Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Solubilidade p-ádica de Pares de Formas Aditivas via Somas Exponenciais

por

Thiago Porto de Almeida Freitas

Brasília
2006

À minha família

Agradecimentos

- À Deus pela presença em minha vida;

- À minha mãe, Izabel, e ao meu irmão, Herculano, pelo apoio e por sempre me receberem de braços e corações abertos quando voltava para casa;

- Ao meu pai, Iran, e ao meu irmão, Ian, que apesar da distância estiveram incentivando e torcendo por esta conquista;

- Aos meus familiares por sempre acreditarem na minha capacidade;

- Ao prof. Hemar Godinho pela orientação, ensinamentos e confiança;

- Às professoras, Aline e Edméia, por aceitarem a participar da banca e pelas correções e sugestões que enriqueceram o trabalho;

- Ao Paulo Henrique e ao Euro pela ajuda oferecida nos momentos de dúvidas;

- Aos amigos, Élida, Porfírio e André Luiz, por terem me acolhido durante o primeiro semestre de mestrado e por todos os conselhos;

- Aos professores do Departamento de Matemática da UnB por terem contribuído na minha formação acadêmica, especialmente: à Profa. Cátia e ao Prof. José Alfredo pelos ensinamentos que ultrapassaram o conhecimento acadêmico;

- Aos professores do Departamento de Matemática do Campus de Catalão - UFG, que semearam a vontade de fazer o mestrado, de modo especial, aos professores: André, Carlos Alberto, Élida, Márcio, Martinha, Paulinho e Plínio.

- Às amigas, Ana Paula, Elcimar e Michele, pelas palavras de incentivo e carinho;

- Aos amigos, Bianka, Fágner, Evander e Walter, pela amizade verdadeira e pela confiança;

- Aos amigos, Adriana, Aline, Anderson, Daniel, Débora, Fabiana, Fernando, Jhone, Juliana e Sandra pelas palavras de apoio e incentivo;

- Às amigas, Anyelle, Flávia e Karise, por terem a paciência de me ensinar alguns passos de forró, sem reclamar das pisadas;

- Aos colegas do Bloco K da Colina, de forma especial, ao Adão e ao Gustavo que tive a oportunidade de partilhar bons momentos no apartamento 102;

- A todos, colegas e amigos, que tive a oportunidade de conhecer durante o mestrado, por todos os momentos que vivenciamos;

- Ao CNPq e a Capes pelo apoio financeiro.

“ Se eu insisto em repetir para mim mesmo que não posso fazer determinada coisa, é possível que acabe me tornando incapaz de fazê-la. Ao contrário, se tenho a convicção de que posso fazê-la, certamente adquirirei a capacidade de realizá-la, ainda que não a tenha no início do processo. ”

Ghandi

Listas de Símbolos

$\mathbb{F}_q$	Corpo finito com q elementos
$mdc(a, b)$	Máximo divisor comum entre a e b
χ, Ψ, ...	Caráter multiplicativo
χ_0	Caráter trivial ou Caráter principal
$\tau_a(\chi)$, $\tau(\chi)$	Soma Gaussiana
f, g, h, ...	Polinômios
Φ	Conjunto de polinômios mônicos sobre $\mathbb{F}_q$
Φ_k	Conjunto de polinômios mônicos de grau k sobre $\mathbb{F}_q$
$R(f, g)$	Resultante de f e g
$N_{E/\mathbb{F}_q}(\alpha)$	Norma de $\alpha \in E$ sobre $\mathbb{F}_q$
$\#A$	Cardinalidade do conjunto A

Resumo

Nesta dissertação estudamos alguns resultados sobre solubilidade p-ádica de pares de formas aditivas. Iniciamos com a teoria de somas exponenciais e o Teorema de Hasse-Weil. E concluímos com as teorias de p-normalização, coloração de variáveis e o Teorema de Meir.

Palavras-chaves : Somas Exponenciais, Teorema de Hasse-Weil, p-normalização, Coloração de Variáveis, Teorema de Meir.

Abstract

In this dissertation we study some results about p-adic solubility of pairs of additive forms. Our starting point is the theory of exponential sums and Hasse-Weil's Theorem. And we conclude this work presenting the theories of p-normalization, coloured variables and the Meir's Theorem.

Keywords : Exponential Sums, Hasse-Weil's theorem, p-normalization, coloured variables, Meir's theorem.

Sumário

Introdução

O matemático E. Artin, em 1920, conjecturou que *" todo polinômio homogêneo de grau k em n variáveis possui zeros p-ádicos não triviais desde que $n \geq k^2+1$"*. Na tentativa de verificar a validade desta conjectura, alguns matemáticos obtiveram sucesso para valores particulares de k, como por exemplo: Hasse, em 1924, verificou a validade quando $k = 2$ e, de maneira independente, foi verificada a validade para $k = 3$, pelos matemáticos Lewis e Demyanov. Por outro lado, o matemático Terjanian exibiu um polinômio homogêneo de grau 4 com 18 variáveis que não possui zeros 2-ádicos e assim, verificando que a conjectura de Artin é falsa. Tais exemplos podem ser encontrados em [10].

Em 1965, os matemáticos Ax e Kochen publicaram o seguinte resultado: *"para todo inteiro k existe um conjunto finito de primos $A = A(k)$ tal que para todo primo $p \notin A$, uma forma de grau k em $n \geq k^2 + 1$ variáveis sobre os números p-ádicos sempre possui zeros p-ádicos não-triviais"*, ver [4]. Esse resultado garante que a conjectura é verdadeira a menos de um conjunto finito de primos. Dessa forma, dizemos que a Conjectura de Artin é "quase" correta.

No caso de formas aditivas, isto é, formas do tipo $a_1x_1^k + \cdots + a_nx_n^k$, a conjectura foi verificada por Davenport e Lewis, ou seja, eles provaram que *"toda forma aditiva de grau k, com coeficientes inteiros, em $n \geq k^2+1$ variávies sempre possui zeros p-ádicos"*, ver [7]. De certo modo, a conjectura de Artin pode ser generalizada, isto é, no caso de um sistema de r formas aditivas de grau k com coeficientes inteiros racionais é esperado que exista solução p-ádica não-trivial, para todo primo p, desde que $n \geq rk^2+1$. Sendo assim, para o caso de sistema de duas formas aditivas, é esperado que exista solução p-ádica não-trivial, para todo primo p, desde que o número de variáveis presente no sistema seja no mínimo $2k^2 + 1$.

Os primeiros estudos sobre sistema de pares de formas aditivas foram feitos por Davenport e Lewis. Para tal, eles introduziram uma nova técnica, conhecida como p-normalização, que impulsionou os estudos desta área.

Com base nesta nova técnica, em 1988, Atkinson e Cook mostraram que *"todo sistema de duas formas aditivas de grau k com coeficientes inteiros racionais possui zero p-ádico não-trivial para todo primo p, $p > k^6$, desde que $n > 4k$"*, onde a condição sobre o número de variáveis é a melhor possível. Esse resultado foi generalizado em 1992, por Atkinson, Brüdern e Cook, que provaram que: *"todo sistema de r formas aditivas de grau k e n variáveis possui solução p-ádica não-trivial para todo primo p, $p > k^{2r+2}$, desde que $n > 2rk$"*.

Em 1997, o matemático Meir diminuiu a restrição sobre o conjunto de primos, dado por Atkinson e Cook, onde se verificava a existência de solução p-ádica não-trivial para um sistema de duas formas aditivas, isto é, sob as mesmas condições sobre o número de variáveis, a solubilidade do sistema é garantida para todo primo p, tal que $p > 3k^4$.

O objetivo desta dissertação é apresentar o resultado mencionado devido a Meir e todos os principais pré-requisitos necessários para entendê-lo. E para isto a dividimos em dois capítulos.

No Capítulo 1 discutimos a Teoria de somas exponenciais e recorremos a Teoria de Corpos Finitos, mais especificamente ao Teorema de Hasse - Weil, para obtermos uma estimativa sobre soma de caracteres multiplicativos.

No Capítulo 2 apresentamos duas técnicas, p-normalização e coloração de variáveis, que são utilizadas na demonstração do Teorema de Meir. Discutimos a relação do número mínimo de variáveis presentes no sistema e a existência de solução não-trivial. Além disso, temos a demonstração do resultado devido a Meir.

Capítulo 1

Somas Exponenciais e o Teorema de Hasse - Weil

1.1 Somas Exponenciais

Nesta seção discutimos sobre somas exponenciais, que consiste em um método bastante utilizado em problemas de natureza aditiva. Através deste método obtemos estimativas que são bastante utilizadas na demostração do teorema a ser apresentado no próximo capítulo, que se deve a Meir.

Definição 1.1. *Seja g uma raíz primitiva módulo p, isto é, g é um gerador de $\mathbb{F}_p^*$, onde p é um número primo. Sejam $d = mdc(k, p-1)$ e ϵ uma raíz primitiva d-ésima da unidade. Para $s = 0, 1, \ldots, d-1$ definimos*

$$\chi_s(x) = \begin{cases} \epsilon^{ts} & se \quad x = g^t \\ 0 & se \quad x = 0 \end{cases}.$$

Tal função é chamada de caráter multiplicativo módulo p. Em particular, quando $s = 0$ denominamos χ_0 como sendo o caráter principal ou caráter trivial.

Lema 1.2. *$\chi_s(1) = 1$ para $s = 0, 1, \ldots, d-1$.*

Demonstração: De fato, como $1 = g^0$, segue pela Definição 1.1 que $\chi_s(1) = \epsilon^{0 \cdot s} = 1$, para $s = 0, 1, \ldots, d-1$. ∎

Lema 1.3. *χ_s é uma função multiplicativa, isto é, para todo x e y em $\mathbb{F}_p$ temos que $\chi_s(xy) = \chi_s(x)\chi_s(y)$.*

Demonstração: Se $x = 0$ ou $y = 0$ a demonstração é imediata. Sendo assim, suponhamos que x e y sejam ambos não nulos. Como g é raíz primitiva, segue que existem inteiros positivos, m e n, tais que, $x = g^m$ e $y = g^n$ e conseqüentemente $xy = g^m g^n = g^{m+n}$. Daí pela Definição 1.1 obtemos

$$\chi_s(xy) = \epsilon^{(m+n)s} = \epsilon^{ms}\epsilon^{ns} = \chi_s(x)\chi_s(y).$$

■

Lema 1.4. *Sejam a e b tais que $a \equiv b \pmod{p}$, então $\chi_s(a) = \chi_s(b)$.*

Demonstração: Como g é raíz primitiva existem u e v tais que $a = g^u$ e $b = g^v$. Logo, pela hipótese, obtemos $g^u \equiv g^v \pmod{p}$, ou seja, $g^{u-v} \equiv 1 \pmod{p}$. Utilizando novamente o fato de g ser uma raíz primitiva temos que $u - v \equiv 0 \pmod{p-1}$, isto é, $u \equiv v \pmod{p-1}$.

Mas $d = mdc(r, p-1)$, logo, $d \mid (p-1)$. Dessa maneira $u \equiv v \pmod{d}$ e daí segue imediatamente pela Definição 1.1 que $\chi_s(a) = \chi_s(b)$. ■

Lema 1.5. *Temos $\sum_{x=0}^{p-1} \chi_s(x) = 0$, desde que $s \neq 0$.*

Demonstração: Como $s \neq 0$, isto é, χ_s não é o caráter principal, então existe a tal que $\chi_s(a) \neq 1$ com $mdc(a, p) = 1$. Logo

$$\chi_s(a)\sum_{x=0}^{p-1}\chi_s(x) = \sum_{x=0}^{p-1}\chi_s(a)\chi_s(x) = \sum_{x=0}^{p-1}\chi_s(ax) = \sum_{x=0}^{p-1}\chi_s(x),$$

onde a segunda e a terceira igualdade acima são justificadas pelos Lemas 1.3 e 1.4, respectivamente.

Assim obtemos $(\chi_s(a) - 1)\sum_{x=0}^{p-1}\chi_s(x) = 0$, de onde concluímos que $\sum_{x=0}^{p-1}\chi_s(x) = 0$, visto que $\chi_s(a) \neq 1$. ■

Lema 1.6. *Temos $\sum_{s=0}^{d-1}\chi_s(x) = \begin{cases} d & se \quad d \mid t \\ 0 & se \quad d \nmid t \end{cases}$ onde $x = g^t$ e $d = mdc(k, p-1)$.*

Demonstração: Seja $x = g^t$. Suponhamos que $d \mid t$, isto é, existe $t_1 \in \mathbb{Z}$ tal que $t = t_1 d$. Pela Definição 1.1 segue que $\chi_s(x) = \epsilon^{ts} = \epsilon^{t_1 ds} = 1$. E assim

$$\sum_{s=0}^{d-1} \chi_s(x) = \sum_{s=0}^{d-1} 1 = d.$$

Por outro lado se $d \nmid t$, então

$$\sum_{s=0}^{d-1} \chi_s(x) = \sum_{s=0}^{d-1} \epsilon^{ts} = 1 + \epsilon^t + (\epsilon^t)^2 + \cdots + (\epsilon^t)^{d-1} = \frac{1 - (\epsilon^t)^d}{1 - \epsilon^t} = 0.$$

■

Definição 1.7. *Sejam p um número primo e $k \in \mathbb{N}$. Definimos $T(b) = \sum_{y=0}^{p-1} \xi^{by^k}$, onde ξ é uma raíz primitiva p-ésima da unidade.*

A partir de agora estamos interessados em entender a soma apresentada na Definição 1.7 quando tivermos $mdc(b, p) = 1$.

Para cada x, tal que $x \in \{0, 1, \ldots, p-1\}$, seja $m(x)$ o número de soluções da congruência $y^k \equiv x \pmod{p}$.

Dessa maneira, seja g uma raíz primitiva módulo p, então fixado x, $x \neq 0$, existe t tal que $x = g^t$. Fazendo $y = g^u$, concluímos que resolver $y^k \equiv x \pmod{p}$ é o mesmo que resolvermos em u a congruência $g^{uk} \equiv g^t \pmod{p}$.

Pelo fato de g ser uma raíz primitiva módulo p temos que $g^{uk-t} \equiv 1 \pmod{p}$, e assim, $uk - t \equiv 0 \pmod{p-1}$, ou seja, $uk \equiv t \pmod{p-1}$.

Uma condição necessária e suficiente para que $uk \equiv t \pmod{p-1}$ admita solução é que $mdc(k, p-1) \mid t$. E no caso de admitir solução temos que possui exatamente $mdc(k, p-1)$ soluções. Tal resultado pode ser encontrado em [11].

Portanto, para $x \neq 0$, obtemos que $m(x) = \begin{cases} mdc(k, p-1) & se \quad d \mid t \\ 0 & se \quad d \nmid t \end{cases}$, onde $x = g^t$. Assim, para $x \neq 0$, segue pelo Lema 1.6 que

$$m(x) = \sum_{s=0}^{d-1} \chi_s(x). \tag{1.1}$$

Daí pela relação (1.1) obtemos

$$T(b) = \sum_{y=0}^{p-1} \xi^{by^k} = \sum_{x=0}^{p-1} m(x)\xi^{bx} = m(0) + \sum_{x=1}^{p-1}\sum_{s=0}^{d-1} \chi_s(x)\xi^{bx}.$$

E como $m(0) = 1$ temos que

$$T(b) = 1 + \sum_{x=1}^{p-1}\sum_{s=0}^{d-1} \chi_s(x)\xi^{bx}. \tag{1.2}$$

Definição 1.8. *Seja χ um caráter multiplicativo módulo p e $a \in \mathbb{N}$. Definimos a Soma Gaussiana como sendo $\tau_a(\chi) = \sum_{x=0}^{p-1} \chi(x)\xi^{ax}$.*

Observação 1.9. *No caso de a ser igual a 1, denotaremos a Soma Gaussiana neste caso como sendo $\tau(\chi)$.*

Lema 1.10. *Se $mdc(a,p) = 1$ e χ é um caráter não-trivial, então $\chi(a)\tau_a(\chi) = \tau(\chi)$.*

Demonstração: Pela Definição 1.8 segue que

$$\chi(a)\tau_a(\chi) = \chi(a)\sum_{x=0}^{p-1} \chi(x)\xi^{ax} = \sum_{x=0}^{p-1} \chi(a)\chi(x)\xi^{ax},$$

e agora, pelos Lemas 1.3 e 1.4, obtemos que

$$\chi(a)\tau_a(\chi) = \sum_{x=0}^{p-1} \chi(ax)\xi^{ax} = \sum_{x=0}^{p-1} \chi(x)\xi^{x} = \tau(\chi).$$

■

Lema 1.11. *Temos* $\sum_{x=0}^{p-1} \xi^{ax} = \begin{cases} p & se \quad a \equiv 0 \pmod{p} \\ 0 & c.c. \end{cases}$, *onde ξ é uma raíz primitiva p-ésima da unidade.*

Demonstração: Suponhamos que $a \equiv 0 \pmod{p}$, logo existe $a_1 \in \mathbb{Z}$ tal que $a = pa_1$. Daí,

$$\sum_{x=0}^{p-1} \xi^{ax} = \sum_{x=0}^{p-1} (\xi^p)^{a_1 x} = \sum_{x=0}^{p-1} 1 = p.$$

Por outro lado, se $a \not\equiv 0 \pmod{p}$, então

$$\sum_{x=0}^{p-1} \xi^{ax} = 1 + \xi^a + (\xi^a)^2 + \cdots + (\xi^a)^{p-1} = \frac{1 - (\xi^a)^p}{1 - \xi^a} = 0.$$

■

Lema 1.12. *Se* $mdc(b,p) = 1$, *então* $T(b) = \sum_{s=1}^{d-1} \chi_s(b)\tau(\overline{\chi}_s)$, *onde* χ *não é o caráter trivial e* $d = mdc(k, p-1)$ *e* $\overline{\chi}_s$ *é o caráter conjugado de* χ_s.

