UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ALAÍDES INÁCIO STIVAL FERREIRA

Condições de Solubilidade p-ádica de Pares de Formas Diagonais e Alguns Casos Especiais

Goiânia
2009

ALAÍDES INÁCIO STIVAL FERREIRA

Condições de Solubilidade p-ádica de Pares de Formas Diagonais e Alguns Casos Especiais

Dissertação apresentada ao Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de concentração: Álgebra.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues

Goiânia
2009

Dados Internacionais de Catalogação-na-Publicação (CIP)

(GPT/BC/UFG)

Ferreira, Alaídes Inácio Stival.
F383c Condições de solubilidade *p*-ádica de pares de formas diagonais e alguns casos especiais [manuscrito] / Alaídes Inácio Stival Ferreira. – 2009.
57f.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues.

Dissertação (Mestrado) – Universidade Federal de Goiás, Instituto de Matemática e Estatística, 2009.

Bibliografia: f.56-57.

1.Teoria dos números 2. Corpos *p*-ádicos 3. Formas aditivas
4. Conjectura de Artin I. Rodrigues, Paulo Henrique de Azevedo
II. Universidade Federal de Goiás, **Instituto de Matemática e Estatística.** III. Título.

CDU: 511

ALAÍDES INÁCIO STIVAL FERREIRA

Condições de Solubilidade p-ádica de Pares de Formas Diagonais e Alguns Casos Especiais

Dissertação defendida no Programa de Pós–Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 28 de Agosto de 2009, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Paulo Henrique de Azevedo Rodrigues
Instituto de Matemática e Estatística – UFG
Presidente da Banca

Prof. Dr. Jorge Fernandes de Lima Neto
Instituto Agricultura e Ambiente – UFAM

Prof. Dr. Ricardo Nunes de Oliveira
Instituto de Matemática e Estatística – UFG

Alaídes Inácio Stival Ferreira

Licenciou-se em Matemática na UFG - Universidade Federal de Goiás. Durante a graduação foi monitora de Geometria Euclidiana. Durante o Mestrado, na UFG - Universidade de Goiás, foi bolsista da CAPES.

À Força Maior, à Energia Superior, que eu chamo de Deus. Deus de bondade e de amor. Que está além do tempo. Que nos cerca de carinho, e em todos momentos. Apesar de, em muitos momentos, chegarmos a pensar o contrário.

Agradecimentos

A minha família, principalmente meu pai Waldemir, que muito me apoiou do seu jeito silencioso, e minha mãe Tereza, que sempre esteve presente em todos momentos, dos alegres aos mais desesperadores.

A Luís Viana, principalmente no final, quando o mundo quase ruiu ele me encorajou a continuar. E durante tantas vezes, por mais de década.

Aos professores que durante a graduação nos ajudaram tanto, nos incentivando, nos animando, nos cobrando, nos ensinando a aprender... São muitos, e importantes. Ao pessoal da secretaria do IME, em especial a Jane e a Marina Maria, que nos escutaram sempre, principalmente quando reclamávamos. Ao professor Alacyr Gomes, principalmente, pela ajuda técnica.

E agora no Mestrado, estão os responsáveis por este momento: meu orientador Paulo Henrique Rodrigues, os professores Jesus Motta, Luciana Maria Ávila, Marina Mizukoshi, Mário José, Maurílio Maurício de Melo e com carinho especial Romildo Pina. Não podendo esquecer o coordenador João Medrado e também ao professor Ronaldo Garcia. E aos colegas.

A todos que de certa forma estiveram envolvidos nesta conquista.

A vocês, meu muito obrigado.

A sorte ajuda às vezes; o trabalho, sempre.

Autor desconhecido ,
Sabedoria Chinesa.

Resumo

Ferreira, Alaídes Inácio Stival. **Condições de Solubilidade p-ádica de Pares de Formas Diagonais e Alguns Casos Especiais**. Goiânia, 2009. 57p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Este texto é sobre solubilidade no corpo dos p-ádicos de sistemas de duas formas aditivas: com grau k e variáveis $n > 4k$ apartir de $p > 3k^4$; com grau k ímpar apartir de $n > 6k+1$ variáveis; e de grau 5 com $p > 101$ para $n \geq 31$ variáveis, e para todo p com $n \geq 36$ variáveis, com exceções de $p = 5$ e $p = 11$.

Palavras–chave

p-ádico, sistema de duas formas aditivas, conjectura de Artin

Abstract

Ferreira, Alaídes Inácio Stival. **Conditions of p-adic Solubility of Pars of Diagonal Forms and Some Special Cases**. Goiânia, 2009. 57p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

This text is above solvability in systems of two forms additive over p-adics fields: with of degree k and variables $n > 4k$ at lesat $p > 3k^4$; with of degree an k odd integer at least $n > 6k+1$ variables; and with of degree 5 and $p > 101$ for $n \geq 31$ variables, and for all p with $n \geq 36$ variables, with the possible exceptions of $p = 5$ and $p = 11$.

Keywords

p-adic, systems of two additive forms, Artin's conjecture

Sumário

Introdução

Apontamentos Históricos sobre a Conjectura de E. Artin

No corpo dos números reais várias equações homogêneas possuem somente a solução trivial $(0,0,\cdots,0)$, um exemplo clássico é

$$x^2+y^2=0.$$

E assim como esta, todo polinômio homogêneo diagonal de grau par, com coeficiente inteiro positivo, possui somente a solução trivial no corpo dos reais. Já no corpo dos números p-ádicos, $\mathbb{Q}_p$, não raro, encontramos exemplos de formas (polinômios homogêneos) aditivas em n variáveis e grau k que possuem zeros não triviais.

Influenciado por exemplos como esses, em 1920 E. Artin fez a seguinte conjectura:

"Qualquer polinômio homogêneo de grau k em $n > k^2$ variáveis tem zero não trivial sobre o corpo dos números p-ádicos, $\mathbb{Q}_p$."

Que foi derrubada por alguns contra exemplos de polinômios homogêneos não diagonais, como os de G. Terjanian [26], que em 1966 exibiu uma forma quártica com 18 variáveis e outra com 20 em $\mathbb{Q}_2$ sem zeros 2-ádicos não triviais. E J. Browkin [6] deu contra exemplos para cada primo p, de polinômios com o número de variáveis de até k^3.

A partir de então, motivados por esta conjectura, vários estudos foram realizados. Resultados importantes foram demonstrados. Vejamos, cronologicamente, alguns deles.

Em 1924, Hasse, veja [5], demonstra que *Qualquer forma quadrática sobre o corpo dos números p-ádicos em cinco ou mais variáveis possui zeros p-ádicos.*

No ano de 1935 Chevalley, veja em [15] ou [17] demonstrou que *Todo polinômio em n variáveis, de grau k e sem termo constante, tem sempre solução não trivial módulo p, desde que* $n > k$.

Lewis [20], também em [15], no ano de 1952, demonstrou que *Toda forma cúbica com coeficientes p-ádicos em* 10 *ou mais variáveis possui zeros p-ádicos*. Birch e Lewis [3], em 1959, com $k = 5$; em 1965, Laxton e Lewis [19] com $k = 7, 11$, mostraram que *Toda forma de grau* $k = 5, 7, 11$ *com coeficientes p-ádicos com número de variáveis*

superior a k^2, tem zeros p-ádicos desde que o corpo de classes residuais seja grande o suficiente.

H. Davenport e D. J. Lewis, desenvolveram um grande trabalho sobre o estudo de sistema de formas aditivas. Procuravam encontrar condições sobre o número de variáveis que garantissem a solubilidade sobre os números p-ádicos. A conjectura de Artin pode ser reformulada num caso particular:

"Um sistema de formas aditivas de grau k em N variáveis,

$$\begin{cases} F_1 = a_{11}x_1^k + \cdots + a_{1N}x_N^k & = 0, \\ & \vdots \\ F_R = a_{R1}x_1^k + \cdots + a_{RN}x_N^k & = 0. \end{cases}$$

com coeficientes inteiros tem solução p-ádica não trivial, desde que $N > Rk^2$."

H. Davenport e D. J. Lewis [10, 13], no ano de 1963, demonstraram esta versão da conjectura para o caso de uma equação, $R = 1$ e $k > 2$, em 1969 para o caso de sistema de duas equações, $R = 2$, com o grau k ímpar . Para sistemas em geral eles provaram a existência de solução p-ádica desde que $N > 48R^2k^3ln(3Rk^2)$, em [12].

J. Birch e D. J. Lewis [4], em 1965, demostraram o caso para um sistema de 3 formas aditivas desde que o grau fosse $k = 2$ e $p > 7$ (e em 1980, S. Schuur [24]).

E. Stevenson [25], demonstrou a validade da versão da conjectura de Artin, ainda com o sistema de 3 formas aditivas, com o grau $k = 3$ e $p \neq 3$ e 7, no ano de 1982.

L. Low, J. Pitman e A. Wolff [22], em 1988, provaram que $N \geq 48Rk^3ln(3Rk^2)$ é suficiente pra garantir zeros p-ádicos nesta versão da conjectura. Quando em 1999, J. Brüdern e H. Godinho [7] chegaram a cota de $N \geq R^3k^2$, quando k é grande comparado com R para a existência de solução p-ádicas não triviais. Em 2001, M. Knapp [18], demonstrou a existências de zeros p-ádicos desde que $N \geq 4R^2K^2$.

E recentemente, 2002, J. Brüdern e H. Godinho [8], encontraram a melhor estimativa que garantissem a existências de zeros p-ádicos para a versão da conjectura de Artin, com qualquer grau k desde que $N \geq 8k^2$.

Desenvolvimento do Trabalho

Apesar de muitos resultados a versão da conjectura com sistema de R equações ainda está em aberto. Assim, o estudo de casos particulares sobre R tem sido de grande valia.

Com o uso de somas exponenciais pode-se estimar o número de soluções de congruências polinomiais, como por exemplo, no caso de se estabelecer soluções p-ádicas não triviais para conjuntos de formas via Lema de Hensel.

Em 1992, Atkinson, Brüdern e Cook [1] provaram o seguinte resultado:

Teorema 1 *Sejam r, k, n inteiros positivos com $k > 1$ e $n > 2rk$. Então o sistema de equações*

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

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

No caso de 2 equações aditivas, $r = 2$, o Teorema 1 garante solução não trivial para todo $p > k^6$, com $n > 4k$ variáveis. Já demonstrado em 1989, por Atkinson e Cook [2].

Um dos objetivos desse trabalho é melhorar este resultado apresentando uma versão mais forte dada por Ivan D. Meir:

Teorema 2 *Sejam k, n inteiros positivos com $k > 1$ e $n > 4k$. Então o sistema de equações*

$$F_i(x) = a_{i1}x_1^k + \cdots + a_{in}x_n^k = 0, \quad i = 1, 2;$$

com coeficientes $a_{ij} \in \mathbb{Z}$, tem solução p-ádica não trivial para todo $p > 3k^4$.

Dimuinuindo a cota de $p > k^{2r+2}$ para $p > 3k^4$ [23]. A demonstração envolve uma modificação considerável no método típico, que usa somas exponênciais. Usaremos no Capítulo 2, soma estimada de caracteres para polinômio em uma variável, para a demonstração desse resultado.

No Capítulo 1 trataremos de introduzir conceitos básicos, porém essenciais para a demonstração deste Teorema 2. Em uma das versões do Lema de Hensel, que garante a solubilidade (que desde agora será a não trivialidade) nos corpo dos p-ádicos apartir da solubilidade de determinada congruência no corpo dos reais. A definição de sistema p-normalizado nos dará, então, condições para utilizar um dos Teoremas de Danverport e Lewis, que reescreve um sistema p-normalizada através de uma reordenação das varáveis, na forma

$$f_i = F_i(x_1, \cdots, x_m) + pG_i(x_{m+1}, \cdots, x_n)$$

para $i = 1, \cdots, R$, com a relação $m \geq \dfrac{n}{k}$, entre outras condições.

No Capítulo 3 veremos uma demostração para o seguinte resultado:

Teorema 3 *Seja p um primo e k um inteiro ímpar tal que p não divide k. Suponha que a equação $ax^k + by^k + cz^k \equiv d \pmod p$, com a, b e c não nulos módulo p, tem uma solução com $xyz \not\equiv 0 \pmod p$, para todo d. Então qualquer sistema de duas formas aditivas de grau k com ao menos $6k + 1$ variáveis sempre tem solução p-ádica não trivial.*

E também uma demostração para outro resultado:

Teorema 4 *Todo sistema de duas formas quínticas aditivas com N variáveis sempre tem solução p-ádica não trivial:*

i) para todo $p > 101$ desde que $N \geq 31$;

ii) para todo p desde que $N \geq 36$, e $p \neq 5$ e 11.

Ambos resultados estão em [16].

CAPÍTULO 1

Preliminares

Seja o sistema de R formas aditivas de grau k:

$$\begin{cases} a_{11}x_1^k & +\cdots+ & a_{1n}x_n^k & = 0 \\ \vdots & & \vdots & \\ a_{R1}x_1^k & +\cdots+ & a_{Rn}x_n^k & = 0, \end{cases} \tag{1-1}$$

onde os coeficientes a_{ij} são números inteiros e $n > R$.

Neste capítulo iremos introduzir conceitos básicos como o Lema de Hensel, o processo de p-normalização e um Teorema de Davenport e Lewis. Afim de obtermos condições de solubilidade para o sistema (1-1).

Neste trabalho estamos assumindo que há familiaridade, do leitor, nos números p-ádicos, $\mathbb{Q}_p$.

No Lema de Hensel teremos a garantia de solubilidade não trivial no corpo dos números p-ádicos, $\mathbb{Q}_p$, de um sistema apartir da solubilidade de um sistema de congruências. A Definição de p-normalização será base para o Teorema de Davenport e Lewis, que reescreve um sistema p-normalizado de formas aditivas $\sum_i^R f_i = 0$ através de uma reordenação das variáveis, na forma:

$$f_i = F_i + pG_i, \text{ para } i = 1, \cdots, R,$$

dentre outras particularidades.

Nossa primeira Definição é sobre solução não-singular em sistema de congruências.

Definição 1.1 *Seja* $\gamma \geq 1$. *Uma solução* $(\xi_1, \cdots, \xi_m)$ *para o sistema de congruências:*

$$\sum_{j=1}^{m} a_{ij}x_j^k \equiv 0 \pmod{p^\gamma} \quad (1 \leq i \leq R), \tag{1-2}$$

com a_{ij} *coeficientes de números inteiros é chamada não-singular se existem índices* $j_1, \cdots, j_R$ *tais que*

$$\xi_{j_1}\xi_{j_2}\cdots\xi_{j_R}Det(c_{j_1},\cdots,c_{j_R}) \not\equiv 0(mod\, p),$$

onde $1 \leq j_1 < j_2 < \cdots < j_R \leq m$, *e* c_j *representa a j-ésima coluna da matriz dos coeficientes do sistema (1-1).*

1.1 Lema de Hensel

O próximo Lema, feito por Hensel, garante solução não trivial no corpo dos p-ádicos para o sistema (1-1), desde que se garanta solução não-singular para o sistema de congruências (1-2). E onde o valor de γ depende da potência de p na fatoração prima de k. Uma versão do Lema de Hensel encontra-se em [14].

Lema 1.2 (Hensel) *Suponha que* τ *seja a maior potência de p tal que* p^τ *divide k. Defina*

$$\gamma = \gamma(k,p) = \begin{cases} \tau+2, & se \;\; p=2, \quad \tau > 0 \\ \tau+1, & c.c. \end{cases} \tag{1-3}$$

Se o sistema de congruênicas (1-2) tem solução não-singular quando γ *é dado por (1-3), então o sistema (1-1) tem solução não trivial em* $\mathbb{Q}_p$.

