mathbf{x}, \mathbf{y}) = f_X(\mathbf{x}, \mathbf{y}) \quad \text{e} \quad h_Y(\mathbf{x}, \mathbf{y}) = f_Y(\mathbf{x}, \mathbf{y}).$$

Assim, as retas tangentes neste ponto $(\mathbf{x}, \mathbf{y})$ das curvas determinadas por $f(X, Y)$ e por $h(X, Y)$ coincidem. Portanto, pela propriedade c) de multiplicidade de interseção, temos

$$\mathcal{I}(P; f, h) \geq 2 \ , \quad \forall P = (\mathbf{x}, \mathbf{y}) \in \mathbf{F}_q \times \mathbf{F}_q \text{ tal que } f(\mathbf{x}, \mathbf{y}) = 0.$$

Concluimos então que:

$$\#C_a(\mathbf{F}_q) = \#\{(\mathbf{x}, \mathbf{y}) \in \mathbf{F}_q \times \mathbf{F}_q \mid f(\mathbf{x}, \mathbf{y}) = 0\} \leq \frac{1}{2} \sum_P \mathcal{I}(P; f, h),$$

onde P percorre os pontos do plano $\overline{\mathbf{F}}_q \times \overline{\mathbf{F}}_q$.

Finalmente, aplicando o teorema de Bezout (Equação (4)), obtemos

$$\frac{1}{2} \sum_P \mathcal{I}(P; f, h) \leq \frac{1}{2}(\deg f) \cdot (\deg h) \leq \frac{1}{2} d \cdot (d + q - 1). \quad \square$$

No caso de curvas de gênero $g = 3$ isto é, curvas planas C não-singulares associadas a polinômios $f(X, Y)$ de grau $d = 4$, o Teorema 4 nos dá a seguinte cota:

$$\#C(\mathbf{F}_q) \quad \leq \quad 2q + 6.$$

O próximo exemplo nos oferece uma situação onde a cota é atingida.

Exemplo 3: (Curva de Fermat) Considere a curva plana projetiva C dada pelo polinômio $f(X, Y) \in \mathbf{F}_{13}[X, Y]$ abaixo:

$$f(X, Y) = \mathbf{w}^2 X^4 + Y^4 + \mathbf{w},$$

onde $\mathbf{w} \in \mathbf{F}_{13}$ é uma raiz terceira da unidade e ainda $\mathbf{w} \neq 1$.

É direta a verificação que o polinômio homogêneo associado $F(X, Y, Z)$ satisfaz a implicação **(1)** e, portanto, a curva associada a $f(X, Y)$ é não-singular e de gênero $g = 3$. Os pontos no infinito são da forma $(\mathbf{x} : \mathbf{y} : 0)$, onde

$$\mathbf{w}^2\mathbf{x}^4 + \mathbf{y}^4 = 0.$$

Assim, os pontos no infinito podem ser escritos na forma $(\mathbf{x} : 1 : 0)$, com

$$\mathbf{x}^4 = -\frac{1}{\mathbf{w}^2} = -\mathbf{w}.$$

Logo, num ponto do infinito $(\mathbf{x} : 1 : 0)$, temos

$$\mathbf{x}^{12} = -\mathbf{w}^3 = -1 \neq 1.$$

Isto mostra que não existem pontos do infinito da curva C no conjunto $C(\mathbf{F}_{13})$; equivalentemente, vale que:

$$\#C(\mathbf{F}_{13}) \quad = \quad \#C_a(\mathbf{F}_{13}).$$

Se $f(\mathbf{x},\mathbf{y}) = 0$ e $\mathbf{x} = 0$, obtemos

$$\mathbf{y}^4 = -\mathbf{w} \quad \text{e} \quad \mathbf{y}^{12} = -\mathbf{w}^3 = -1.$$

Se $f(\mathbf{x},\mathbf{y}) = 0$ e $\mathbf{y} = 0$, obtemos

$$\mathbf{x}^4 = -\frac{1}{\mathbf{w}} \quad \text{e} \quad \mathbf{x}^{12} = -\frac{1}{\mathbf{w}^3} = -1.$$

Assim, se $(\mathbf{x},\mathbf{y}) \in C_a(\mathbf{F}_{13})$, então $\mathbf{x} \neq 0 \quad \text{e} \quad \mathbf{y} \neq 0$.