Demonstração: Da relação (1.2) obtemos que

$$T(b) = 1 + \sum_{x=1}^{p-1} \xi^{bx} + \sum_{x=1}^{p-1}\sum_{s=1}^{d-1} \chi_s(x)\xi^{bx} = \sum_{x=0}^{p-1} \xi^{bx} + \sum_{x=1}^{p-1}\sum_{s=1}^{d-1} \chi_s(x)\xi^{bx}.$$

Como $mdc(b,p) = 1$ segue pelo Lema 1.11 que $\sum_{x=0}^{p-1} \xi^{bx} = 0$ e assim

$$T(b) = \sum_{x=1}^{p-1}\sum_{s=1}^{d-1} \chi_s(x)\xi^{bx} = \sum_{s=1}^{d-1}\sum_{x=0}^{p-1} \chi_s(x)\xi^{bx} = \sum_{s=1}^{d-1} \tau_b(\chi_s). \tag{1.3}$$

Aplicando o Lema 1.10 na relação (1.3) obtemos que

$$T(b) = \sum_{s=1}^{d-1} (\chi_s(b))^{-1}\tau(\chi_s) = \sum_{s=1}^{d-1} \overline{\chi_s(b)}\tau(\chi_s),$$

onde a última igualdade se deve ao fato que $\mid \chi_s(b) \mid = 1$, ou seja, $\chi_s(b)\overline{\chi_s(b)} = 1$, isto é, $(\chi_s(b))^{-1} = \overline{\chi_s(b)}$. O que conclui a demonstração. ∎

Teorema 1.13. *Se* χ *um caráter não-trivial e* $a \in \mathbb{N}$ *tal que* $mdc(a,p) = 1$, *então* $\mid \tau_a(\chi) \mid = \sqrt{p}$.

Demonstração: Temos por hipótese que $mdc(a,p) = 1$ e χ é diferente do caráter trivial. Dessa maneira $\mid \chi(a) \mid = 1$ e conseqüentemente obtemos pelo Lema 1.10 que $\chi(a)\tau_a(\chi) = \tau(\chi)$, isto é, $\mid \tau_a(\chi) \mid = \mid \tau(\chi) \mid$.

Pela última igualdade é suficiente mostrar que $\mid \tau(\chi) \mid^2 = p$. Como $\mid \chi(a) \mid = 1$, temos

$$\overline{\chi(a)} = (\chi(a))^{-1}. \tag{1.4}$$

Novamente pelo Lema 1.10 obtemos

$$\tau_a(\chi) = (\chi(a))^{-1}\tau(\chi). \tag{1.5}$$

De (1.4) e (1.5) segue

$$\overline{\tau_a(\chi)} = \overline{(\chi(a))^{-1}}\ \ \overline{\tau(\chi)} = \chi(a)\overline{\tau(\chi)}. \tag{1.6}$$

Através de (1.5) e (1.6) obtemos

$$\tau_a(\chi)\overline{\tau_a(\chi)} = \tau(\chi)\overline{\tau(\chi)} = \mid \tau(\chi) \mid^2 . \tag{1.7}$$

Pela relação (1.7) segue

$$\sum_{a=0}^{p-1} \tau_a(\chi)\overline{\tau_a(\chi)} = \tau_0(\chi)\overline{\tau_0(\chi)} + \sum_{a=1}^{p-1} \mid \tau(\chi) \mid^2 .$$

Mas, pela Definição 1.8 segue que $\tau_0(\chi) = \sum_{x=0}^{p-1} \chi(x) = 0$, onde a última igualdade é devida ao Lema 1.5, pois χ não é o caráter trivial.

Assim

$$\sum_{a=0}^{p-1} \tau_a(\chi)\overline{\tau_a(\chi)} \ = \ \sum_{a=1}^{p-1} \mid \tau(\chi) \mid^2 \ = \ \mid \tau(\chi) \mid^2 \sum_{a=1}^{p-1} 1 \ = \ (p-1) \mid \tau(\chi) \mid^2 . \tag{1.8}$$

Por outro lado, novamente pela Definição 1.8 temos que

$$\tau_a(\chi)\overline{\tau_a(\chi)} = \left(\sum_{x=0}^{p-1} \chi(x)\xi^{ax}\right)\left(\sum_{y=0}^{p-1} \overline{\chi(y)}\xi^{-ay}\right) = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \chi(x)\overline{\chi(y)}\xi^{a(x-y)}.$$

Dessa maneira,

$$\sum_{a=0}^{p-1} \tau_a(\chi)\overline{\tau_a(\chi)} = \sum_{a=0}^{p-1}\left(\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \chi(x)\overline{\chi(y)}\xi^{a(x-y)}\right) = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \chi(x)\overline{\chi(y)}\sum_{a=0}^{p-1}\xi^{a(x-y)}. \tag{1.9}$$

Pelo Lema 1.11 concluímos que

$$\sum_{a=0}^{p-1} \xi^{a(x-y)} = \begin{cases} p & se \quad x \equiv y \pmod{p} \\ 0 & c.c. \end{cases} . \tag{1.10}$$

De (1.9) e (1.10) segue que

$$\sum_{a=0}^{p-1} \tau_a(\chi)\overline{\tau_a(\chi)} = p\sum_{x=0}^{p-1} \chi(x)\overline{\chi(x)} = p\sum_{x=1}^{p-1} \chi(x)\overline{\chi(x)} = p\sum_{x=1}^{p-1} 1 = p(p-1). \tag{1.11}$$

Comparando as relações (1.8) e (1.11) obtemos $(p-1) \mid \tau(\chi) \mid^2 = p(p-1)$, ou seja, $\mid \tau(\chi) \mid^2 = p$, e assim concluindo a demonstração. ∎

Lema 1.14. *Se* $T(b)=\sum_{x=0}^{p-1}\xi^{bx^k}$ *com* $mdc(b,p)=1$ *e* $k \mid (p-1)$, *então* $\mid T(b) \mid \leq (k-1)\sqrt{p}$.

Demonstração: Temos pela relação (1.3) obtida na demonstração do Lema 1.12 que $T(b)=\sum_{s=1}^{k-1}\tau_b(\chi_s)$. Daí

$$\mid T(b) \mid \;=\; \left|\sum_{s=1}^{k-1}\tau_b(\chi_s)\right| \;\leq\; \sum_{s=1}^{k-1} \mid \tau_b(\chi_s) \mid . \tag{1.12}$$

Mas sabemos pelo Teorema 1.13 que $\mid \tau_b(\chi_s) \mid = \sqrt{p}$, logo em (1.12) obtemos que

$$\mid T(b) \mid \;\leq\; \sum_{s=1}^{k-1}\sqrt{p} \;=\; \sqrt{p}\sum_{s=1}^{k-1}1 \;=\; \sqrt{p}(k-1).$$

O que conclui a demonstração. ∎

Lema 1.15. *Se* $T(b)=\sum_{x=0}^{p-1}\xi^{bx^k}$ *com* $mdc(b,p)=1$ *e* $k \mid (p-1)$, *então* $\sum_{b=1}^{p-1} \mid T(b) \mid^2 = p(p-1)(k-1)$.

Demonstração: Por hipótese segue que

$$\sum_{b=0}^{p-1} \mid T(b) \mid^2 = \sum_{b=0}^{p-1} T(b)\overline{T(b)} = \sum_{b=0}^{p-1}\left(\sum_{x=0}^{p-1}\xi^{bx^k}\right)\left(\sum_{y=0}^{p-1}\xi^{-by^k}\right) = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{b=0}^{p-1}\xi^{b(x^k-y^k)}. \tag{1.13}$$

Pelo Lema 1.11 temos que

$$\sum_{b=0}^{p-1}\xi^{b(x^k-y^k)} = \begin{cases} p, & \text{se} \quad x^k-y^k \equiv 0 \pmod{p} \\ 0, & \text{c.c.} \end{cases}. \tag{1.14}$$

Assim de (1.14) em (1.13) obtemos que

$$\sum_{b=0}^{p-1} \mid T(b) \mid^2 = pM, \tag{1.15}$$

onde M é o número de soluções da equação $x^k-y^k \equiv 0 \pmod{p}$.

Se $x = 0$, então a congruência $y^k \equiv 0 \pmod{p}$ tem apenas uma solução, a saber $y = 0$. Se $x = a \neq 0$, então a congruência $y^k \equiv a^k \pmod{p}$ tem exatamente $mdc(k, p-1)$ soluções, ou seja, possui exatamente k soluções, pois $k \mid (p-1)$. Logo

$$M = 1 + (p-1)k. \tag{1.16}$$

Por outro lado,

$$\sum_{b=0}^{p-1} \mid T(b) \mid^2 \;=\; \mid T(0) \mid^2 + \sum_{b=1}^{p-1} \mid T(b) \mid^2 \;=\; p^2 + \sum_{b=1}^{p-1} \mid T(b) \mid^2, \tag{1.17}$$

visto que $T(0) = p$.

Pelas relações (1.15), (1.16) e (1.17) obtemos

$$p^2 + \sum_{b=1}^{p-1} \mid T(b) \mid^2 = p(1 + (p-1)k),$$

ou seja,

$$\sum_{b=1}^{p-1} \mid T(b) \mid^2 = p(1 + (p-1)k - p).$$

E portanto $\sum_{b=1}^{p-1} \mid T(b) \mid^2 = p(p-1)(k-1)$. ∎

Lema 1.16. *Para n inteiro positivo seja $S_n = \sum_{b=1}^{p-1} \mid T(b) \mid^n$, onde $T(b) = \sum_{x=0}^{p-1} \xi^{bx^k}$ e $k \mid (p-1)$. Então $S_n \leq (k-1)^{n-1} p^{\frac{n}{2}+1}$.*

Demonstração: Temos que $S_n = \sum_{b=1}^{p-1} \mid T(b) \mid^n \;=\; \sum_{b=1}^{p-1} \mid T(b) \mid^{n-2} \mid T(b) \mid^2$. Assim, pelo Lema 1.14, obtemos que

$$S_n \leq \sum_{b=1}^{p-1} (\sqrt{p}\;\; (k-1))^{n-2} \mid T(b) \mid^2 \;=\; p^{\frac{n-2}{2}} (k-1)^{n-2} \sum_{b=1}^{p-1} \mid T(b) \mid^2 .$$

Em seguida, aplicando o Lema 1.15 temos

$$S_n \leq p^{\frac{n-2}{2}} (k-1)^{n-2} p(p-1)(k-1) = p^{\frac{n}{2}} (p-1)(k-1)^{n-1},$$

ou seja,

$$S_n \leq p^{\frac{n}{2}+1}(k-1)^{n-1}$$

afinal, $p-1 \leq p$. ∎

Lema 1.17. *Sejam a, b e λ números reais tais que $a \geq 0$, $b \geq 0$ e $0 < \lambda < 1$. Então $a^{\lambda}b^{1-\lambda} \leq \lambda a + (1-\lambda)b$.*

Demonstração: Se $b = 0$, então a desigualdade é facilmente verificada, devido as condições sobre a e λ. Suponhamos que $b \neq 0$. Seja $f(t) = t^{\lambda} - \lambda t$, para todo $t \geq 0$. Derivando f em relação a t, obtemos que $f'(t) = \lambda(t^{\lambda-1} - 1)$. Utilizando ferramentas de cálculo, obtemos que 1 é o único ponto crítico de f e tal ponto é ponto de máximo de f. Logo

$$f(t) \leq f(1), \text{ para } t \geq 0,$$

ou seja,

$$t^{\lambda} \leq \lambda t + (1-\lambda), \text{ para } t \geq 0. \tag{1.18}$$

Como $b \neq 0$, segue da relação (1.18) para $t = \dfrac{a}{b}$ que

$$\left(\frac{a}{b}\right)^{\lambda} \leq \lambda\left(\frac{a}{b}\right) + (1-\lambda),$$

isto é,

$$a^{\lambda}b^{1-\lambda} \leq \lambda a + (1-\lambda)b.$$

∎

Lema 1.18 (Desigualdade de Hölder). *Sejam x_i e y_i números complexos, então $\displaystyle\sum_{i=1}^{n} |x_i y_i| \leq \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p} \left(\sum_{i=1}^{n} |y_i|^q\right)^{1/q}$, onde p e q são números reais tais que $p, q > 1$ e $\dfrac{1}{p} + \dfrac{1}{q} = 1$.*

Demonstração: Consideremos $A = \left(\displaystyle\sum_{i=1}^{n} |x_i|^p\right)^{1/p}$ e $B = \left(\displaystyle\sum_{i=1}^{n} |y_i|^q\right)^{1/q}$. Se $A = 0$ ou $B = 0$, então a desigualdade é facilmente verificada. Sendo assim, suponhamos que $A \neq 0$ e $B \neq 0$.

Consideremos $a = \left(\frac{|x_i|}{A}\right)^p$, $b = \left(\frac{|y_i|}{B}\right)^q$ e $\lambda = \frac{1}{p}$. Observemos que $a \geq 0$, $b \geq 0$ e $0 < \lambda < 1$, logo pelo Lema 1.17 temos

$$\left[\left(\frac{|x_i|}{A}\right)^p\right]^{1/p}\left[\left(\frac{|y_i|}{B}\right)^q\right]^{1-1/p} \leq \frac{1}{p}\left(\frac{|x_i|}{A}\right)^p + \left(1-\frac{1}{p}\right)\left(\frac{|y_i|}{B}\right)^q,$$

ou seja,

$$\frac{|x_i|}{A}\frac{|y_i|}{B} \leq \frac{1}{p}\left(\frac{|x_i|}{A}\right)^p + \frac{1}{q}\left(\frac{|y_i|}{B}\right)^q,$$

visto que $\frac{1}{p} + \frac{1}{q} = 1$.

Daí,

$$\frac{\sum_{i=1}^{n}|x_iy_i|}{AB} \leq \frac{1}{p}\frac{\sum_{i=1}^{n}|x_i|^p}{A^p} + \frac{1}{q}\frac{\sum_{i=1}^{n}|y_i|^q}{B^q} = \frac{1}{p}+\frac{1}{q} = 1,$$

ou seja,

$$\sum_{i=1}^{n}|x_iy_i| \leq AB = \left(\sum_{i=1}^{n}|x_i|^p\right)^{1/p}\left(\sum_{i=1}^{n}|y_i|^q\right)^{1/q},$$

provando a desigualdade desejada. ∎

Lema 1.19. *Sejam $x_{1_i}, \ldots, x_{k_i}$ números complexos e k inteiro positivo, tal que $k \geq 2$. Então $\sum_{i=1}^{n}|x_{1_i}x_{2_i}\ldots x_{k_i}| \leq \left(\sum_{i=1}^{n}|x_{1_i}|^{j_1}\right)^{1/j_1}\ldots\left(\sum_{i=1}^{n}|x_{k_i}|^{j_k}\right)^{1/j_k}$, onde $j_1, \ldots, j_k$ são números reais maiores do que 1 e $\frac{1}{j_1}+\cdots+\frac{1}{j_k} = 1$.*

Demonstração: A demonstração segue por indução sobre k. O caso $k = 2$ é o Lema 1.18. ∎

Lema 1.20. *Sejam k inteiro positivo e p um número primo tais que $k \mid (p-1)$ e $p > k^4$. Se $abc \not\equiv 0 \pmod{p}$, então a congruência $ax^k+by^k+cz^k \equiv d \pmod{p}$ tem uma solução (x, y, z) tal que $xyz \not\equiv 0 \pmod{p}$.*

Demonstração: Considere N o número de soluções da congruência $ax^k + by^k + cz^k \equiv d \pmod{p}$. Pelo Lema 1.11

$$\sum_{u=0}^{p-1}\xi^{u(ax^k+by^k+cz^k-d)} = \begin{cases} p, & se \quad ax^k+by^k+cz^k \equiv d \pmod{p} \\ 0, & c.c. \end{cases}. \tag{1.19}$$

Assim, de (1.19) podemos concluir que N é

$$N = \frac{1}{p}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{z=0}^{p-1}\sum_{u=0}^{p-1}\xi^{u(ax^k+by^k+cz^k-d)}. \tag{1.20}$$

Pela Definição 1.7 obtemos em (1.20) que

$$Np = \sum_{x,y,z,u=0}^{p-1}\xi^{aux^k}\xi^{buy^k}\xi^{cuz^k}\xi^{-du} = \sum_{u=0}^{p-1}\left[\left(\sum_{x=0}^{p-1}\xi^{aux^k}\right)\left(\sum_{y=0}^{p-1}\xi^{buy^k}\right)\left(\sum_{z=0}^{p-1}\xi^{cuz^k}\right)\xi^{-du}\right],$$

isto é,

$$Np = \sum_{u=0}^{p-1}T(au)T(bu)T(cu)\xi^{-du} = p^3 + \sum_{u=1}^{p-1}T(au)T(bu)T(cu)\xi^{-du},$$

visto que $T(0) = p$.

