Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Condições de Solubilidade p-Ádica para Formas Aditivas de Grau Ímpar

por

Juliana Paula Riani Motinha

Brasília
2008

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Condições de Solubilidade p-Ádica para Formas Aditivas de Grau Ímpar

por

Juliana Paula Riani Motinha*

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 22 de julho de 2008.

Comissão Examinadora:

Prof. Dr. Hemar Teixeira Godinho - UnB (Orientador)

Prof. Dra. Aline Gomes da Silva Pinto - UnB (Membro)

Prof. Dr. Paulo Henrique de Azevedo Rodrigues - UFG (Membro)

*A autora foi bolsista do CNPq durante a elaboração deste trabalho.

Aos meus pais,
Ana Maria e José Motinha;
amo muito vocês...

Agradecimentos

Agradeço primeiramente a Deus, se hoje estou aqui é graças à Ele.

Aos meus pais Ana Maria de Paula Riani Motinha e José Motinha da Costa, por terem me apoiado sempre, por conseguirem na distância estarem sempre ao meu lado, pelo imenso carinho... Vocês fazem parte de tudo em minha vida.

Ao professor Hemar pela orientação, pelo respeito e cordialidade com que sempre me falou e chamou a atenção quando precisei. Aprendi muito e esta lição vou levar para toda minha vida.

Ao CNPq/CAPES pelo apoio financeiro.

Aos funcionários da secretaria do MAT, Tânia, Gari, Manoel, Luiz, Eveline que sempre nos ajudaram.

Ao Sérgio, meu amor, pelo companheirismo e carinho... agora seremos um só... Agradeço também à sua família que me acolheu e hoje também são minha família.

Aos meus familiares, tios e tias, primos, primas e avós. A todos que se alegraram com minha conquista, que torceram para que eu conseguisse realizar mais essa etapa. Agradeço em especial à minha vó Olga, que reza sempre por mim... obrigada vozinha!

Agradeço ao Leo Dog, Vagto, Miguxa, Flavinha e Zapata por tantos momentos bons, tantas risadas na cozinha... Até bem pouco tempo não nos conhecíamos e dividimos nossa vida...

Aos amigos Flávio, Igor, Jeferson, João, Lu, Manu, Michael, Paty, Simone, Susanne e Washington pela torcida de sempre e pelas cinucas de vez em quando... Agradeço em especial à Su que dividiu comigo sua casa e sua família quando precisei.

A todos os amigos que fiz durante a graduação e no mestrado, sei que não é possível citar todos os nomes, são tantos... São amigos de disciplinas, de dias de estudos para os exames, de banquinho... Vou lembrá-los sempre com muito carinho...

Aos amigos que fizeram parte de minha vida lá em Alvarenga, sei que eles torcem muito por mim. Todos eles estão longe, mas nosso carinho é para sempre...

Todas as pessoas que passaram em minha vida e deixaram boas lembraças merecem meu agradecimento, pois todas fazem parte de uma história de felicidade e esta história foi fundamental para contrução dessa realidade que vivo hoje. Obrigada a todos...

Resumo

O presente trabalho é baseado nos artigos de Tietäväinen e Low, Pitman e Wolff, onde ambos investigam condições para solubilidade p-ádica de formas aditivas, em n variáveis, de grau k ímpar. É verificado para uma forma que, se $n \geq [(\log 2)^{-1} k \log k]$, então esta forma possui zeros p-ádicos não triviais, para todo primo p. Posteriormente, estudamos sistemas de R formas de mesmo grau. Uma característica importante deste trabalho é a técnica de partição de matrizes e uma definição diferenciada de sistema normalizado, diferente da introduzida por Davenport e Lewis. Com essa nova abordagem, temos uma significativa melhora nos resultados obtidos por Davenport e Lewis.

Palavras-chave: formas aditivas, grau ímpar, matrizes particionáveis, normalização

Abstract

This work is based on articles of Tietäväinen and Low, Pitman and Wolff, where both investigate conditions for p-ádic solubility from additive forms, in n variables, of odd degree k. It is checked for a form that, if $n \geq [(\log 2)^{-1} k \log k]$, then this form has non-trivial p-ádics zeros, for any prime p. Subsequently, we studied systems of R forms with the same degree. An important feature of this work is the technique of matrices' partition and a different definition of normalised system, different from that introduced by Davenport and Lewis. With this new approach, we have a significant improvement in the results obtained by Davenport and Lewis.

Keywords: additive forms, odd degree, particionable matrices, normalisation

Índice

Introdução

Na década de 20, E. Artin apresentou a seguinte conjectura: *Qualquer polinômio homogêneo de grau k em n variáveis tem zeros p-ádicos desde que $n \geq k^2 + 1$.* Os resultados de H. Hasse, em 1924, confirmaram a conjectura para formas quadráticas, (ver [2]). Posteriormente, Lewis [14] verificou a validade da conjectura para formas de grau três. Vários outros resultados apareceram, mas em 1966, Terjanian apresentou uma forma de grau quatro com 18 variáveis que não possui zeros 2-ádicos, o primeiro contra-exemplo para essa conjectura, (ver [18] ou [10]).

Pesquisas na área continuaram e do encontro de H. Davenport e D. J. Lewis seguiu-se uma série de resultados onde se buscava condições de solubilidade p-ádica não trivial para o caso particular de formas aditivas,

$$F = a_1 x_1^k + \ldots + a_n x_n^k \, .$$

Em 1963, H. Davenport e D. J. Lewis [7] mostraram que: *Toda forma aditiva de grau k com coeficientes inteiros em $n \geq k^2+1$ variáveis sempre possui zeros p-ádicos não triviais.* Para tal, eles introduziram uma técnica importante, e até hoje muito utilizada, conhecida como p-normalização. Em [3], Chowla foi o primeiro a mostrar que o número de variáveis podia ser menor quando a potência k das formas fosse ímpar. Ele também foi o primeiro a mostrar que o número de variáveis era da ordem de $k \log k$. Pesquisas se seguiram na tentativa de determinar qual constante acompanharia esse termo. Denotando por ϑ essa contante, Chowla e Shimura [4] mostraram que

$$\frac{1}{\log 2} \leq \vartheta \leq \frac{2}{\log 2} \, .$$

Tietäväinen [19] mostrou que essa constante é $1/\log 2$.

Ainda com Davenport e Lewis, pesquisas foram desenvolvidas para sistemas de formas aditivas, primeiro com duas formas e depois para R formas. Em conexão com seus estudos sobre sistemas de equações diofantinas

$$F_1 = F_2 \ldots = F_R = 0,$$

eles investigaram condições que asseguravam a existência de soluções não triviais para congruências

$$F_1 \equiv F_2 \equiv \ldots \equiv F_R \equiv 0 \pmod{p^s}$$

para toda potência de primo p^s. Em [8], eles mostraram condições para a solubilidade p-ádica para R formas de grau k e, em particular, quando k é ímpar, eles mostraram que basta

$$n \geq [9R^2k \log(3Rk)].$$

Ainda considerando R formas aditivas, Lewis Low, Jane Pitman e Alison Wolff mostraram, para formas de grau ímpar, utilizando técnicas diferentes, que o número de variáveis pode ser reduzido significativamente. Eles mostraram que

$$n \geq \left\lceil \frac{R^2k}{\log 2} \log(3Rk) \right\rceil.$$

A diferença fundamental desse trabalho para o de Davenport e Lewis [8] está no uso da partição de matrizes, que consiste em uma especialização de resultados sobre partição de matróides, (ver [1]). E também, baseado nessa técnica, temos uma diferenciação no conceito de sistema normalizado.

Nesta dissertação, consideramos formas aditivas de grau k ímpar. Iniciamos nosso trabalho com um estudo sobre somas exponenciais e apresentamos o resultado de Tietäväinen para uma forma aditiva. Descrevemos os métodos de partição de matrizes e de normalização e apresentamos também o resultado de Low, Pitman e Wolff para R formas como mencionado anteriormente.

Capítulo 1

Resultados Preliminares e Solubilidade de uma Equação Aditiva

1.1 Somas Exponenciais

Nesta seção discutiremos somas exponenciais, um método bastante utilizado para estimar o número de soluções de equações de natureza aditiva. Utilizaremos este método em alguns de nossos principais resultados neste e no próximo capítulo.

Definição 1.1. Sejam G um grupo abeliano finito e U o grupo multiplicativo das raizes da unidade em $\mathbb{C}$. Todo homomorfismo $\chi : G \longrightarrow U$ é dito ser um caráter de G.

Da definição acima decorre que todo caráter de G é uma função multiplicativa pois, sendo χ um homomorfismo, ele satisfaz

$$\chi(g_1 * g_2) = \chi(g_1)\chi(g_2),$$

onde $*$ denota a operação em G.

Considere também a seguinte definição:

Definição 1.2. Seja χ um caráter de um grupo abeliano finito G. Então

(*i*) Se $\chi(g) = 1$ para todo $g \in G$, então χ é dito ser o caráter trivial denotado também por χ_0;

(ii) O caráter conjugado de χ, denotado por $\overline{\chi}$ é definido por $\overline{\chi}(g) = \overline{\chi(g)}$;

(iii) Sejam χ e λ dois caracteres em G. Definimos o produto de χ por λ como

$$(\chi\lambda)(g) = \chi(g)\lambda(g), \text{ para todos os } g \in G.$$

Seja G^* o conjunto de todos os caracteres de G.

Lema 1.3. *Com a operação apresentada na Definição 1.2, G^* é um grupo finito com elemento neutro χ_0.*

Demonstração: Seja $\psi \neq \chi_0$ e seja $g \in G$. Então $\psi\chi_0(g) = \psi(g)\chi_0(g) = \psi(g)$, e por outro lado, $\chi_0\psi(g) = \chi_0(g)\psi(g) = \psi(g)$. Portanto, χ_0 é elemento neutro.

Seja $|G| = n$. Logo, para todo $g \in G$ temos que $g^n = e$, onde e é o elemento neutro de G. Logo, $\chi(g^n) = \chi(e) = 1$ e desta forma, $(\chi(g))^n = 1$. Mostrando assim que para todo $\chi \in G^*$ temos que $\chi^n = \chi_0$ logo, $\chi\chi^{n-1} = \chi_0$, ou seja, $\chi^{-1} = \chi^{n-1}$. Portanto, G^* é um grupo finito. ■

Dos resultados acima podemos verificar as seguintes propriedades.

Proposição 1.4. *Considere χ um caráter de um grupo abeliano finito G. Então*

(i) $\chi(e) = 1$ *e* $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$;

(ii) *Temos* $\sum_{\chi \in G^*} \chi(g) = \begin{cases} |G^*| & se \quad g = e \\ 0 & se \quad g \neq e \end{cases}$;

(iii) *Temos* $\sum_{g \in G} \chi(g) = \begin{cases} 0 & se \quad \chi \neq \chi_0 \\ |G| & se \quad \chi = \chi_0 \end{cases}$;

(iv) $|G^*| = |G|$.

Demonstração:

(i) Por definição, $\chi : G \longrightarrow U$ é um homomorfismo de grupos, logo leva elemento neutro em elemento neutro e $\chi(g^{-1}) = \chi(g)^{-1}$. E a igualdade $\chi(g)^{-1} = \overline{\chi(g)}$ segue do fato que $\chi(g)$ é raíz da unidade.

(*ii*) Seja $g = e$, por (i), $\chi(e) = 1$ para todo $\chi \in G^*$. Então

$$\sum_{\chi \in G^*} \chi(e) = \sum_{\chi \in G^*} 1 = |G^*|.$$

Por outro lado, se $g \neq e$, então existe $\psi \in G^*$ tal que $\psi(g) \neq 1$. Logo

$$\psi(g) \sum_{\chi \in G^*} \chi(g) = \sum_{\chi \in G^*} (\psi\chi)(g) = \sum_{\chi \in G^*} \chi(g),$$

pois $\psi\chi$ percorre o grupo G^* quando χ percorre G^*. Portanto $\sum\limits_{\chi \in G^*} \chi(g) = 0$.

(*iii*) Se $\chi \neq \chi_0$, então existe $a \in G$ tal que $\chi(a) \neq 1$. Portanto

$$\chi(a) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(ag) = \sum_{g \in G} \chi(g),$$

pois ag percorre G quando g percorre G. Assim obtemos

$$(\chi(a) - 1) \sum_{g \in G} \chi(g) = 0,$$

de onde concluímos que $\sum\limits_{g \in G} \chi(g) = 0$, pois $\chi(a)$ é diferente de 0 e 1.

Por outro lado, se $\chi = \chi_0$, temos

$$\sum_{g \in G} \chi_0(g) = \sum_{g \in G} 1 = |G|.$$

(*iv*) Por (ii), temos que

$$|G^*| = \sum_{g \in G} \sum_{\chi \in G^*} \chi(g) = \sum_{\chi \in G^*} \sum_{g \in G} \chi(g) = |G|,$$

onde a última igualdade segue de (iii).

■

Lema 1.5. *Sejam p um primo, $x \in \mathbb{Z}$ e $\xi \in \mathbb{C}$ uma raiz primitiva p-ésima da unidade. Então*

$$\sum_{s=0}^{p-1} \xi^{sx} = \begin{cases} p & se \quad x \equiv 0 \pmod{p} \\ 0 & se \qquad c.c. \end{cases}.$$

Demonstração: Suponha que $x = lp$. Logo $\xi^{sx} = 1$ e isto implica que $\sum_{s=0}^{p-1} 1 = p$.

Caso contrário, temos $mdc(x, p) = 1$. Nestas condições, ξ^x é também uma raiz primitiva da unidade. Como $\xi^x \neq 1$ e $(\xi^x)^p = 1$, então $(\xi^x)^p$ é raiz do polinômio $y^p - 1$. Mas, $y^p - 1 = (y-1)(y^{p-1} + \ldots + y^2 + y + 1)$, portanto

$$(\xi^x)^{p-1} + \ldots + (\xi^x)^2 + (\xi^x) + 1 = \sum_{s=0}^{p-1} \xi^{sx} = 0 \ .$$

■

Lema 1.6. *Seja $F \in \mathbb{Z}[x_1, \ldots, x_n]$ e considere a congruência*

$$F(x_1, \ldots, x_n) \equiv 0 \ (\mathrm{mod}\, p).$$

Seja N o número de soluções da congruência acima. Então

$$N = \frac{1}{p} \sum_{s=0}^{p-1} \sum_{(x_1,\ldots,x_n) \in \mathbb{F}_p^n} \xi^{sF(x_1,\ldots,x_n)}.$$

Demonstração: Temos que

$$\sum_{s=0}^{p-1} \sum_{(x_1,\ldots,x_n) \in \mathbb{F}_p^n} \xi^{sF(x_1,\ldots,x_n)} = \sum_{s=0}^{p-1} \sum_{\substack{(x_1,\ldots,x_n) \in \mathbb{F}_p^n \\ F(x_1,\ldots,x_n) \equiv 0 \ (p)}} \xi^{sF(x_1,\ldots,x_n)} + \sum_{s=0}^{p-1} \sum_{\substack{(x_1,\ldots,x_n) \in \mathbb{F}_p^n \\ F(x_1,\ldots,x_n) \not\equiv 0 \ (p)}} \xi^{sF(x_1,\ldots,x_n)} = Np$$

pois, pelo Lema 1.5, $\sum_{s=0}^{p-1} \sum_{\substack{(x_1,\ldots,x_n) \in \mathbb{F}_p^n \\ F(x_1,\ldots,x_n) \not\equiv 0 \ (p)}} \xi^{sF(x_1,\ldots,x_n)} = 0$.