Seja agora $H = \{1, \mathbf{w}, \mathbf{w}^2\}$ o único subgrupo de $(\mathbf{F}_{13})^*$ de ordem $|H| = 3$ e considere o homomorfismo φ sobrejetivo de grupos

$$\varphi\colon (\mathbf{F}_{13})^* \to H$$

$$\mathbf{x} \mapsto \mathbf{x}^4.$$

Claramente, como o núcleo de φ é o (único) subgrupo de $(\mathbf{F}_{13})^*$ de ordem igual a quatro, vemos que:

$$\#\varphi^{-1}(\mathbf{z}) = 4, \quad \forall \mathbf{z} \in H. \tag{5}$$

Seja $(\mathbf{x},\mathbf{y}) \in C_a(\mathbf{F}_{13})$. Como $\mathbf{x} \in \mathbf{F}_{13}$ e como $\mathbf{x} \neq 0$, temos então que $\mathbf{x}^4 \in H = \{1, \mathbf{w}, \mathbf{w}^2\}$.
Se $\mathbf{x}^4 = \mathbf{w}^2$, temos

$$f(\mathbf{x}, Y) = \mathbf{w}^4 + Y^4 + \mathbf{w} = Y^4 + 2\mathbf{w}.$$

Assim, não existem pontos $(\mathbf{x},\mathbf{y}) \in C_a(\mathbf{F}_{13})$ com $\mathbf{x}^4 = \mathbf{w}^2$ (utilize aqui a equação $\mathbf{w}^2 + \mathbf{w} + 1 = 0$ e que $\mathbf{y}^4 \in H$).

Se $\mathbf{x}^4 = 1$, obtemos

$$f(\mathbf{x}, Y) = \mathbf{w}^2 + Y^4 + \mathbf{w}.$$

Assim, os pontos $(\mathbf{x}, \mathbf{y}) \in C_a(\mathbf{F}_{13})$ com $\mathbf{x}^4 = 1$ satisfazem também $\mathbf{y}^4 = 1$.
Se $\mathbf{x}^4 = \mathbf{w}$, obtemos

$$f(\mathbf{x}, Y) = \mathbf{w}^3 + Y^4 + \mathbf{w} = 1 + Y^4 + \mathbf{w}.$$

Assim, os pontos $(\mathbf{x}, \mathbf{y}) \in C_a(\mathbf{F}_{13})$ com $\mathbf{x}^4 = \mathbf{w}$ satisfazem $\mathbf{y}^4 = \mathbf{w}^2$.

A conclusão é então que $C_a(\mathbf{F}_{13})$ é a união dos conjuntos C_1 e $C_{\mathbf{w}}$ abaixo:

$$C_1 = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}^4 = \mathbf{y}^4 = 1\} \quad \text{e} \quad C_{\mathbf{w}} = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}^4 = \mathbf{w} \text{ e } \mathbf{y}^4 = \mathbf{w}^2\}.$$

Como, utilizando a igualdade **(5)**, temos

$$\#C_1 = \#C_{\mathbf{w}} = 16,$$

concluimos $\#C(\mathbf{F}_{13}) = \#C_a(\mathbf{F}_{13}) = 32 = 2.13 + 6$.

Deixamos ao leitor a verificação de que o polinômio $f(X, Y)$ considerado neste Exemplo 3 não divide o polinômio abaixo:

$$f_{XX} f_Y^2 - 2 f_{XY} f_X f_Y + f_{YY} f_X^2 \ .$$

O exercício seguinte nos fornece um outro exemplo onde a cota no Teorema 4 é atingida.

Exercício. Considere a curva C associada a

$$f(X, Y) = X^4 + Y^4 - 2 \ \in \ \mathbf{F}_5[X, Y].$$

a) Mostre que $g(C) = 3$ e $\#C(\mathbf{F}_5) = 16 = 2 \cdot 5 + 6$.

b) Mostre que as hipóteses do Teorema 4 estão satisfeitas.

§5. O Método de Serre

Este método é conhecido como *fórmulas explícitas* (vide [13]). Será conveniente introduzir a notação seguinte: Para uma curva C definida sobre o corpo finito $\mathbf{F}_q$, denotamos

$$N_r \;=\; \#C(\mathbf{F}_{q^r}).$$

Na demonstração da Proposição 2 (desigualdade de Ihara) usamos a desigualdade óbvia $N_2 \geq N_1$; o método de Serre explora o fato que $N_r \geq N_1$, $\forall r \in \mathbf{N}$.