Logo

$$\mid Np - p^3 \mid = \left|\sum_{u=1}^{p-1}T(au)T(bu)T(cu)\xi^{-du}\right| \leq \sum_{u=1}^{p-1}\mid T(au)T(bu)T(cu)\xi^{-du}\mid,$$

ou seja,

$$\mid Np - p^3 \mid \leq \sum_{u=1}^{p-1}\mid T(au)T(bu)T(cu)\mid. \tag{1.21}$$

Utilizando a Desigualdade de Hölder no lado direito da relação (1.21) obtemos que

$$\mid Np - p^3 \mid \leq \left\{\sum_{u=1}^{p-1}\mid T(au)\mid^3\sum_{u=1}^{p-1}\mid T(bu)\mid^3\sum_{u=1}^{p-1}\mid T(cu)\mid^3\right\}^{\frac{1}{3}}. \tag{1.22}$$

Por hipótese temos que $abc \not\equiv 0 \pmod{p}$. Assim quando u percorre os valores $1, 2, \ldots, p-1$ temos que au, bu e cu percorrem estes mesmos valores módulo p. Então

$$\sum_{u=1}^{p-1}\mid T(au)\mid^3 = \sum_{u=1}^{p-1}\mid T(bu)\mid^3 = \sum_{u=1}^{p-1}\mid T(cu)\mid^3 = \sum_{u=1}^{p-1}\mid T(u)\mid^3. \tag{1.23}$$

Dessa maneira, segue através das relações (1.22) e (1.23) que

$$\mid Np - p^3 \mid \leq \left\{\left(\sum_{u=1}^{p-1}\mid T(u)\mid^3\right)^3\right\}^{\frac{1}{3}} = \sum_{u=1}^{p-1}\mid T(u)\mid^3. \tag{1.24}$$

Observe que temos do lado direito de (1.24) o que definimos no Lema 1.16 como sendo S_3. E aplicando a estimativa de S_3 obtida no Lema 1.16 em (1.24) obtemos

$$\mid Np - p^3 \mid \ \leq \ (k-1)^2 p^{\frac{5}{2}}. \tag{1.25}$$

De (1.25) temos que

$$p^3 - (k-1)^2 p^{\frac{5}{2}} \ \leq \ Np \ \leq \ p^3 + (k-1)^2 p^{\frac{5}{2}}.$$

Dividindo ambos os membros da desigualdade acima por p obtemos

$$p^2 - (k-1)^2 p^{\frac{3}{2}} \ \leq \ N \ \leq \ p^2 + (k-1)^2 p^{\frac{3}{2}}. \tag{1.26}$$

Agora estimamos o número de soluções de $ax^k + by^k + cz^k \equiv d \pmod{p}$ tal que $xyz \equiv 0 \pmod{p}$.

Se $x \equiv 0 \pmod{p}$, temos que $by^k + cz^k \equiv d \pmod{p}$. Esta equação possui no máximo k soluções para cada valor de y fixado, pois sabemos pela hipótese que $k \mid (p-1)$. Como existem p valores possíveis para y, obtemos que a equação possui no máximo kp soluções.

Repetindo tal processo para $y \equiv 0 \pmod{p}$ e $z \equiv 0 \pmod{p}$, chegamos a conclusão de que a congruência $ax^k + by^k + cz^k \equiv d \pmod{p}$ possui no máximo $3kp$ soluções com $xyz \equiv 0 \pmod{p}$.

Logo para verificarmos se a congruência $ax^k + by^k + cz^k \equiv d \pmod{p}$ possui solução com $xyz \not\equiv 0 \pmod{p}$ é suficiente mostrar que

$$p^2 - (k-1)^2 p^{\frac{3}{2}} > 3kp, \tag{1.27}$$

onde o lado esquerdo de (1.27) é a cota inferior para N obtida em (1.26).

A relação (1.27) é verdadeira. De fato, por hipótese sabemos que $p > k^4$. Logo $p^{\frac{1}{2}} > k^2$ e assim $-3kp^{-\frac{1}{2}} > -3k^{-1}$.

Das desigualdades acima obtemos

$$p^{\frac{1}{2}} - 3kp^{-\frac{1}{2}} > k^2 - \frac{3}{k}. \tag{1.28}$$

Mas $2k^2 - k > 3$ para todo $k \geq 2$, isto é,

$$2k - 1 > \frac{3}{k}. \tag{1.29}$$

De (1.28) e (1.29) obtemos que

$$p^{\frac{1}{2}} - 3kp^{-\frac{1}{2}} > k^2 - 2k + 1 = (k-1)^2.$$

Multiplicando a desigualdade acima por $p^{\frac{3}{2}}$ obtemos a relação desejada, isto é,

$$p^2 - 3kp > (k-1)^2 p^{\frac{3}{2}},$$

ou melhor,

$$p^2 - (k-1)^2 p^{\frac{3}{2}} > 3kp.$$

■

1.2 Teorema de Hasse - Weil

Esta seção será devotada à demonstração de um resultado que nos fornece uma estimativa para determinada soma de caracteres multiplicativos. Tal resultado é devido a Hasse e Weil. A demonstração é feita tendo como suporte a Teoria de Corpos Finitos, e dessa forma, alguns conceitos (corpos finitos e suas propriedades, norma, caráter multiplicativo, polinômio característico e outros) desta teoria não serão tratados neste momento, mas podem ser encontrados em [6, p. 1-11] e [12]. No final da seção obtemos, como conseqüência do Teorema de Hasse - Weil, uma estimativa que será utilizada para demonstrar o Teorema de I. D. Meir, a ser apresentado no próximo capítulo.

Consideremos λ, $\lambda : \Phi \longrightarrow D$, uma aplicação onde Φ é o conjunto de polinômios mônicos sobre $\mathbb{F}_q$ e $D = \{z \in \mathbb{C}; \mid z \mid \leq 1\}$, tal que $\lambda(1) = 1$ e λ é uma função multiplicativa. Definimos a seguinte série

$$L(z) = \sum_{k=0}^{\infty} \left(\sum_{g \in \Phi_k} \lambda(g) \right) z^k, \tag{1.30}$$

onde Φ_k é o conjunto de polinômios mônicos de grau k sobre $\mathbb{F}_q$.

Observemos que a série $L(z)$ converge absolutamente para $\mid z \mid < \frac{1}{q}$.

Como $\mathbb{F}_q[x]$ é um domínio de fatoração única, utilizando o fato de λ ser multiplicativa, obtemos

$$\begin{aligned} L(z) &= \sum_{k=0}^{\infty}\left(\sum_{g\in\Phi_k}\lambda(g)\right)z^k = \sum_{g\in\Phi}\lambda(g)z^{grau(g)} \\ &= \prod_f\left(1+\lambda(f)z^{grau(f)}+\lambda(f^2)z^{grau(f^2)}+\lambda(f^3)z^{grau(f^3)}+\dots\right) \\ &= \prod_f\left(1+\lambda(f)z^{grau(f)}+\lambda(f)^2z^{2grau(f)}+\lambda(f)^3z^{3grau(f)}+\dots\right) \\ &= \prod_f\left(1+\lambda(f)z^{grau(f)}+(\lambda(f)z^{grau(f)})^2+(\lambda(f)z^{grau(f)})^3+\dots\right) \\ &= \prod_f\left(\frac{1}{1-\lambda(f)z^{grau(f)}}\right), \end{aligned}$$

onde f são os polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$.

Dessa forma,

$$log(L(z)) = log\left(\prod_f\left(\frac{1}{1-\lambda(f)z^{grau(f)}}\right)\right) = \sum_f log\left(\frac{1}{1-\lambda(f)z^{grau(f)}}\right),$$

isto é,

$$log(L(z)) = \sum_f -log(1-\lambda(f)z^{grau(f)}),$$

onde a soma é feita sobre todos os polinômios mônicos e irredutíveis com coeficientes em $\mathbb{F}_q$.

Daí

$$\begin{aligned} z\frac{d}{dz}log(L(z)) &= z\frac{d}{dz}\sum_f -log(1-\lambda(f)z^{grau(f)}) &&= z\sum_f -\frac{d}{dz}log(1-\lambda(f)z^{grau(f)}) \\ &= z\sum_f\frac{\lambda(f)grau(f)z^{grau(f)-1}}{1-\lambda(f)z^{grau(f)}} &&= \sum_f\frac{\lambda(f)grau(f)z^{grau(f)}}{1-\lambda(f)z^{grau(f)}}. \end{aligned}$$

E assim,

$$\begin{aligned} z\frac{d}{dz}log(L(z)) &= \sum_f\lambda(f)grau(f)z^{grau(f)}\left(1+\lambda(f)z^{grau(f)}+\lambda(f)^2z^{2grau(f)}+\dots\right) \\ &= \sum_f grau(f)\left(\lambda(f)z^{grau(f)}+\lambda(f)^2z^{2grau(f)}+\lambda(f)^3z^{3grau(f)}+\dots\right). \end{aligned}$$

Agrupando os termos acima segundo a potência de z, obtemos

$$z\frac{d}{dz}log(L(z)) = \sum_{s=1}^{\infty}L_sz^s, \tag{1.31}$$

onde

$$L_s = \sum_f grau(f)\lambda(f)^{s/grau(f)}, \tag{1.32}$$

tal que a soma é feita sobre os polinômios mônicos e irredutíveis em $\mathbb{F}_q$ cujo grau é divisor de s.

Agora, suponhamos que exista t, inteiro positivo, tal que $\sum_{g\in\Phi_k} \lambda(g) = 0$, para todo $k > t$. Logo $L(z) = \sum_{k=0}^{t} \left(\sum_{g\in\Phi_k} \lambda(g) \right) z^k$. Observamos que $L(z)$ é um polinômio de grau t. Em $\mathbb{C}$ podemos fatorar $L(z)$ da seguinte forma:

$$L(z) = (1-\omega_1 z)\dots(1-\omega_t z),$$

com $\omega_1, \dots, \omega_t \in \mathbb{C}$.

Daí,

$$\begin{aligned}
z\frac{d}{dz}log(L(z)) &= z\frac{d}{dz}log\left(\prod_{m=1}^{t}(1-\omega_m z)\right) &&= z\frac{d}{dz}\sum_{m=1}^{t} log(1-\omega_m z)\\
&= z\sum_{m=1}^{t}\frac{d}{dz}log(1-\omega_m z) &&= z\sum_{m=1}^{t}\frac{-\omega_m}{1-\omega_m z}\\
&= -\sum_{m=1}^{t} z\omega_m \frac{1}{1-\omega_m z} &&= -\sum_{m=1}^{t} z\omega_m(1+\omega_m z+\omega_m^2 z^2+\dots)\\
&= -\sum_{m=1}^{t} z\omega_m \sum_{j=0}^{\infty}\omega_m^j z^j &&= -\sum_{m=1}^{t}\sum_{j=0}^{\infty}\omega_m^{j+1} z^{j+1}\\
& && = -\sum_{j=0}^{\infty}\left(\sum_{m=1}^{t}\omega_m^{j+1}\right) z^{j+1}.
\end{aligned}$$

Fazendo $s = j+1$, obtemos que

$$z\frac{d}{dz}log(L(z)) = -\sum_{s=1}^{\infty}\left(\sum_{m=1}^{t}\omega_m^s\right) z^s. \tag{1.33}$$

Comparando as relações (1.31) e (1.33) temos que

$$L_s = -\omega_1^s - \dots - \omega_t^s. \tag{1.34}$$

Definição 1.21. *Sejam* $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ *e* $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$ *pertencentes a* $\mathbb{F}_q[x]$*, polinômios de grau* n *e* m*, respectivamente. Definimos a resultante de* f *e* g*,* $R(f,g)$*, como*

$$R(f,g) = det \begin{bmatrix} a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & a_2 & \dots & a_n \\ b_0 & b_1 & b_2 & \dots & b_m & 0 & \dots & 0 \\ 0 & b_0 & b_1 & b_2 & \dots & b_m & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & \dots & b_0 & b_1 & \dots & b_m \end{bmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} m \ \ linhas \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} n \ \ linhas \end{matrix} \tag{1.35}$$

Observemos que a matriz acima tem ordem $m+n$ e decorre imediatamente da definição que $R(f,g) \in \mathbb{F}_q$.

Quando conhecemos as raízes de f, ou seja, $f(x) = a_0(x-\alpha_1)\dots(x-\alpha_n)$ pode-se mostrar que a resultante de f e g neste caso é dada por

$$R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i), \tag{1.36}$$

onde m é o grau de g, ver [12].

Lema 1.22. *Nas condições da Definição 1.21, temos que* $R(f,g) = (-1)^{mn}R(g,f)$*.*

Demonstração: De fato, basta observarmos que o determinante de uma matriz muda de sinal quando permutamos uma linha. Como queremos permutar m linhas n vezes segue o resultado desejado. ∎

Seja Ψ um caráter multiplicativo de $\mathbb{F}_q$ de ordem m, com $m > 1$. Seja f um polinômio mônico de grau positivo e que não é uma m-ésima potência. A partir de agora, consideraremos a seguinte aplicação

$$\lambda : \Phi \longrightarrow D, \text{ tal que, } \lambda(1) = 1 \text{ e } \lambda(g) = \Psi(R(g,f)), \tag{1.37}$$

onde $R(g,f)$ é a resultante de g e f.

Observemos que para $g \in \Phi_k$, se $g(x) = (x-\alpha_1)\dots(x-\alpha_k)$, segue pela relação (1.36) que

$$R(g,f) = f(\alpha_1)\dots f(\alpha_k). \tag{1.38}$$

Substituindo a relação (1.38) na definição de λ obtemos que

$$\lambda(g) = \Psi(R(g,f)) = \Psi(f(\alpha_1)\dots f(\alpha_n)). \tag{1.39}$$

A função λ definida acima possui duas propriedades importantes. Tais propriedades são a essência dos próximos dois lemas a serem discutidos.

Lema 1.23. *A aplicação λ é multiplicativa, isto é, $\lambda(gh) = \lambda(g)\lambda(h)$, para todo $g, h \in \Phi$.*

Demonstração: De fato, sejam $g, h \in \Phi$ tais que $g(x) = (x-\beta_1)\dots(x-\beta_r)$ e $h(x) = (x-\beta_{r+1})\dots(x-\beta_{r+s})$, nos respectivos corpos de decomposição sobre $\mathbb{F}_q$. Assim, segue que

$$(gh)(x) = (x-\beta_1)\dots(x-\beta_r)(x-\beta_{r+1})\dots(x-\beta_{r+s}).$$

Logo, pela definição de λ e por (1.38) temos que

$$\lambda(gh) = \Psi(R(gh,f)) = \Psi(f(\beta_1)\dots f(\beta_r)f(\beta_{r+1})\dots f(\beta_{r+s})).$$

Como Ψ é um caráter multiplicativo

$$\lambda(gh) = \Psi(f(\beta_1)\dots f(\beta_r))\Psi(f(\beta_{r+1})\dots f(\beta_{r+s})) = R(g,f)R(h,f) = \lambda(g)\lambda(h),$$

o que conclui a demonstração. ∎

Observação 1.24. ***(Teorema Chinês do Resto)*** *Seja F um corpo. Sejam $f_1, \dots, f_r \in F[x]$ polinômios não-nulos que são coprimos dois a dois. Sejam $h_1, \dots, h_r \in F[x]$ polinômios arbitrários. Então a congruência $g \equiv h_i \pmod{f_i}$, para $i = 1, \dots, r$ tem solução e tal solução é unicamente determinada módulo $f_1 \dots f_r$, ver [12].*

Lema 1.25. *Seja λ a aplicação definida em (1.37). Seja d o número de raízes distintas de f em seu corpo de decomposição sobre $\mathbb{F}_q$. Logo, $\sum_{g\in\Phi_k} \lambda(g) = 0$ para $k \geq d$.*

Demonstração: Escrevamos f da seguinte forma, $f = f_1^{e_1}\dots f_r^{e_r}$, onde $f_1, \dots, f_r$ são polinômios distintos, mônicos e irredutíveis sobre $\mathbb{F}_q$. Suponhamos que f_j tenha grau d_j.

Como f_j é irredutível de grau d_j, segue que f_j possui d_j raízes distintas em uma extensão E_j de $\mathbb{F}_q$, com $[E_j : \mathbb{F}_q] = d_j$.

Sendo assim,

$$R(f,g) = \prod_{(1)} g(y) = \prod_{j=1}^{r} \prod_{(2)} g(y_j) = \prod_{j=1}^{r} \left(\prod_{(3)} g(\overline{y_j}) \right)^{e_j} = \prod_{j=1}^{r} (R(f_j, g))^{e_j}, \tag{1.40}$$

onde em (1.40) temos que (1), (2) e (3) significam que o produto é feito sobre todas as raízes de f, $f_j^{e_j}$ e f_j, respectivamente.