Prova.

Observação 1.3 *Usaremos a informação que, se* $x^k \equiv m\ (mod\ p^\gamma)$ *tem solução com* $m \not\equiv 0$ *(mod p), então* $y^k \equiv m\ (mod\ p^v)$ *tem solução com* $v \geq \gamma$ *e* $y \equiv x\ (mod\ p)$.

Este resultado se encontra em [17].

O sistema (1-2) pode ser reescrito na forma:

$$\begin{cases} f_1(x) = & a_{11}x_1^k & +\cdots+ & a_{1n}x_n & \equiv 0(mod\, p^\gamma) \\ \quad\vdots & \quad\vdots & & \quad\vdots & \\ f_R(x) = & a_{R1}x_1^k & +\cdots+ & a_{Rn}x_n & \equiv 0(mod\, p^\gamma), \end{cases} \tag{1-4}$$

onde γ é dado por (1-3).

Seja $\xi = (\xi_1,\cdots,\xi_n)$ a solução não-singular do sistema (1-4) com γ dado por (1-3). Então existem R elementos $\xi_{j_1},\cdots,\xi_{j_R}$ em ξ tais que

$$\xi_{j_1}\cdots\xi_{j_R}Det(c_{j_1},\cdots,c_{j_R}) \not\equiv 0 \ (\text{mod } p).$$

Sem perda de generalidade, tomemos $\xi_{j_1},\cdots,\xi_{j_R}$ por $\xi_1,\cdots,\xi_R$.

Seja $v > \gamma$ um inteiro positivo. Como o determinante das R colunas da matriz dos coeficientes de (1-4) é não divisível por p, podemos reescrever (1-4) por

$$\begin{cases} g_1 = & b_{11}x_1^k & & & +\psi_1(x_{R+1},\cdots,x_n) \\ & & \cdots & & \vdots \\ g_R = & & & b_{RR}x_R^k & +\psi_R(x_{R+1},\cdots,x_n) \end{cases} \tag{1-5}$$

onde $b_{11}b_{22}\cdots b_{RR} \not\equiv 0 \pmod{p}$. Temos que $g_1(\xi) \equiv 0 \pmod{p^\gamma}$,$\cdots$,$g_R(\xi) \equiv 0 \pmod{p^\gamma}$. Assim,

$$\psi_i(\xi_{R+1},\cdots,\xi_n) \equiv -b_{ii}\xi_i^k \not\equiv 0 \pmod{p},\ (i = 1,\cdots,R).$$

Pela Observação (1.3) acima, existem $\eta_1,\cdots,\eta_R$, tais que

$$b_{ii}\eta_i^k + \psi_i(\xi_{R+1},\cdots,\xi_n) \equiv 0 \pmod{p^v},$$

onde $i = 1,\cdots,R$ e $\eta_i \equiv \xi_i \pmod{p}$. Logo, $\eta_1,\cdots,\eta_R,\xi_{R+1},\cdots,\xi_n$ é uma solução de

$$f_1 \equiv 0 \ \ (mod \ \ p^v),\cdots,f_R \equiv 0 \ \ (mod \ \ p^v) \tag{1-6}$$

onde nenhum dos elementos $x_1,\cdots,x_R$ são divisíveis por p.

Demonstramos a existência de uma solução para (1-6) para qualquer $v > \gamma$.

Seja $(a_1^{(v)},\cdots,a_n^{(v)})$, com $v > \gamma$, uma sequência de soluções de (1-6) em $\mathbb{Z}_p^n$. Como $\mathbb{Z}_p$, o conjunto dos números inteiros p-ádicos, é compacto, em cada uma das coordenadas de $(a_1^{(v)},\cdots,a_n^{(v)})$ podemos determinar uma subsequência convergente $\left\{a_i^{(v_j)}\right\}$ para um inteiro p-ádico α_i. Teremos então

$$f_i(\alpha_1,\cdots,\alpha_n) \equiv f_i(a_1^{(v_j)},\cdots,a_n^{(v_j)}) \equiv 0 \pmod{p^{v_j}}\ (i = 1,\cdots,R)$$

para todo $v_j > \gamma$. Logo $\mid f_i(\alpha_1\cdots,\alpha_n) \mid_p = 0$ quando $v_j \to \infty$, ou seja,

$$f_i(\alpha_1\cdots,\alpha_n) = 0\ (i = 1,\cdots,R).$$

□

A partir de agora, buscaremos resolver sistemas de congruências módulo p^γ. Seja $A = (a_{ij})$ a matriz de coeficientes de (1-1), e c_j a j-ésima coluna de A.

Definição 1.4 *Uma variável x_j está no nível l se p^l divide todos os elementos da coluna c_j mas p^{l+1} não divide todos os elementos de c_j.*

Transformaremos o sistema (1-1), dividindo em níveis menores que k, utilizando reordenação e mudança de variáveis. Reescrevendo no seguinte sistema:

$$\begin{cases} f_{11} & +pf_{12}+ & \cdots & +p^{k-1}f_{1k} = & 0 \\ f_{21} & +pf_{22}+ & \cdots & +p^{k-1}f_{2k} = & 0 \\ \vdots & \vdots & & \vdots & \\ f_{R1} & +pf_{R2}+ & \cdots & +p^{k-1}f_{Rk} = & 0, \end{cases} \tag{1-7}$$

onde f_{ij} são formas aditivas de grau k nas variáveis x_j. A existência de uma solução não trivial em $\mathbb{Q}_p$ para (1-7) implica na existência de uma solução não trivial em $\mathbb{Q}_p$ para (1-1).

Sejam f_i $i = 1, \cdots, R$, as equações aditivas do sistema (1-1), denotadas por

$$f_i = a_{i1}x_1^k + \cdots + a_{in}x_n^k, \quad (i = 1, \cdots, R).$$

Defina

$$\theta(f_1, \cdots, f_R) = \prod_{j_1, \cdots, j_R} Det(c_{j_1}, \cdots, c_{j_R}) \tag{1-8}$$

onde os subíndices $\{j_1, \cdots, j_R\} \subset \{1, \cdots, n\}$ são distintos. Subconjuntos iguais são tais que possuem os mesmos elementos dispostos na mesma ordem. Assim, o número de subconjuntos distintos será

$$M = n(n-1)\cdots(n-R+1) = \frac{n!}{(n-R)!}.$$

O próximo Lema estabelece algumas propriedades de θ.

Lema 1.5 *i) Se* $f_i'(x_1, \cdots, x_n) = f_i(p^{\partial_1}x_1, \cdots, p^{\partial_n}x_n)$ *para* $\partial_i \in \mathbb{Z}$ *e* $i = 1, \cdots, R$ *, então*

$$\theta(f_1', \cdots, f_R') = p^{\frac{kRM\partial}{n}}\theta(f_1, \cdots, f_R)$$

onde $\partial = \partial_1 + \cdots + \partial_n$.
ii)Se $f_i''(x_1, \cdots, x_n) = \sum_{j=1}^{R} d_{ij}f_j$, *para* $i = 1, \cdots, R$, *com* $d_{ij} \in \mathbb{Q}$ *e* $Det(d_{ij}) = D \neq 0$,*então*

$$\theta(f_1'', \cdots, f_R'') = D^M\theta(f_1, \cdots, f_R).$$

Prova.

i)Seja $f_i'(x_1, \cdots, x_n) = f_i(p^{\partial_1}x_1, x_2, \cdots, x_n)$, para $i = 1, \cdots, R$. Nesse caso $\partial = \partial_1$ e temos as seguintes equações:

$$\begin{cases} f_1' = & p^{k\partial}a_{11}x_1^k & +a_{12}x_2^k + & \cdots & + & a_{1n}x_n^k \\ \vdots & \vdots & \vdots & & & \vdots \\ f_R' = & p^{k\partial}a_{R1}x_1^k & +a_{R2}x_2^k + & \cdots & + & a_{Rn}x_n^k. \end{cases} \tag{1-9}$$

Indicando por c_j' a j-ésima coluna do sistema (1-9) obtemos

$$\begin{cases} Det(c_{j_1}', \cdots, c_{j_R}') = p^{k\partial}Det(c_{j_1}, \cdots, c_{j_R}), & se\ 1 \in \{j_1, \cdots, j_R\}, \\ Det(c_{j_1}', \cdots, c_{j_R}') = Det(c_{j_1}, \cdots, c_{j_R}), & se\ 1 \notin \{j_1, \cdots, j_R\}. \end{cases}$$

Existem $\dfrac{RM}{n}$ conjuntos $\{j_1, \cdots, j_R\}$ tais que $1 \in \{j_1, \cdots, j_R\}$. Então

$$\begin{aligned}\theta(f'_1,\cdots,f'_R) &= \prod_{\{j_1,\cdots,j_R\}} Det(c'_{j_1},\cdots,c'_{j_R}) \\ &= \prod_{1\in\{j_1,\cdots,j_R\}} Det(c'_{j_1},\cdots,c'_{j_R}) \prod_{1\notin\{j_1,\cdots,j_R\}} Det(c'_{j_1},\cdots,c'_{j_R}) \\ &= p^{\frac{kRM\partial}{n}}\theta(f_1,\cdots,f_R).\end{aligned}$$

Considere agora o caso geral que $\partial = \partial_1 + \cdots + \partial_n$ e

$$\left\{\begin{array}{rcccc} f'_1 &= p^{k\partial_1}a_{11}x_1^k &+ \cdots + & p^{k\partial_n}a_{1n}x_n^k \\ \vdots & \vdots & & \vdots \\ f'_R &= p^{k\partial_1}a_{R1}x_1^k &+ \cdots + & p^{k\partial_n}a_{Rn}x_n^k. \end{array}\right. \tag{1-10}$$

Para qualquer conjunto $\{j_1,\cdots,j_R\}$ temos que

$$Det(c'_{j_1},\cdots,c'_{j_R}) = p^{k\partial_{j_1}}\cdots p^{k\partial_{j_R}}Det(c_{j_1},\cdots,c_{j_R}). \tag{1-11}$$

Efetuando o produto dos determinantes de (1-11) para todos os conjuntos $\{j_1,\cdots,j_R\}$, concluímos que cada termo $p^{k\partial_{j_i}}$ aparece $\dfrac{RM}{n}$ vezes nesse produto. Assim

$$\theta(f'_1,\cdots,f'_R) = p^{\frac{kRM\partial_1}{n}}\cdots p^{\frac{kRM\partial_n}{n}} \prod_{j_1,\cdots,j_R} Det(c_{j_1},\cdots,c_{j_R}) = p^{\frac{kRM\partial}{n}}\theta(f_1,\cdots,f_R).$$

ii) Suponha que

$$\left\{\begin{array}{rcccc} f''_1 &= a''_{11}x_1^k &+ \cdots + & a''_{1n}x_n^k = & 0 \\ \vdots & \vdots & & \vdots & \\ f''_R &= a''_{R1}x_1^k &+ \cdots + & a''_{Rn}x_n^k = & 0. \end{array}\right. \tag{1-12}$$

Vamos representar por c''_j a j-ésima coluna da matriz $A'' = (a''_{ij})_{R\times n}$. Temos que

$$a''_{ij} = \sum_{h=1}^{R} d_{ih}a_{hj}$$

assim

$$A'' = \begin{bmatrix} d_{11} & \cdots & d_{1R} \\ \vdots & & \vdots \\ d_{R1} & \cdots & d_{RR} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{R1} & a_{R2} & \cdots & a_{Rn} \end{bmatrix}. \tag{1-13}$$

Obtemos então a igualdade

$$Det(c''_{j_1},\cdots,c''_{j_R}) = D.Det(c_{j_1},\cdots,c_{j_R}),$$

onde $D = Det(d_{ij}) \neq 0$ e consequentemente

$$\theta(f_1'', \cdots, f_R'') = D^M \theta(f_1, \cdots, f_R).$$

□

A próxima Definição nos diz sobre a p-equivalência para conjuntos de formas.

Definição 1.6 *Dizemos que dois conjuntos de formas $f_1, \cdots, f_R$ e $f_1', \cdots, f_R'$, com coeficientes inteiros, são $p-$equivalentes se um pode ser obtido do outro por uma combinação das operações (i) e (ii) do Lema (1.5) assumindo que $\partial_1, \cdots, \partial_n$ são inteiros e d_{ij} são números racionais com $D \neq 0$.*

Das definições anteriores podemos observar que as operações (i) e (ii) são comutativas e que se as equações $f_1 = 0, \cdots, f_R = 0$ admitem uma solução simultânea não trivial em $\mathbb{Q}_p$, então as equações de qualquer sistema p-equivalente também possuem uma solução simultânea não trivial em $\mathbb{Q}_p$.

1.2 Processo de p-normalização

Com os Lemas vistos e a Definição de sistemas p-equivalentes, daremos atenção ao processo de p-normalização propriamente dito.

Definição 1.7 *Sejam $f_1 = 0, \cdots, f_R = 0$ as equações de um sistema de formas aditivas de grau k. Diremos que esse sistema é $p-$normalizado se forem satisfeitas as seguintes condições:*
(1) $\theta(f_1, \cdots, f_R) \neq 0$.
(2) *A potência de p dividindo $\theta(f_1, \cdots, f_R)$ é a menor possível dentre todos os sistemas com coeficientes inteiros, que são p-equivalentes a $f_1 = 0, \cdots, f_R = 0$.*

1.3 Teorema de Davenport e Lewis

Seja A_0 a matriz dos coeficientes das formas diagonais presentes no nível zero do sistema (1-7). O próximo Lema garante que a matriz A_0 de sistema p-normalizado não é nula, veja em [11] ou [12].

Lema 1.8 (Davenport e Lewis) *i) Um sistema p-normalizado de formas aditivas $f_1 = 0, \cdots, f_R = 0$ pode ser escrito, após uma reordenação das variáveis, na forma,*

$$f_i = F_i(x_1, \cdots, x_m) + pG_i(x_{m+1}, \cdots, x_n) \tag{1-14}$$

para $i = 1, \cdots, R$, *onde*

$$m \geq \frac{n}{k};$$

e se $1 \leq j \leq m$, *então pelo menos um dos coeficientes de algum* x_j^k *não é divisível por p.*

ii) *Para* $1 \leq r \leq R$, *se* q_r *representa o menor número de colunas não nulas módulo p em qualquer r combinações lineares das linhas de* A_0, *independentes módulo p, então*

$$q_r \geq \frac{nr}{Rk}.$$

Prova.

Para obtermos a expressão (1-14) aplique sobre o sistema a separação por níveis, reordenando as variáveis se preciso. Como m representa o número de variáveis do nível zero do sistema devemos mostrar que $m \geq \frac{n}{k}$. Considere que o conjunto de formas aditivas,

$$p^{-1} f_i(px_1, \cdots, px_m, x_{m+1}, \cdots, x_n) = p^{k-1} F_i(x_1, \cdots, x_m) + G_i(x_{m+1}, \cdots, x_n), \ \ com\ i = 1, \cdots, R. \tag{1-15}$$

Essas formas derivam das formas $f_i(x_1, \cdots, x_n)$ através de uma combinação das operações (i) e (ii) do Lema (1.5). A operação (i) é utilizada com $\partial = m$ e a operação (ii) com $D = p^{-R}$. Portanto o valor de θ desse novo conjunto será

$$\theta(p^{-1} f_1, \cdots, p^{-1} f_R) = p^{\frac{kRMm}{n} - RM} \theta(f_1, \cdots, f_R).$$

Como o novo conjunto de formas (1-15) possui coeficientes inteiros, pela minimalidade de sistemas p-normalizados, temos que

$$\frac{kRMm}{n} - RM \geq 0,$$

donde $m \geq \frac{n}{k}$.