Portanto, temos o resultado desejado. ■

Vamos considerar equações aditivas homogêneas de grau k como

$$F(x_1, \ldots, x_n) = a_1 x_1^k + \ldots + a_n x_n^k \equiv 0 \ (\mathrm{mod}\, p), \ \text{ com } mdc(a_i, p) = 1.$$

Quando $n \geq 2$, temos a seguinte expressão para o número de soluções da congruência

acima.

$$\begin{aligned} N &= \frac{1}{p}\sum_{s=0}^{p-1}\sum_{x_1,\ldots,x_n=0}^{p-1}\xi^{s(a_1x_1^k+\ldots+a_nx_n^k)} \\ &= \frac{1}{p}\sum_{s=0}^{p-1}\left[\left(\sum_{x_1=0}^{p-1}\xi^{sa_1x_1^k}\right)\ldots\left(\sum_{x_n=0}^{p-1}\xi^{sa_nx_n^k}\right)\right]. \end{aligned}$$

Vamos discutir as propriedades de somas da forma $\sum_y \xi^{sy^k}$, com $s \not\equiv 0 \pmod p$.

Definição 1.7. Sejam p um primo, $k \in \mathbb{N}$ e $\Lambda \not\equiv 0 \pmod p$. Definimos $T(\Lambda) = \sum_{y=0}^{p-1}\xi^{\Lambda y^k}$, onde ξ é uma raiz primitiva p-ésima da unidade.

Seja $m(x)$ o número de soluções da congruência $y^k \equiv x \pmod p$. Vamos encontrar uma fórmula explícita para $m(x)$ quando $x \not\equiv 0 \pmod p$.

Seja g uma raiz primitiva módulo p, isto é, $x \in \mathbb{F}_p^*$, então

$$x \equiv g^b \pmod p, \tag{1.1}$$

onde o expoente b é unicamente determinado módulo $p-1$. Seja $y \equiv g^v \pmod p$. Então resolver a congruência $y^k \equiv x \pmod p$ é equivalente a resolver em v, a congruência $g^{kv} \equiv g^b \pmod p$.

Como g é uma raiz primitiva módulo p, temos que $g^{kv-b} \equiv 1 \pmod p$, e assim $kv - b \equiv 0 \pmod{p-1}$, ou seja, $kv \equiv b \pmod{p-1}$.

A congruência $kv \equiv b \pmod{p-1}$ tem solução se, e somente se, d divide b, onde $d = mdc(k, p-1)$. Neste caso, existem d soluções incongruentes módulo $p-1$. Tal resultado pode ser encontrado em [12].

Desta forma,

$$m(x) = \begin{cases} d & se \quad b \equiv 0 \pmod d \\ 0 & se \qquad c.c. \end{cases}. \tag{1.2}$$

Vamos ainda encontrar uma fórmula mais conveniente para $m(x)$.

Definição 1.8. Seja ϵ uma raiz d-ésima da unidade. Definimos

$$\chi_s(x) = \begin{cases} \epsilon^{bs} & se \quad x = g^b \\ 0 & se \quad x = 0 \end{cases},$$

para $s = 0, 1, 2, \ldots, d-1$, onde b é determinado pela congruência (1.1). Esta função é chamada de caráter multiplicativo módulo p. Quando temos $s = 0$, denotamos por χ_0 como sendo o caráter trivial.

Proposição 1.9. *Considere a função χ_s. Então*

(i) χ_s *é uma função multiplicativa;*

(ii) $\chi_s(1) = 1$ *e* $\chi_s(a^{-1}) = \chi_s(a)^{-1}$ *para* $s = 0, 1, \ldots, d-1$*;*

(iii) *Temos* $\sum_{s=0}^{d-1} \chi_s(x) = \begin{cases} d & se \quad d \; divide \; b \\ 0 & c.c. \end{cases}$,
onde $x = g^b$, $x \not\equiv 0 (\mathrm{mod}\, p)$ *e* $d = mdc(k, p-1)$,

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

Demonstração:

(*i*) Note que χ é multiplicativa pois, pela definição é homorofismo.

(*ii*) Temos que

$$\chi(e) = \chi(e\, e) = \chi(e)\chi(e).$$

Logo $\chi(e)(\chi(e) - 1) = 0$, mas $\chi(e) \in \mathbb{C}$ portanto, $\chi(e) = 1$.

Dado $a \in G$, temos

$$1 = \chi(e) = \chi(aa^{-1}) = \chi(a)\chi(a^{-1}).$$

Portanto, $\chi(a^{-1}) = \chi(a)^{-1}$.

A prova de (*iii*) e (*iv*) seguem as mesmas idéias da prova da Proposição 1.4, considerando as devidas modificações. ■

Desta forma, por (1.2) e pelo item (*iii*) da Proposição 1.9 acima, temos que

$$m(x) = \sum_{s=0}^{d-1} \chi_s(x). \tag{1.3}$$

Da Definição 1.7 de $T(\Lambda)$ e da expressão acima para $m(x)$, segue que

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

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

$$T(\Lambda) = 1 + \sum_{x=1}^{p-1}\sum_{s=0}^{d-1} \chi_s(x)\xi^{\Lambda x}. \tag{1.4}$$

Definição 1.10. Sejam χ um caráter multiplicativo módulo p e $\Lambda \in \mathbb{N}$. Defina a Soma Gaussiana relativa a χ por

$$\tau_\Lambda(\chi) = \sum_{x=0}^{p-1} \chi(x)\xi^{\Lambda x}.$$

Em particular, quando temos $\Lambda = 1$, denotamos $\tau_\Lambda(\chi)$ simplesmente por $\tau(\chi)$.

Lema 1.11. *Seja χ um caráter não trivial e suponha que $mdc(\Lambda, p) = 1$, então*

$$\chi(\Lambda)\tau_\Lambda(\chi) = \tau(\chi).$$

Demonstração: Pela definição de τ_Λ temos que

$$\chi(\Lambda)\tau_\Lambda(\chi) = \chi(\Lambda)\sum_{x=0}^{p-1} \chi(x)\xi^{\Lambda x} = \sum_{x=0}^{p-1} \chi(\Lambda)\chi(x)\xi^{\Lambda x},$$

que pelo item (i) da Proposição 1.9 segue que

$$\chi(\Lambda)\tau_\Lambda(\chi) = \sum_{x=0}^{p-1} \chi(\Lambda x)\xi^{\Lambda x} = \sum_{y=0}^{p-1} \chi(y)\xi^{y} = \tau(\chi).$$

■

Lema 1.12. *Sejam χ um caráter não trivial, $d = mdc(k, p-1)$. Se $mdc(\Lambda, p) = 1$, então* $T(\Lambda) = \sum_{s=1}^{d-1} \tau_\Lambda(\chi_s)$.

Demonstração: Da expressão (1.4) obtemos

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

Como $mdc(\Lambda, p) = 1$, segue pelo Lema 1.5 que $\sum_{x=0}^{p-1} \xi^{\Lambda x} = 0$ e assim,

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

■

Teorema 1.13. *Sejam χ um caráter multiplicativo módulo p, $\chi \neq \chi_0$, e $mdc(\Lambda, p) = 1$. Então*

$$|\tau_\Lambda(\chi)| = \sqrt{p}\ .$$

Demonstração: Por hipótese $\chi \neq \chi_0$ e $mdc(\Lambda, p) = 1$, desta forma $|\chi(\Lambda)| = 1$ e conseqüentemente pelo Lema 1.11, temos que

$$|\tau(\chi)| = |\chi(\Lambda)\tau_\Lambda(\chi)| = |\chi(\Lambda)|\,|\tau_\Lambda(\chi)| = |\tau_\Lambda(\chi)|\,.$$

Portanto, é suficiente provar que

$$|\tau(\chi)|^2 = p.$$

Considere a soma

$$\sum_{\Lambda=0}^{p-1} \tau_\Lambda(\chi)\overline{\tau_\Lambda(\chi)}.$$

Como $|\chi(\Lambda)| = 1$, então $(\chi(\Lambda))^{-1} = \overline{\chi(\Lambda)}$. Além disso, pelo Lema 1.11, segue que

$$(\chi(\Lambda))^{-1}\tau(\chi) = \tau_\Lambda(\chi)\,,$$

Assim

$$\overline{\tau_\Lambda(\chi)} = \overline{(\chi(\Lambda))^{-1}\tau(\chi)} = \chi(\Lambda)\overline{\tau(\chi)}\ .$$

Logo,

$$\tau_\Lambda(\chi)\overline{\tau_\Lambda(\chi)} = \tau(\chi)\overline{\tau(\chi)} = |\tau(\chi)|^2\ .$$

Mas, novamente pela Definição 1.7 segue que $\tau_0(\chi) = \sum_{x=0}^{p-1} \chi(x) = 0$, onde a última igualdade é devida ao item (iv) da Proposição 1.9. Portanto

$$\sum_{\Lambda=0}^{p-1} \tau_\Lambda(\chi)\overline{\tau_\Lambda(\chi)} = \sum_{\Lambda=0}^{p-1} |\tau(\chi)|^2 = (p-1)\,|\tau(\chi)|^2\ . \tag{1.5}$$

Por outro lado, pela Definição 1.7, temos que

$$\tau_\Lambda(\chi)\overline{\tau_\Lambda(\chi)} = \left(\sum_{x=0}^{p-1}\chi(x)\xi^{\Lambda x}\right)\left(\sum_{x=y}^{p-1}\overline{\chi(y)}\xi^{-\Lambda y}\right) = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\chi(x)\overline{\chi(y)}\xi^{\Lambda(x-y)}\ .$$

Pelo Lema 1.5

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

Mas como $x, y \in \{0, 1, \ldots, p-1\}$, então $x \equiv y \pmod p$ e isto implica que $x = y$.

E usando o fato que $\chi(0) = 0$, segue que

$$\begin{aligned}\sum_{\Lambda=0}^{p-1}\tau_\Lambda(\chi)\overline{\tau_\Lambda(\chi)} &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{\Lambda=0}^{p-1}\chi(x)\overline{\chi(y)}\xi^{\Lambda(x-y)} \\ &= p\sum_{z=0}^{p-1}\chi(z)\overline{\chi(z)} = p\sum_{z=1}^{p-1}|\chi(z)|^2 = p(p-1)\,. \qquad (1.6)\end{aligned}$$

Comparando (1.5) e (1.6) temos que

$$(p-1)\,|\tau(\chi)|^2 = p(p-1) \text{ e isto implica que } |\tau(\chi)|^2 = p\ ,$$

e assim concluímos a demonstração. ■

Lema 1.14. *Sejam* $d = mdc(k, p-1)$ *e* $T(\Lambda) = \sum_{y=0}^{p-1}\xi^{\Lambda y^k}$ *com* $\Lambda \not\equiv 0 \pmod p$. *Então*

$$|T(\Lambda)| \leq (d-1)\sqrt{p}.$$

Demonstração: Pelo Lema 1.12 temos que $T(\Lambda) = \sum_{s=1}^{d-1}\tau_\Lambda(\chi_s)$. Daí

$$|T(\Lambda)| = \left|\sum_{s=1}^{d-1}\tau_\Lambda(\chi_s)\right| \leq \sum_{s=1}^{d-1}|\tau_\Lambda(\chi_s)|.$$

Mas sabemos pelo Teorema 1.13 que $|\tau(\chi)| = \sqrt{p}$, logo obtemos que

$$|T(\Lambda)| \leq \sum_{s=1}^{d-1}\sqrt{p} = (d-1)\sqrt{p}.$$

O que conclui a demonstração. ■

Para nosso trabalho o que vimos sobre somas exponenciais e caracteres de grupo são suficientes, para mais detalhes veja [2] ou [15].

1.2 p-Normalização

Nesta seção descreveremos o método de p-normalização para uma forma aditiva. Considere o seguinte resultado.

Lema 1.15. *Sejam $v_0, v_1, \ldots, v_{k-1} \in \mathbb{R}$ e $n = v_0 + v_1 + \ldots + v_{k-1}$. Vamos assumir que $v_{k+i} = v_i$ para todo $i \in \mathbb{N} \cup \{0\}$. Então existe $r \in \mathbb{N}$, tal que*

$$v_r + v_{r+1} + \ldots + v_{r-1+t} \geq \frac{tn}{k} \text{ para } t = 1, 2, \ldots, k.$$

Demonstração: Temos que

$$\sum_{i=0}^{k-1} v_i = n \Leftrightarrow \sum_{i=0}^{k-1} \left(v_i - \frac{n}{k}\right) = 0\,.$$

Desta forma, podemos supor, sem perda de generalidade, que $n = 0$ e o que temos que provar é a existência de r tal que

$$v_r + v_{r+1} + \ldots + v_{r-1+t} \geq 0 \text{ para } t = 1, 2, \ldots, k.$$

Vamos supor por contradição que a conclusão seja falsa. Logo para todo $t \in \mathbb{N}$, existe $r \in \mathbb{N}$ onde $t \leq r \leq t + k - 1$ é tal que $v_t + v_{t+1} + \ldots + v_r < 0$.

Como vale para todo t, tome t_1 e determine o respectivo r_1 que torna a afirmação falsa. Escolha também $t_2 = r_1 + 1$ e determine o respectivo r_2, e assim sucessivamente. Com isso, criamos uma seqüência infinita de intervalos fechados e consecutivos, $[t_1, r_1], [t_2, r_2], \ldots, [t_l, r_l], \ldots$ tais que para cada intervalo $[t_l, r_l]$ temos $\sum_{t_l}^{r_l} v_i < 0$.

Como esta seqüência é infinita, certamente existirão índices t_α, t_β onde $t_\beta = t_\alpha + dk$

e portanto, por hipótese, teremos $v_{t_\alpha} = v_{t_\beta}$. Logo

$$\begin{aligned}\sum_{t_\alpha}^{t_\beta-1} v_i &= v_{t_\alpha} + v_{t_\alpha+1} + \ldots + v_{t_\alpha+k-1} + \\ &\quad v_{t_\alpha+k} + v_{t_\alpha+k+1} + \ldots + v_{t_\alpha+2k-1} + \\ &\quad \ldots \\ &\quad v_{t_\alpha+(d-1)k} + v_{t_\alpha+(d-1)k+1} + \ldots + v_{t_\alpha+dk-1} = 0 \ ,\end{aligned}$$

pois, por hipótese, $\sum_l^{l+k-1} v_i = 0$. Por outro lado,

$$\begin{aligned}\sum_{t_\alpha}^{t_\beta-1} v_i &= \sum_{t_\alpha}^{r_\alpha} v_i + \sum_{t_{\alpha+1}}^{r_{\alpha+1}} v_i + \ldots + \sum_{t_{\beta-1}}^{r_{\beta-1}} v_i = \sum_{t_\alpha}^{t_{\alpha+1}-1} v_i + \sum_{t_{\alpha+1}}^{t_{\alpha+2}-1} v_i + \ldots + \sum_{t_{\beta-1}}^{t_\beta-1} v_i \\ &= v_{t_\alpha} + \ldots + v_{t_{\alpha+1}-1} + \\ &\quad v_{t_{\alpha+1}} + \ldots + v_{t_{\alpha+2}-1} + \\ &\quad \ldots \\ &\quad v_{t_{\beta-1}} + \ldots + v_{t_\beta-1} < 0 \ ,\end{aligned}$$

pois $\sum_{t_{\alpha+j}}^{t_{\alpha+j+1}-1} v_i < 0$, já que $t_{\alpha+j+1} - 1 = r_{\alpha+j}$. Temos portanto uma contradição. Assim se conclui a demonstração do lema. ■

O próximo resultado é, propriamente dito, o método da p-normalização e sua propriedade fundamental.

Lema 1.16. *Seja $F = a_1x_1^k + a_2x_2^k + \ldots + a_nx_n^k$ uma forma aditiva de grau k em n variáveis. Então F pode ser escrita como*

$$F = F_0 + pF_1 + \ldots + p^{k-1}F_{k-1} \ ,$$

onde F_j é uma subforma em v_j variáveis, para $j = 0, 1, \ldots, k-1$, com todos os coeficientes não côngruos a zero módulo p e onde $v_0, v_1, \ldots, v_{k-1}$ satisfazem

$$v_0 + v_1 + \ldots + v_{k-1} \geq \frac{tn}{k} \text{ para } t = 1, 2, \ldots, k.$$

Desta forma, F é dita p-normalizada.