Estaremos interessados aqui em polinômios não-nulos $\Psi(t)$ a coeficientes reais positivos. Escrevemos

$$\Psi(t) = \sum_{r=1}^{m} c_r t^r \in \mathbf{R}[t], \tag{6}$$

onde c_r é um número real positivo; i.e., $c_r \geq 0$.
A um tal polinômio $\Psi(t)$, associamos a função racional $\mathbf{f}(t) \in \mathbf{R}(t)$ abaixo:

$$\mathbf{f}(t) = 1 + \Psi(t) + \Psi(t^{-1}).$$

Note que $\gamma = 0$ é o único polo afim desta função $\mathbf{f}(t)$. Note também que:

$$\mathbf{f}(\gamma) \in \mathbf{R}, \quad \forall \gamma \in \mathbf{C} \quad \text{com} \quad |\gamma| = 1.$$

Isto decorre do fato que para números complexos $\gamma \in \mathbf{C}$ com $|\gamma| = 1$, temos $\overline{\gamma} = \gamma^{-1}$, e da hipótese que o polinômio $\Psi(t)$ tem coeficientes reais.

Enunciamos agora o teorema (fórmulas explícitas) devido a J.-P. Serre.

Teorema 5. *Seja $\Psi(t) \in \mathbf{R}[t]$ um polinômio não-nulo a coeficientes reais positivos. Suponha que a função racional $\mathrm{f}(t)$ associada a $\Psi(t)$,*

$$\mathrm{f}(t) = 1 + \Psi(t) + \Psi(t^{-1}),$$

satisfaça: $\forall \gamma \in \mathbf{C}$ com $|\gamma| = 1$, temos $\mathrm{f}(\gamma) \geq 0$.

Então, para uma curva não-singular C definida sobre $\mathbf{F}_q$, vale

$$\#C(\mathbf{F}_q) \leq \frac{g}{\Psi(q^{-1/2})} + \frac{\Psi(q^{1/2})}{\Psi(q^{-1/2})} + 1,$$

onde g denota o gênero da curva C.

Demonstração: Observamos inicialmente que $\Psi(q^{-1/2}) > 0$, pois $\Psi(t)$ é um polinômio não-nulo a coeficientes reais positivos; i.e., usando a notação em (6) acima, temos que existe $r \in \{1, 2, \ldots, m\}$ tal que $c_r > 0$. De maneira análoga, vemos que $\Psi(q^{1/2}) > 0$.

A igualdade $(*_r)$ diz que:

$$N_r = 1 + q^r - \sum_{i=1}^{g} (\alpha_i^r + \overline{\alpha}_i^r),$$

onde ordenamos os números complexos $\alpha_1, \ldots, \alpha_{2g}$ como na demonstração do Teorema 1.

Multiplicando por $q^{-r/2}$, obtemos

$$N_r q^{-r/2} = q^{-r/2} + q^{r/2} - \sum_{i=1}^{g} \left[\left(\alpha_i q^{-1/2} \right)^r + \left(\overline{\alpha}_i q^{-1/2} \right)^r \right].$$

Denotando $\gamma_i = \alpha_i q^{-1/2}$, temos $|\gamma_i| = 1$ e

$$N_r q^{-r/2} = q^{-r/2} + q^{r/2} - \sum_{i=1}^{g} (\gamma_i^r + \gamma_i^{-r}). \qquad (7)$$

Multiplicando a igualdade (7) por c_r e somando estas equações, para $r = 1, 2, \ldots, m$, obtemos

$$\sum_{r=1}^{m} N_r c_r q^{-r/2} = \Psi(q^{-1/2}) + \Psi(q^{1/2}) + g - \sum_{i=1}^{g} \mathrm{f}(\gamma_i),$$

onde $\mathrm{f}(t)$ é a função racional associada a $\Psi(t)$.
Somando $N_1 \Psi(q^{-1/2})$ a ambos os lados, podemos reescrever a igualdade anterior na forma:

$$N_1 \Psi(q^{-1/2}) = \Psi(q^{-1/2}) + \Psi(q^{1/2}) + g - R,$$

onde $R = \sum_{i=1}^{g} \mathrm{f}(\gamma_i) + \sum_{r=1}^{m} (N_r - N_1) c_r q^{-r/2}$.

Por hipótese temos que $\mathrm{f}(\gamma_i) \geq 0$, $\forall i = 1, 2, \ldots, g$, e, para $r = 1, 2, \ldots, m$, vale que $c_r \geq 0$. Usando agora o fato (óbvio) que $N_r \geq N_1$, concluimos que $R \geq 0$. Consequentemente,

$$N_1 \Psi(q^{-1/2}) \leq \Psi(q^{-1/2}) + \Psi(q^{1/2}) + g. \quad \square$$

Denotamos por

$$N_q(g) = \max\{\#C(\mathbf{F}_q) \mid g(C) = g\}.$$

Isto é, $N_q(g)$ é o número máximo de pontos racionais sobre o corpo finito $\mathbf{F}_q$ que uma curva algébrica não-singular C de gênero igual a g pode ter. Uma curva C de gênero g é dita *otimal* se

$$\#C(\mathbf{F}_q) = N_q(g).$$

Claramente, as curvas consideradas nos Exemplos 1 e 2 são curvas otimais. No exemplo seguinte apresentamos outra curva otimal, utilizando agora o método das fórmulas explícitas. Este exemplo corresponde à curva de Deligne-Lusztig [2] associada ao grupo de Suzuki.

