UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

KAMILLA MACHADO PALHARES

Solubilidade de sistemas de duas formas aditivas de grau ímpar e de três formas aditivas cúbicas sobre o corpo dos números p-ádicos

Goiânia
2009

KAMILLA MACHADO PALHARES

Solubilidade de sistemas de duas formas aditivas de grau ímpar e de três formas aditivas cúbicas sobre o corpo dos números p-ádicos

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

Kamilla Machado Palhares

Licenciou-se em Matemática pela Universidade Federal de Goiás (2006). Durante a graduação foi bolsista de Iniciação científica do CNPq. Durante o Mestrado , foi bolsista CAPES.

Agradecimentos

Agradeço primeiramente a Deus e à Nossa Senhora Aparecida.

Aos meus pais: Aparecida e Carlos Palhares.

Ao professor Paulo Henrique, meu orientador, pelo incentivo, pela paciência e pelo tempo dedicado à minha orientação.

A todos os professores, funcionários e amigos do Instituto de Matemática e Estatística da UFG.

Ao Tiago e ao Hugo, meus companheiros de estudo. Aos momentos sérios e divertidos que passamos juntos durante esta etapa da minha vida.

À CAPES, pela ajuda financeira.

À minha família de Orizona que de longe sempre torceram por mim.

À tia Eleen, Núbia, Silvanete, Su, Jajá e todos os meus amigos que de alguma forma contribuíram para a conclusão desta etapa, com muitas festas, choros e risos.

Resumo

Palhares, K. M.. **Solubilidade de sistemas de duas formas aditivas de grau ímpar e de três formas aditivas cúbicas sobre o corpo dos números p-ádicos**. Goiânia, 2009. 64p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

O presente trabalho é baseado nos artigos de H. Davenport e D. J. Lewis [10] e de E. Stevenson [19], onde todos investigam a solubilidade não trivial de sistemas de formas aditivas sobre o corpo dos números p-ádicos para alguns casos particulares de número de equações e graus. Motivado pela Conjectura de Artin e através da teoria de normalização de Davenport e Lewis, é verificado que sistemas de duas formas aditivas de grau ímpar com no mínimo $2k^2+1$ variáveis e, para três formas aditivas de grau três, com não menos do que 28 variáveis, possuem solução p-ádica não trivial.

Palavras–chave

Formas aditivas, Conjectura de Artin, Corpos p-ádicos

Abstract

Palhares, K. M.. **t**. Goiânia, 2009. 64p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

This work is based on articles of H. Davenport and D. J. Lewis [10] and of E. Stevenson [19], where every one investigate the non-trivial solubility of systems of additive forms in p-adic fields for particular cases of the number of equations and degrees. The motivation given by Artin's conjecture and through of Davenport and Lewis's normalization theory it is verify that systems of two additive forms of odd degree with at least $2k^2+1$ variables and three additive forms of degree three, with no less than 28 variables have non-trivial p-adic solution.

Keywords

Additive forms, Artin's conjecture, p-adic fieds

Sumário

Introdução **7**

1 Preliminares **10**
- 1.1 Soluções Não Singulares 10
- 1.2 p-Normalização 14

2 Sistemas de duas formas aditivas **20**
- 2.1 Um pouco de combinatória 20
- 2.2 Congruências 25
- 2.3 Demonstração do Teorema 1 33
  - 2.3.1 Solubilidade das equações (2-1), quando $\delta \neq (p-1)/2$ ou $\delta \neq p-1$ 37
  - 2.3.2 Solubilidade das equações (2-1), quando $\delta = (p-1)/2 \geq 3$. 37
  - 2.3.3 Solubilidade das equações (2-1), quando $p = 3$ e $\delta = 1$ 40
  - 2.3.4 Demonstração do Teorema 1 46

3 Sistemas de três formas aditivas cúbicas **47**
- 3.1 Congruências 49
- 3.2 Demonstração do Teorema 2 55

Apêndice **61**

Referências Bibliográficas **63**

Introdução

Um problema clássico, relacionado a sistemas de formas aditivas sobre o corpo dos números p-ádicos, é garantir a solubilidade não trivial p-ádica de tais sistemas encontrando uma relação entre o grau dessas formas aditivas e o número de variáveis. Na década de 20, E. Artin conjecturou que *um sistema de formas aditivas de grau k em n variáveis,*

$$\begin{cases} f_1 &= a_{11}x_1^k + \ldots + a_{1n}x_n^k = 0, \\ &\vdots \\ f_R &= a_{R1}x_1^k + \ldots + a_{Rn}x_n^k = 0, \end{cases} \tag{0-1}$$

com coeficientes inteiros tem solução p-ádica não trivial, se $n \geq Rk^2 + 1$.

Na verdade, a conjectura não se restringe apenas a formas aditivas, mas também a polinômios homogêneos em geral. Porém, em 1966, Terjanian [20] apresentou um contra-exemplo à conjectura exibindo uma forma quártica 2-ádica com 18 variáveis sem zeros 2-ádicos não triviais; mais tarde ele deu outro contra-exemplo com 20 variáveis. Generalizando a construção de Terjanian, Browkin [3] deu contra-exemplos, para cada primo p, de polinômios com a quantidade de variáveis menor do que k^3. Entretanto, para formas aditivas, até hoje não foi apresentado nenhum contra-exemplo à conjectura e nem foi provado sua veracidade por completo.

Nas décadas de 50 e 60 foram obtidos importantes resultados relacionados à Conjectura de Artin. Dentre esses resultados, em 1952, Lewis [16] provou que a conjectura é verdadeira para $R = 1$ e $k = 3$ e, em 1963, Davenport e Lewis [7] garantiram a validade da conjectura para $R = 1$ e $k \geq 3$, já que as condições de solubilidade para $k = 2$ eram conhecidas (provado por H. Hasse [2] em 1924). Davenport e Lewis [10], em 1967, mostraram que a conjectura de Artin era verdadeira para $R = 2$ e k ímpar e, para k qualquer, eles conseguiram estimar $n \geq 7k^3$. Estudos mais recentes feitos por Brüdern e Godinho [5] em 2002, melhoraram essa estimativa para $n \geq 8k^2$. Outra contribuição importante de Davenport e Lewis [9] mostra que as condições

$$n \geq 9R^2k\ln(3Rk), \qquad \text{para } k \text{ ímpar},$$

e

$$n \geq 48R^2k^3 \ln(3Rk^2), \qquad \text{para } k > 2 \text{ par},$$

são suficientes para se obter soluções p-ádicas em sistemas de R formas. Este resultado também já foi melhorado em 1988 por Low, Pitman e Wolff [17] que provaram que as cotas

$$n \geq 2R^2k \ln k, \qquad \text{para } k \text{ ímpar},$$

e

$$n \geq 48Rk^3 \ln(3Rk^2), \text{ para } k > 2 \text{ par},$$

são suficientes. Em 1998, Brüdern e Godinho [4] provaram que $n \geq R^3k^2$ garante a solubilidade p-ádica de (0-1), que foi melhorada por Knapp [14] com a cota $n \geq 4R^2k^2$.

Além desses resultados mencionados, vários outros resultados já foram obtidos e novas técnicas ainda estão sendo desenvolvidas acerca da conjectura. Havendo ainda muito a desenvolver, o estudo de casos particulares de R é muito útil para uma maior compreensão do tema. Com essa motivação, iremos demonstrar nessa dissertação a validade da conjectura de Artin para dois casos: quando $R = 2$ e k é ímpar e quando $R = 3$ e $k = 3$. Veremos que há uma certa diferença entre as técnicas usadas para as demonstrações desses dois casos.

Provaremos os seguintes resultados:

Teorema 1 *Se k é ímpar e $n \geq 2k^2 + 1$, então, para todo primo p, duas equações aditivas de grau k têm solução p-ádica não trivial em comum.*

Teorema 2 *Três equações aditivas cúbicas com n variáveis têm solução p-ádica não trivial em comum se $n \geq 28$ e $p \neq 3$ ou $p \neq 7$.*

Estes resultados se encontram em [10] e [19], respectivamente.

No desenvolvimento desses resultados utilizaremos como principais ferramentas a teoria de normalização, desenvolvida por Davenport e Lewis, juntamente com o Lema de Hensel e o Teorema de Chevalley, todos descritos no primeiro capítulo como resultados preliminares para o desenrolar das demonstrações.

No segundo capítulo apresentaremos o Teorema 1. Iniciaremos o capítulo demonstrando um lema combinatório que nos será bastante útil como estratégia da demonstração deste teorema. Na seção 2.2 deste capítulo serão apresentados alguns resultados sobre sistemas de congruências de formas aditivas e, já na seção 2.3, exibiremos uma estratégia geral para a demonstração do teorema principal do capítulo, provando-o subsequentemente.

No terceiro capítulo também apresentaremos alguns resultados sobre sistemas de congruências de formas aditivas de grau três na seção 3.1 e logo a seguir, na seção 3.2, faremos a demonstração do principal teorema do capítulo, o Teorema 2.

Este trabalho tem a intenção de esclarecer melhor ao leitor os textos originais desenvolvidos pelos precursores dos estudos dessa temática, tornando-os mais simples por meio de uma leitura interessante e que faz parte da problemática acerca da Conjectura de Artin, que muito falta para ser completamente solucionada.

CAPÍTULO 1

Preliminares

Considere o seguinte sistema de R formas aditivas de grau k

$$\begin{cases} f_1 & = a_{11}x_1^k & +\ldots+ & a_{1n}x_n^k & = & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ f_R & = a_{R1}x_1^k & +\ldots+ & a_{Rn}x_n^k & = & 0 \end{cases} \tag{1-1}$$

onde os coeficientes a_{ij} são números inteiros e $n > R$. Neste capítulo apresentaremos resultados que irão estabelecer condições para que o sistema (1-1) tenha solução não trivial em $\mathbb{Q}_p$, o corpo dos números p-ádicos, para todo primo p, e iremos desenvolver a teoria de p-normalização de sistemas de equações aditivas, de grande relevância no decorrer de todo o trabalho.

1.1 Soluções Não Singulares

Definição 1.1 *Seja* $\gamma \geq 1$. *Uma solução* $\xi = (\xi_1, \ldots, \xi_n)$ *para o sistema de congruências:*

$$\begin{cases} f_1 & = a_{11}x_1^k & +\ldots+ & a_{1n}x_n^k & \equiv 0 & \pmod{p^\gamma} \\ \vdots & \vdots & & \vdots & & \vdots \\ f_R & = a_{R1}x_1^k & +\ldots+ & a_{Rn}x_n^k & \equiv 0 & \pmod{p^\gamma} \end{cases} \tag{1-2}$$

é chamada não singular se a matriz $(a_{ij}\xi_j)_{R\times n}$ *tem posto R módulo p.*

O resultado pelo qual a princípio estamos interessados, uma versão do Lema de Hensel que logo apresentaremos, é de grande importância para esse trabalho, pois mostra que, para garantir a solubilidade do sistema (1-1) em $\mathbb{Q}_p$, basta garantirmos uma solução não singular para o sistema (1-2), onde γ depende da potência de p na fatoração prima de k.

Assim, escreveremos $k = p^{\tau}k_0$, onde $mdc(k_0,\ p) = 1$ e definiremos

$$\gamma = \begin{cases} \tau + 2, & \text{se } p = 2 \\ \tau + 1, & \text{se } \tau > 0 \text{ e } p > 2 \\ 1, & \text{se } \tau = 0 \end{cases} . \tag{1-3}$$

Antes de enunciar e demonstrar o resultado mencionado anteriormente, precisaremos do seguinte lema (ver [13]):

Lema 1.2 *Se a congruência*

$$x^k \equiv m \pmod{p^{\gamma}}$$

tem solução, onde $mdc(m,p) = 1$ *e* γ *é como definido em 1-3, então a congruência*

$$y^k \equiv m \pmod{p^{\nu}}$$

tem solução para todo $\nu \geq \gamma$.

Lema 1.3 *(Lema de Hensel) Se o sistema de congruências (1-2) tem uma solução não singular, quando* γ *é dado por (1-3), então o sistema (1-1) tem uma solução p-ádica não trivial.*

Prova.

Seja $\xi = (\xi_1, ..., \xi_n)$ a solução não singular de (1-2). Então existem R índices $j \in \{1, ..., n\}$ em ξ tais que o determinante da matriz $(a_{ij}\xi_j)_{R\times R}$, para os índices j convenientes, não é nulo módulo p. Sem perda de generalidade, podemos considerar $1, ..., R$ os tais índices. Assim teremos

$$\xi_1\xi_2...\xi_R Det(c_1c_2...c_R) \not\equiv 0 \pmod{p},$$

onde os c_j's são as j-ésimas colunas da matriz (a_{ij}).

Como o determinante das R primeiras colunas da matriz dos coeficientes de (1-2) não é divisível por p, então é possível obter combinações lineares de $f_1, ..., f_R$, de forma que se possa reescrever (1-2) na forma

$$\begin{cases} \phi_1 = & b_{11}x_1^k & & & +\psi_1(x_{R+1}, ..., x_n) & \equiv 0 & \pmod{p^{\gamma}} \\ \vdots & & \dots & & \vdots & \vdots & \\ \phi_R = & & & b_{RR}x_R^k & +\psi_R(x_{R+1}, ..., x_n) & \equiv 0 & \pmod{p^{\gamma}} \end{cases} \tag{1-4}$$

onde $b_{11}b_{22}...b_{RR} \not\equiv 0 \pmod{p}$.

Portanto, temos que

$$\phi_1(\xi) \equiv 0 \pmod{p^\gamma}, ..., \phi_R(\xi) \equiv 0 \pmod{p^\gamma}.$$

Além disso, por definição de solução não singular, nenhum dos elementos $\xi_1, ..., \xi_R$ são divisíveis por p, portanto $b_{ii}\xi_i \not\equiv 0 \pmod{p}$ implicando que

$$-b_{ii}\xi_i \equiv \psi_i(\xi_{R+1}, ..., \xi_n) \not\equiv 0 \pmod{p} \text{ com } i \in \{1, ..., R\}.$$

Seja $\nu > \gamma$ um inteiro positivo, pelo Lema 1.2, existem $\eta_1, ..., \eta_R$ tais que

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

onde $i \in \{1, ..., R\}$.

Assim, $\eta_1, ..., \eta_R, \xi_{R+1}, ..., \xi_n$ constitui uma solução de

$$f_1 \equiv 0 \pmod{p^\nu}, ..., f_R \equiv 0 \pmod{p^\nu} \tag{1-5}$$

onde nenhum dos elementos $x_1, ..., x_R$ é divisível por p.

Portanto, existe solução para (1-5), para qualquer $\nu > \gamma$. Podemos formar então uma sequência de soluções $(a_1^{(\nu)}, ..., a_n^{(\nu)})$ do sistema (1-5) em $\mathbb{Z}_p^n$, onde $\mathbb{Z}_p$ indica o conjunto dos inteiros p-ádicos. Como $\mathbb{Z}_p$ é compacto (ver [13]), em cada uma das coordenadas de $(a_1^{(\nu)}, ..., a_n^{(\nu)})$ podemos determinar uma subsequência convergente $\{a_i^{(\nu_j)}\}$ para um inteiro p-ádico α_i (note que tais subsequências são determinadas de modo que cada coordenada i possua os mesmos índices ν_j). Assim, temos que

$$f_i(\alpha_1, ..., \alpha_n) \equiv f_i(a_1^{(\nu_j)}, ..., a_n^{(\nu_j)}) \equiv 0 \pmod{p^{\nu_j}}, \ \ i \in \{1, ..., R\}$$

para todo $\nu_j > \gamma$.

Logo, quando $\nu_j \to \infty$, temos $\mid f_i(\alpha_1, ..., \alpha_s) \mid_p = 0$, ou seja,

$$f_i(\alpha_1, ..., \alpha_s) = 0, \ i \in \{1, ..., R\}.$$

□

Com esse resultado, passamos agora a nos preocupar em encontrar solução não singular para um sistema de congruências como em (1-2). Um importante resultado que nos ajudará nessa procura é o Teorema de Chevalley, que estabelece uma relação entre o número de variáveis e os graus das formas aditivas para garantir solução para o sistema de congruências.

Definição 1.4 *Definimos "o grau total de um polinômio f" como sendo o maior grau dentre os graus de seus monômios, onde o grau de um monômio é igual a soma dos graus de suas variáveis.*

Teorema 1.5 *(Teorema de Chevalley) Sejam $f_1,...,f_m$ polinômios em n variáveis, sem termo constante e com graus totais $d_1,...,d_m$, respectivamente. Se $n > d_1 + ... + d_m$, então existe $(b_1,...,b_n) \neq (0,...,0)$ tal que*

$$f_1(b_1,...,b_n) \equiv ... \equiv f_m(b_1,...,b_n) \equiv 0 \pmod{p}$$

tem um zero simultâneo para $f_1,...,f_m$ módulo p.

Antes de iniciarmos a demonstração deste teorema precisamos de algums resultados apresentados a seguir (ver [13]).

Lema 1.6 *(Pequeno Teorema de Fermat) Seja $p \in \mathbb{N}$ um número primo. Então $n^p \equiv n \pmod{p}$ para qualquer $n \in \mathbb{N}$.*

Definição 1.7 *Sejam f e g dois polinômios em n variáveis, com coeficientes inteiros.*

(i) Dizemos que f é congruente a g módulo m, denotado por $f \equiv g \pmod{m}$, se os coeficientes dos termos de f e g são congruentes módulo m.

(ii) Dizemos que f é equivalente a g módulo m se

$$f(c_1,...,c_n) \equiv g(c_1,...,c_n) \pmod{m}$$

para toda n-upla de inteiros $(c_1,...,c_n)$.

Dado um polinômio f, vamos reduzir o grau de suas variáveis através de sucessivas aplicações do Pequeno Teorema de Fermat, fazendo $x_i^p \equiv x_i \pmod{p}$. Ao final deste processo encontraremos um polinômio equivalente a f, onde todas as variáveis apresentam graus menores do que p, e neste caso diremos que este polinômio equivalente está na "forma reduzida módulo p".

Lema 1.8 *Todo polinômio f é equivalente a um polinômio na forma reduzida cujo grau total é sempre menor do que ou igual ao grau total de f.*

Lema 1.9 *Se o polinômio $F(x_1,...,x_n)$ está na forma reduzida e tem a propriedade de que $F(x_1,...,x_n) \equiv 0 \pmod{p}$ em todo ponto diferente de $(a_1,...,a_n)$, e $F(a_1,...,a_n) \equiv 1 \pmod{p}$, então*

$$F(x_1,...,x_n) \equiv (-1)^n[(x_1-a_1)^{p-1}-1]...[(x_n-a_n)^{p-1}-1].$$

Podemos, agora, demonstrar o Teorema de Chevalley.