Sejam $F_1', \cdots, F_r'$ qualquer r combinações lineares de $F_1, \cdots, F_R$ independentes módulo p, e sejam $f_1', \cdots, f_r'$ qualquer r combinações lineares de $f_1, \cdots, f_R$. Qualquer um desses conjuntos pode ser completado (tomando os $R - r$ elementos restantes de $F_1, \cdots, F_R$ ou $f_1, \cdots, f_R$) para se obter um conjunto de R combinações lineares, independentes módulo p. Seja $q = q_r$ o menor número de variáveis que aparecem em pelo menos uma das combinações de $F_1', \cdots, F_r'$ com um coeficiente não divisível por p. Denominaremos essas variáveis por $x_1, \cdots, x_q$. Considere as formas

$$p^{-1} f_i'(px_1, \cdots, px_q, x_{q+1}, \cdots, x_n) \quad (i = 1, \cdots, r),$$

$$f_i'(px_1, \cdots, px_q, x_{q+1}, \cdots, x_n) \quad (i = r+1, \cdots, R).$$

Além de possuir coeficientes inteiros elas derivam das formas $f_1, \cdots, f_R$ por uma combinação da operação (i), com $\partial = q$ e da operação (ii), com $D = p^{-r}D_0$, donde D_0 é não divisível por p. Pelo mesmo argumento anterior temos

$$\frac{kRMq}{n} - rM \geq 0$$

o que implica que $q \geq \dfrac{nr}{Rk}$. □

Esses são alguns Lemas e Definições que precisaremos para o desenvolvimento dos próximos capítulos.

CAPÍTULO 2

Sistema de Duas Formas Aditivas de Grau k Inteiro Positivo

Neste capítulo desenvolveremos soluções para problemas de estabelecer cotas sobre os primos p para solução no corpo dos p-ádicos, com a hipótese de um número fixo de variáveis. Assim, como caso particular do Teorema 1 de Atkinson, Brüdern e Cook [1], fixamos em 2 o número de equações, onde tem-se que a cota é de $p > k^{2r+2}$. Este capítulo se concentra na demonstração do próximo Teorema, com $p \equiv 1 \pmod{k}$, em que se melhora o caso do Teorema 1:
Sejam r, k, n inteiro positivos com $k > 1$ e $n > 2rk$. Então o sistema de equações

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

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

2.1 Teorema

O seguinte Teorema, cuja demonstração é um dos objetivos deste trabalho, para o caso de um sistema de 2 equações aditivas, melhora o resultado do Teorema 1.

Teorema 2.1 *Sejam n, k inteiros positivos com $k > 1$, $n > 4k$. Então o sistema de equações*

$$\begin{cases} f(x) = a_1x_1^k + \cdots + a_nx_n^k = 0; \\ g(x) = b_1x_1^k + \cdots + b_nx_n^k = 0. \end{cases} \tag{2-1}$$

com coeficientes $a_i, b_i \in \mathbb{Z}$, tem uma solução não trivial p-ádica para todo $p > 3k^4$.

Para a demonstração deste resultado vale observar que $\gamma = 1$, pelo Lema de Hensel, desde que $p > 3k^4$.

Desde que $n > 4k$, pelo Lema de Daveport e Lewis (1.8), com $R = 2$, temos $m = 5$, $q \geq 3$. Partindo as variáveis $x_1, \cdots, x_m$ do sistema (1-2) em blocos tal que em cada bloco as razões $\dfrac{a_{1j}}{a_{2j}}$ são iguais (mod p). Seja r o comprimento do maior bloco de razões

comuns $\frac{a_{1j}}{a_{2j}}$, e t o comprimento do segundo bloco. Assim temos que r é o número de colunas do sistema (2.1) que estão no mesmo espaço vetorial de dimensão 1.

Afirmamos que se $t \geq 3$ então a congruência (1-2) com $R = 2$ tem uma solução geral de posto 2. Sabendo que uma congruência simples

$$ax^k + by^k + cz^k \equiv 0 \pmod{p},$$

com $(p, abc) = 1$, possui uma solução não trivial para todo $p > k^4$, veja em [9], assim nossa afirmação segue do fato que a congruência (1-2), com $R = 2$, contém duas congruências distintas com 3 variáveis. Assumindo que $t \leq 2$ e reduzindo m ao valor inicial de 5, pelo descarte de variáveis para o maior bloco de razões comuns. Chegamos, então, que a congruência (1-2) com $R = 2$, satisfaz:

$$m = 5,\ q \geq 3 \text{ e } r \leq 2,$$

desde que $r = m - q$. Para assegurar uma solução p-ádica (não trivial) é necessário que a solução tenha posto 2. Segue da Definição (1.1) que uma solução

$$\overrightarrow{\xi} = (\xi_1, \cdots, \xi_n)$$

de (1-2) tem posto 2 se a matriz $(a_{ij}\xi_j^{k-1})$ tem posto 2 módulo p.

Com isso dividiremos nossa demonstração em duas partes. A primeira para $r = 1$ e a outra para $r = 2$.

Para a sua demonstração primeiramente reduziremos a procura de solução em inteiros p-ádicos para uma solução em congruência módulo p, via Lema de Hensel. Com o sistema p-normalizado, usando o Teorema de Davenport e Lewis com $q = \partial$ na operação $i)$ do Lema (1.5) e sendo r e t descritos acima. Dividiremos a demonstração em duas etapas, donde a primeira teremos $r = 1$ e na segunda $r = 2$.

2.2 Definições Importantes e Lemas Sobre Somas Exponenciais

Nesta seção vamos analisar sobre somas exponenciais, que é um método muito usado para estimativa do número de soluções de equações de natureza aditiva.

Definição 2.2 *Sejam p um primo, $k > 1$ inteiro e $u \not\equiv 0$ (mod p). Defina*

$$T(u) = \sum_{x=1}^{p} \varepsilon^{ux^k},$$

onde ε é uma raiz primitiva p-ésima da unidade, $\varepsilon = e^{\frac{2\pi i}{p}}$, denotado por $\varepsilon = e(\frac{2\pi i}{p})$.

Observação 2.3

$$T(u) = \sum_{x=1}^{p} e(\frac{2\pi i}{p} u x^k)$$

$$\Rightarrow T(0) = \sum_{x=1}^{p} 1 = p.$$

O próximo Lema nos diz sobre a soma de raízes p-ésimas da unidade.

Lema 2.4 *Sejam p um primo, $x \in \mathbb{Z}$ e $\varepsilon \in \mathbb{C}$ uma raiz p-ésima da unidade, $\varepsilon = e^{\frac{2\pi i}{p}}$. Então*

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

Prova.

Suponha $x = lp$. Logo $\varepsilon^{sx} = 1$ e assim $\sum_{s=0}^{p-1} 1 = p$.

Caso contrário, temos $mdc(x,p) = 1$. Nestas condições, ε^x é também uma raiz primitiva da unidade. Como $\varepsilon^x \neq 1$ e $(\varepsilon^x)^p = 1$, então(ε^x) é raiz do polinômio $x^p - 1$. Mas

$$0 = x^p - 1 = (x-1)(x^{p-1} + ... + x^2 + x + 1),$$

portanto

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

□

Os próximos resultados são sobre caráter de $\mathbb{F}_p^*$.

Definição 2.5 $\chi : \mathbb{F}_p^* \to \mathbb{C}$ *homomorfismo é chamado de caráter multiplicativo módulo p. E*
i)Se $\chi(g) = 1$, $\forall g \in \mathbb{F}_p^*$ denotaremos χ por χ_0 chamado de caráter trivial;
ii)Se $\mathbf{F}_p^* = \{\chi : \mathbb{F}_p^* \to \mathbb{C} | \chi$ é caráter$\}$ defina em $\mathbf{F}_p^*$ a seguinte operação $(\chi\lambda)(g) = \chi(g)\lambda(g)$, $\forall g \in \mathbb{F}_p^*$;
iii)O conjugado de χ denotado por $\overline{\chi}$ é definido por $\overline{\chi}(g) = \overline{\chi(g)}$.

Observação 2.6 $\mathbf{F}_p^*$ *com a operação definida em (ii) é grupo. Defina a ordem de $\chi \in \mathbb{F}_p^*$ como $o(\chi) = |\langle\chi\rangle|$.*

Pela Definição temos a seguinte Proposição:

Proposição 2.7 *Considere χ um caráter $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$. Então*
i)$\chi(1) = 1$,
ii)$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$.

Prova.
i) Como χ é multiplicativo, temos que

$$\chi(1) = \chi(1.1) = \chi(1)\chi(1).$$

Logo $\chi(1)(\chi(1)-1) = 0$, mas $\chi(1) \in \mathbb{C}^*$ portanto, $\chi(1) = 1$.
ii) Dado $g \in \mathbb{F}_p^*$, temos que

$$1 = \chi(1) = \chi(gg^{-1}) = \chi(g)\chi(g^{-1}).$$

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

Seja $m(x)$ o número de soluções da congruência $y^k \equiv x(mod\, p)$. Vamos encontrar uma fórmula explícita para $m(x)$ quando $x \not\equiv 0(mod\, p)$. Seja g uma raiz primitiva módulo p, isto é, $x \in \mathbb{F}_p^*$, então

$$x = g^b, \tag{2-2}$$

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

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

A congruência $kv \equiv b(mod\, p-1)$ tem solução se, e somente se, d divide b, onde $d = mdc(k, p-1)$. Neste caso, existem d soluções incongruentes módulo $p-1$. Este resultado está em [21]. Portanto,

$$m(x) = \begin{cases} d, & se\ b \equiv 0 \pmod{d} \\ 0, & c.c. \end{cases} \tag{2-3}$$

Definição 2.8 *Seja ζ uma raiz d-ésima da unidade. Defina*

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

para $s = 0, 1, \cdots, d-1$, onde b é determinado pela equação (2-2). Esta função é chamada de caráter multiplicativo módulo p.

Quando $s = 0$, denotamos por χ_0 como sendo o caráter trivial. E temos que $\chi_s|_{\mathbb{F}_p^*}$ é homomorfismo de $\mathbb{F}_p^*$ em C.

Proposição 2.9 *Considere a função χ_s. Então*
i)χ_s é uma função multiplicativa;
ii)$\chi_s(1) = 1$ e $\chi_s(g^{-1}) = \chi_s(g)^{-1}$ para $s = 0, 1, \cdots, d-1$.

Prova.
i) Queremos mostrar que $\chi_s(ab) = \chi_s(a)\chi_s(b)$. Escreva $a = g^k$, $b = g^l$, teremos

$$\chi_s(ab) = \varepsilon^{(k+l)s} = \varepsilon^{ks}\varepsilon^{ls} = \chi_s(a)\chi_s(b).$$

ii) Para $\chi_s(1) = 1$. Sendo $1 = g^0$ temos que

$$\chi_s(1) = \varepsilon^{0s} = 1.$$

E também temos que

$$1 = \chi_s(1) = \chi_s(gg^{-1}) = \chi_s(g)\chi_s(g^{-1}).$$

Portanto,

$$\chi_s(g^{-1}) = \chi_s(g)^{-1}.$$

□

Definição 2.10 *Sejam χ_s um caráter multiplicativo módulo p e $\Lambda \in \mathbb{N}$, onde $\Lambda_i = a_i + b_i$ é forma linear em u e v. Defina a Soma Gaussiana relativa a χ_s por*

$$\tau_\Lambda(\chi_s) = \sum_{x=1}^{p} \chi_s(x)\varepsilon^{\Lambda x}.$$

Em particular, quando $\Lambda = 1$, denotamos

$$\tau_1(\chi_s) = \tau(\chi_s).$$

De posse das definições acima, chegamos relação do próximo Lema.

Lema 2.11 *Seja χ_s um caráter não trivial e suponha que $mdc(\Lambda, p) = 1$, então*

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

Prova.

Pela definição de τ_Λ, temos

$$\begin{aligned}\chi_s(\Lambda)\tau_\Lambda(\chi_s) &= \chi_s(\Lambda)\sum_{x=1}^{p}\chi_s(x)\varepsilon^{\Lambda x} \\ &= \sum_{x=1}^{p}\chi_s(\Lambda)\chi_s(x)\varepsilon^{\Lambda x}.\end{aligned}$$

Como χ_s é uma função multiplicativa, segue que

$$\begin{aligned}\chi_s(\Lambda)\tau_\Lambda(\chi) &= \sum_{x=1}^{p}\chi_s(\Lambda x)\varepsilon^{\Lambda x}\\ &= \sum_{y=1}^{p}\chi_s(y)\varepsilon^{y}\\ &= \tau(\chi_s).\end{aligned}$$

□

O próximo Teorema nos dá mais algumas propriedades da função χ_s.

Teorema 2.12 *Considere a função χ_s. Então*
i) $\sum_{s=0}^{d-1}\chi_s(x) = \begin{cases} d, & \text{se } d \text{ divide } b \\ 0, & \text{se c.c.;}\end{cases}$
onde $x \in \mathbb{F}_p$, $x = g^b$, $x \neq 0$, e $d = mdc(k, p-1)$.
ii) $\sum_{x=0}^{p-1}\chi_s(x) = 0$, *desde que* $s \neq 0$, *e* $\sum_{x=0}^{p-1}\chi_0(x) = p-1$.

Prova.
i) Se $x = 0$ temos que $\sum_{s=0}^{d-1}\chi_s(0) = 0$. Se $x \neq 0$ teremos $x = g^b$, logo
ou $d|b$ então, $b = dg'$, assim $\varepsilon^b = 1$ e

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

ou d não divide b então $\varepsilon^b \neq 1$ e $\varepsilon^{kd} = 1$, $\forall k$, assim,

$$\sum_{s=0}^{d-1}\chi_s(x) = \sum_{s=0}^{d-1}\varepsilon^{bs} = \varepsilon^{0s} + \varepsilon^{1s} + \cdots + \varepsilon^{(d-2)s} + \varepsilon^{(d-1)s} = \frac{1-(\varepsilon^{b})^{d}}{1-\varepsilon^{b}} = 0,$$

usando a soma de termos de uma progressão geométrica finita de razão $\varepsilon^b \neq 1$.
ii)Pela definição de χ_0 temos que

$$\sum_{x=0}^{p-1}\chi_0(x) = \sum_{x=0}^{p-1}1 = p-1.$$

Suponha $s \neq 0$. Com $\chi_s \neq \chi_0$, existe $a \in \mathbb{F}_p^*$ tal que $\chi_s(a) \neq 1$. Assim,

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

pois ax percorre $\{0,1,\cdots,p-1\}$ quando x percorre $\{0,1,\cdots,p-1\}$. Logo,

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

Portanto, $\sum_{x=0}^{p-1}\chi_s(x)=0$, desde que $\chi_s(a)\neq 1$ e $\chi_s\neq\chi_0$. □

Assim por i) da propriedade acima e por (2-3) temos que

$$m(x)=\sum_{s=0}^{d-1}\chi_s(x). \tag{2-4}$$

O próximo Lema relaciona Soma Gaussiana e caráter.