Demonstração: Vamos começar escrevendo

$$F = \sum_{i \geq 0} p^i F_i,$$

onde F_i são formas nas variáveis x_j de F e i é a maior potência de p que divide a_j, com a_j sendo o coeficiente de x_j. Observe que todas as subformas F_i's possuem unidades p-ádicas como coeficientes. Podemos desta forma, assumir que

$$F = F_0 + pF_1 + \ldots + p^{k-1}F_{k-1}\,.$$

Pois, para os índices $i > k-1$, digamos $i = kt + r$ com $r < k$, substituímos as variáveis x_j de F_i por $p^t x_j = \mathbf{x_j}$ e então as incluimos à forma F_r. E estas novas variáveis ainda possuem unidades p-ádicas como coeficientes.

Seja v_i o número de variáveis de F_i. Assim, $v_0 + v_1 + \ldots + v_{k-1} = n$. Portanto, aplicando o Lema anterior, temos que existe r tal que $v_r + v_{r+1} + \ldots + v_{r-1+t} \geq tn/k$ para $t = 1, 2, \ldots, k$. Vamos então fazer a seguinte permutação cíclica das variáveis de F: substitua todas as variáveis x_s das formas F_j's, com $j < r$, por $x_s = px'_s$ e depois divida a forma F por p^r. Teremos assim

$$F^* = \frac{F}{p^r} = F_r + pF_{r+1} + \ldots + p^{k-1-r}F_{k-1} + p^{k-r}F_0 + \ldots + p^{k-1}F_{r-1}.$$

Assim, $F^* = F_0^* + pF_1^* + \ldots + p^{k-1}F_{k-1}^*$ e $v_0^* + v_1^* + \ldots + v_{t-1}^* \geq tn/k \;\; para \;\; t = 1, 2, \ldots, k$. Claramente se a forma F^* possuir zeros p-ádicos, a forma F também os terá. Portanto podemos supor que F tem a forma descrita e que

$$v_0 + v_1 + \ldots + v_{t-1} \geq \frac{tn}{k} \;\text{ para }\; t = 1, 2, \ldots, k\;.$$

■

1.3 Solubilidade de uma Equação Aditiva

Nesta seção vamos investigar condições para a solubilidade não trivial de formas aditivas

$$F(x_1, \ldots, x_n) = a_1 x_1^k + a_2 x_2^k + \ldots + a_n x_n^k = 0\;, \tag{1.7}$$

onde k é ímpar, e $a_1, a_2, \ldots, a_n$ são inteiros dados. Considere o seguinte resultado.

Lema 1.17. *Seja $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. A congruência*

$$F(x_1, \ldots, x_n) \equiv 0 (\mathrm{mod}\, p^s),$$

tem solução para todo $s \geq 1$ se, e somente se, a equação

$$F(x_1, \ldots, x_n) = 0\,,$$

tem solução em $\mathbb{Z}_p$, onde $\mathbb{Z}_p$ denota o anel dos inteiros p-ádicos.

Demonstração: Suponha que $F(\alpha_1, \ldots, \alpha_n) = 0$ em $\mathbb{Z}_p$. Então, para todo s, existem inteiros $\alpha_1^{(s)}, \ldots, \alpha_n^{(s)}$ tais que $\alpha_1 \equiv \alpha_1^{(s)} (\mathrm{mod}\, p^s), \ldots, \alpha_n \equiv \alpha_n^{(s)} (\mathrm{mod}\, p^s)$, (ver [12]). Conseqüentemente

$$0 = F(\alpha_1^{(s)}, \ldots, \alpha_n^{(s)}) \equiv F(\alpha_1, \ldots, \alpha_n) \equiv 0 (\mathrm{mod}\, p^s), \text{ para todo } s \in \mathbb{N}.$$

Reciprocamente, suponha que $(\alpha_1^{(s)}, \ldots, \alpha_n^{(s)})$ seja uma seqüência de soluções das congruências $F(\vec{x}) \equiv 0 (\mathrm{mod}\, p^s)$, para todo s. Como em cada uma das coordenadas temos uma seqüência de inteiros p-ádicos, podemos determinar uma subseqüência convergente $\left\{\alpha_i^{(s_j)}\right\}$ para cada inteiro p-ádico α_i, (ver [12]). Assim temos que

$$F(\alpha_1, \ldots, \alpha_n) \equiv F(\alpha_1^{(s_j)}, \ldots, \alpha_n^{(s_j)}) \equiv 0 (\mathrm{mod}\, p^{s_j}), \text{ para todo } s_j \in \mathbb{N}.$$

Logo $|F(\alpha_1, \ldots, \alpha_n)|_p = 0$, ou seja $F(\alpha_1, \ldots, \alpha_n) = 0$, onde $|.|_p$ denota a valorização p-ádica.

■

Portanto, pelo Lema 1.17, determinar condições para a solubilidade da forma (1.7) é o mesmo que determinar condições para a solubilidade não trivial da congruência

$$F(x_1, \ldots, x_n) = a_1 x_1^k + a_2 x_2^k + \ldots + a_n x_n^k \equiv 0 (\mathrm{mod}\, p^s)\,, \tag{1.8}$$

para toda potência de primos p^s, onde $s \geq 1$.

1.3.1 Lemas Importantes

Precisaremos do próximo resultado para demonstrar a Proposição 1.19.

Lema 1.18. *Sejam $S(h,j)$ números reais, com $1 \leq h \leq q-1$ e $1 \leq j \leq n$, tais que*

$$S(h,j) \geq -u \, (u \geq 0) \ ,$$

$$\sum_{j=1}^{n} \sum_{h=1}^{q-1} S(h,j) \geq 0 \ ,$$

e

$$\sum_{j=1}^{n} \sum_{h=1}^{q-1} (S(h,j))^2 = K \ .$$

Então

$$\sum_{h=1}^{q-1} \prod_{j=1}^{n} (u + S(h,j)) \geq (q-1)u^n - \frac{1}{4} n u^{n-2} K \ .$$

Para a prova deste Lema, veja [20] página 4.

A próxima proposição é o resultado fundamental dessa seção.

Proposição 1.19. *Seja G um grupo abeliano aditivo finito de q elementos. Sejam G_j para $j = 1, 2, \ldots, n$ subconjuntos de G tais que (i) $0 \in G_j$; (ii)Se $a \in G_j$, então $-a \in G_j$; (iii)$|G_j| = r$, onde $r \geq 3$ para todo j. Se*

$$2^{n-2} > n^2 \frac{(q-1)}{(r-1)}. \tag{1.9}$$

Então existem $g_1, g_2, \ldots, g_n \in G$, com $g_j \in G_j$, não todos nulos tais que

$$g_1 + \ldots + g_n = 0, \quad g_j \in G_j \, .$$

Demonstração: Seja $G^* = \{\chi_0, \chi_1, \ldots, \chi_{q-1}\}$, o grupo de todos os caracteres de G. Então, pela Proposição 1.4, temos que

$$\sum_{s=0}^{q-1} \chi_s(g) = \begin{cases} q & se \ \ g = 0 \\ 0 & \text{c.c.} \end{cases} \ . \tag{1.10}$$

Seja H, algum dos subconjuntos $G_1, \ldots, G_n$. Denote

$$\chi_s(H) = \sum_{h \in H} \chi_s(h).$$

Pela Definição 1.1, temos que a parte real de $\chi_s(h)$ é sempre maior ou igual à -1, para todo $h \in H$. Como $\chi_s(-h)$ é o conjugado de $\chi_s(h)$ no grupo das unidades de $\mathbb{C}$, então a soma $\chi_s(h) + \chi_s(-h)$ nos dá somente a parte real. Usando os fatos mencionados, lembrando que $\chi_s(0) = 1$ e usando (ii) e (iii), temos que

$$\chi_s(H) \geq -r + 2\,. \tag{1.11}$$

Além disso, por (1.10) e (i), segue que

$$\sum_{s=0}^{q-1} \chi_s(H) = \sum_{h \in H} \sum_{s=0}^{q-1} \chi_s(h) = q.$$

Decorre de (i) da Definição 1.2 e de (iii) que

$$\chi_0(H) = \sum_{h \in H} \chi_0(h) = \sum_{h \in H} 1 = r, \tag{1.12}$$

logo

$$\sum_{s=1}^{q-1} \chi_s(H) = \sum_{s=0}^{q-1} \chi_s(H) - \chi_0(H) = q - r \geq 0. \tag{1.13}$$

Observe que, fixando $h_1 \in H$ temos

$$\sum_{h_2 \in H} \sum_{s=0}^{q-1} \chi_s(h_1 + h_2) = \begin{cases} q & se \;\; h_2 = -h_1 \\ 0 & c.c., \end{cases} \tag{1.14}$$

por (i) e (iii), temos r possibilidades de escolha para h_1. Por (ii), se temos h_1, então também temos h_2 tal que $h_2 = -h_1$.

Portanto

$$\sum_{s=0}^{q-1} (\chi_s(H))^2 = \sum_{h_1 \in H} \sum_{h_2 \in H} \sum_{s=0}^{q-1} \chi_s(h_1 + h_2) = rq. \tag{1.15}$$

Observe novamente, por (iii), que

$$(\chi_0(H))^2 = \sum_{h_1\in H}\sum_{h_2\in H}\chi_s(h_1+h_2) = \sum_{h_1\in H}\sum_{h_2\in H} 1 = r^2,$$

conseqüentemente,

$$\sum_{s=1}^{q-1}(\chi_s(H))^2 = \sum_{s=0}^{q-1}(\chi_s(H))^2 - (\chi_0(H))^2 = rq - r^2 = r(q-r). \tag{1.16}$$

De modo a podermos usar o Lema 1.18, considere

$$S(h,j) = \chi_s(G_j),\ \ u = r-2 \ \text{ e } \ K = nr(q-r).$$

Segue por (1.11), (1.13), (1.16) que

$$\sum_{s=1}^{q-1}\prod_{j=1}^{n}(r-2+\chi_s(G_j)) \geq (q-1)(r-2)^n - \frac{1}{4}n^2(r-2)^{n-2}r(q-r)\ . \tag{1.17}$$

Suponha, por contradição, que $g_1+\ldots+g_n \neq 0$ se $g_j \neq 0$, para algum j. Coloque $1 \leq \alpha \leq n$. Sejam $i_1, i_2, \ldots, i_\alpha$ diferentes elementos do conjunto $\{1,2,\ldots,n\}$. Logo

$$g_{i_1}+\ldots+g_{i_\alpha} \neq 0, \quad g_{i_k}\in G_{i_k} \quad \text{com algum} \ \ g_{i_k}\neq 0\ .$$

Desta forma, por (1.10), seque que

$$\sum_{g_{i_1}\in G_{i_1}}\cdots\sum_{g_{i_\alpha}\in G_{i_\alpha}}\sum_{s=0}^{q-1}\chi_s\left(\sum_{k=1}^{\alpha}g_{i_k}\right) = q,$$

ou equivalentemente,

$$\sum_{s=0}^{q-1}\prod_{k=1}^{\alpha}\chi_s(G_{i_k}) = q. \tag{1.18}$$

Observe ainda que

$$\prod_{j=1}^{n}(r-2+\chi_s(G_j)) = (r-2)^n + (r-2)^{n-1}(\chi_s(G_1)+\ldots+\chi_s(G_n))+$$

$$+(r-2)^{n-2}\left(\sum_{\substack{i,j=1\\ i<j}}^{n}\binom{n}{2}\chi_s(G_i)\chi_s(G_j)\right)+\ldots+\chi_s(G_1)\chi_s(G_2)\ldots\chi_s(G_n).$$

Decorre, da igualdade acima e de (1.18), que

$$\begin{aligned}
&\sum_{s=0}^{q-1}\prod_{j=1}^{n}(r-2+\chi_s(G_j)) = \sum_{s=0}^{q-1}(r-2)^n + \sum_{s=0}^{q-1}\left((r-2)^{n-1}(\chi_s(G_1)+\ldots+\chi_s(G_n))\right)\\
+ &\sum_{s=0}^{q-1}\left((r-2)^{n-2}\left(\sum_{\substack{i,j=1\\ i<j}}^{n}\binom{n}{2}\chi_s(G_i)\chi_s(G_j)\right)\right)+\ldots+\sum_{s=0}^{q-1}(\chi_s(G_1)\chi_s(G_2)\ldots\chi_s(G_n))\\
= &\ q(r-2)^n + nq(r-2)^{n-1} + \binom{n}{2}q(r-2)^{n-2}+\ldots+q\\
= &\ q\left((r-2)^n + n(r-2)^{n-1} + \binom{n}{2}(r-2)^{n-2}+\ldots+1\right) = q(r-2+1)^n.
\end{aligned}$$

Portanto

$$\sum_{s=0}^{q-1}\prod_{j=1}^{n}(r-2+\chi_s(G_j)) = q(r-1)^n. \tag{1.19}$$

Pela expressão (1.12) temos que $\chi_0(G_j) = r$ para todo $j \in \{1,2,\ldots,n\}$. Logo

$$\prod_{j=1}^{n}(r-2+\chi_0(G_j)) = \prod_{j=1}^{n}2(r-1) = 2^n(r-1)^n.$$

Da igualdade acima e pela expressão (1.17), segue que

$$\sum_{s=0}^{q-1}\prod_{j=1}^{n}(r-2+\chi_s(G_j)) \geq 2^n(r-1)^n + (q-1)(r-2)^n - \frac{1}{4}n^2(r-2)^{n-2}r(q-r)\ .$$

Combinando o resultado acima com (1.19), temos

$$\begin{aligned}
q &\geq 2^n + (q-1)\left(\frac{r-2}{r-1}\right)^n - \frac{1}{4}\frac{n^2(r-2)^{n-2}r(q-r)}{(r-1)^n}\\
&\geq 2^n + \left(1-\frac{1}{r-1}\right)^n\left[(q-1) - \frac{n^2r(q-r)}{4(r-2)^n}\right].
\end{aligned} \tag{1.20}$$

Como $r \geq 3$, segue que

$$\frac{r(q-r)}{4(r-2)^n} < \frac{3(q-1)}{2(r-1)}. \tag{1.21}$$

Além disso, por indução, temos

$$\left(1-\frac{1}{r-1}\right)^n \geq 1 - \frac{n}{r-1}. \tag{1.22}$$

Logo, substituindo (1.21) e (1.22) em (1.20), temos

$$q \geq 2^n + \left(1 - \frac{n}{r-1}\right)(q-1)\left[1 - \frac{3n^2}{2(r-1)}\right]. \tag{1.23}$$

Vamos denotar por β a seguinte expressão de (1.23)

$$\beta = \left(1 - \frac{n}{r-1}\right)(q-1)\left[1 - \frac{3n^2}{2(r-1)}\right].$$

Logo $q \geq 2^n + \beta$, assim

$$q - 1 \geq 2^n + \beta - 1. \tag{1.24}$$

Suponha que $n = r - 1$. Por (1.9), segue que

$$\frac{2^n}{4n} > q - 1,$$

Mas assim temos que

$$\frac{2^n}{4n} > 2^n - 1,$$

visto que $\beta = 0$ quando $n = r - 1$. No entanto, temos um absurdo para todo n positivo. Suponha agora, que $n > r - 1$. Nessas condições é fácil ver que β é sempre positivo. Novamente usando (1.9), temos

$$\frac{2^n(r-1)}{4n^2} > q - 1,$$

segue que

$$\frac{2^n(r-1)}{4n^2} > 2^n + \beta - 1$$

que nos dá uma impossibilidade.