Exemplo 4. (Curva de Suzuki) Considere a curva projetiva C associada ao polinômio $f(X,Y)$ abaixo:

$$f(X,Y) = Y^q - Y - X^{q_0}(X^q - X) \in \mathbf{F}_q[X,Y],$$

onde $q = 2^{2e+1}$ e $q_0 = 2^e$ $(e \in \mathbf{N})$.

O polinômio $F(X,Y,Z)$ homogêneo associado é dado por

$$F(X,Y,Z) = Y^q Z^{q_0} - Y Z^{q+q_0-1} - X^{q_0+q} + X^{q_0+1} Z^{q-1}.$$

Assim, $(\mathbf{x} : \mathbf{y} : \mathbf{z}) = (0 : 1 : 0)$ é o único ponto no infinito da curva C. Também, ele é o único ponto singular de C; i.e., temos

$$F(\mathbf{x},\mathbf{y},\mathbf{z}) = F_X(\mathbf{x},\mathbf{y},\mathbf{z}) = F_Y(\mathbf{x},\mathbf{y},\mathbf{z}) = F_Z(\mathbf{x},\mathbf{y},\mathbf{z}) = 0$$

$$\Rightarrow \quad \mathbf{x} = \mathbf{y} = \mathbf{z} = 0 \quad \text{ou} \quad (\mathbf{x} : \mathbf{y} : \mathbf{z}) = (0 : 1 : 0).$$

É possível mostrar que o polinômio $f(X,Y)$ é absolutamente irredutível e que o gênero g da curva C é dado por

$$g = g(C) = q_0 \cdot (q-1) = \frac{q^{1/2}}{\sqrt{2}}(q-1). \tag{8}$$

Claramente, a curva afim associada C_a passa por todos os pontos $(\mathbf{x}, \mathbf{y})$ do plano finito $\mathbf{F}_q \times \mathbf{F}_q$. Somando o ponto do infinito, obtemos

$$\#C(\mathbf{F}_q) = q^2 + 1.$$

Seja $q = 2^{2e+1}$ e $q_0 = 2^e$, onde $e \in \mathbf{N}$. Vamos mostrar que a curva C deste Exemplo 4 é *otimal*. Para isso, mostramos abaixo (via fórmulas explícitas) que o número N_1 de pontos racionais sobre $\mathbf{F}_q$ de uma curva não-singular qualquer, de gênero g dado pela fórmula (8), satisfaz:

$$N_1 \leq 1 + q^2.$$

Considere o polinômio $\Psi(t) \in \mathbf{R}[t]$ dado por

$$\Psi(t) = \frac{1}{\sqrt{2}} \cdot t + \frac{1}{4} \cdot t^2. \tag{9}$$

Para um número complexo $\gamma \in \mathbf{C}$ com $|\gamma| = 1$, escrevemos $\gamma = e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta$ (onde $i^2 = -1$). A função racional $\mathrm{f}(t) = 1 + \Psi(t) + \Psi(t^{-1})$ calculada nestes valores $\gamma \in \mathbf{C}$, é então:

$$\mathrm{f}(\gamma) = 1 + \frac{1}{\sqrt{2}}e^{i\theta} + \frac{1}{4}e^{i2\theta} + \frac{1}{\sqrt{2}}e^{-i\theta} + \frac{1}{4}e^{-2i\theta} = 1 + \sqrt{2}\cos\theta + \frac{1}{2}\cos 2\theta.$$

Usando que $\cos 2\theta = 2\cos^2\theta - 1$, concluimos

$$\mathrm{f}(\gamma) = \left(\frac{1}{\sqrt{2}} + \cos\theta\right)^2 \geq 0.$$

Segue agora do Teorema 5, a desigualdade abaixo:

$$N_1 \;\leq\; \frac{g}{\Psi(q^{-1/2})} + \frac{\Psi(q^{1/2})}{\Psi(q^{-1/2})} + 1,$$

onde o gênero g é dado pela fórmula (8) e o polinômio $\Psi(t)$ é escolhido como em (9).