Prova.Considere o seguinte polinômio

$$F(x_1,...,x_n) = (-1)^m(f_1^{p-1}-1)...(f_m^{p-1}-1).$$

Suponha que para qualquer $(b_1,...,b_n) \neq (0,...,0)$ o sistema $f_1,...,f_m \equiv 0 \pmod{p}$ não possua solução.

Note, então, que $F(x_1,...,x_n) \equiv 0 \pmod{p}$ em todo ponto diferente de $(0,...,0)$ e $F(0,...,0) \equiv 1 \pmod{p}$ (pelo Pequeno Teorema de Fermat). De acordo com o Lema 1.9, $F \equiv (-1)^n(x_1^{p-1}-1)...(x_n^{p-1}-1)$, onde este último polinômio tem grau total $n(p-1)$. Portanto, o grau total de F é no mínimo $n(p-1)$, pelo Lema 1.8. Mas, pela definição de F temos que o grau de F é $(d_1+...+d_m)(p-1)$, logo

$$d_1+...+d_m \geq n.$$

Contradição! □

1.2 p-Normalização

Para iniciar a teoria de normalização, consideremos o sistema (1-1) e definamos

$$\vartheta(f_1,...,f_R) = \prod_{j_1,...,j_R} Det(c_{j_1},...,c_{j_R})$$

onde os sub-índices $\{j_1,...,j_R\}$ são todos os arranjos possíveis de R termos distintos do conjunto $\{1,...,n\}$. O número de subconjuntos distintos, que denotaremos por M, será

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

O próximo resultado estabelecerá algumas propriedades de ϑ:

Lema 1.10 *(i) Se* $f_i'(x_1,...,x_n) = f_i(p^{\theta_1}x_1,...,p^{\theta_n}x_n)$, *onde* $\theta_i \in \mathbb{Z}$ *e* $i \in \{1,...,R\}$, *então*

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

onde $\theta = \theta_1+...+\theta_n$.

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

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

Prova.

(i) Inicialmente, vamos supor que $f_i'(x_1,...,x_n) = f_i(p^{\theta_1}x_1, x_2, ..., x_n)$, onde $i \in \{1,...,R\}$ e, neste caso, $\theta = \theta_1$. Assim obtemos

$$\begin{cases} f_1' = & p^{k\theta}.a_{11}x_1^k & + a_{12}x_2^k & +...+ & a_{1n}x_n^k \\ \vdots & \vdots & \vdots & & \vdots \\ f_R' = & p^{k\theta}.a_{R1}x_1^k & + a_{R2}x_2^k & +...+ & a_{Rn}x_n^k \end{cases} \tag{1-6}$$

Seja c_j' a j-ésima coluna da matriz dos coeficientes do sistema (1-6). Temos que

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

Veja que existem $\frac{RM}{n}$ conjuntos $\{j_1, ..., j_R\}$ tais que $1 \in \{j_1, ..., j_R\}$. Então

$$\vartheta(f_1', ..., f_R') = \prod_{j_1,...,j_R} Det(c_{j_1}', ..., c_{j_R}')$$

$$= \prod_{1\in\{j_1,...,j_R\}} Det(c_{j_1}', ..., c_{j_R}'). \prod_{1\notin\{j_1,...,j_R\}} Det(c_{j_1}', ..., c_{j_R}') = p^{\frac{kRM\theta}{n}}\vartheta(f_1, ..., f_R).$$

Repetindo esse processo para as outras variáveis $x_2, ..., x_n$, uma por uma, obteremos o caso geral

$$\begin{cases} f_1' = & p^{k\theta_1}a_{11}x_1^k & +...+ & p^{k\theta_n}a_{1n}x_n^k \\ \vdots & \vdots & & \vdots \\ f_R' = & p^{k\theta_1}a_{R1}x_1^k & +...+ & p^{k\theta_n}a_{Rn}x_n^k \end{cases}, \tag{1-7}$$

onde $\theta = \theta_1 + ... + \theta_n$ Para qualquer conjunto $\{j_1, ..., j_R\}$ temos que

$$Det(c_{j_1}', ..., c_{j_R}') = p^{k\theta_{j_1}}...p^{k\theta_{j_R}}.Det(c_{j_1}, ..., c_{j_R}). \tag{1-8}$$

Efetuando o produto dos determinantes descritos em (1-8) para todos os conjuntos $\{j_1, ..., j_R\}$, concluímos que cada termo $p^{k\theta_{j_i}}$ aparece $\frac{RM}{n}$ vezes nesse produto. Assim,

$$\vartheta(f_1', ..., f_R') = p^{\frac{kRM\theta_1}{n}}...p^{\frac{kRM\theta_n}{n}} \prod_{j_1,...,j_R} Det(c_{j_1}, ..., c_{j_R}) = p^{\frac{kRM\theta}{n}}\vartheta(f_1, ..., f_R).$$

(ii) Agora suponha que

$$\begin{cases} f_1'' = & a_{11}''x_1^k & +...+ & a_{1n}''x_n^k \\ \vdots & \vdots & & \vdots \\ f_R'' = & a_{R1}''x_1^k & +...+ & a_{Rn}''x_n^k \end{cases}$$

Seja c_j'' a j-ésima coluna da matriz $A'' = (a_{ij}'')_{R\times n}$. Temos que

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

e, assim,

$$A'' = \begin{bmatrix} d_{11} & \dots & d_{1R} \\ \vdots & & \vdots \\ d_{R1} & \dots & d_{RR} \end{bmatrix} . \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{R1} & \dots & a_{Rn} \end{bmatrix} .$$

Obtemos então a igualdade

$$Det(c_{j_1}'', ..., c_{j_R}'') = D.Det(c_{j_1}, ..., c_{j_R})$$

e, consequentemente

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

□

Definição 1.11 *Dois sistemas de formas como em (1-1), são ditos p-equivalentes se um pode ser obtido do outro por uma combinação das operações (i) e (ii) do Lema 1.10, onde* $\theta_1, ..., \theta_n$ *são inteiros e cada* d_{ij} *é racional com* $D \neq 0$.

Note que, se um sistema do tipo de (1-1) possui solução p-ádica não trivial, então qualquer sistema equivalente a ele também possui.

Definição 1.12 *Sejam* $f_1 = 0, ..., f_R = 0$ *as equações de um sistema de formas aditivas de grau k onde* $\vartheta(f_1, ..., f_R) \neq 0$. *De todos os sistemas p-equivalentes a* $f_1 = 0, ..., f_R = 0$, *com coeficientes inteiros, consideremos aquele cuja potência de p que divide* $\vartheta(f_1, ..., f_R)$ *seja mínima (potência não negativa). Diremos que tal sistema é p-normalizado.*

Considere $A = (a_{ij})$ a matriz dos coeficientes do sistema (1-1) e c_j a sua j-ésima coluna.

Definição 1.13 *Dizemos que* 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.

Antes de enunciar o próximo lema, iremos reescrever o sistema (1-1) de outro modo, separando as variáveis por níveis. Utilizando apenas reordenação e mudança de variáveis obteremos um sistema dividido em níveis menores do que k. Desse modo, teremos o seguinte sistema:

$$\begin{cases} f_{11} & +pf_{12} & +...+ & p^{k-1}f_{1k} & =0 \\ f_{21} & +pf_{22} & +...+ & p^{k-1}f_{2k} & =0 \\ \vdots & \vdots & & \vdots & \\ f_{R1} & +pf_{R2} & +...+ & p^{k-1}f_{Rk} & =0 \end{cases} \tag{1-9}$$

onde f_{ij} são formas diagonais de grau k nas variáveis x_j.

Note que a existência de solução não trivial em $\mathbb{Q}_p$ para (1-9) implica na existência de solução não trivial em $\mathbb{Q}_p$ para (1-1). Note ainda que, as formas de cada coluna possuem as mesmas variáveis e ao menos um dos coeficientes de x_j, presentes em alguma das formas, é co-primo com p.

Lema 1.14 *(Davenport e Lewis) Um sistema p-normalizado de formas aditivas* $f_1 = 0, ..., f_R = 0$ *de grau k, pode ser escrito na forma*

$$f_i = F_i(x_1, ..., x_s) + pG_i(x_{s+1}, ..., x_n) \tag{1-10}$$

para $i \in \{1, ..., R\}$, *onde*

$$s \geq \frac{n}{k}.$$

Mais ainda, se $1 \leq j \leq s$, *então pelo menos um dos coeficientes de algum* x_j *não é divisível por p. Além disso, para* $1 \leq t \leq R$, *se* A_0 *é a matriz dos coeficientes das formas no nível zero e* q_t *representa o menor número de colunas, não nulas módulo p, em qualquer t combinações lineares das linhas de* A_0, *independentes módulo p, então*

$$q_t \geq \frac{nt}{Rk}.$$

Prova. Para obter (1-10) basta aplicar sobre o sistema o método da separação por níveis, como visto anteriormente, onde s representa o número de variáveis do nível zero do sistema.

Inicialmente iremos mostrar que $s \geq \frac{n}{k}$.

Assim, considere o conjunto de formas aditivas,

$$p^{-1}f_i(px_1, ..., px_s, x_{s+1}, ..., x_n) = p^{k-1}F_i(x_1, ..., x_s) + G_i(x_{s+1}, ..., x_n) \tag{1-11}$$

Note que estas formas são obtidas de $f_i(x_1, ..., x_n)$ através de uma combinação das operações (i) e (ii) do Lema 1.10, com $\theta = s$ e $D = p^{-R}$. Portanto, o valor de ϑ para

esse novo conjunto de formas será

$$\vartheta(p^{-1}f_1',...,p^{-1}f_R') = p^{\frac{kRMs}{n}-RM}\vartheta(f_1,...,f_R).$$

Como estas novas formas (1-11) possuem coeficientes inteiros, segue da minimalidade de sistemas p-normalizados que

$$\frac{kRMs}{n} - RM \geq 0 \quad \Rightarrow \quad \frac{ks}{n} \geq 1 \quad \Rightarrow \quad s \geq \frac{n}{k}.$$

Agora, para a outra parte da demonstração, considere $f_1',...,f_t'$ quaisquer t combinações lineares de $f_1,...,f_R$ independentes módulo p e sejam $F_1',...,F_t'$ as formas das mesmas combinações lineares de $F_1,...,F_R$. Para obtermos um conjunto de R combinações lineares basta completarmos as novas formas com $R-t$ elementos de $f_1,...,f_R$ ou $F_1,...,F_R$. Seja q_t o menor número de variáveis que aparecem em pelo menos uma das combinações $F_1',...,F_t'$ com coeficientes não divisíveis por p. Chamaremos essas variáveis de $x_1,...,x_{q_t}$. Considere as formas

$$p^{-1}f_i'(px_1,...,px_{q_t},x_{q_t+1},...,x_n) \text{ para } i = 1,...,t$$

e,

$$f_i'(px_1,...,px_{q_t},x_{q_t+1},...,x_n) \text{ para } i = t+1,...,R.$$

Além de possuir coeficientes inteiros, essas formas foram obtidas de $f_1,...,f_R$ por uma combinação das operações (i) e (ii), com $\theta = q_t$ e $D = p^{-t}D_0$, onde D_0 é o determinante da matriz utilizada na operação (ii) para obter $f_1',...,f_t'$ de $f_1,...,f_R$. Assim, pela minimalidade de sistemas p-normalizados, temos que

$$\frac{kRMq_t}{n} - tM \geq 0 \quad \Rightarrow \quad \frac{kRq_t}{n} \geq t \quad \Rightarrow \quad q_t \geq \frac{nt}{kR}.$$

Como queríamos. □

Proposição 1.15 *Suponha que qualquer sistema do tipo (1-1) que possua a propriedade $\vartheta(f_1,...,f_R) \neq 0$, possua solução p-ádica não trivial. Então, todo sistema do tipo (1-1) tal que $\vartheta(f_1,...,f_R) = 0$, também possui solução p-ádica não trivial.*

Prova.Considere o sistema (1-1) e suponha que $\vartheta(f_1,...,f_R) = 0$. Vamos construir uma sequência de formas aditivas

$$f_i^{(\mu)}(x_1,...,x_n) = a_{i1}^{(\mu)}x_1^k + ... + a_{in}^{(\mu)}x_n^k = 0 \quad (i = 1,...,R), \tag{1-12}$$

com coeficientes inteiros, tais que cada $a_{ij}^{(\mu)} - a_{ij}$ seja divisível por p^{μ} e $\vartheta(f_1^{(\mu)},...,f_R^{(\mu)}) \neq 0$. Basta tomarmos $a_{ij}^{(\mu)} = a_{ij} + q_{ij}^{(\mu)} p^{(\mu)}$, com $q_{ij}^{(\mu)}$ conveniente.

Por hipótese, os sistemas (1-12) têm soluções p-ádicas não triviais, digamos $\xi^{(\mu)} = (\xi_1^{(\mu)},...,\xi_n^{(\mu)}) \in \mathbb{Z}_p^n$. Como as equações são homogêneas, podemos assumir que ao menos uma das coordenadas de $\xi^{(\mu)}$ não é divisível por p. Como $\mathbb{Z}_p$ é compacto, a sequência $\{\xi_s^{(\mu)}\}$ de cada coordenada $s = 1,...,n$ possui uma subsequência convergente $\{\xi_s^{(\mu_j)}\}$ para um inteiro p-ádico ξ_i, nem todos iguais a zero. Agora note que, pela continuidade de f_i,

$$\lim_{\mu_j \to \infty} f_i(\xi^{(\mu_j)}) = f_i(\xi)$$

e, como $f_i^{(\mu_j)}(\xi^{(\mu_j)}) = 0$,

$$\begin{aligned} | f_i(\xi^{(\mu_j)}) |_p &= | f_i(\xi^{(\mu_j)}) - f_i^{(\mu_j)}(\xi^{(\mu_j)}) |_p \\ &= | \textstyle\sum_{s=1}^{n} (a_{is} - a_{is}^{(\mu_j)})(\xi_s^{(\mu_j)})^k |_p \\ &\leq p^{-\mu_j}. \end{aligned}$$

Portanto $f_i(\xi) = 0$, isto é, o sistema (1-1) tem solução p-ádica não trivial.

□

Este resultado irá nos permitir assumir, de agora em diante, que em (1-1) temos $\vartheta(f_1,...,f_R) \neq 0$ e, mais ainda, no decorrer do trabalho iremos considerar apenas sistemas p-normalizados.

CAPÍTULO 2

Sistemas de duas formas aditivas

Neste capítulo nosso objetivo é investigar a solubilidade de um sistema de duas equações aditivas com n variáveis e grau $k > 0$ como o sistema

$$\begin{cases} f = & a_1x_1^k + \ldots + a_nx_n^k & = & 0 \\ g = & b_1x_1^k + \ldots + b_nx_n^k & = & 0 \end{cases} \tag{2-1}$$

onde os coeficientes a_i e b_i são inteiros. Estamos interessados na solubilidade deste sistema sobre o corpo dos números p-ádicos, para todo p primo.

Para este caso, a Conjectura de Artin diz que se o número de variáveis for no mínimo $2k^2+1$, então o sistema do tipo de 2-1, possui solução p-ádica não trivial. Mas, entretanto, neste trabalho será confirmada a conjectura apenas para k ímpar.

Enfim, nosso objetivo é provar o seguinte teorema (ver [10]):

Teorema 1 *Se k é ímpar e $n \geq 2k^2+1$, então, para todo primo p, as equações aditivas (2-1) têm solução p-ádica não trivial em comum.*

2.1 Um pouco de combinatória

Para provar o Teorema 1 precisamos significativamente do lema combinatorial demonstrado a seguir:

Lema 2.1 *Seja S a união de w conjuntos não-vazios e disjuntos $S_1, \ldots, S_w$, onde $w \geq 2$. Seja $l_i = \mid S_i \mid$, e suponha que*

$$l_1 \geq l_i \text{ para } i = 1, \ldots, w. \tag{2-2}$$

Faça

$$m = l_1 + \ldots + l_w, \quad q = l_2 + \ldots + l_w. \tag{2-3}$$

Seja δ um inteiro positivo e defina r por

$$r = min\{[m/(2\delta+1)], [q/(\delta+1)]\}. \tag{2-4}$$

Então, existem r conjuntos disjuntos $T_1, ..., T_r$ *contidos em S tais que*

$$2\delta + 1 \leq | T_i | \leq 2\delta + 2, \tag{2-5}$$

para $i = 1, ..., r$, *e*

$$| T_i | - | T_i \cap S_j | \geq \delta + 1, \tag{2-6}$$

para $i = 1, ..., r$ *e* $j = 1, ..., w$. *Além disso, existe*

$$s = min\{[m/2], q\} \tag{2-7}$$

pares disjuntos de elementos de S tais que nenhum par se encontra em um mesmo conjunto S_j.

Prova. A prova da primeira afirmação será por indução em r. O resultado é trivialmente verdadeiro se $r = 0$. Basta provar a validade de (2-5) e (2-6) para $r \geq 1$. Assim, suponhamos que a primeira afirmação do lema é verdadeira para $r - 1$ conjuntos, isto é, de acordo com a definição para r em (2-4), temos que existem $r - 1$ conjuntos disjuntos $T_1, ..., T_{r-1}$ contidos em S tais que valham (2-5) e (2-6).

Para iniciarmos a demonstração, consideremos um conjunto T formado por elementos de S, convenientemente. Sejam $S'_1, ..., S'_w$ os conjuntos dos elementos restantes dos conjuntos $S_1, ..., S_w$ depois da retirada de seus elementos para compor T. Seja w' o número de conjuntos S'_j que não são vazios e sejam ainda m', q' e r' definidos para os conjuntos S'_j assim como m, q e r foram definidos para os conjuntos S_j. Veja que devemos renumerar os conjuntos S'_j de modo que

$$| S'_1 | \geq | S'_2 | \geq ... \geq | S'_{w'} | \geq 1,$$

ou seja,

$$l'_1 \geq l'_2 \geq ... \geq l'_{w'} \geq 1.$$

Note que a hipótese de indução assegura que podemos encontrar $r - 1$ conjuntos no conjunto $S' = S - T$ com as propriedades (2-5) e (2-6). Basta então provarmos que o conjunto T existe, também satisfazendo (2-5) e (2-6), e satisfazendo

$$r' \geq r - 1 \text{ e } w' \geq 2, \text{ para } r > 1. \tag{2-8}$$

Provando assim a existência dos r subconjuntos desejados de S.