Concluimos portanto, que devemos ter $n < r - 1$. Conseqüentemente, temos que

$$\begin{aligned} q &> 4n^2\frac{(q-1)}{(r-1)} + \left(1 - \frac{n}{r-1}\right)\left[q - 1 - n^2\frac{3(q-1)}{2(r-1)}\right] \\ &> 4n^2\frac{(q-1)}{(r-1)} + q - 1 - \frac{(3n^2+2n)(q-1)}{2(r-1)} > q, \end{aligned}$$

que nos dá uma contradição. Desta forma o Lema está provado. ■

1.3.2 Teorema de Tietäväinen

Definição 1.20. Definamos $\Gamma^*(k)$ como sendo o menor inteiro n com a seguinte propriedade: para cada potência de primo p^s e cada seqüência de inteiros $a_1, a_2, \ldots, a_n$, a congruência

$$F(x_1, \ldots, x_n) = a_1x_1^k + a_2x_2^k + \ldots + a_nx_n^k \equiv 0(\mathrm{mod}\, p^s) \ ,$$

tem uma solução com pelo menos um x_j coprimo com p, para todo primo p.

A fim de determinarmos o coeficiente que acompanha $k \log k$, como mencionado na introdução, defina

$$\vartheta = \limsup_{k\to\infty} \left\{\Gamma^*(k)(k\log k)^{-1}\right\} \ , \tag{1.25}$$

onde k é tomado sobre todos os k ímpares.

Seja $k = p^\tau k_0$, onde $mdc(k_0, p) = 1$. Definamos

$$\gamma = \gamma(k,p) = \begin{cases} 1 & se \quad \tau = 0 \\ \tau + 1 & se \quad \tau > 0 \ e \ p > 2 \\ \tau + 2 & se \quad \tau > 0 \ e \ p = 2 \end{cases} \ . \tag{1.26}$$

Denote por $S_p(k)$ o menor inteiro n tal que, sempre que $a_1 \ldots a_n \not\equiv 0(\mathrm{mod}\, p)$, então a congruência

$$a_1x_1^k + a_2x_2^k + \ldots + a_nx_n^k \equiv 0(\mathrm{mod}\, p^\gamma) \ , \tag{1.27}$$

tem uma solução com pelo menos um x_j coprimo com p, para um primo p fixado.

Desta forma, obtemos uma relação entre $\Gamma^*(k)$ e $S_p(k)$. A relação a seguir foi obtida por M. Dodson, (ver [9]).

Proposição 1.21. *Temos que*

$$\Gamma^*(k) \leq 1 + k \max_p \left\{S_p(k) - 1\right\}.$$

Onde o máximo é tomado sobre todos os primos p.

Demonstração: Seja F como em (1.7). Podemos considerar a forma F p-normalizada, isto é, satisfazendo as hipóteses do Lema 1.16. Assim, para a congruência (1.27), temos

$$F = F_0 + pF_1 + \ldots + p^{k-1}F_{k-1} \equiv 0(\mathrm{mod}\, p^\gamma).$$

Suponha que o número de variáveis n satisfaça

$$n \geq 1 + k \max_{p} \{S_p(k) - 1\}.$$

Como a forma F é p-normalizada, temos que $v_0 \geq S_p(k)$. Onde, por definição de $S_p(k)$, podemos resolver a congruência $F_0 \equiv 0 (\mathrm{mod}\, p^\gamma)$, com pelo menos uma das variáveis em F_0 divisíveis por p. Desta forma, temos uma solução para (1.27), atribuindo o valor zero para as variáveis de $F_1, \ldots, F_{k-1}$. E, a partir dessa solução módulo p^γ, podemos determinar solução módulo p^s para todo $s > 0$, (ver [10], Lema 4.6).

Como $\Gamma^*(k)$ é o menor número que satisfaz às hipóteses, então temos o resultado desejado. ■

Pelo Lema anterior, se conseguirmos determinar uma cota para $S_p(k)$, automaticamente estaremos determinando uma cota para $\Gamma^*(k)$. Para isso, é suficiente provar o seguinte resultado.

Teorema 1.22 (Tietäväinen). *Para cada $\epsilon > 0$, existe um $k_0(\epsilon)$ tal que*

$$S_p(k) < (1 + \epsilon)\frac{\log k}{\log 2},$$

para todo $k > k_0(\epsilon)$ e para todo primo p.

Demonstração: Considere a congruência (1.27). Suponha que k seja ímpar e suponha também que $a_1 \ldots a_n \not\equiv 0 (\mathrm{mod}\, p)$. A prova do caso $p = 2$ é trivial, pois isto implica que $\gamma = 1$, (ver (1.26)), e como $x^k \equiv x (\mathrm{mod}\, 2)$, temos uma congruência linear e esta tem solução sempre que n for par. Podemos assim supor que p seja ímpar. Denote por $\delta = mdc(\varphi(p^\omega), k)$, onde φ é a função de Euler.

Seja $L = \mathbb{Z}/p^\omega\mathbb{Z}$ o anel dos resíduos módulo p^ω e M o grupo aditivo das k-ésimas potências da classe residual relativamente prima com p. Logo

$$|L| = p^\omega \quad \text{e} \quad |M| = \frac{\varphi(p^\omega)}{\delta},$$

Seja assim,

$$G = L \;\; e \;\; G_j = \{0\} \cup \left\{y; 1 \leq y \leq p^\omega, y \equiv a_j x_j^k (\mathrm{mod}\, p^\omega) \text{ com } \; x_j \; \text{coprimo com p}\right\},$$

para $1 \leq j \leq n$. Desta forma,

$$|G| = p^{\omega} \quad \text{e} \quad |G_j| = r = 1 + \frac{\varphi(p^{\omega})}{\delta}.$$

Como $\varphi(p^{\omega})$ é par, então $\varphi(p^{\omega})/\delta \geq 2$ e por isso, $r \geq 3$. Pela Proposição 1.19, com $q = p^{\omega}$ e $r - 1 = \frac{\varphi(p^{\omega})}{\delta}$, temos que se

$$2^{n-2} > n^2 \frac{(p^{\omega} - 1)\delta}{\varphi(p^{\omega})},$$

então temos a solução desejada. Mas, observe que

$$\varphi(p^{\omega}) = p^{\omega}\left(1 - \frac{1}{p}\right) \geq p^{\omega}\left(\frac{1}{2}\right) > \frac{p^{\omega} - 1}{2}.$$

Observando também que $\delta \leq k$, obtemos que

$$n^2 \frac{(p^{\omega} - 1)\delta}{\varphi(p^{\omega})} \leq 2n^2 k,$$

Logo, se

$$2^{n-2} \geq 2n^2 k,$$

temos a solução desejada. Desta forma, se verificarmos que para $n = (1+\epsilon)\log k/\log 2$ temos $2^{n-3} \geq n^2 k$, para $k \geq k_0(\epsilon)$ suficientemente grande, então teremos provado o Lema. Mas

$$\begin{aligned}
2^{(1+\epsilon)\frac{\log k}{\log 2} - 3} &\geq \left((1+\epsilon)\frac{\log k}{\log 2}\right)^2 k \Leftrightarrow \\
\left((1+\epsilon)\frac{\log k}{\log 2} - 3\right)\log 2 &\geq 2\log\left((1+\epsilon)\frac{\log k}{\log 2}\right) + \log k \Leftrightarrow \\
\epsilon\,\log k - 2\,\log(\log k) &\geq 2\,\log(1+\epsilon) - 2\,\log(\log 2) + 3\,\log 2\,,
\end{aligned}$$

o que é verdade para k suficientemente grande.

Portanto, como $S_p(k)$ é o menor n que garante a solubilidade da congruência (1.27), para um p fixado, temos o resultado desejado. ■

Logo, pelo Teorema 1.22, temos que

$$\begin{aligned}\Gamma^*(k) &\leq 1 + k \max_p \{S_p(k) - 1\} \\ &\leq 1 + k \max_p \left\{ (1+\epsilon)\frac{\log k}{\log 2} - 1 \right\} \\ &= k(1+\epsilon)\frac{\log k}{\log 2} - k + 1.\end{aligned}$$

Portanto, pela expressão (1.25), lembrando que o limite é tomado sobre k ímpar, temos

$$\begin{aligned}\vartheta &= \limsup_{k\to\infty} \left\{ \Gamma^*(k)(k\log k)^{-1} \right\} \\ &\leq \limsup_{k\to\infty} \left\{ \frac{k(1+\epsilon)\frac{\log k}{\log 2} - k + 1}{k\log k} \right\} \\ &= \limsup_{k\to\infty} \left\{ \frac{1}{\log 2} + \frac{\epsilon}{k\log 2} - \frac{1}{\log k} + \frac{1}{k\log k} \right\} \\ &= \frac{1}{\log 2}\ .\end{aligned}$$

Mostramos assim que $\vartheta \leq 1/\log 2$ mas, como dissemos na introdução, Chowla e Shimura [4] mostraram que $\vartheta \geq 1/\log 2$. Desta forma, obtemos a igualdade desejada.

Portanto uma forma aditiva de grau k, ímpar, em n varáveis tem solução p-ádica não trivial desde que

$$n \geq \frac{1}{\log 2} k \log k.$$

Resultado obtido por Tietäväinen em [19].

Capítulo 2

Sistemas de R Formas Aditivas de Grau Ímpar

Vamos considerar $F_1, F_2, \ldots, F_R$ formas aditivas de grau $k > 1$ em n variáveis,

$$F_i(\vec{x}) = F_i(x_1, x_2, \ldots, x_n) = a_{i_1}x_1^k + a_{i_2}x_2^k + \ldots + a_{i_n}x_n^k \quad (1 \leq i \leq R),$$

e a matriz dos coeficientes, denotada por A, de tamanho $R \times n$, definida como

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{R1} & \cdots & a_{Rn} \end{bmatrix}.$$

Neste capítulo consideraremos o caso do grau k ser ímpar. Provaremos algumas condições sobre o número de variáveis e o grau das formas de modo a garantir a solubilidade do sistema

$$\begin{cases} F_1(x_1, \ldots, x_n) &= 0 \\ \vdots & \\ F_R(x_1, \ldots, x_n) &= 0 \end{cases}$$

2.1 Matrizes Particionáveis

Seja A uma matriz $R \times n$ sobre um corpo $\mathbb{K}$

$$A = [\vec{a_1} \quad \vec{a_2} \quad \dots \quad \vec{a_n}],$$

cujas colunas $\vec{a_1}, \vec{a_2}, \dots, \vec{a_n}$ são vetores em $\mathbb{K}^R$. Para $J \subseteq \{1, 2, \dots, n\}$ denotamos por A_J a sub-matriz de A formada pelas colunas $\vec{a_j}$ com $j \in J$. Por exemplo,

$$A_{\{1,4,6\}} = [\vec{a_1} \quad \vec{a_4} \quad \vec{a_6}].$$

Para uma sub-matriz A_J de A, nós escrevemos

$$r(A_J) = \text{posto de } A_J = \text{dimensão linear } \{\vec{a_j}\,; j \in J\}.$$

Definição 2.1. Dizemos que uma matriz $R \times n$, A, sobre um corpo $\mathbb{K}$ é m-particionável se $n = Rm$ e as colunas de A podem ser rearranjadas de tal forma que a matriz obtida seja da forma

$$A = [A_1 | A_2 | \dots | A_m],$$

onde cada A_i seja uma matriz $R \times R$ não singular, isto é, com determinante, em $\mathbb{K}$, diferente de zero, para cada $1 \leq i \leq m$.

Lema 2.2. *Sejam A uma matriz sobre um corpo $\mathbb{K}$, m um inteiro positivo e t um inteiro não negativo. Suponha que*

$$|J| \leq m\ r(A_J) + t$$

para todo $J \subseteq \{1, 2, \dots, n\}$, onde $|J|$ denota a cardinalidade de J. Então existem

$$S_1, S_2, \dots, S_m \subseteq \{1, 2, \dots, n\}$$

que particionam $\{1, 2, \dots, n\}$ e são tais que

$$n \leq \sum_{i=1}^{m} r(A_{S_i}) + t$$

A prova deste resultado encontra-se no Apêndice A.

O lema a seguir apresenta condições necessárias e suficientes para que uma matriz

$R \times n$ possua uma sub-matriz m-particionável.

Lema 2.3. *Sejam A uma matriz $R \times n$ sobre um corpo $\mathbb{K}$ e m um inteiro positivo. A matriz A possui uma sub-matriz m-particionável $R \times Rm$ se, e somente se,*

$$n - |J| \geq m\left(R - r\left(A_J\right)\right) \quad \textit{para todo} \quad J \subseteq \{1, 2, \ldots, n\}\,. \tag{2.1}$$

Demonstração: Como a matriz A é $R \times n$, o posto máximo de qualquer $J \subseteq \{1, 2, \ldots, n\}$ é R. Suponha que A tenha uma sub-matriz m-particionável. Então $n = Rm + w$, onde $w \geq 0$. Assim, se $r\left(A_J\right) = R$, então

$$n - |J| \geq 0 = m(R - r(A_J)).$$

Portanto, basta mostrar que vale (2.1) quando $r\left(A_J\right) = t < R$. Note que o pior caso é quando temos $t = 1$ e o subconjunto com maior número de elementos que podemos ter com esta condição é $|J| = m + w$, que equivale a considerar todas as colunas fora das m sub-matrizes e uma coluna em cada uma das m sub-matrizes. Logo

$$\begin{aligned} n - (m + w) &\geq m(R - 1) \Leftrightarrow \\ Rm + w - m - w &\geq m(R - 1) \Leftrightarrow \\ m(R - 1) &\geq m(R - 1) \end{aligned}$$

e temos a igualdade. Portanto a desigualdade (2.1) é satisfeita para todo $J \subseteq \{1, 2, \ldots, n\}$.

Reciprocamente, suponha que valha (2.1) para todo $J \subseteq \{1, \ldots, n\}$. Agora notamos que (2.1) pode ser reescrito como

$$|J| \leq m\ r\left(A_J\right) + n - mR$$

colocando $t = n - mR$ temos $|J| \leq m\ r\left(A_J\right) + t$ para todo $J \subseteq \{1, 2, \ldots, n\}$. Pelo Lema 2.2, existem $S_1, S_2, \ldots, S_m \subseteq \{1, \ldots, n\}$ que particionam n tais que

$$n \leq r\left(A_{S_1}\right) + r\left(A_{S_2}\right) + \ldots + r\left(A_{S_m}\right) + t\ .$$

Pela definição de t, segue que necessariamente devemos ter $r\left(A_{S_i}\right) = R$. Assim, contém sub-matrizes, $R \times R$, não singulares. E a sub-matriz

$$\left[A_{S_1} | A_{S_2} | \ldots | A_{S_m}\right],$$

é m-particionável. ■

Lema 2.4. *Considere A uma matriz $R \times Rm$ sobre um corpo $\mathbb{K}$. A matriz A é m-particionável se, e somente se,*

$$|J| \leq m\ r\left(A_J\right) \quad \textit{para todo } J \subseteq \{1, 2, \ldots, n\}\ . \tag{2.2}$$

Demonstração: É conseqüência direta do Lema 2.3, tomando $n = Rm$. ■

O lema a seguir mostra que para o estudo de sistemas de equações aditivas, podemos nos concentrar no caso onde a matriz dos coeficientes é m-particionável.

Lema 2.5. *Seja $\mathbb{K}$ um corpo e suponha que para todo $R, k \in \mathbb{N}$ exista*

$$m(R) = m(R, \mathbb{K}, k),$$

com a seguinte propriedade: Todo sistema de R formas aditivas de grau k, com matriz de coeficientes $m(R)$-particionável, tem solução não trivial em $\mathbb{K}$. Então todo sistema $G_1 = G_2 = \ldots = G_R = 0$ de formas aditivas de grau k em n variáveis tem solução não trivial em $\mathbb{K}$ sempre que $n \geq Rm(R)$.