Lema 2.13 *i) Se p não divide Λ então*

$$T(\Lambda)=\sum_{r=1}^{k-1}\chi^r(\Lambda)\tau(\chi^{-r}),$$

onde χ é um caráter não trivial de ordem k, e τ é a soma Gaussiana

$$\tau(\chi)=\sum_{x=1}^{p}\chi(x)\varepsilon^{\Lambda x}.$$

ii)E também temos que

$$|\ \tau(\chi^{-r})\ |=\sqrt{p}\ ,\ para\ 1\leq r\leq k-1$$

Prova.
i) Seja $m(x)$ o número de soluções da congruência $y^k\equiv x(mod p)$,
dado por

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

Pela Definição (2.2),

$$\begin{aligned}T(\Lambda) &= \sum_{x=1}^{p}e(\frac{2\pi i}{p}\Lambda x^k)\\ &= \sum_{x=1}^{p}\varepsilon^{\Lambda x^k}\\ &= \sum_{y=1}^{p}m(y)\varepsilon^{\Lambda y}\\ &= \sum_{y=1}^{p}\sum_{r=0}^{k-1}\chi_r(y)\varepsilon^{\Lambda y}\\ &= \sum_{y=1}^{p}\chi_0(y)\varepsilon^{\Lambda y}+\sum_{y=1}^{p}\sum_{r=1}^{k-1}\chi_r(y)\varepsilon^{\Lambda y}.\end{aligned} \tag{2-5}$$

Pela Definição (2.5) temos

$$\begin{aligned} T(\Lambda) &= \sum_{y=1}^{p} \chi_0(y)\varepsilon^{\Lambda y} + \sum_{y=1}^{p}\sum_{r=1}^{k-1} \chi_r(y)\varepsilon^{\Lambda y} \\ &= \sum_{y=1}^{p} \varepsilon^{\Lambda y} + \sum_{y=1}^{p}\sum_{r=1}^{k-1} \chi_r(y)\varepsilon^{\Lambda y} \\ &= \sum_{y=0}^{p-1} \varepsilon^{\Lambda y} + \sum_{y=1}^{p}\sum_{r=1}^{k-1} \chi_r(y)\varepsilon^{\Lambda y}. \end{aligned} \tag{2-6}$$

Pelo Lema (2.4) tendo que p não divide Λ, e pela Definição (2.10),

$$\begin{aligned} T(\Lambda) &= \sum_{y=0}^{p-1} \varepsilon^{\Lambda y} + \sum_{y=1}^{p}\sum_{r=1}^{k-1} \chi_r(y)\varepsilon^{\Lambda y} \\ &= 0 + \sum_{y=1}^{p}\sum_{r=1}^{k-1} \chi_r(y)\varepsilon^{\Lambda y} \\ &= \sum_{y=1}^{k-1}(\sum_{y=1}^{p} \chi_r(y)\varepsilon^{\Lambda y}) \\ &= \sum_{r=1}^{k-1} \tau_\Lambda(\chi_r). \end{aligned} \tag{2-7}$$

Pelo Lema (2.11),

$$\begin{aligned} T(\Lambda) &= \sum_{r=1}^{k-1} \tau_\Lambda(\chi_r) \\ &= \sum_{r=1}^{k-1} (\chi_r(\Lambda))^{-1}\tau(\chi_r) \\ &= \sum_{r=1}^{k-1} \chi^{-r}(\Lambda)\tau(\chi^r) \\ &= \sum_{r=1}^{k-1} \chi^{r}(\Lambda)\tau(\chi^{-r}). \end{aligned} \tag{2-8}$$

Portanto, $T(\Lambda) = \sum_{r=1}^{k-1} \chi^r(\Lambda)\tau(\chi^{-r})$.

ii)Mostraremos este fato para o caso geral no próximo Lema.

□

Lema 2.14 *Sejam χ uma caráter multiplicativo módulo p, $\chi \neq \chi_0$, e $mdc(\Lambda, p) = 1$. Então $\mid \tau_\Lambda(\chi) \mid = \sqrt{p}$.*

Prova.

Temos que $\chi \neq \chi_0$ e $mdc(\Lambda, p) = 1$, então $\Lambda^{p-1} \equiv 1 (mod\, p)$, e

$$\begin{aligned}\chi(\Lambda)^{p-1} &= \chi(\Lambda^{p-1})\\ &= \chi(1)\\ &= 1,\end{aligned}$$

assim $|\,\chi(\Lambda)\,| = 1$. Temos, pelo Lema (2.11), que

$$\begin{aligned}|\,\tau(\chi)\,| &= |\,\chi(\Lambda)\tau_\Lambda(\chi)\,|\\ &= |\,\chi(\Lambda)\,||\,\tau_\Lambda(\chi)\,|\\ &= |\,\tau_\Lambda(\chi)\,|\,.\end{aligned}$$

Mostraremos, então que $|\,\tau(\chi)\,|^2 = p$. Como $|\,\chi(\Lambda)\,| = 1$, ainda pelo Lema (2.11) e $(\chi(\Lambda))^{-1} = \overline{\chi(\Lambda)}$,

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

logo

$$\begin{aligned}(\tau_\Lambda(\chi))^{-1} &= \left[(\chi(\Lambda))^{-1}\tau(\chi)\right]^{-1}\\ &= \chi(\Lambda)(\tau(\chi))^{-1},\end{aligned}$$

portanto

$$\begin{aligned}\tau_\Lambda(\chi)(\tau_\Lambda(\chi))^{-1} &= \tau(\chi)(\tau(\chi))^{-1}\\ &= |\,\tau(\chi)\,|^2\,.\end{aligned}$$

Pois, $|\tau|^2 = \tau\overline{\tau}$, e neste caso $\overline{\tau} = \tau^{-1}$.

Agora,

$$\sum_{\Lambda=0}^{p-1}\tau_\Lambda(\chi)(\tau_\Lambda(\chi))^{-1} = \sum_{\Lambda=0}^{p-1}|\,\tau(\chi)\,|^2 = (p-1)\,|\,\tau(\chi)\,|^2\,. \tag{2-9}$$

Por outro lado

$$\begin{aligned}\tau_\Lambda(\chi)(\tau_\Lambda(\chi))^{-1} &= \Big(\sum_{x=1}^{p}\chi(x)\varepsilon^{\Lambda x}\Big)\Big(\sum_{y=1}^{p}(\chi(y))^{-1}\varepsilon^{-\Lambda y}\Big)\\ &= \sum_{x=1}^{p}\sum_{y=1}^{p}\chi(x)\,[\chi(y)]^{-1}\,\varepsilon^{\Lambda(x-y)}.\end{aligned}$$

Pelo Lema (2.4)

$$\sum_{\Lambda=0}^{p-1}\varepsilon^{\Lambda(x-y)} = \begin{cases} p, & \text{se } x \equiv y(mod\,p)\\ 0, & \text{c.c.}\end{cases}$$

Como x, $y \in \{0,1,\cdots,p-1\}$, então $x \equiv y \ (mod\ p)$ e isto implica que $x = y$. Lembramos que $\chi(0) = 0$,

$$\begin{aligned}\sum_{\Lambda=0}^{p-1} \tau_\Lambda(\chi)(\tau_\Lambda(\chi))^{-1} &= \sum_{x=1}^{p}\sum_{y=1}^{p}\sum_{\Lambda=0}^{p-1} \chi(x)(\chi(y))^{-1}\varepsilon^{\Lambda(x-y)} \\ &= p\sum_{x=1}^{p}\sum_{y=1}^{p} \chi(x)(\chi(y))^{-1} \\ &= p\sum_{z=1}^{p} \chi(z)(\chi(z))^{-1} \\ &= p\sum_{z=1}^{p} \mid \chi(z) \mid^2 \\ &= p(p-1).\end{aligned} \tag{2-10}$$

Comparando (2-9) e (2-10) temos que $(p-1) \mid \tau(\chi) \mid^2 = p(p-1)$ o que implica $\mid \tau(\chi) \mid^2 = p$. O que conclui a demonstração. □

O próximo Lema, será usado na demonstração do Lema posterior.

Lema 2.15 (Hasse-Weil) *Seja p um número primo e seja χ algum caráter não trivial $(mod\ p)$ de ordem k, onde k divide $(p-1)$. Seja $B(x)$ um polinômio da forma*

$$(x-a_1)^{\alpha_1}\cdots(x-a_t)^{\alpha_t},$$

onde os a_i são todos distintos $(mod\ p)$, e $0 < \alpha_i < k$. Então

$$\mid \sum_{x\ mod\ p} \chi(B(x)) \mid \leq (t-1)\sqrt{p}$$

onde o somatório é sobre um conjunto completo de resíduos $mod\, p$.

A prova deste Lema está em [21].

Lema 2.16 *Seja χ um caráter não trivial de ordem k, onde $a_i,\ b_i \in Z$, com a_ib_j-$a_jb_i \not\equiv 0(mod\, p)$ para $i \neq j$, e $a_i \not\equiv 0(mod\, p)$ para $i = 1,\cdots,t$. Sejam $r_1,\cdots,r_t$ inteiros tais que $0 < r_i < k$. Então*

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

Prova.

Sendo χ multiplicativo e $a_i \not\equiv 0(mod\, p)$ temos

$$\begin{aligned}\chi(\prod_{i=1}^{t}(a_i\lambda + b_i)^{r_i}) &= \chi(\prod_{i=1}^{t} a_i^{r_i}\prod_{i=1}^{t}(\lambda + \frac{b_i}{a_i})^{r_i}) \\ &= \chi(\prod_{i=1}^{t} a_i^{r_i})\chi(\prod_{i=1}^{t}(\lambda + c_i)^{r_i})\end{aligned}$$

onde os c_i's são distintos pois $a_ib_j - a_jb_i \not\equiv 0(mod p)$ e $\frac{b_i}{a_i}$ são definidos mod p.

Assim

$$\begin{aligned}
|\sum_{\lambda=1}^{p-1}\chi(\prod_{i=1}^{t}(a_i\lambda+b_i)^{r_i})| &= |\sum_{\lambda=1}^{p-1}\chi(\prod_{i=1}^{t}a_i^{r_1})\chi(\prod_{i=1}^{t}(\lambda+c_i)^{r_i})| \\
&= |\chi(\prod_{i=1}^{t}a_i^{r_i})||\sum_{\lambda=1}^{p-1}\chi(\prod_{i=1}^{t}(\lambda+c_i)^{r_i})| \\
&= |\sum_{\lambda=0}^{p-1}\chi(\prod_{i=1}^{t}(\lambda+c_i)^{r_i}) - \chi(\prod_{i=1}^{t}(c_i)^{r_i})| \\
&\leq |\sum_{\lambda=1}^{p}\chi(\prod_{i=1}^{t}(\lambda+c_i)^{r_i})| + |\chi(\prod_{i=1}^{t}(c_i)^{r_i}| \\
&\leq |\sum_{\lambda=1}^{p}\chi(\prod_{i=1}^{t}(\lambda+c_i)^{r_i})| + 1
\end{aligned}$$

Pelo Lema (2.15) temos

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

□

Lema 2.17 *Seja* $S_n = \sum_{u=1}^{p-1} |T(u)|^n$, *com*

$$\begin{aligned}
T(u) &= \sum_{x=1}^{p} e(\frac{2\pi i}{p}ux^k) \\
&= \sum_{r=1}^{k-1}\chi^r(u)\tau(\chi^{-r}).
\end{aligned}$$

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

Prova.

Por (2-7)

$$\begin{aligned}
|T(u)| &= |\sum_{r=1}^{k-1}\tau_u(\chi_r)| \\
&\leq \sum_{r=1}^{k-1}|\tau_u(\chi^r)|.
\end{aligned}$$

Pelo Lema (2.13) *ii*),

$$\begin{aligned}
|T(u)| &\leq \sum_{r=1}^{k-1}|\tau_u(\chi^r)| \\
&= \sum_{r=1}^{k-1}\sqrt{p} \\
&= (k-1)p^{\frac{1}{2}},
\end{aligned} \tag{2-11}$$

ou seja, $|T(u)| \leq (k-1)p^{\frac{1}{2}}$. E temos que

$$|T(u)|^2 = T(u)\overline{T(u)},$$

assim, usando a Definição (2.2),

$$\begin{aligned}\sum_{u=0}^{p-1}|T(u)|^2 &= \sum_{u=0}^{p-1}T(u)\overline{T(u)} \\ &= \sum_{u=0}^{p-1}\sum_{x=0}^{p-1}\varepsilon^{ux^k}\sum_{y=0}^{p-1}\varepsilon^{-uy^k} \\ &= \sum_{u=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\varepsilon^{u(x^k-y^k)}.\end{aligned} \tag{2-12}$$

Se $x^k \equiv y^k \pmod p$, pelo Lema (2.4), $\sum_{u=0}^{p-1}\varepsilon^{u(x^k-y^k)} = p$. Seja M o número máximo de soluções de $x^k \equiv y^k \pmod p$, teremos, para

$$y = 0 \Rightarrow M = 1,$$

$$y \neq 0 \Rightarrow M = (p-1)(k-1),$$

assim, $M = 1+(p+1)(k-1)$ e,

$$\sum_{u=0}^{p-1}|T(u)|^2 = pM = p(1+(k-1)(p-1)). \tag{2-13}$$

Se $x^k \not\equiv y^k \pmod p$, pelo Lema (2.4), $\sum_{u=0}^{p-1}\varepsilon^{u(x^k-y^k)} = 0$. Portanto,

$$\sum_{u=0}^{p-1}|T(u)|^2 = |T(0)|^2 + \sum_{u=1}^{p-1}|T(u)|^2$$

$$\begin{aligned}\sum_{u=1}^{p-1}|T(u)|^2 &= \sum_{u=0}^{p-1}|T(u)|^2 - |T(0)|^2 \\ &\leq p(1+(k-1)(p-1)) - (\sqrt{p})^2 \\ &= p + p(k-1)(p-1) - p \\ &= (k-1)(p-1)\end{aligned} \tag{2-14}$$

Agora,

$$\begin{aligned} S_n &= \sum_{u=1}^{p-1} |T(u)|^n \\ &= \sum_{u=1}^{p-1} |T(u)|^{n-2} |T(u)|^2. \end{aligned}$$

Usando o resultado acima (2-11), nesta demonstração:

$$\begin{aligned} S_n &= \sum_{u=1}^{p-1} |T(u)|^{n-2} |T(u)|^2 \\ &\leq \sum_{u=1}^{p-1} ((k-1)p^{\frac{1}{2}})^{n-2} |T(u)|^2 \\ &= (k-1)^{n-2} p^{\frac{n}{2}-1} p(k-1)(p-1) \\ &\leq (k-1)^{n-1} p^{\frac{n}{2}+1}. \end{aligned}$$

Portanto,

$$|S_n| \leq (k-1)^{n-1} p^{\frac{n}{2}+1}, \tag{2-15}$$

concluindo a demonstração. □

Lema 2.18 *Seja $p \equiv 1$ (mod k), $p > k^4$. Se $abc \not\equiv 0$ (mod p) então a congruência*

$$ax^k + by^k + cz^k \equiv d (mod p) \tag{2-16}$$

tem solução com $xyz \not\equiv 0$ (mod p).

Prova.