Dessa maneira, pelo Lema 1.22 temos que

$$R(g,f) = (-1)^{kn} R(f,g) = (-1)^{kn} R(f_1, g)^{e_1} \dots R(f_r, g)^{e_r}. \tag{1.41}$$

Seja β_j uma raíz de f_j. Então todas as raízes de f_j são dadas pelos conjugados de β_j e assim pela relação (1.36) temos

$$R(f_j, g) = g(\beta_j) g(\beta_j^q) \dots g(\beta_j^{q^{d_j - 1}}). \tag{1.42}$$

Como g é um polinômio com coeficientes em $\mathbb{F}_q$ e sabemos que $x^q = x$ para todo $x \in \mathbb{F}_q$, segue de (1.42) que

$$R(f_j, g) = g(\beta_j)(g(\beta_j))^q \dots (g(\beta_j))^{q^{d_j - 1}} = N_{E_j/\mathbb{F}_q}(g(\beta_j)). \tag{1.43}$$

Da relação (1.41) obtemos

$$\lambda(g) = \Psi(R(g,f)) = \Psi((-1)^{kn} R(f_1, g)^{e_1} \dots R(f_r, g)^{e_r}),$$

e como Ψ é multiplicativo segue que

$$\lambda(g) = \Psi((-1)^{kn}) \Psi(R(f_1, g))^{e_1} \dots \Psi(R(f_r, g))^{e_r},$$

donde concluímos pela relação (1.43) que

$$\lambda(g) = \Psi((-1)^{kn}) \Psi^{e_1}(N_{E_1/\mathbb{F}_q}(g(\beta_1))) \dots \Psi^{e_r}(N_{E_r/\mathbb{F}_q}(g(\beta_r))).$$

Fazendo $\varepsilon_k = \Psi((-1)^{kn})$ e $\tau_j = \Psi^{e_j} \circ N_{E_j/\mathbb{F}_q}$, obtemos

$$\lambda(g) = \varepsilon_k \tau_1(g(\beta_1)) \dots \tau_r(g(\beta_r)). \tag{1.44}$$

Defina

$$\begin{array}{rccc} \Gamma: & \Phi_k & \longrightarrow & E_1 \times \cdots \times E_r \\ & g & \longmapsto & (g(\beta_1), \ldots, g(\beta_r)) \end{array}.$$

Agora, gostaríamos de saber quantos polinômios g em Φ_k existem, com $k \geq d$, onde d é o número de raízes distintas de f, tais que $\Gamma(g) = (v_1, \ldots, v_r)$.

Seja $(v_1, \ldots, v_r) \in E_1 \times \cdots \times E_r$. Como $E_i = \mathbb{F}_q[\beta_i]$, existe $h_i \in \mathbb{F}_q[x]$ tal que $v_i = h_i(\beta_i)$.

Temos que $\Gamma(g) = (v_1, \ldots, v_r)$ se, e somente se, g é solução do sistema de congruências $g \equiv h_i \pmod{f_i}$, para $i = 1, \ldots, r$. De fato, suponhamos que $\Gamma(g) = (v_1, \ldots, v_r)$. Logo $g(\beta_i) = v_i$, para $i = 1, \ldots, r$. Por outro lado, sabemos que $v_i = h_i(\beta_i)$, para $i = 1, \ldots, r$. Sendo assim, obtemos que $(g - h_i)(\beta_i) = 0$, para $i = 1, \ldots, r$. Como f_i é o polinômio minimal de β_i, segue que $f_i \mid (g - h_i)$, isto é, $g \equiv h_i \pmod{f_i}$, para $i = 1, \ldots, r$. Reciprocamente, basta observarmos que $h_i(\beta_i) = v_i$ e $f_i(\beta_i) = 0$ para $i = 1, \ldots, r$.

Daí concluímos, utilizando o Teorema Chinês do Resto, que

$$g \equiv G \pmod{f_1 \ldots f_r}, \text{ com } grau(G) < grau(f_1 \ldots f_r) = d_1 + \cdots + d_r = d.$$

Assim, $g = f_1 \ldots f_r F + G$, para algum polinômio mônico $F \in \mathbb{F}_q[x]$ com $grau(F) = k - d$, visto que $grau(g) = k$. Dessa maneira, para sabermos quantos polinômios g existem, basta contarmos quantos polinômios F existem tais que $g = f_1 \ldots f_r F + G$. Visto que F é um polinômio mônico de grau $k - d$ com coeficientes em $\mathbb{F}_q$, segue que existem q^{k-d} polinômios. Logo, obtemos para $k \geq d$ a partir da relação (1.44) que

$$\sum_{g \in \Phi_k} \lambda(g) = \sum_{g \in \Phi_k} \varepsilon_k \tau_1(g(\beta_1)) \ldots \tau_r(g(\beta_r)) = \varepsilon_k q^{k-d} \sum_{\substack{v_1, \ldots, v_r \\ v_i \in E_i}} \tau_1(v_1) \ldots \tau_r(v_r),$$

ou seja,

$$\sum_{g \in \Phi_k} \lambda(g) = \varepsilon_k q^{k-d} \left(\sum_{v_1 \in E_1} \tau_1(v_1) \right) \ldots \left(\sum_{v_r \in E_r} \tau_r(v_r) \right). \tag{1.45}$$

Pela definição da aplicação λ, sabemos que f não é uma m-ésima potência, logo existe i tal que e_i não é múltiplo de m. Como Ψ é um caráter de ordem m, logo Ψ^{e_i} não é o caráter trivial e consequentemente τ_i.

Dessa forma, $\sum_{v_i \in E_i} \tau_i(v_i) = 0$.

Assim, obtemos na relação (1.45) que

$$\sum_{g\in\Phi_k}\lambda(g)=0,\ \text{para } k\geq d. \tag{1.46}$$

■

Teorema 1.26. *Seja Ψ um caráter multiplicativo de $\mathbb{F}_q$ de ordem m, com $m>1$. Seja $f\in\mathbb{F}_q[x]$ um polinômio mônico de grau positivo e que não é uma m-ésima potência. Seja d o número de raízes distintas de f em seu corpo de decomposição sobre $\mathbb{F}_q$. Suponha que $d\geq 2$. Então existem números complexos $\omega_1,\ldots,\omega_{d-1}$, dependendo somente de f e Ψ, tal que para todo inteiro positivo s temos que*

$$\sum_{\gamma\in\mathbb{F}_{q^s}}\Psi^{(s)}(f(\gamma)) \quad =-\omega_1^s-\cdots-\omega_{d-1}^s,$$

onde $\Psi^{(s)}=\Psi\circ N_{\mathbb{F}_{q^s}/\mathbb{F}_q}$.

Demonstração: Consideremos a aplicação $\lambda:\Phi\longrightarrow D$, tal que $\lambda(1)=1$ e $\lambda(g)=\Psi(R(g,f))$ para $g\in\Phi_k$, onde f é o polinômio dado pela hipótese. Pelo Lema 1.23 temos que λ é multiplicativa.

Sabemos pelo Lema 1.25 que $\sum_{g\in\Phi_k}\lambda(g)=0$, para $k\geq d$. Aplicando o que foi feito inicialmente nesta seção para esta função λ que estamos considerando, temos pela relação (1.34) que

$$L_s=\sum_{j=1}^{d-1}\omega_j^s, \tag{1.47}$$

para todo inteiro $s\geq 1$.

Por outro lado, pela relação (1.32), temos $L_s=\sum_h grau(h)\lambda(h)^{s/grau(h)}$, onde a soma é feita sobre os polinômios mônicos e irredutíveis sobre $\mathbb{F}_q$ com grau divisor de s.

Consideremos h um polinômio mônico irredutível sobre $\mathbb{F}_q$ tal que $grau(h)\mid s$. Seja $E=\mathbb{F}_{q^s}$. Tome γ uma raíz de h, logo $\gamma\in E$. Desta maneira, $h^{s/grau(h)}$ é o polinômio característico de γ sobre $\mathbb{F}_q$, de onde segue que

$$h^{s/grau(h)}(x)=(x-\gamma)(x-\gamma^q)\ldots(x-\gamma^{q^{s-1}}). \tag{1.48}$$

Por (1.48) e visto que λ é multiplicativa temos

$$\lambda(h)^{s/grau(h)} = \lambda(h^{s/grau(h)}) = \Psi(R(h^{s/grau(h)}, f)) = \Psi(f(\gamma)f(\gamma^q)\dots f(\gamma^{q^{s-1}})).$$

Como os coeficientes de f estão em $\mathbb{F}_q$ temos então que

$$\lambda(h)^{s/grau(h)} = \Psi\left(N_{E/\mathbb{F}_q}(f(\gamma))\right) = \Psi^{(s)}(f(\gamma)), \tag{1.49}$$

onde $\Psi^{(s)} = \Psi \circ N_{E/\mathbb{F}_q}$.

Da relação (1.49) e sabendo que $grau(h)$ é igual ao número de raízes de h temos que

$$grau(h)\lambda(h)^{s/grau(h)} = \sum_{\substack{\gamma \in E \\ h(\gamma)=0}} \lambda(h)^{s/grau(h)} = \sum_{\substack{\gamma \in E \\ h(\gamma)=0}} \Psi^{(s)}(f(\gamma)). \tag{1.50}$$

De (1.50),

$$L_s = \sum_{h} \sum_{\substack{\gamma \in E \\ h(\gamma)=0}} \Psi^{(s)}(f(\gamma)) = \sum_{\gamma \in E} \Psi^{(s)}(f(\gamma)). \tag{1.51}$$

Portanto pelas relações (1.47) e (1.51) segue

$$\sum_{\gamma \in E} \Psi^{(s)}(f(\gamma)) = -\omega_1^s - \dots - \omega_{d-1}^s.$$

■

Definição 1.27. *Seja K um corpo. Dizemos que um polinômio $f \in K[x,y]$ é absolutamente irredutível sobre K se é irredutível sobre qualquer extensão algébrica de K.*

Pelo método de Stepanov e Schmidt, ver [12], obtemos o próximo resultado.

Teorema 1.28. *Seja $m > 2$ um divisor de $q-1$ e seja $f \in \mathbb{F}_q[x]$ com $grau(f) = k \geq 1$ tal que $y^m - f(x)$ é absolutamente irredutível. Então para $q \geq 100mk^2$, o número N de soluções da equação $y^m = f(x)$ em $\mathbb{F}_q^2$ satisfaz $|N - q| < 4km^{\frac{3}{2}}q^{\frac{1}{2}}$.*

Lema 1.29. *Seja K um corpo. Seja t um elemento pertencente a uma extensão de K, onde $t^n \in K$, para algum $n \in \mathbb{N}$. Se w é o menor inteiro positivo tal que $t^w \in K$, então $w \mid u$, para todo $u \in \mathbb{N}$ tal que $t^u \in K$.*

Demonstração: De fato, caso contrário se $u = wq_1 + r_1$, com $0 < r_1 < w$, então $t^{r_1} = t^{u-wq_1} = t^u(t^w)^{-q_1}$, ou seja, $t^{r_1} \in K$, visto que, $t^u, t^w \in K$. Isto é um absurdo, pois w é o menor inteiro que possui esta propriedade. ∎

Definição 1.30. *Seja K um corpo. Denotaremos $K(x)$ o corpo de funções racionais sobre K, isto é, o corpo que consiste das frações da forma $\frac{f}{g}$ com f e $g \in K[x]$, $g \neq 0$.*

Teorema 1.31. *Seja K um corpo. Seja $f \in K[x]$ com $grau(f) \geq 1$ e seja $m \in \mathbb{N}$. Suponhamos $f(x) = a(x-\alpha_1)^{e_1} \dots (x-\alpha_d)^{e_d}$ é a fatoração de f no seu corpo de decomposição sobre K, onde $a \in K$ e $\alpha_1, \dots, \alpha_d$ são as raízes distintas de f. Então $y^m - f(x)$ é absolutamente irredutível se, e somente se, $mdc(m, e_1, \dots, e_d) = 1$.*

Demonstração: Mostraremos que $y^m - f(x)$ não é absolutamente irredutível se, e somente se, $mdc(m, e_1, \dots, e_d) > 1$.

Suponhamos que $y^m - f(x)$ é redutível sobre uma extensão algébrica L de K. Sem perda de generalidade, podemos supor que em L o polinômio $y^m - 1$ se decompõe. Logo $y^m - 1 = (x-\xi_1)\dots(x-\xi_m)$, onde ξ_i são as raízes m-ésimas da unidade e $\xi_i \in L$.

Como $y^m - f(x)$ é redutível em L, temos que

$$y^m - f(x) = r(x,y)s(x,y), \tag{1.52}$$

com $r(x,y), s(x,y) \in L[x,y]$, $grau(F) > 0$ e $grau(G) > 0$. Consideremos $y^m - f(x)$ como um polinômio em y com coeficientes em $L(x)$. Se Y é uma raíz de $y^m - f(x)$ no corpo de decomposição sobre $L(x)$, então

$$y^m - f(x) = (y - \xi_1 Y)\dots(y - \xi_m Y). \tag{1.53}$$

Observemos que $y - \xi_i Y$, para $i = 1, \dots, m$, são polinômios mônicos e irredutíveis no corpo de decomposição de $y^m - f(x)$ sobre $L(x)$. Pela fatoração única, segue das relações (1.52) e (1.53) que

$$r(x,y) = \alpha(y - \xi_{j_1}Y)\dots(y - \xi_{j_n}Y), \tag{1.54}$$

para algum $j_1, \dots, j_n \in \{1, \dots, m\}$ e $\alpha \neq 0 \in L$ com $1 \leq n < m$.

Como $r(x,y) \in L[x,y]$, segue de (1.54) que $(-1)^n \alpha \xi_{j_1} \dots \xi_{j_n} Y^n \in L[x]$, e assim, $Y^n \in L[x]$, visto que $(-1)^n \alpha \xi_{j_1} \dots \xi_{j_n} \in L$.

Seja w o menor inteiro positivo tal que $Y^w \in L(x)$. Logo $w \leq n < m$.

Como Y é raíz de $y^m - f(x)$ temos que $Y^m = f(x)$, ou seja, $Y^m \in L(x)$. Assim pelo Lema 1.29 temos que $w \mid m$.

Considere $t = \dfrac{m}{w}$. Como $w \leq n < m$ e $w \mid m$ temos que $t > 1$.

Escreva $Y^w = \dfrac{g}{h}$, tal que $g, h \in L[x]$, com $h \neq 0$.

Logo,

$$f = Y^m = Y^{tw} = (Y^w)^t = \left(\frac{g}{h}\right)^t, \text{ ou seja, } \quad fh^t = g^t.$$

Por hipótese, $f(x) = a(x-\alpha_1)^{e_1} \ldots (x-\alpha_d)^{e_d}$. Assim

$$a(x-\alpha_1)^{e_1} \ldots (x-\alpha_d)^{e_d} h^t = g^t,$$

de onde concluímos que $t \mid e_1, \ldots, t \mid e_d$. Dessa maneira, visto que $t \mid m$, obtemos $mdc(m, e_1, \ldots, e_d) \geq t > 1$.

Reciprocamente, suponhamos que $e = mdc(m, e_1, \ldots, e_d) > 1$. Seja K_1 o corpo de decomposição de f sobre K. Como $a \neq 0$, em uma certa extensão de K_1 existe um elemento β tal que $\beta^e = a$. Coloque $s = \dfrac{m}{e}$ e considere $f_1(x) = \beta(x-\alpha_1)^{\frac{e_1}{e}} \ldots (x-\alpha_d)^{\frac{e_d}{e}}$.

Daí,

$$y^m - f(x) \;=\; (y^s)^e - (f_1(x))^e \;=\; (y^s - f_1(x))(y^{s(e-1)} + y^{s(e-2)} f_1(x) + \cdots + f_1(x)^{e-1}),$$

isto é, $y^m - f(x)$ não é absolutamente irredutível. ∎

Teorema 1.32. *Sejam $\omega_1, \ldots, \omega_n$ números complexos. Sejam B e C constantes positivas tais que $|\omega_1^s + \cdots + \omega_n^s| \leq CB^s$, para todo inteiro positivo s. Então $|\omega_j| \leq B$, para $j = 1, \ldots, n$.*

Demonstração: Seja z uma variável complexa, então

$$log(1 - \omega_j z) = -\sum_{s=1}^{\infty} \frac{1}{s} \omega_j^s z^s, \text{ para } j = 1, \ldots, n,$$

desde que $|\omega_j z| \leq 1$, isto é, $|z| \leq \dfrac{1}{|\omega_j|}$, ver [3]. Daí

$$log((1-\omega_1 z)\ldots(1-\omega_n z)) \;=\; log(1-\omega_1 z) + \cdots + log(1-\omega_n z) \;=\; -\sum_{s=1}^{\infty} \frac{1}{s}(\omega_1^s + \cdots + \omega_n^s) z^s. \tag{1.55}$$

Pela hipótese obtemos que

$$\left|\frac{1}{s}(\omega_1^s + \cdots + \omega_n^s)\right| \quad \leq \quad |\omega_1^s + \cdots + \omega_n^s| \quad \leq \quad CB^s. \tag{1.56}$$

Observemos que para $|z| < \dfrac{1}{B}$ temos que a série $\displaystyle\sum_{s=1}^{\infty} B^s z^s$ converge absolutamente, e consequentemente a série $C\displaystyle\sum_{s=1}^{\infty} B^s z^s$. Logo da relação (1.56), concluímos que a série $\displaystyle\sum_{s=1}^{\infty} \frac{1}{s}(\omega_1^s + \cdots + \omega_n^s) z^s$ converge absolutamente, para $|z| < \dfrac{1}{B}$.

Sendo assim, a função $log((1-\omega_1 z)\ldots(1-\omega_n z))$ é analítica para $|z| < \dfrac{1}{B}$. Dessa maneira, $1 - \omega_j z \neq 0$, para $j = 1, \ldots, n$ em $|z| < \dfrac{1}{B}$.