Demonstração: Podemos assumir sem perda de generalidade que $m(R)$ seja minimal para cada R e desta forma, a seqüência $(m(R))$ é não decrescente. Utilizando este fato, provaremos o lema usando indução sobre R. Suponha $R = 1$. Então A é da forma

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \end{bmatrix},$$

com $n \geq m(1)$. Se $a_{1j} = 0$ para algum j, nós obtemos uma solução $\vec{x} \neq \vec{0}$ colocando $x_j = 1$ e $x_i = 0$ para $i \neq j$. Se todos os coeficientes são diferentes de zero, a matriz

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m(1)} \end{bmatrix},$$

é $m(1)$-particionável e obtemos uma forma correspondente G_1 em $m(1)$ variáveis colocando $x_i = 0$ para $i > m(1)$. Pelas hipóteses em $m(1)$, existe uma solução não trivial de $G_1 = 0$ em $\mathbb{K}$, e assim temos uma solução não trivial para a forma considerada inicialmente.

Considere como hipótese de indução que todo sistema de t formas com no mínimo $tm(t)$ variáveis, com $t < R$, tenha solução não trivial em $\mathbb{K}$.

Considere um sistema de R formas, como descrito acima, em n variáveis com $n \geq Rm(R)$. Atribuindo o valor zero às variáveis excedentes, podemos assumir que $n = Rm(R)$. Se a matriz A deste sistema é $m(R)$-particionável, então por nossas hipóteses em $m(R)$, existe uma solução não trivial em $\mathbb{K}$.

Por outro lado, se a matriz A não é $m(R)$-particionável, procedemos como a seguir. Pelo Lema 2.4, existe $J \subseteq \{1, 2, \ldots, Rm(R)\}$ tal que

$$|J| > m(R)r\left(A_J\right) \quad \text{e} \quad R > r\left(A_J\right) = t\,.$$

Colocando $x_i = 0$ para todo $i \notin J$, obtemos um sistema de equações em $|J|$ variáveis com matriz coeficiente A_J. Desde que A_J tenha posto t menor que R, as $R - t$ equações são combinações lineares das outras e o sistema é equivalente a um sistema de t equações com no mínimo $tm(t)$ variáveis. Como escolhemos $t < R$, segue da hipótese de indução que este sistema tem uma solução não trivial com os valores das variáveis em $\mathbb{K}$ e isto implica em uma solução não trivial do sistema original de R equações.

Portanto, se possuir solução para todo sistema de t equações com $t < R$, também possuirá para sistemas de R equações. E assim a validade do lema, para todo inteiro positivo, segue por indução. ■

2.2 Normalização

Seja A uma matriz $R \times n$, m-particionável da forma

$$A = [A_1|A_2|\ldots|A_m]\,, \tag{2.3}$$

onde

$$detA_j \neq 0 \quad (1 \leq j \leq m)\,. \tag{2.4}$$

Definimos

$$\Delta(A) = \prod_{j=1}^{m} |detA_j| \tag{2.5}$$

Definição 2.6. Suponha que p seja um primo divisor de $\Delta(A)$. Uma p-operação sobre as formas inteiras $F_1, F_2, \ldots, F_R$, ou equivalentemente sobre a matriz A, é uma operação que modifica de maneira reversível as formas consideradas e consiste dos seguintes passos:

(*i*) Multiplicar a matriz A por uma matriz unimodular com entradas no conjunto $\{0, 1, \ldots, p-1\}$, onde uma matriz inteira unimodular é uma matriz com determinante igual a unidade do corpo $\mathbb{K}$ considerado;

(*ii*) Multiplicar no máximo $n - R$ colunas por p^k;

(*iii*) Dividir uma ou mais linhas por p, obtendo coeficientes ainda inteiros.

O passo (*i*) corresponde a substituir o sistema inicial por um equivalente composto por combinações lineares das formas originais. O passo (*ii*) corresponde a uma mudança de variáveis

$$x_j = py_j$$

para os x_j's correspondentes às relevantes colunas.

Se um primo p divide $\Delta(A)$, então p divide pelo menos um dos $det(A_j)$'s. Por outro lado, se a matriz A_j tem determinante igual a zero em $\mathbb{F}_p$, então existe uma de suas linhas que é combinação linear das demais, assim aplicando a matriz unimodular adequada podemos garantir que, (ver passo (*i*)), existe uma linha de A_j onde todas as coordenadas são divisíveis por p, assim vemos que é possível aplicar o passo (*iii*) nessa situação. Desta forma, as p-operações definidas acima são possíveis para todo primo que divide $\Delta(A)$.

Lema 2.7. *Sejam $F_1, \ldots, F_R$ formas aditivas de grau k e matriz dos coeficientes A. Suponha que A seja m-particionável. Seja p um primo divisor de $\Delta(A)$. Vamos denotar por B a matriz obtida de uma p-operação. Então*

$$\Delta(B) = p^{kc-ml}\Delta(A),$$

onde c denota o número colunas multiplicadas por p^k e l denota o número de linhas divididas por p.

Demonstração: Temos que $A = [A_1|A_2|\ldots|A_m]$ e $detA_i \neq 0$ para todo $1 \leq i \leq m$. Observe que multiplicar a matriz A por uma matriz unimodular U, não altera o valor de $\Delta(A)$, pois

$$UA = [UA_1|UA_2|\ldots|UA_m]$$

e como $detU = 1$, temos os mesmos valores dos determinantes. Portanto não temos alteração do valor de $\Delta(A)$.

Agora, observe que multiplicar um número c_1 de colunas de uma sub-matriz A_J, $R\times R$, de A por p^k nos dá a seguinte relação no determinante dessa matriz

$$detA'_j = p^{kc_1} detA_j.$$

Desta forma, se denotarmos por $c_1, \ldots, c_m$ o número de colunas de cada matriz A_j, para $1 \leq j \leq m$, que foi multiplicada por p^k no passo (ii) de uma p-operação, temos que

$$\Delta(B) = p^{k(c_1+\ldots+c_m)}\Delta(A) = p^{kc}\Delta(A), \tag{2.6}$$

onde $c = c_1 + \ldots + c_m$.

Observe também que dividir um número l de linhas de uma sub-matriz A_J, $R \times R$, de A por p nos dá a seguinte relação no determinante dessa matriz

$$detA'_j = p^{-l} detA_j.$$

Como temos m sub-matrizes, então

$$\Delta(B) = p^{-ml}\Delta(A). \tag{2.7}$$

Desta forma, combinando (2.6) e (2.7), segue que

$$\Delta(B) = p^{kc-ml}\Delta(A).$$

■

Uma p-operação é dita permissível se, e somente se, $\Delta(B) < \Delta(A)$, ou seja, $kc-ml < 0$. Da mesma forma que Davenport e Lewis [8], precisamos introduzir uma definição de normalização.

Definição 2.8. O sistema de formas $F_1, \ldots, F_R$, ou equivalentemente a matriz A, é dito normalizado se para todo primo p divisor de $\Delta(A)$, p-operações não são mais permissíveis, ou seja, se $\Delta(A)$ não pode mais ser reduzido por nenhuma p-operação. Desta forma, denotando por B a matriz depois de aplicada todas as p-operação permissíveis, temos que $\Delta(B)$ é estritamente reduzido.

Note que a técnica de partição de matrizes modifica o conceito de sistema normalizado introduzido por Davenport e Lewis [8]. Davenport e Lewis [8] consideravam a

normalização para cada p, ou seja, definiam um sistema p-normalizado, e com esta nova técnica temos um sistema normalizado onde são realizadas p-operações para cada primo que divide $\Delta(A)$, isto é, não temos aqui um primo fixado.

Observação 2.9. Se o sistema normalizado obtido de p-operações possuir solução não trivial em $\mathbb{K}$, então o sistema original também terá solução não trivial em $\mathbb{K}$. Isto é possível porque apenas realizamos uma redução nos determinantes de cada sub-matriz, e cada passo de uma p-operação pode ser revertido.

Desta forma, quando investigamos o número de variáveis necessárias para a solubilidade não trivial do sistema de R formas considerado, nos inteiros ou nos p-ádicos, podemos assumir que temos um sistema normalizado. Veremos agora a principal propriedade de matrizes normalizadas.

Lema 2.10. *Sejam $F_1, \ldots, F_R$ formas aditivas de grau $k > 1$ em n variáveis e matriz dos coeficientes A. Suponha que A seja m-particionável e normalizada. Então para todo primo p, a matriz A contém uma sub-matriz η-particionável com os determinantes das η sub-matrizes $R \times R$ não divisíveis por p, onde*

$$\eta = \left[\frac{m}{k}\right]$$

e $[\tau]$ denota o maior inteiro menor ou igual a τ.

Demonstração: Considere os primos que não dividem $\Delta(A)$. Por A ser m-particionável e por valer (2.4), já temos o resultado requerido, e observe também que temos um número até maior que η de tais sub-matrizes. Portanto, vamos considerar os primos que dividem $\Delta(A)$. Para um $J \subseteq \{1, \ldots, n\}$ definamos

$$t = r_p(A_J) = \text{ posto de } A_J \pmod p,$$

isto é, t é o posto de A_J quando vista como uma matriz sobre o corpo $\mathbb{Z}/p\mathbb{Z}$. Assim, as $R-t$ linhas de A_J devem ser congruentes módulo p à combinações lineares das outras linhas. Deve existir uma matriz inteira unimodular U, com entradas no conjunto $\{1, \ldots, p-1\}$, tal que UA_J tenha $n-R$ linhas divisíveis por p. Logo, podemos (i) multiplicar a matriz A por essa matriz unimodular inteira U; (ii) multiplicar as $n-|J|$ colunas por p^k; (iii)dividir as $R-t$ linhas por p. Assim, aplicamos uma p-operação nas formas consideradas e

denotando por B a matriz obtida, temos que

$$\Delta(B) = p^{k(n-|J|)-m(R-t)}\Delta(A).$$

Como por hipótese, temos A uma matriz normalizada, temos que $\Delta(B) \geq \Delta(A)$, e assim, o expoente de p na equação acima deve ter grau não negativo. Desta forma, usando $\eta = [m/k]$, vemos que para $J \subseteq \{1, \ldots, n\}$ temos

$$n - |J| \geq m(R-t)/k \geq \eta(R-t),$$

com $t = r_p(A_J)$.

Pela aplicação do Lema 2.3, concluímos que a matriz A quando vista como uma matriz sobre $\mathbb{Z}/p\mathbb{Z}$, é η-particionável, o que conclui a demonstração do lema. ■

2.3 Congruências

Vamos considerar o sistema de congruências

$$F_i \equiv b_i (\mathrm{mod}\, p^s), \text{ para } 1 \leq i \leq R,$$

onde $b_1, \ldots, b_R$ são inteiros dados e $s > 0$.

Definição 2.11. Uma solução $\vec{x} = \vec{\xi}$ deste sistema é dita ser de posto R módulo p, ou equivalentemente, ser não singular módulo p se a matriz

$$\frac{1}{k}\begin{bmatrix} a_{11}\xi_1^{k-1} & \ldots & a_{1n}\xi_n^{k-1} \\ \vdots & & \vdots \\ a_{R1}\xi_1^{k-1} & \ldots & a_{Rn}\xi_n^{k-1} \end{bmatrix},$$

tiver posto R quando vista como uma matriz sobre $\mathbb{Z}/p\mathbb{Z}$. E isto acontece se existe um $J \subseteq \{1, \ldots, n\}$ tal que

$$|J| = R \quad \text{e} \quad detA_J \prod_{j \in J} \xi_j \not\equiv 0 \pmod{p}. \tag{2.8}$$

Caso contrário, dizemos que a solução é singular módulo p.

Vamos novamente considerar a definição de γ apresentada no primeiro capítulo.

Definição 2.12. Seja $k > 1$ inteiro e p um primo. Seja p^τ a maior potência de p que divide k. Definamos

$$\gamma = \gamma(k,p) = \begin{cases} 1 & se \quad \tau = 0 \\ \tau + 1 & se \quad \tau > 0 \text{ e } p > 2 \\ \tau + 2 & se \quad \tau > 0 \text{ e } p = 2 \end{cases}.$$

Lema 2.13. *Sejam $F_1, \ldots, F_R$ formas aditivas de grau k e $b_1, \ldots, b_R$ inteiros dados. Para cada $s \geq 1$, seja $M(p^s) = M(F_1, \ldots, F_R; b_1, \ldots, b_R; p^s)$ o número de distintas soluções módulo p^s do sistema*

$$F_i \equiv b_i (\mathrm{mod}\, p^s), \quad para \ 1 \leq i \leq R, \tag{2.9}$$

e seja $N(p^s) = N(F_1, \ldots, F_R; b_1, \ldots, b_R; p^s)$ o número de soluções de posto R módulo p deste sistema. Então para $s > \gamma$,

$$M(p^s) \geq p^{(n-R)(s-\gamma)} N(p^\gamma).$$

Demonstração: O resultado a seguir é clássico e pode ser encontrado, por exemplo, em [10]. Vamos usá-lo no decorrer de nossa demonstração.

Se $x^k \equiv m (\mathrm{mod}\, p^\gamma)$ possui solução, onde γ é como na Definição 2.12 e $m \not\equiv 0 (\mathrm{mod}\, p)$. Então a equação $y^k \equiv m (\mathrm{mod}\, p^s)$ possui solução para todo $s > \gamma$ com $y \equiv x (\mathrm{mod}\, p^\gamma)$.

Seja $\vec{x} = \vec{\xi}$ uma solução de posto R módulo p do sistema de congruências (2.9) com $s = \gamma$. Então, por (2.8), existem R valores de j tais que $\xi_j \not\equiv 0 (\mathrm{mod}\, p)$ para todo $j = 1, \ldots, R$ e tais que as colunas correspondentes na matriz (a_{ij}) tenham posto $R \ (\mathrm{mod}\, p)$. Podemos assumir sem perda de generalidade que as primeiras R colunas de A tenham posto $R \ (\mathrm{mod}\, p)$ e assim, $\xi_1 \ldots \xi_R \not\equiv 0 (\mathrm{mod}\, p)$.

Seja $s > \gamma$ um inteiro positivo. Como o determinante das R primeiras colunas é não divisível por p, existem R combinações lineares de $F_1, \ldots, F_R$ as quais, consideradas módulo p^s, são da seguinte forma

$$\begin{array}{rcccl} F_1' & = & c_1 x_1^k + \ldots + 0 x_R^k & + & \psi_1(x_{R+1}, \ldots, x_n) \\ & & \ddots & & \vdots \\ F_R' & = & 0 x_1^k + \ldots + c_R x_R^k & + & \psi_R(x_{R+1}, \ldots, x_n) \end{array},$$

onde $c_1c_2\ldots c_R \not\equiv 0(\mathrm{mod}\, p)$. Estas combinações lineares são formadas com múltiplos inteiros racionais dos quais o determinante não é divisível por p. Além disso, temos

$$F_1'(\vec{\xi}) \equiv 0(\mathrm{mod}\, p^\gamma), \ldots, F_R'(\vec{\xi}) \equiv 0(\mathrm{mod}\, p^\gamma),$$

e como $\xi_1, \xi_2, \ldots, \xi_R$ não são divisíveis por p, segue que

$$\psi_i(\xi_{R+1}, \ldots, \xi_n) \not\equiv \ 0(\mathrm{mod}\, p) \ \ 1 \leq i \leq R.$$

Assim, pelo resultado mencionado no começo dessa demonstração, existem $\mu_1, \ldots, \mu_R$ tais que

$$c_i\mu_i^k + \psi_i(\xi_{R+1}, \ldots, \xi_n) \equiv 0(\mathrm{mod}\, p^s),$$

para $i = 1, \ldots, R$ e $\mu_i \equiv \xi_i(\mathrm{mod}\, p^\gamma)$. Desta forma,

$$\mu_1, \ldots, \mu_R, \xi_{R+1}, \ldots, \xi_n$$

constituem uma solução também de posto $R \ (\mathrm{mod}\, p)$ para

$$F_1 \equiv 0(\mathrm{mod}\, p^s), F_2 \equiv 0(\mathrm{mod}\, p^s), \ldots, F_R \equiv 0(\mathrm{mod}\, p^s).$$

Substituindo $\xi_{R+1}, \ldots, \xi_n$ pelas $p^{(n-R)(s-\gamma)}$ distintas $(n-R)$-uplas $(\mathrm{mod}\, p^s)$, as quais são congruentes a $\xi_{R+1}, \ldots, \xi_n(\mathrm{mod}\, p^\gamma)$ e considerando que podemos encontrar outros elementos côngruos a $\xi_1, \xi_2, \ldots, \xi_R$ diferentes de $\mu_1, \mu_2, \ldots, \mu_R$, obtemos o resultado desejado.