Por (2-4), temos

$$m \geq (2\delta + 1)r \text{ e } q \geq (\delta + 1)r. \tag{2-9}$$

Podemos supor que

$$l_1 \geq l_2 \geq ... \geq l_w \geq 1.$$

Se $l_1 > l_2$, a retirada de um único elemento de S_1 diminuirá m por 1 mas não mudará q, desde que $l_1 - 1 \geq l_j$ para $j = 2, ..., w$. Se $l_1 = l_2$, a retirada de algum elemento de S_1 diminuirá m e q por 1, já que o número de elementos no maior conjunto, agora S_2, não foi diminuído. Usando estas duas operações podemos obter conjuntos para que a igualdade valha em ao menos uma das sentenças em (2-9). Por exemplo, inicialmente iremos retirar de S_1 elementos, de modo que $l_1 \geq l_j$ para $j = 2, ..., w$, até que a primeira sentença de (2-9) seja uma igualdade; se chegarmos em um momento em que $l_1 = l_2$ e a primeira sentença ainda é uma inequação estrita, então usamos a segunda operação, havendo a possibilidade da segunda sentença ser uma igualdade, e assim por diante. Logo, poderemos supor que se existe a inequação estrita na primeira delas, então $l_1 = l_2$. Assim, é suficiente considerar os dois casos:

$$m = (2\delta + 1)r \text{ e } q \geq (\delta + 1)r; \qquad (I)$$

$$m > (2\delta + 1)r,\ q = (\delta + 1)r \text{ e } l_1 = l_2; \qquad (II)$$

Caso (I). Neste caso, $w \geq 3$, pois se $w = 2$, teríamos

$$m = l_1 + l_2 \text{ e } q = l_2,$$

daí, $q \leq \dfrac{l_1 + l_2}{2} = \dfrac{(2\delta + 1)r}{2} = (\delta + \dfrac{1}{2})r$, que é impossível.

Para essa parte da demonstração temos dois subcasos: para $l_1 \leq \delta$ e $l_1 > \delta$.

Se $l_1 \leq \delta$, então $\mid S_j \mid \leq \delta$ para $j = 1, ..., w$. Neste caso, formemos T com $2\delta + 1$ elementos de S, o que já satisfaz (2-5). Daí, como $\mid T \cap S_j \mid \leq \delta$, para cada j, então

$$\begin{aligned} \mid T \mid - \mid T \cap S_j \mid &= 2\delta + 1 - \mid T \cap S_j \mid \\ &\geq 2\delta + 1 - \delta = \delta + 1 \end{aligned}$$

e (2-6) também é satisfeito. Além disso, (2-8) vale quando $r > 1$, desde que

$$m' = m - (2\delta + 1) = (2\delta + 1)(r - 1)$$

e

$$q' = m' - l_1' \geq m' - l_1 \geq m' - \delta = (2\delta + 1)(r - 1) - \delta \geq (\delta + 1)(r - 1).$$

Assim, $r' = r - 1$ e desde que m' e q' satisfaz a condição (I) temos, como no parágrafo anterior, que $w' \geq 3$.

Agora suporemos que $l_1 > \delta$. Podemos satisfazer (2-5) e (2-6) fazendo T consistir de δ elementos de S_1 e $\delta + 1$ elementos de $S_2, ..., S_w$, mas não todos do mesmo conjunto

(note que, como $w \geq 3$, isto é possível). Se $r > 1$, então

$$m' = m - \mid T \mid = (2\delta+1)r - (2\delta+1) = (2\delta+1)(r-1)$$

e, trivialmente,

$$q' \geq q - (2\delta+1).$$

Colocando

$$q = (\delta+1)r + \alpha, \text{ onde } \alpha \geq 0,$$

teremos $q' \geq (\delta+1)(r-1) + (\alpha-\delta)$.

Se $\alpha \geq \delta$, então $q' \geq (\delta+1)(r-1)$, com $r' = r-1$ e $w' \geq 3$.

Agora suponha que $\alpha < \delta$. Temos

$$l_1 = m - q = (2\delta+1)r - [(\delta+1)r + \alpha] = \delta r - \alpha.$$

Se $l_2 \leq \delta r - \delta$, podemos formar T com $\delta - \alpha$ elementos de S_1, de modo que assim $l_1' = \delta r - \delta$, e pegando $\delta + \alpha + 1$ elementos dos conjuntos $S_2, ..., S_w$, com a condição de que não seja pego mais que δ elementos em um mesmo conjunto. Isto é possível já que $q = (\delta+1)r + \alpha > \delta + 1 + \alpha$ e o número de elementos de todos os conjuntos dentre $S_2, ..., S_w$, com excessão de S_2, é ao menos

$$l_3 + ... + l_w = q - l_2 \geq (\delta+1)r + \alpha - (\delta r - \delta) = r + \alpha + \delta > \alpha + 1.$$

Depois de formar este conjunto T, teremos exatamente $m' = (2\delta+1)(r-1)$ e $q' = m' - l_1' = (\delta+1)(r-1)$, onde $r' = r-1$ e $w' \geq 3$.

Agora suponha que $\alpha < \delta$ e $l_2 > \delta r - \delta \geq l_3$. Iremos formar T tomando δ elementos de S_1 e δ elementos de S_2, que é possível já que $r \geq 2$ implica em $l_2 > \delta r - \delta = \delta(r-1) \geq \delta$. Tomemos ainda um elemento de S_3 para compor T. Temos então que

$$l_1' = l_1 - \delta \leq \delta r - \delta,$$

$$m' = (2\delta+1)(r-1)$$

e

$$q' = m' - l_1' \geq (\delta+1)(r-1).$$

Assim, $r' = r-1$ e $w' \geq 3$.

Finalmente suponha que, $\alpha < \delta$ e $l_t > \delta r - \delta \geq l_{t+1}$, onde $t \geq 3$. Façamos $l_i = \delta r - \delta + \eta_i$ para $i = 1, ..., t$. Então, como $l_i \leq l_1$ temos que

$$l_i \leq \delta r - \alpha \Rightarrow \delta r - \delta + \eta_i \leq \delta r - \alpha \Rightarrow \eta_i \leq \delta - \alpha.$$

Além disso,

$$q = l_2 + ... + l_w \geq l_2 + ... + l_t = (t-1)(\delta r - \delta) + \eta_2 + ... + \eta_t,$$

daí

$$\begin{aligned} \eta_2 + ... + \eta_t &\leq q - (t-1)(\delta r - \delta) \leq q - 2(\delta r - \delta) \\ &= (\delta + 1)r + \alpha - 2\delta r + 2\delta \\ &= -(\delta - 1)r + 2\delta + \alpha \leq \delta + \alpha + 1. \end{aligned}$$

Assim, formaremos T tomando $\delta - \alpha$ elementos de S_1, e $\delta + \alpha + 1$ de $S_2, ..., S_w$, com a condição de que não seja tomado nem mais que δ e nem menos que η_i elementos em cada S_i, para $i = 1, ..., t$. Isto é possível já que $l_2 \geq \delta$, $l_3 \geq \delta$, e $\eta_2 + ... + \eta_t \leq \delta + \alpha + 1$. Com esta escolha de T, temos que $m' = (2\delta + 1)(r-1)$ e $q' = (\delta + 1)(r-1)$, daí $r' = r - 1$ e $w' \geq 3$.

Caso II. Para este caso temos

$$q = (\delta + 1)r,\ m = (2\delta + 1)r + \beta, \text{ com } \beta > 0 \text{ e } l_1 = l_2.$$

Se $w = 2$, temos que $l_1 = l_2 = (\delta + 1)r$ e podemos, obviamente, formar T tomando $\delta + 1$ elementos de S_1 e $\delta + 1$ elementos de S_2. Com esta escolha, temos $l'_1 = l'_2 = q' = (\delta + 1)(r-1)$ e $m' = 2(\delta + 1)(r-1)$, daí a condição (2-8) é válida.

Se $w \geq 3$, temos

$$l_3 + ... + l_w = q - l_2 = q - l_1 = q - (m - q) = 2q - m = r - \beta.$$

Assim, $l_1 = l_2 = \delta r + \beta$ e, como $l_3 \leq r - \beta$,

$$l_1 - l_3 = \delta r + \beta - l_3 \geq \delta r + \beta - r - \beta = (\delta - 1)r + 2\beta \geq \delta - 1 + 2\beta \geq \delta + 1,$$

desde que $r \geq 1$ e $\beta \geq 1$. Consequentemente, $l_3 \leq l_1 - (\delta + 1)$. Para satisfazer (2-5) e (2-6), formaremos T tomando $\delta + 1$ elementos de S_1 e $\delta + 1$ de S_2. Logo,

$$l'_1 = l'_2 = \delta r + \beta - \delta - 1 = \delta(r-1) + \beta - 1 \geq \delta(r-1),$$

$$m' = m - (2\delta + 2) \geq (2\delta + 1)(r-1)$$

e

$$q' = q - (\delta + 1) = (\delta + 1)(r-1),$$

daí $r' = r - 1$ e, se $r > 1$, então $w' \geq 2$. Assim, (2-8) é satisfeito. Isto completa o prova da primeira afirmação do lema.

Agora provaremos a segunda afirmação. Precisamos mostrar a existência de

$$s = min\{\frac{m}{2}, q\}$$

pares disjuntos de elementos de S, onde nenhum par se encontra em um mesmo conjunto S_j. Se $m \geq 2q$, então $l_1 \geq q$ e podemos obviamente formar $q \leq \frac{m}{2}$ pares tomando um elemento de S_1 e um elemento dos conjuntos $S_2, ..., S_w$. Se $m < 2q$, podemos formar tais pares, par por par, escolhendo um elemento de cada dois maiores conjuntos. Este último processo nos dará $\frac{m}{2} < q$ pares disjuntos.

□

2.2 Congruências

Nesta seção apresentaremos alguns resultados de congruências necessários para a prova do Teorema 1. Primeiro consideraremos as congruências

$$\begin{cases} f & = & a_1x_1^k + ... + a_nx_n^k & \equiv & 0 \pmod{p} \\ g & = & b_1x_1^k + ... + b_nx_n^k & \equiv & 0 \pmod{p} \end{cases} \tag{2-10}$$

onde ao menos um coeficiente de cada par a_i, b_i não é divisível por p.

Consideremos

$$\delta = mdc(k, p-1), \quad k = p^\tau \delta k_0, \quad \text{onde } mdc(k_0, p) = 1. \tag{2-11}$$

Se J_m é o conjunto das m-ésimas potências módulo p, então $J_k = J_\delta$. Concluímos este fato de um resultado da Teoria Elementar dos Números que afirma que, para $a, k, p \in \mathbb{N}$, com p primo e $\delta = mdc(k, p-1)$, a congruência

$$x^k \equiv a \pmod{p}$$

tem solução se, e somente se, a congruência

$$x^\delta \equiv a \pmod{p}$$

também tem solução (ver [13], cap. 4).

Lema 2.2 *Se $n \geq 2\delta + 1$, então as congruências (2-10) têm uma solução não trivial.*

Prova. Pelo Teorema de Chevalley, demonstrado no capítulo anterior, vimos que o sistema de congruências (2-10) tem solução se $n > 2k$, isto é, se $n \geq 2k + 1$. Note então que, pelo

que foi afirmado no parágrafo anterior, isto é o mesmo que dizer que (2-10) tem solução se $n \geq 2\delta + 1$.

Lema 2.3 *Se $n \geq 2\delta+1$ e toda forma $\alpha f + \beta g$, $(\alpha, \beta \not\equiv 0, 0 \pmod{p})$ contém ao menos $\delta+1$ variáveis com coeficientes não divisíveis por p, então as congruências (2-10) têm uma solução cuja matriz*

$$\Delta^* = \begin{pmatrix} a_1 x_1 & \ldots & a_n x_n \\ b_1 x_1 & \ldots & b_n x_n \end{pmatrix} \tag{2-12}$$

tem posto 2 módulo p, isto é, o sistema (2-10) tem solução não singular.

Para provar este lema precisaremos de outros dois resultados (ver Apêndice).

Lema 2.4 *Seja p um primo e*

$$F(x_1, \ldots, x_m) = a_1 x_1^k + \ldots + a_m x_m^k,$$

onde k divide $p-1$ e onde $a_1 \ldots a_m \not\equiv 0 \pmod{p}$. Então, se $m \leq k$, o número de classes de restos módulo p distintas, diferentes de zero, representadas por F é ao menos $m(p-1)/k$.

Lema 2.5 *Seja p um primo e k um fator de $p-1$. Sejam G, H formas aditivas de grau k em $y_1, \ldots, y_s$, onde $s > k$. Seja $\gamma_1, \ldots, \gamma_\mu$ classes de restos módulos p não nulas, onde*

$$\mu > (p-1)(2k-s)/k.$$

Então existem $y_1, \ldots, y_s$, nem todos nulos módulo p, tais que,

$$G(y_1, \ldots, y_s) \equiv 0 \pmod{p}$$

e

$$H(y_1, \ldots, y_s) \equiv 0 \text{ ou } \gamma_i \pmod{p}$$

para algum i.

Agora podemos provar o Lema 2.3.

Prova. Desde que $J_k = J_\delta$, podemos assumir, sem perder a generalidade, que k divide $p-1$. Pelo Lema 2.2, garantimos que o sistema (2-10) possui solução não trivial. Tomemos uma solução que tenha o maior número possível de $x_1, \ldots, x_n \not\equiv 0$. Através de permutação de variáveis, podemos supor que esta solução é

$$(\xi_1, \ldots, \xi_R, 0, \ldots, 0),$$

onde cada $\xi_i \not\equiv 0$. Podemos assumir que esta solução é singular e, portanto,

$$a_1 b_j - b_1 a_j \equiv 0 \pmod{p} \text{ para } 1 \leq j \leq R. \tag{2-13}$$

Se existem valores de j maiores do que R, para que (2-13) valha, então pegamos estes valores, seja de $R+1,...,r$, e de outro modo façamos $r = R$. Vamos supor que $a_1 \not\equiv 0 \pmod{p}$. A forma $g_1 = a_1 g - b_1 f$ tem seus r primeiros coeficientes nulos. Iremos trabalhar com o par de formas f, g_1 ao invés de f, g.

Podemos escrever

$$\begin{aligned} f &= a_1 x_1^k + ... + a_r x_r^k + A_1 y_1^k + ... + A_s y_s^k, \\ g_1 &= B_1 y_1^k + ... + B_s y_s^k, \end{aligned}$$

onde todos os a_i's e todos os B_i's não são nulos módulo p. Temos

$$r + s = n \geq 2k + 1,$$

e pela segunda hipótese do lema temos

$$s \geq k + 1.$$

Caso I. Suponha $r \geq k$. Como $s \geq k+1$, pelo Teorema de Chevalley, existe uma solução de $g_1 \equiv 0 \pmod{p}$ com $y_1, ..., y_s$ não todos nulos. Para esta solução, temos

$$A_1 y_1^k + ... + A_s y_s^k \not\equiv 0 \pmod{p},$$

caso contrário, $(\xi_1, ..., \xi_r, y_1, ..., y_s)$ seria solução de $f \equiv g_1 \equiv 0$, com mais de R valores não nulos, contrariando a construção.

Pelo Lema 2.4, com $m = k \leq r$, a forma $a_1 x_1^k + ... + a_r x_r^k$ assume todos os valores diferentes de 0. Em particular, ela assume o valor

$$-(A_1 y_1^k + ... + A_s y_s^k),$$

e obviamente, faz com que $x_1, ..., x_r$ sejam nem todos nulos. As congruências $f \equiv g_1 \equiv 0$ agora tem a solução

$$(x_1, ..., x_r, y_1, ..., y_s),$$

e esta é não singular com $x_i y_j \not\equiv 0$ para algum $i \leq r$ e algum $j \leq s$, e $a_i B_j \not\equiv 0$, como comentado anteriormente.

Caso II. Suponha $r < k$. Temos que $s = n - r > 2k - r$. Pelo Lema 2.4, a forma $a_1 x_1^k + ... + a_r x_r^k$ assume ao menos $r(p-1)/k$ valores não nulos distintos. Chame estes

valores de $-\gamma_1, ..., -\gamma_\mu$, onde

$$\mu \geq r(p-1)/k > (2k-s)(p-1)/k.$$

Pelo Lema 2.5, existe uma solução de $g_1 \equiv 0$ com $y_1, ..., y_s$, nem todos nulos, para que

$$A_1 y_1^k + ... + A_s y_s^k \equiv 0$$

ou

$$A_1 y_1^k + ... + A_s y_s^k \equiv \gamma_j,$$

para algum j. A primeira alternativa é impossível pelo mesmo motivo mencionado no Caso I. Logo, as congruências $f \equiv g_1 \equiv 0$ têm a solução

$$(x_1, ..., x_r, y_1, ..., y_s),$$

e esta é novamente não singular, com $x_i y_j \not\equiv 0$ para algum $i \leq r$ e algum $j \leq s$. □

Lema 2.6 *Se* $c_1 c_2 ... c_{\delta+1} \not\equiv 0 \pmod{p}$, *então a congruência*

$$c_1 x_1^k + ... + c_{\delta+1} x_{\delta+1}^k \equiv 0 \pmod{p} \tag{2-14}$$

tem uma solução com $x_1 \not\equiv 0 \pmod{p}$.

Prova. Como $J_k = J_\delta$, podemos trocar k por δ em (2-14). Se a conclusão do lema não é verdadeira, então

$$c_1 + c_2 x_2^\delta + ... + c_{\delta+1} x_{\delta+1}^\delta \not\equiv 0 \pmod{p}$$

para todo $x_2, ..., x_{\delta+1}$. Daí, pelo Pequeno Teorema de Fermat,

$$(c_1 + c_2 x_2^\delta + ... + c_{\delta+1} x_{\delta+1}^\delta)^{p-1} - 1 \equiv 0 \pmod{p}$$

para todo $x_2, ..., x_{\delta+1}$. Como é bem conhecido, isto implica que a congruência se torna uma identidade quando, em cada produto de potências na expansão da parcela do lado esquerdo, x_j^p é trocado por x_j, para cada j repetidamente, até cada expoente ser no máximo $p-1$. Mas, essa expansão, contém um termo

$$a(x_2^\delta ... x_{\delta+1}^\delta)^{(p-1)/\delta} = a x_2^{p-1} ... x_{\delta+1}^{p-1}$$

com $a \not\equiv 0 \pmod{p}$, que não é afetado por tais operações. Todos os outros termos contém ao menos uma das variáveis $x_2, ..., x_{\delta+1}$ com uma potência menor do que $p-1$. Daí, o

polinômio não pode ser reduzido a uma identidade e isto prova o lema. □

Lema 2.7 *Se* $\delta = (p-1)/2 \geq 3$*, então a congruência*

$$\chi = d_1 x_1^k + ... + d_\delta x_\delta^k \equiv 0 \pmod{p}$$

tem uma solução não trivial módulo p.