Basta então mostrar a igualdade

$$\frac{g}{\Psi(q^{-1/2})} + \frac{\Psi(q^{1/2})}{\Psi(q^{-1/2})} + 1 \;=\; q^2 + 1,$$

ou, equivalentemente, a igualdade

$$g + \Psi(q^{1/2}) \;=\; q^2 \cdot \Psi(q^{-1/2}).$$

Esta última igualdade segue das seguintes computações:

$$\begin{aligned} g + \Psi(q^{1/2}) &= \frac{q^{1/2}}{\sqrt{2}}(q-1) + \frac{q^{1/2}}{\sqrt{2}} + \frac{q}{4} \\ &= \frac{q^{3/2}}{\sqrt{2}} + \frac{q}{4} \\ &= q^2 \cdot \left(\frac{q^{-1/2}}{\sqrt{2}} + \frac{q^{-1}}{4} \right) \\ &= q^2 \cdot \Psi(q^{-1/2}). \end{aligned}$$

Exercício. Seja C a curva projetiva considerada no Exemplo 4. Utilizando as notações da demonstração do Teorema 5, mostre

a) $N_2 = N_1$ e $\mathrm{f}(\gamma_j) = 0$, $\forall j = 1, 2, \ldots, g$.

b) Escrevendo $\gamma_j = \cos\theta_j + i \operatorname{sen}\theta_j$ e utilizando que $\mathrm{f}(\gamma_j) = (\frac{1}{\sqrt{2}} + \cos\theta_j)^2$, conclua que

$$\gamma_j = \alpha_j \cdot q^{-1/2} = -\frac{1}{\sqrt{2}} \pm i \cdot \frac{1}{\sqrt{2}} \;.$$

Logo, temos $(\alpha_j + \overline{\alpha}_j) = -2 \cdot \frac{q^{1/2}}{\sqrt{2}} = -2q_0$.

c) Verifique agora que:

$$\prod_{j=1}^{2g}(1 - \alpha_j t) \;=\; (1 + 2q_0 t + qt^2)^g.$$

Observação: Escrevendo $\gamma = e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta$, para um número complexo γ com $|\gamma| = 1$ e, por abuso de linguagem, denotando $\mathbf{f}(\theta) = \mathbf{f}(e^{i\theta})$, temos que a função racional $\mathbf{f}(t)$ associada ao polinômio $\Psi(t)$ dado pela Equação (6) satisfaz:

$$\mathbf{f}(\theta) = 1 + \sum_{r=1}^{m} 2c_r \cos r\theta.$$

Uma maneira, muitas vezes conveniente, de escolher a função racional $\mathbf{f}(t)$ satisfazendo as hipóteses no Teorema 5, será tomando o polinômio trigonométrico $\mathbf{f}(\theta)$ na forma abaixo:

$$\mathbf{f}(\theta) = b^{-1} \cdot (1 + 2 \cdot \sum_{n\geq 1} b_n \cos n\theta)^2,$$

onde $b_n \in \mathbf{R}$, $b_n \geq 0$ e $b = 1 + 2 \cdot \sum_{n\geq 1} b_n^2$.

Para curvas algébricas C definidas sobre o corpo finito com dois elementos $\mathbf{F}_2$, a cota de Serre do Teorema 1 nos dá:

$$\#C(\mathbf{F}_2) \leq 2g + 3.$$

A escolha $b_1 = 1$; $b_2 = 0,7$; $b_3 = 0,2$ e $b_n = 0$, $\forall n \geq 4$, nos dá:

$$\#C(\mathbf{F}_2) \leq 0,83g + 5,35.$$

Para curvas C de gênero $g = 3$, temos então

$$\#C(\mathbf{F}_2) \leq 7,84 \quad \text{e, logo,} \quad \#C(\mathbf{F}_2) \leq 7.$$

A escolha $b_1 = 1$; $b_2 = 0,8$; $b_3 = 0,6$; $b_4 = 0,4$; $b_5 = 0,1$ e $b_n = 0$, $\forall n \geq 6$, nos dá:

$$\#C(\mathbf{F}_2) \leq 0,6272g + 9,562.$$

As cotas obtidas acima para $\#C(\mathbf{F}_2)$, usando o método das fórmulas explícitas, são atingidas para certos valores do gênero g. No entanto, para $g \geq 5$, é muito difícil determinar os polinômios que dão origem a tais curvas otimais. O exercício seguinte determina uma tal curva otimal sobre $\mathbf{F}_2$ no caso de gênero $g = 3$.

Exercício. Considere a curva projetiva C associada ao polinômio $f(X, Y) \in \mathbf{F}_2[X, Y]$ abaixo:

$$f(X, Y) = X^3Y + Y^3 + X + X^2Y^2 + Y^2 + X^2 + X^2Y + XY^2.$$

a) Mostre que a curva C é não-singular e conclua que esta curva tem gênero $g = 3$.

b) Mostre que a curva C tem 3 pontos no infinito e que

$$f(\mathbf{x}, \mathbf{y}) = 0, \quad \forall (\mathbf{x}, \mathbf{y}) \in \mathbf{F}_2 \times \mathbf{F}_2.$$

Conclua então que $\#C(\mathbf{F}_2) = 7$.