Portanto devemos ter

$$\frac{1}{B} \quad \leq \quad \frac{1}{|\omega_j|}, \quad j = 1, \ldots, n, \text{ ou seja,} \quad |\omega_j| \quad \leq \quad B, \quad j = 1, \ldots, n.$$

■

Teorema 1.33. *Seja Ψ um caráter multiplicativo de $\mathbb{F}_q$ de ordem m, com $m > 1$. Seja $f \in \mathbb{F}_q[x]$ um polinômio mônico de grau positivo e que não é uma m-ésima potência. Seja d o número de raízes distintas de f em seu corpo de decomposição sobre $\mathbb{F}_q$. Suponha que $d \geq 2$. Então os números complexos $\omega_1, \ldots, \omega_{d-1}$ do Teorema 1.26 satisfazem $|\omega_j| \leq q^{\frac{1}{2}}$, para $j = 1, \ldots, d-1$.*

Demonstração: Seja $k = grau(f)$. Escolhamos $r \in \mathbb{N}$ tal que $q^r \geq 100mk^2$ e o corpo de decomposição de f esteja contido em $\mathbb{F}_{q^r}$. Como, por hipótese, f é um polinômio mônico com d raízes distintas, $f(x) = (x-\alpha_1)^{e_1}\ldots(x-\alpha_d)^{e_d}$, onde $\alpha_1, \ldots, \alpha_d$ são as raízes distintas de f.

Consideremos $e = mdc(m, e_1, \ldots, e_d)$. Como f não é uma m-ésima potência segue que $e \neq m$, pois existe e_i tal que $m \nmid e_i$. E assim, e é um divisor próprio de m.

Seja $g(x) = (x-\alpha_1)^{e_1/e}\ldots(x-\alpha_d)^{e_d/e}$. Observemos que $g(x) \in \mathbb{F}_{q^r}[x]$ e $f = g^e$.

Fixemos $s \in \mathbb{N}$. Seja $E = \mathbb{F}_{q^{rs}}$. Consideremos os seguintes caracteres, $\lambda = \psi^{(rs)}$ e $\tau = \lambda^e$, definidos sobre E. Como ψ é um caráter multiplicativo de ordem m, segue que λ tem ordem m e τ tem ordem $n = \dfrac{m}{e} > 1$.

Daí, como $f = g^e$ e λ é um caráter multiplicativo, temos

$$\sum_{\gamma\in E}\lambda(f(\gamma)) \;=\; \sum_{\gamma\in E}\lambda(g^e(\gamma)) \;=\; \sum_{\gamma\in E}\lambda^e(g(\gamma)) \;=\; \sum_{\gamma\in E}\tau(g(\gamma)). \tag{1.57}$$

Agora, consideremos ρ uma raíz primitiva n-ésima da unidade. Para $j = 0, 1, \ldots, n-1$, definimos $U_j = \{\alpha \in E;\ \ \tau(\alpha) = \rho^j\}$. Fixe $\xi \in U_1$. Temos que $\alpha \in U_0$ se, e somente se, $\alpha\xi^{-j} \in U_j$. Isto decorre imediatamente da definição de U_j.

Observemos que se $\alpha\xi^{-j} \in U_0$, então $\tau(\alpha\xi^{-j}) = 1$. Como τ é um caráter de ordem n segue que $\alpha\xi^{-j} = \beta^n$ para algum $\beta \in E^* = \mathbb{F}_{q^{rs}}^*$.

Definamos A_j como sendo o número de $\gamma \in E$ com $g(\gamma) \in U_j$, ou seja, pela observação feita acima, A_j consiste na quantidade de elementos de E tais que $\xi^{-j}g(\gamma) = \beta^n$ para algum $\beta \in E^*$ e B_j como o número de soluções de $y^n = \xi^{-j}g(x)$ em $E \times E^*$. Pelas definições de A_j e B_j segue que

$$A_j \;=\; \frac{B_j}{n}. \tag{1.58}$$

Seja N_j o número total de soluções de $y^n = \xi^{-j}g(x)$ em $E \times E$.

Como $e = mdc(m, e_1, \ldots, e_d)$, segue que

$$1 = mdc\left(\frac{m}{e}, \frac{e_1}{e}, \ldots, \frac{e_d}{e}\right), \text{ ou seja, } \quad mdc\left(n, \frac{e_1}{e}, \ldots, \frac{e_d}{e}\right) = 1.$$

Sendo assim, pelo Teorema 1.31 obtemos que o polinômio $y^n - \xi^{-j}g(x)$ é absolutamente irredutível.

Agora, como ψ e τ são caracteres multiplicativos de $\mathbb{F}_q$ e $\mathbb{F}_{q^{rs}}$, respectivamente, segue que $m \mid (q-1)$ e $n \mid (q^{rs}-1)$, visto que ψ é de ordem m e τ é de ordem n.

Observemos que $q^{rs} \geq q^r \geq 100mk^2 \geq 100n(grau(g))^2$, visto que $n \mid m$ e $grau(f) = k \geq grau(g)$. Assim, pelo Teorema 1.28 obtemos

$$|N_j - q^{rs}| < 4\left(\frac{k}{e}\right) n^{3/2}(q^{rs})^{1/2}, \tag{1.59}$$

pois $grau(g) = \dfrac{k}{e}$, devido $f = g^e$.

Temos também que

$$|N_j - B_j| \leq \frac{k}{e}. \tag{1.60}$$

De fato, pelas definições de N_j e B_j, concluímos que a diferença $N_j - B_j$ nos fornece o número de soluções da equação $y^n - \xi^{-j} g(x)$ quando $y = 0$. Como $grau(g) = \dfrac{k}{e}$, obtemos a estimativa desejada.

Das relações (1.59) e (1.60) temos

$$\begin{aligned} |B_j - q^{rs}| &= |B_j - N_j + N_j - q^{rs}| &&\leq |B_j - N_j| + |N_j - q^{rs}| \\ &\leq \frac{k}{e} + 4\frac{k}{e} n^{3/2} q^{rs/2} &&\leq 5\frac{k}{e} n^{3/2} q^{rs/2}, \end{aligned}$$

ou seja,

$$|B_j - q^{rs}| \leq 5\frac{k}{e} n^{3/2} q^{rs/2}, \text{ para } j = 0, 1, \ldots, n-1. \tag{1.61}$$

Escrevamos

$$A_j = \frac{1}{n} q^{rs} + R_j. \tag{1.62}$$

Logo, pelas relações (1.58) e (1.61) temos que

$$|R_j| = \left| A_j - \frac{1}{n} q^{rs} \right| = \frac{1}{n} |B_j - q^{rs}| \leq \frac{1}{n} 5\frac{k}{e} n^{3/2} q^{rs/2},$$

isto é,

$$|R_j| \leq 5\frac{k}{e} n^{1/2} q^{rs/2}, \text{ para } j = 0, 1, \ldots, n-1. \tag{1.63}$$

Segue da relação (1.57) que

$$\left| \sum_{\gamma \in E} \lambda(f(\gamma)) \right| = \left| \sum_{\gamma \in E} \tau(g(\gamma)) \right| = \left| \sum_{\substack{\gamma \in E \\ g(\gamma) \in U_0}} \tau(g(\gamma)) + \cdots + \sum_{\substack{\gamma \in E \\ g(\gamma) \in U_{n-1}}} \tau(g(\gamma)) \right|$$

$$= \left| \sum_{\substack{\gamma \in E \\ g(\gamma) \in U_0}} \rho^0 + \cdots + \sum_{\substack{\gamma \in E \\ g(\gamma) \in U_{n-1}}} \rho^{n-1} \right| = \left| \rho^0 A_0 + \cdots + \rho^{n-1} A_{n-1} \right| = \left| \sum_{j=0}^{n-1} A_j \rho^j \right|.$$

Agora, da relação (1.62), segue que

$$\left| \sum_{\gamma \in E} \lambda(f(\gamma)) \right| = \left| \sum_{j=0}^{n-1} \left(\frac{1}{n} q^{rs} + R_j \right) \rho^j \right| = \left| \frac{1}{n} q^{rs} \sum_{j=0}^{n-1} \rho^j + \sum_{j=0}^{n-1} R_j \rho^j \right|$$

$$= \left| \frac{1}{n} q^{rs} \frac{1 - \rho^n}{1 - \rho} + \sum_{j=0}^{n-1} R_j \rho^j \right| = \left| \sum_{j=0}^{n-1} R_j \rho^j \right| \leq \sum_{j=0}^{n-1} |R_j|.$$

Da relação (1.63) obtemos que

$$\left|\sum_{\gamma\in E}\lambda(f(\gamma))\right| \leq 5\frac{k}{e}n^{1/2}q^{rs/2}\sum_{j=0}^{n-1}1 = 5\frac{k}{e}n^{3/2}q^{rs/2}. \tag{1.64}$$

Do Teorema 1.26, temos que $\sum_{\gamma\in\mathbb{F}_{q^{rs}}}\lambda(f(\gamma)) = -\omega_1^{rs} - \cdots - \omega_{d-1}^{rs}$. Assim, substituindo na relação (1.64), obtemos

$$|(\omega_1^r)^s + \cdots + (\omega_{d-1}^r)^s| \leq 5\frac{k}{e}n^{3/2}(q^{r/2})^s.$$

Do Teorema 1.32, segue então que $|\omega_j^r| \leq q^{r/2}$, para $j = 1, \ldots, d-1$, e assim, $|\omega_j| \leq q^{1/2}$, para $j = 1, \ldots, d-1$. O que conclui a demonstração do teorema. ∎

Teorema 1.34. ***(Teorema de Hasse - Weil)*** *Seja Ψ um caráter multiplicativo de $\mathbb{F}_q$ de ordem $m > 1$. Seja $f \in \mathbb{F}_q[x]$ um polinômio mônico de grau positivo e que não é uma m-ésima potência. Seja d o número de raízes distintas de f em seu corpo de decomposição sobre $\mathbb{F}_q$. Então para todo $\alpha \in \mathbb{F}_q$ temos que* $\left|\sum_{c\in\mathbb{F}_q}\Psi(\alpha f(c))\right| \leq (d-1)\sqrt{q}$.

Demonstração: Se $d = 1$, como f não é uma m-ésima potência, segue que $f = (x-\alpha_1)^n$, com $m \nmid n$.

Assim,

$$\sum_{c\in\mathbb{F}_q}\Psi(\alpha f(c)) = \sum_{c\in\mathbb{F}_q}\Psi(\alpha)\Psi((c-\alpha_1)^n) = \Psi(\alpha)\sum_{c\in\mathbb{F}_q}\Psi^n(c-\alpha_1) = \Psi(\alpha)\sum_{d\in\mathbb{F}_q}\Psi^n(d) = 0,$$

visto que, Ψ é caráter multiplicativo de ordem m e Ψ^n não é o caráter trivial. E assim, segue o resultado desejado.

Agora, suponhamos que $d \geq 2$. Pelo Teorema 1.26 segue que

$$\sum_{c\in\mathbb{F}_q}\Psi(\alpha f(c)) = \Psi(\alpha)\sum_{c\in\mathbb{F}_q}\Psi(f(c)) = -\Psi(\alpha)(\omega_1 + \cdots + \omega_{d-1}).$$

Logo,

$$\left|\sum_{c\in\mathbb{F}_q}\Psi(\alpha f(c))\right| = \left|-\Psi(\alpha)(\omega_1 + \cdots + \omega_{d-1})\right| \leq |\,\omega_1\,| + \cdots + |\,\omega_{d-1}\,|\,.$$

Segue do Teorema 1.33 que

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

■

Corolário 1.35. *Seja p um número primo e χ um caráter multiplicativo módulo p de ordem k diferente do caráter principal, tal que $k \mid (p-1)$. Seja $B(x)$ um polinômio do tipo $(x-a_1)^{\alpha_1}\dots(x-a_t)^{\alpha_t}$, onde $a_i \not\equiv a_j \pmod{p}$ para $i \neq j$ e $0 < \alpha_i < k$. Então $\left|\sum_x \chi(B(x))\right| \leq (t-1)\sqrt{p}$, onde x percorre um sistema completo de resíduos módulo p.*

Demonstração: Decorre imediatamente do Teorema anterior. ■

Corolário 1.36. *Seja χ um caráter multiplicativo módulo p de ordem k diferente do caráter principal. Consideremos a_i e b_j inteiros satisfazendo as seguintes relações: $a_ib_j - a_jb_i \not\equiv 0 \pmod{p}$ para $i \neq j$ e $a_i \not\equiv 0 \pmod{p}$ para $i = 1,\dots,t$. Sejam $r_1,\dots,r_t$ inteiros tais que $0 < r_i < k$. Então $\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right)\right| \leq (t-1)\sqrt{p}+1$.*

Demonstração: Sabemos, por hipótese, que χ é multiplicativo e $a_i \not\equiv 0 \pmod{p}$ para todo $i = 1,\dots,t$. Dessa forma, segue que

$$\begin{aligned}\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right) &= \chi\left(\prod_{i=1}^{t}\left[a_i\left(\lambda+\frac{b_i}{a_i}\right)\right]^{r_i}\right) = \chi\left(\prod_{i=1}^{t}a_i^{r_i}\left(\lambda+\frac{b_i}{a_i}\right)^{r_i}\right)\\ &= \chi\left(\prod_{i=1}^{t}a_i^{r_i}\prod_{i=1}^{t}\left(\lambda+\frac{b_i}{a_i}\right)^{r_i}\right) = \chi\left(\prod_{i=1}^{t}a_i^{r_i}\right)\chi\left(\prod_{i=1}^{t}\left(\lambda+\frac{b_i}{a_i}\right)^{r_i}\right).\end{aligned}$$

Fazendo $c_i = \dfrac{b_i}{a_i}$, temos

$$\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right) = \chi\left(\prod_{i=1}^{t}a_i^{r_i}\right)\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right). \tag{1.65}$$

Observamos que $c_i \not\equiv c_j \pmod{p}$ para todo $i \neq j$. De fato, suponhamos que exista um par de índices i e j tais que $c_i \equiv c_j \pmod{p}$. Dessa maneira, $\dfrac{b_i}{a_i} \equiv \dfrac{b_j}{a_j} \pmod{p}$, ou seja, $a_ib_j - a_jb_i \equiv 0 \pmod{p}$, o que é um absurdo devido a hipótese.

Daí por (1.65) segue que

$$\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right)\right| = \left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}a_i^{r_i}\right)\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right|$$

$$= \left|\chi\left(\prod_{i=1}^{t}a_i^{r_i}\right)\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right| = \left|\chi\left(\prod_{i=1}^{t}a_i^{r_i}\right)\right|\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right|$$

$$= \left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right| = \left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)+\chi\left(\prod_{i=1}^{t}(0+c_i)^{r_i}\right)-\chi\left(\prod_{i=1}^{t}(0+c_i)^{r_i}\right)\right|$$

$$= \left|\sum_{\lambda=0}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)-\chi\left(\prod_{i=1}^{t}(0+c_i)^{r_i}\right)\right| \leq \left|\sum_{\lambda=0}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right|+\left|\chi\left(\prod_{i=1}^{t}c_i^{r_i}\right)\right|,$$

onde a última desigualdade decorre da Desigualdade Triangular.

Assim

$$\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right)\right| \leq \left|\sum_{\lambda=0}^{p-1}\chi\left(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}\right)\right|+1. \tag{1.66}$$

Observe que temos todas as hipóteses do Corolário 1.35 satisfeitas e dessa forma segue de (1.66) que

$$\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i}\right)\right| \leq (t-1)\sqrt{p}+1.$$

■

Capítulo 2

Soluções p-ádicas para Pares de Formas Aditivas

2.1 Resultados Preliminares

Nesta seção apresentamos duas técnicas que nos auxiliam na busca de zeros p-ádicos para pares de formas aditivas: a p-normalização e a coloração de variáveis. Dado um par de formas aditivas f e g de grau k em n variáveis, a primeira técnica mencionada, consiste em uma maneira de agrupar as variáveis de f e g com determinada propriedade e saber estimar o número mínimo de variáveis presentes em cada grupo formado. Agora a segunda técnica será aplicada em um dos grupos formados, de tal forma que separaremos as variáveis deste grupo por cores e obteremos uma condição para que o par f e g possua zeros p-ádicos. As principais referências desta seção são [5], [9] e [10].

2.1.1 p-normalização

Sejam f e g duas formas aditivas de grau k em n variáveis com coeficientes inteiros, ou seja,

$$\begin{cases} f &= a_1x_1^k + \cdots + a_nx_n^k \\ g &= b_1x_1^k + \cdots + b_nx_n^k \end{cases}. \tag{2.1}$$

Associamos às formas f e g a seguinte função

$$\theta(f,g) = \prod_{i \neq j} (a_i b_j - a_j b_i),$$

isto é, $\theta(f,g)$ é o produto dos determinantes das possíveis submatrizes 2×2 obtidas a partir da matriz dos coeficientes do sistema.

Propriedade 2.1. *Se* $\begin{cases} f^* = f(p^{v_1}x_1, \ldots, p^{v_n}x_n) \\ g^* = g(p^{v_1}x_1, \ldots, p^{v_n}x_n) \end{cases}$ *, então* $\theta(f^*, g^*) = p^{2k(n-1)\sum v_i}\theta(f,g)$.

Propriedade 2.2. *Se* $\begin{cases} f^* = \lambda f + \mu g \\ g^* = \rho f + \sigma g \end{cases}$ *, então* $\theta(f^*, g^*) = (\lambda\sigma - \mu\rho)^{n(n-1)}\theta(f,g)$.