Prova. Observe que, se dermos a cada variável x_i os valores 0 ou 1, nós obtemos 2^δ valores para a forma χ. Como existem no máximo p valores distintos de $\chi \pmod{p}$ e como $2^\delta > 2\delta + 1 = p$, para $\delta \geq 3$, no mínimo dois destes valores são congruentes. Digamos

$$d_1 \xi_1^k + ... + d_\delta \xi_\delta^k \equiv d_1 \eta_1^k + ... + d_\delta \eta_\delta^k \pmod{p},$$

e então

$$d_1(\xi_1^k - \eta_1^k) + ... + d_\delta(\xi_\delta^k - \eta_\delta^k) \equiv 0 \pmod{p}.$$

Mas $\xi_i^k - \eta_i^k \equiv 0,\ 1\ ou\ -1 \pmod{p}$ e, ao menos uma dessas diferenças não é nula. Como 0, 1 e -1 estão em J_k, então nós obtemos a solução necessária. □

Lema 2.8 *Se* $c_1, ..., c_n, d_1, ..., d_n$ *são inteiros e* $n \geq (2\delta+1)^m$*, então as congruências*

$$\begin{aligned} \Gamma &= c_1 x_1^k + ... + c_n x_n^k \equiv 0 \pmod{p^m}, \\ B &= d_1 x_1^k + ... + d_n x_n^k \equiv 0 \pmod{p^m}, \end{aligned} \tag{2-15}$$

têm uma solução $x_1, ..., x_n$ *de inteiros nem todos divisíveis por p.*

Prova. Provaremos por indução em m. O resultado é verdadeiro para $m = 1$, pois para algum i, se tivermos $c_i \equiv d_i \equiv 0 \pmod{p}$, a solução obviamente existe. Se este não é o caso, podemos aplicar o Lema 2.2.

Suponha que o resultado seja verdadeiro para $m-1$. Vamos dividir as n variáveis em $2\delta+1$ conjuntos disjuntos de modo que cada conjunto contenha ao menos $(2\delta+1)^{m-1}$ variáveis. Isto é possível, pois por hipótese

$$n \geq (2\delta+1)^m, \text{ logo } \frac{n}{2\delta+1} \geq (2\delta+1)^{m-1}.$$

Seja $\Gamma_j = \sum c_i x_i^k$ e $B_j = \sum d_i x_i^k$, onde os somatórios têm as variáveis do j-ésimo conjunto. Pela hipótese de indução, para cada j, o par de congruências

$$\Gamma_j \equiv 0 \pmod{p^{m-1}}, \quad B_j \equiv 0 \pmod{p^{m-1}}$$

tem soluções $\xi^{(j)}$, com nem todas as coordenadas divisíveis por p. Façamos então

$$\Gamma_j(\xi^{(j)}) = p^{m-1}.q_j \text{ e } B_j(\xi^{(j)}) = p^{m-1}.s_j.$$

Agora, para cada j, multiplique $\xi^{(j)}$ por uma variável t_j e veja que

$$\Gamma_j(\xi^{(j)}t_j) = p^{m-1}.q_j t_j^k \text{ e } B_j(\xi^{(j)}t_j) = p^{m-1}.s_j t_j^k,$$

logo

$$\Gamma = p^{m-1}\gamma(t_1,...,t_{2\delta+1}), \quad B = p^{m-1}\beta(t_1,...,t_{2\delta+1}),$$

onde γ e β são formas aditivas de grau k. Para o caso $m = 1$, as congruências

$$\gamma(t_1,...,t_{2\delta+1}) \equiv 0 \pmod{p}, \quad \beta(t_1,...,t_{2\delta+1}) \equiv 0 \pmod{p}$$

tem uma solução, com nem todos os $t_i's$ divisíveis por p, pelo Lema 2.2. Mas, então,

$$t_1\xi^{(1)},...,t_{2\delta+1}\xi^{(2\delta+1)}$$

é uma solução de (2-15). Isto prova o Lema 2.8. □

Considere a seguinte adaptação do Lema de Hensel para sistemas de duas formas aditivas:

Lema 2.9 *Se as congruências*

$$f \equiv 0 \pmod{p^\gamma}, \quad g \equiv 0 \pmod{p^\gamma}, \tag{2-16}$$

onde f, g são as formas da esquerda em (2-10) e γ é como foi definido no Capítulo 1, têm uma solução não singular nos inteiros, ou seja, para o qual a matriz

$$\begin{pmatrix} a_1x_1 & \dots & a_Nx_N \\ b_1x_1 & \dots & b_Nx_N \end{pmatrix} \tag{2-17}$$

tem posto dois módulo p, então as equações (2-10) têm uma solução p-ádica não trivial.

O lema a seguir é semelhante ao Lema 1.14 para sistemas com duas formas aditivas, mas que menciona também quanto ao número de variáveis em outros níveis além do nível zero. Fato que precisaremos mais adiante.

Lema 2.10 *Um par de formas aditivas p-normalizadas, como em (2-1), de grau k pode ser escrito como*

$$\begin{aligned} f &= f_0 + pf_1 + \ldots + p^{k-1}f_{k-1}, \\ g &= g_0 + pg_1 + \ldots + p^{k-1}g_{k-1}, \end{aligned} \tag{2-18}$$

onde f_i, g_i são formas com m_i variáveis, onde estes conjuntos de variáveis são disjuntos para $i \in \{0,1,...,k-1\}$. Mais ainda, cada uma das m_i variáveis estão explícitas em ao menos uma das formas f_i, g_i e temos

$$m_0 + \ldots + m_{j-1} \geq \frac{jn}{k} \text{ para } j \in \{1,...,k\}. \tag{2-19}$$

E mais ainda, se q_j denota o número mínimo de variáveis que aparecem explicitamente em uma combinação linear não trivial módulo p, $\gamma f_j + \mu g_j$, então

$$m_0 + \ldots + m_{j-1} + q_j \geq \frac{(2j+1)n}{2k} \text{ para } j \in \{1,...,k\}. \tag{2-20}$$

*Prova.*Como foi dito no Capítulo 1, através de separação por níveis, podemos escrever (2-1) como está em (2-18) e, obviamente, os conjuntos de variáveis de cada par f_j, g_j são disjuntos.

Agora provaremos que as formas f_j e g_j são vazias se $j \geq k$. Isto segue da propriedade de minimalidade de $\vartheta(f,g)$. Sejam $a_i x_i^k$ e $b_i x_i^k$ termos arbitrários de f,g com a_i, b_i não divisíveis por p^k simultaneamente, então poderíamos diminuir a potência de p de $\vartheta(f,g)$ usando a operação (i) do Lema 1.10 colocando $x_i = p^{-1}x_i'$, sempre preservando a característica inteira dos coeficientes do sistema.

Sejam $x_1,...,x_m$, onde $m = m_0 + ... + m_{j-1}$, as variáveis em f_0, g_0; f_1, g_1; ...; f_{j-1}, g_{j-1}. Então temos as formas

$$f' = p^{-j} f(px_1,...,px_m,x_{m+1},...,x_n),$$

$$g' = p^{-j} g(px_1,...,px_m,x_{m+1},...,x_n),$$

com coeficientes inteiros e que são equivalentes a f,g. Pelo Lema 1.10

$$\vartheta(f',g') = p^{-2jn(n-1)} p^{2k(n-1)m} \vartheta(f,g)$$

e, pela definição de sistema normalizado,

$$-2jn(n-1) + 2k(n-1)m \geq 0 \Rightarrow m \geq \frac{jn}{k},$$

provando (2-19).

Para provar (2-20) podemos supor, sem perda de generalidade, que q_j é o número de variáveis que aparecem explicitamente em g_j. Considere $x_{m+1},...,x_{m+q}$ essas tais variáveis, com $q = q_j$. Então, as formas

$$f'' = p^{-j} f(px_1,...,px_{m+q},x_{m+q+1},...,x_n),$$

$$g'' = p^{-j-1} g(px_1, ..., px_{m+q}, x_{m+q+1}, ..., x_n),$$

tem coeficientes inteiros e são equivalentes a f, g. Pelo Lema (1.10),

$$\vartheta(f'', g'') = p^{-(2j+1)n(n-1)} p^{2k(n-1)(m+q)} \vartheta(f, g).$$

Assim, $m+q \geq (j+\frac{1}{2})n/k$, implicando (2-20). Isto completa a prova do Lema 2.10.

□

Lema 2.11 *Cada par de formas aditivas com coeficientes racionais e $\vartheta \neq 0$ é p-equivalente a um par $f,\ g$ p-normalizado possuindo as seguintes propriedades:*

(i) *g_0 contém exatamente q_0 variáveis explícitas.*

(ii) *Uma das formas $f_1,\ g_1$ contém exatamente q_1 variáveis explícitas.*

(iii) *g_0 tem a forma*

$$g_0 = p^2 \sum_{1}^{u} \alpha_i x_i^k + p \sum_{u+1}^{m_0-q_0} \beta_i x_i^k + \sum_{m_0-q_0+1}^{m_0} \gamma_i x_i^k. \tag{2-21}$$

onde $\beta_{u+1}, ..., \beta_{m_0-q_0},\ \gamma_{m_0-q_0+1}, ..., \gamma_{m_0}$ não são nulos módulo p, e

$$m_0 + v - N/k \geq u \geq (m_0 - q_0)/p, \tag{2-22}$$

onde v é o número de variáveis explícitas g_1. Mais ainda, se a_i é o coeficiente de x_i em f_0, então as razões $a_i/\beta_i \pmod p$, com $u+1 \leq i \leq m_0 - q_0$, dividem-se em conjuntos de razões iguais com nenhum conjunto contendo mais do que u razões.

Prova. Por definição, cada par de formas aditivas com $\vartheta \neq 0$ é p-equivalente a um par p-normalizado. Se $f,\ g$ é um par p-normalizado, então existem $\gamma_0\mu_0 \not\equiv 0 \pmod p$ tais que $\gamma_0 f + \mu_0 g$ contém exatamente q_0 variáveis explícitas. Neste caso, um dos dois pares p-equivalentes

$$f,\ \gamma_0 f + \mu_0 g \quad ou \quad \gamma_0 f + \mu_0 g,\ g$$

também é um par p-normalizado, pois a potência de p que divide ϑ continua sendo a mesma já que γ_0 e μ_0 não são divisíveis por p. Daí, sem perda de generalidade, podemos assumir que $f,\ g$ tem a propriedade (i).

Agora suporemos que g_1 contém mais que q_1 variáveis explícitas. Então existem γ_1 e μ_1, com $\gamma_1 \not\equiv 0 \pmod p$ tal que $\gamma_1 f_1 + \mu_1 g_1$ contém exatamente q_1 variáveis explícitas módulo p. O par $f' = \gamma_1 f + \mu_1 g,\ g$ é p-equivalente ao par p-normalizado $f,\ g$, satisfaz (i) e é tal que f_1' contém exatamente q_1 variáveis explícitas. Daí podemos assumir que $f,\ g$ satisfaz (i) e (ii).

Agora nós podemos supor que

$$\begin{array}{lll} f_0 = & a_1x_1^k + ... & +a_{m_0}x_{m_0}^k \\ g_0 = & p(c_1x_1^k + ... + c_{m_0-q_0}x_{m_0-q_0}^k) & +(b_{m_0-q_0+1}x_{m_0-q_0+1}^k ... b_{m_0}x_{m_0}^k) \end{array},$$

onde $a_1, ..., a_{m_0-q_0}$ e $b_{m_0-q_0+1}, ..., b_{m_0}$ não são nulos módulo p. As razões $c_i/a_i \pmod p$ dividem-se no máximo em p conjuntos. Após uma renumeração de variáveis, podemos supor que

$$c_1/a_1 \pmod p, ..., c_u/a_u \pmod p$$

é o conjunto com o maior número de elementos. Assim,

$$u \geq \frac{m_0 - q_0}{p}.$$

Mais ainda, $f,\ g' = a_1g - c_1pf$ é um par de formas p-normalizado que é p-equivalente a $f,\ g$ e que satisfaz (i) e (ii). Além disso, g_0' tem a forma (2-21).

Agora multipliquemos as $m_0 - u + v$ variáveis por p, onde $u+1 \leq i \leq m_0$ ou x_i é uma das v variáveis com coeficientes em g_1' não nulos módulo p. Então

$$g' = p^2g'',$$

onde g'' é uma forma aditiva com coeficientes inteiros, e

$$\vartheta(f, g'') = p^{-2n(n-1)+2k(n-1)(m_0-u+v)}\vartheta(f, g).$$

Como $f,\ g$ é p-normalizado, segue que

$$-2n(n-1) + 2k(n-1)(m_0 - u + v) \geq 0,$$

logo,

$$k(m_0 - u + v) \geq n,$$

e isto implica 2-22. Isto completa a prova do Lema 2.11. □

2.3 Demonstração do Teorema 1

Para a demonstração do teorema principal desse capítulo iremos traçar um plano geral. A estratégia será decompor o conjunto das m_0 variáveis que aparecem em f_0, g_0 em

conjuntos disjuntos $S_0, S_1, ..., S_t$ tais que as subcongruências

$$\sum_{i \in X_j} a_i x_i^k \equiv 0 \pmod{p}, \sum_{i \in X_j} b_i x_i^k \equiv 0 \pmod{p}$$

para $j = 1, ..., t$, tem uma solução $\xi^{(j)}$ não trivial módulo p.

Se x_i está em X_j, para $j = 1, ..., t$ fixaremos $x_i = \xi_i^{(j)} y_j$ e se x_i está em X_0 fixaremos $x_i = 0$. Então teremos

$$f(x_1, ..., x_n) = p\Phi_1(y_1, ..., y_t, x_{m_0+1}, ..., x_n),$$

$$g(x_1, ..., x_n) = p\Psi_1(y_1, ..., y_t, x_{m_0+1}, ..., x_n).$$

Se a solução $\xi^{(j)}$ é tal que

$$\Delta_j = \begin{pmatrix} a_i \xi_i^{(j)} \\ b_i \xi_i^{(j)} \end{pmatrix}, \text{ para } i \in S_j, \tag{2-23}$$

tem posto dois módulo p, diremos que y_j é uma *variável primária de nível um*. As variáveis em Φ_1, Ψ_1 que não são primárias, mas que tem um coeficiente ou em Φ_1 ou em Ψ_1 não divisível por p são ditas *variáveis secundárias de nível um*. Veja que a quantidade de variáveis secundárias de nível um são ao menos m_1.

Agora decomponha as variáveis primárias e secundárias de nível um em conjuntos disjuntos $S_0', S_1', ..., S_s'$ de forma que os pares de subcongruências associadas aos conjuntos $S_1', ..., S_s'$ tenham uma solução $\eta^{(j)}$ não-trivial módulo p em comum. Se uma variável está no conjunto S_j', para $j = 1, ..., s$, faremos ela ser igual ao produto de uma nova variável z_j pela solução $\eta^{(j)}$ e se a variável está em S_0' fixaremos ela como igual a 0, como feito anteriormente. Assim teremos

$$f(x_1, ..., x_n) = p^2\Phi_2(z_1, ..., z_s, x_{m_0+m_1+1}, ..., x_n),$$

$$g(x_1, ..., x_n) = p^2\Psi_2(z_1, ..., z_s, x_{m_0+m_1+1}, ..., x_n).$$

Se o conjunto S_j' contém uma variável primária de nível um cujo valor na solução $\eta^{(j)}$ não é divisível por p, diremos que a variável associada z_j é uma *variável primária de nível dois*. E novamente, variáveis que não são primárias de nível dois, mas cujos coeficientes em Φ_2 ou em Ψ_2 não são divisíveis por p, constituem as *variáveis secundárias de nível dois*.

Continuando esse processo pode-se aumentar os níveis. Tal processo nos garante que alguma solução de $f, g \equiv 0 \pmod{p}$, com variáveis primárias não todas nulas módulo

p, terá a matriz

$$\Delta = \begin{pmatrix} a_1x_1 & \dots & a_nx_n \\ b_1x_1 & \dots & b_nx_n \end{pmatrix} \tag{2-24}$$

com posto dois módulo p.

Na verdade em nossa demonstração não precisaremos aumentar mais o nível além do nível dois. Daí, a prova do Teorema 1 se baseia em provar que existem ao menos $(2\delta+1)^{\gamma-1}$ variáveis primárias de nível um ou ao menos $(2\delta+1)^{\gamma-2}$ variáveis primárias de nível dois, pois assim, pelo Lema 2.8, conseguiremos garantir uma solução não singular para o sistema

$$\Phi_1 \equiv 0 \pmod{p^{\gamma-1}}, \qquad \Psi_1 \equiv 0 \pmod{p^{\gamma-1}},$$

ou

$$\Phi_2 \equiv 0 \pmod{p^{\gamma-2}}, \qquad \Psi_2 \equiv 0 \pmod{p^{\gamma-2}},$$

respectivamente. Logo, teremos uma solução das congruências $f \equiv 0 \pmod{p^{\gamma}}$, $g \equiv 0 \pmod{p^{\gamma}}$ para o qual a matriz Δ tenha posto dois módulo p. Segue então do Lema 2.9 que as equações $f = 0,\ g = 0$ tem uma solução p-ádica não trivial em comum.

Iremos seguir essa estratégia em três casos separados de acordo com os valores de δ: para $\delta \neq (p-1)/2$ ou $\delta \neq p-1$; para $\delta = (p-1)/2 \geq 3$ e para $\delta = 1$ quando $p = 3$. Em todos os casos suporemos que $\vartheta(f,g) \neq 0$ e que f, g tem as propriedades especificadas no Lema 2.10.

Inicialmente consideremos o sistema (2-18) e consideremos as m_0 variáveis das formas f_0 e g_0. Iremos dividir essas variáveis em conjuntos cujas razões dos coeficientes associados a essas variáveis em f_0 e g_0, $a_ib_i^{-1}$, sejam iguais módulo p. Digamos que esses conjuntos sejam $S_1, \dots, S_w$, onde

$$| S_1 | = m_0 - q_0 \geq | S_j | \text{ para } j = 2, \dots, w.$$

Pelo Lema 2.1, podemos formar

$$r = \min\left\{ \left[\frac{m_0}{2\delta+1} \right], \left[\frac{q_0}{\delta+1} \right] \right\}$$

conjuntos disjuntos de variáveis $T_1, \dots, T_r$, onde

$$2\delta+1 \leq | T_j | \leq 2\delta+2$$

e

$$| T_j | - | T_j \cap S_t | \geq \delta+1,$$

para $j = 1, ..., r$ e $t = 1, ..., w$, ou seja, as subformas

$$F_j = \sum_{i \in T_j} a_i x_i^k \text{ e } G_j = \sum_{i \in T_j} b_i x_i^k$$

são tais que existem ao menos $\delta + 1$ razões módulo p dentre $a_i b_i^{-1}$, $i \in T_j$, que são distintas de alguma razão específica. Logo, pelo Lema 2.3, as congruências $F_j \equiv 0 \pmod{p}$ e $G_j \equiv 0 \pmod{p}$ tem uma solução em comum $\xi^{(j)}$ para que Δ_j dado em (2-24) tenha posto dois módulo p. Assim, cada um dos conjuntos $T_1, ..., T_r$ contribuem com uma variável primária de nível um.