Cota superior para o número N de pontos racionais sobre $\mathbf{F}_2$ de curvas de gênero g

$g =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$N \leq$	5	6	7	8	9	10	11	11	12	13	14	15	15	16	17	18
$g =$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$N \leq$	18	19	20	21	21	22	23	23	24	25	25	26	27	27	28	29
$g =$	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$N \leq$	29	30	31	31	32	33	33	34	35	35	36	37	37	38	38	39
$g =$	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
$N \leq$	40	40	41	42	42	43	43	44	45	45	46	47	47	48	48	49
$g =$	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
$N \leq$	50	50	51	51	52	53	53	54	54	55	56	56	57	57	58	59
$g =$	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
$N \leq$	59	60	60	61	62	62	63	63	64	65	65	66	66	67	68	68
$g =$	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
$N \leq$	69	69	70	70	71	72	72	73	73	74	75	75	76	76	77	77
$g =$	113	114	115	116	117	118	119	120	...	...	...	...	...	...	...	...
$N \leq$	78	79	79	80	80	81	82	82	...	...	...	...	...	...	...	...

A tabela acima aparece em [14]. As cotas superiores foram obtidas usando "fórmulas explícitas" e os polinômios trigonométricos de Oesterlé.

§6. A Cota Assintótica de Drinfeld-Vladut

Denotando, como na seção anterior, por $N_q(g)$ o número máximo de pontos racionais sobre $\mathbf{F}_q$ de curvas algébricas não-singulares de gênero g, a desigualdade de Ihara (Proposição 2) afirma que:

$$\text{Se} \quad g > \frac{q - q^{1/2}}{2} \ , \quad \text{então} \quad N_q(g) < 1 + q + 2g\sqrt{q} \ .$$

Este resultado assegura que se o gênero g da curva é "grande" com relação a cardinalidade q do corpo finito, então o número de seus pontos racionais é estritamente menor que a cota superior de Weil. Fixando o corpo finito $\mathbf{F}_q$, queremos aqui estudar o comportamento de $N_q(g)$ quando o gênero g da curva vai aumentando. Para isto, introduzimos a notação seguinte:

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

Pelo Teorema 1 (Cota de Serre), temos

$$A(q) \leq [2\sqrt{q}].$$

Esta cota para $A(q)$ foi melhorada por Ihara [7], que obteve:

$$A(q) \leq \frac{1}{2}\left(\sqrt{8q+1} - 1\right).$$

O próximo teorema, devido a Drinfeld-Vladut [3], foi obtido através de refinamentos de idéias de Ihara. Ele nos dá a melhor cota superior atualmente conhecida para estimar $A(q)$.

Teorema 6. (Cota Assintótica) Com as notações acima, temos

$$A(q) \leq \sqrt{q} - 1.$$

Demonstração: Utilizaremos aqui também o método das fórmulas explícitas. Para cada $m \in \mathbf{N}$, consideramos o polinômio $\Psi_m(t)$:

$$\Psi_m(t) = \sum_{r=1}^{m} c_r t^r = \sum_{r=1}^{m} (1 - \frac{r}{m}) t^r.$$

Note que $\deg(\Psi_m) = (m-1)$. Para $t \neq 1$, podemos reescrever

$$\Psi_m(t) = \frac{t}{(t-1)^2} \cdot \left(\frac{t^m - 1}{m} + 1 - t \right). \qquad (10)$$

De fato, a igualdade **(10)** é equivalente a igualdade abaixo:

$$(t-1)^2 \cdot \sum_{r=1}^{m} (1 - \frac{r}{m}) t^{r-1} \;=\; \frac{1}{m} t^m - t + (1 - \frac{1}{m}).$$

Para verificar a validade desta última igualdade, escrevemos

$$(t^2 - 2t + 1) \cdot \sum_{r=1}^{m-1} (1 - \frac{r}{m}) t^{r-1} \;=\; \sum_{j=0}^{m} b_j t^j.$$

Claramente, temos que :

$$b_0 = (1 - \frac{1}{m}); \quad b_1 = (1 - \frac{2}{m}) - 2(1 - \frac{1}{m}) = -1;$$

$$b_{m-1} = (1 - \frac{m-2}{m}) - 2(1 - \frac{m-1}{m}) = 0 \quad \text{e} \quad b_m = 1 - \frac{m-1}{m} = \frac{1}{m}.$$