A demonstração de tais propriedades podem ser encontradas em [9] e [10].

Definição 2.3. *Dois pares de formas aditivas, com coeficientes inteiros, são ditos equivalentes se um puder ser obtido do outro por alguma combinação das operações apresentadas nas hipóteses das Propriedades 2.1 e 2.2, considerando* $v_1, \ldots, v_n \in \mathbb{Z}$ *e* $\lambda, \mu, \rho, \sigma \in \mathbb{Q}$*, com* $\lambda\sigma - \mu\rho \neq 0$.

Observemos que se um par de formas aditivas f e g possui zeros p-ádicos, então todos os outros pares equivalentes a ele também possuem.

Coloquemos o sistema (2.1) da seguinte forma:

$$\begin{cases} f = f_0 + pf_1 \\ g = g_0 + pg_1 \end{cases},$$

onde f_i e g_i são subformas nas variáveis x_j de f e g, para $j = 1, 2, \ldots, n$ e cada uma das variáveis presentes em f_0 e g_0 tem pelo menos um dos coeficientes não divisível por p.

Definição 2.4. *Definimos* m_0*, como o número de variáveis presentes no par* f_0 *e* g_0*. E definimos* q_0*, como o menor número de variáveis que aparece com coeficientes coprimos com* p *em* $\lambda f_0 + \mu g_0$*, com* p *não dividindo* λ *e* μ *simultaneamente.*

A partir de agora, restringimos o nosso estudo aos pares de formas aditivas, f e g, de grau k e n variávies, tais que $\theta(f,g) \neq 0$, pois é conhecido que garantir a existência de solução não-trivial para sistemas com esta propriedade também nos garante solução não-trivial para sistemas onde a função θ é zero, ver [10]. Com esta restrição obtemos estimativas para m_0 e q_0 do sistema considerado.

Definição 2.5. *Um par de formas aditivas f e g é dito ser p-normalizado se for o elemento de sua classe com $v_p(\theta(f,g))$ mínimo, onde v_p é a valorização p-ádica.*

Lema 2.6. *Se f e g são p-normalizados, então $m_0 \geq \frac{n}{k}$ e $q_0 \geq \frac{n}{2k}$.*

Demonstração: Ver [9] e [10]. ∎

Definição 2.7. *Sejam k um inteiro positivo e p um primo. Escreva $k = p^\tau k_0$, com $mdc(k_0, p) = 1$. Defina γ da seguinte forma:*

$$\gamma = \begin{cases} \tau + 1 & se \quad p > 2 \\ \tau + 2 & se \quad p = 2 \end{cases}.$$

Lema 2.8. *Sejam f e g formas aditivas em n variáveis e de grau k. Seja γ como na Definição 2.7. Se o sistema*

$$\begin{cases} f \equiv 0 \pmod{p^\gamma} \\ g \equiv 0 \pmod{p^\gamma} \end{cases} \tag{2.2}$$

tem uma solução $(\xi_1, \ldots, \xi_n)$, onde $\xi_i \in \mathbb{Z}$, $i = 1, \ldots, n$ tal que a matriz

$$\begin{pmatrix} a_1\xi_1 & \ldots & a_n\xi_n \\ b_1\xi_1 & \ldots & b_n\xi_n \end{pmatrix} \tag{2.3}$$

tem posto 2 módulo p, então o par f e g possui um zero p-ádico não-trivial. Neste caso, dizemos que $(\xi_1, \ldots, \xi_n)$ é uma solução não-singular.

Demonstração: Ver [9] e [10]. ∎

2.1.2 Coloração de variáveis

Em $\mathbb{F}_p^2$ consideremos os vetores $e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $e_v = \begin{pmatrix} v \\ 1 \end{pmatrix}$ para $v = 1, \ldots, p$.

Definimos $L_v = \{te_v; 1 \leq t \leq p-1\}$ para $v = 0, 1, \ldots, p$. Observamos que L_v é um subconjunto de $\mathbb{F}_p^2$, cujos os elementos são múltiplos de e_v.

Lema 2.9. *Temos que $\mathbb{F}_p^2 \setminus \{(0,0)\}$ é a união disjunta dos conjuntos L_v com $v = 0, 1, \ldots, p-1$.*

Demonstração: É fácil ver que $\mathbb{F}_p^2 \setminus \{(0,0)\} = \bigcup_{v=0}^{p-1} L_v$. Só resta mostrarmos que tal união é disjunta. De fato, seja $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{F}_p^2$ e suponhamos que existam r e s, com $0 \leq r \leq p$, $0 \leq s \leq p$ e $r \neq s$, tais que $\begin{pmatrix} a \\ b \end{pmatrix} \in L_r$ e $\begin{pmatrix} a \\ b \end{pmatrix} \in L_s$. Suponhamos $r \neq 0$ e $s \neq 0$. Assim pela definição temos por um lado que $\begin{pmatrix} a \\ b \end{pmatrix} = c_1 \begin{pmatrix} r \\ 1 \end{pmatrix}$ e por outro $\begin{pmatrix} a \\ b \end{pmatrix} = c_2 \begin{pmatrix} s \\ 1 \end{pmatrix}$.

Logo

$$a = c_1 r \qquad b = c_1, \tag{2.4}$$

e

$$a = c_2 s \qquad b = c_2. \tag{2.5}$$

Assim das relações (2.4) e (2.5) obtemos que $r = b^{-1}a = s$, o que contradiz o fato de $r \neq s$.

O caso quando $r = 0$ ou $s = 0$ segue de maneira semelhante.

Portanto, dado um elemento de $\mathbb{F}_p^2$, temos que ele pertence a apenas um dos conjuntos L_v com $v = 0, 1, \ldots, p$. ∎

Seja f e g um par de formas aditivas p-normalizado. A partir de agora, estamos interessados somente nas variáveis presentes nas subformas f_0 e g_0. Pelo Lema 2.9, sabemos que para estas variáveis existe um único $v = v(j)$ tal que $\begin{pmatrix} a_j \\ b_j \end{pmatrix}$ pertence a L_v. Neste caso definimos v como sendo a **cor** da variável x_j.

Definição 2.10. *Para v tal que $0 \leq v \leq p$, definimos $I_v = \{1 \leq j \leq m_0; v(j) = v\}$, isto é, I_v é o conjunto de índices das variáveis presentes em f_0 e g_0 cuja cor é v.*

Definição 2.11. *Para v tal que $0 \leq v \leq p$, definimos $\mathbb{I}_v = \mid I_v \mid$, isto é, $\mathbb{I}_v$ é a quantidade de variáveis em f_0 e g_0 que possuem a cor v.*

Exemplo 2.12. *Em $\mathbb{F}_7$ consideremos o seguinte sistema:*

$$\begin{cases} 2x_1^k & +4x_2^k & +2x_3^k & +3x_4^k & +6x_5^k & +2x_6^k & = 0 \\ x_1^k & +6x_2^k & +4x_3^k & +x_4^k & +3x_5^k & +3x_6^k & = 0 \end{cases}.$$

Observamos que x_1 e x_5 são variáveis de cor 2; x_2, x_4 e x_6 são variáveis de cor 3 e x_3 é uma variável de cor 4.

Lema 2.13. *Para todo v, $\mathbb{I}_0 \geq \mathbb{I}_v$.*

Demonstração: De fato, basta separarmos as variáveis de f_0 e g_0 por cores. Seja $v \neq 0$ a cor que possui o maior número de variáveis. Utilizando escalonamento podemos transformar as variáveis de cor v em variáveis de cor 0. E assim, o novo sistema obtido possui mais variáveis de cor 0 e é equivalente ao inicial. ∎

Definição 2.14. *Seja $(\xi_1, \ldots, \xi_n)$ uma solução qualquer de* $\begin{cases} f(x_1, \ldots, x_n) \equiv 0 \pmod{p^\gamma} \\ g(x_1, \ldots, x_n) \equiv 0 \pmod{p^\gamma} \end{cases}$, *onde γ é como na Definição 2.7. Definimos o suporte como o conjunto de todas as variáveis tais que $mdc(\xi_i, p) = 1$.*

Lema 2.15. *Seja $(\xi_1, \ldots, \xi_n)$ uma solução de* $\begin{cases} f(x_1, \ldots, x_n) \equiv 0 \pmod{p^\gamma} \\ g(x_1, \ldots, x_n) \equiv 0 \pmod{p^\gamma} \end{cases}$, *onde γ é como na Definição 2.7. Temos que $(\xi_1, \ldots, \xi_n)$ é uma solução não-singular se, e somente se, o suporte contém duas variáveis com cores diferentes.*

Demonstração: Suponhamos $(\xi_1, \ldots, \xi_n)$ solução não-singular. Logo existem i e j tais que $(a_i b_j - a_j b_i)\xi_i \xi_j \not\equiv 0 \pmod{p}$. Assim $mdc(\xi_i, p) = 1$ e $mdc(\xi_j, p) = 1$, ou seja, x_i e x_j pertencem ao suporte. Além disso, x_i e x_j são variáveis de cores diferentes pois, $(a_i b_j - a_j b_i) \not\equiv 0 \pmod{p}$. A recíproca é imediata. ∎

Definição 2.16. *Uma cor v é dita ser representante de zero se para γ como na Definição 2.7 as congruências $\sum_{j \in I_v} a_j x_j^k \equiv \sum_{j \in I_v} b_j x_j^k \equiv 0 \pmod{p^\gamma}$, tem uma solução primitiva, ou seja, uma solução com pelo menos uma das coordenadas coprima com p.*

Lema 2.17. *Se duas cores são representantes de zero, então as congruências*

$$\begin{cases} f_0 \equiv 0 \pmod{p^\gamma} \\ g_0 \equiv 0 \pmod{p^\gamma} \end{cases} \tag{2.6}$$

possui uma solução não-singular.

Demonstração: Sejam v_1 e v_2 duas cores representantes de zero. Logo pela Definição 2.16 temos que

$$\sum_{j\in I_{v_1}} a_j x_j^k = \sum_{j\in I_{v_1}} b_j x_j^k \equiv 0 \pmod{p^\gamma}$$

e

$$\sum_{j\in I_{v_2}} a_j x_j^k = \sum_{j\in I_{v_2}} b_j x_j^k \equiv 0 \pmod{p^\gamma}$$

têm solução primitiva. Assim existem uma variável de cor v_1 e uma variável de cor v_2 que estão no suporte, ou seja, duas variáveis no suporte com cores diferentes. Portanto, pelo Lema 2.15, o sistema (2.6) possui solução não-singular. ∎

Lema 2.18 (Olson). *Sejam δ, σ e s números inteiros tais que $\delta \geq \sigma \geq 1$ e $s \geq p^\delta + p^\sigma - 1$. Sejam $a_j, b_j \in \mathbb{Z}$. Então, o sistema*

$$\begin{cases} a_1 x_1^k + \cdots + a_s x_s^k \equiv 0 \pmod{p^\delta} \\ b_1 x_1^k + \cdots + b_s x_s^k \equiv 0 \pmod{p^\sigma} \end{cases},$$

possui solução $\overrightarrow{\xi} = (\xi_1, \ldots, \xi_s)$, com $\xi_j \in \{0, 1\}$ para $1 \leq j \leq s$ e algum $\xi_j \neq 0$.

Demonstração: Ver [14]. ∎

Lema 2.19. *Se $\mathbb{I}_v \geq p^\gamma + p^{\gamma-1} - 1$, então a cor v é representante de zero.*

Demonstração: Suponhamos que $1 \leq v \leq p$. Para toda variável x_j de cor v, temos que $\begin{pmatrix} a_j \\ b_j \end{pmatrix} = \lambda \begin{pmatrix} v \\ 1 \end{pmatrix}$, isto é, $a_j \equiv b_j v \pmod{p}$, ou seja, existe $t_j \in \mathbb{Z}$ tal que $a_j = v b_j + p t_j$.

Pela Definição 2.16, devemos mostrar que o sistema $\sum_{j\in I_v} a_j x_j^k \equiv \sum_{j\in I_v} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ possui solução primitiva. Observemos que este sistema é equivalente ao sistema

$$\sum_{j\in I_v} t_j x_j^k \equiv 0 \pmod{p^{\gamma-1}} \; ; \quad \sum_{j\in I_v} b_j x_j^k \equiv 0 \pmod{p^\gamma}.$$

Segue pelo Lema 2.18, devido a hipótese, que o sistema acima possui solução primitiva e assim v é representante de zero.

Para o caso $v = 0$, inverta as linhas do sistema e aplique o raciocínio anterior para a cor p. ∎

Lema 2.20. *Seja Ω a união de todos I_v tais que a cor v não é representante de zero. Se $|\Omega| \geq 2p^\gamma - 1$, então o sistema $\sum_{j=1}^{m_0} a_j x_j^k \equiv \sum_{j=1}^{m_0} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ tem uma solução não-singular.*

Demonstração: Para demonstrarmos o Lema, é suficiente mostrarmos que o sistema $\sum_{j\in\Omega} a_j x_j^k \equiv \sum_{j\in\Omega} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ tem uma solução primitiva, e isto ocorre devido ao Lema 2.18, visto que $|\Omega| \geq 2p^\gamma - 1$.

Assim, o sistema $\sum_{j=1}^{m_0} a_j x_j^k \equiv \sum_{j=1}^{m_0} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ possui solução, e esta é não-singular pois o suporte contém duas variáveis em cores diferentes. ∎

Lema 2.21. *Se $q_0 \geq 2p^\gamma - 1$, então o sistema $\sum_{j=1}^{m_0} a_j x_j^k \equiv \sum_{j=1}^{m_0} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ tem uma solução não-singular.*

Demonstração: Sem perda de generalidade, assumiremos que o sistema possui no máximo uma cor representante de zero, pois caso houvesse duas cores representantes de zero, o resultado segue pelo Lema 2.17.

Deste modo, suponhamos que u, $u \in \{0, 1, \ldots, p\}$, é a única cor representante de zero do sistema. Seja Ω a união de todos I_v com $0 \leq v \leq p$ e $v \neq u$. Logo,

$$|\Omega| = m_0 - I_u \geq m_0 - I_0 = q_0,$$

visto que $I_0 \geq I_v$, para todo v. Como por hipótese $q_0 \geq 2p^\gamma - 1$ segue então que $|\Omega| \geq 2p^\gamma - 1$. Daí, pelo Lema 2.20 obtemos que o sistema possui uma solução não-singular.

Agora, quando não existe cor representante de zero, basta utilizarmos novamente o Lema 2.20 tendo observado que $|\Omega| = m_0$ e $m_0 \geq q_0$. ∎

Lema 2.22. *Sejam s e τ inteiros positivos tais que $2^s > p^{2\tau}$. Sejam $a_j, b_j \in \mathbb{Z}$. Suponhamos que -1 é uma k-ésima potência módulo p^τ. Então o sistema $\sum_{j=1}^{s} a_j x_j^k \equiv \sum_{j=1}^{s} b_j x_j^k \equiv 0 \pmod{p^\tau}$ tem uma solução com $x_j \in \{0, 1, -1\}$.*

Demonstração: Ver [8]. ∎

Lema 2.23. *Se -1 é uma k-ésima potência módulo p^γ e $2^{q_0} > p^{2\gamma}$, então o sistema $\sum_{j=1}^{m_0} a_j x_j^k \equiv \sum_{j=1}^{m_0} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ tem uma solução não-singular.*

Demonstração: Suponhamos que exista no máximo uma cor representante de zero. Pelo mesmo raciocínio da demonstração do Lema 2.21 obtemos que $|\Omega| \geq q_0$, onde Ω é a união de todos I_v tais que v não é representante de zero.

Por hipótese, temos que -1 é uma k-ésima potência módulo p^γ e $2^{q_0} > p^{2\gamma}$. Logo $2^{|\Omega|} > p^{2\gamma}$. Assim pelo Lema 2.22 o sistema $\sum_{j\in\Omega} a_j x_j^k \equiv \sum_{j\in\Omega} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ possui solução primitiva.

Daí segue que o sistema $\sum_{j=1}^{m_0} a_j x_j^k \equiv \sum_{j=1}^{m_0} b_j x_j^k \equiv 0 \pmod{p^\gamma}$ possui solução não-singular, visto que o suporte contém duas variáveis com cores diferentes.

■

2.2 Solubilidade de Pares de Formas Aditivas

Nesta seção mencionamos dois resultados sobre zeros p-ádicos não-triviais de formas aditivas, onde o primeiro é a motivação para o resultado de Meir. E além disso, apresentamos dois exemplos que nos mostram a relação do número mínimo de variáveis do sistema com a existência de solução não-trivial.

É conhecido devido a Atkinson e Cook, ver [2], o seguinte resultado:

Teorema 2.24 (Atkinson e Cook). *Sejam k e n inteiros positivos tais que $k > 1$ e $n > 4k$. Então o sistema de equações*

$$\begin{cases} a_1 x_1^k + \cdots + a_n x_n^k = 0 \\ b_1 x_1^k + \cdots + b_n x_n^k = 0 \end{cases},$$

com coeficientes $a_j, b_j \in \mathbb{Z}$, tem uma solução p-ádica não-trivial para todo primo p, tal que $p > k^6$.

O resultado acima foi de certa forma generalizado, por Atkinson, Brüdern e Cook, ver [1].