Nosso objetivo passa a ser então mostrar que

$$r \geq (2\delta + 1)^{\gamma - 1}. \tag{2-25}$$

Pois, mostrando isso, teremos pelo Lema 2.8, que as congruências

$$\Phi_1(y_1, ..., y_r, 0, ..., 0) \equiv 0 \pmod{p^{\gamma-1}},$$

$$\Psi_1(y_1, ..., y_r, 0, ..., 0) \equiv 0 \pmod{p^{\gamma-1}},$$

possuem solução em comum com nem todas as variáveis divisíveis por p. Daí poderemos concluir que tais congruências são solúveis com alguma variável primária não divisível por p e, portanto, as hipóteses do Lema 2.9 são válidas.

Portanto provemos (2-25).

Consideremos $k = p^\tau \delta k_0$, onde $mdc(p, k_0) = 1$ e $\delta = mdc(p-1, k)$. Como consideraremos $n \geq 2k^2 + 1$, pelo Lema 2.10

$$m_0 \geq 2k + 1 \quad \text{e} \quad q_0 \geq k + 1.$$

Veja que, se $\tau = 0$, então $\gamma = 1$ e $m_0 \geq 2\delta + 1$ e $q_0 \geq \delta + 1$. Assim, neste caso, $r \geq 1$ e (2-25) vale. Mas, se $\tau > 0$, então $\gamma = \tau + 1$ e, para mostrar que (2-25) vale para todos os casos de δ estudados adiante, é suficiente mostrar que

$$m_0 \geq (2\delta + 1)^{\tau+1} \quad \text{e} \quad q_0 \geq (\delta + 1)(2\delta + 1)^\tau. \tag{2-26}$$

De fato, mostrar (2-26) é equivalente a mostrar (2-25) já que

$$r \geq \frac{m_0}{2\delta + 1} \geq \frac{(2\delta + 1)^{\tau+1}}{2\delta + 1} = (2\delta + 1)^\tau$$

e

$$r \geq \frac{q_0}{\delta + 1} \geq (2\delta + 1)^\tau.$$

Agora estudaremos os casos mencionados anteriormente.

2.3.1 Solubilidade das equações (2-1), quando $\delta \neq (p-1)/2$ ou $\delta \neq p-1$

Seja $\delta < (p-1)/2$, então $p \geq 5$ e $\delta \leq (p-1)/3$, ou seja, $p \geq 3\delta+1$.
Façamos primeiramente $3 \leq \delta < (p-1)/2$. Temos que

$$q_0 > k \geq p^\tau \delta \geq (3\delta+1)^\tau \delta \geq (2\delta+1)^\tau(\delta+1)$$

para todo $\tau \geq 1$, já que

$$\frac{\delta}{\delta+1} > \frac{2\delta+1}{3\delta+1}, \text{ para } \delta \geq 3.$$

Ainda temos que

$$m_0 > 2k > 2p^\tau \delta \geq 2(2\delta+1)^\tau(\delta+1) > (2\delta+1)^{\tau+1}.$$

Mas, se $\delta = 2 < (p-1)/2$, então $p \geq 7$ e

$$q_0 \geq k+1 \geq \delta p^\tau + 1 \geq 2.7^\tau + 1 \geq 3.5^\tau = (\delta+1)(2\delta+1)^\tau$$

e

$$m_0 \geq 2k+1 \geq 4.7^\tau + 1 \geq 5^{\tau+1},$$

para todo $\tau \geq 1$.

Agora, se $\delta = 1 < (p-1)/2$, então $p \geq 5$ e

$$q_0 \geq k+1 \geq 5^\tau + 1 \geq 2.3^\tau = (\delta+1)(2\delta+1)^\tau$$

e

$$m_0 \geq 2k+1 \geq 2.5^\tau + 1 \geq 3^{\tau+1} = (2\delta+1)^\tau,$$

para todo $\tau \geq 1$.

Assim, para todos os valores de $\delta < (p-1)/2$, a relação (2-26) é válida e, consequentemente para este caso, o sistema (2-1) possui solução p-ádica não trivial.

2.3.2 Solubilidade das equações (2-1), quando $\delta = (p-1)/2 \geq 3$.

Consideremos $\delta \geq 3$ e assim teremos $p \geq 7$. Vamos supor que (2-26) não é verdadeiro para este caso.

Inicialmente suporemos que

$$m_0 \geq 2q_0 \tag{2-27}$$

Neste caso, construiremos os conjuntos T_j de forma que eles irão consistir de δ variáveis do maior subconjunto de razões iguais módulo p e δ variáveis dos outros subconjuntos. Claramente, existem

$$t \geq \frac{q_0}{\delta}$$

de tais conjuntos. As subcogruências correspondentes à cada conjunto são da forma

$$\begin{aligned} a_1x_1^k + \ldots + a_\delta x_\delta^k + \quad & A_1y_1^k + \ldots + A_\delta y_\delta^k \equiv 0 \pmod{p}, \\ & B_1y_1^k + \ldots + B_\delta y_\delta^k \equiv 0 \pmod{p}, \end{aligned} \tag{2-28}$$

onde $a_1 \ldots a_\delta B_1 \ldots B_\delta \not\equiv 0 \pmod{p}$. Pelo Lema 2.7, a segunda congruência tem uma solução não trivial módulo p, digamos η. Seja

$$A = A_1\eta_1^k + \ldots + A_\delta\eta_\delta^k.$$

Se $A \not\equiv 0 \pmod{p}$, então pelo Lema 2.6, a congruência

$$a_1x_1^k + \ldots + a_\delta x_\delta^k + A \equiv 0 \pmod{p} \tag{2-29}$$

tem uma solução e, desta solução, ao menos um de $x_1, \ldots, x_\delta$ não é divisível por p. Mas, se $A \equiv 0 \pmod{p}$, então podemos aplicar o Lema 2.7 para obter uma solução de (2-29) com ao menos um de $x_1, \ldots, x_\delta$ não divisível por p.

Em qualquer caso, o par de congruências (2-28) tem uma solução comum para que a matriz

$$\begin{pmatrix} a_1x_1 & \ldots & a_\delta x_\delta & A_1y_1 & \ldots & A_\delta y_\delta \\ 0 & \ldots & 0 & B_1y_1 & \ldots & B_\delta y_\delta \end{pmatrix}$$

tenha posto dois módulo p.

Como $q_0 > k \geq p^\tau\delta$ temos que

$$t \geq \frac{q_0}{\delta} \geq p^\tau = (2\delta+1)^\tau.$$

Assim, existem ao menos $(2\delta+1)^\tau$ variáveis primárias de nível um e segue então que, para p ímpar, as hipóteses do Lema 2.9 são válidas.

Finalmente podemos supor que $m_0 \leq 2q_0 - 1$. Suponhamos ainda, por absurdo,

que

$$m_0 < (2\delta+1)^{\tau+1} = p^{\tau+1} \qquad \text{ou} \qquad q_0 < (\delta+1)(2\delta+1)^{\tau} = (\delta+1)p^{\tau}. \quad (2\text{-}30)$$

Na verdade suporemos que

$$m_0 \leq 2p^{\tau}(\delta+1) - 2.$$

Isto é possível já que, de outra forma,

$$m_0 \leq 2p^{\tau}(\delta+1) - 1 = p^{\tau}(2\delta+2) - 1 = p^{\tau+1} + p^{\tau} - 1 > p^{\tau+1},$$

e

$$q_0 \geq \frac{m_0+1}{2} \geq \frac{p^{\tau+1}+p^{\tau}}{2} = \frac{p^{\tau(p+1)}}{2} = p^{\tau}(\delta+1),$$

contrariando (2-30).

Pelo Lema 2.1, podemos formar r conjuntos, que chamaremos de conjuntos primários por contribuírem com ao menos uma variável primária de nível um, onde

$$\begin{aligned} r = \min\left\{\frac{m_0}{2\delta+1}, \frac{q_0}{\delta+1}\right\} &\geq \min\left\{\frac{2k+1}{2\delta+1}, \frac{k+1}{\delta+1}\right\} \\ &\geq \min\left\{2p^{\tau-1}\delta, \frac{p^{\tau}\delta}{\delta+1}\right\} \\ &\geq p^{\tau-1}(2\delta-1), \end{aligned} \quad (2\text{-}31)$$

já que

$$\frac{p^{\tau}\delta}{\delta+1} = p^{\tau-1}\frac{\delta(2\delta+1)}{\delta+1} \qquad \text{e} \qquad \frac{\delta(2\delta+1)}{\delta+1} > 2\delta - 1.$$

Notemos então que não garantimos uma quantidade suficiente de variáveis primárias de nível um.

Como $m_0 \leq 2p^{\tau}(\delta+1) - 2$, segue do Lema 2.10 que

$$m_1 \geq 4k+1-m_0 \geq 4p^{\tau}\delta + 1 - [2p^{\tau}(\delta+1) - 2] = 2p^{\tau}(\delta-1) + 3,$$

$$q_1 \geq 3k+1-m_0 \geq 3p^{\tau}\delta + 1 - [2p^{\tau}(\delta+1) - 2] = p^{\tau}(\delta-2) + 3.$$

Portanto, pelo Lema 2.1, podemos formar

$$\min\left\{\frac{m_1}{2}, q_1\right\} \geq p^{\tau}(\delta-2) + 1 > p^{\tau-1} \quad (2\text{-}32)$$

pares de variáveis secundárias de nível um, onde cada par consiste de variáveis cujas razões dos coeficientes $(a_i b_i^{-1})$ não são congruentes módulo p.

Por (2-31) e (2-32) podemos formar $p^{\tau-1}$ conjuntos disjuntos T_j' de variáveis primárias e secundárias de nível um, onde cada conjunto T_j' consiste de $2\delta - 1$ variáveis

primárias e um par de variáveis secundárias cujas razões de seus coeficientes são diferentes módulo p. Agora, pelo Lema 2.2, as subcongruências correspondentes a cada T_j' tem uma solução não trivial em comum e em tal solução os valores para as variáveis primárias não podem ser todos nulos módulo p, já que as variáveis secundárias possuem as razões de seus coeficientes diferentes módulo p. Assim, cada um dos conjuntos T_j' dão origem a uma variável primária de nível dois e, já que existem $p^{\tau-1} = (2\delta+1)^{\tau-1}$ conjuntos T_j', segue do Lema 2.8 que as hipóteses do Lema 2.9 são válidas. Logo, as equações (2-1) tem uma solução p-ádica não trivial quando $\delta = (p-1)/2 \geq 3$.

2.3.3 Solubilidade das equações (2-1), quando $p = 3$ e $\delta = 1$

Neste caso $k = 3^{\tau}k_0$ e, pelo Lema 2.10, temos

$$m_0 \geq \frac{n}{k} \geq \frac{2k^2+1}{k} = 2k + \frac{1}{k} \quad \Rightarrow \quad m_0 \geq 2.3^{\tau} + 1;$$

$$q_0 \geq \frac{n}{2k} \geq \frac{2k^2+1}{2k} = k + \frac{1}{2k} \quad \Rightarrow \quad q_0 \geq 3^{\tau} + 1;$$

$$m_0 + m_1 \geq \frac{2n}{k} \geq \frac{2(2k^2+1)}{k} = 4k + \frac{2}{k} \quad \Rightarrow \quad m_0 + m_1 \geq 4.3^{\tau} + 1;$$

$$m_0 + q_1 \geq \frac{3n}{2k} \geq \frac{3(2k^2+1)}{2k} = 3k + \frac{3}{2k} \quad \Rightarrow \quad m_0 + q_1 \geq 3.3^{\tau} + 1.$$

A estratégia aqui será dividir em casos pelos valores de m_i e q_i, onde iremos mostrar que existem 3^{τ} variáveis primárias de nível um ou $3^{\tau-1}$ variáveis primárias de nível dois e assim verificar a validade das hipóteses do Lema 2.9.

Caso 1. Suponha que $m_0 \geq 3^{\tau+1}$ e $q_0 \geq 2.3^{\tau}$, então pelo Lema 2.1 podemos encontrar

$$r = \min\left\{\frac{m_0}{2\delta+1}, \frac{q_0}{\delta+1}\right\} \geq \min\left\{\frac{3^{\tau+1}}{3}, \frac{2.3^{\tau}}{2}\right\} = 3^{\tau}$$

conjuntos disjuntos dentre as variáveis de $f_0,\ g_0$ que determinam as variáveis primárias de nível um.

Caso 2. Suponha que $q_0 \geq 4.3^{\tau-1}$ e $m_1 \geq 3^{\tau-1}$. Como $m_0 \geq 2.3^{\tau} + 1$, então pelo Lema 2.1

$$r \geq \min\left\{\frac{2.3^{\tau}+1}{3}, \frac{4.3^{\tau-1}}{2}\right\} = 2.3^{\tau-1}.$$

Logo, podemos construir $2.3^{\tau-1}$ conjuntos disjuntos dentre as variáveis de $f_0,\ g_0$, onde cada conjunto possui uma variável primária de nível um. Agora, formemos $3^{\tau-1}$ conjuntos consistindo de duas variáveis primárias de nível um e uma variável de $f_1,\ g_1$. Pelo Lema 2.2, cada uma das subcongruências correspondentes aos conjuntos formados por essas três variáveis tem uma solução não trivial módulo 3. Como a variável que não é primária tem

ao menos um coeficiente não nulo módulo 3 dentre as duas equações, podemos garantir que ao menos uma das variáveis primárias não é divisível por 3, caso contrário teríamos uma solução trivial. Assim, cada um dos $3^{\tau-1}$ conjuntos determina uma variável primária de nível dois, como queríamos.

Caso 3. Suponha que $q_0 \geq 4.3^{\tau-1}$ e $m_1 < 3^{\tau-1}$. Veja que, neste caso, $m_0 \geq 11.3^{\tau-1}+2$. Basta usarmos o Lema 2.10 e verificarmos que

$$m_0 \geq 4.3^{\tau}+1-m_1 > 4.3^{\tau}+1-3^{\tau-1} = 11.3^{\tau-1}+1.$$

Além disso, por causa do Caso 1, podemos supor que $2.3^{\tau} > q_0 \geq 4.3^{\tau-1}$. Então fixemos

$$\frac{q_0}{2} = 2.3^{\tau-1}+\alpha, \text{ onde } \alpha < 3^{\tau-1}$$

(caso $\alpha \geq 3^{\tau-1}$, contrariaríamos nossa hipótese de que $2.3^{\tau} > q_0$).

Segue do Lema 2.1 que podemos construir

$$r = \min\left\{\frac{m_0}{3}, \frac{q_0}{2}\right\} = 2.3^{\tau-1}+\alpha$$

conjuntos disjuntos com as variáveis de f_0, g_0, onde cada conjunto determina uma variável primária de nível um.

Primeiramente consideremos $m_1+\alpha \geq 3^{\tau-1}$. Daí podemos considerar as variáveis primárias e secundárias de nível um para construirmos $3^{\tau-1}$ conjuntos disjuntos onde cada conjunto possui duas variáveis primárias, como feito no Caso 2. Assim, conseguiremos determinar as $3^{\tau-1}$ variáveis primárias de nível dois.

Agora suponhamos que $m_1+\alpha < 3^{\tau-1}$. Façamos

$$T = 3^{\tau-1}-m_1-\alpha > 0.$$

Neste caso,

$$m_0 \geq 4.3^{\tau}+1-m_0 = 4.3^{\tau}+1+T+\alpha-3^{\tau-1} = 11.3^{\tau-1}+\alpha+T+1,$$

e

$$\begin{aligned} m_0-2q_0-3T &\geq 11.3^{\tau-1}+\alpha+T+1-2(4.3^{\tau-1}+2\alpha+1)-3T \\ &= 3.3^{\tau-1}-3\alpha-2T+1 \geq 3(3^{\tau-1}-\alpha-T) = 3m_1 \geq 0. \end{aligned}$$

Sabemos ainda que existem m_0-q_0 variáveis em f_0, g_0 com coeficientes em g_0 divisíveis por 3 e, consequentemente, tais variáveis têm coeficientes em f_0 que são congruentes a 1 ou -1 módulo 3. Como

$$m_0-q_0 \geq 3T+q_0 \geq 3T+4,$$

podemos encontrar T conjuntos formados, cada um, por três destas variáveis que acabamos de mencionar tais que seus coeficientes sejam iguais módulo 3. Daí, cada subcongruência correspondente a cada conjunto possui soluções não triviais tais como $(1,1,1)$ ou $(1,-1,0)$, etc., o que nos garante a existência de uma variável secundária de nível um, onde podemos escolher seu coeficiente em Φ_1 para que não seja divisível por 3. Ainda temos $m_0 - 3T \geq 2q_0$ variáveis no nível zero e, as q_0 variáveis que restam serão no máximo $m_0 - 3T - q_0 \geq q_0$. Contudo, podemos usar o Lema 2.1 para encontrarmos

$$\min\left\{\frac{m_0-3T}{3}, \frac{q_0}{2}\right\} = \frac{q_0}{2} = 2.3^{\tau-1} + \alpha$$

conjuntos disjuntos que determinam variáveis primárias de nível um. Assim, temos $2.3^{\tau-1}+\alpha$ variáveis primárias e $m_1 + T$ variáveis secundárias de nível um. Como $\alpha + T + m_1 = 3^{\tau-1}$, podemos, como anteriormente, construir $3^{\tau-1}$ conjuntos disjuntos com duas variáveis primárias e uma variável dentre o restante de variáveis primárias e as variáveis secundárias de nível um. Daí, garantimos as $3^\tau - 1$ variáveis primárias de nível dois, como fizemos anteriormente, provando o Caso 3.

Para os casos restantes, suporemos que

$$3^\tau + 1 \leq q_0 < 4.3^{\tau-1}.$$

Façamos

$$\frac{q_0}{2} = 2.3^{\tau-1} - \beta, \text{ onde } 0 < \beta \leq \frac{3^{\tau-1}}{2}. \tag{2-33}$$

Será suficiente mostrar que existem ao menos $2.3^{\tau-1} - \beta$ variáveis primárias e $3^{\tau-1} + \beta$ variáveis secundárias de nível um, onde existem ao menos β pares disjuntos de variáveis secundárias cujas razões de seus coeficientes em Φ_1 e Ψ_1 sejam diferentes módulo 3. Mostrando isso poderemos decompor as variáveis primárias e secundárias de nível um em ao menos $3^{\tau-1}$ conjuntos disjuntos de três elementos, onde cada conjunto terá duas variáveis primárias e uma variável secundária ou uma primária e duas variáveis secundárias de nível um com as razões de seus coeficientes diferentes módulo 3. Em qualquer um dos casos, cada subcongruência correspondente a cada um dos conjuntos construídos possui solução, de modo que a variável primária não é divisível por 3. Logo, cada um dos $3^{\tau-1}$ conjuntos determinarão uma variável primária de nível dois.

De acordo com os argumentos anteriores, provemos então os próximos casos.