Então, para completar a prova da validade de **(10)**, basta verificar que $b_j = 0$ para cada j tal que $2 \leq j \leq m-2$. De fato, para $2 \leq j \leq m-2$, temos

$$b_j = (1 - \frac{j-1}{m}) - 2(1 - \frac{j}{m}) + (1 - \frac{j+1}{m}) = 0.$$

Agora, as seguintes igualdades podem ser facilmente verificadas:

$$\frac{t}{(t-1)^2} = \frac{t^{-1}}{(t^{-1}-1)^2} = \frac{-1}{(t-1)(t^{-1}-1)}.$$

Destas igualdades e de computações simples, segue

$$\frac{t}{(t-1)^2} \cdot \frac{t^m - 1}{m} + \frac{t^{-1}}{(t^{-1}-1)^2} \cdot \frac{t^{-m}-1}{m} = \frac{2 - (t^m + t^{-m})}{m(t-1)(t^{-1}-1)}.$$

Usando **(10)**, obtemos

$$\begin{aligned} \mathbf{f}_m(t) &= 1 + \Psi_m(t) + \Psi_m(t^{-1}) \\ &= 1 + \frac{t}{(t-1)^2}(\frac{t^m-1}{m} + 1 - t) + \frac{t^{-1}}{(t^{-1}-1)^2}(\frac{t^{-m}-1}{m} + 1 - t^{-1}) \\ &= \frac{t}{(t-1)^2} \cdot \frac{t^m - 1}{m} + \frac{t^{-1}}{(t^{-1}-1)^2} \cdot \frac{t^{-m}-1}{m} \end{aligned}$$

Obtemos então a seguinte expressão para $\mathbf{f}_m(t)$:

$$\mathbf{f}_m(t) = \frac{2 - (t^m + t^{-m})}{m(t-1)(t^{-1}-1)} \qquad \textbf{(11)}$$

Para números complexos $\gamma \neq 1$ com $|\gamma| = 1$, temos que $(\gamma - 1) \cdot (\gamma^{-1} - 1)$ é um número real estritamente positivo; isto decorre da igualdade $\gamma^{-1} = \overline{\gamma}$. Assim, o valor de $\mathbf{f}_m(t)$ no ponto $t = \gamma$ (i.e., $\mathbf{f}_m(\gamma)$) está bem definido e

$$\mathbf{f}_m(\gamma) = \frac{2 - (\gamma^m + \gamma^{-m})}{m(\gamma - 1)(\gamma^{-1} - 1)} = \frac{2 - (\gamma^m + \overline{\gamma}^m)}{m\,|\gamma - 1|^2}$$

Claramente, temos $(\gamma^m + \overline{\gamma}^m) \in \mathbf{R}$. Sendo $|\gamma| = 1$, obtemos $|\gamma^m| = 1$ e então

$$|\gamma^m + \overline{\gamma}^m| \leq |\gamma^m| + |\overline{\gamma}^m| = 1 + 1 = 2.$$

Assim, o número real $(\gamma^m + \gamma^{-m})$ está no intervalo fechado $[-2, 2]$; isto é,

$$-2 \leq (\gamma^m + \gamma^{-m}) \leq 2.$$

Concluimos que a função racional $\mathbf{f}_m(t)$ dada pela Expressão **(11)** satisfaz:

$$\mathbf{f}_m(\gamma) \geq 0, \quad \forall \gamma \in \mathbf{C} \quad \text{com} \quad |\gamma| = 1.$$

Podemos agora aplicar o Teorema 5 obtendo então, para cada $m \in \mathbf{N}$, a desigualdade:

$$\frac{N_q(g)}{g} \leq \frac{1}{\Psi_m(q^{-1/2})} + \frac{1}{g}\left(\frac{\Psi_m(q^{1/2})}{\Psi_m(q^{-1/2})} + 1\right). \qquad \textbf{(12)}$$

Da Expressão **(10)**, vemos que:

$$\lim_{m \to \infty} \Psi_m(q^{-1/2}) = (\sqrt{q} - 1)^{-1}.$$

Assim para qualquer número real $\varepsilon > 0$, podemos escolher um número natural $n = n(\varepsilon)$ tal que

$$\Psi_n(q^{-1/2})^{-1} \quad < \quad (\sqrt{q} - 1) + \varepsilon/2.$$

Fixado o número natural $n = n(\varepsilon)$, para cada valor de $\varepsilon > 0$, podemos escolher $g_0 = g_0(\varepsilon)$ tal que

$$\frac{1}{g}\left(\frac{\Psi_n(q^{1/2})}{\Psi_n(q^{-1/2})} + 1\right) < \frac{\varepsilon}{2} \ , \quad \forall g \geq g_0 \ .$$