■

Investigamos agora as congruências

$$F_1 \equiv \ldots \equiv F_R \equiv 0(\mathrm{mod}\, p^s).$$

De forma a podermos usar o Lema 2.13, desejamos estabelecer a existência de pelo menos uma solução de posto $R \ (\mathrm{mod}\, p)$ do sistema

$$F_1 \equiv \ldots \equiv F_R \equiv 0(\mathrm{mod}\, p^\gamma) \tag{2.10}$$

onde $\gamma = \gamma(k, p)$ é como na Definição 2.12.

Lema 2.14. *Sejam $F_1, \ldots, F_R$ formas aditivas de grau k, ímpar, em $n = Rm$ variáveis*

e matriz dos coeficientes A. Suponha que A seja m-particionável e que os determinantes das m sub-matrizes $R \times R$ sejam não divisíveis por p primo. Se

$$2^m > p^{\gamma R},$$

então o sistema (2.10) tem uma solução de posto R módulo p.

Demonstração: Como A é m-particionável temos que

$$A = [A_1|A_2|\ldots|A_m],$$

onde para cada j temos

$$detA_j \not\equiv 0(\mathrm{mod}\, p).$$

Seja $S_0 = \{(x_1, \ldots, x_m); x_j \in \{0,1\}$, para todo $j = 1, \ldots, m\}$. É simples ver que $|S_0| = 2^m$. Considere as formas lineares

$$L_i(\vec{y}) = L_i(y_1, \ldots, y_m) = c_{i1}y_1 + c_{i2}y_2 + \ldots + c_{im}y_m \text{ para } 1 \leq i \leq R, \tag{2.11}$$

Agora, módulo p^γ, existem, no máximo, $p^{\gamma R}$ vetores do tipo $(L_1(\vec{y}), \ldots, L_R(\vec{y}))$, com as coordenadas variando entre 1 e p^γ. Logo, se $2^m > p^{\gamma R}$ existirão $\vec{y_0}$ e $\vec{y_1} \in S_0$ distintos tais que

$$(L_1(\vec{y_0}), \ldots, L_R(\vec{y_0})) \equiv (L_1(\vec{y_1}), \ldots, L_R(\vec{y_1}))(\mathrm{mod}\, p^\gamma),$$

ou seja,

$$(L_1(\vec{y_0} - \vec{y_1}), \ldots, L_R(\vec{y_0} - \vec{y_1})) \equiv (0, \ldots, 0)(\mathrm{mod}\, p^\gamma)$$

e $\vec{y_0} - \vec{y_1} \neq (0, \ldots, 0)$, pois são distintos.

Observe que as coordenadas do vetor $\vec{y_0} - \vec{y_1}$ pertencem ao conjunto $\{-1, 0, 1\}$. Retornando ao sistema $F_1 \equiv \ldots \equiv F_R \equiv 0(\mathrm{mod}\, p^\gamma)$, defina

$$\left\{\begin{array}{lcccccccc} c_{i1} & = & a_{i1} & + & a_{i2} & + & \ldots & + & a_{iR} \\ c_{i2} & = & a_{iR+1} & + & a_{iR+2} & + & \ldots & + & a_{i2R} \\ \vdots & & & & \vdots & & & & \\ c_{im} & = & a_{i(m-1)R-m} & + & a_{i(m-1)R-(m+1)} & + & \ldots & + & a_{imR} \end{array}\right. \tag{2.12}$$

com $1 \leq i \leq R$ e considere as formas (2.11) com estes coeficientes. Como visto acima, existe uma solução não trivial para $L_1 \equiv \ldots \equiv L_R \equiv 0(\mathrm{mod}\, p^\gamma)$, e as coordenadas

dessa solução pertencem ao conjunto $\{-1,0,1\}$. Por hipótese, temos k ímpar, logo $x^k = x$ quando $x \in \{-1,0,1\}$, logo vemos que existe uma solução não trivial para $F_1 \equiv \ldots \equiv F_R \equiv 0(\mathrm{mod}\, p^\gamma)$ dentro do conjunto

$$S = \left\{(x^{\vec{(1)}}, x^{\vec{(2)}}, \ldots, x^{\vec{(m)}});\ x^{\vec{(j)}} = \vec{a}, \vec{b} \text{ ou } \vec{c} \text{ para todo } 1 \leq j \leq m\right\} \subseteq \mathbb{Z}^n, n = Rm\ ,$$

onde $\vec{a} = (0,\ldots,0)$, $\vec{b} = (1,\ldots,1)$ e $\vec{c} = (-1,\ldots,-1)$ são vetores com R coordenadas, pela construção (2.12) dos coeficientes das L_j's. Como a solução é não trivial, existe j tal que $x^{\vec{(j)}} \neq \vec{a}$. Como $detA_j \not\equiv 0(\mathrm{mod}\, p)$, segue que esta solução é de posto R módulo p. ■

2.4 Resultados Importantes

Lema 2.15. *Sejam $F_1,\ldots,F_R$ formas aditivas de grau k em $n = Rm$ variáveis, $b_1,\ldots,b_R$ inteiros e $\delta = mdc(k, p-1)$. Seja M o número de soluções do sistema*

$$F_i \equiv b_i(\mathrm{mod}\, p) \ \textit{para}\ 1 \leq i \leq R\ . \tag{2.13}$$

Então

$$\left|M - p^{R(m-1)}\right| \leq p^{R(m-1)}\left[\left((\delta-1)^m p^{1-m/2}\right)^R - 1\right]. \tag{2.14}$$

Demonstração: Vamos encontrar um limite inferior para o número total de soluções do sistema (2.13) considerado. Escrevendo $\xi^\alpha = exp(2\pi i\alpha/p)$, temos a típica expressão para M em termos de somas exponenciais:

$$M = p^{-R} \sum_{u_1,\ldots,u_R=0}^{p-1} \sum_{x_1,\ldots,x_n=0}^{p-1} \xi^{[u_1(F_1-b_1)+\ldots+u_R(F_R-b_R)]}.$$

Vamos tirar do somatório acima o elemento obtido quando $u_1 = u_2 = \ldots = u_R = 0$ e indicaremos por Σ' essa nova soma. Desta forma

$$M = p^{(n-R)} + p^{-R} \sum_{u_1,\ldots,u_R=0}^{p-1}{}' \sum_{x_1,\ldots,x_n=0}^{p-1} \xi^{[u_1(F_1-b_1)+\ldots+u_R(F_R-b_R)]}.$$

Como $n = Rm$, temos que $p^{n-R} = p^{R(m-1)}$. Reescrevendo $u_1F_1 + u_2F_2 + \ldots + u_RF_R$ para

a forma

$$u_1(a_{11}x_1^k + a_{12}x_2^k + \ldots + a_{1n}x_n^k) + \ldots + u_R(a_{R1}x_1^k + a_{R2}x_2^k + \ldots + a_{Rn}x_n^k)$$
$$= (u_1a_{11} + u_2a_{21} + \ldots + u_Ra_{R1})x_1^k + \ldots + (u_1a_{1n} + u_2a_{2n} + \ldots + u_Ra_{Rn})x_n^k.$$

E colocando $\Lambda_j = \Lambda_j(u_1, \ldots, u_R) = \sum_{i=1}^{R} a_{ij}u_i$ para $1 \leq j \leq n$, obtemos que $u_1F_1 + \ldots + u_RF_R = \Lambda_1x_1^k + \ldots + \Lambda_nx_n^k$. Portanto, segue que

$$M - p^{R(m-1)} = p^{-R} \sum_{u_1,\ldots,u_R=0}^{p-1}{}' \left[\left(\sum_{x_1=0}^{p-1} \xi^{\Lambda_1 x_1^k} \right) \ldots \left(\sum_{x_n=0}^{p-1} \xi^{\Lambda_n x_n^k} \right) \xi^{[-u_1b_1 - \ldots - u_Rb_R]} \right],$$

e pela Definição (1.7), apresentada no Capítulo 1, temos

$$M - p^{R(m-1)} = p^{-R} \sum_{u_1,\ldots,u_R=0}^{p-1}{}' T(\Lambda_1)\ldots T(\Lambda_n)\xi^{[-u_1b_1 - \ldots - u_Rb_R]}.$$

Portanto,

$$\left|M - p^{R(m-1)}\right| \leq p^{-R} \sum_{u_1,\ldots,u_R=0}^{p-1}{}' |T(\Lambda_1)\ldots T(\Lambda_n)|.$$

Aplicando a Desigualdade de Hölder ao somatório do lado direito da desigualdade acima temos

$$\sum_{u_1,\ldots,u_R=0}^{p-1}{}' |T(\Lambda_1)\ldots T(\Lambda_n)| \leq \tag{2.15}$$
$$\left(\sum_{u_1,\ldots,u_R=0}^{p-1}{}' |T(\Lambda_1)\ldots T(\Lambda_R)|^m \right)^{1/m} \ldots \left(\sum_{u_1,\ldots,u_R=0}^{p-1}{}' \left|T(\Lambda_{n-(m-1)R})\ldots T(\Lambda_n)\right|^m \right)^{1/m},$$

e como temos m blocos de Λ's, os expoentes da desigualdade acima satisfazem

$$\frac{1}{m} + \ldots + \frac{1}{m} = 1.$$

Agora observe que se cada $u_1, \ldots, u_R$ percorre o conjunto de resíduos módulo p, então o mesmo vale para $\Lambda_1, \ldots, \Lambda_R$, uma vez que os $\det A_j$'s não são divisíveis por p. Além disso, todos os u_i's são divisíveis por p se, e somente se, o mesmo vale para todos os $\Lambda_1, \ldots, \Lambda_R$.

Usando este fato, somando e subtraindo o valor quando $u_1 = \ldots = u_R = 0$, temos

$$\begin{aligned}
\sum_{u_1,\ldots,u_R=0}^{p-1}{}' \; |T(\Lambda_1)\ldots T(\Lambda_R)|^m &= \sum_{u_1,\ldots,u_R=0}^{p-1}{}' \; |T(u_1)\ldots T(u_R)|^m \\
&= \sum_{u_1,\ldots,u_R=0}^{p-1} |T(u_1)\ldots T(u_R)|^m - T(0)^{Rm} \\
&= \left(\sum_{u=0}^{p-1} |T(u)|^m\right)^R - T(0)^{Rm}.
\end{aligned}$$

De (2.15) e usando a observação acima para os m blocos de R Λ's distintos nós obtemos

$$\begin{aligned}
\left|M - p^{R(m-1)}\right| &\leq \left[\left(\sum_{u_1,\ldots,u_R=0}^{p-1}{}' \; |T(u_1)\ldots T(u_R)|^m\right)^{1/m}\right]^m \\
&= \left(\sum_{u=0}^{p-1} |T(u)|^m\right)^R - T(0)^{Rm}.
\end{aligned}$$

Pelo Lema 1.14, temos que $|T(u)| \leq (\delta-1)\sqrt{p}$. Logo $\sum_{u=0}^{p-1}|T(u)|^m \leq (\delta-1)^m p^{1+m/2}$ e usando o fato que $T(0) = p$, segue que

$$\begin{aligned}
\left|M - p^{R(m-1)}\right| &\leq \left((\delta-1)^m p^{1+m/2}\right)^R - p^{Rm} \\
&= p^{R(m-1)}\left[\left((\delta-1)^m p^{1-m/2}\right)^R - 1\right].
\end{aligned}$$

■

Lema 2.16. *Considere as mesmas hipóteses do lema anterior. Seja S o número de soluções singulares módulo p do sistema (2.13). Então*

$$S \leq \delta^R p^{R(m-1)} \left(\frac{R}{p}\right)^{m-1}. \tag{2.16}$$

Demonstração: Vamos escrever

$$\vec{x} = (\vec{x^{(1)}}, \vec{x^{(2)}}, \ldots, \vec{x^{(m)}}),$$

onde cada $\vec{x^{(j)}}$ pertence a $\mathbb{Z}^R$. Se $\vec{x}$ é uma solução singular módulo p, então cada $\vec{x^{(j)}}$ deve ter pelo menos uma componente divisível por p. Vamos obter um limite superior para S.

O número de R-uplas com componentes no conjunto $\{0, 1, \ldots, p-1\}$ e com pelo menos uma componente zero é

$$p^R - (p-1)^R \leq p^R \left(\frac{R}{p}\right).$$

Portanto, o número de possibilidades para $(\vec{x^{(2)}}, \vec{x^{(3)}}, \ldots, \vec{x^{(m)}})$ é no máximo

$$p^{R(m-1)} \left(\frac{R}{p}\right)^{m-1}.$$

Uma vez que estes são escolhidos, os valores de $x_1^k, x_2^k, \ldots, x_R^k$ são unicamente determinados pelo sistema (2.13). E o número de possibilidades para cada $x_1, x_2, \ldots, x_R$ é no máximo δ, onde δ é o número de k-ésimas potências em $\mathbb{Z}/p\mathbb{Z}$. Portanto

$$S \leq \delta^R p^{R(m-1)} \left(\frac{R}{p}\right)^{m-1}.$$

■

Lema 2.17. *Sejam $F_1, \ldots, F_R$ formas aditivas de grau $k > 1$ em $n = Rm$ variáveis, $m \geq 3$. Seja A a matriz dos coeficientes. Suponha que A seja m-particionável e os determinantes das m sub-matrizes $R \times R$ sejam não divisíveis por p primo. Sejam $N(p)$ o número de soluções de posto R módulo p do sistema (2.13) e $\delta = mdc(p-1, k)$. Suponha que*

$$p \geq \max\left\{(2\delta^R)^{1/(m-1)}R, (3R(\delta-1)^m)^{2/(m-2)}\right\}. \tag{2.17}$$

Então o sistema acima tem pelo menos uma solução de posto R módulo p. Em particular, se

$$\begin{array}{rcl} m & \geq & max\left\{R+1, 4\right\} \\ p & \geq & 3Rk^{2m/(m-2)} \end{array},$$

então vale a condição sobre p dada em (2.17).

Demonstração: Como A é m-particionável temos que

$$A = [A_1|A_2|\ldots|A_m],$$

onde para cada j temos

$$detA_j \not\equiv 0 (\mathrm{mod}\, p).$$

Considere $p \geq (2\delta^R)^{1/(m-1)}R$. Substituindo esta condição em (2.16) do Lema 2.16,

temos

$$S \leq \delta^R p^{R(m-1)} \left(\frac{R}{(2\delta^R)^{1/(m-1)} R} \right)^{m-1} = \frac{1}{2} p^{R(m-1)}. \tag{2.18}$$

Considere agora $p \geq (3R(\delta-1)^m)^{2/(m-2)}$. Daí, $p^{m-2/2} \geq 3R(\delta-1)^m$ e denotando por $X = (\delta-1)^m p^{1-m/2}$ temos que $X \leq 1/3R < \log\left(\frac{3}{2}\right)/R$. Assim

$$X^R = \exp R \log X \leq \exp RX < \frac{3}{2}\ .$$

Desta forma nós temos

$$M - p^{R(m-1)} > -\frac{1}{2} p^{R(m-1)} \ \Leftrightarrow\ M > 1/2 p^{R(m-1)}. \tag{2.19}$$

Por (2.18) e (2.19) temos, portanto, que

$$N(p) = M - S > 0.$$

Precisamos ainda mostrar que as condições $m \geq max\left\{R+1, 4\right\}$ e $p \geq 3Rk^{2m/(m-2)}$ equivalem à condição (2.17).