Sendo N_1 o número de todas as soluções de (2-16), e temos que $T(v) = \sum_{x=0}^{p-1} \varepsilon^{vx^k}$, onde ε é a raíz p-ésima da unidade, $\varepsilon = e^{\frac{2\pi i}{p}}$. Pela Definição (2.2) e pela Observação (2.3) temos ainda que

$$\begin{cases} T(0) = p \\ T(v) = 0 \quad \text{se } v \not\equiv 0 \ (mod\ p) \end{cases}$$

Usando somas exponenciais, com x, y e $z \in \mathbb{F}_p$, fazendo x^k por $ax^k + by^k + cz^k - d$, teremos:

$$pN_1 = \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{v=0}^{p-1} \varepsilon^{v(ax^k + by^k + cz^k - d)}$$

$$= \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} \sum_{v=0}^{p-1} \varepsilon^{vax^k} \varepsilon^{vby^k} \varepsilon^{vcz^k} \varepsilon^{-vd}$$

$$= \sum_{v=0}^{p-1} (\sum_{x=0}^{p-1} \varepsilon^{vax^k})(\sum_{y=0}^{p-1} \varepsilon^{vby^k})(\sum_{z=0}^{p-1} \varepsilon^{vcz^k})\varepsilon^{-vd}$$

$$= \sum_{v=0}^{p-1} T(va)T(vb)T(vc)\varepsilon^{-vd}$$

Separando o termo $v = 0 \pmod p$, pela Observação (2.3),

$$T(0a)T(0b)T(0c)\varepsilon^{0d} = (T(0))^3 = p^3 \tag{2-17}$$

teremos,

$$pN_1 = T(0a)T(0b)T(0c)\varepsilon^{0d} + \sum_{v=1}^{p-1} T(va)T(vb)T(vc)\varepsilon^{-vd}$$

$$= p^3 + \sum_{v=1}^{p-1} T(va)T(vb)T(vc)\varepsilon^{-vd}$$

Assim,

$$pN_1 - p^3 = \sum_{v=1}^{p-1} (av)T(bv)T(cv)\varepsilon^{-dv}$$

Como $|\varepsilon^{-dv}| = 1$, teremos

$$\begin{aligned} |pN_1 - p^3| &= |\sum_{v=1}^{p-1} T(av)T(bv)T(cv)\varepsilon^{-dv}| \\ &\leq \sum_{v=1}^{p-1} |T(av)T(bv)T(cv)|. \end{aligned} \tag{2-18}$$

Pela Desigualdade de Hölder:

$$\sum |a_1 \cdots a_n| \leq (\sum |a_1|^n)^{\frac{1}{n}} \cdots (\sum |a_n|^n)^{\frac{1}{n}}$$

teremos,

$$|pN_1 - p^3| \leq \{\sum_{v=1}^{p-1} |T(av)|^3 \sum_{v=1}^{p-1} |T(bv)|^3 \sum_{v=1}^{p-1} |T(cv)|^3\}^{\frac{1}{3}}.$$

Como v percorre $1, 2, \cdots, p-1$, também será para av, bv e cv. Assim cada soma

$$\sum_{v=1}^{p-1} |T(av)|^3 = \sum_{v=1}^{p-1} |T(bv)|^3 = \sum_{v=1}^{p-1} |T(cv)|^3 = S_3;$$

logo, usando o Lema (2.17), teremos:

$$|pN_1 - p^3| \leq S_3 \leq (k-1)^2 p^{\frac{5}{2}}$$

$$\Rightarrow N_1 \geq p^2 - (k-1)^2 p^{\frac{3}{2}}$$

para $p > k^4$ e $k \geq 2 \Rightarrow p^2 - (k-1)^2 p^{\frac{3}{2}} > 3kp$,

$$\Rightarrow N_1 > 3kp$$

Quando $x \equiv 0 \pmod{p}$, a congruência (2-16) transforma-se em $by^k + cz^k \equiv d \pmod{p}$ e o número de soluções (x,y,z) é no máximo kp. Pois para algum dado valor de y existe um número máximo k de soluções para z. Assim o número N_0 de soluções de (2-16) com $xyz \equiv 0 \pmod{p}$ é no máximo $3kp$,

$$N_0 \leq 3kp.$$

Portanto, sendo N_2 o número de soluções para $xyz \not\equiv 0$, $N_1 = N_0 + N_2$, teremos $N_2 > 0$, desde que $p > k^4$ e $k \geq 2$. O que conclui a demonstração. □
Assim chegamos que o sistema (2-16) com $xyz \not\equiv 0 \pmod{p}$ tem solução.

2.3 Demonstração do Teorema (2-1)

Desde que $n > 4k$, pelo Lema de Daveport e Lewis (1.8), com 2 equações, temos que

$$m = 5,\ q \geq 3.$$

Partindo as variáveis $x_1, \cdots, x_m$ do sistema (1-2), com duas equações, em blocos tal que em cada bloco as razões $\frac{a_{1j}}{a_{2j}}$ são iguais (mod p). Seja r o comprimento do maior bloco de razões comuns $\frac{a_{1j}}{a_{2j}}$, e t o comprimento do segundo bloco. Assumindo $t \leq 2$ e reduzindo m para o valor inicial de 5, teremos $r \leq 2$, desde que $r = m - q$. Lembre-se que r é o número de colunas do sistema (2.1) que estão no mesmo espaço vetorial de dimensão 1.

Aqui dividiremos a demonstração do Teorema (2-1) em duas partes. Uma vez que $n > 4k$, $R = 2$ e pelo Lema de Danvenport e Lewis (1.8), obtemos que $m \geq \frac{n}{4}$ e que $q \geq \frac{nr}{Rk}$, logo

$$q \geq 3 \text{ e } m \geq 5.$$

2.4 Teorema (2-1): o caso $r = 1$

Aqui, qualquer solução não trivial tem posto 2 módulo p. Com operações elementares reescreva o sistema (1-2) de congruências na forma

$$\begin{cases} f_0 = & x_1^k + & & a_3 x_3^k + \cdots + a_m x_m^k \equiv 0 & \mod p \\ g_0 = & & x_2^k + & b_3 x_3^k + \cdots + b_m x_m^k \equiv 0 & \mod p \end{cases} \tag{2-19}$$

Seja $\Lambda_i = \Lambda_i(u,v) = ua_i + vb_i$ uma forma linear em u e v. Pela Observação (2.3) e pelo Lema (2.4), calculemos o número de soluções para o caso geral de $x \in \mathbb{F}_p^m$. Temos que

$$\sum_{u=0}^{p-1} \varepsilon^{u(f(x))} \sum_{v=0}^{p-1} \varepsilon^{v(g(x))} = \begin{cases} p^2, & f(x) \equiv g(x) \equiv 0 \ (mod\ p) \\ 0 & c.c. \end{cases}$$

Assim,

$$\begin{aligned} p^2 N &= \sum_{x \in \mathbb{F}_p^m} \sum_{u=0}^{p-1} \varepsilon^{u(a_1 x_1^k + \cdots + a_m x_m^k)} \sum_{v=0}^{p-1} \varepsilon^{v(b_1 x_1^k + \cdots + b_m x_m^k)} \\ &= \sum_{x \in \mathbb{F}_p^m} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \varepsilon^{(ua_1+vb_1)x_1^k} \cdots \varepsilon^{(a_m+vb_m)x_m^k} \\ &= \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \Big(\sum_{x=0}^{p-1} \varepsilon^{\Lambda_1 x_1^k} \Big) \cdots \Big(\sum_{x=0}^{p-1} \varepsilon^{\Lambda_m x_m^k} \Big) \\ &= \sum_{u,v} T(\Lambda_1) \cdots T(\Lambda_m). \end{aligned}$$

Tomando $m = 5$, dado pelo Lema de Davenport e Lewis (1.8), desde que $n > 4k$, em um sistema de 2 equações. Portanto, o número N de soluções da congruência (2-19) é dado por

$$p^2 N = \sum_{u,v} T(\Lambda_1) \cdots T(\Lambda_5).$$

Observação 2.19 *No Capítulo (1), concluímos que a congruência*

$$\begin{cases} f_0 = & a_1 x_1^k + \cdots + a_m x_m^k \equiv 0 & mod\ p \\ g_0 = & b_1 x_1^k + \cdots + b_m x_m^k \equiv 0 & mod\ p \end{cases}$$

satisfaz

$$m = 5,\ q \geq 3 \ e \ r \leq 2,$$

desde que $r = m - q$. Para assegurar uma solução p-ádica não trivial, basta que a solução tenha posto 2. Donde faremos a demonstração do Teorema (2.1) em duas partes: $r = 1$ e $r = 2$ (em seção posterior).

Separando os termos onde $u = v = 0$, temos

$$\begin{aligned} p^2 N &= \sum_{(u,v)=(0,0)} T(\Lambda_1) \cdots T(\Lambda_5) + \sum_{(u,v)\neq(0,0)} T(\Lambda_1) \cdots T(\Lambda_5) \\ &= p^5 + \textstyle\sum_{(u,v)\neq(0,0)} T(\Lambda_1) \cdots T(\Lambda_5). \end{aligned}$$

Portanto,

$$p^2N - p^5 = \sum_{(u,v)\neq(0,0)} T(\Lambda_1)\cdots T(\Lambda_5). \tag{2-20}$$

Agora, separando a soma em termos em que um dos Λ_i's é zero (mod p), denotado por Σ_1, e em termos que nenhum dos Λ_i's é zero (mod p), denotado por Σ_0.

A estimativa de Σ_1 é dada usando o Lema (2.18). E a estimativa de Σ_0 é dada através do Lema (2.16).

2.4.1 Estimativa para Σ_0

Substituindo a expressão de T, dada no Lema (2.13), em $\sum_0$:

$$\begin{aligned}
\Sigma_0 &= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0(p)}} T(\Lambda_1)\cdots T(\Lambda_5) \\
&= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0(p)}} \sum_{\substack{r_1,\cdots,r_5 \\ 1\le r_i\le k-1}} \chi(\Lambda_1^{r_1}\cdots\Lambda_5^{r_5})\tau(\chi^{-r_1})\cdots\tau(\chi^{-r_5}) \\
&= \sum_{\substack{r_1,\cdots,r_5 \\ 1\le r_i\le k-1}} \Big[\sum_{\substack{u,v \\ \Lambda_i \not\equiv 0(p)}} \chi(\Lambda_1^{r_1}\cdots\Lambda_5^{r_5})\tau(\chi^{-r_1})\cdots\tau(\chi^{-r_5})\Big]
\end{aligned}$$

$$\Sigma_0 = \sum_{\substack{r_1,\cdots,r_5 \\ 1\le r_i\le k-1}} \tau(\chi^{-r_1})\cdots\tau(\chi^{-r_5})\Big[\sum_{\substack{u,v \\ \Lambda_i \not\equiv 0(p)}} \chi(\Lambda_1^{r_1}\cdots\Lambda_5^{r_5})\Big].$$

Fixando $r_1,\cdots,r_5$ e avaliando a soma interna. Seja

$$\begin{aligned}
S_0 &= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0(mod\ p)}} \chi\Big(\prod_{i=1}^{5}\Lambda_i^{r_1}\Big) \\
&= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0(mod\ p)}} \chi\Big(\prod_{i=1}^{5}(a_iu+b_iv)^{r_i}\Big) \\
&= \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0(mod\ p)}} \chi\Big(\prod_{i=1}^{5}v^{r_i}(a_i\frac{u}{v}+b_i)^{r_i}\Big)
\end{aligned}$$

$$S_0 = \sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 (mod\ p)}} \chi(v^{r_1+\cdots+r_5} \prod_{i=1}^{5} (a_i \frac{u}{v} + b_i)^{r_i}). \tag{2-21}$$

Note que $\frac{u}{v}$ está bem definido, desde que $v = \Lambda_2 \not\equiv 0 \pmod p$. As condições $\Lambda_1 \not\equiv 0 \pmod p$, $\Lambda_2 \not\equiv 0 \pmod p$ diz que podemos substituir o somatório $\sum_{\substack{u,v \\ \Lambda_i \not\equiv 0 (mod\ p)}}$ por $\sum_{u=1}^{p-1} \sum_{v=1}^{p-1}$. Podemos ignorar a restrição $\Lambda_i \not\equiv 0 \pmod p$, desde que, se $\Lambda_j \equiv 0 \pmod p$ para algum j então $\chi(\prod_{i=1}^{5} \Lambda_i^{r_i} = 0)$ e não contribui para a soma. Assim tomaremos a soma sobre $1 \leq v \leq p-1$. As mudanças de variáveis $v \to v$, $\frac{u}{v} \to \lambda$, é não singular sobre $\mathbb{F}_p^* \times \mathbb{F}_p^*$, assim

$$\begin{aligned} S_0 &= \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} \chi(v^{r_1+\cdots+r_5} \prod_{i=1}^{5} (a_i \frac{u}{v} + b_i)^{r_i}) \\ &= \sum_{v=1}^{p-1} \sum_{\lambda=1}^{p-1} \chi(v^{r_1+\cdots+r_5} \prod_{i=1}^{5} (a_i \lambda + b_i)^{r_i}) \\ &= \sum_{v=1}^{p-1} \chi(v^{r_1+\cdots+r_5} \sum_{\lambda=1}^{p-1} \chi(\prod_{i=1}^{5} (a_i \lambda + b_i)^{r_i}) \end{aligned} \tag{2-22}$$

Separando em duas situações:

i) $r_1 + \cdots + r_5 \not\equiv 0 \pmod k$ e,

ii) $r_1 + \cdots + r_5 \equiv 0 \pmod k$.

Vejamos a primeira, seja $R = r_1 + \cdots + r_5 \not\equiv 0 \pmod k$. Desde que χ tenha ordem k, $\chi^R \neq \chi_0$. Portanto,

$$\begin{aligned} \sum_{v=1}^{p-1} \chi(v^{r_1+\cdots+r_5}) &= \sum_{v=1}^{p-1} \chi(v^R) \\ &= \sum_{v=1}^{p-1} \chi^R(v) \\ &= \sum_{v=0}^{p-1} \chi^R(v) \\ &= 0. \end{aligned}$$

pois, $\chi(0) = 0$ e pela Propriedade (2.12 *ii*) $\sum_{v=0}^{p-1} \chi^R(v) = 0$.

$$\Rightarrow S_0 = \sum_{v=1}^{p-1} \chi(v^{r_1+\cdots+r_5}) \sum_{\lambda=1}^{p-1} \chi(\prod_{i=1}^{5} (a_i \lambda + b_i)^{r_i}) = 0.$$

Portanto $S_0 = 0$ para esses valores de $r_1, \cdots, r_5$.