Teorema 2.25 (Atkinson, Brüdern e Cook). *Sejam r, k e n inteiros positivos tais que $k > 1$ e $n > 2rk$. Então o sistema de equações*

$$F_i(x) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \qquad i = 1, \ldots, r,$$

com coeficientes $a_{ij} \in \mathbb{Z}$, tem uma solução p-ádica não-trivial para todo primo p, tal que $p > k^{2r+2}$.

O resultado de Meir será discutido na próxima seção, mas sua relevância se deve ao fato de garantir solução p-ádica não-trivial para um sistema de duas formas aditivas, sob as mesmas condições do número de variáveis do Teorema 2.24, para todos os primos tais que $p > 3k^4$, ou seja, tal resultado garante a existência de zeros p-ádicos não-triviais para um conjunto maior de primos do que aquele proposto por Atkinson e Cook.

Um fato importante que podemos destacar é a relação existente entre o número de variáveis do sistema considerado e a garantia de solubilidade para ele, isto é, garantir a existência de solução p-ádica não-trivial para o sistema para todo primo p, ou para todo primo suficientemente grande, é necessário no sistema uma quantidade mínima de variáveis. No caso de p suficientemente grande, a melhor cota para o número de váriaveis é de $4k + 1$, onde k é o grau do sistema. Por outro lado, como é esperado pela conjectura de Artin, para garantir solubilidade para todo primo, veremos que é necessário no mínimo $2k^2 + 1$ variáveis e tal cota é a melhor possível para este caso.

Nas próximas observações, apresentamos dois sistemas com $4k$ e $2k^2$ variáveis que possuem somente solução trivial.

Observação 2.26. *Exemplo de um sistema de duas formas aditivas em $4k$ variáveis que possui somente a solução trivial.*

Consideremos o seguinte sistema de equações:

$$\begin{cases} f = \displaystyle\sum_{i=1}^{k} p^{i-1}(x_i^k - qy_i^k) & = 0 \\ g = \displaystyle\sum_{i=k+1}^{2k} p^{i-(k+1)}(\overline{x_i}^k - q\overline{y_i}^k) & = 0 \end{cases} \tag{2.7}$$

onde q não é uma k-ésima potência módulo p.

Suponhamos que o sistema (2.7) possui solução p-ádica não-trivial. Observamos que para resolver o sistema (2.7), basta resolvermos as equações que o constituem separadamente, pois, as equações não possuem variáveis em comum.

Dessa maneira, seja $\overrightarrow{\xi} = (\xi_1, \ldots, \xi_{2k})$ uma solução não-trivial para a primeira equação do sistema (2.7). Sem perda de generalidade, podemos supor que existe alguma coordenada coprima com p.

Assim, $f(\overrightarrow{\xi}) = 0$, ou seja, $\xi_1^k - q\xi_2^k \equiv 0 \pmod{p}$. Como q não é uma k-ésima potência segue que $\xi_1 = \xi_2 \equiv 0 \pmod{p}$, ou seja,

$$\xi_1 = p\xi_1' \text{ e } \xi_2 = p\xi_2', \tag{2.8}$$

para algum ξ_1' e ξ_2'.

Por outro lado, temos que

$$f(\overrightarrow{\xi}) = \xi_1^k - q\xi_2^k + \sum_{i=2}^{k} p^{i-1}(\xi_{2i-1}^k - q\xi_{2i}^k) = 0. \tag{2.9}$$

Substituindo (2.8) em (2.9) vemos $\dfrac{f(\overrightarrow{\xi})}{p} = 0$, ou seja, $\xi_3^k - q\xi_4^k \equiv 0 \pmod{p}$.

Analogamente concluímos que $\xi_3 = \xi_4 \equiv 0 \pmod{p}$, visto que q não é uma k-ésima potência. Repetindo este processo obteremos que ξ é uma solução com nenhuma coordenada coprima com p, o que é um absurdo. Logo a forma f possui somente o zero trivial. Repetindo este mesmo raciocínio, concluímos que g possui somente solução trivial.

Dessa forma o sistema (2.7) não possui solução além da trivial.

Observação 2.27. *Segundo a Conjectura de Artin, um sistema de duas formas aditivas de grau k e n variáveis possui zeros p-ádicos não-triviais desde que $n > 2k^2$. Quando k é ímpar a validade de tal conjectura foi verificada por Davenport e Lewis. Embora não esteja totalmente verificada sabemos que $2k^2$ é a melhor cota para o número de variáveis presente no sistema pois, existem expoentes para os quais é possível determinar sistemas com $2k^2$ variáveis e que não possuem solução não-trivial, como veremos no seguinte exemplo.*

Consideremos $k \in \mathbb{Z}$ tal que $k + 1 = p$, onde p é um número primo. É bem conhecido que $x^k \equiv 0$ ou $1 \pmod{p}$. Dessa forma, é fácil perceber que, a equação $x_1^k + \cdots + x_k^k$ possui somente zero trivial módulo p. Sendo assim, consideremos o sistema abaixo:

$$\begin{cases} F = \sum_{i=0}^{k-1} p^i(x_{1i}^k + \cdots + x_{ki}^k) & = 0 \\ G = \sum_{i=k}^{2k-1} p^{i-k}(\overline{x_{1(i-k)}}^k + \cdots + \overline{x_{k(i-k)}}^k) & = 0 \end{cases} \tag{2.10}$$

Iremos mostrar que F e G possuem somente solução trivial, afinal, qualquer solução do sistema (2.10) é formada pelas soluções de F e G, pois, F e G são equações independentes.

De fato, suponhamos que F possua zero não-trivial, isto é, existe $\overrightarrow{\xi}$ tal que $F(\overrightarrow{\xi}) = 0$. Seja $\overrightarrow{\xi} = (\xi_{10}, \ldots, \xi_{k0}, \xi_{11}, \ldots, \xi_{k1}, \ldots, \xi_{1(k-1)}, \ldots, \xi_{k(k-1)})$. Sem perda de generalidade, podemos supor que existem índices i e j tais que ξ_{ij} é coprimo com p.

Podemos olhar F de uma outra maneira, isto é, escrevemos F da seguinte forma: $F = \sum_{i=0}^{k-1} p^i f_i$, onde $f_i = x_{1i}^k + \cdots + x_{ki}^k$, para $i = 0, 1, \ldots, k-1$. Considerando $\overrightarrow{\xi_i} = (\xi_{1i}, \ldots, \xi_{ki})$, para $i = 0, 1, \ldots, k-1$, segue pelo fato de $\overrightarrow{\xi}$ ser zero de F que

$$F(\overrightarrow{\xi}) = f_0(\overrightarrow{\xi_0}) + pf_1(\overrightarrow{\xi_1}) + \cdots + p^{k-1} f_{k-1}(\overrightarrow{\xi_{k-1}}) = 0. \tag{2.11}$$

Logo, em (2.11), temos que $F(\overrightarrow{\xi}) \equiv 0 \pmod{p}$, ou seja, $\xi_{10}^k + \cdots + \xi_{k0}^k \equiv 0 \pmod{p}$, donde segue pela observação feita inicialmente que $\xi_{i0} \equiv 0 \pmod{p}$, para $i = 1, \ldots, k$, isto é, $\overrightarrow{\xi_0} \equiv 0 \pmod{p}$, ou ainda, $\overrightarrow{\xi_0} = p\overrightarrow{\omega_0}$.

Dessa forma, em (2.11), obtemos que

$$F(\overrightarrow{\xi}) = p^k f_0(\overrightarrow{\omega_0}) + pf_1(\overrightarrow{\xi_1}) + \cdots + p^{k-1} f_{k-1}(\overrightarrow{\xi_{k-1}}).$$

Mas, $\dfrac{F(\overrightarrow{\xi})}{p} = 0$, ou seja,

$$f_1(\overrightarrow{\xi_1}) + \cdots + p^{k-2} f_{k-1}(\overrightarrow{\xi_{k-1}}) + p^{k-1} f_0(\overrightarrow{\omega_0}) = 0.$$

Analogamente, obtemos que $\overrightarrow{\xi_1} = p\overrightarrow{\omega_1}$. Repetindo este processo, concluímos que $\overrightarrow{\xi_i} = p\overrightarrow{\omega_i}$ para $i = 1, \ldots, k-1$. O que contradiz o fato de $\overrightarrow{\xi}$ ser solução com pelo menos uma coordenada coprima com p. Portanto F possui somente solução trivial. Do mesmo modo, concluímos que G possui somente solução trivial. Portanto a única solução do sistema (2.10) é a trivial.

2.3 Teorema de Meir

Nesta seção discutimos o resultado sobre zeros p-ádicos não-triviais de pares de formas aditivas que se deve a Meir, ver [13]. Para isto, utilizamos diversos resultados apresentados anteriormente.

Lema 2.28. *Sejam $k \in \mathbb{N}$, p número primo e $d = mdc(k, p-1)$. Então a congruência $x^k \equiv m \pmod{p}$ tem solução se, e somente se, a congruência $x^d \equiv m \pmod{p}$ tem solução.*

Demonstração: Para mostrar o lema, basta mostrarmos que toda k-ésima potência módulo p é uma d-ésima potência módulo p e vice-versa.

Para isto, vamos definir $A_k = \left\{ x^k \;\middle|\; x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}} \right\}$ e $A_d = \left\{ x^d \;\middle|\; x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}} \right\}$. Desse modo, devemos verificar que $A_k = A_d$.

Seja $x \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ com $x \neq 0$.

Como $d = mdc(k, p-1)$ segue que existem inteiros x_0 e y_0 tais que $kx_0 + (p-1)y_0 = d$. Logo $x^d = x^{kx_0+(p-1)y_0} = (x^{x_0})^k (x^{p-1})^{y_0} = (x^{x_0})^k$, isto é, $x^d \in A_k$, e assim, $A_d \subset A_k$.

Por outro lado, temos que $d \mid k$, isto é, $k = dr$ para algum inteiro r.

Assim $x^k = x^{dr} = (x^r)^d$, ou seja, $x^k \in A_d$, isto é, $A_k \subset A_d$.

Portanto $A_d = A_k$, o que conclui a demonstração. ∎

Teorema 2.29 (Meir). *Sejam n, k inteiros positivos com $k > 1$ e $n > 4k$. Então o sistema de equações*

$$\begin{cases} f(x) &= a_1 x_1^k + \cdots + a_n x_n^k &= 0 \\ g(x) &= b_1 x_1^k + \cdots + b_n x_n^k &= 0 \end{cases},$$

com coeficientes a_i, b_i inteiros, tem uma solução p-ádica não-trivial para $p > 3k^4$.

Demonstração: Pelo Lema 2.28 podemos assumir, sem perda de generalidade, que $k \mid (p-1)$.

Como $p > 3k^4$ segue que $mdc(p, k) = 1$ e assim pela Definição 2.7 temos que $\gamma = 1$.

Pela seção anterior, consideramos também que f e g formam um sistema p-normalizado. Afim de garantir solução p-ádica para o sistema utilizamos o Lema 2.8, isto é, mostramos que o sistema

$$\begin{cases} f_0 \equiv 0 \pmod{p} \\ g_0 \equiv 0 \pmod{p} \end{cases}, \tag{2.12}$$

tem uma solução $(\xi_1, \ldots, \xi_{m_0})$ tal que a matriz $\begin{pmatrix} a_1\xi_1 & \ldots & a_{m_0}\xi_{m_0} \\ b_1\xi_1 & \ldots & b_{m_0}\xi_{m_0} \end{pmatrix}$ tenha posto 2 módulo p.

Por hipótese temos que $n > 4k$, assim, segue do Lema 2.6 que $m_0 \geq \dfrac{n}{k} > \dfrac{4k}{k}$ e $q_0 \geq \dfrac{n}{2k} > \dfrac{4k}{2k}$, ou seja,

$$m_0 \geq 5 \tag{2.13}$$

e

$$q_0 \geq 3. \tag{2.14}$$

Agora, agrupemos as variáveis presentes no par f_0, g_0 segundo suas respectivas cores. Sabemos pelo Lema 2.13 que podemos considerar $\mathbb{I}_0 \geq \mathbb{I}_v$ para todo v, $0 \leq v \leq p$. Seja $r = \mathbb{I}_0$ e seja t a quantidade de váriaveis do segundo maior grupo de variáveis de mesma cor, as quais podemos assumir serem da cor p, isto é, $t = \mathbb{I}_p$.

Suponhamos que $t \geq 3$. Logo devemos ter $r \geq 3$. Como $p > 3k^4 > k^4$, segue pelo Lema 1.20 que as cores 0 e p são representantes de zero, donde concluímos pelo Lema 2.17 que o sistema (2.12) tem solução não-singular.

Assim podemos supor que $t \leq 2$. A partir deste ponto consideraremos, dentre as m_0 variáveis, um subsistema com 5 variáveis (se necessário descartando o excesso de variáveis). Respeitando a condição (2.14), isto é, $q_0 \geq 3$, chegamos a seguinte conclusão: $r = 1$ e $q_0 = 4$ ou $r = 2$ e $q_0 = 3$, visto que $t \leq 2$.

2.3.1 Caso: r = 2

Por um simples argumento envolvendo escalonamento, e após uma reenumeração de variáveis, podemos supor que o sistema tenha a seguinte forma:

$$\begin{cases} f_0 &= x_1^k + a_2x_2^k + a_3x_3^k + a_4x_4^k + a_5x_5^k \equiv 0 \pmod{p} \\ g_0 &= b_3x_3^k + b_4x_4^k + b_5x_5^k \equiv 0 \pmod{p} \end{cases}, \tag{2.15}$$

Agora, precisamos mostrar que o sistema (2.15) admite uma solução não-singular.

Como $r = 2$ podemos constatar no sistema (2.15) que $b_3b_4b_5 \not\equiv 0 \pmod{p}$.

Lema 2.30. *Seja $p \equiv 1 \pmod{k}$. Se $r = 2$, então o sistema (2.15) tem uma solução de posto 2 módulo p, desde que $p > k^4$.*

Demonstração: Estamos assumindo que $p > k^4$. Segue, pelo Lema 1.20, que a congruência $b_3x_3^k + b_4x_4^k + b_5x_5^k \equiv 0 \pmod{p}$ tem solução com $x_3x_4x_5 \not\equiv 0 \pmod{p}$, visto que estamos considerando $p > k^4$.

Seja $A = a_3x_3^k + a_4x_4^k + a_5x_5^k$. Se $A \equiv 0 \pmod{p}$, então basta fazer $x_1 = x_2 = 0$ para obtermos uma solução para o sistema (2.15) e a solução é de posto 2 módulo p pois, a solução $(0, 0, x_3, x_4, x_5)$ envolve pelo menos duas colunas de coeficientes em cores diferentes.

Agora se $A \not\equiv 0 \pmod{p}$, então consideramos a seguinte congruência

$$x_1^k + a_2x_2^k + Ay^k \equiv 0 \pmod{p},$$

onde y é uma nova variável. Aplicando novamente o Lema 1.20, a congruência acima possui solução com $x_1x_2y \not\equiv 0 \pmod{p}$. Dessa maneira $(x_1, x_2, yx_3, yx_4, yx_5)$ é uma solução do sistema (2.15), visto que (x_3, x_4, x_5) é solução da segunda congruência do sistema. Pelo mesmo motivo do caso $A \equiv 0 \pmod{p}$ temos que a solução é de posto 2 módulo p. ∎

2.3.2 Caso: r = 1

Por raciocínio análogo ao caso anterior, podemos supor que neste caso, o sistema possui a seguinte forma:

$$\begin{cases} f_0 &= x_1^k + &&+a_3x_3^k + a_4x_4^k + a_5x_5^k \equiv 0 \pmod{p} \\ g_0 &= &x_2^k &+b_3x_3^k + b_4x_4^k + b_5x_5^k \equiv 0 \pmod{p} \end{cases}, \tag{2.16}$$

Dessa maneira, precisamos mostrar que o sistema (2.16) admite uma solução não-singular.

Observamos que qualquer solução não-trivial do sistema (2.16) terá pelo menos duas coordenadas não nulas. E esta solução é de posto 2, pois, envolve pelo menos duas colunas de coeficientes em cores diferentes, pois estamos assumindo que $r = 1$.

Seja N o número de soluções do sistema (2.16). Assim pelo Lema 1.11 segue que

$$\sum_{u=0}^{p-1} \xi^{u(x_1^k+a_3x_3^k+a_4x_4^k+a_5x_5^k)} \sum_{v=0}^{p-1} \xi^{v(x_2^k+b_3x_3^k+b_4x_4^k+b_5x_5^k)} = \begin{cases} p^2, \text{ se } (x_1,\ldots,x_5) \text{ é solução de (2.16)} \\ 0, \quad \text{caso contrário} \end{cases}. \tag{2.17}$$

De (2.17) obtemos que

$$Np^2 = \sum_{x_1=0}^{p-1}\sum_{x_2=0}^{p-1}\sum_{x_3=0}^{p-1}\sum_{x_4=0}^{p-1}\sum_{x_5=0}^{p-1}\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} \xi^{ux_1^k+vx_2^k+(a_3u+b_3v)x_3^k+(a_4u+b_4v)x_4^k+(a_5u+b_5v)x_5^k}. \tag{2.18}$$

Fazendo $\Lambda_1 = u$, $\Lambda_2 = v$, $\Lambda_3 = a_3u + b_3v$, $\Lambda_4 = a_4u + b_4v$ e $\Lambda_5 = a_5u + b_5v$ podemos reescrever (2.18) como

$$Np^2 = \sum_{u=0}^{p-1}\sum_{v=0}^{p-1} T(\Lambda_1)T(\Lambda_2)T(\Lambda_3)T(\Lambda_4)T(\Lambda_5),$$

onde $T(\Lambda)$ é definido em 1.7.