Considere $p \geq (2\delta^R)^{1/(m-1)} R$. Observe que $\delta \leq k$ e $\frac{2m}{m-2} \geq \frac{R}{m-1}$. Logo

$$k^{2m/m-2} \geq \delta^{R/m-1},$$

e portanto

$$3Rk^{2m/m-2} \geq 2^{1/m-1} Rk^{2m/m-2} \geq 2^{1/m-1} R\delta^{R/m-1} = (2\delta^R)^{1/m-1} R.$$

Para $p \geq (3R(\delta-1)^m)^{2/(m-2)}$, basta observar que $\delta \leq k$, então $\delta - 1 < k$, logo $\sqrt[m-2]{3^2} \leq 3$ e $\sqrt[m-2]{R^2} \leq R$.

Portanto

$$3^{2/(m-2)} R^{2/(m-2)} (\delta-1)^{2m/(m-2)} \leq 3^{2/(m-2)} R^{2/(m-2)} (k)^{2m/(m-2)} \leq 3Rk^{2m/(m-2)}.$$

Desta forma, temos uma equivalência nas condições. Portanto $N(p) \geq 1$. ■

Lema 2.18. *Suponha que valha as mesmas condições do lema anterior. Suponha também que* $m \geq 6$ *e* $p > \sqrt{C}$*, onde*

$$C = C(R,k) = k^R R^2 + 2^R k^6.$$

Então temos

$$N(p) \geq p^{R(m-1)}(1 - p^{-2}C) > 0.$$

Demonstração: Considerando $X = (\delta - 1)^m p^{1-\frac{m}{2}}$, como na prova do Lema 2.17, temos que $0 < X < 1$. Assim

$$X^R - 1 \leq (1+X)^R - 1 = X(1 + (1+X) + (1+X)^2 + \ldots + (1+X)^{R-1}) < 2^R X.$$

Logo, substituindo essa cota na expressão (2.14) do Lema 2.15, temos

$$\left|M - p^{R(m-1)}\right| < p^{R(m-1)}\left(2^R k^m p^{1-m/2}\right).$$

Logo

$$M > p^{R(m-1)}\left(1 - 2^R k^m p^{1-m/2}\right).$$

Considerando S como no Lema 2.16 e usando o fato de que $N(p) = M - S$, temos

$$\begin{aligned} N(p) &= M - S \\ &= p^{R(m-1)}\left(1 - 2^R k^m p^{1-m/2}\right) - \delta^R p^{R(m-1)} \left(\frac{R}{p}\right)^{m-1} \\ &= p^{R(m-1)} \left(1 - \left(\delta^R \left(\frac{R}{p}\right)^{m-1} + 2^R k^m p^{1-m/2}\right)\right). \end{aligned}$$

Vamos encontrar uma estimativa para $Y = \delta^R (R/p)^{m-1} + 2^R k^m p^{1-m/2}$. Para $m \geq 6$, temos que $1 - m/2 \leq -2$. Portanto $p^{1-m/2} \leq p^{-2}$. E $m - 1 \geq 5 > 2$ desta forma, pelas condições em p, temos que $R/p < 1$. Logo, $(R/p)^{m-1} \leq (R/p)^2$. Portanto, para $m \geq 6$, temos

$$Y \leq \delta^R \left(\frac{R}{p}\right)^2 + 2^R k^6 p^{-2} \leq k^R \left(\frac{R}{p}\right)^2 + 2^R k^6 p^{-2} = p^{-2} C\,.$$

E multiplicando por -1, temos a desigualdade desejada. Portanto substituindo a cota encontrada para Y na igualdade em $N(p)$, temos o resultado desejado. ■

O próximo resultado trata-se de uma aproximação alternativa baseada no resultado

de Tietäväinen[19]. Portanto, é válido somente para k ímpar.

Lema 2.19. *Sejam $F_1, \ldots, F_R$ formas aditivas de grau k, ímpar, em $n = Rm$ variáveis e matriz dos coeficientes A. Suponha que A seja m-particionável e os determinantes das m sub-matrizes, $R \times R$, não divisíveis por p primo. Seja também $\delta = mdc(\varphi(p^\gamma), k)$, onde a função φ é a função de Euler. Se*

$$2^{m-2} \geq m^2(2\delta)^R \, .$$

Então o sistema de congruências $F_1 \equiv \ldots \equiv F_R \equiv 0 (\mathrm{mod}\, p^\gamma)$ tem uma solução de posto R módulo p.

Demonstração: Como A é m-particionável, novamente temos que

$$A = [A_1 | A_2 | \ldots | A_m] \, ,$$

onde para cada j temos

$$detA_j \not\equiv 0 (\mathrm{mod}\, p).$$

Se $p^\gamma = 2$, então $x^k \equiv x (\mathrm{mod}\, 2)$ para todo x. Assim, nosso problema é reduzido à solução de um sistema linear de equações e, obviamente, pode ser resolvido não trivialmente desde que o número de variáveis seja par. Assim, basta tomar $m \geq 2$ e temos uma solução.

Portanto, podemos assumir que $p^\gamma > 2$. Sejam $L = \mathbb{Z}/p^\gamma\mathbb{Z}$ o anel de resíduos módulo p^γ e M o grupo das k-ésimas potências da classe de resíduos relativamente prima com p. Temos que

$$|L| = p^\gamma \;\text{ e }\; |M| = \frac{\varphi(p^\gamma)}{\delta} \, .$$

Vamos verificar as condições da Proposição 1.19 para

$$G = L^R \;\text{ e }\; G_j = \left\{ A_j \vec{y} \; ; \; \vec{y} \in M^R \cup \{0\} \right\}, \;\text{ com }\; 1 \leq j \leq m \, .$$

Temos que $|L| = p^\gamma$ e como $detA_j$ é uma unidade em L, obtemos que

$$|G_j| = \left| M^R \cup \{0\} \right| = \left(\frac{\varphi(p^\gamma)}{\delta} \right)^R + 1 \;\text{ para }\; 1 \leq j \leq m.$$

Usando o fato de que se $a \in M$ então $-a \in M$ e que cada $detA_j$ é uma unidade em L,

colocando $q = p^{\gamma R}$ e $r - 1 = (\varphi(p^\gamma)/\delta)^R$ temos, pela Proposição 1.19, que se

$$2^{m-2} > m^2(p^{\gamma R} - 1)\frac{\delta^R}{(\varphi(p^\gamma))^R} \ .$$

Então

$$g_1 + g_2 + \ldots + g_m = 0 \quad \text{com } g_j \in G_j \, ,$$

tem uma solução não trivial e portanto uma solução de posto R módulo p do sistema considerado. Mas as hipóteses acima são satisfeitas pois

$$(\varphi(p^\gamma))^R = p^{\gamma R}\left(1 - \frac{1}{p}\right)^R \geq p^{\gamma R}\left(\frac{1}{2}\right)^R > 2^{-R}\left(p^{\gamma R} - 1\right) ,$$

e isto implica que

$$m^2(p^{\gamma R} - 1)\frac{\delta^R}{(\varphi(p^\gamma))^R} \leq m^2(p^{\gamma R} - 1)\frac{\delta^R}{2^{-R}(p^{\gamma R} - 1)} = m^2(2\delta)^R.$$

Desta forma, a hipótese do Lema assegura a validade da solução. Portanto completamos a prova. ■

2.5 Teorema de Low, Pitman e Wolff

Nesta seção vamos considerar que a condição abaixo é válida em todos os resultados.

Seja $m_0 = m_0(k, R)$ o menor inteiro positivo tal que

$$2^{m-2} \geq \min\left\{m^2(2k)^R, (3Rk^2)^R\right\} \ . \tag{2.20}$$

Proposição 2.20. *Suponha $n = Rm$, com $m \geq m_0$. Sejam $F_1, \ldots, F_R$ formas aditivas de grau $k > 1$, ímpar, em n variáveis e matriz dos coeficientes A. Suponha que A seja m-particionável e os determinantes das m sub-matrizes, $R \times R$, não divisíveis por p primo. Então o sistema de congruências $F_1 \equiv \ldots \equiv F_R \equiv 0 (\mathrm{mod}\, p^\gamma)$, com γ como na Definição 2.12, tem uma solução de posto R módulo p. Além disso, para $b_1, b_2, \ldots, b_R$, se $p > \sqrt{C}$, com $C = C(R, k)$ como definido no Lema 2.18, o número $N(p)$ de soluções de posto R módulo p para o sistema (2.13) satisfaz*

$$N(p) \geq p^{R(m-1)}(1 - p^{-2}C) > 0$$

Demonstração: Primeiro consideramos o sistema $F_1 \equiv \ldots \equiv F_R \equiv 0(\mathrm{mod}\, p^\gamma)$. A existência de uma solução de posto R módulo p é imediata pelo Lema 2.19 se as hipóteses são satisfeitas, isto é, se $2^{m-2} \geq m^2(2\delta)^R$.

Portanto, podemos supor que $2^{m-2} \geq (3Rk^2)^R$.

Considere $\gamma > 1$. Pela Definição 2.12 de γ, temos que $k = p^\tau l$, onde $mdc(l, p) = 1$, e assim $k^2 = (p^\tau)^2 l^2$. Logo $p^\gamma \leq k^2$, assim

$$2^m \geq 2^{m-2} \geq (3Rk^2)^R \geq (3R)^R k^{2R} \geq (3R)^R p^{\gamma R} \geq p^{\gamma R},$$

portanto pelo Lema 2.14, temos uma solução de posto R módulo p. Desta forma, podemos assumir que $\gamma = 1$.

Se $p < 2^{m/R}$, novamente pelo Lema 2.14, temos uma solução de posto R módulo p.

Portanto, basta considerar

$$p \geq 2^{m/R} = (2^{m-2})^{m/R(m-2)} \ .$$

Observe que $2^{m-2} \geq (3Rk^2)^R \geq (2Rk^2)^R \geq 2^R$, portanto temos $m \geq R + 2 \geq R + 1$ e também que $m \geq 6$. Assim

$$p \geq ((3Rk^2)^R)^{m/R(m-2)} = (3R)^{m/m-2} k^{2m/m-2} \geq 3Rk^{2m/m-2} \ ,$$

e pelo Lema 2.17 temos a solução desejada. A última parte segue direto do Lema 2.18 visto que quando $p > \sqrt{C}$ implica que $p > k$ e assim temos que $\gamma = 1$. ■

Corolário 2.21. *Sejam $F_1, \ldots, F_R$ formas aditivas de grau k ímpar em $n = RV$ variáveis e matriz dos coeficientes A. Suponha que A seja V-particionável e normalizada. Se*

$$V \geq km_0.$$

Então para toda potência de primo p^s com $s > 0$, o sistema de congruências módulo p^s, $F_1 \equiv \ldots \equiv F_R \equiv 0(\mathrm{mod}\, p^s)$, tem uma solução de posto R módulo p. E, se além disso, $p > \sqrt{C}$, com $C = C(R, k)$ como definido no Lema 2.18, então o número total $M(p^s)$ de soluções desse sistema satisfaz

$$M(p^s) \geq p^{(n-R)s}(1 - Cp^{-2}) > 0 \ .$$

Demonstração: Considere p um primo fixado. Pelo Lema 2.10, encontramos m sub-matrizes $R \times R$, disjuntas e com determinantes não divisíveis por p, onde $m = [V/k]$. Portanto, pela hipótese, temos que $m \geq m_0$. Atribua o valor zero à todas as colunas $\vec{a_j}$'s fora das m sub-matrizes. Neste novo sistema temos $n = Rm$ e $m \geq m_0$, logo, pela Proposição 2.20, o sistema considerado com $s = \gamma$ possui uma solução de posto R módulo p. Portanto, pela demonstração do Lema 2.13, temos uma solução de posto R módulo p para todo $s > \gamma$.

Suponha, além disso, que $p > \sqrt{C}$, com $C = C(R,k)$ como definido no Lema 2.18. Segue que $p > k$ e então temos que $\gamma = 1$. Como $p > k$, temos que x_j^k é também um resíduo módulo p, para todo $1 \leq j \leq n$. Vamos agora, no sistema original, atribuir valores de $\{0, 1, \ldots, p-1\}$ a todas as colunas $\vec{a_j}$'s fora das m sub-matrizes. Podemos fazer essas atribuições de p^{n-Rm} maneiras, e para cada nova atribuição obtemos um sistema da forma $F_i \equiv b_i (\mathrm{mod}\, p)$, para $1 \leq i \leq R$, para os quais vale a conclusão do Lema 2.18. Logo

$$N(p^\gamma) \geq p^{n-Rm} p^{R(m-1)} (1 - Cp^{-2}) > 0.$$

Mas pelo Lema 2.13,

$$M(p^s) \geq p^{(n-R)(s-1)} N(p^\gamma) \geq p^{(n-R)(s-1)} p^{n-Rm} p^{R(m-1)} (1 - Cp^{-2}) = p^{(n-R)s} (1 - Cp^{-2}) > 0\,.$$

Como queríamos mostrar. ■

Teorema 2.22 (Low, Pitman e Wolff). *Sejam $F_1, \ldots, F_R$ formas aditivas de grau k ímpar em n variáveis. Suponha que*

$$n \geq Rkm_0\ .$$

Então o sistema

$$\begin{cases} F_1(x_1, \ldots, x_n) &=& a_{11}x_1^k + a_{12}x_2^k + \ldots + a_{1n}x_n^k &=& 0 \\ \vdots & & \vdots & & \\ F_R(x_1, \ldots, x_n) &=& a_{R1}x_1^k + a_{R2}x_2^k + \ldots + a_{Rn}x_n^k &=& 0 \end{cases} \tag{2.21}$$

tem uma solução p-ádica não trivial para todo primo p.

Demonstração: Podemos reescrever o sistema (2.21) acima como

$$\begin{cases} F_1 &= a_{11}x_1^k + \ldots + a_{1R}x_R^k + \theta_1(x_{R+1}^k, \ldots, x_n^k) \\ \vdots & \vdots \\ F_R &= a_{R1}x_1^k + \ldots + a_{RR}x_R^k + \theta_R(x_{R+1}^k, \ldots, x_n^k) \end{cases} \tag{2.22}$$

Pelo Lema 2.5 e pela Observação 2.9, é suficiente provar este resultado para

$$n = Rkm_0$$

quando a matriz A é km_0-particionável e normalizada. Sob estas condições, pelo Corolário 2.21, temos que o sistema de congruências $F_1 \equiv \ldots \equiv F_R \equiv 0(\mathrm{mod}\, p^s)$ tem solução $\vec{\xi}$ de posto R módulo p para todo $s \geq 1$. Logo existem R coordenadas de $\vec{\xi}$ que são não divisíveis por p. Sem perda de generalidade, podemos assumir que as R primeiras coordenadas sejam não divisíveis por p. Como, por hipótese a matriz é km_0-particionável, podemos reescrever o sistema (2.22) como

$$\begin{cases} F_1^* &= A_1x_1^k + \ldots + 0 + \theta_1^*(x_{R+1}^k, \ldots, x_n^k) \\ \vdots & \vdots \\ F_R^* &= 0 + \ldots + A_Rx_R^k + \theta_R^*(x_{R+1}^k, \ldots, x_n^k) \end{cases} \tag{2.23}$$

E as formas

$$\begin{gathered} A_1x_1^k \equiv \theta_1^*(x_{R+1}^k, \ldots, x_n^k)(\mathrm{mod}\, p^s) \\ \vdots \\ A_Rx_R^k \equiv \theta_R^*(x_{R+1}^k, \ldots, x_n^k)(\mathrm{mod}\, p^s) \end{gathered}$$

consideradas separadamente têm solução para todo $s \geq 1$, logo pelo Lema 1.17, tem solução p-ádica não trivial para todo primo p.