Para a segunda situação, seja, $R = r_1 + \cdots + r_5 = kw$, para algum w, e assim

$$\chi(v^{r_1+\cdots+r_5}) = \chi(v^{kw}) = 1,$$

desde que χ tenha ordem k, pois, $\chi(1) = 1, k \equiv 0 \pmod{p}$. Portanto

$$\begin{aligned} S_0 &= \sum_{v=1}^{p-1} \chi(v^{r_1+\cdots+r_5}) \sum_{\lambda=1}^{p-1} \chi(\prod_{i=1}^{5}(a_i\lambda + b_i)^{r_i}) \\ &= \sum_{v=1}^{p-1} \chi(v^{kw}) \sum_{\lambda=1}^{p-1} \chi(\prod_{i=1}^{5}(a_i\lambda + b_i)^{r_i}) \\ &= \sum_{v=1}^{p-1} 1 \sum_{\lambda=1}^{p-1} \chi(\prod_{i=1}^{5}(a_i\lambda + b_i)^{r_i}), \end{aligned}$$

$$S_0 = (p-1) \sum_{\lambda=1}^{p-1} \chi(\prod_{i=1}^{5}(a_i\lambda + b_i)^{r_i}).$$

Quando $a_2 \equiv 0 \pmod{p}$ e $b_2 \equiv 1 \pmod{p}$ então,

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

Desde que $r = 1$, nenhum outro $a_i \equiv 0 \pmod{p}$, e podemos aplicar o Lema (2.16) com $t = 4$, para ter

$$S_0 \leq (p-1)(3\sqrt{p} + 1).$$

Podemos, então, completar a estimação sobre $|\Sigma_0|$:

$$\begin{aligned} \Sigma_0 &= \sum_{\substack{r_1, \cdots, r_5 \\ 1 \leq r_i \leq k-1}} \tau(\chi^{-r_1}) \cdots \tau(\chi^{-r_5}) [\sum_{\substack{u, v \\ \Lambda_i \not\equiv 0(p)}} \chi(\Lambda_1^{r_1} \cdots \Lambda_5^{r_5})] \\ &= \sum_{\substack{r_1, \cdots, r_5 \\ 1 \leq r_i \leq k-1}} \tau(\chi^{-r_1}) \cdots \tau(\chi^{-r_5}) S_0. \end{aligned}$$

Mas, para cada conjunto de valores de $(r_1, \cdots, r_5)$,

$$|\tau(\chi^{-r_1}) \cdots \tau(\chi^{-r_5})| = p^{\frac{5}{2}},$$

por (ii) do Lema (2.13). Agora,

$$\Sigma_0 = \sum_{r_1+\cdots+r_5=0(k)} \tau(\chi^{-r_1})\cdots\tau(\chi^{-r_5})S_0 + \sum_{r_1+\cdots+r_5\neq 0(k)} \tau(\chi^{-r_1})\cdots\tau(\chi^{-r_5})S_0.$$

Portanto,

$$\begin{aligned}|\Sigma_0| &\leq \sum_{r_1+\cdots+r_5=0(k)} |\tau(\chi^{-r_1})\cdots\tau(\chi^{-r_5})||S_0| + \sum_{r_1+\cdots+r_5\neq 0(k)} |\tau(\chi^{-r_1})\cdots\tau(\chi^{-r_5})||S_0| \\ &= p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5=0(k)} |S_0| + p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5\neq 0(k)} |S_0| \\ &= p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5=0(k)} |S_0| + 0.\end{aligned}$$

Donde

$$\begin{aligned}|\Sigma_0| &\leq p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5=0(k)} |S_0| \\ &\leq p^{\frac{5}{2}} \sum_{r_1+\cdots+r_5=0(k)} (p-1)(3\sqrt{p}+1).\end{aligned}$$

Note que o conjunto $\{r_1+\cdots+r_5 \equiv 0 \pmod{k}: 1 \leq r_i \leq k-1\}$ é formado pelos vetores $(r_1,\cdots,r_5)$ e a soma $r_1+\cdots+r_5 \equiv 0 \pmod{k}$ é linear. Assim fixando 4 vetores, se existir solução, ela será única. E por contagem, onde $1 \leq r_i \leq (k-1)$, temos que a cardinalidade deste conjunto é $0(k-1)$ ou $1(k-1)$. Portanto $\sharp\{r_1+\cdots+r_5 \equiv 0 \pmod{k}: 1 \leq r_i \leq k-1\} \leq (k-1)^4$.

Portanto,

$$|\Sigma_0| \leq p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4. \tag{2-23}$$

2.4.2 Estimativa para Σ_1

Vamos assumir que $u \equiv \Lambda_1 \equiv 0 \pmod{p}$. Estimando a soma de (2-20),

$$p^2N - p^5 = \sum_{(u,v)\neq(0,0)} T(\Lambda_1)\cdots T(\Lambda_5),$$

com $u \equiv 0 \pmod{p}$, desde que $b_i \not\equiv 0 \pmod{p}$ para $2 \leq i \leq 5$. Teremos

$$\begin{aligned}\Lambda_i = a_iu + b_iv, \text{ com } u \equiv \Lambda_1 \equiv 0 \pmod{p}, \\ \Rightarrow \Lambda_i = b_iv, \quad 2 \leq i \leq 5.\end{aligned}$$

Seja

$$\begin{aligned}\Sigma &= \sum_{u,v} T(\Lambda_2)\cdots T(\Lambda_5) \\ &= \sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\prod_{i=2}^{5} T(\Lambda_i) \\ &= \sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\prod_{i=2}^{5} T(b_iv) \\ &= (p-1)\sum_{v=1}^{p-1}\prod_{i=2}^{5} T(b_iv).\end{aligned}$$

Fazendo $b_i v \to v$, teremos, pela definição do Lema (2.17),

$$\begin{aligned}\Sigma &= (p-1)\sum_{v=1}^{p-1}\prod_{i=2}^{5} T(v);\\ |\Sigma| &\leq (p-1)\sum_{v=1}^{p-1}|T(v)|^4\\ &= (p-1)S_4,\end{aligned}$$

desde que $b_i \not\equiv 0 \pmod{p}$ para $2 \leq i \leq 5$. E pelo Lema (2.17),

$$\begin{aligned}\Sigma &\leq (p-1)S_4\\ &\leq (p-1)(k-1)^3 p^3\\ &\leq p^4(k-1)^3.\end{aligned}$$

Multilicando por 5, pois cada Λ_i pode ser zero (mod p),

$$|\Sigma_1| = 5|\Sigma| \leq 5p^4(k-1)^3. \tag{2-24}$$

Pelas Equações (2-20), (2-23) e (2-24), temos que

$$\begin{aligned}|p^2N - p^5| &\leq |\Sigma_0| + |\Sigma_1|\\ &\leq p^{\frac{5}{2}}(p-1)(3\sqrt{p}+1)(k-1)^4 + 5p^4(k-1)^3,\end{aligned}$$

para que $N > 0$, precisamos de

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

ou, o equivalente,

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

Pois se $N = 0$ teríamos

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

Para $p > 3k^4$,

$$\begin{aligned}(3+\frac{1}{\sqrt{p}})(k-1)^4 &= 3(k-1)^4 + \frac{1}{\sqrt{p}}(k-1)^4\\ &< 3(k-1)^4 + \frac{(k-1)^4}{\sqrt{3}k^2}\\ &< 3(k-1)^4 + \frac{(k-1)^4}{k^2}\\ &< 3(k-1)^4 + k^2.\end{aligned}$$

Perceba que $\frac{p-1}{p} < 1$, e com $p > 3k^4$, temos

$$\begin{aligned}\frac{(p-1)}{p}(3+\frac{1}{\sqrt{p}})(k-1)^4+5(k-1)^3 &< (3+\frac{1}{\sqrt{p}})(k-1)^4+5(k-1)^3\\ &< 3(k-1)^4+k^2+5(k-1)^3\\ &< 3k^4\\ &< p.\end{aligned}$$

Observe que,

$$\begin{aligned}3(k-1)^4+k^2+5(k-1)^3-3k^4 &= -7k^3+4k^2+3k-2\\ &= k^3(-7+\frac{4}{k}+\frac{3}{k^2}-\frac{2}{k^3})\\ &< k^3(-4-\frac{2}{k^3})\\ &< 0.\end{aligned}$$

Isto significa que, temos solução ($N > 0$) para todo $p > 3k^4$.

2.5 Teorema (2-1): o caso $r = 2$

Na segunda parte da demonstração, estamos assumindo que $r = 2$, onde r é o número de colunas do sistema (2.1) que estão no mesmo espaço vetorial de dimensão 1, ou ainda, r é o comprimento do maior bloco de razões comuns $\frac{a_{1j}}{a_{2j}} \pmod p$ do sistema (1-2), com duas equações, ou seja $R = 2$. E com

$$m = 5 \text{ e } q \geq 3.$$

Com operações elementares, reescreva a congruência na forma

$$\begin{cases} f_0 = & x_1^k + a_2x_2^k + & a_3x_3^k + \cdots + a_5x_5^k \equiv 0 \pmod p \\ g_0 = & & b_3x_3^k + \cdots + b_5x_5^k \equiv 0 \pmod p, \end{cases} \tag{2-25}$$

onde, possivelmente, $a_4 \equiv 0 \pmod p$, $a_5 \not\equiv 0 \pmod p$ e $b_3b_4b_5 \not\equiv 0 \pmod p$.

Lema 2.20 *Seja $p \equiv 1 \pmod k$. Se $r = 2$ então a congruência (2-25) tem uma solução de ordem 2 mod p, com a condição de $p > 3k^4$.*

Prova.

Resolva

$$b_3x_3^k + \cdots + b_5x_5^k \equiv 0 \pmod p$$

com $x_3x_4x_5 \not\equiv 0 \pmod{p}$, usando o Lema 2.18. Esta solução envolve duas colunas de coeficientes linearmente independentes. Seja $A = a_3x_3^k + \cdots + a_5x_5^k \equiv 0$. Se $A \equiv 0 \pmod{p}$, basta tomar $x_1 = x_2 = 0$ para dar uma solução. Se $A \not\equiv 0 \pmod{p}$, multiplique x_3, x_4 e x_5 por ξ e resolva

$$x_1^k + a_2x_2^k + A\xi^k \equiv 0(mod\, p)$$

com $x_1x_2\xi \not\equiv 0 \pmod{p}$ e então use o Lema (2.18), para dar uma solução. □

Assim, podemos combinar os dois resultados, para $r = 1$ e $r = 2$. O que mostra que a congruência (1-2)

$$\sum_{j=1}^{n} a_{ij}x_j^k \equiv 0(mod\, p^\gamma) \quad (1 \le i \le R)$$

para $R = 2$,

$$\begin{aligned} f_0 &= a_1x_1^k + \cdots + a_sx_s^k \equiv 0 \qquad (\text{mod } p) \\ g_0 &= b_1x_1^k + \cdots + b_sx_s^k \equiv 0 \qquad (\text{mod } p), \end{aligned}$$

tem solução de ordem 2 (mod p) para todo $p > 3k^4$.

Portanto, pelo Lema (Hensel) (1.2), a equação (2-1):

$$\begin{aligned} f(x) &= a_1x_1^k + \cdots + a_nx_n^k = 0; \\ g(x) &= b_1x_1^k + \cdots + b_nx_n^k = 0. \end{aligned}$$

tem solução p-ádica não trivial para todo p, o que demonstra o Teorema (2.1).

CAPÍTULO 3

Sistemas de Duas Formas Aditivas de Grau 5

Neste capítulo iremos demonstrar em sistemas de duas equações, ou seja $R = 2$, em um primeiro momento que a solução é garantida com $N \geq 6k+1$. E outro caso, com o grau da forma aditiva $k = 5$, chegaremos a solução apartir de 31 variáveis.

No Capítulo 1, tínhamos que o valor de p era grande, $p > 3k^4$, se comparada com o grau k e com a quantidade de variáveis: $n > 4k$. Neste Capítulo o objetivo é encontrar cotas para o número n de variáveis apartir de valores de p com o grau fixo $k = 5$, das formas aditivas, quando aqui ainda estamos fixando o número de equações do sistema em $R = 2$.

3.1 Teoremas

Teorema 3.1 *Seja p um primo e k um inteiro ímpar tal que p não divide k. Suponha que a equação*

$$ax^k + by^k + cz^k \equiv d \ (mod\ p),$$

com a, b e c não nulos módulo p, tem uma solução com $xyz \not\equiv 0 \ (mod\ p)$*, para todo d. Então qualquer sistema de duas formas aditivas de grau k com ao menos* $6k+1$ *variáveis sempre tem solução p-ádica não trivial.*

Se fizermos uma comparação deste Teorema com o Teorema (2-1), onde $k > 1$, $n > 4k$ e $p > 3k^4$. Aqui temos que k é ímpar, um aumento pequeno, relativamente, no número de variáveis: $n > 6k+1$, porém temos que p é qualquer desde que satisfaça a hipótese adicional com respeito a solubilidade da congruência

$$ax^k + by^k + cz^k \equiv d \ (\text{mod } p).$$

.

Corolário 3.2 *Seja k um inteiro ímpar e p um primo, com* $p > k^4$*. Então qualquer sistema de duas formas aditivas de grau ímpar k com pelo menos* $6k+1$ *variáveis sempre tem solução p-ádicas não trivial.*

Prova.

Como $p > k^4$ então p não divide k. Pelo Lema (2.18) a equação

$$ax^k + by^k + cz^k \equiv d(\text{mod } p),$$

tem solução com $xyz \not\equiv 0 \pmod{p}$. □

O Teorema (3.1) foi adaptado da conjectura de E. Artin, que vimos na Introdução, para sistemas de duas formas aditivas, agora com grau ímpar $k \geq 5$, usando hipóteses adicionais. Para o caso especial de sistemas de duas formas aditivas de grau 5 temos o próximo resultado:

Teorema 3.3 *Todo sistema de duas formas quínticas aditivas com N variáveis sempre tem solução p-ádica não trivial*
i) *para todo* $p > 101$ *desde que* $N \geq 31$*;*
ii) *para todo p desde que* $N \geq 36$*, e* $p \neq 5$ *e* 11.

Se observamos a relação deste Teorema com o Capítulo (2), aqui temos que $k = 5$, e voltando ao Teorema (2-1), temos que $n > 20$ e teríamos $p > 1875$ para o Teorema (3.3). Portanto, com este Teorema, para a garantia de solubilidade do sistema basta um pequeno aumento no número de variáveis $n > 31$ para se ter uma redução colossal no valor de p, $p > 101$. Já na segunda parte do Teorema (3.3) para qualquer valor de $p \neq 5$ e 11, a quantidade de variáveis que garante a solubilidade do sistema é um pouco maior que na primeira parte: $n > 36$; mas ainda bastante pequena se compararmos o valor de p no Teorema (2-1).

Sendo $\mathbb{F}_p^*$, visto no Capítulo(2) em (2.2), o grupo de todos os elementos não nulos de $\mathbb{F}_p$, e seja K o subgrupo de $\mathbb{F}_p^*$ de todas as k-ésimas potências. Desde que estamos assumindo $p \equiv 1 \pmod{k}$, existe $\delta \in (\mathbb{F}_p^* - K)$ tal que

$$\mathbb{F}_p^* = K \cup \delta K \cup \delta^2 K \cup \cdots \cup \delta^{k-1} K \quad \text{(união disjunta)}.$$

Denotaremos por S o seguinte conjunto de representantes das k classes

$$\mathtt{S} = \{1, \delta, \delta^2, \cdots, \delta^{k-1}\}.$$

Segue dessas considerações que todo $\alpha \in \mathbb{F}_p^*$ pode ser escrito na forma

$$\alpha = \delta^i a^k \tag{3-1}$$

para algum $a \in \mathbb{F}_p^*$ e algum $\delta^i \in \mathtt{S}$.

3.2 Congruências módulo p

A prova do próximo lema foi dada por D. Atkinson e R. J. Cook [2], em 1989.

Lema 3.4 *Seja $p > 11$, $p \equiv 1$ (mod 5) e considere a equação*

$$a_1 x_1^5 + \cdots + a_r x_r^5 \equiv d \ (mod\ p)$$

com $a_1 \cdots a_r \not\equiv 0$ e para todo d.
i) Se $r \geq 3$ então a equação tem solução não trivial.
ii) Se $r \geq 3$ e $p > 101$ então o sistema tem solução com $x_1 x_2 x_3 \not\equiv 0$ (mod p).

Este lema nos dá solução para a equação

$$ax^k + by^k + cz^k \equiv d \pmod{p},$$

com $xyz \not\equiv 0 \pmod{p}$ e $k = 5$ apartir de $p > 101$. Se voltarmos ao Lema (2.18) a solução da equação só é garantida com $p > 625$.

Lema 3.5 *Seja a, b e c inteiros não nulos módulo p. A equação*

$$ax^k + by^k \equiv -c (mod p) \tag{3-2}$$

tem solução com $xy \not\equiv 0$ (mod p) se, e somente se, a equação correspondente

$$ax^k + by^k + cz^k \equiv 0 \ (mod\ p)$$

tem solução com $xyz \not\equiv 0$ (mod p).

Prova.

Seja (ξ_1, ξ_2, ξ_3) solução da equação $ax^k + by^k + cz^k \equiv 0 \pmod{p}$, logo $(\xi_1 \xi_3^{-1}, \xi_2 \xi_3^{-1})$ é solução de $ax^k + by^k \equiv -c \pmod{p}$.