Caso 4. Suponha que $q_0 < 4.3^{\tau-1}$, $m_1 \geq 3^{\tau-1} + \beta$ e $q_1 \geq \beta$. Como $m_0 > 2.3^\tau$, pelo Lema 2.1 podemos determinar ao menos $2.3^{\tau-1} - \beta$ variáveis primárias de nível um. Além disso, como $m_1 \geq 3^{\tau-1} + \beta > 2\beta$, a última afirmação do Lema 2.1 nos diz que podemos formar

$$\min\left(\frac{m_1}{2}, q_1\right) \geq \beta$$

pares de variáveis de f_1, g_1 cujas razões dos seus coeficientes sejam diferentes. Assim temos $m_1 \geq 3^{\tau-1} + \beta$ variáveis secundárias, como desejávamos.

Caso 5. Suponha que $q_0 < 4.3^{\tau-1}$, $3^{\tau-1} \leq m_1 < 3^{\tau-1} + \beta$ e $q_1 \geq \beta$. Como no Caso 4, podemos formar β pares de variáveis secundárias cujas razões de seus coeficientes em Φ_1 e Ψ_1 são diferentes módulo 3. Veja que, como $\beta \leq (3^{\tau-1} - 1)/2$ e precisamos mostrar que existem ao menos $3^{\tau-1} + \beta \geq 3\beta + 1$ variáveis secundárias, então ainda resta mostrar que existem mais β variáveis secundárias de nível um. Podemos ver que essas variáveis derivam dos β conjuntos formados por três variáveis de f_0, g_0 selecionadas como no Caso 3 de modo que em cada trio os coeficientes de f_0 são todos congruentes a 1 ou todos congruentes a -1 módulo 3 e os coeficientes em g_0 são nulos módulo 3. Isto é possível já que

$$\begin{aligned} m_0 - q_0 &\geq 2.3^{\tau} + 1 - (4.3^{\tau-1} - 2\beta) \\ &= 6.3^{\tau-1} - 4.3^{\tau-1} + 2\beta + 1 \\ &> 2.3^{\tau-1} + 2\beta \\ &\geq 2.(2\beta + 1) + 2\beta \qquad \text{(por (2-33))} \\ &> 3\beta + 4 \qquad \text{(pois } \tau > 1\text{).} \end{aligned}$$

Caso 6. Suponha neste caso que $q_0 < 4.3^{\tau-1}$, $m_1 \geq 3^{\tau-1}$ e $q_1 < \beta$. Desse modo teremos $m_0 \geq 3.3^{\tau} - \beta + 2$, já que $m_0 + q_1 \geq 3.3^{\tau} + 1$. Além disso

$$m_0 - 2q_0 - 3\beta \geq 3^{\tau-1} > 0 \tag{2-34}$$

Suponha primeiramente que f_1 contém exatamente q_1 variáveis com coeficientes não divisíveis por 3. Por (2-34),

$$\begin{aligned} m_0 - q_0 &\geq 3^{\tau-1} + 3\beta + q_0 \\ &\geq 3^{\tau-1} + 3\beta + (4.3^{\tau-1} - 2\beta) \\ &\geq 3\beta + 4 \qquad \text{(pois } \tau > 1\text{),} \end{aligned}$$

logo, podemos encontrar β conjuntos disjuntos contendo três variáveis de f_0, g_0 tais que as variáveis em todos esses trios tenham os coeficientes iguais módulo 3 em f_0 e em g_0 eles sejam nulos módulo 3. Como no Caso 3, cada um destes conjuntos determina uma variável secundária de nível um, com coeficiente em Φ_1 não divisível por 3. Temos então ao menos $m_1 + \beta \geq 3^{\tau-1} + \beta$ variáveis secundárias de nível um. Como $q_1 < \beta$ e $m_1 \geq 3^{\tau-1}$, existem ao menos

$$m_1 - q_1 \geq m_1 - \beta \geq \frac{3^{\tau-1} + 1}{2} > \beta$$

variáveis secundárias de nível um com coeficientes em Φ_1 divisíveis por 3. Assim, existem β pares disjuntos de variáveis secundárias cujas razões dos coeficientes de Φ_1 e Ψ_1 são

diferentes módulo 3.

Restaram $m_0 - 3\beta$ variáveis em f_0, g_0 depois da retirada dos β conjuntos. Como $m_0 - q_0 - 3\beta > q_0$, depois da retirada das 3β variáveis, o conjunto restante de razões iguais de maior cardinalidade contém $m_0 - q_0 - 3\beta$ variáveis. Podemos, portanto, usar o Lema 2.1 para construir

$$\min\left\{\frac{m_0 - 3\beta}{3}, \frac{q_0}{2}\right\} = \frac{q_0}{2} = 2.3^{\tau-1} - \beta$$

conjuntos dentre as variáveis restantes em f_0, g_0, obtendo assim $2.3^{\tau-1} - \beta$ variáveis primárias, fato que restava demonstrar.

Suponha agora que g_1 contém exatamente q_1 variáveis com coeficientes não divisíveis por 3. Por (2-22), no Lema 2.11, se u é o número de variáveis em g_0 com coeficientes divisíveis por 9, então

$$\frac{m_0 - q_0}{3} \leq u \leq m_0 + q_1 - \frac{n}{k}.$$

Mas, como

$$m_0 - q_0 \geq 3.3^{\tau} - \beta + 2 - (4.3^{\tau-1} - 2\beta) = 5.3^{\tau-1} + \beta + 2,$$

existem ao menos $5.3^{\tau-1} + \beta + 2$ variáveis em g_0 com coeficientes nulos módulo 3. Assim temos que

$$u \geq \frac{5.3^{\tau-1} + \beta + 2}{3} > \beta$$

e existem mais que β variáveis em g_0 com coeficientes divisíveis por 9 e, como

$$\begin{aligned}(m_0 - q_0) - u \geq (m_0 - q_0) - (m_0 + q_1 - \tfrac{n}{k}) &= \tfrac{n}{k} - q_1 - q_0 \\ &\geq 2.3^{\tau} - \beta - q_0 \\ &\geq 2.3^{\tau} - 4.3^{\tau-1} + \beta - 1 > \beta,\end{aligned}$$

existem ao menos β variáveis em g_0 com coeficientes divisíveis por 3 e não por 9. Assim, podemos encontrar β pares de variáveis em f_0, g_0 onde cada par contém uma variável com coeficiente em g_0 divisível por 9 e uma variável com coeficiente em g_0 divisível por 3 e não por 9. As razões dos coeficientes das variáveis de f_0 e de cada par T_l são da forma $a_i(9\alpha_i)^{-1}$ e $a_j(3\mu_j)^{-1}$, com $a_i a_j \mu_j \not\equiv 0 \pmod 3$. Para cada par T_l faremos $x_i = -a_j w_l$ e $x_j = a_i w_l$. Logo, w_l é uma variável secundária de nível um com seus coeficientes em Ψ_1 não nulos módulo 3. Agora temos ao menos $3^{\tau-1} + \beta$ variáveis secundárias de nível um e, como no caso anterior (de f_1 com q_1 variáveis), existem β pares de variáveis cujas razões dos coeficientes são diferentes módulo 3. Ainda há $m_0 - 2\beta$ variáveis restantes de f_0, g_0 e, como $m_0 - q_0 - 2\beta > q_0$, podemos, como anteriormente, construir $2.3^{\tau-1} - \beta$ variáveis

primárias de nível um, completando a prova para este caso.

Caso 7. Suponha que $q_0 < 4.3^{\tau-1}$ e $m_1 < 3^{\tau-1}$. Façamos ainda

$$\sigma = 3^{\tau-1} - m_1 > 0.$$

Assim, como $m_0 + m_1 \geq 4.3^{\tau} + 1$, temos que

$$\begin{aligned} m_0 &\geq 4.3^{\tau} + 1 - m_1 = 4.3^{\tau} + 1 - (3^{\tau-1} - \sigma) \\ m_0 &\geq 12.3^{\tau-1} - 3^{\tau-1} + 1 + \sigma \\ m_0 &\geq 11.3^{\tau-1} + 1 + \sigma \end{aligned}$$

e

$$\begin{aligned} m_0 - 2q_0 - 2\beta - 3^{\tau} &\geq 11.3^{\tau-1} + 1 + \sigma - 2(4.3^{\tau-1} - 2\beta) - 2\beta - 3.3^{\tau-1} \\ &= 2\beta + 1 + \sigma - 3^{\tau-1} \qquad (2\text{-}35) \\ &\geq 2\beta - 1 > 0 \qquad (\text{pois } \tau > 1 \text{ e } \sigma > 0). \end{aligned}$$

Por (2-22) existem ao menos $(m_0 - q_0)/3 \geq 3^{\tau-1} > \beta$ variáveis em f_0, g_0 com coeficientes divisíveis po 9. Além disso, não existe mais do que $m_0 + m_1 - \frac{n}{k}$ de tais variáveis, já que

$$m_0 + v - \frac{n}{k} < m_0 + m_1 - \frac{n}{k}.$$

Assim, existem

$$\begin{aligned} (m_0 - q_0) - u > (m_0 - q_0) - (m_0 + m_1 - \tfrac{n}{k}) &= \tfrac{n}{k} - q_0 - m_1 \\ &> 2.3^{\tau} - 4.3^{\tau-1} + 2\beta - 3^{\tau-1} > \beta \end{aligned}$$

variáveis em g_0 com coeficientes divisíveis por 3 e não por 9. Assim, podemos formar os β pares de razões diferentes módulo 3 para obter as β variáveis secundárias de nível um com seus coeficientes em Ψ_1 não nulos módulo 3. Ainda restaram $m_0 - q_0 - 2\beta$ variáveis em f_0, g_0 com coeficientes nulos módulo 3 em g_0. Mas,

$$\begin{aligned} m_0 - q_0 - 2\beta &\geq (11.3^{\tau-1} + 1 + \sigma) - (4.3^{\tau-1} - 2\beta) - 2\beta \\ &= 7.3^{\tau-1} + 1 + \sigma \\ &\geq 7.3^{\tau-1} + 2 = 3.3^{\tau-1} + 4.3^{\tau-1} + 2 \\ &> 3.3^{\tau-1} + 12. \end{aligned}$$

Daí, podemos formar $3^{\tau-1}$ trios das variáveis restantes de f_0, g_0 tal que para cada trio os coeficientes em f_0 são todos iguais a 1 ou -1 módulo 3 e, os coeficientes em g_0, são mutualmente congruentes módulo 3. Fazendo uma escolha conveniente para as três

variáveis, como no Caso 3, estes trios nos garante $3^{\tau-1}$ variáveis secundárias de nível um com coeficientes em Ψ_1 nulos módulo 3. Finalmente, como $m_0 - q_0 - 2\beta - 3^{\tau} > q_0$, o maior conjunto de razões iguais módulo 3, após a retirada dos β pares e os $3^{\tau-1}$ trios, excede q_0. Logo, podemos usar o Lema 2.1 a fim de obter

$$\min\left\{\frac{m_0 - 2\beta - 3^{\tau}}{3}, \frac{q_0}{2}\right\} = \frac{q_0}{2} = 2.3^{\tau-1} - \beta$$

conjuntos das variáveis restantes, o que nos fornecerá as $2.3^{\tau-1} - \beta$ variáveis primárias de nível um desejadas, completando a prova para este último caso.

Portanto, as equações (2-1) são solúveis quando $p = 3$ e $\delta = 1$.

2.3.4 Demonstração do Teorema 1

Teorema 1. *Se k é ímpar e $n \geq 2k^2 + 1$, então, para todo primo p, as equações aditivas (2-1) têm uma solução p-ádica não trivial.*

Prova. Como foi dito no Capítulo 1, podemos assumir que f, g, de (2-1), é um sistema p-normalizado e que $\vartheta(f,g) \neq 0$. Observe que quando k é ímpar δ também é e os casos desenvolvidos nas sub-seções 2.3.1, 2.3.2 e 2.3.3 apontam todas as possibilidades para os valores de δ. Logo, as equações aditivas (2-1) tem uma solução p-ádica não trivial. □

CAPÍTULO 3

Sistemas de três formas aditivas cúbicas

Neste capítulo iremos verificar a validade da Conjectura de Artin com relação à solubilidade de um sistema de três equações aditivas cúbicas sobre o corpo dos números p-ádicos, para $p \neq 3$ ou $p \neq 7$. Para este caso particular, a Conjectura diz que o sistema terá solução se possuir uma quantidade de variáveis superior a 27.

Considere então o seguinte sistema de três formas aditivas cúbicas com n variáveis

$$\begin{cases} F = a_1x_1^3 + \ldots + a_nx_n^3 &= 0 \\ G = b_1x_1^3 + \ldots + b_nx_n^3 &= 0 \\ H = c_1x_1^3 + \ldots + c_nx_n^3 &= 0 \end{cases} \tag{3-1}$$

onde os coeficientes são inteiros. Como principal objetivo deste capítulo, iremos provar o seguinte teorema:

Teorema 2 *Três equações aditivas cúbicas com n variáveis têm solução p-ádica não trivial em comum se* $n \geq 28$ *e* $p \neq 3$ *ou* $p \neq 7$.

Mas, com o Lema de Hensel (1.3), visto no capítulo 1, o nosso objetivo passa a ser provar o seguinte lema:

Lema 3.1 *Se F, G, H é um trio de formas p-normalizadas com* $n \geq 28$ *variáveis e* $p \neq 3$ *ou* $p \neq 7$*, então as congruências*

$$F \equiv G \equiv H \equiv 0 \pmod{p}$$

tem uma solução não singular.

Como os coeficientes das equações são inteiros, consideraremos então cada forma com os coeficientes no corpo $\mathbb{F}_p$, que são congruentes aos coeficientes originais. Diremos que o posto de uma forma é o número de variáveis que aparecem nela explicitamente, isto é, o número de variáveis cujos coeficientes não são nulos módulo p.

Assumiremos que F, G, H são formas diagonais cúbicas com exatamente 28 variáveis p-normalizadas. Em particular, pela conclusão do Lema 1.14, temos que

$$m_0 \geq 10 \text{ e } q_0 \geq 4.$$

Considere ainda f,g,h as formas no nível zero das respectivas formas F,G,H. Como $m_0 \geq 10$ podemos assumir que o sistema $f \equiv g \equiv h \equiv 0 \pmod{p}$ tem exatamente 10 variáveis, pois mesmo que não tenha apenas 10, basta considerarmos o restante das variáveis iguais a 0. Assumiremos, a partir de agora, um sistema equivalente ao original, da forma

$$\begin{cases} f \equiv a_1x_1^3 + \ldots + a_7x_7^3 & +x_8^3 & & \equiv 0 \pmod{p}, \\ g \equiv b_1x_1^3 + \ldots + b_7x_7^3 & & +x_9^3 & \equiv 0 \pmod{p}, \\ h \equiv c_1x_1^3 + \ldots + c_7x_7^3 & & & +x_{10}^3 \equiv 0 \pmod{p}. \end{cases} \tag{3-2}$$

Se R denota o posto mínimo de alguma forma $\alpha f + \beta g + \gamma h$, onde α, β, γ não são todos nulos módulo p, então segue do Lema 1.14 que $R \geq 4$. Temos ainda que $R \leq 8$, pois, mesmo se obtivermos 9 ou 10 variáveis a partir de alguma combinação linear de f, g e h, ainda podemos fazer outra combinação de modo que $R \leq 8$ por causa das variáveis x, y e z.

Proposição 3.2 *Definamos a função*

$$\begin{array}{rccc} \varphi: & \mathbb{F}_p^* & \to & \mathbb{F}_p^* \\ & x & \mapsto & x^3, \end{array}$$

onde $\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$.

(i) Se $p \not\equiv 1 \pmod{3}$ *então* φ *é um isomorfismo.*

(ii) Se $p \equiv 1 \pmod{3}$ *então* $|\, Im\varphi \,| = \frac{p-1}{3}$.

Esta proposição nos diz que, se $p \not\equiv 1 \pmod{3}$, todo elemento de $\mathbb{F}_p$ é cubo de algum elemento do próprio conjunto. Daí, com relação ao nosso sistema, podemos dizer que as formas diagonais cúbicas são formas lineares e podem ser resolvidas com $x \not\equiv 0$, $y \not\equiv 0$ e $z \not\equiv 0 \pmod{p}$, de maneira que a solução será não singular. Mas, se $p \equiv 1 \pmod{3}$, então $[\mathbb{F}_p^* : Im\varphi] = 3$, ou seja, podemos formar três classes laterais de $Im\varphi$ em $\mathbb{F}_p^*$, de forma que $\mathbb{F}_p^* = Im\varphi \cup AIm\varphi \cup BIm\varphi$ (união disjunta). Diremos que A e B são representantes das classes não cúbicas de $\mathbb{F}_p^*$. Então, de agora em diante, assumiremos que $p \equiv 1 \pmod{3}$ e $p > 7$.

Para provar o Lema 3.1 e, assim o Teorema 2, precisaremos ainda de alguns resultados relacionados a congruências que serão apresentados a seguir, nos lemas de 3.3 a 3.10.

3.1 Congruências

Lema 3.3 *A congruência*

$$ax^3 + by^3 + cz^3 \equiv d \pmod{p}$$

sempre é solúvel se $abcd \not\equiv 0 \pmod{p}$.

Prova. A prova segue do Lema (2.4), tomando $k = 3$. □

Lema 3.4 *A congruência*

$$ax^3 + by^3 + cz^3 \equiv 0 \pmod{p} \tag{3-3}$$

sempre é solúvel com ao menos uma das variáveis x, y ou z não nulas módulo p.

Prova. Seja $\mathbb{F}_p^3$ o grupo dos cubos dos elementos de $\mathbb{F}_p^*$. Podemos assumir que $abc \not\equiv 0$, caso contrário o resultado seria verdadeiro. Vimos que, se $p \not\equiv 1 \pmod{3}$, então $\mathbb{F}_p^* = \mathbb{F}_p^3$ e a forma $ax^3 + by^3 + cz^3$ pode ser vista como uma forma linear, que é solúvel. Por exemplo, se $a = k_1^3$ e $b = k_2^3$, então poderemos reescrever a congruência (3-3) assim:

$$(k_1x)^3 + (k_2y)^3 + cz^3 \equiv 0 \pmod{p}$$

e $(1, -k_2^{-1}k_1, 0)$ seria solução. Mas, se $p \equiv 1 \pmod{3}$ então, dado $\delta \notin \mathbb{F}_p^3$, temos a união disjunta

$$\mathbb{F}_p^* = \mathbb{F}_p^3 \cup \delta\mathbb{F}_p^3 \cup \delta^2\mathbb{F}_p^3.$$

Demonstraremos agora para este caso.

Suponha que ao menos dois dos coeficientes a, b e c pertençam à mesma classe, que indicaremos por $\lambda\mathbb{F}_p^3$, com $\lambda = 1$, δ, ou δ^2. Podemos escrever então, por exemplo, $a = \lambda k_1^3$ e $b = \lambda k_2^3$ e, da mesma maneira que no parágrafo anterior, poderemos reescrever a congruência (3-3) assim:

$$\lambda(k_1x)^3 + \lambda(k_2y)^3 + cz^3 \equiv 0 \pmod{p}$$

e $(1, -k_2^{-1}k_1, 0)$ seria solução.