Utilizando a desigualdade **(12)**, concluimos: para cada valor de $\varepsilon > 0$, existe $g_0 = g_0(\varepsilon)$ tal que

$$\frac{N_q(g)}{g} \quad < \quad (\sqrt{q} - 1) + \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = (\sqrt{q} - 1) + \varepsilon, \quad \forall g \geq g_0 \ .$$

Isto mostra que:

$$\limsup_{g \to \infty} \frac{N_q(g)}{g} \quad \leq \quad (\sqrt{q} - 1). \qquad \square$$

Observação: Quando a cardinalidade q é um quadrado, Ihara [7] demonstra a igualdade

$$A(q) = \sqrt{q} - 1.$$

Esta demonstração utiliza técnicas sofisticadas da Geometria Algébrica, particulamente a Teoria de Curvas Modulares. Recentemente (vide [5]), foi conseguida uma prova mais elementar para esta igualdade (q sendo um quadrado).

Quando a cardinalidade q não é um quadrado, não é conhecido até agora o valor exato de $A(q)$. No entanto, utilizando a Teoria de Corpos de Classes, J.-P. Serre demonstra que

$$A(q) > 0, \quad \forall q.$$

A igualdade $A(q) = \sqrt{q} - 1$ é básica para a prova do famoso teorema de Tsfasman, Vladut e Zink [17] que assegura a existência de sequências de *códigos lineares* sobre $\mathbf{F}_q$, para q quadrado e $q \geq 49$, que são melhores que a cota de Gilbert-Varshamov.

REFERÊNCIAS

[1] Artin. E. - *Quadratische Körper im Gebiet der höheren Kongruenzen*, Math. Z. **19** (1924), 153–246.

[2] Deligne, P. e Lusztig, G. - *Representations of Reductive Groups over Finite Fields*, Ann. Math. **103** (1976), 103–161.

[3] Drinfeld, V.G. e Vladut, S.G. - *Number of Points of an Algebraic Curve*, Func. Anal. **17** (1983), 53–54.

[4] Fulton, W. - *Algebraic Curves*, Benjamin, New York, (1969).

[5] Garcia, A. e Stichtenoth, H. - *A Tower of Artin-Schreier Extensions of Function Fields Attaining the Drinfeld-Vladut Bound*, to appear in Inventiones Math.

[6] Hasse, H. - *Zur Theorie der abstrakten elliptischen Funktionenkörper*, J. Reine Angew. Math. **175** (1936), 69-88 e 193–208.

[7] Ihara, Y. - *Some Remarks on the Number of Rational Points of Algebraic Curves over Finite Fields*, J. Fac. Sci. Tokyo **28** (1981), 721–724.

[8] Lidl, R. e Niederreiter, H. - *Finite Fields* (Encyclopedia of Math. and its Appl., vol **20**), Addison-Wesley, Reading-Mass. (1983).

[9] Mattuck, A. e Tate, J. - *On the inequality of Castelnuovo-Severi*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 295–299.

[10] Rück, H.G. e Stichtenoth, H. – *A Characterization of Hermitian Function Fields over Finite Fields*, to appear in J. Reine Angew. Math.

[11] Schmidt, W.M. - *Equations over Finite Fields: An Elementary Approach*, Lect. Notes in Math. **536** (1976), Springer-Verlag, Berlin-Heidelberg-New York.

[12] Serre, J.-P. - *Résumé des cours 1983–1984*, in "Annuaire du Collège de France" (1984), 79–83.

[13] Serre, J.-P. - *Sur le nombre des points rationelles d'une courbe algébrique sur un corps fini*, C.R. Acad. Sci. Paris **296** (1983), 397–402.

[14] Serre, J.-P. - *Rational Points on Curves over Finite Fields*, Notes from Lectures given at Harvard Univ. (Sept-Dec 1985).

[15] Stichtenoth, H. - *Algebraic Function Fields and Codes*, (Universitext) Springer-Verlag, Berlin-Heidelberg (1993).

[16] Stöhr, K.-O. e Voloch, J.F. - *Weierstrass Points and Curves over Finite Fields*, Proc. London Math. Soc. (3), **52** (1986), 1–19.

[17] Tsfasman, M.A., Vladut, S.G. e Zink, T. - *Modular Curves, Shimura Curves and Goppa Codes, better than the Varshamov-Gilbert Bound*, Math. Nachr. **109** (1982), 21–28.

[18] Weil, A. - *Courbes algébriques et variétés abéliennes*, Herman, Paris, (1971).

Impresso na Gráfica do
impa
pelo Sistema Xerox /1090