□

Lema 3.6 *Seja $p > 11$ e $p \equiv 1$ (mod 5). A equação*

$$a_1 x_1^5 + a_2 x_2^5 + a_3 x_3^5 \equiv 0 \ (mod\ p),$$

com $a_1 a_2 a_3 \not\equiv 0$ (mod p) tem solução com $x_1 x_2 x_3 \not\equiv 0$ (mod p) se a_1, a_2 e a_3 estão em distintas classes laterais módulo o subgrupo das quintas potências de $\mathbb{F}_p^*$.

Prova.

Pelo Lema (3.4) existe solução não trivial (ξ_1,ξ_2,ξ_3) para esta equação. Se $\xi_i \equiv 0 \pmod{p}$, então $a_j \equiv a_k(\xi_k\xi_j^{-1})^5 \pmod{p}$, o que é impossível, porque todos os três coeficientes estão em classes laterais distintas.

□

O próximo Lema está provado em O. D. Atkinson e R. J. Cook, 1989, [2].

Lema 3.7 *Seja $p > 11$ e $p \equiv 1$ (mod 5). O sistema*

$$\begin{cases} a_1x_1^5 + \cdots + a_6x_6^5 \equiv 0 (mod\, p) \\ b_1x_1^5 + \cdots + b_6x_6^5 \equiv 0 (mod\, p) \end{cases},$$

tem solução não trivial módulo p.

3.3 Demonstração dos Teoremas (3.1) e (3.3).

3.3.1 Demonstração do Teorema (3.1)

Neste capítulo consideramos sistemas de duas formas aditivas p-normalizadas de grau k ímpar, onde p não divide k, com pelo menos $6k+1$ variáveis, com hipótese adicional de que a equação

$$ax^k + by^k + cz^k \equiv d \pmod{p}$$

com $abc \not\equiv 0 \pmod{p}$ tem solução com $xyz \not\equiv 0 \pmod{p}$, para todo d.

Seja o sistema

$$\begin{cases} F_1(x_1,\cdots,x_N) = a_{11}x_1^k + \cdots + a_{1N}x_N^k = 0 \\ F_2(x_1,\cdots,x_N) = a_{21}x_1^k + \cdots + a_{2N}x_N^k = 0 \end{cases}, \tag{3-3}$$

com $a_{ij} \in \mathbb{Q}_p$ e $N > 6k+1$. Se multiplicarmos cada uma destas equações por um inteiro p-ádico conveniente podemos considerar que $a_{ij} \in \mathbb{Z}_p$.

Como cada inteiro p-ádico é congruente a um inteiro racional módulo p, veja por exemplo em [17], então podemos resolver essas congruências módulo p, considerando que $a_{ij} \in \mathbb{Z}$. Podemos considerar que (3-3) é p-normalizado, usando o Lema de Davenport e Lewis (1.8) reescreva o sistema (3-3) na forma

$$\begin{cases} F_1 = f_1(x_1,\cdots,x_n) + pg_1(x_{n+1},\cdots,x_N) = 0 \\ F_2 = f_2(x_1,\cdots,x_n) + pg_2(x_{n+1},\cdots,x_N) = 0 \end{cases}, \tag{3-4}$$

onde

$$n \geq 7 \; e \; q_1 \geq 4. \tag{3-5}$$

Pelo Lema de Hensel (1.2) é suficiente garantir a existência de uma solução de posto 2 módulo p para o sistema

$$\begin{cases} f_1(x_1,\cdots,x_n) \equiv 0(mod p) \\ f_2(x_1,\cdots,x_n) \equiv 0(mod p) \end{cases}. \tag{3-6}$$

A prova do Teorema (3.1) segue pela próxima proposição.

Proposição 3.8 *Seja k um inteiro ímpar e suponha que a equação*

$$ax^k + by^k + cz^k \equiv d \ (mod\ p)$$

com a, b e c não nulos módulo p, tenha solução com $xyz \not\equiv 0 \ (mod\ p)$, para algum d. Considere o sistema

$$\begin{cases} f = a_{11}x_1^k + \cdots + a_{1n}x_n^k \equiv A \ (mod p), \\ g = a_{21}x_1^k + \cdots + a_{2n}x_n^k \equiv B \ (mod p). \end{cases}$$

Seja q o menor número de variáveis ocorrendo em alguma combinação linear não-nula $\lambda f + \mu g$ módulo p. Então (3.8) tem uma solução posto 2 para algum A, $B \in \mathbb{F}_p$, com a condição de

$$n \geq 7 \ e \ q \geq 3.$$

Prova.

Seja r o número máximo de soluções da matriz coeficiente deste sistema linear que estão no subespaço unidimensional de $\mathbb{F}_p^2$. Segue das hipóteses que $r+q \geq 7$, e o sistema (3.8) é equivalente a

$$\begin{cases} a_1x_1^k + \cdots + a_rx_r^k + b_1y_1^k + \cdots + b_qy_q^k \equiv \alpha(mod p) \\ c_1y_1^k + \cdots + c_qy_q^k \equiv \beta(mod p) \end{cases}. \tag{3-7}$$

Seja $(\xi_1,\cdots,\xi_q)$ uma solução para $c_1y_1^k + \cdots + c_qy_q^k \equiv \beta(mod p)$ com pelo menos três coordenadas não-nulas módulo p, que é possível pelas hipóteses. Agora, seja $b_1\xi_1^k + \cdots + b_q\xi_q^k \equiv \tau(mod p)$ e considere a congruência

$$a_1x_1^k + \cdots + a_rx_r^k \equiv \alpha - \tau(mod p). \tag{3-8}$$

Se $r \geq 3$ então, pelas hipóteses, podemos encontrar uma solução não-trivial

$$(\varepsilon_1,\cdots,\varepsilon_r)$$

para (3-8), e

$$(\varepsilon_1,\cdots,\varepsilon_r,\xi_1,\cdots,\xi_q)$$

é uma solução posto 2 para (3-7).

Suponha $r = 2$. Se $\tau \equiv \alpha \pmod{p}$ então

$$(0, 0, \xi_1, \cdots \xi_q)$$

é uma solução posto 2 para (3-7), por causa desta solução temos pelo menos três coordenadas não-nulas módulo p e $r = 2$. Agora, suponha $\alpha - \tau \not\equiv 0 \pmod{p}$. Pelo Lema (3.5), existe uma solução

$$(\varepsilon_1, \varepsilon_2)$$

para (3-8) e então

$$(\varepsilon_1, \varepsilon_2, \xi_1, \cdots \xi_q)$$

é uma solução posto 2 para (3-7).

Suponha agora que $r = 1$ e que $q \geq 6$. Podemos considerar o caso $c_1, \cdots, c_q \in \mathtt{S}$ (veja (3-1)). Suponha que existam índices $1 \leq i < j \leq q$ tal que $c_i = c_j$, podemos dizer que $c_1 = c_2$. Agora observe que devemos ter $b_1 \not\equiv b_2 (\text{mod } p)$, para $r = 1$.

Pelas hipóteses, podemos encontrar uma solução não-trivial $(\xi_3, \cdots, \xi_q)$ para $c_3 y_3^k + \cdots + c_q y_q^k \equiv \beta \pmod{p}$. Seja $b_3 \xi_3^k + \cdots + b_q \xi_q^k \equiv \tau \pmod{p}$. Se $\tau \equiv \alpha \pmod{p}$, a demonstração segue como acima e

$$(0, 0, 0, \xi_3, \cdots, \xi_q)$$

é solução de (3-7). Se $\tau \not\equiv \alpha \pmod{p}$. Escrevendo $y_1 = -y_2 = T$ podemos formar a congruência

$$a_1 x_1^k + (b_1 - b_2) T^k \equiv \alpha - \tau (mod p). \tag{3-9}$$

Esta congruência tem solução não-trivial

$$(\varepsilon_1, \varepsilon_2),$$

pelo Lema 3.5, e então

$$(\varepsilon_1, \varepsilon_2, -\varepsilon_2, \xi_3, \cdots, \xi_q)$$

é uma solução posto 2 para (3-7), desde $r = 1$.

Agora suponha que $c_1, \cdots, c_q$ estão todos em distintas classes laterais módulo o subgrupo K das k-ésimas potências de $\mathbb{F}_p^*$. Desde que $r = 1$ e $q \geq 6$, podemos reescrever o sistema 3-7 na forma

$$\begin{cases} a_1 x_1^k + & b_1 y_1^k + \cdots + b_{q-1} y_{q-1}^k & & \equiv \alpha (mod p) \\ & c_1 y_1^k + \cdots + c_{q-1} y_{q-1}^k & + c_q y_q^k & \equiv \beta (mod p) \end{cases} \tag{3-10}$$

com todos coeficientes b_i e c_j diferentes de zero módulo p e com possíveis substituições de α e β.

Pelas hipóteses, encontramos soluções não-triviais $(\varepsilon_1,\xi_1,\xi_2)$ e $(\xi_3,\cdots,\xi_{q-1})$ para $a_1x_1^k+b_1y_1^k+b_2y_2^k\equiv 0\ (\text{mod } p)$ e $b_3y_3^k+\cdots+b_{q-1}y_{q-1}^k\equiv\alpha\ (\text{mod } p)$ respectivamente, com $\varepsilon_1\xi_1\cdots\xi_{q-1}\not\equiv 0\ (\text{mod } p)$. Seja $c_1\xi_1^k+c_2\xi_2^k\equiv\gamma\ (\text{mod } p)$ e $c_3\xi_3^k+\cdots+c_{q-1}\xi_{q-1}^k\equiv\tau$ (mod p).

Se $\tau\equiv\beta\ (\text{mod } p)$ então

$$(0,0,0,\xi_3,\cdots,\xi_{q-1},0)$$

é uma solução posto 2 para (3-10), desde que $r=1$.

Se $\tau\not\equiv\beta\ (\text{mod } p)$ e observe que devemos ter $\gamma\not\equiv 0(\text{mod } p)$, pois c_1 e c_2 estão em classes laterais distintas. Do contrário teríamos $c_1\xi_1^k+c_2\xi_2^k\equiv 0$ e c_1 e c_2 na mesma classe módulo k, o que é uma contradição.

Depois multiplique a solução $(\varepsilon_1,\xi_1,\xi_2)$ por uma nova variável T, podemos formar a congruência

$$\gamma T^k+c_qy_q^k\equiv\beta-\tau\ (mod\ p) \tag{3-11}$$

que tem solução não-trivial, pelo Lema (3.5),

$$(\rho,\xi_q).$$

Então

$$(\varepsilon_1\rho,\xi_1\rho,\xi_2\rho,\xi_3,\cdots,\xi_{q-1},\xi_q)$$

é uma solução posto 2 para (3-10).

□

3.3.2 Demonstração do Teorema (3.3)

Para a parte (i) do Teorema (3.3), segue do Teorema (3.1), desde que para $k=5$ e $p>101$, a equação $ax^5+by^5+cz^5\equiv d\ (\text{mod } p)$ tem solução com $xyz\not\equiv 0\ (\text{mod } p)$, conforme Lema (3.4).

Para a parte (ii) do Teorema (3.3), suponha o par de formas aditivas de grau 5, p-normalizado, com 36 variáveis. Pelo Capítulo (1), pelo Lema de Davenport e Lewis (1.8), basta demonstrar que qualquer sistema

$$\begin{cases} f_1(x_1,\cdots,x_n)\equiv 0 \quad (mod\ \ p) \\ f_2(x_1,\cdots,x_n)\equiv 0 \quad (mod\ \ p) \end{cases} \tag{3-12}$$

de grau 5 e satisfazendo

$$n \geq 8 \ \ e \ \ q_1 \geq 4, \tag{3-13}$$

tem solução posto 2 módulo p. Se $p \not\equiv 1 \pmod 5$, reduza este sistema a duas congruências lineares, e por (3-13), teremos soluções posto 2. A demonstração do Teorema (3.3(ii)), para $p \equiv 1 \pmod 5$, é dada como consequência da próxima proposição.

Proposição 3.9 *Seja $p > 11$ e $p \equiv 1$ (mod 5) e considere o sistema*

$$\begin{cases} f = a_1x_1^5 + \cdots + a_8x_8^5 \equiv A \ \ (mod \ \ p) \\ g = b_1x_1^5 + \cdots + b_8x_8^5 \equiv B \ \ (mod \ \ p) \end{cases}.$$

Seja q o número mínimo de variáveis que aparecem em toda combinação linear não-nula $\lambda f + \mu g$ módulo p. Então este sistema tem solução posto 2 para quaisquer A, $B \in \mathbb{F}_p$ desde que $q \geq 3$.

O sistema acima equivale ao sistema

$$\begin{cases} a_1^5 + \cdots + a_rx_r^5 + \quad b_1y_1^5 + \cdots + b_q^5y_q^5 \equiv \alpha \ \ (mod \ p) \\ \qquad\qquad\qquad\qquad\quad c_1y_1^5 + \cdots + c_q^5y_q^5 \equiv \beta \ \ (mod \ p) \end{cases}, \tag{3-14}$$

satisfazendo $r+q = 8$ e $q \geq 3$. Os próximos três lemas são suficientes para a demonstração desta Proposição (3.9).

Lema 3.10 *Se $r \geq 3$ então o sistema (3-14) tem solução posto 2 módulo p, para todo α, $\beta \in \mathbb{F}_p$.*

Prova.

Seja $b_1y_1^5 + \cdots + b_q^5y_q^5 \equiv \gamma \pmod p$. O Lema (3.4) nos garante uma solução não trivial para $c_1y_1^5 + \cdots + c_q^5y_q^5 \equiv \beta \pmod p$, pois $q \geq 3$ e $p > 11$ e $p \equiv 1 \pmod 5$. Seja $(\xi_1, \cdots, \xi_q)$ esta solução. Ainda usando o Lema (3.4) para

$$a_1x_1^5 + \cdots + a_r^5x_r^5 \equiv \alpha - \gamma \ (mod \ p) \tag{3-15}$$

temos uma solução, digamos, $(\rho_1, \cdots, \rho_r)$.

Assim

$$(\rho_1, \cdots, \rho_r, \xi_1, \cdots, \xi_q)$$

é uma solução não trivial de posto 2 para o sistema (3-14).

□

Lema 3.11 *Se $r = 2$ então o sistema (3-14) tem solução, posto 2, módulo p, para todo α, $\beta \in \mathbb{F}_p$.*

Prova.

Como $r = 2$ temos $q = 6$, pelo sistema da Proposição (3.9). Suponha que $c_1, \cdots, c_6 \in \mathtt{S}$, onde $|\mathtt{S}| = 5$, visto em (3-1).

Caso 1 : Sendo dois destes coeficientes iguais, digamos $c_5 = c_6$. Suponha $b_5 \not\equiv b_6 \pmod p$.

E usando o Lema (3.4) para $c_1y_1^5 + c_2y_2^5 + c_3y_3^5 \equiv \beta - c_4 \pmod p$, temos uma solução não trivial (ξ_1, ξ_2, ξ_3). Seja $b_1\xi_1^5 + b_2\xi_2^5 + b_3\xi_3^5 + b_4 1^5 \equiv \gamma \pmod p$. Fixe $y_5 = -y_6 = T$, e obtemos a congruência

$$a_1x_1^5 + a_2x_2^5 + (b_5 - b_6)T^5 \equiv \alpha - \gamma (mod\ p), \tag{3-16}$$

que, ainda pelo Lema 3.4 tem solução não trivial, digamos,

$$(\rho_1, \rho_2, \rho_3).$$

Portanto,

$$(\rho_1, \rho_2, \xi_1, \xi_2, \xi_3, 1, \rho_3, -\rho_3)$$

é uma solução de posto 2 para (3-14), com pelo menos três coordenadas não-nulas, e por hipótese $r = 2$.