Assim, resta o caso onde a, b e c se encontram em diferentes classes de $\mathbb{F}_p^*$. O seguinte resultado, encontrado em [15] e adaptado de acordo com nosso interesse, completa a prova do Lema 3.4:

Lema 3.5 *Se* $p \equiv 1 \pmod 3$*, então existe um elemento não nulo* δ *de* $\mathbb{F}_p$ *que não está em* $\mathbb{F}_p^3$ *e tal que a equação*

$$1+\delta = \delta^2 z^3$$

tem solução em $\mathbb{F}_p$*.*

Prova. Seja W um conjunto de elementos não nulos de $\mathbb{F}_p^*$ da forma $\rho^3 - 1$. Já que temos $(p-1)/3$ elementos da forma ρ^3 e temos que retirar o 1 desse grupo de elementos (pois W é um conjunto de elementos não nulos), então W contém exatamente $\frac{p-1}{3} - 1 = \frac{p-4}{3}$ elementos distintos. Seja W^{-1} o conjunto dos inversos multiplicativos dos elementos de W e faça $V = \mathbb{F}_p^3 \cup W \cup W^{-1}$. Então V contém no máximo $p-3$ elementos. Seja δ algum elemento não nulo de $\mathbb{F}_p$ que não está em V. Claramente, δ e $1+\delta$ não estão em $\mathbb{F}_p^3$, pois se $1+\delta$ estivesse em $\mathbb{F}_p^3$ teríamos $\delta \in W$. E ainda temos que δ^{-1} não está em V, assim $1+\delta^{-1}$ não está em $\mathbb{F}_p^3$, e conseqüentemente $1+\delta$ não está em $\delta\mathbb{F}_p^3$. Como -1 está em $\mathbb{F}_p^3$, $1+\delta \neq 0$, logo, segue que $1+\delta$ está em $\delta^2\mathbb{F}_p^3$. □

Como $abc \not\equiv 0$, então podemos considerar a equação (3-3) como sendo

$$x^3 + \alpha y^3 + \beta z^3 \equiv 0 \pmod p.$$

Agora vamos supor então, que $\alpha \in \delta\mathbb{F}_p^3$ e $\beta \in \delta^2\mathbb{F}_p^3$, isto é, existem $\alpha', \beta' \in \mathbb{F}_p^3$ tais que $\alpha = \delta\alpha'^3$ e $\beta = \delta^2\beta'^3$. Afirmamos que $(1, \alpha'^{-1}, t)$ é solução desta última equação, para algum $t \in \mathbb{F}_p^3$, basta usarmos o lema anterior. Isto completa a prova do Lema 3.4. □

Lema 3.6 *Se* $p \equiv 1 \pmod 3$ *e* $p > 7$*, a congruência*

$$ax^3 + by^3 \equiv c \pmod p$$

sempre é solúvel desde que $abc \not\equiv 0 \pmod p$.

Prova. Para provarmos esse lema vamos citar o seguinte resultado (ver Teorema 3 em [6]):

Seja

$$a_1 \ldots a_n \not\equiv 0 \pmod p \text{ e } mdc(p-1,k) < \tfrac{p-1}{2}$$

então, $a_1 x_1^k + \ldots + a_n x_n^k$ *representa todos os restos módulo p ou representa ao menos* $(2n-1)\frac{(p-1)}{(p-1,k)} + 1$ *restos módulo p.*

Fazendo $k = 3$ e $n = 2$ temos que $ax^3 + by^3$ representa ao menos $(2.2-1)\frac{(p-1)}{(p-1,3)} + 1 = 3.\frac{p-1}{3} + 1 = p$ restos módulo p, incluindo o zero. Note que $mdc(p-1,3) = 3$, pois $p \equiv 1 \pmod 3$. Daí, em particular, $ax^3 + by^3 \equiv c \pmod p$ possui solução. □

Lema 3.7 *Se* $p \equiv 1 \pmod 3$, $p > 7$ *e* $ab \not\equiv 0 \pmod p$, *a congruência*

$$ax^3 + by^3 + z^3 \equiv 0 \pmod p$$

sempre é solúvel com $xy \not\equiv 0 \pmod p$.

Prova. Suponha que a e b são ambos cubos módulo p. Assim, faça $a = \alpha^3$ e $b = \beta^3$. Logo, temos que $(1, -\alpha\beta^{-1}, 0)$ é solução da congruência acima.

Agora, suponha que b não é um cubo. Façamos $y \equiv -1$ e, usando o Lema 3.6, concluímos que a congruência

$$ax^3 + z^3 \equiv b \pmod p$$

possui solução. Veja que, caso $x \equiv 0$ então b seria um cubo. Contradição! Daí, $xy \not\equiv 0$. □

O próximo Lema é um caso particular do Teorema de Chevalley (ver capítulo 1).

Lema 3.8 *O sistema*

$$\begin{cases} a_1x_1^3 + \ldots + a_nx_n^3 \equiv 0 \pmod p \\ b_1x_1^3 + \ldots + b_nx_n^3 \equiv 0 \pmod p \\ c_1x_1^3 + \ldots + c_nx_n^3 \equiv 0 \pmod p \end{cases}$$

tem uma solução não trivial se $n > 9$.

Lema 3.9 *Considere as formas*

$$\begin{cases} f = a_1z_1^3 + a_2z_2^3 + a_3z_3^3 + z_4^3 \\ g = b_1z_1^3 + b_2z_2^3 + b_3z_3^3 + z_5^3 \end{cases}$$

onde cada variável está explicita em ao menos uma das formas f *e* g *e onde toda combinação linear não trivial destas duas formas tem ao menos posto dois módulo* p. *Sejam* a *e* b *inteiros, não nulos módulo* p, *simultaneamente, então as congruências*

$$\begin{cases} f \equiv a \pmod p \\ g \equiv b \pmod p \end{cases}$$

tem uma solução em comum com ao menos duas das variáveis $z_1, \ldots, z_5$ *não nulas módulo* p.

Prova. É suficiente resolver o sistema homogêneo

$$\begin{cases} a_1z_1^3 + a_2z_2^3 + a_3z_3^3 \quad + z_4^3 \qquad\quad + az^3 \equiv 0 \pmod{p} \\ b_1z_1^3 + b_2z_2^3 + b_3z_3^3 \qquad\quad + z_5^3 \quad + bz^3 \equiv 0 \pmod{p} \end{cases} \tag{3-4}$$

com $z \not\equiv 0$ e com duas outras variáveis não nulas módulo p.

Seja S o posto mínimo de alguma combinação linear não trivial módulo p das formas em (3-4). Por hipótese, $S \geq 2$. Substitua as formas em (3-4) por formas equivalentes f' e g', onde

$$f' = \alpha_2z_2^3 + \ldots + \alpha_4z_4^3 + z_5^3 + \alpha z^3$$

e onde g' tem posto S, isto é, onde g' possui apenas S variáveis explícitas. Podemos dizer que z_1 está em g' e portanto tal variável pode ser eliminada de f'.

Assim, demonstremos o lema para cada valor de S.

Se $S = 2$ podemos assumir, sem perda de generalidade, que

$$g' = z_1^3 + \beta_2z_2^3. \qquad \textit{(caso I)}$$

Para resolver $f' \equiv g' \equiv 0 \pmod{p}$, façamos $z_1 \equiv z_2 \equiv 0$. Daí a equação $f' \equiv 0 \pmod{p}$ torna-se

$$\alpha_3z_3^3 + \alpha_4z_4^3 + z_5^3 + \alpha z^3 \equiv 0 \pmod{p},$$

onde $\alpha_3\alpha_4\alpha \not\equiv 0 \pmod{p}$. Tomemos z_5, $z \not\equiv 0$ tal que

$$z_5^3 + \alpha z^3 \equiv -\delta \not\equiv 0 \pmod{p}.$$

Conseqüentemente, pelo Lema 3.6, a congruência

$$\alpha_3z_3^3 + \alpha_4z_4^3 \equiv \delta \pmod{p}$$

tem solução. Podemos garantir que z_3 ou $z_4 \not\equiv 0$, pois $\delta \not\equiv 0$. Assim, z e duas outras variáveis não são congruentes a zero.

Se $S = 3$, temos dois casos e podemos fazer

$$g' = z_1^3 + \beta_2z_2^3 + \beta z^3 \qquad \textit{(caso II)}$$

ou

$$g' = z_1^3 + \beta_2z_2^3 + \beta_3z_3^3. \qquad \textit{(caso III)}$$

Em qualquer caso, podemos usar o Lema 3.7 para resolver $g' \equiv 0 \pmod{p}$ com duas ou

três variáveis não congruentes a zero, incluindo z no *caso II*, pois $z \not\equiv 0$ por hipótese. A equação $f' \equiv 0 \pmod{p}$ torna-se uma equação, possivelmente não homogênea, de três variáveis. No *caso II*, podemos usar o Lema 3.3 ou 3.4 para resolvê-la, com ao menos uma variável não nula módulo p. No *caso III*, façamos $z \equiv 1$ e, usando o Lema 3.6, concluímos que a equação tem solução.

Suponha que $S = 4$. Assim, ou

$$g' = z_1^3 + \beta_2 z_2^3 + \beta_3 z_3^3 + \beta z^3 \qquad \textit{(caso IV)}$$

ou

$$g' = z_1^3 + \beta_2 z_2^3 + \beta_3 z_3^3 + \beta_4 z_4^3 \qquad \textit{(caso V)}.$$

No *caso IV*, vamos resolver $g' \equiv 0 \pmod{p}$ escolhendo z_3, $z \not\equiv 0$, de modo que $\beta_3 z_3^3 + \beta z^3 \not\equiv 0$. Façamos $\beta_3 z_3^3 + \beta z^3 \equiv -\phi$. Agora temos que a equação resultante, com as variáveis z_1 e z_2, tem solução, basta usarmos o Lema 3.6.

Assim, a equação $f' \equiv 0 \pmod{p}$ torna-se uma equação, possivelmente não homogênea, de duas variáveis (z_4 e z_5). Se tal equação é homogênea, façamos $z_4 \equiv z_5 \equiv 0$. Caso contrário, podemos concluir que ela é solúvel pelo Lema 3.6.

Para resolver $g' \equiv 0 \pmod{p}$, considerando o *caso V*, vamos escolher representantes A e B para as duas classes de restos não cúbicos módulo p tal que

$$1 + A + B \equiv 0 \pmod{p}.$$

Isto é possível, pois se A_0 e B_0 são representantes arbitrários, o Lema 3.4 diz que a congruência

$$x^3 + A_0 y^3 + B_0 z^3 \equiv 0 \pmod{p}$$

tem uma solução não trivial. Como A_0, B_0 e $A_0 B_0^{-1}$ não são cubos módulo p, esta solução satisfaz a última equação com $xyz \not\equiv 0$. Assim, podemos tomar $A = A_0 y^3 x^{-3}$ e $B = B_0 z^3 x^{-3}$. Sem perda de generalidade, podemos assumir que os coeficientes não nulos de g' são restritos aos valores 1, *A e B*.

Daí, um dos quatro coeficientes não nulos de g' – 1, β_2, β_3 e β_4 – é repetido. Digamos $\beta_i \equiv \beta_j$, onde algum β pode ser 1, o coeficiente de z_1^3. Resolvamos $g' \equiv 0 \pmod{p}$ fazendo $\xi \equiv z_i \equiv -z_j$ e as duas variáveis restantes congruentes a zero. A equação $f' \equiv 0 \pmod{p}$ passa a ter a forma

$$z_5^3 + \alpha' \xi^3 + \alpha z^3 \equiv 0 \pmod{p},$$

onde $\alpha' \not\equiv 0 \pmod{p}$. Pelo Lema 3.7, esta última congruência é solúvel, com $\xi z \not\equiv 0$ (e daí temos que $z_i z_j z \not\equiv 0$).

Finalmente, suporemos $S = 5$. Então podemos assumir

$$g' = z_1^3 + \beta_2 z_2^3 + \beta_3 z_3^3 + \beta_4 z_4^3 + \beta_5 z_5^3. \qquad \textit{(caso VI)}$$

Como anteriormente, vamos resolver a congruência $g' \equiv 0 \pmod{p}$ assumindo que os cinco coeficientes não nulos de g' estão restritos aos valores 1, A *e* B. Primeiro suponha que existem dois pares de coeficientes congruentes: digamos, $\beta_i \equiv \beta_j$ e $\beta_k \equiv \beta_l$. Façamos ainda $\xi \equiv z_i \equiv -z_j$, $\eta \equiv z_k \equiv -z_l$ e a variável restante congruente a zero. A equação $f' \equiv 0 \pmod{p}$ passa a ter a forma

$$\alpha'\xi^3 + \alpha''\eta^3 + \alpha z^3 \equiv 0 \pmod{p}, \tag{3-5}$$

onde $\alpha'\alpha'' \not\equiv 0$, caso contrário estaríamos em um dos casos anteriores. Note que neste caso $\alpha_2\alpha_3\alpha_4 \not\equiv 0$. Pelo Lema 3.7 temos que (3-5) possui solução com $\eta z \not\equiv 0$ e, conseqüentemente, $z_k z_l z \not\equiv 0$.

Se não existem dois pares de coeficientes congruentes em g' então as possibilidades para os coeficientes, com excessão de permutações, são :

$$\begin{array}{lccccc} (i) & 1 & A & A & A & B, \\ (ii) & 1 & B & B & B & A, \\ (iii) & B & 1 & 1 & 1 & A. \end{array}$$

Suponha que em cada caso para a forma de g', os coeficientes estejam dispostos nesta ordem, do primeiro ao quinto. Se não estiver, basta renumerar convenientemente as variáveis. Se $\alpha_4 \not\equiv -1 \pmod{p}$, podemos resolver $g' \equiv 0 \pmod{p}$ com $\xi \equiv z_2 \equiv -z_3$ e $\eta \equiv z_1 \equiv z_4 \equiv z_5$. Mas, caso $\alpha_4 \equiv -1 \pmod{p}$, então necessariamente $\alpha_3 \not\equiv -1 \pmod{p}$, pois senão estaríamos em um caso anterior com $S = 3$. Neste caso, resolveremos $g' \equiv 0 \pmod{p}$ com $\xi \equiv z_2 \equiv -z_4$ e $\eta \equiv z_1 \equiv z_3 \equiv z_5$. Para os dois casos, $f' \equiv 0 \pmod{p}$ passa a ter a forma (3-5). Sendo $\eta z \not\equiv 0$, basta usarmos o Lema 3.7 novamente. Isto completa a prova deste lema. □

Lema 3.10 *Um sistema da forma*

$$\begin{cases} x_1^3 + d_2 x_2^3 + & a_1 w_1^3 + \ldots + a_6 w_6^3 & & & \equiv 0 & \pmod{p}, \\ & b_1 w_1^3 + \ldots + b_6 w_6^3 & + y^3 & & \equiv 0 & \pmod{p}, \\ & c_1 w_1^3 + \ldots + c_6 w_6^3 & & + z^3 & \equiv 0 & \pmod{p}, \end{cases}$$

onde $d_2 \not\equiv 0$ *e algum* $a_i \not\equiv 0$*, tem uma solução não singular.*

Prova. Digamos que $a_1 \not\equiv 0$. Façamos $w_1yz \not\equiv 0$ tal que $b_1w_1^3 + y^3$ e $c_1w_1^3 + z^3$ são ambos não congruentes a zero. A segunda e a terceira equações passam a ter a forma daquelas equações do Lema 3.9 com as variáveis $w_2, ..., w_6$, que possui solução. Daí, a primeira equação torna-se uma equação de x_1 e x_2, que é solúvel. De fato, basta usar o Lema 3.6 se a equação não for homogênea ou $x_1 \equiv x_2 \equiv 0$ se a equação obtida for homogênea. Note que

$$Det \begin{pmatrix} a_1w_1 & 0 & 0 \\ b_1w_1 & y & 0 \\ c_1w_1 & 0 & z \end{pmatrix} = a_1w_1yz \not\equiv 0.$$

Portanto, a solução encontrada é não singular. □

3.2 Demonstração do Teorema 2

Nesta seção provaremos o Lema 3.1 considerando as cinco possibilidades para R, o número mínimo de variáveis em alguma combinação linear das formas f, g, h, como mencionado no início do capítulo.

Lema 3.11 *Suponha que $p \neq 3$ ou 7. Se $R = 4$ então as congruências*

$$f \equiv g \equiv h \equiv 0 \pmod{p} \tag{3-6}$$

tem uma solução não singular.

Prova. Podemos assumir que o sistema é

$$\begin{cases} a_1x_1^3 + ... + a_4x_4^3 + & a_5x_5^3 + ... + a_7x_7^3 & +x_8^3 & & & \equiv 0 \pmod{p} \\ b_1x_1^3 + ... + b_4x_4^3 + & b_5x_5^3 + ... + b_7x_7^3 & & +x_9^3 & & \equiv 0 \pmod{p} \\ & c_5x_5^3 + ... + c_7x_7^3 & & & +x_{10}^3 & \equiv 0 \pmod{p} \end{cases} \tag{3-7}$$

onde $c_i \not\equiv 0$, $i \in \{5,\ 6,\ 7\}$, e onde podemos assumir $a_ib_i \not\equiv 0$, para $i \in \{1,\ 2,\ 3,\ 4\}$, caso contrário (3-7) terá a forma do sistema no Lema 3.10 e daí já teria uma solução não singular.

Como na prova do Lema 3.9, podemos assumir que o c_i está restrito aos valores 1, A e B. Daí, existe um par de coeficientes congruentes no conjunto dos coeficientes de h. Digamos que $c_i \equiv c_j$, onde algum c pode ser 1, o coeficiente de x_{10}^3. Faça $\xi \equiv x_i \equiv -x_j$ e faça as duas variáveis restantes congruentes a zero. O sistema (3-7) passa a ser

$$\begin{cases} a_1x_1^3 + ... + a_4x_4^3 + a\xi^3 & +x_8^3 & & \equiv 0 \pmod{p}, \\ b_1x_1^3 + ... + b_4x_4^3 + b\xi^3 & & +x_9^3 & \equiv 0 \pmod{p}. \end{cases}$$

Agora seja $\xi \equiv 1$ e escolha $x_8 \not\equiv 0$ tal que $a + x_8^3 \equiv -\alpha \not\equiv 0$. Assim as equações anteriores passam a ter a forma

$$\begin{cases} a_1x_1^3 + \ldots + a_4x_4^3 & \equiv \alpha \pmod{p}, \\ b_1x_1^3 + \ldots + b_4x_4^3 + x_9^3 & \equiv \beta \pmod{p}, \end{cases}$$

onde α e β não são ambos congruentes a zero. Estas equações são equivalentes módulo p àquelas que ocorrem no Lema 3.9. Logo, elas possuem uma solução em comum, com algum $x_i \not\equiv 0$, $i \in \{1, \ldots, 4\}$. Concluímos então que (3-7) possui uma solução não singular, onde a não-singularidade existe por causa das variáveis ξ, x_8 e x_i, com $i \in \{1, \ldots, 4, \}$, pois $b_i \not\equiv 0$. □

Lema 3.12 *Suponha que $p \neq 3$ ou 7. Se $R = 5$ então as congruências (3-6) tem uma solução não singular.*

Prova. Podemos assumir que o sistema é

$$\begin{cases} a_1x_1^3 + \ldots + a_3x_3^3 + & a_4x_4^3 + \ldots + a_7x_7^3 & + x_8^3 & & & \equiv 0 \pmod{p} \\ b_1x_1^3 + \ldots + b_3x_3^3 + & b_4x_4^3 + \ldots + b_7x_7^3 & & + x_9^3 & & \equiv 0 \pmod{p} \\ & c_4x_4^3 + \ldots + c_7x_7^3 & & & + x_{10}^3 & \equiv 0 \pmod{p} \end{cases} \tag{3-8}$$

onde $c_i \not\equiv 0$, $i \in \{4, \ldots, 7\}$ e onde podemos assumir que $a_ib_i \not\equiv 0$, com $i \in \{1, 2, 3\}$, como no Lema 3.11. Assim como na prova do caso VI do Lema 3.9, podemos resolver $h \equiv 0 \pmod{p}$ com duas variáveis ξ e η. Reescrevendo o sistema temos

$$\begin{cases} a_1x_1^3 + \ldots + a_3x_3^3 + a\xi^3 + a'\eta^3 & + x_8^3 & & \equiv 0 \pmod{p} \\ b_1x_1^3 + \ldots + b_3x_3^3 + b\xi^3 + b'\eta^3 & & + x_9^3 & \equiv 0 \pmod{p} \end{cases}$$

onde podemos assumir que a variável ξ está explícita no sistema. Se não estivesse o sistema seria equivalente módulo p a um sistema do tipo do Lema 3.10 e portanto teria uma solução não singular.

Considere $\eta \equiv 1$ e escolha $x_8 \not\equiv 0$ tal que $a' + x_8^3 \equiv -\alpha \not\equiv 0$. O sistema passa a ser

$$\begin{cases} a_1x_1^3 + \ldots + a_3x_3^3 + a\xi^3 & & \equiv \alpha \pmod{p} \\ b_1x_1^3 + \ldots + b_3x_3^3 + b\xi^3 & + x_9^3 & \equiv \beta \pmod{p}. \end{cases}$$

Este sistema é equivalente módulo p a um sistema do tipo do Lema 3.9. Portanto, ele tem uma solução com $x_i \not\equiv 0$ para $i \in \{1, 2, 3, 9\}$. Consequentemente, (3-8) possui solução não singular, onde a não-singularidade existe pelas variáveis η, x_8 e x_i para $i \in \{1, 2, 3, 9\}$, pois $b_i \not\equiv 0$.

□

Lema 3.13 *Suponha que $p \neq 3$ ou 7. Se $R = 6$ então as congruências (3-6) tem uma solução não singular.*

*Prova.*Podemos assumir que o sistema é

$$\begin{cases} a_1x_1^3 + a_2x_2^3 + \quad a_3x_3^3 + \ldots + a_7x_7^3 \quad + x_8^3 \qquad\qquad\quad \equiv 0 \pmod{p} \\ b_1x_1^3 + b_2x_2^3 + \quad b_3x_3^3 + \ldots + b_7x_7^3 \qquad + x_9^3 \qquad\quad \equiv 0 \pmod{p} \\ \qquad\qquad\quad c_3x_3^3 + \ldots + c_7x_7^3 \qquad\qquad + x_{10}^3 \equiv 0 \pmod{p} \end{cases} \tag{3-9}$$

onde $c_i \not\equiv 0$, $i \in \{3, \ldots, 7\}$, e onde $a_ib_i \not\equiv 0$, para $i = 1,\ 2$, como na prova do Lema 3.11. Vamos resolver $h \equiv 0 \pmod{p}$ com duas variáveis ξ e η assumindo que c_i está restrito aos valores 1, A e B. Logo, existem ao menos dois pares de coeficientes congruentes no conjunto $\{c_3, \ldots, c_7,\ 1\}$. Digamos $c_i \equiv c_j$ e $c_k \equiv c_l$, onde algum c pode ser 1, o coeficiente de x_{10}^3. Seja $\xi \equiv x_i \equiv -x_j$, $\eta \equiv x_k \equiv -x_l$ e faça o restante das variáveis de h congruentes a zero. O sistema (3-9) passa a ser

$$\begin{cases} a_1x_1^3 + a_2x_2^3 + a\xi^3 + a'\eta^3 \quad + x_8^3 \qquad \equiv 0 \pmod{p}, \\ b_1x_1^3 + b_2x_2^3 + b\xi^3 + b'\eta^3 \qquad + x_9^3 \equiv 0 \pmod{p}, \end{cases} \tag{3-10}$$

onde podemos assumir que as variáveis ξ e η estão explicitas no sistema, pois, de outro modo, o sistema seria equivalente módulo p a um sistema do tipo do Lema 3.10 e assim já teria uma solução não singular.

Agora, faça $\eta \equiv 1$. O sistema anterior passa ter a forma de um sistema equivalente módulo p ao sistema do Lema 3.9. Assim, ele tem uma solução com ao menos duas variáveis não congruentes a zero. Se $\xi \not\equiv 0$, esta solução de (3-9) tem ao menos cinco variáveis não nulas módulo p – x_i, x_j, x_k, x_l e outra variável de (3-10), garantida pelo Lema 3.9). Se esta solução fosse singular, então poderíamos formar uma combinação linear módulo p não trivial de f, g e h de posto menor que 6. Assim, (3-9) seria equivalente módulo p a um sistema com $R \leq 5$, uma contradição pois $R = 6$. Portanto, uma solução para (3-10) com $\xi \not\equiv 0$ só pode ser não singular. Se $\xi \equiv 0$, então $x_8,\ x_9 \not\equiv 0$ ou $x_8,\ x_i \not\equiv 0$ ou $x_9,\ x_i \not\equiv 0$ ou $x_1,\ x_2 \not\equiv 0$. Em cada um dos casos, a solução de (3-9) é não singular, pois, de outro modo, o sistema seria equivalente módulo p a um sistema como o do Lema 3.10. □

Lema 3.14 *Suponha que $p \neq 3$ ou 7. Se $R = 7$, então as congruências (3.7) tem uma solução não singular.*

Prova.Podemos assumir que o sistema é

$$\begin{cases} a_1x_1^3 & +a_2x_2^3+\ldots+a_7x_7^3 & +x_8^3 & & & \equiv 0 \pmod{p} \\ b_1x_1^3 & +b_2x_2^3+\ldots+b_7x_7^3 & & +x_9^3 & & \equiv 0 \pmod{p} \\ & c_2x_2^3+\ldots+c_7x_7^3 & & & +x_{10}^3 & \equiv 0 \pmod{p} \end{cases} \tag{3-11}$$

onde $c_i \not\equiv 0$, onde $i = 2, \ldots, 7$, e $a_1b_1 \not\equiv 0$.

Como nas provas dos lemas anteriores iremos assumir que os coeficientes da forma h são 1, A ou B. Como há sete coeficientes nesta forma, teremos a possibilidade de termos três pares de coeficientes congruentes e as seguintes possibilidades para $c_2, \ldots, c_7$, desconsiderando as permutações:

$$\begin{array}{cccccccc} (i) & A, & A, & A, & B, & B, & B; \\ (ii) & A, & 1, & 1, & B, & B, & B; \\ (iii) & B, & 1, & 1, & A, & A, & A; \\ (iv) & B, & A, & A, & A, & A, & A; \\ (v) & A, & B, & B, & B, & B, & B; \\ (vi) & A, & 1, & 1, & B, & 1, & 1. \end{array}$$

Suponha inicialmente que existam três pares de coeficientes congruentes no conjunto $\{c_2, \ldots, c_7, 1\}$. Digamos $c_i \equiv c_j$, $c_k \equiv c_l$ e $c_m \equiv c_n$, onde algum dos c's pode ser 1, o coeficiente de x_{10}^3. Para resolver $h \equiv 0 \pmod{p}$, façamos $\xi \equiv x_i \equiv -x_j$, $\eta \equiv x_k \equiv -x_l$, $\nu \equiv x_m \equiv -x_n$ e a variável restante faça ser congruente a zero.

Se não existem três pares de coeficientes congruentes, então considere os casos de (i) a (vi), citados anteriormente, na ordem em que estão dispostos.

Nos casos de (i) até (v), note que se $a_5 \equiv a_6$ e $b_5 \equiv b_6$ teríamos a quinta e sexta coluna linearmente dependentes, voltando assim em um tipo de sistema já estudado. Logo, podemos assumir que as congruências $a_5 \equiv a_6$ e $b_5 \equiv b_6$ não são satisfeitas ao mesmo tempo. Suponha que $a_2 \not\equiv -a_5$ ou $b_2 \not\equiv -b_5$. Resolvamos $h \equiv 0 \pmod{p}$ fazendo

$$\xi \equiv x_3 \equiv -x_4, \eta \equiv x_6 \equiv -x_7 \text{ e } \nu \equiv x_2 \equiv x_5 \equiv x_{10}.$$

Caso contrário, se $a_2 \equiv -a_5$ e $b_2 \equiv -b_5$ teremos $a_2 \not\equiv -a_6$ ou $b_2 \not\equiv -b_6$ e podemos resolver $h \equiv 0 \pmod{p}$ fazendo

$$\xi \equiv x_3 \equiv -x_4, \eta \equiv x_5 \equiv -x_7 \text{ e } \nu \equiv x_2 \equiv x_6 \equiv x_{10}.$$

No caso (vi), $h \equiv 0 \pmod{p}$ pode ser resolvido de maneira semelhante, como por exemplo, fazendo

$$\xi \equiv x_3 \equiv -x_4, \eta \equiv x_6 \equiv -x_7, \nu \equiv x_2 \equiv x_5 \equiv x_{10}.$$

Com cada uma das escolhas anteriores para ξ, η e ν, o sistema (3-11) passa a ser

$$\begin{cases} a_1x_1^3 + a\xi^3 + a'\eta^3 + a''\nu^3 \quad + x_8^3 \quad\quad\quad \equiv 0 \pmod{p}, \\ b_1x_1^3 + b\xi^3 + b'\eta^3 + b''\nu^3 \quad\quad\quad + x_9^3 \equiv 0 \pmod{p}, \end{cases}$$

onde as variáveis ξ, η e ν estão explícitas no novo sistema, pela maneira que elas foram escolhidas. Seja $\xi \equiv 1$. O sistema anterior passa a ter a forma de um sistema equivalente módulo p ao do Lema 3.9. Assim, existe uma solução com ao menos duas das variáveis não nulas módulo p. Se esta solução fosse singular, poderíamos formar uma combinação linear módulo p não trivial de f, g e h de posto menor do que sete, uma contradição. Daí existe uma solução não singular para (3-11).

□

Lema 3.15 *Suponha que $p \neq 3$ ou 7. Se $R = 8$, então as congruências (3.7) tem uma solução não singular.*

Prova. Podemos assumir que o sistema é

$$\begin{cases} a_1x_1^3 + \ldots + a_7x_7^3 \quad + x_8^3 \quad\quad\quad\quad \equiv 0 \pmod{p} \\ b_1x_1^3 + \ldots + b_7x_7^3 \quad\quad + x_9^3 \quad\quad \equiv 0 \pmod{p} \\ c_1x_1^3 + \ldots + c_7x_7^3 \quad\quad\quad + x_{10}^3 \equiv 0 \pmod{p} \end{cases} \tag{3-12}$$

onde $c_i \not\equiv 0$, onde $i \in \{1, \ldots, 7\}$. Pelo Lema 3.8, existe uma solução não trivial para (3-12). Se nesta solução há exatamente duas variáveis que não são nulas módulo p, podemos fazer (3-12) ser equivalente módulo p a um sistema do tipo do Lema 3.10 e daí concluirmos que o sistema possui uma solução não singular. Se três ou mais variáveis na solução não são congruentes a zero, então necessariamente, ela é não singular, caso contrário existiria uma combinação linear módulo p não trivial de f, g e h de posto menor do que oito, o que seria uma contradição. □

Lema 3.1 *Se F, G, H é um trio de formas p-normalizadas com $n \geq 28$ variáveis e $p \neq 3$ ou 7, então as congruências*

$$F \equiv G \equiv H \equiv 0 \pmod{p}$$

tem uma solução não singular.

Prova. A conclusão segue dos Lemas 3.11 a 3.15. □

Enfim podemos demonstrar o Teorema 2.

Teorema 2 *Três equações com n variáveis como em (3-1) tem solução não trivial em comum, nos inteiros p-ádicos, se* $n \geq 28$ *e* $p \neq 3$ *ou 7.*

Prova. Se $\vartheta(F,\ G,\ H) \neq 0$, basta aplicarmos então o Lema de Hensel e o Lema 3.1 (se $\vartheta(F,\ G,\ H) = 0$, segue como no Capítulo 1). □

Apêndice

Lema 2.4 *Seja p um primo e*

$$F(x_1,...,x_m) = a_1x_1^k + ... + a_mx_m^k,$$

onde k divide $p-1$ e onde $a_1...a_m \not\equiv 0 \ (mod\ p)$. Então, se $m \leq k$, o número de classes de restos $(mod\ p)$ distintas, diferentes de zero, representadas por F é ao menos $m(p-1)/k$.
*Prova.*O número de classes de restos distintas, incluindo o zero, representada por $a_ix_i^k$ é $1+(p-1)/k$. Pelo Teorema de Cauchy-Davenport (ver [6]), na adição das classes de restos $(mod\ p)$, o número de classes distintas representadas por $a_1x_1^k + a_2x_2^k$ é ao menos $2[1+(p-1)/k]-1 = 1+2(p-1)/k$. Logo, o número de classes distintas representadas por F é ao menos $1+m(p-1)/k$, onde uma destas é a classe 0. □

Lema 2.5 *Seja p um primo e k um fator de $p-1$. Sejam G,H formas aditivas de grau k em $y_1,...,y_s$, onde $s > k$. Sejam $\gamma_1,...,\gamma\mu$ classes de restos $(mod\ p)$ não nulas, onde*

$$\mu > (p-1)(2k-s)/k.$$

Então existem $y_1,...,y_s$, nem todos $\equiv 0$, tais que,

$$G(y_1,...,y_s) \equiv 0 \ (mod\ p)$$

e

$$H(y_1,...,y_s) \equiv 0 \ ou\ \gamma_i \ (mod\ p)$$

para algum i.
Prova. Seja $\beta_1,...,\beta_\rho$ classes de restos não nulas diferentes de $\gamma_1,...,\gamma\mu$. Então

$$\rho = p-1-\mu < (p-1)(s-k)/k.$$

Considere o polinômio

$$(1-G^{p-1})\prod_{i=1}^{\rho}(\beta_i - H) - \beta_1...\beta_\rho(1-y_1^{p-1})...(1-y_s^{p-1}).$$

Este polinômio contém o termo

$$\pm\beta_1 ... \beta_\rho y_1^{p-1} ... y_s^{p-1},$$

de grau total $s(p-1)$ e, todos os outros termos tem grau menor, já que o grau da primeira parte do polinômio é

$$(p-1)k + \rho k < s(p-1).$$

Pelo princípio usado na prova do Lema 2.4, o polinômio não poderá ser $\equiv 0$ para todos os valores de $y_1, ..., y_s$. Ele será $\equiv 0$ se $y_1, ..., y_s$ forem todos 0, desde então $G \equiv H \equiv 0 \pmod{p}$. Daí, que existam $y_1, ..., y_s$, não todos $\equiv 0$, tais que

$$G \equiv 0 \ (mod\ p) \text{ e } H \not\equiv \beta_i \ (mod\ p)$$

para todo i. Esta última sentença implica que $H \equiv 0$ ou $H \equiv \gamma_j$ para algum j. Isto prova o lema. □

Referências Bibliográficas

[1] BIRCH, B. J., LEWIS, D. J., MURPHY, T. G., *Simultaneous quadratic forms*, Amer. J. Math. 84 (1962), 110-115.

[2] BOREVICH, Z. I., SHAFAREVICH, I. R., *Number theory*, Academic Press, New York, (1966).

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

[4] BRÜDERN, J., GODINHO, H., *On Artin's conjecture I: systems of diagonal forms*, Bull. London Math. Soc. 31 (1999), 305-313.

[5] BRÜDERN, J., GODINHO, H., *On Artin's conjecture II: pairs of additive forms*, Proc. London Math. Soc. (3) 84 (2002), 305-313.

[6] CHOWLA, S., MANN, H. B. & STRAUS, E. G., *Some applications of the Cauchy-Davenport theorem*, Kongelige Norske Videnskabers Selskabs Forhandlinger Bind 32 (1959), Nr 13.

[7] DAVENPORT, H., LEWIS, D. J., *Homogêneous additive equations*, Proc. Roy. Soc. London, Ser. A, 274 (1963), 443-460.

[8] DAVENPORT, H., LEWIS, D. J., *Notes on congruences III*, Quart. J. Math. Oxford, Ser. (2), 17 (1996), 339-344.

[9] DAVENPORT, H., LEWIS, D. J., *Simultaneous equations of additive type*, Philos. Trans. Roy. Soc. London Ser. A 264 (1969), 557-595.

[10] DAVENPORT, H., LEWIS, D. J., *Two Additive Equations*, Proceedings Symposia in Pure Math., 12 (Houston, 1967), 74-98.

[11] GODINHO, H., *Polinômios Homogêneos sobre Números p-Ádicos*, Universidade de Lisboa, MAT-UL-2000-01.

[12] GODINHO, H., LIMA NETO, J. F., RODRIGUES, P. H. A., *On pairs of additive congruences of odd degrees*, JP J. Algebra Number Theory Appl., 4(1) (2004), 55-78.

[13] GODINHO, H., SHOKRANIAN, S., SOARES, M., *Teoria dos números*, Editora Univeridade de Brasília, 1994.

[14] KNAPP, M., *Systems of diagonal equation over p-adic fields*, J. London Math. Soc. (2) 63 (2001) 257-267.

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

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

[17] LOW, L., PITMAN, J., WOLFF, A., *Simultaneous diagonal congruences*, J. Number Theory 29 (1988) 31-59.

[18] NOVAIS, MARCELO SANTOS, *Sistemas de equações diagonais sobre corpos p-ádicos*, Dissertação de Mestrado, Universidade de Brasília (2003).

[19] STEVENSON, EDIE, *The Artin Conjecture for Three Diagonal Cubic Forms* J. Number Theory 14 (1982), p. 374-390.

[20] TERJANIAN, G., *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris, 262 (1996), 612.

Livros Grátis

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

Milhares de Livros para Download:

Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas

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