Portanto, quando substituímos estas soluções p-ádicas no sistema (2.23), temos uma solução p-ádica não trivial simultânea para o sistema de R formas. ■

A condição $2^{m-2} \geq (3Rk^2)^R$ produz uma significativa redução na cota obtida por Davenport e Lewis[8]. Pois,

$$\begin{aligned} 2^{m-2} &\geq (3Rk^2)^R \Leftrightarrow \\ (m-2)\log 2 &\geq R\log(3Rk^2) \Leftrightarrow \\ m &\geq \frac{R}{\log 2}\log(3Rk^2) + 2. \end{aligned}$$

Como $n \geq Rkm_0$ temos $n \geq \frac{R^2k}{\log 2}\log(3Rk^2) + 2Rk$. Portanto,

$$n \geq \left[\frac{R^2k}{\log 2}\log(3Rk)\right].$$

A condição $2^{m-2} \geq m^2(2k)^R$ determina em muitos casos o tamanho de m_0. Para isto, vemos que dados $\epsilon > 0$ e R temos

$$m_0 < (R+\epsilon)\frac{\log k}{\log 2},$$

para todo k ímpar suficientemente grande.

Afirmamos se $m = (R+\epsilon)\log k/\log 2$ implicar em $2^{m-2} \geq m^2(2k)^R$ para $k \geq k_0(\epsilon)$ suficientemente grande, então teremos $m_0 < (R+\epsilon)\log k/\log 2$.

De fato,

$$\begin{aligned}
2^{(R+\epsilon)\frac{\log k}{\log 2}-2} &\geq \left((R+\epsilon)\frac{\log k}{\log 2}\right)^2 (2k)^R \Leftrightarrow \\
\left((R+\epsilon)\frac{\log k}{\log 2} - 2\right)\log 2 &\geq 2\log\left((R+\epsilon)\frac{\log k}{\log 2}\right) + R\log 2k \Leftrightarrow \\
\epsilon\log k - 2\log(\log k) &\geq 2\log(R+\epsilon) + R\log 2 + 2\log 2 - 2\log(\log 2).
\end{aligned}$$

Que é verdade para k suficientemente grande. Como m_0 é o menor número que satisfaz a desigualdade $2^{m-2} \geq m^2(2k)^R$, temos então que $m_0 < (R+\epsilon)\log k/\log 2$.

Como vemos, temos uma generalização do Teorema 1.22 de Tietäväinen, com $R = 1$.

Colocando $\epsilon = (2\log 2 - 1)R$, obtemos um corolário do Teorema de Low, Pitman e Wolff, pois

$$m_0 < (R + (2\log 2 - 1)R)\log k/\log 2 = 2R\log k.$$

Logo, pelo Teorema de Low, Pitman e Wolff, teremos

$$n \geq 2kR^2\log k.$$

Podemos enunciar esse resultado da seguinte forma.

Corolário 2.23. *Existe uma constante $k_0 = k_0(R)$ tal que se*

$$n \geq 2kR^2 \log k, \qquad k > k_0,$$

então o sistema de R formas aditivas de grau k em n variáveis tem solução p-ádica não trivial para todo primo p.

Apêndice A

Demonstração do Lema 2.2

Para maior comodidade, escrevemos novamente o enunciado do Lema 2.2

Sejam A uma matriz sobre um corpo $\mathbb{K}$, m um inteiro positivo e t um inteiro não negativo. Suponha que

$$|J| \leq m\ r\left(A_J\right) + t$$

para todo $J \subseteq \{1, 2, \ldots, n\}$, onde $|J|$ denota a cardinalidade de J. Então existem $S_1, S_2, \ldots, S_m \subseteq \{1, 2, \ldots, n\}$ que particionam $\{1, 2, \ldots, n\}$ e são tais que

$$n \leq \sum_{i=1}^{m} r\left(A_{S_i}\right) + t$$

Em sua demonstração, usaremos o resultado a seguir.

Lema A.1. *Sejam A uma matriz $R \times n$ sobre um corpo $\mathbb{K}$, m um inteiro positivo e t um inteiro não negativo. Suponha que $S_1, S_2, \ldots, S_m \subseteq \{1, 2, \ldots, n\}$ sejam tais que*

$$|J| \leq \sum_{i=1}^{m} r\left(A_{S_i \cap J}\right) + t\,, \tag{A.1}$$

para todo $J \subseteq \{1, 2, \ldots, n\}$.

(i) Se valer a igualdade em (A.1) para $L \subseteq \{1, \ldots, n\}$ e $M \subseteq \{1, \ldots, n\}$, então a igualdade irá valer para $L \cup M$.

(ii) Para cada $j \in \{1, 2, \ldots, n\}$ existe um único conjunto maximal $J^{(j)}$ tal que $j \notin J$ e

vale a igualdade em (A.1) com $J = J^{(j)}$. (Note que $J^{(j)}$ pode ser vazio).

(iii) Se $J^{(j)}$, como definido acima, é não vazio, então existe um sub-índice $i_j \in \{1, \ldots, m\}$ tal que $S = S_{i_j}$, contendo j, e satisfazendo

$$r\left(A_{S\cap(J\cup\{j\})}\right) = r\left(A_{S\cap J}\right) + 1\,, \tag{A.2}$$

para todo J tal que vale a igualdade em (A.1) e $j \notin J$.

Demonstração: Primeiro observamos que o posto de uma matriz pode ser visto como a dimensão de um espaço vetorial. Considere V,W espaços vetorias, então

$$dim(V + W) = dim(V) + dim(W) - dim(V \cap W).$$

Observamos também que $(V \cup W) \subset (V + W)$, assim $dim(V \cup W) \leq dim(V + W)$ e portanto, $dim(V \cup W) + dim(V \cap W) \leq dim(V) + dim(W)$. Logo, vendo novamente como posto de matrizes, considerando L e M subconjuntos de $\{1, 2, \ldots, n\}$, temos que

$$r\left(A_{L\cup M}\right) + r\left(A_{L\cap M}\right) \leq r\left(A_L\right) + r\left(A_M\right). \tag{A.3}$$

(i) Suponha que a igualdade em (A.1) seja válida para $J = L$ e $J = M$ então, usando (A.1) em $L \cup M$ e $L \cap M$, (A.3) e a igualdade em (A.1) para L e M, obtemos

$$\begin{aligned}
|L \cup M| + |L \cap M| &\leq \sum_{i=1}^{m} \left(r\left(A_{S_i\cap(L\cup M)}\right) + r\left(A_{S_i\cap(L\cap M)}\right)\right) + 2t \\
&= \sum_{i=1}^{m} \left(r\left(A_{(S_i\cap L)\cup(S_i\cap M)}\right) + r\left(A_{(S_i\cap L)\cap(S_i\cap M)}\right)\right) + 2t \\
&\leq \sum_{i=1}^{m} \left(r\left(A_{S_i\cap L}\right) + r\left(A_{S_i\cap M}\right)\right) + 2t = |L| + |M|\,.
\end{aligned}$$

Uma vez que $|L| + |M| = |L \cup M| + |L \cap M|$, devemos ter a igualdade para cada estágio acima e portanto temos o resultado para $|L \cup M|$.(O mesmo valendo para $|L \cap M|$).

(ii) Se não existe J tal que $j \notin J$ e a igualdade em (A.1) então, $J^{(j)}$ é vazio. Caso contrário, usando o primeiro item vemos que

$$J^{(j)} = \bigcup \left\{J\,; j \notin J, J \subseteq \{1, 2, \ldots, n\}\,, \text{ e com a igualdade em } (A.1)\right\}.$$

E pela construção, esse conjunto é maximal com essa propriedade.

(*iii*) Suponha que $J^{(j)}$ seja não vazio e considere $J = J^{(j)}$. Se não existe i_j satisfazendo (A.2), então $A_{S_i \cap (J \cup \{j\})}$ tem posto $r\left(A_{S_i \cap J}\right)$ e nós temos

$$1 + |J| = |J \cup \{j\}| \leq \sum_{i=1}^{m} r\left(A_{S_i \cap (J \cup \{j\})}\right) + t = \sum_{i=1}^{m} r\left(A_{S_i \cap J}\right) + t = |J|$$

uma vez que J satisfaça a igualdade em (A.1), temos uma contradição. Portanto, existe um i_j tal que $S = S_{i_j}$ satisfazendo (A.2) para $J = J^{(j)}$. Observamos também que (A.2) é válida se, e somente se, $j \in S$ e a_j não pertence ao subespaço formado pelas colunas de $A_{S \cap J}$. Desta forma, a verdade de (A.2) para $J = J^{(j)}$ implica que $j \notin J$ e que (A.2) é válida para todo subconjunto J de $J^{(j)}$ e portanto, pelo segundo item do lema, para todo J tal que valha a igualdade em (A.1) e $j \notin J$.

■

Demonstração: **(Lema2.2)** Considere coleções de m subconjuntos $S_1, S_2, \ldots, S_m \subseteq \{1, 2, \ldots, n\}$, que não necessariamente particionam o conjunto $\{1, 2, \ldots, n\}$, tais que para todo $J \subseteq \{1, 2, \ldots, n\}$ valha (A.1). Estaremos especialmente interessados em subconjuntos J para os quais assumam a igualdade, isto é,

$$|J| = \sum_{i=1}^{m} r\left(A_{S_i \cap J}\right) + t\,,$$

Comecemos com $S_1 = S_2 = \ldots = S_m = \{1, 2, \ldots, n\}$ tais que $S_i \cap J = J$ para todo j e tais que as hipóteses do lema impliquem que valha (A.1). Modificaremos a coleção $S_1, S_2, \ldots, S_m$ em n passos.

Para o passo j, consideramos o conjunto $J^{(j)}$ como definido no Lema A.1 . Se $J^{(j)}$ está vazio, definimos $i_j = 1$, caso contrário, definimos i_j como em (iii) do lema anterior. Definimos também

$$T_i = \begin{cases} S_i \setminus \{j\}\,, & \text{se} \quad i \neq i_j \\ S_i, & \text{se} \quad i = i_j \end{cases}\,. \tag{A.4}$$

Então j pertence a exatamente um $T_1, \ldots, T_m$(o i_j - ésimo) e os conjuntos $T_1, \ldots, T_m$ ainda cobrem $\{1, 2, \ldots, n\}$. Mostramos agora que $T_1, T_2, \ldots, T_m$ e J sempre satisfazem

(A.1) para todo $J \subseteq \{1, 2, \ldots, n\}$. Seja $J \subseteq \{1, 2, \ldots, n\}$. Se $j \notin J$ então

$$T_i \cap J = S_i \cap J \text{ para todo } i$$

e portanto, $T_1, T_2, \ldots, T_m$ e J satisfazem (A.1). Assim supomos que $j \in J$ e escrevemos

$$J = L \cup \{j\} \text{ com } j \notin L. \tag{A.5}$$

Existem dois casos a considerar:

Caso 1- Se valer desigualdade estrita em (A.1) para $S_1, S_2, \ldots, S_m$ e L, então

$$|J| = 1 + |L| < 1 + \sum_{i=1}^{m} r\left(A_{S_i \cap L}\right) + t,$$

e daí,

$$|J| \leq \sum_{i=1}^{m} r\left(A_{S_i \cap L}\right) + t \leq \sum_{i=1}^{m} r\left(A_{T_i \cap J}\right) + t,$$

uma vez que (A.4) e (A.5) implicam que para todo i

$$S_i \cap L = (S_i \setminus \{j\}) \cap L \subseteq T_i \cap J. \tag{A.6}$$

E portanto, fica provada a igualdade de (A.1) para $T_1, T_2, \ldots, T_m$ e J.

Caso 2- Supomos agora que valha a igualdade em (A.1) para $S_1, S_2, \ldots, S_m$ e L.

Conseqüentemente,

$$|J| = 1 + |L| = 1 + \sum_{i=1}^{m} r\left(A_{S_i \cap L}\right) + t.$$

E como é válida a igualdade em (A.1) para $S_1, S_2, \ldots, S_m$ e L, então $J^{(j)}$ deve ser não vazio e por isso, por (iii) do lema anterior e (A.4) para i_j, o conjunto $S = S_i = S_{i_j} = T_i$ satisfaz

$$1 + r\left(A_{S_i \cap L}\right) = r\left(A_{S_i \cap (L \cup \{j\})}\right) = r\left(A_{T_i \cap J}\right).$$

Usando isto com (A.6) para todo $i \neq i_j$, temos

$$|J| \leq \sum_{i=1}^{m} r\left(A_{T_i \cap J}\right) + t,$$

e assim vale a igualdade em (A.1) para $T_1, T_2, \ldots, T_m$ e J.

Completamos o passo j renomeando $T_1, T_2, \ldots, T_m$ como $S_1, S_2, \ldots, S_m$. Desta forma, com o fim desse passo, temos excluído o inteiro j de todos os S_i's exceto um, mas os S_i's ainda cobrem o conjunto $\{1, 2, \ldots, n\}$ e satisfazem (A.1) para todo $J \subseteq \{1, 2, \ldots, n\}$.

Aplicando o passo j para $j = 1, 2, \ldots, n$, chegamos a uma situação onde $S_1, S_2, \ldots, S_m$ é uma partição de $\{1, 2, \ldots, n\}$ e satisfaz (A.1) para todo $J \subseteq \{1, 2, \ldots, n\}$. Assim, colocando $J = \{1, 2, \ldots, n\}$, obtemos

$$n \leq \sum_{i=1}^{m} r\left(A_{S_i}\right) + t$$

como queríamos mostrar. ■

Referências Bibliográficas

[1] M. Aigner *"Combinatorial Theory"*, Springer-Verlag, New York/Heidelberg/Berlin, (1979).

[2] Z. I. Borevich and I. R. Shafarevich, *"Number Theory"*, Academic Press, New York, (1966).

[3] S. Chowla, *On a conjecture of Artin I, II*, Norske Vid. Selsk. Forh.(Trondheim) **36** (1963), 135-141.

[4] S. Chowla and Shimura, *On the representation of zero by a linear combination of k-th powers*, Norske Vid. Selsk. Forh.(Trondheim) **36** (1963), 169-176.

[5] H. Davenport, *"Analytic for Diophantine Equations and Diophantine Inequalities"*, Cambridge University Press, Cambridge, (2005), second edition.

[6] H. Davenport and D. J. Lewis, *Two additive equations*, Proc. Sympos. Pure Math. **12** (AMS, Providence, RI-1972), 74-98.

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

[8] H. Davenport and D. J. Lewis, *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. London Ser. A **264** (1969), 557-595.

[9] M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London Ser. A **261** (1967), 163-210.

[10] H. Godinho, *Polinômios Homogêneos sobre Números p-ádicos*, Textos e Notas de Matemática, Universidade de Lisboa, Portugal (1999).

[11] H. Godinho, *A pair of additive quartic forms*, Ph.D. Thesis,University of Michigan (1992).

[12] H. Godinho, S. Shokranian e M. Soares, *"Teoria dos Números"*, Editora Universidade de Brasília, Brasil(1999), 2 edição.

[13] M. J. Greenberg, *"Lectures on Forms in Many Variables"*, W. A. Benjamin, Inc., New York (1969).

[14] D. J. Lewis, *Cubic congruences*, Michigan Math. J. **4** (1957), 85-95.

[15] R. Lidl, H. Niederreiter, *"Introduction to finite fields and their applications"*, Cambrigde University Press, Cambridge(1988).

[16] 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).

[17] L. Low,J. Pitman and A. Wolff, *Simultaneous diagonal congruences*, Journal of Number Theory **29** (1988), 31-59.

[18] M. G. Terjanian, *Um contre-exemple à une conjecture d'Artin*, C. R. Acad. Sc. Paris **262**, (1966), 612.

[19] A. Tietäväinen, *On a problem of Chowla and Shimura*, Journal of Number Theory **3** (1971), 247-252.

[20] A. Tietäväinen, *On a homogeneous congruence of odd degree*, Ann. Univ. Turku. Ser A. I **131** (1969), 3-6.