Caso 2 : Se houver três coordenadas iguais entre $c_1, \cdots, c_6$ digamos, $c_i = c_j = c_l$, então o caso $b_i \equiv b_j \equiv b_l \pmod p$ não ocorre, para $r = 2$. Em seguida reenumere as variáveis y_i, y_j, y_l, e faça $c_5 = c_6$ e $b_5 \not\equiv b_6 \pmod p$ e de modo análogo a acima, obtenha uma solução de posto 2 para o sistema (3-14).

Caso 3 : Duas das coordenadas iguais, suponha $c_5 = c_6$, e $b_5 \equiv b_6$.Também assuma que c_i e c_j são tais que c_i, c_j e c_6 são distintos dois a dois. Se necessário reenumere as variáveis $y_1, \cdots, y_6$ para obter esta distinção. Assim o sistema será equivalente a

$$\begin{cases} a_1x_1^5 + a_2x_2^5 + & b_1y_1^5 + b_2y_2^5 + b_3y_3^5 + b_4y_4^5 & & \equiv \alpha\ (mod\ p) \\ & c_1y_1^5 + c_2y_2^5 + c_3y_3^5 + c_4y_4^5 & + c_5y_5^5 + c_6y_6^5 & \equiv \beta\ (mod\ p) \end{cases}. \tag{3-17}$$

Pelo Lema (3.6) temos que a equação

$$c_1y_1^5 + c_2y_2^5 + c_6y_6^5 \equiv 0\ (mod\ p) \tag{3-18}$$

tem solução não trivial, com as três coordenads não nulas módulo p, seja ela (ξ_1, ξ_2, ξ_6).

Primeiro suponha que $b_1\xi_1^5 + b_2\xi_2^5 \equiv \psi \not\equiv 0 \pmod p$. E pelo Lema (3.4) faça (τ_3, τ_4, τ_5) uma solução de $c_3y_3^5 + c_4y_4^5 + c_5y_5^5 \equiv \beta \pmod p$. Seja $b_3\tau_3^5 + b_4\tau_4^5 \equiv \phi \pmod p$,

e multiplique a solução (ξ_1, ξ_2, ξ_6) por uma variável T, e teremos a congruência

$$a_1x_1^5 + a_2x_2^5 + \psi T^5 + \phi \equiv \alpha (mod\ p), \tag{3-19}$$

que, ainda pelo Lema (3.4) tem solução não trivial, digamos (ρ_1, ρ_2, ρ_3). Portanto,

$$(\rho_1, \rho_2, \rho_3\xi_1, \rho_3\xi_2, \tau_3, \tau_4, \tau_5, \rho_3\xi_6)$$

é uma solução para (3-17).

Se $\rho_3 \not\equiv 0 \pmod p$, como ξ_1, ξ_2, ξ_6 são todos não nulos módulo p e pelo menos um τ_i é não nulo, assim teremos pelo menos quatro coordenadas não nulas para a solução do sistema (3-17), e como $r = 2$, essa solução tem posto 2. Se $\rho_3 \equiv 0 \pmod p$, ou ρ_1 ou ρ_2 é não-nulo módulo p, suponha $\rho_1 \not\equiv 0 \pmod p$. Como algum τ_i é não-nulo módulo p, a solução possui posto 2, para $(a_1c_j - 0 \cdot b_j)\rho_1\tau_j \not\equiv 0 \pmod p$.

Agora suponha $b_1\xi_1^5 + b_2\xi_2^5 \equiv 0 \pmod p$ e observe que $c_1\xi_1^5 + c_2\xi_2^5 \not\equiv 0 \pmod p$, desde que assumimos que c_1 e c_2 estão em diferentes classes laterais. Usando o Lema (3.4) seja (ρ_1, ρ_2, ρ_3) uma solução para $a_1x_1^5 + a_2x_2^5 + b_3y_3^5 \equiv \alpha \pmod p$. Multiplicando a solução (ξ_1, ξ_2) por T, temos a congruência

$$c_3\rho_3^5 + (c_1\xi_1^5 + c_2\xi_2^5)T^5 + c_5y_5^5 + c_6y_6^5 \equiv \beta\ (mod\ p), \tag{3-20}$$

que pelo Lema (3.4) possui solução não trivial, digamos (τ_1, τ_5, τ_6). Assim

$$(\rho_1, \rho_2, \xi_1\tau_1, \xi_2\tau_1, \rho_3, 0, \tau_5, \tau_6)$$

é uma solução para (3-17).

Se $\tau_1 \not\equiv 0 \pmod p$, como (ξ_1, ξ_2) são ambos não nulos módulo p, teremos pelo menos três coordenadas não-nulas para a solução do sistema (3-17), e como $r = 2$, essa solução tem posto 2. Se $\tau_1 \equiv 0 \pmod p$, então, ou τ_5, ou τ_6 é não nulo módulo p, digamos que seja $\tau_5 \not\equiv 0 \pmod p$, como algum ρ_j é não nulo, a solução tem posto 2, para ou $(c_5a_j)\tau_5\rho_j \not\equiv 0$ ou $(c_5b_3 - 0 \cdot c_3)\tau_5\rho_3 \not\equiv$ módulo p.

□

Lema 3.12 *Se $r = 1$ e $q = 7$ então o sistema (3-14) tem solução de posto 2 módulo p, para todo $\alpha, \beta \in \mathbb{F}_p$.*

Prova.

Como $r = 1$, o sistema (3-14) equivale a

$$\begin{cases} a_1x_1^5 + & b_1y_1^5 + b_2y_2^5 + b_3y_3^5 + b_4y_4^5 + b_5y_5^5 + b_6y_6^5 & & \equiv \alpha\ (mod\ p) \\ & c_1y_1^5 + c_2y_2^5 + c_3y_3^5 + c_4y_4^5 + c_5y_5^5 + c_6y_6^5 & + c_7y_7^5 & \equiv \beta\ (mod\ p) \end{cases}. \tag{3-21}$$

Caso 1 : Se $\alpha \equiv \beta \equiv 0 \pmod{p}$, tome $a_1x_1^5 \equiv 0$ e $c_7y_7^5 \equiv 0 \pmod{p}$ e pelo Lema (3.7) temos uma solução não trivial para (3-21) e como $r = 1$ esta solução possui posto 2.

Agora suponha que pelo menos um entre α ou β seja não-nulo módulo p, digamos que $\beta \not\equiv 0 \pmod{p}$, e que $c_1, c_2, \cdots, c_7 \in \mathbb{S}$.

Caso 2 : Sejam dois pares de coeficientes iguais, entre $c_1, \cdots, c_7$. Digamos $c_1 = c_2$ e $c_3 = c_4$. Com isso teremos $b_1 \neq b_2$ e $b_3 \neq b_4$ módulo p, para $r = 1$. Para a congruência

$$c_5y_5^5 + c_6y_6^5 + c_7y_7^5 \equiv \beta \ (mod\ p), \tag{3-22}$$

o Lema (3.4) nos garante uma solução

$$(\xi_5, \xi_6, \xi_7)$$

não trivial. Faça $b_5\xi_5^5 + b_6\xi_6^5 \equiv \gamma \pmod{p}$, $y_1 = -y_2 = T$ e $y_3 = -y_4 = S$, dando-nos a congruência

$$a_1x_1^5 + (b_1 - b_2)T^5 + (b_3 - b_4)S^5 + \gamma \equiv \alpha \ (mod\ p). \tag{3-23}$$

Ainda pelo Lema (3.4), temos uma solução não trivial para esta congruência, seja

$$(\rho_1, \rho_2, \rho_3)$$

esta solução. Então uma solução para (3-21) será

$$(\rho_1, \rho_2, -\rho_2, \rho_3, -\rho_3, \xi_5, \xi_6, \xi_7).$$

Pelo menos um dos ρ_i e pelo menos um dos ξ_i são não-nulos módulo p, como duas coordenadas, ao menos, são não-nulas módulo p, esta solução tem posto 2, para $r = 1$.

Caso 3 : Sejam $c_1 = c_2 = c_3$ e c_3, c_4, c_5, c_6 e c_7 distintos dois a dois. Fazendo $c_3y_3^5 + c_4y_4^5 + c_5y_5^5 \equiv 0 \pmod{p}$, o Lema (3.6) nos garante uma solução não trivial (ξ_3, ξ_4, ξ_5) com $\xi_3\xi_4\xi_5 \not\equiv 0 \pmod{p}$, que também será solução de $c_2y_3^5 + c_4y_4^5 + c_5y_5^5 \equiv 0 \pmod{p}$ (e de $c_1y_3^5 + c_4y_4^5 + c_5y_5^5 \equiv 0 \pmod{p}$, mas que não iremos precisar). Como $b_2 \not\equiv b_3 \pmod{p}$, então uma das situações acontece: ou $b_3\xi_3^5 + b_4\xi_4^5 + b_5\xi_5^5 \not\equiv 0 \pmod{p}$ ou $b_2\xi_3^5 + b_4\xi_4^5 + b_5\xi_5^5 \not\equiv 0 \pmod{p}$. Sem perda de generalidade podemos supor que

$$b_3\xi_3^5 + b_4\xi_4^5 + b_5\xi_5^5 \equiv \phi \not\equiv 0 \ (mod\ p). \tag{3-24}$$

Considere a congruência $c_6y_6^5 + c_7y_7^5 - \beta z^5 \equiv 0 \pmod{p}$, o Lema (3.4) nos garante uma solução não trivial, digamos (ρ_6, ρ_7, ρ). E o Lema (3.6) nos dá que ρ é não nulo módulo p, do contrário c_6 e c_7 seriam da mesma classe lateral, o que é impossível, pois $c_6 \neq c_7$, e $c_6, c_7 \in \mathbb{S}$. Portanto a equação

$${}_6y_6^5 + c_7y_7^5 \equiv \beta \ (mod\ p) \tag{3-25}$$

tem uma solução dada por

$$(\rho^{-1}\rho_6, \rho^{-1}\rho_7).$$

Faça $y_1 = -y_2 = T$, e da congruência (3-24) multiplicando por S a solução (ξ_3, ξ_4, ξ_5), obtendo a congruência

$$a_1 x_1^5 + (b_1 - b_2)T^5 + \phi S^5 + b_6(\rho^{-1}\rho_6)^5 \equiv \alpha \ (mod\ p) \tag{3-26}$$

que, pelo Lema (3.4), tem uma solução não trivial, (τ_1, τ_2, τ_3). Após esta construção chegamos que

$$(\tau_1, \tau_2, -\tau_2, \tau_3\xi_3, \tau_3\xi_4, \tau_3\xi_5, \rho^{-1}\rho_6, \rho^{-1}\rho_7)$$

é uma solução para o sistema (3-21). Observe que, se $\tau_3 \not\equiv 0 \pmod{p}$ então $\tau_3\xi_3 \not\equiv 0$, $\tau_3\xi_4 \not\equiv 0$ e $\tau_3\xi_5 \not\equiv 0$ módulo p. Assim, esta solução tem posto 2, para $r = 1$. Se $\tau_3 \equiv 0 \pmod{p}$, temos que ou $\tau_1 \not\equiv 0 \pmod{p}$ ou $\tau_2 \not\equiv 0$. Como pelo menos um dentre $\rho^{-1}\rho_6$ e $\rho^{-1}\rho_7$ é não nulo módulo p, dando que esta solução possui posto 2.

□

Concluindo assim, com estes lemas, a demonstração da Proposição (3.9). E também a prova do Teorema (3.3).

Referências Bibliográficas

[1] ATKINSON, O. D; BRÜDERN, J; COOK, R. J. **Simultancous additive congruences to a large prime modulus**. Mathematika, 39(1):1–9, 1992.

[2] ATKINSON, O. D; COOK, R. J. **Pairs of additive congruences to a large prime modulus**. J. Austral. Math. Soc. A, p. 438–455, 1989.

[3] BIRCH, B. J; LEWIS, D. J. ***p*-adic forms**. J. Indian Math. Soc., (23):11–32, 1959.

[4] BIRCH, B. J; LEWIS, D. J. **Systems of three quadratic forms**. Acta Arith., (310):423–442, 1965.

[5] BOREVICH, Z. I; SHAFAREVICH, D. J. **Number Theory**. Academic Press, New York, 1966.

[6] BROWKIN, J. **On forms over *p*-adics fields**. Bull. Acad. Polon. Sci. Math. Astronom. Phys, (14):489–492, 1966.

[7] BRÜDERN, J; GODINHO, H. **On artin's conjecture, i: Systems of diagonal forms**. Bull. London Math. Soc., (31):305–313, 1999.

[8] BRÜDERN, J; GODINHO, H. **On artin's conjecture, ii: Pairs of additive forms**. Proc. London Math. Soc., 3(84):513–538, 2002.

[9] CHOWLA, I. **On the number of solutions of some congruences in the variables**. Proc. Nat. Acad. Sci. India Ser., (5):40–44, 1937.

[10] DAVENPORT, H; LEWIS, D. J. **Homogeneous additive equations**. Proc. Roy. Soc. London Ser., (274):443–460, 1963.

[11] DAVENPORT, H; LEWIS, D. J. **Cubic equations of additive type**. Philos. Trans. Roy. Soc. London Ser., (261):97–136, 1966.

[12] DAVENPORT, H; LEWIS, D. J. **Simultaneous equations of additive type**. Philos. Trans. Roy. Soc. London Ser., (246):557–595, 1969.

[13] DAVENPORT, H; LEWIS, D. J. **Two additive equations**. In: LeVeque, W. J; Straus, E. G, editors, NUMBER THEORY, volume 12 de **Proceedings of Symposia in Pure Mathematics**, p. 74–98. American Mathematical Society, Providence, RI, 1969.

[14] DAVENPORT, H; LEWIS, D. J. **Two additive equations**. Proc. Sympos. Pure Math, (12):74–98, 1976.

[15] GODINHO, H. **Polinômios homogênios sobre os números *P*-ádicos**. Technical report, Universidade de Lisboa, Lisboa, Portugal, 2000.

[16] GODINHO, H; RODRIGUES, P. H. A. **Conditions for the solvability of systems of two and three additive forms over *P*-adic filds**. Proc. London Math. Soc., 3(91):545–572, 2005.

[17] GODINHO, H; SHOKRANIAN, S; SOARES, M. **Teoria dos Números**. Universidade de Brasília, Brasília, 1994.

[18] KNAPP, M. **Systems of diagonal equations over *P*-adic fields**. J. London Math. Soc., 2(63):257–267, 2001.

[19] LAXTON, R. R; LEWIS, D. J. **Forms of degrees 7 and 11 over *P*-adic fields**. Proc. Sym. Pure Math (AMS, Providence, RI), (8):16–21, 1965.

[20] LEWIS, D. J. **Cubic homogeneus polynomials over *p*-adic fields**. Ann. of Math., 2(56):473–478, 1952.

[21] LIDL, R; NIEDERREITER, H. **Finite fields**, volume 20 de **Encyclopedia of Mathematics and Its Applications**. Cambridge University Press, Cambridge, 1983.

[22] LOW, L; PITMAN, J; WOLFF, A. **Simultaneous diagonal congruences**. J. Number Theory, (29):31–59, 1988.

[23] MEIR, I. D. **Pair of additive congruences to a large prime modulus**. Journal of number theory, (63):132–142, 1997.

[24] SCHUUR, S. **On systems of three quadratic forms**. Acta arith., (36):315–322, 1980.

[25] STEVENSON, E. **The artin conjecture for three diagonal cubic forms**. J. Number Theory, (14):374–390, 1982.

[26] TERJANIAN, G. **Un contre-exemple à une conjecture d'artin**. C. R. Acad. Sci. Paris, (262):612, 1966.

Livros Grátis

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

Milhares de Livros para Download:

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