Assim

$$Np^2 = p^5 + \sum_{(u,v)\neq(0,0)} T(\Lambda_1)T(\Lambda_2)T(\Lambda_3)T(\Lambda_4)T(\Lambda_5),$$

visto que $T(0) = p$.

Assim

$$Np^2 - p^5 = \sum_{(u,v)\neq(0,0)} T(\Lambda_1)T(\Lambda_2)T(\Lambda_3)T(\Lambda_4)T(\Lambda_5). \tag{2.19}$$

Separemos a soma do lado direito de (2.19) em duas somas: Σ_1 e Σ_0, onde Σ_1 corresponde a soma dos termos onde pelo menos um dos Λ_i é zero módulo p e Σ_0 corresponde a soma dos termos onde nenhum dos Λ_i é zero módulo p.

Logo da relação (2.19) obtemos que

$$Np^2 - p^5 = \Sigma_0 + \Sigma_1. \tag{2.20}$$

A partir de agora o nosso objetivo é encontrar uma estimativa para N. Para isto estimaremos Σ_0 e Σ_1.

Estimativa de Σ_0

Temos que

$$\Sigma_0 = \sum_{\substack{(u,v)\neq(0,0)\\ \Lambda_i \not\equiv 0 \pmod p}} T(\Lambda_1)T(\Lambda_2)T(\Lambda_3)T(\Lambda_4)T(\Lambda_5). \tag{2.21}$$

Pelo Lema 1.12 temos que $T(\Lambda_i) = \sum_{s=1}^{k-1} \chi_s(\Lambda_i)\tau(\overline{\chi_s})$, onde χ não é o caráter trivial, visto que $k \mid (p-1)$ e $mdc(\Lambda_i, p) = 1$. Assim em (2.21) obtemos que

$$\Sigma_0 = \sum_{\substack{(u,v)\neq(0,0)\\ \Lambda_i \not\equiv 0 \pmod p}} \left(\sum_{r_1=1}^{k-1} \chi_{r_1}(\Lambda_1)\tau(\overline{\chi_{r_1}})\right) \ \dots \ \left(\sum_{r_5=1}^{k-1} \chi_{r_5}(\Lambda_5)\tau(\overline{\chi_{r_5}})\right),$$

ou seja,

$$\Sigma_0 = \sum_{\substack{(u,v)\neq(0,0)\\ \Lambda_i \not\equiv 0 \pmod p}} \sum_{\substack{r_1,\dots,r_5\\ 1\le r_i\le k-1}} \chi_{r_1}(\Lambda_1)\dots\chi_{r_5}(\Lambda_5)\tau(\overline{\chi_{r_1}})\dots\tau(\overline{\chi_{r_5}}).$$

Logo,

$$\Sigma_0 = \sum_{\substack{r_1,\dots,r_5\\ 1\le r_i\le k-1}} \tau(\overline{\chi_{r_1}})\dots\tau(\overline{\chi_{r_5}}) \sum_{\substack{(u,v)\neq(0,0)\\ \Lambda_i \not\equiv 0 \pmod p}} \chi(\Lambda_1^{r_1}\Lambda_2^{r_2}\Lambda_3^{r_3}\Lambda_4^{r_4}\Lambda_5^{r_5}), \tag{2.22}$$

visto que χ é multiplicativo.

Seja $S = \sum_{\substack{(u,v)\neq(0,0)\\ \Lambda_i \not\equiv 0 \pmod p}} \chi(\Lambda_1^{r_1}\Lambda_2^{r_2}\Lambda_3^{r_3}\Lambda_4^{r_4}\Lambda_5^{r_5})$. Como $\Lambda_i = a_iu + b_iv$, segue que

$$S = \sum_{\substack{(u,v)\neq(0,0)\\ \Lambda_i \not\equiv 0 \pmod p}} \chi\left(\prod_{i=1}^{5}(a_iu+b_iv)^{r_i}\right) = \sum_{\substack{(u,v)\neq(0,0)\\ \Lambda_i \not\equiv 0 \pmod p}} \chi\left(\prod_{i=1}^{5}\left(v\left(a_i\frac{u}{v}+b_i\right)\right)^{r_i}\right),$$

onde colocamos v em evidência pois, $v = \Lambda_2 \not\equiv 0 \pmod{p}$. Portanto

$$S = \sum_{\substack{(u,v) \neq (0,0) \\ \Lambda_i \not\equiv 0 \pmod{p}}} \chi\left(v^{r_1+r_2+r_3+r_4+r_5} \prod_{i=1}^{5} \left(a_i \frac{u}{v} + b_i\right)^{r_i}\right). \tag{2.23}$$

Como $u = \Lambda_1 \not\equiv 0 \pmod{p}$ e $v = \Lambda_2 \not\equiv 0 \pmod{p}$, podemos em (2.23) substituir o somatório $\sum_{\substack{(u,v) \neq (0,0) \\ \Lambda_i \not\equiv 0 \pmod{p}}}$ pelo duplo somatório, $\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}$. Afinal se $\Lambda_j \equiv 0 \pmod{p}$ para algum j, então $\chi\left(\prod_{i=1}^{5} \Lambda_i^{r_i}\right) = 0$ e este termo não contribui com a soma.

Assim em (2.23) temos que

$$S = \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} \chi\left(v^{r_1+r_2+r_3+r_4+r_5} \prod_{i=1}^{5} \left(a_i \frac{u}{v} + b_i\right)^{r_i}\right). \tag{2.24}$$

Façamos $\lambda = \dfrac{u}{v}$. Para cada v fixado, com $v \in \{1, \ldots, p-1\}$, temos que λ percorre este mesmo conjunto quando u também o percorre. Dessa forma, juntamente com o fato de χ ser multiplicativo, segue de (2.24) que

$$S = \sum_{v=1}^{p-1} \chi(v^{r_1+r_2+r_3+r_4+r_5}) \sum_{\lambda=1}^{p-1} \chi\left(\prod_{i=1}^{5} (a_i\lambda + b_i)^{r_i}\right) \tag{2.25}$$

Seja $R = r_1 + r_2 + r_3 + r_4 + r_5$, e suponhamos que $R \not\equiv 0 \pmod{k}$. Logo, pelo fato de χ ser multiplicativo, temos

$$\sum_{v=1}^{p-1} \chi(v^R) = \sum_{v=1}^{p-1} \chi^R(v) = 0,$$

onde a última igualdade é devido ao Lema 1.5 visto que χ^R não é o caráter trivial, pois χ é de ordem k. Neste caso concluímos em (2.25) que

$$S = 0. \tag{2.26}$$

Agora suponhamos que $R \equiv 0 \pmod{k}$. Assim $R = kw$, para algum inteiro w. Daí como χ é multiplicativo e tem ordem k segue

$$\sum_{v=1}^{p-1} \chi(v^R) = \sum_{v=1}^{p-1} \chi^R(v) = \sum_{v=1}^{p-1} 1 = p - 1.$$

Nessas condições obtemos em (2.25) que

$$S = (p-1)\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1}^{5}(a_i\lambda + b_i)^{r_i}\right) \tag{2.27}$$

Observe que $a_2 \equiv 0 \pmod{p}$ e $b_2 \equiv 1 \pmod{p}$, pois $\Lambda_2 = v$. Dessa maneira

$$\prod_{i=1}^{5}(a_i\lambda + b_i)^{r_i} = \prod_{i=1,\ i\neq 2}^{5}(a_i\lambda + b_i)^{r_i}. \tag{2.28}$$

Assumindo ainda que $R \equiv 0 \pmod{k}$, obtemos de (2.27) e (2.28) que

$$|S| = (p-1)\left|\sum_{\lambda=1}^{p-1}\chi\left(\prod_{i=1,\ i\neq 2}^{5}(a_i\lambda + b_i)^{r_i}\right)\right|. \tag{2.29}$$

Como $a_i \not\equiv 0 \pmod{p}$ para $i = 1, 3, 4, 5$ e como estamos no caso $r = 1$, temos que as hipóteses do Corolário 1.36 são satisfeitas e então em (2.29) obtemos

$$|S| \leq (p-1)(3\sqrt{p}+1). \tag{2.30}$$

Voltando em (2.22) temos que

$$\Sigma_0 = \sum_{\substack{r_1+\cdots+r_5 \equiv 0 \pmod{k} \\ 1\leq r_i \leq k-1}} \tau(\overline{\chi_{r_1}})\ldots\tau(\overline{\chi_{r_5}})S + \sum_{\substack{r_1+\cdots+r_5 \not\equiv 0 \pmod{k} \\ 1\leq r_i \leq k-1}} \tau(\overline{\chi_{r_1}})\ldots\tau(\overline{\chi_{r_5}})S. \tag{2.31}$$

Por (2.26) obtemos em (2.31) que

$$\Sigma_0 = \sum_{\substack{r_1+\cdots+r_5 \equiv 0 \pmod{k} \\ 1\leq r_i \leq k-1}} \tau(\overline{\chi_{r_1}})\ldots\tau(\overline{\chi_{r_5}})S \tag{2.32}$$

Pelo Teorema 1.13 e pela relação (2.30) obtemos em (2.32) que

$$|\Sigma_0| \leq p^{\frac{5}{2}}|S| \sum_{\substack{r_1+\cdots+r_5 \equiv 0 \pmod{k} \\ 1\leq r_i \leq k-1}} 1 \leq p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1) \sum_{\substack{r_1+\cdots+r_5 \equiv 0 \pmod{k} \\ 1\leq r_i \leq k-1}} 1 \tag{2.33}$$

Mas $\#\{r_1+\cdots+r_5 \equiv 0 \pmod{k}; 1 \leq r_i \leq k-1, i = 1,\ldots,5\} \leq (k-1)^4$, logo na relação (2.33) obtemos que

$$|\Sigma_0| \leq p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4. \tag{2.34}$$

Estimativa de Σ_1

Sabemos que Σ_1 corresponde a soma onde pelo menos um dos Λ_i é zero módulo p. Observamos que não podemos ter simultaneamente $\Lambda_i \equiv 0 \pmod{p}$ e $\Lambda_j \equiv 0 \pmod{p}$ para $i \neq j$. De fato, caso contrário teremos

$$a_i u + b_i v \equiv 0 \pmod{p} \quad \text{e} \quad a_j u + b_j v \equiv 0 \pmod{p},$$

que resulta $\frac{a_i}{b_i} \equiv \frac{a_j}{b_j} \pmod{p}$, o que é um absurdo, pois $r = 1$.

Seja Σ' a parte de Σ_1 onde em cada parcela ocorre $\Lambda_1 \equiv 0 \pmod{p}$. Isto é

$$\Sigma' = \sum_{\substack{(u,v) \neq (0,0) \\ u = \Lambda_1 \equiv 0 \pmod{p}}} T(0)T(\Lambda_2)T(\Lambda_3)T(\Lambda_4)T(\Lambda_5).$$

Logo,

$$\Sigma' = p \sum_{v=1}^{p-1} \left(\prod_{i=2}^{5} T(b_i v) \right), \tag{2.35}$$

visto que $T(0) = p$.

Como $mdc(b_i, p) = 1$ para $i = 2, \ldots, 5$, obtemos da relação (2.35) utilizando a Desigualdade de Hölder que

$$|\Sigma'| \leq p \sum_{v=1}^{p-1} \left(\prod_{i=2}^{5} |T(b_i v)| \right) \leq p \sum_{v=1}^{p-1} |T(v)|^4. \tag{2.36}$$

Aplicando o Lema 1.16 para $n = 4$ em (2.36), obtemos que $|\Sigma'| \leq pp^3(k-1)^3$, ou seja,

$$|\Sigma'| \leq p^4(k-1)^3. \tag{2.37}$$

Repetindo o mesmo raciocínio para as somas cujas parcelas possuem algum $\Lambda_i \equiv 0 \pmod{p}$, a estimativa a ser obtida é a mesma da relação (2.37). Sendo assim, obtemos que

$$|\Sigma_1| \leq 5p^4(k-1)^3. \tag{2.38}$$

Conclusão do caso $r = 1$

Por (2.34) e (2.38) temos estimativas para Σ_0 e Σ_1, respectivamente. Dessa maneira em (2.20), temos que

$$|Np^2 - p^5| \leq |\Sigma_0| + |\Sigma_1| \leq p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4 + 5p^4(k-1)^3.$$

Logo devemos ter

$$Np^2 \geq p^5 - p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4 - 5p^4(k-1)^3,$$

de onde segue que se dividirmos ambos os membros por p^2 obteremos

$$N \geq p^3 - p^{\frac{1}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4 - 5p^2(k-1)^3. \tag{2.39}$$

Afim de que o sistema (2.16) tenha solução não-trivial, basta mostrarmos que $N > 1$. Para isto, analisando a ordem de grandezas, é suficiente mostrar que

$$p > p^{-\frac{3}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4 + 5(k-1)^3. \tag{2.40}$$

Iniciemos a verificação da relação (2.40).

Para $k \in \mathbb{N}$ temos que $(k-1)^4 < k^4 < \sqrt{3}k^4$, ou seja, $\dfrac{(k-1)^4}{\sqrt{3}k^2} < k^2$.

Por hipótese temos que $p > 3k^4$. Logo $\dfrac{1}{\sqrt{p}} < \dfrac{1}{\sqrt{3}k^2}$. Assim,

$$\frac{(k-1)^4}{\sqrt{p}} < \frac{(k-1)^4}{\sqrt{3}k^2} < k^2. \tag{2.41}$$

Da relação (2.41) segue que

$$\left(3 + \frac{1}{\sqrt{p}}\right)(k-1)^4 = 3(k-1)^4 + \frac{(k-1)^4}{p^{\frac{1}{2}}} < 3(k-1)^4 + k^2. \tag{2.42}$$

Mas $\dfrac{p-1}{p} < 1$, logo em (2.42) obtemos

$$\left(\frac{p-1}{p}\right)\left(3 + \frac{1}{\sqrt{p}}\right)(k-1)^4 < 3(k-1)^4 + k^2,$$

acrescentando $5(k-1)^3$ em ambos os membros da desigualdade, vemos que

$$\left(\frac{p-1}{p}\right)\left(3+\frac{1}{\sqrt{p}}\right)(k-1)^4+5(k-1)^3 \quad < \quad 3(k-1)^4+k^2+5(k-1)^3.$$

Agora efetuando a multiplicação do denominador do lado esquerdo da expressão acima e desenvolvendo os cálculos do lado direito, obtemos

$$p^{-\frac{3}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4+5(k-1)^3 \quad < \quad 3k^4-7k^3+4k^2+3k-2. \tag{2.43}$$

Observe que $7k^2+3k>0$ para todo $k\in\mathbb{N}$. Logo $7k^2(k-1)+3k(k-1)>0$, e assim

$$7k^2(k-1)+3k(k-1)+2>0, \quad \text{ou seja,} \quad 7k^3-4k^2-3k+2>0,$$

isto é,

$$-7k^3+4k^2+3k-2<0. \tag{2.44}$$

De (2.44) e lembrando que $p>3k^4$ teremos em (2.43) que

$$p^{-\frac{3}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4+5(k-1)^3 \quad < \quad 3k^4 \quad < \quad p,$$

ou seja, a relação (2.40) é verdadeira.

Assim concluímos o caso $r=1$. E portanto o Teorema está demonstrado. ∎

Referências Bibliográficas

[1] O. D. Atkinson, J. Brüdern,; R. J. Cook, *Simultaneous additive congruences to a large prime modulus*, Mathematika, 39 (1992), pp. 1–9.

[2] O. D. Atkinson; R. J. Cook, *Pairs of additive congruences to a large prime modulus*, J. Austral. Math. Soc. Ser. A, 46 (1989), pp. 438–455.

[3] G. S. S. Ávila, *Funções de uma Variáveil Complexa*, Editora Universidade de Brasília, 1974.

[4] J. Ax; S. Kochen, *Diophantine problems over local fields. I*, Amer. J. Math., 87 (1965), pp. 605–630.

[5] J. Brüdern; H. Godinho, *On Artin's conjecture. II. Pairs of additive forms*, Proc. London Math. Soc. (3), 84 (2002), pp. 513–538.

[6] E. F. da Silva, *Número de soluções de equações diagonais sobre corpos finitos*, Dissertação de Mestrado, Universidade de Brasília, 1994.

[7] H. Davenport; D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. Ser. A, 274 (1963), pp. 443–460.

[8] ——, *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. London Ser. A, 264 (1969), pp. 557–595.

[9] J. F. de Lima Neto, *Condições de solubilidade p-ádica para pares de formas aditivas de grau ímpar e um resultado sobre várias formas aditivas de grau p*, Tese de Doutorado, Universidade de Brasília, 2005.

[10] H. Godinho, *Polinômios homogêneos sobre números p-ádicos.* Textos e Notas de Matemática da Universidade de Lisboa, 2000.

[11] L. K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin, 1982. Translated from the Chinese by Peter Shiu.

[12] R. Lidl; H. Niederreiter, *Finite fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

[13] I. D. Meir, *Pairs of additive congruences to a large prime modulus*, J. Number Theory, 63 (1997), pp. 132–142.

[14] J. E. Olson, *A combinatorial problem on finite Abelian groups. I*, J. Number Theory, 1 (1969), pp. 8–10.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo