UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

JEAN CARLOS A. LELIS

Uma Confirmação da Conjectura de Artin para Pares de Formas Diagonais de Graus 2 e 3.

Goiânia
2015

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR AS TESES E DISSERTAÇÕES ELETRÔNICAS (TEDE) NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1 **1. Identificação do material bibliográfico**: **[X] Dissertação** **[ ] Tese**

1 **2. Identificação da Tese ou Dissertação**

Autor (a):	Jean Carlos de Aguiar Lelis				
E-mail:	Jeanlelis.math@gmail.com				
Seu e-mail pode ser disponibilizado na página? [X]Sim [ ] Não					
Vínculo empregatício do autor	Aluno de Pós-Graduação				
Agência de fomento:	Coordenação de aperfeiçoamento de pessoal de nível superior			Sigla:	CAPES
País:	Brasil	UF:	GO	CNPJ:	
Título:	Uma Confirmação da Conjectura de Artin para Pares de Formas Diagonais de Graus 2 e 3.				
Palavras-chave:	Conjectura de Artin, pares de formas aditivas, números p-ádicos, p-normalização de sistemas de formas aditivas.				
Título em outra língua:					
Palavras-chave em outra língua:					
Área de concentração:	Álgebra				
Data defesa: (dd/mm/aaaa)	14/112015				
Programa de Pós-Graduação:	Programa de Pós-Graduação em Matemática				
Orientador (a):	Paulo Henrique de Azevedo Rodrigues				
E-mail:	paulo.mat.ufg@gmail.com				
Co-orientador(a):*					
E-mail:					

*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC da tese ou dissertação.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses e ou dissertações, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.

_____ Data: _____ / _____ / _____

Assinatura do (a) autor (a)

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

JEAN CARLOS A. LELIS

Uma Confirmação da Conjectura de Artin para Pares de Formas Diagonais de Graus 2 e 3.

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: Teoria do Números.

Orientador: Prof. Paulo Henrique A. Rodrigues

Goiânia
2015

Ficha catalográfica elaborada automaticamente
com os dados fornecidos pelo(a) autor(a), sob orientação do Sibi/UFG.

Lelis, Jean Carlos de Aguiar
Uma Confirmação da Conjectura de Artin para Pares de Formas Diagonais de Graus 2 e 3 [manuscrito] / Jean Carlos de Aguiar Lelis. - 2015.
83 f.

Orientador: Prof. Dr. Paulo Henrique de Azevedo Rodrigues.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME) , Programa de Pós-Graduação em Matemática, Goiânia, 2015.
Bibliografia. Apêndice.

1. Conjectura de Artin. 2. pares de formas aditivas. 3. números p ádicos. 4. p-normalização de sistemas de formas aditivas. I. Rodrigues, Paulo Henrique de Azevedo, orient. II. Título.

JEAN CARLOS DE AGUIAR LELIS

UMA CONFIRMAÇÃO DA CONJECTURA DE ARTIN PARA PARES DE FORMAS DIAGONAIS DE GRAUS 2 E 3

Dissertação defendida no Programa de Pós-Graduação do Instituto de Matemática e Estatística da Universidade Federal de Goiás como requisito parcial para obtenção do título de Mestre em Matemática, aprovada no dia 10 de novembro de 2015, pela Banca Examinadora constituída pelos professores:

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

Prof. Dr. Hemar Teixeira Godinho
Departamento de Matemática - UnB

Profa. Dra. Ana Paula de Araujo Chaves
Instituto de Matemática e Estatística - UFG

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador(a).

Jean Carlos A. Lelis

Bacharel em Matemática pela Universidade Federal de Goiás - UFG.

A meus pais e minha namorada Anna.

Agradecimentos

A meus pais e minhas irmãs pelo suporte familiar que sempre tive, e por serem os primeiros a acreditarem em mim.

A minha namorada Anna pelo companheirismo, cumplicidade e carinho que sempre teve comigo.

A meus colegas de graduação e mestrado que me apoiaram nesses anos de muito estudo; juntos tivemos momentos difíceis, mas também realizações.

A meu orientador de mestrado, prof. Dr. Paulo Henrique de Azevedo Rodrigues, por me aceitar como orientando, e acreditar em mim; terei como objetivo maior na minha carreira acadêmica corresponder a confiança que depositou em mim.

Aos prof. Dr. Jhone Caldeira e prof. Dr. Walterson, por superarem todas as expectativas que eu tinha com o curso de Matemática ainda no meu primeiro semestre de graduação.

A Olimpíada Brasileira de Matemática das Escolas Publica (OBMEP), especialmente na pessoa do prof. Dr. José Hilário da Cruz, por criar novos horizontes na minha vida.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro.

"Minha mente está aberta."

Paul Erdös.

Resumo

Lelis, Jean Carlos. **Uma Confirmação da Conjectura de Artin para Pares de Formas Diagonais de Graus 2 e 3.** . Goiânia, 2015. 83p. Dissertação de Mestrado. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

Nesse trabalho, nós apresentamos alguns dos métodos usados no estudo de formas aditivas sobre corpos locais, e uma prova para um caso particular da Conjectura de Artin, que afirma que todo sistema de R formas aditivas de graus $k_1, k_2, ..., k_R$ possui solução p-ádica não trivial para todo p primo, se o número s de variáveis for maior que $k_1^2 + k_2^2 + \cdots + k_R^2$, dada por Wooley [12], onde ele mostra que $\Gamma(3,2) = 11$.

Palavras–chave

Conjectura de Artin, pares de formas aditivas, números p-ádicos, p-normalização de sistemas de formas aditivas.

Abstract

Lelis, Jean Carlos. **titulo em inglês**. Goiânia, 2015. 83p. MSc. Dissertation. Instituto de Matemática e Estatística, Universidade Federal de Goiás.

In this work we present some methods used in the study of systems of additive forms on local fields, and a proof for a particular case of Artin's Conjecture, which says that every systems with R additive forms of degrees $k_1,...,k_R$ has non trivial p-adic solution for any prime p, if the number s of variables is higher than $k_1^2+k_2^2+\cdots+k_R^2$, given by Wooley [12], where he shows that $\Gamma(3,2)=11$.

Keywords

Artin's Conjecture, pairs of additive forms, p-adic number, p-normalization for systems of additive forms.

Sumário

1 Introdução. **10**
- 1.1 Os Números p-Ádicos. 11
- 1.2 A Conjectura de Artin e formas aditivas. 13

2 Resultados preliminares. **16**
- 2.1 A p-Normalização de um sistema de formas aditivas. 16
- 2.2 O Lema de Hensel. 25
- 2.3 Alguns resultados sobre congruências. 32

3 A confirmação da Conjectura de Artin para $\Gamma(3,2)$. **38**
- 3.1 Abordando o caso padrão quando $p > 5$. 38
- 3.2 Soluções não singulares usando somas exponenciais. 51
- 3.3 Algumas demonstrações diretas do teorema para os primos 2, 3 e congruentes a $5\ (mod 12)$. 68
- 3.4 O método computacional para os primos 3, 7, 11, 13, 19, 23 e 31. 76
- 3.5 Garantindo soluções p-ádica. 78

4 Apêndice: Rotina para encontrar soluções não singulares $(mod\ p)$. **81**

Referências Bibliográficas **83**

CAPÍTULO 1

Introdução.

Introdução

Uma das grandes motivações de estudar formas aditivas sobre o corpo dos números p-ádicos é a Conjectura de Artin, que afirma existir uma cota inferior para o número de variáveis em um sistema de formas aditivas, tal que qualquer sistema de formas aditivas com pelo menos esse número de variáveis admite solução não trivial nos inteiros p-ádicos. Essa conjectura tem sido abordada com as técnicas introduzidas por Davenport e Lewis a uns 50 anos atrás. Vamos começar apresentando os corpos dos números p-ádicos, para um primo p dado, a Conjectura de Artin juntamente com um histórico desse estudo.

No capítulo seguinte, introduziremos as principais ferramentas usadas no estudo de sistemas de formas aditivas sobre o corpo dos números p-ádicos sobre o enfoque dado pela Conjectura de Artin, a p-normalização e o Lema de Hensel, além de alguns resultados sobre congruências que também serão importantes. Já no terceiro capítulo, usaremos as técnicas apresentadas no capítulo anterior para estudar uma importante confirmação da Conjectura de Artin em um caso particular, dada por Wooley [12]. Nesse trabalho ele prova que todo sistema da forma

$$\begin{aligned} F = c_1x_1^3 + c_2x_2^3 + \cdots + c_sx_s^3 &= 0 \\ G = d_1x_1^2 + d_2x_2^2 + \cdots + d_sx_s^2 &= 0 \end{aligned} \tag{1-1}$$

possui zero não trivial nos inteiros p-ádicos, para todo p primo, desde que, o número de variáveis s seja maior ou igual a 11. Esse será o resultado principal estudado nesse trabalho, mesmo assim, quando apresentarmos as ferramentas e resultados básicos para

prova-lo tentaremos não nos restringir apenas ao necessário para esse resultado, com o objetivo de que esse trabalho possa servir de referência para algum outro estudo que faça uso das mesmas ferramentas.

1.1 Os Números p-Ádicos.

Como nosso principal objetivo é estudar o problema de garantir solução p-ádica não trivial para um sistema de equações diofantinas, para todo primo p, faremos uma breve abordagem desses conjuntos numéricos, que, como veremos aqui, possuem propriedades bastante diferentes das que estamos habituados, por exemplo nos números reais, para construir esses conjuntos vamos introduzir a ideia de valorização p-ádica e, em consequência dessa valorização, iremos introduzir um valor absoluto sobre os números racionais do qual as mais interessantes propriedades irão emergir.

Seja p um número primo e n um número inteiro qualquer, o Teorema Fundamental da Aritmética nos garante que podemos escrever $n = p^{\varepsilon}m$ onde $\varepsilon \in \mathbb{N} \cup \{0\}$, e $(m, p) = 1$, assim definimos:

Definição 1.1 *Dado n inteiro tal que $n = p^{\varepsilon}m$, onde $(m,p) = 1$ e p primo, definimos a valorização p-ádica $\upsilon_p(n) := \varepsilon$. Por convenção definimos $\upsilon_p(0) := \infty$.*

Vale citar algumas propriedades de fácil dedução sobre a função definida acima,

Propriedades 1 *Dado um número inteiro n qualquer e um número primo p, vale que:*

1. $\upsilon_p(n) \geq 0$;
2. $\upsilon_p(ab) = \upsilon_p(a) + \upsilon_p(b)$;
3. $\upsilon_p(a+b) \geq min\{\upsilon_p(a), \upsilon_p(b)\}$.

Podemos agora definir o valor absoluto p-ádico, com o qual construiremos o conjunto dos números p-ádicos, e deduzir algumas das suas propriedades.

Definição 1.2 (Valor Absoluto p-ádico) *Dado $a \in \mathbb{Z}$, definimos,*

$$\|a\|_p = \begin{cases} p^{-\upsilon_p(a)}, & se \quad a \neq 0, \\ 0, & se \quad a = 0. \end{cases} \tag{1-2}$$

Propriedades 2 *Dados $a,b \in \mathbb{Z}$, temos que:*

1. $\|a\|_p \geq 0$ *e* $\|a\|_p = 0 \Leftrightarrow a = 0$;
2. $\|ab\|_p = \|a\|_p \|b\|_p$;
3. $\|a+b\|_p \leq max\{\|a\|_p, \|b\|_p\}$, *(em particular* $\|a+b\| \leq \|a\|_p + \|b\|_p$*).*

De forma bastante natural, podemos extender essa norma a todos os números racionais, ou seja, dado $\frac{a}{b} \in \mathbb{Q}$, definimos,

$$\upsilon_p\left(\frac{a}{b}\right) = \upsilon_p(a) - \upsilon_p(b), \qquad \left\|\frac{a}{b}\right\|_p = p^{-\upsilon_p(\frac{a}{b})}.$$

Note que, a propriedade 2.3 é bem mais forte do que a desigualdade triangular usual, essa desigualdade é conhecida como *desigualdade ultramétrica*, e dela seguem várias propriedades geométricas que não são válidas nos números reais. Para citar algumas propriedades interessantes dessa nova norma, podemos notar que se $a,b \in \mathbb{Q}$ tal que $\|a-b\|_p < \|a\|_p$, então, $\|a\|_p = \|b\|_p$. De fato, temos que $\|b\|_p = \|b-a+a\|_p \leq max\{\|b-a\|_p, \|a\|_p\}$, logo $\|b\|_p \leq \|a\|_p$, por outro lado, $\|a\|_p = \|a-b+b\|_p \leq max\{\|a-b\|_p, \|b\|_p\}$, como $\|a-b\|_p < \|a\|_p$ temos $\|a\|_p \leq \|b\|_p$, ou seja $\|a\|_p = \|b\|_p$.

Outra propriedade que vai contra a nossa intuição é que se $D(a,r) = \{b \in \mathbb{Q}; \|a-b\|_p < r\}$ é o disco de raio r e centro a, temos para todo $b \in D(a,r)$ que $D(a,r) = D(b,r)$. Com efeito, temos que se $b_0 \in D(a,r)$, então $\|a-b_0\|_p < r$, dado $d \in D(a,r)$, vale que $\|d-b_0\|_p = \|d-a+a-b\|_p$, daí $\|d-b_0\|_p \leq max\{\|d-a\|_p, \|a-b_0\|_p\}$, ou seja, $d \in D(b_0,r)$. Analogamente, se $c \in D(b_0,r)$ teremos $c \in D(a,r)$, assim $D(a,r) = D(b_0,r),\ \forall b_0 \in D(a,r)$, isso nos diz que todos os pontos de um disco são centros, o que claramente não vale em $\mathbb{R}$. Essas propriedades diferentes, e mesmo contra intuitivas, são consequências da propriedade 2.3 da norma p-ádica. Uma norma com essa propriedade é chamada de ultramétrica. Note que isso implica que a norma p-ádica não é arquimediana, ou seja $\|n\|_p \leq \|1\|_p,\ \forall n \in \mathbb{N}$.

Fazendo uso dessa norma, podemos agora ver o conjunto dos números p-ádicos $\mathbb{Q}_p$, como sendo o completamento de $\mathbb{Q}$ pela norma $\|\cdot\|_p$, ou seja, tomamos todas as sequências $\{z_n\}_{n\in\mathbb{N}}$, em $\mathbb{Q}$, de Cauchy com respeito a norma $\|\cdot\|_p$, cortadas pela relação de equivalência

$$(z_n),(w_n) \subset \mathbb{Q},\ (z_n) \sim (w_n) \Leftrightarrow \lim_{n\to\infty} \|z_n - w_n\|_p = 0.$$

Então, $\mathbb{Q}_p$ será o conjunto dos limites de todas essas classe de equivalência.

1.2 A Conjectura de Artin e formas aditivas.

Muitos estudos com respeito a polinômios homogêneos sobre o corpo dos números p-ádicos, têm sido feitos, no decorrer desse ultimo século, tendo como foco principal uma conjectura feita por E. Artin, que apresenta uma relação entre o número de variáveis do polinômio e a existência de zeros não triviais nos inteiros p-ádicos, a saber.

Conjectura 1 (Artin, 1920) *Qualquer polinômio homogêneo de grau k em n variáveis, tem zero p-ádico não trivial desde que* $n \geq k^2 + 1$.

Listaremos, apenas em caracter de curiosidade, alguns resultados clássicos nessa direção, para que o leitor possa entender a linha de pesquisa que motivou o trabalho que é o principal foco desse nosso estudo. As demonstrações dos resultados que seguem não fazem parte do objetivo desse trabalho, mesmo sendo todas elas muito importantes para a teoria como um todo.

O primeiro resultado importante nesse estudo veio com H. Hasse, confirmando a conjectura para formas quadráticas.

Teorema 1.3 (Hasse, 1924) *Qualquer forma quadrática sobre o corpo dos números p-ádicos em cinco ou mais variáveis, possui zero p-ádico não trivial.*

Mais tarde Lewis mostrou mais uma uma confirmação da conjectura, agora para formas cúbicas.

Teorema 1.4 (Lewis, 1952) *Toda forma cúbica com coeficientes p-ádicos em 10 ou mais variáveis, possui zero p-ádico não trivial.*

Na sequência temos também,

Teorema 1.5 (Birch-Lewis $k = 5$ **(1959), Laxton-Lewis** $k = 7, 11$ **(1962))** *Toda forma de grau* $k = 5, 7, 11$ *e coeficientes p-ádicos com número de variáveis superior a* k^2*, possui zeros p-ádicos não trivial desde que o corpo de classe residuais seja grande o suficiente, ou seja, para p grande.*

Todos esses resultados estavam direcionados para a confirmação da Conjectura de Artin, porém um primeiro contra exemplo foi dado por Terjanian em 1966, ao apresentar um polinômio homogêneo de grau 4 com 18 variáveis que não possui zero 2-ádico não trivial. Restou a pergunta, sobre quais condições vale a Conjectura de Artin? Veremos agora que a conjectura vale para uma classe especial de polinômios homogêneos chamados de *formas aditivas* ou simplesmente *diagonais*, e essa confirmação vai nos levar ao estudo de um problema análogo para sistemas de formas aditivas: quantas variáveis são necessárias para garantir zeros p-ádicos não triviais para um sistema de formas aditivas?

Da parceria de H. Davenport e D. J. Lewis, surgiram uma série de artigos buscando garantir zeros não triviais nos inteiros p-ádicos para formas do tipo aditivas, ou seja,

$$f = a_1x^k + \cdots + a_sx_s^k \qquad a_i \in \mathbb{Z}.$$

É deles a confirmação da conjectura de Artin para formas aditivas, os primeiros resultados para sistemas de formas aditivas, além do desenvolvimento de técnicas que são, ainda hoje, aplicadas e que foram usadas no trabalho que direcionou nosso atual estudo. Aqui, novamente, vamos listar os resultados clássicos para sistemas de formas aditivas, apenas na intensão de localizar o leitor com respeito ao problema geral, e encerraremos apresentando, o que tem sido visto como, uma releitura da Conjectura de Artin para sistemas de formas aditivas.

Trabalhando com sistemas de formas aditivas, Davenport e Lewis mostraram em 1969 que se o grau de todas as formas do sistema é k a existência de solução p-ádica é garantida desde que o número s de variáveis satisfaça

$$s \geq \begin{cases} 9R^2k\log(3Rk), & \text{se } k \text{ é impar,} \\ 48R^2k^3\log(3Rk^2), & \text{se } k \text{ é par.} \end{cases}$$

Em 1972 eles provaram que $s \geq 2k^2+1$ variáveis são suficientes para garantir a existência de soluções p-ádicas não triviais se sistemas de pares de formas aditivas de grau k ímpar. Para o k par a condição é $s \geq 7k^3$. Em 1988 Low, Pitman e Wolff provaram que o sistema tem zero não trivial em $\mathbb{Q}_p$ se o número de variáveis satisfaz

$$s \geq \begin{cases} 48Rk^3\log(3Rk^2), & \text{se } k > 2, \\ 2R^2k\log(k), & \text{se } k \text{ é ímpar e suficientemente grande.} \end{cases}$$

E Brüdern e Godinho, em 1998, mostraram que

$$s \geq \begin{cases} R^3k^2, & \text{se } R \geq 3 \text{ e } k \geq 3, \\ 36k^2, & \text{se } r = 3 \text{ e } k = 2^n,\ n \in \mathbb{N} \end{cases}$$

é suficiente para que exista solução não trivial em $\mathbb{Q}_p$. Existem trabalhos recentes, que variam tanto pelo número de formas aditivas, quanto pelo grau das formas.

Denotando por $\Gamma_p(k_1,...,k_R)$ o número mínimo de variáveis que garante à qualquer sistema de R formas aditivas de graus $k_1,...,k_R$ uma solução não trivial em $\mathbb{Z}_p$, e por $\Gamma(k_1,...,k_R) := sup\{\Gamma_p(k_1,...,k_R) :\ p \in \mathbb{P}\}$, a Conjectura de Artin para sistemas de formas aditivas diz que:

Conjectura 2 (Artin para sistemas de formas aditivas)

$$\Gamma(k_1,...,k_R) \leq (k_1^2 + ... + k_R^2) + 1.$$

No capítulo três, vamos provar que $\Gamma(3,2) = 11$, confirmando a Conjectura de Artin no caso $k_1 = 3, k_2 = 2$.

CAPÍTULO 2

Resultados preliminares.

Como já é tradicional nesse estudo, nós apresentaremos a p-normalização de um sistema de formas aditivas na primeira seção, com a qual poderemos nos restringir a estudar uma classe menor de sistemas. Na segunda seção, apresentaremos o Lema de Hensel, que vai nos dar uma forma de relacionar soluções $(mod\ p)$ com soluções no conjunto $\mathbb{Z}_p$. É importante notar que para nós $\mathbb{Z}_p$ e $\mathbb{Z}/p\mathbb{Z}$ representam conjuntos distintos, o primeiro representa o conjunto dos inteiros p-ádicos e o segundo o conjunto das classe laterais de $p\mathbb{Z}$ sobre $\mathbb{Z}$. Importante também dizer que tentaremos apresentar tanto a p-normalização quanto o Lema de Hensel nas suas formas mais gerais, com respeito ao estudo de formas aditivas sobre $\mathbb{Q}_p$, para que esse possa ser uma referência para leituras além daquele que apresentaremos no próximo capítulo.

2.1 A p-Normalização de um sistema de formas aditivas.

Uma das técnicas introduzidas no estudo de sistemas de formas aditivas sobre os números p-ádicos, é a p-normalização. Esse processo permite restringir o nosso estudo a uma classe de sistemas, que chamaremos de sistemas p-normalizados. Porém, a existência de solução não trivial de um sistema p-normalizado irá garantir solução não trivial para qualquer sistema equivalente à ele, onde definiremos quando dois sistemas são equivalentes. Nós consideramos importante que esse estudo seja feito de forma mais geral possível, então não iremos nos restringir a p-normalização de pares de formas aditivas de graus 2 e 3, que é o nosso principal objetivo. Em vez disso, estudaremos a p-normalização de um sistema qualquer. Para isso suponhamos que $k_1,...,k_R$ são inteiros positivos, e $F=(F_1,...,F_R)$ é um sistema de $R \leq s$ formas diagonais em s variáveis

$$F_i(x) = F_i(x_1,...,x_s) = a_{i1}x_1^{k_i} + ... + a_{is}x_s^{k_i} \quad (i=1,...,R), \tag{2-1}$$

e defina $k = max\{k_i;\ i=1,...,R\}$. Vamos supor aqui que, nenhuma das $F_i(x)$ é combinação linear de outras $F_j(x)$, ou seja, o sistema é linearmente independente.

Sejam

$$K = \prod_{j=1}^{R} k_j,$$

e

$$S = \{(j_1, ..., j_R) \in \{1, ..., s\}^R;\ j_l \neq j_i \text{ para } l \neq i\},$$

definimos M como sendo $|S| = s(s-1)\cdots(s-R+1) = M$. Dado $\sigma = (j_1, ..., j_R) \in S$, vamos definir também

$$D_\sigma(F) = det(a_{i,j_m}^{k_i'})_{1 \leq i,m \leq R},$$

onde $k_i' = \dfrac{K}{k_i}$. Portanto, $D_\sigma(F)$ é o determinante que obtemos tomando uma submatriz $R \times R$ da matriz dos coeficientes do sistema inicial, onde as colunas estão ordenadas segundo a permutação σ, e elevando os coeficientes da forma diagonal de grau k_i à $k_i' = \dfrac{K}{k_i}$. Com isso podemos definir a função ϑ sobre um sistema F do tipo (2-1) como sendo

$$\vartheta(F) = \prod_{\sigma \in S} D_\sigma(F). \tag{2-2}$$

A forma aparentemente complicada de definir $\vartheta(F)$ se justifica para manter a "homogeneidade"com respeito aos coeficiente de F. Nos trabalho de Davenport e Lewis citados, uma função semelhante é definida com o objetivo de construir um sistema p-normalizado equivalente a um sistema dado, mas lá não aparecem os expoentes do nosso caso, pois nos casos tratados nesse trabalhos todas as formas eram de mesmo grau. Seguindo esse método bem sucedido, e fazendo as adaptações necessárias, chegamos a essa que será uma ferramenta importante para que possamos tratar uma quantidade menor de sistemas mediante uma relação de equivalência que definiremos mais adiante.

Para exemplificar a definição acima, dado o sistema (1-1) nós temos

$$\vartheta(F, G) = \prod_{i \neq j} (c_i^2 d_j^3 - c_j^2 d_i^3).$$

Para simplificar a notação nos resultados que seguem, vamos definir uma relação de equivalência $\sim$ sobre $\{1, ..., R\}$ dada por

$$i \sim j \text{ se, e somente se, } k_i = k_j.$$

Denotaremos a classe de equivalência que contém i por $[i]$, e o conjunto das classes de equivalências por $\Im = \{1, ..., R\}/\sim$.

Lema 2.1 *Dado um sistema F da forma (2-1), $\vartheta(F)$ satisfaz as seguintes propriedades:*

(I) se $\omega_1, ..., \omega_s$ são inteiros, e

$$F'(x_1, ..., x_s) = F(p^{\omega_1} x_1, ..., p^{\omega_s} x_s),$$

então

$$\vartheta(F') = p^{\frac{M}{s}\omega RK} \cdot \vartheta(F),$$

onde $\omega = \omega_1 + \cdots + \omega_s$;

(II) Se λ_{ij} $(1 \leq i, j \leq R)$ *são números racionais, e o sistema* F'' *é definido por*

$$F_i''(x) = \sum_{j \in [i]} \lambda_{ij} F_j(x) \quad (i = 1, ..., R),$$

então nós temos

$$\vartheta(F'') = J^M \cdot \vartheta(F),$$

onde

$$J = \prod_{\alpha \in \Im} det(\lambda_{ij}^{k_i'})_{i,j \in \alpha}.$$

Prova: (*I*) Denotando por $\rho_i = p^{\omega_i}$, e por a_{ij}' o coeficiente de $x_j^{k_i}$ em $F_i'(x)$, temos que se $\sigma = (j_1, ..., j_R) \in S$, então

$$\begin{aligned} D_\sigma(F') &= det({a'_{ij_m}}^{k_i'})_{1 \leq i,m \leq R} \\ &= det(\rho_{j_m}^K {a_{ij_m}}^{k_i'})_{1 \leq i,m \leq R} \\ &= \rho_{j_1}^K \cdots \rho_{j_R}^K det({a_{ij_m}}^{k_i'})_{1 \leq i,m \leq R} \\ &= \rho_{j_1}^K \cdots \rho_{j_R}^K \cdot D_\sigma(F) \end{aligned}$$

então

$$\vartheta(F') = \prod_{\sigma \in S} (D_\sigma(F) \cdot (\rho_{j_1} \cdots \rho_{j_R})^K),$$

como

$$\sum_{\sigma \in S} (\omega_{j_1} + \cdots + \omega_{j_R}) = R\omega \frac{M}{s},$$

nós temos

$$\vartheta(F') = p^{\frac{M}{s}\omega RK} \cdot \vartheta(F).$$

(*II*) Denotando por a_{ij}'' o coeficiente de $x_j^{k_i}$ em $F_i''(x)$, temos que se $\sigma = (j_1, ..., j_R) \in S$, então

$$det({a''_{ij_m}}^{k_i'})_{1 \leq i,m \leq R} = det(H) \cdot det({a_{ij_m}}^{k_i'})_{1 \leq i,m \leq R},$$

onde as linhas e colunas da matriz H podem ser arranjadas de modo a formar um matriz em blocos.

$$\begin{pmatrix} C_1 & 0 & \dots & 0 \\ 0 & C_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C_r \end{pmatrix},$$

sendo $r = |\mathfrak{I}|$, e cada C_i correspondendo a um único $\alpha \in \mathfrak{I}$, tendo como determinante

$$det(C_i) = det(\lambda_{ij}^{k_i'})_{i,j\in\alpha},$$

como o número de fatores na definição de $\vartheta(F'')$ é $|S| = M$, temos

$$\begin{aligned} \vartheta(F'') &= \prod_{\sigma\in S} D_\sigma(F'') \\ &= \prod_{\sigma\in S} D_\sigma(F)\cdot det(H) \\ &= det(H)^M \cdot \prod_{\sigma\in S} D_\sigma(F), \end{aligned}$$

onde podemos notar que

$$det(H) = J = \prod_{\alpha\in\mathfrak{I}} det(\lambda_{ij}^{k_i'})_{i,j\in\alpha}.$$

□

Seguindo os trabalhos de Davenport e Lewis [4, 5, 6], Wooley [12] diz que dois sistemas da forma (2-1) são equivalentes se um pode ser obtido do outro por operações do tipo *(I)* e *(II)* do Lema 2.1. Aqui vamos pedir que o determinante de J seja não nulo, para que a operação do tipo *(II)* não seja trivial. Notemos que as operações *(I)* e *(II)* são comutativas, e além disso, se o sistema $F(x) = 0$ tem solução não trivial sobre $\mathbb{Q}_p$, então também tem solução não trivial qualquer sistema equivalente a F.

Um sistema F é dito *p-normalizado* se a potência do primo p dividindo $\vartheta(F)$ é minimal entre todos os sistemas equivalentes a F. Isto é possível, pois essa potência é não negativa. Note que um sistema p-normalizado não é único, pois qualquer operação do tipo *(II)* com J não divisível por p transforma um sistema p-normalizado em outro sistema p-normalizado. Tal transformação é conhecida como uma mudança unimodular das bases.

Para qualquer sistema F com coeficientes inteiros existe um sistema correspondente F^* com coeficientes em $\mathbb{Z}/p\mathbb{Z}$, sendo esses coeficientes congruentes $(mod\ p)$ aos coeficientes correspondentes de F. Claramente, existem variáveis que aparecem em F, mas não aparecem explicitamente em F^*.

Faremos agora um lema que nos permite dar uma estimativa para o número de variáveis que aparecem explicitamente em um sistema F p-normalizado, e também no sistema F^*.

Lema 2.2 *Um sistema F p-normalizado pode ser escrito da forma*

$$F_i = F_{i,0} + pF_{i,1} + \cdots + p^{k-1}F_{i,k-1} \qquad (i = 1,...,R),$$

onde $F_{i,j}$ são formas em m_j variáveis, e essas formas são disjuntas para $j = 0,...,k-1$. Além disso, cada uma das m_j variáveis ocorrem em pelo menos uma das $F_{i,j}$ $(i = 1,...,R)$ com um coeficiente não divisível por p.

Podemos verificar as seguintes desigualdades:

(i) Nós temos

$$m_0 + \cdots + m_{j-1} \geq \frac{js}{\kappa}, \qquad j = 1,...,k_{min},$$

onde κ é a média harmonica dos k_i e k_{min} é o menor dos k_i.

(ii) Suponha que $\alpha \in \mathfrak{I}$ com $k_i = h$ para $i \in \alpha$ e que temos L combinações lineares quaisquer, da forma

$$f_i^*(x) = \sum_{j\in\alpha} \lambda_{i,j}^* F_j^*(x) \qquad (i = 1,...,L),$$

onde $L \geq |\alpha|$, e os $(\lambda_{i,j}^*)_{j\in\alpha}$ são linearmente independentes sobre $\mathbb{Z}/p\mathbb{Z}$. Então denotando por $Q(L,h)$ o número de variáveis que ocorrem explicitamente em pelo menos umas dessas combinações, nós temos

$$Q(L,h) \geq \frac{Ls}{Rh} \qquad L = 1,...,|\alpha|.$$

(iii) Denotando por $q_{i,j}$ o número de variáveis que ocorrem explicitamente na forma $F_{i,j}^*$, nós temos

$$m_0 + \cdots + m_{j-1} + q_{i,j} \geq \frac{js}{\kappa} + \frac{s}{Rk_i} \qquad 0 \leq j \leq \min\{k_{min}, k_i - 1\}.$$

Prova:Claramente é possível expressar um sistema p-normalizado na forma

$$F_i = F_{i,0} + pF_{i,1} + \cdots \qquad (i = 1,...,R),$$

onde em cada $p^jF_{i,j}$ aparecem os termos $a_{in}x_n^{k_i}$ para os quais p^j é a maior potência de p dividindo qualquer a_{in}, $(i = 1,...,R)$. Então os conjuntos de variáveis que ocorrem em cada $F_{i,j}$, $(j = 0,1,...)$ são disjuntos.

Mas se $j \geq k$, então as formas $F_{i,j}$ são vazias, onde $k = max\{k_i;\ i = 1,...,R\}$. De fato, se F é um sistema p-normalizado então a potência de p dividindo $\vartheta(F)$ é minimal, e assim se $a_{in}x_n^{k_i}$ forem termos de $F_i(x)$, $(i = 1,...,R)$ com todos os a_{in} divisíveis por p^k, nós podemos reduzir a potência de p dividindo $\vartheta(F)$ com uma operação do tipo *(I)* do Lema 2.1, a saber, tomando $x_n = p^{-1}x'_n$, e mantendo os outros coeficientes. Além disso cada variável aparece em pelo uma das $F_{i,j}$ com um coeficiente não divisível por p, uma vez que foi tirada a potência maxima que dividia todos os coeficientes de cada variável.

(1) Sejam $x_1,...,x_m$, onde $m = m_0 + \cdots + m_{j-1}$, as variáveis em $F_{i,0},...,F_{i,j-1}$, $(1 \leq j \leq k_{min})$. Então o sistema

$$F'_i(x) = p^{-j}F_i(px_1,...,px_m,x_{m+1},...,x_s) \qquad (i = 1,...,R),$$

tem coeficientes inteiros e é equivalente ao sistema F, de fato, escrevendo

$$F_i = F_{i,0} + pF_{i,1} + \cdots + p^{k-1}F_{i,k-1},$$

temos que

$$F'_i = p^{-j} \cdot (F'_{i,0} + \cdots + p^{j-1}F'_{i,j-1}) + F_{i,j} + \cdots + p^{k-1-j}F_{i,k-1},$$

onde as variáveis de $F'_{i,0},...,F'_{i,j-1}$ são $x'_1 = px_1,...,x'_m = px_m$, como $(1 \leq j \leq k_{min})$, os coeficientes de $p^{-j} \cdot (F'_{i,0} + \cdots + p^{j-1}F'_{i,j-1})$ são inteiros e temos que o sistema F' é obtido do sistema F por meio de uma operação do tipo (II) com $\lambda_{lt} = p^{-j}$ quando $l = t$ $\lambda_{lt} = 0$ quando $l \neq t$, composta com uma operação do tipo (I) com $\omega_1 = \cdots = \omega_m = 1$ e $\omega_{m+1} = \cdots = \omega_s = 0$. Pelo Lema 2.1 seja

$$\begin{aligned} J &= \left(\prod_{\alpha \in I} det(\lambda_{lt}^{k'_l})_{l,t \in \alpha}\right) \\ J &= p^{\left[-j\cdot(k'_1+\cdots+k'_R)\right]}, \end{aligned}$$

segue que

$$\begin{aligned} \vartheta(F') &= J^M p^{\left[\frac{MR\omega K}{s}\right]}\vartheta(F) \\ \vartheta(F') &= p^{\left[-j\cdot(k'_1+\cdots+k'_R)\right]M} p^{\left[\frac{MR\omega K}{s}\right]}\vartheta(F) \\ \vartheta(F') &= p^{\left[-jM\cdot(k'_1+\cdots+k'_R)+\frac{MRmK}{s}\right]}\vartheta(F) \end{aligned}$$

Como F é um sistema p-normalizado por hipótese, temos que

$$\begin{aligned} -j\cdot(k_1'+\cdots+k_R') + \frac{RKm}{s} &\geq 0 \\ \frac{RK}{s}m &\geq j\cdot(k_1'+\cdots+k_R') \\ m &\geq \frac{s}{RK}j\cdot(k_1'+\cdots+k_R') \\ m &\geq js\cdot\frac{\frac{k_1'}{K}+\cdots+\frac{k_R'}{K}}{R} \\ m &\geq js\cdot\frac{\frac{1}{k_1}+\cdots+\frac{1}{k_R}}{R} \\ m &\geq \frac{js}{\kappa}. \end{aligned}$$

(2) Sela $\alpha\in I$, ou seja, α é o conjunto de indices tal que $k_i=k_j$ para $i,j\in\alpha$, e seja $h=k_i$ para todo $i\in\alpha$, podemos reagrupar as equações de forma que $\alpha=\{1,...,r\}$. Daí, dadas quaisquer L combinações lineares de F_j com $j\in\alpha$,

$$f_i(x)=\sum_{j=1}^{r}\lambda_{ij}F_j(x), \qquad (i=1,...,L),$$

onde $1\leq L\leq r$, e os $(\lambda_{ij})_{1\leq j\leq r}$ são linearmente independentes sobre $\mathbb{Z}/p\mathbb{Z}$. Esse conjunto pode ser completado, de modo a termos r combinações lineares que são independentes $(mod\ p)$. Então $f_1,...,f_r$ são obtidas de F_j $(1\leq j\leq r)$ por operações do tipo *(II)* do Lema 2.1 com J não divisível por p. Seja $Q(L,h)$ o número de variáveis que ocorrem em pelo menos uma das $f_1,...,f_L$ com coeficientes não divisíveis por p, e tome essas variáveis como sendo $x_i,...,x_Q$, então o sistema

$$f_i'(x)=\begin{cases} p^{-1}f_i(px_1,...,px_Q,x_{Q+1},...,x_s) & (i=1,...,L), \\ f_i(px_1,...,px_Q,x_{Q+1},...,x_s) & (i=L+1,...,r), \end{cases}$$

tem coeficientes inteiros, além disso é obtido do sistema $\mathbf{f}$ com uma combinação da operação *(I)* do Lema 2.1 com $\omega_1=\cdots=\omega_Q=1$ e da operação *(II)* do mesmo lema, com $J=p^{-L}J_0$, onde J_0 não é divisível por p. Então escrevendo $h'=\frac{K}{h}$, nós temos

$$\begin{aligned} \vartheta(f') &= p^{\frac{RKMQ}{s}-MLh'}J_0^M\vartheta(f) \\ &= p^{\frac{RKMQ}{s}-MLh'}J_0^M(det(\lambda_{ij}^{h'})_{i,j\in\alpha})^M\vartheta(F). \end{aligned}$$

Como J_0 não é divisível por p e os $(\lambda_{ij})_{1\leq j\leq r}$ são linearmente independentes

sobre $\mathbb{Z}/p\mathbb{Z}$, temos que $det(\lambda_{ij}^{h'})_{i,j\in\alpha}$ também não é divisível por p, donde,

$$\|\vartheta(f')\|_p = p^{MLh' - \frac{RKMQ}{s}} \|\vartheta(F)\|_p,$$

mas f' e F são equivalentes é pela definição de sistema p-normalizado, nós temos que $\frac{RKMQ}{s} \leq MLh'$. Assim temos que

$$Q \geq \frac{Ls}{Rh}.$$

(3) Suponha que o número de variáveis ocorrendo explicitamente em $F_{n,j}^*$ é q. Denotemos essas variáveis por $x_{m+1},...,x_{m+q}$, onde $m = m_1 + \cdots + m_{j-1}$, e por $x_1,...,x_m$ as variáveis ocorrendo em $F_{i,0},...,F_{i,j-1}$ $(i+1,...,R)$. Então para $0 \leq j \leq min\{k_{min}, k_n - 1\}$, o sistema

$$\begin{aligned} F_i''(x) &= p^{-j} F_i(px_1,...,px_{m+q},x_{m+q+1},...,x_s) \qquad (i \neq n), \\ F_n''(x) &= p^{-(j+1)} F_n(px_1,...,px_{m+q},x_{m+q+1},...,x_s). \end{aligned}$$

Aplicando o Lema 2.1 novamente, temos que

$$\vartheta(F'') = p^{\left[\frac{RKM(m+q)}{s} - (j(k_1' + \cdots + k_R') + k_n')M\right]} \vartheta(F),$$

Como F é por hipótese um sistema p-normalizado, temos

$$\begin{aligned} \frac{RKM(m+q)}{s} &\geq M(j(k_1' + \cdots + k_R') + k_n') \\ m+q &\geq \frac{s}{RK} \cdot (j(k_1' + \cdots + k_R') + k_n') \\ m+q &\geq \frac{sj}{\kappa} + \frac{s}{Rk_n}. \end{aligned}$$

□

A importância desse lema está no fato de que os resultados que vão garantir o teorema principal são na maioria resultados combinatórios, logo garantir um número mínimo de variáveis para que possamos contar número de soluções é fundamental, o proximo lema vai nos permitir refinar um pouco mais a conta do número de variáveis em um sistema p-normalizado.

Lema 2.3 *Cada forma $F_{i,j}$, do lema anterior, podem ser escritas na forma*

$$F_{i,j} = F_{i,j,0} + pF_{i,j,1} + p^2F_{i,j,2} + \cdots \quad (1 \leq i \leq R),\ (0 \leq i \leq k-1),$$

onde $F_{i,j,h}$ são formas em $r_{i,j,h}$ variáveis, e esses conjuntos de variáveis são disjuntos para $h = 0,1,2,....$ Além disso, cada uma das $r_{i,j,h}$ variáveis ocorrem em $F_{i,j,h}$ com coeficientes

não divisíveis por p.

Com as mesmas notações do lema anterior, vale as seguintes relações:

(i)

$$\sum_{h=0}^{\infty} r_{i,j,h} = m_j;$$

(ii)

$$r_{i,j,0} = q_{i,j};$$

(iii)

$$T_{i,H} = \sum_{j=0}^{H} \left(\sum_{h=0}^{H-j} r_{i,j,h} \right) \geq \frac{s(H+1)}{tk_i} \qquad (H = 0, ..., k_i - 1).$$

Prova: Que $F_{i,j}$ pode ser escrito dessa forma com as subformas $F_{i,j,h}$ disjuntas, segue da mesma construção feita no Lema 2.2, note que todas as $r_{i,j,h}$ ocorrem de fato na subforma $F_{i,j,h}$. somando todos os $r_{i,j,h}$ temos o número de variáveis em $F_{i,j}$, ou seja, $m_{i,j}$ o que demonstra *(i)*, $r_{i,j,0}$ são as variáveis que aparecem em $F_{i,j,0}$, ou seja, as variáveis de $F_{i,j}$ cujos coeficientes não são divisíveis por p, logo $r_{i,j,0} = q_{i,j}$, o que garante *(ii)*, vamos então provar *(iii)*.

Sejam $H \leq k_n - 1$, $T = T_{n,H}$ como definido acima, e $x_1, ..., x_T$ as variáveis que ocorrem na forma

$$(F_{n,0,0} + pF_{n,0,1} + \cdots + p^H F_{n,0,H}) + p(F_{n,1,0} + \cdots + p^H F_{n,0,H-1}) + \cdots + p^H F_{n,H,0},$$

que são, as variáveis ocorrendo explicitamente na forma $F_n \ (mod\ p^{H+1})$. Então o sistema

$$\begin{aligned} F_n'(x) &= p^{-(H+1)} F_n(px_1, ..., px_T, x_{T+1}, ..., x_s), \\ F_i'(x) &= F_i(px_1, ..., px_T, x_{T+1}, ..., x_s), \quad i \neq n, \end{aligned}$$

tem coeficientes inteiros e é equivalente ao sistema F. Pelo Lema 2.1 nós temos

$$\vartheta(F') = p^{\left[-(H+1)Mk_n' + \frac{RKMT}{s}\right]} \vartheta(F).$$

Então pela definição de sistema p-normalizado,

$$\begin{aligned} T &\geq \frac{(H+1)sk_n'}{RK} \\ &= \frac{(H+1)s}{Rk_n}. \end{aligned}$$

□

Vamos agora aplicar os Lemas 2.2 e 2.3 ao nosso sistema (1-1), para exemplificar, e também para termos em mãos algumas estimativas para o número de variáveis que ocorrem em um sistema p-normalizado equivalente ao nosso sistema, lembrando que será com essas estimativas dos números de variáveis que iremos trabalhar, aplicando métodos combinatórios e de resolução de equações diofantinas para garantir o que mais adiante iremos definir como solução não singular para o sistema.

Então seja (F,G) um sistema de formas aditivas como em (1-1), com número de variáveis $s \geq 11$, então temos que

$$\begin{array}{ccc} m_0 \geq 5, & q_{F,0} = T_{F,0} \geq 2, & q_{G,0} = T_{G,0} \geq 3, \\ m_0 + m_1 \geq 10, & m_0 + q_{F,1} \geq 7, & m_0 + q_{G,1} \geq 8, \\ T_{F,1} \geq 4, & T_{G,1} \geq 6, & T_{F,2} \geq 6. \end{array} \tag{2-3}$$

2.2 O Lema de Hensel.

O proximo resultado que queremos apresentar vai nos permitir relacionar soluções de sistema de formas aditivas $(mod\ p)$ com soluções nos inteiros p-ádicos, esse resultado é um entre os vários que ficaram conhecidos por Lema de Hensel. K. Hensel foi o primeiro a desenvolver a teoria dos números p-ádicos na busca de informações locais dentro dos racionais, de uma maneira análoga a teoria das sequências e séries existentes nos números reais. Mas antes iremos apresentar alguns resultados que serão importantes na demonstração do Lema de Hensel, começaremos provando algumas propriedades simples do espaço $\mathbb{Q}_p^n$.

Primeiramente, dado o espaço vetorial $\mathbb{Q}_p^n$ sobre o corpo de escalares $\mathbb{Q}_p$, definindo nele a norma do máximo, ou seja, dado um vetor $z = (x_1, ..., x_n)$ em $\mathbb{Q}_p^n$ a norma de z é dada por $\|z\|_{max} = max\{\|x_1\|_p, ..., \|x_n\|_p\}$, não é difícil verificar que de fato se trata de uma norma, e além disso ela também satisfaz a desigualdade ultramétrica. De maneira análoga podemos definir uma matriz $M_{n\times n}$ em $\mathbb{Q}_p^{n\times n}$, naturalmente o conjunto das matrizes sobre $\mathbb{Q}_p$ é um espaço vetorial, e podemos definir o produto $M \cdot z$ onde z pertence a $\mathbb{Q}_p^n$ da mesma forma que o feito sobre $\mathbb{R}$ e também podemos definir nele uma norma semelhante a norma de um operadores linear. Ou seja, dada $M_{n\times n}$ uma matriz em $\mathbb{Q}_p^{n\times n}$ definimos

$$\|M\|_1 = sup\left\{\|M \cdot z\|_{max}; z \in \mathbb{Z}_p^n\right\}.$$

Note que $\mathbb{Z}_p^n$ é compacto com a norma do máximo, uma vez que $\mathbb{Z}_p^n = \{z \in \mathbb{Q}_p^n; \|z\|_{max} \leq 1\}$ é um subconjunto fechado e limitado de $\mathbb{Q}_p^n$ que é um espaço de dimensão finita. Aqui iremos verificar as propriedades de norma, ou seja

(i) $\|M\|_1 = 0 \Leftrightarrow M = \overline{0}$;

De fato, se $M = \overline{0}_{n\times n}$, temos que $M \cdot z = \overline{0}_{n\times 1}$ para qualquer que seja z em $\mathbb{Z}_p^n$, donde $\|M\|_1 = 0$. Reciprocamente, suponha que $\|M\|_1 = 0$, então para qualquer que seja z em $\mathbb{Z}_p^n$ temos que $M \cdot z = \overline{0}_{n\times 1}$, em particular tomando $e_1 = (1,0,...,0), ..., e_n = (0,0,...,1)$, ou seja $M = \overline{0}_{n\times n}$.

(ii) $\|\alpha \cdot M\|_1 = \|\alpha\|_p \cdot \|M\|_1$, para todo α em $\mathbb{Q}_p$;

De fato,

$$\begin{aligned} \|\alpha \cdot M\|_1 &= sup\left\{\|\alpha \cdot M \cdot z\|_{max}; z \in \mathbb{Z}_p^n\right\} \\ &= sup\left\{\|\alpha\|_p \cdot \|M \cdot z\|_{max}; z \in \mathbb{Z}_p^n\right\} \\ &= \|\alpha\|_p \cdot \|M\|_1. \end{aligned}$$

(iii) $\|M+N\|_1 \leq \|M\|_1 + \|N\|_1$.

De fato,

$$\begin{aligned} \|M+N\|_1 &= sup\left\{\|(M+N) \cdot z\|_{max}; z \in \mathbb{Z}_p^n\right\} \\ &= sup\left\{\|M \cdot z + N \cdot z\|_{max}; z \in \mathbb{Z}_p^n\right\} \\ &\leq sup\left\{|M \cdot z\|_{max} + \|N \cdot z\|_{max}; z \in \mathbb{Z}_p^n\right\} \\ &\leq \|M\|_1 + \|N\|_1. \end{aligned}$$

Com isso colocamos uma estrutura de espaço vetorial normado nas matrizes sobre $\mathbb{Q}_p$, veremos no próximo resultado que essa norma tem uma propriedade semelhante a existente para matrizes sobre $\mathbb{R}$ definidas de modo análogo.

Lema 2.4 *Dada um matriz M em $\mathbb{Q}_p^{n\times n}$, temos que $\|M \cdot z\|_{max} \leq \|M\|_1 \cdot \|z\|_{max}$ para todo z em $\mathbb{Z}_p^n$.*

Prova: De fato, note primeiramente que dado x em $\mathbb{Z}_p^*$, temos que $\|x\|_p = p^{-\upsilon(x)}$, daí que $\|\|x\|_p\|_p = p^{\upsilon(x)}$, ou seja, $\|x\|_p = \|\|x\|_p\|_p^{-1}$, donde

$$\begin{aligned} \left\|\frac{x}{\|x\|_p}\right\|_p &= \frac{\|x\|_p}{\|\|x\|_p\|_p} \\ &= \|x\|_p^2 \\ &\leq 1 \qquad \forall x \in \mathbb{Z}_p^*, \end{aligned}$$

Note que o mesmo vale para z em $\mathbb{Z}_p^{n*}$, com a norma $\|\cdot\|_{max}$, ou seja, se z pertence a $\mathbb{Z}_p^{n*}$, então $w = \|z\|_{max}^{-1} \cdot z$ também pertence a $\mathbb{Z}_p^n$, donde

$$\begin{aligned}\frac{\|M\cdot z\|_{max}}{\|z\|_{max}} &= \|M\cdot(\|z\|_{max}^{-1}\cdot z)\|_{max}\\ &= \|M\cdot w\|_{max} \qquad w\in\mathbb{Z}_p^{n*}\\ &\leq \|M\|_1.\end{aligned}$$

□

Note a importância de tomar o $\|M\|_1 = \sup\{\|M\cdot z\|_{max}\}$ com z em $\mathbb{Z}_p^n$ para que a norma de M cumpra essa última propriedade. Pela desigualdade ultramétrica essa norma será limitada pela maior norma das entradas da matriz M, isto vai nos garantir que se a matriz tem todas as suas entradas pertencentes a $\mathbb{Z}_p$, então sua norma é menor ou igual a 1, o que caracteriza de forma bastante útil as matrizes inteiras, e será importante na demonstração do Lema de Hensel. O próximo lema vai nos permitir avaliar a norma p-ádica de um polinômio aplicado a um ponto.

Lema 2.5 *sejam $p(x_1,...,x_n)$ pertencente a $\mathbb{Z}_p[x_1,...,x_n]$, e $(\xi_1,...,\xi_n)$ em $\mathbb{Z}_p^n$, se $p(x_1,...,x_n)$ não possui termos com grau menor que k, então*

$$\|p(\xi_1,...,\xi_n)\|_p \leq \|(\xi_1,...,\xi_n)\|_{max}^k.$$

Prova: De fato temos que se nenhum termo de $p(x_1,...,x_n)$ aparece com grau menor que k, então

$$p(x_1,...,x_n) = \sum c_i\cdot x_1^{k_{1i}}\cdots x_n^{k_{ni}},$$

onde apenas um número finito de c_i é diferente de zero, e

$$\sum_{j=1}^{n} k_{ji} \geq k,$$

para todo i em $\mathbb{N}$. Daí suponha que $\|(\xi_1,...,\xi_n)\|_{max} = \|\xi_t\|_p$, então

$$\begin{aligned}\|p(\xi_1,...,\xi_n)\|_p &= \left\|\sum c_i\cdot\xi_1^{k_{1i}}\cdots\xi_n^{k_{ni}}\right\|_p\\ &\leq max\{\|c_i\cdot\xi_1^{k_{1i}}\cdots\xi_n^{k_{ni}}\|_p\}\\ &\leq max\{\|\xi_1^{k_{1i}}\cdots\xi_n^{k_{ni}}\|_p\}\\ &\leq \|\xi_t\|_p^k = \|(\xi_1,...,\xi_n)\|_{max}^k.\end{aligned}$$

□

Note que estamos usando o fato de $\|x+y\|_p \leq max\{\|x\|_p, \|y\|_p\}$, para todos x e y em $\mathbb{Q}_p$, e que $\|c\|_p \leq 1$ para todo c em $\mathbb{Z}_p$, como são fatos bastante usados e fundamentais nos números p-ádicos, usaremos daqui em diante sem mais ressalvas.

Agora dados $F_1,...,F_n$ polinômios em $\mathbb{Z}_p[x_1,...,x_n]$, podemos usar a notação vetorial e definir

$$F = (F_1,...,F_n),$$

como um vetor que tem como componentes os polinômios $F_1,...,F_n$, onde se $x = (x_1,...,x_n)$ é um vetor em $\mathbb{Q}_p^n$, então denotamos por $F(x)$ o vetor

$$F(x) = (F_1(x),...,F_n(x)),$$

em $\mathbb{Q}_p^n$. Vamos denotar a matriz jacobiana de F por,

$$J_F = \left(\frac{\partial F_i}{\partial x_j}\right),$$

e seu determinante (jacobiano) por,

$$\Delta_F = \det\left(\frac{\partial F_i}{\partial x_j}\right).$$

Vamos considerar também que cada componente do vetor F é uma série formal de potências em n variáveis sobre $\mathbb{Q}_p$. Nesse caso $F(x)$ só fará sentido para um x em $\mathbb{Q}_p^n$ se cada uma das séries $F_i(x)$ converge. Certamente essas séries convergem se todas as componentes de x são divisíveis por p. Se G é outro vetor de séries formais de potências, precisaremos considerar a composta das séries

$$F \circ G = F(G),$$

obtida pela substituição por G_i das variáveis x_i em F, novamente, isso pode não fazer sentido, mas isso vai representar um sistema unicamente determinado de séries de potência se nós soubermos que G é um sistema de séries sem termos constantes, com coeficientes em $\mathbb{Z}_p$, já que potências dessas séries são também convergentes. Um problema natural é determinar aqueles sistemas F que são invertíveis sob essa lei de composição, ou seja, para quais sistemas existe G tal que

$$F \circ G = G \circ F = x,$$

onde $x = (x_1,...,x_n)$.

Lema 2.6 *seja F um sistema de n séries formais em n variáveis sem termos constantes.*

Assuma que o jacobiano $\Delta_F(0)$ de F na origem é uma unidade em $\mathbb{Q}_p$. Então F possui um sistema inverso G, com respeito a composição, que é unicamente definido.

Prova: Note que $\Delta_F(0)$ é o determinante da matriz (a_{ij}) onde a_{ij} é o coeficiente do termo linear x_j na série F_i. Introduzimos um novo vetor de variáveis $y = (y_1, ..., y_n)$. Nos queremos resolver o sistema de equações

$$x_i = \sum_{j=1}^{n} a_{ij} y_i + \sum_k a_{ik} y^k \qquad (1 \leq i \leq n),$$

para y, onde no segundo somatório $k = (k_1, ..., k_n)$, e $y^k = (y_1^{k_1} y_2^{k_2} \cdots y_n^{k_n})$ com $k_1 + \cdots + k_n \geq 2$, ou seja, todos os termos do segundo somatório tem grau maior que 1.

Por hipótese a matriz $A(a_{ij})$ tem inversa $B = (b_{ij})$ com coeficientes em $\mathbb{Q}_p$. Reescrevendo o sistema anterior de equações como uma equação vetorial

$$x = F(y),$$

operando os dois lados com a matriz B temos a equação vetorial equivalente

$$z = B \cdot F(y),$$

onde $z = Bx$, e onde o coeficiente de y_j na i-ésima componente do lado direito é δ_{ij} (delta de Kronecker). Podemos então assumir que

$$a_{ij} = \delta_{ij},$$

para todos i, j, de modo que temos que encontrar um sistema G nas variáveis x tal que

$$x_i = G_i + \sum_k a_{ik} G_1^{k_1} G_2^{k_2} \cdots G_n^{k_n} \qquad (1 \leq i \leq n),$$

Daí temos que a parte de G_i de grau menor que 2 deve ser simplesmente x_i. Por indução, suponha que a soma H_{id} dos termos de grau menor que d está determinado para todo i. Então a parte homogênea G_{id} de grau d em G_i é unicamente determinada como sendo a parte homogênea de grau d na série

$$-\sum_k a_{ik} H_1^{k_1} H_2^{k_2} \cdots H_n^{k_n} \qquad (1 \leq i \leq n),$$

uma vez que H_{id} não possui termo constante. Assim F tem um inverso a direita unicamente determinado G. Como nós temos

$$\Delta_G(0) = \Delta_F(0)^{-1},$$

o mesmo argumento mostra que G possui um inverso a direita E. Mas então

$$E = x \circ E = (F \circ G) \circ E = F \circ (G \circ E) = F \circ x = F.$$

□

Agora estamos prontos para provar a seguinte versão do Lema de Hensel, que será utilizada amplamente no próximo capítulo, garantindo soluções não triviais para o nosso sistema de formas aditivas.

Lema 2.7 (Lema de Hensel) *Seja $F : \mathbb{Q}_p^n \to \mathbb{Q}_p^n$ uma aplicação tal que*

$$F(x_1,...,x_n) = (F_1(x_1,...,x_n),...,F_n(x_1,...,x_n)),$$

onde $F_1(x_1,...,x_n),...,F_n(x_1,...,x_n) \in \mathbb{Z}_p[x_1,...,x_n]$, e seja $z_0 = (a_1,...,a_n)$ pertencente a $\mathbb{Z}_p^n$ tal que

$$\|F(z_0)\|_{max} = \|(F_1(z_0),...,F_n(z_0))\|_{max} < \|\Delta_0\|_p^2,$$

com

$$\Delta_0 = \det(J_F(a_1,...,a_n)),$$

não nulo, onde $J_F(a_1,...,a_n)$ é a matriz jacobiana de F calculada em z_0, sendo as entradas da matriz jacobiana dadas pelas derivadas formais de cada polinômio. Nessas condições existe um único $z = (\xi_1,...,\xi_n)$ em $\mathbb{Z}_p^n$ tal que $F(z) = (0,...,0)$ e

$$\|z - z_0\|_{max} = \|(\xi_1 - a_1,...,\xi_n - a_n)\|_{max} \leq p^{-1}\|\Delta_0\|_p.$$

Prova: Vamos aqui utilizar o resultado de álgebra linear que afirma que se N é a matriz adjunta de $J_F(z_0)$, então nós temos que

$$J_F(z_0)N = \Delta_0 I,$$

onde I é a matriz identidade, note que por hipótese os termo da matriz $J_F(z_0)$ são todos inteiros p-ádicos, e daí, segue pela construção da matriz adjunta que os termos da matriz N também são. Como Δ_0 é não nulo, existem δ finito, e u uma unidade tal que

$$\Delta_0 = up^{\delta},$$

Aplicando a fórmula de Taylor para cada polinômio em F temos a equação vetorial

$$F(z_0 + p^{\delta}x) = F(z_0) + J_H(z_0) \cdot p^{\delta}x + p^{2\delta}R(x),$$

onde $R(x)$ é um vetor de polinômios, cada um deles sem termos de grau menor que 2. Se $N' = u^{-1}N$, esta fórmula pode ser reescrita como

$$F(z_0 + p^{\delta}x) = F(z_0) + J_H(z_0) \cdot p^{\delta}x + J_F(z_0)N' \cdot p^{\delta}R(x),$$

se nós denotarmos por

$$G(x) = x + N'R(x),$$

nós temos

$$F(z_0 + p^{\delta}x) = F(z_0) + J_H(z_0) \cdot p^{\delta}G(x).$$

Note que G é um sistema de n polinômios em n variáveis sem termos constantes, e o jacobiano da G na origem é 1, logo nós podemos aplicar o Lema 2.6 para o sistema G, que vai nos garantir que existe um sistema H de séries formais de potências unicamente determinado sem termos constantes que é inverso do sistema G de polinômios pela composição. Substituindo x por $H(x)$ na fórmula acima temos

$$F(z_0 + p^{\delta}H(x)) = F(z_0) + J_H(z_0) \cdot p^{\delta}x,$$

onde nessa identidade podemos substituir x por qualquer vetor x em $\mathbb{Q}_p^n$ com $\|x\|_{max}$ menor que 1, para garantir a convergência da série formal. Por hipótese

$$\|F(z_0)\|_{max} < \|\Delta_0\|_p^2,$$

ou seja $F(z_0) = p^{2\delta}c$ onde $\|c\|_{max} < 1$. Portanto, temos que encontrar x, com $\|x\|_{max} < 1$ tal que

$$0 = p^{2\delta} \cdot c + J_H(z_0) \cdot p^{\delta}x,$$

ou, usando novamente $p^{\delta} = J_H(z_0)N'$, temos

$$0 = p^{\delta}J_H(z_0) \cdot (N'c + x),$$

como Δ_0 é não nulo, $J_H(z_0)$ admite inversa, logo esse sistema possui uma única solução

$$x = -N'c,$$

pelo Lema 2.4 $\|x\|_{max} \leq \|c\|_{max} < 1$, logo

$$z = z_0 + p^{\delta}H(-N'c),$$

é solução, e além disso temos que

$$\|z - z_0\|_{max} = \|p^{\delta} H(-N'c)\|_{max},$$

pelos Lemas 2.4 e 2.5,

$$\begin{aligned} \|z - z_0\|_{max} &\leq p^{-\delta} \|c\|_{max} \\ &\leq p^{-\delta-1} \\ &\leq p^{-1} \|\Delta_0\|_p. \end{aligned}$$

□

Note que esse resultado pode ser facilmente generalizado para sistemas de R formas em $s \geq R$ variáveis, simplesmente fixando $s - R$ variáveis. Com o Lema de Hensel agora em mão, garantir solução para um sistema de formas irá se resumir a encontrar um z_0 que esteja nas hipóteses do lema, o que equivale, como veremos no proximo capítulo, a encontrar um tipo especial de solução do sistema p-normalizado visto $(mod p)$ que chamaremos de solução não singular. Então, de fato, é o Lema de Hensel uma das mais importantes ferramentas nesse estudo, pois ele nos permite passar de um problema em um conjunto que conhecemos muito pouco para um problema nos inteiros $(mod p)$, então nos próximos capítulos vamos entender como é feita essa passagem, e como resolver o novo problema para o caso específico de duas formas aditivas em graus 2 e 3.

2.3 Alguns resultados sobre congruências.

Vamos agora apresentando alguns resultados importantes sobre congruências que vão nos auxiliar no próximo capítulo. O primeiro resultado devido a Chevalley não será usado diretamente no resultado, mas achamos conveniente apresenta-lo aqui devido sua grande importância na teoria.

Teorema 2.8 (Chevalley 1935) *Todo polinômio em n variáveis, de grau d e sem termos constante, tem sempre uma solução não trivial módulo p, desde que $n > d$.*

Prova: Para provar esse teorema, vamos usar o seguinte lema:

Lema 2.9 *Seja $f(x_1, ..., x_n) \in \mathbb{Z}/p\mathbb{Z}[x_1, ..., x_n]$ com $gr(f(x_1, ..., x_n)) < n(p-1)$. Então*

$$\sum_{c_1, ..., c_n \in \mathbb{Z}/p\mathbb{Z}} f(c_1, ..., c_n) = 0.$$

Prova:

$$\sum_{c_1,...,c_n\in\mathbb{Z}/p\mathbb{Z}} c_1^{k_1}\cdots c_n^{k_n} = \sum_{c_1\in\mathbb{Z}/p\mathbb{Z}} c_1^{k_1}\cdots \sum_{c_n\in\mathbb{Z}/p\mathbb{Z}} c_n^{k_n},$$

portanto, existe um $k_j < p-1$, onde $j \in \{1,2...,n\}$, tal que $p-1 \nmid k_j$, portanto

$$\sum_{c_j\in\mathbb{Z}/p\mathbb{Z}} c_j^{k_j} = 0$$

$$\Rightarrow \sum_{c_1,...,c_n\in\mathbb{Z}/p\mathbb{Z}} f(c_1,...,c_n) = 0.$$

□

Prova do Teorema de Chevalley: Dado o polinômio $f(x_1,...,x_n) \in \mathbb{Z}/p\mathbb{Z}[x_1,...,x_n]$ de grau $d < n$ sem termo constante, defina o polinômio $F(x_1,...,x_n) = 1 - f(x_1,...,x_n)^{p-1}$, o qual tem grau menor que $n(p-1)$.

$$F(c_1,...,c_n) = \begin{cases} 0 & \text{se } f(x_1,...,x_n) \neq 0, \\ 1 & \text{c.c.} \end{cases}$$

logo

$$\sum_{c_1,...,c_n\in\mathbb{Z}/p\mathbb{Z}} F(c_1,...,c_n) = N,$$

onde N é o número de soluções de $f(x_1,...,x_n) = 0$ em $\mathbb{Z}/p\mathbb{Z}$. Mas pelo lema anterior temos que

$$\sum_{c_1,...,c_n\in\mathbb{Z}/p\mathbb{Z}} F(c_1,...,c_n) = 0$$

em $\mathbb{Z}/p\mathbb{Z}$, donde $N \equiv 0 \ (mod\ p)$. Porém com f não possui termos constantes, temos que $(0,...,0)$
$mathbbZ/p\mathbb{Z}^n$ é uma solução de $f(x_1,...,x_n) = 0$, ou seja, $N \geq 1$, como $N \equiv 0 \ (mod\ p)$, então existe uma solução não trivial $(mod\ p)$.

□

Daremos aqui apenas uma ideia da demonstração do lema a seguir, uma demonstração mais completa pode ser encontrada em Nathanson [10], Teorema 2.8.

Lema 2.10 *Seja $p > 3$ um número primo, e seja k um inteiro positivo tal que $(k, p-1) < \frac{p-1}{2}$. Sejam $c_1,...,c_n$ elementos não nulos do corpo $\mathbb{Z}/p\mathbb{Z}$, então temos que*

$$f(x_1,...,x_n) = c_1x_1^k + ... + c_nx_n^k,$$

representa pelo menos $R = min\left\{p, 1+\frac{(2n-1)(p-1)}{d}\right\}$ *resíduos* $(mod\ p)$*, onde* $d = (k, p-1)$.

Prova: Se $k = 1$ e $n \geq 1$ é fácil ver que $R = p \leq (1+(2n-1)(p-1))$ para todo n, então vamos supor $k > 1$.

Seja

$$g(x_1, ..., x_n) = c_1 x_1^d + ... + c_n x_n^d.$$

Defina $R(g)$ como sendo o número de resíduos $(mod\ p)$ representados por g. Seja $A_k = \{x^k; x \in \mathbb{Z}/p\mathbb{Z}\}$ e $A_d = \{x^d; x \in \mathbb{Z}/p\mathbb{Z}\}$. Não é difícil mostrar que $A_k = A_d$, e daí segue que $R = R(f) = R(g)$, onde $R(f)$ é o número de resíduos $(mod\ p)$ representados por f, logo podemos assumir que $k = (k, p-1)$. Então

$$p = ks + 1,$$

onde $s \geq 3$, e $|A_k| = s+1$. Vamos provar que

$$R \geq min\{p, (2n-1)s+1\}.$$

A prova será feita por indução sobre n. Se $n = 1$, então $f(x_1) = c_1 x_1^k$, onde $c_1 \neq 0$, e então

$$|R| = |A_k| = s+1 = min(p, s+1).$$

Suponha que o lema vale para $n \geq 2$. Seja

$$A = \left\{\sum_{i=1}^{n-1} c_i x_i^k;\ x_1, ..., x_{n-1} \in \mathbb{Z}/p\mathbb{Z}\right\},$$

e

$$B = \{c_n x_n^k;\ x_n \in \mathbb{Z}/p\mathbb{Z}\}.$$

Então $|B| = |A_k| = s+1$. Temos que o conjunto $|A|$ é o número de resíduos representados por uma forma aditiva em $n-1$ variáveis, então pela hipótese de indução

$$|A| \geq min\{p, (2n-3)s+1\}.$$

Temos que

$$R = A + B,$$

então pelo teorema de Cauchy-Davenport (Nathanson [10] Teorema 2.2)

$$\begin{aligned} |R| &= |A+B| \\ &\geq min(p, |A|+|B|-1) \\ &\geq min(p, (2n-2)s+1). \end{aligned}$$

Se $|R| = p$, não temos mais o que mostrar. Então suponha que $|R(f)| \leq p-1$, daí

$$R = |A+B| \geq |A|+|B|-1 \geq (2n-2)s+1.$$

Agora vamos primeiramente mostrar que $|R(f)| > (2n-2)s+1$. De fato, suponha por contradição que $|R(f)| = (2n-2)s+1$, ou seja, $|A+B| = |A|+|B|-1$, então pelo Teorema de Vosper (Nathanson [10] Teorema 2.7) pelo menos uma das condições abaixo devem ser satisfeitas

(1º) ou $min(|A|,|B|) = 1$. O que é claramente falso.

(2º) ou $|R(f)| = |A+B| = p-1 = ks$. O que também é falso, pois temos que $R(f) \equiv 1 \ (mod\ s)$ (Nathanson [10] Lema 2.9)

(3º) ou, finalmente, A e B são progressões aritméticas com a mesma razão, o que é falso, pois nem A_k nem B possuem progressões aritméticas (Nathanson [10] Lema 2.11).

Logo,

$$|R(f)| \geq (2n-2)s+2.$$

porem

$$|R(f)| \equiv 1 \ (mod\ p),$$

daí segue que

$$|R(f)| \geq (2n-1)s+1.$$

□

Corolário 2.11 *Seja $p > 7$ e $\alpha_1\alpha_2 \not\equiv 0 \ (mod\ p)$. Então $\alpha_1 x_1^3 + \alpha_2 x_2^3$ representa todos os resíduos $(mod\ p)$.*

Prova: De fato, pelo Lema 2.10 temos que

$$R = min\left\{p, 1 + \frac{(2n-1)(p-1)}{d}\right\},$$

como $n = 2$ e $d \leq 3$ o resultado segue.

□

Corolário 2.12 *Seja $p > 5$ e $\alpha_1\alpha_2 \not\equiv 0 \ (mod\ p)$. Então $\alpha_1 x_1^2 + \alpha_2 x_2^2$ representa todos os resíduos $(mod\ p)$.*

Prova: De fato, pelo Lema 2.10 temos que

$$R = min\left\{ p, 1 + \frac{(2n-1)(p-1)}{d} \right\},$$

como $n = 2$ e $d \leq 2$ o resultado segue.

□

Lema 2.13 *A congruência* $ax^3 + by^3 + cz^3 \equiv 0 \ (mod\ p)$ *é sempre solúvel com pelo menos um dos* $x, y, z \not\equiv 0 \ (mod\ p)$.

Prova: Seja $\mathbb{Z}/p\mathbb{Z}^*$ o grupo multiplicativo de $\mathbb{Z}/p\mathbb{Z}$, e seja $\mathbb{Z}/p\mathbb{Z}^3$ o grupo das potências cúbicas de $\mathbb{Z}/p\mathbb{Z}^*$. Se $p \equiv 2 \ (mod\ 3)$, nós temos que $(p-1, 3) = 1$, logo $\mathbb{Z}/p\mathbb{Z}^3 = \mathbb{Z}/p\mathbb{Z}^*$. Se $p \equiv 1 \ (mod\ 3)$, então $\mathbb{Z}/p\mathbb{Z}^3 \neq \mathbb{Z}/p\mathbb{Z}^*$. De fato, $\mathbb{Z}/p\mathbb{Z}^3$ contêm exatamente $\dfrac{p-1}{3}$ elementos, e se δ não está em $\mathbb{Z}/p\mathbb{Z}^3$, então $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z}^3 \cup \delta\mathbb{Z}/p\mathbb{Z}^3 \cup \delta^2\mathbb{Z}/p\mathbb{Z}^3$.

Como $abc \not\equiv 0 \ (mod\ p)$, temos que se $ab^{-1} \in \mathbb{Z}/p\mathbb{Z}^3$, seja $e^3 = ab^{-1}$, então $(1, -e, 0)$ é uma solução para $ax^3 + by^3 + cz^3 \equiv 0 \ (mod\ p)$. Nós obtemos soluções semelhantes se ac^{-1} ou bc^{-1} pertence a $\mathbb{Z}/p\mathbb{Z}^3$. Então podemos supor que a, b e c estão em classes laterais diferentes de $\mathbb{Z}/p\mathbb{Z}$, módulo $\mathbb{Z}/p\mathbb{Z}^3$, uma situação que só pode acontecer se $p \equiv 1 \ (mod\ 3)$.

Afirmamos que se $p \equiv 1 \ (mod\ 3)$, então existe um elemento não nulo δ de $\mathbb{Z}/p\mathbb{Z}$ que não está em $\mathbb{Z}/p\mathbb{Z}^3$ tal que a equação

$$1 + \delta \equiv \delta^2 z^3 \ (mod\ p)$$

possui uma solução em $\mathbb{Z}/p\mathbb{Z}$.

De fato, seja W o conjunto de todos os elementos não nulos de $\mathbb{Z}/p\mathbb{Z}^*$ da forma $\rho^3 - 1$. Então W contém exatamente $\dfrac{p-4}{3}$ elementos distintos. Seja W^{-1} o conjunto dos inversos multiplicativos dos elementos de W, e seja $V = \mathbb{Z}/p\mathbb{Z}^3 \cup W \cup W^{-1}$. Então V contêm no máximo $p-3$ elementos. Seja $\delta \in \mathbb{Z}/p\mathbb{Z}$, tal que $\delta \notin V$. Claramente, δ e $\delta + 1$ não estão em $\mathbb{Z}/p\mathbb{Z}^3$. Além disso, δ^{-1} não esta em V, consequentemente $1 + \delta^{-1}$ não está em $\mathbb{Z}/p\mathbb{Z}^3$, daí $\delta + 1$ não está em $\delta\mathbb{Z}/p\mathbb{Z}^3$. Como -1 está em $\mathbb{Z}/p\mathbb{Z}^3$, $1 + \delta \neq 0$, e segue que $1 + \delta$ está em $\delta^2\mathbb{Z}/p\mathbb{Z}^3$ como queríamos. Suponha, sem perda de generalidade, que $a = e_1^3$, $b = \delta e_2^3$ e $c = \delta^2 e_3^3$, então existe z_0 tal que $(e_1^{-1}, e_2^{-1}, z_0)$ é uma solução para $ax^3 + by^3 + cz^3 \equiv 0 \ (mod\ p)$.

□

Lema 2.14 *Suponha que* $abc \not\equiv 0 \ (mod\ 7)$. *Então a congruência* $ax^3 + by^3 \equiv c \ (mod\ 7)$ *é solúvel a menos que* $b \equiv \pm a$ *e* $c \equiv \pm 4a$.

Prova: Suponha $ax^3 + by^3 \equiv c \ (mod\ 7)$ não pode ser resolvido, nós temos pelo Lema 2.13 que existe solução para a congruência $ax^3 + bx^3 + cz^3 \equiv 0 \ (mod\ 7)$, com pelo um dos $x, y, z \not\equiv 0 \ (mod\ 7)$, logo $z \equiv 0 \ (mod\ 7)$, daí temos que $x, y \not\equiv 0 \ (mod\ 7)$, como apenas $\{0, 1, -1\}$ são cubos $(mod\ 7)$, segue que $b \equiv \pm a \ (mod\ 7)$, e assim $ax^3 + by^3$ representa os resíduos $\{0, \pm a, \pm 2a\}$, dessa forma temos que $c \equiv \pm 4a \ (mod\ 7)$.

□

Note que, em particular, os Corolários do Lema 2.10 dizem que todo resíduo não trivial é representado não trivialmente pelas respectivas formas. Note também que se $abc \not\equiv 0 \ (mod\ p)$, então a conclusão do Lema 2.14 implica que pelo menos dois dos x, y, z são não triviais $(mod\ p)$.

CAPÍTULO 3

A confirmação da Conjectura de Artin para $\Gamma(3,2)$.

Apresentaremos agora o trabalho realizado pelo matemático Trevor D. Wooley que foi publicado em 1991, onde ele prova que $\Gamma(3,2) = 11$, confirmando a Conjectura de Artin. Utilizando os métodos introduzidos por Davenport e Lewis que apresentamos no capítulo anterior, e o Lema de Hensel que também já apresentamos, e dividindo o problema em diversos casos, para os quais, apresentou soluções simples e elegantes, ele conseguiu demonstrar esse resultado, um dos primeiros resultados de grande relevância que trata de pares de formas aditivas em graus distintos. Nas primeiras duas seções vamos apresentar como ele aplicou o método mais usual no tratamento do problema, que consiste em garantir soluções não singulares $(mod\ p)$ e usar o Lema de Hensel para concluir que existe solução não trivial em $\mathbb{Z}_p$, para garantir o resultado para todos os primos, a menos de um número finito deles, que trataremos nas seções finais.

3.1 Abordando o caso padrão quando $p > 5$.

Voltamos agora a nossa atenção ao sistema

$$\begin{aligned} F(x) = c_1x_1^3 + \cdots + c_sx_s^3 &= 0, \\ G(x) = d_1x_1^2 + \cdots + d_sx_s^2 &= 0. \end{aligned} \tag{3-1}$$

Vamos assumir que $\vartheta(F,G) \neq 0$ e que $s \geq 11$, além disso vamos reagrupar e também renomear variáveis e coeficientes se for preciso para escrever ou sistema $(F,G)^*$ da seguinte forma

$$\begin{aligned} F_0^* &= a_1x_1^3 + \cdots + a_ux_u^3 + b_1y_1^3 + \cdots + b_vy_v^3 \equiv 0 \ (mod\ p), \qquad (3\text{-}2) \\ G_0^* &= c_1y_1^2 + \cdots + c_vy_v^2 + d_1z_1^2 + \cdots + d_wz_w^2 \equiv 0 \ (mod\ p). \end{aligned}$$

Onde nenhum dos $a_i,\ b_i,\ c_i,\ d_i$ são divisíveis por p, pelas contas feitas em (2-3) tomando um sistema p-normalizado equivalente ao (3-1) podemos garantir que

$$m_0 = u+v+w \geq 5, \quad q_{F,0} = u+v \geq 2, \quad q_{G,0} = v+w \geq 3. \qquad (3\text{-}3)$$

Nessa seção vamos provar que sujeito a hipótese

(H) para toda congruência da forma (3-2) satisfazendo $u+v+w \geq 5$, $u \leq 1$, e $w \leq 1$, nós temos uma solução que é não singular $(mod\ p)$,

para $p > 5$, todo sistema p-normalizado da forma (3-1) tem solução p-ádica não trivial. Assim iremos supor que u ou v é maior que 1 e provar que a congruência (3-2) possui solução não singular $(mod\ p)$, e na seção seguinte vamos provar a hipótese *(H)*, usando somas exponenciais para quase todos os primos, a menos de um número finito, que serão tratados separadamente.

Acima aparece o conceito de *solução não singular*, para definir esse conceito, seja (F,G) um sistema da forma (3-1), e x um elemento de $\mathbb{Z}_p^s$, definimos

$$\Delta(i,j) = \Delta(F,G,i,j) = 6x_ix_j(c_id_jx_i - c_jd_ix_j),$$

e

$$\Delta^*(F,G) = max\{\|\Delta(i,j)\|_p \ 1 \leq i,j \leq s\}.$$

Então diremos que um solução x do sistema $F \equiv G \equiv 0 \ (mod\ p)$ é não singular $(mod\ p)$ quando $\Delta^*(F,G) = 1$ em x. Isso equivale a dizer que a matriz jacobiana de (F,G) calculada em x tem posto 2 $(mod\ p)$. Note que dada uma solução não singular $x = (x_1,...,x_s)$, se fixarmos $s-2$ variáveis no Lema de Hensel apresentado no capítulo anterior, e calcularmos $\Delta(x_i,x_j) = \det(J_{(F,G)}(x_i,x_j))$, onde x_i,x_j são tais que $\|\Delta(i,j)\|_p = \Delta^*(F,G) = 1$, ou seja, vamos ter $\|\Delta(x_i,x_j)\|_p = 1$, como x é uma solução do sistema $F \equiv G \equiv 0 \ (mod\ p)$, temos que $\|(F(x),G(x))\|_{max} < 1 = \|\Delta(x_i,x_j)\|_p^2$ e a existência de solução inteira p-ádica não trivial segue diretamente do Lema de Hensel.

Nós vamos começar provando a existência de solução não trivial sobre $\mathbb{Z}_p$ para (3-1) no caso onde $q_{F,0} \geq 3$ e $p > 7$. Na sequência vamos tratar $p = 7$, ainda supondo que $q_{F,0} \geq 3$, e por fim assumiremos que $q_{F,0} = 2$ e provaremos a existência de solução não trivial p-ádica para todo $p > 5$.

Lema 3.1 *Seja $p > 7$. Então todo sistema p-normalizado da forma (3-1) satisfazendo $s \geq 11$, $q_{F,0} \geq 3$, e $u > 1$ ou $w > 1$, possui solução não trivial sobre $\mathbb{Z}_p$.*

Prova: Vamos dividir a demonstração em casos de acordo com o valor de v.

(i) $v = 0$. Então por (3-3) $w \geq 3$, e como estamos supondo $q_{F,0} \geq 3$, temos $u \geq 3$. Pelo Lema 2.13 nós podemos resolver o sistema de congruências

$$a_1 x_1^3 + \cdots + a_u x_u^3 \equiv 0 \ (mod \ p)$$

com pelo menos uma variável diferente de zero, digamos x_i. Também pelo Corolário 2.12 do Lema 2.10, nós podemos resolver a congruência

$$d_1 z_1^2 + \cdots + d_w z_w^2 \equiv 0 \ (mod \ p)$$

independentemente com pelo menos uma variável não nula, digamos z_j. Então o sistema pode ser resolvido $(mod \ p)$ com $\Delta^*(F,G) \geq \|6x_i z_j (a_i d_j x_i)\|_p = 1$.

(ii) $v = 1$. Então por (3-3), $w \geq 2$ e como estamos supondo $q_{F,0} \geq 3$, temos $u \geq 2$. Vamos fixar $y_1 = 1$, pelo Corolário 2.11 do Lema 2.10, nós podemos resolver a congruência

$$a_1 x_1^3 + \cdots + a_u x_u^3 + b_1 \equiv 0 \ (mod \ p)$$

com pelo menos uma variável diferente de zero, digamos x_i. Também, pelo Corolário 2.12 do Lema 2.10, nós podemos resolver a congruência

$$c_1 + d_1 z_1^2 + \cdots + d_w z_w^2 \equiv 0 \ (mod \ p)$$

independentemente com pelo menos uma variável não nula, digamos z_j. Então novamente o sistema pode ser resolvido $(mod \ p)$ com $\Delta^*(F,G) \geq \|6x_i z_j (a_i d_j x_i)\|_p = 1$.

(iii) $v \geq 2$. Existem dois casos:

(a) $w \geq 2$.

(1) $p \equiv 1 \ (mod \ 3)$. Uma vez que $q_{F,0} \geq 3$, pelo Lema 2.13 nós podemos resolver a congruência

$$a_1 x_1^3 + \cdots + a_u x_u^3 + b_1 y_1^3 + \cdots + b_v y_v^3 \equiv 0 \ (mod \ p)$$

não trivialmente (aqui x_i pode não aparecer se $u = 0$). E mais, nós podemos garantir que pelo menos uma das variáveis y_i é diferente de zero usando o

Corolário 2.11 e o Lema 2.13. Sejam $1,\ c,\ c'$ as três raízes cúbicas distintas da unidade $(mod\ p)$. Então fixando y_i de modo a resolver a congruência cúbica, nós podemos encontrar $g_i \in \{1, c, c'\}$ para $i = 1, ..., v$, de modo que

$$c_1(g_1y_1)^2 + \cdots + c_v(g_vy_v)^2 \not\equiv 0\ (mod\ p). \tag{3-4}$$

Então nós temos uma solução para a congruência cúbica com a congruência quadrática (3-4) não nula.

(2) $p \not\equiv 1\ (mod\ 3)$ e $u > 0$. Então todo resíduo $(mod\ p)$ é um resíduo cúbico. Nós podemos tomar $x_2 = \cdots = x_u = y_2 = \cdots = y_v = 0$ e resolver a congruência $a_1x_1^3 + b_1y_1^3 \equiv 0\ (mod\ p)$ não trivialmente.

(3) $p \not\equiv 1\ (mod\ 3)$ e $u = 0$. Então $v \geq 3$. Assim, nós temos $b_i \equiv \beta_i^3\ (mod\ p)$ para algum $\beta_i \not\equiv 0\ (mod\ p)$ $(i = 1, 2, 3)$. Mas se supormos que

$$c_1\beta_2^2 + c_2\beta_1^2 \equiv c_2\beta_3^2 + c_3\beta_2^2 \equiv c_3\beta_1^2 + c_1\beta_3^2 \equiv 0\ (mod\ p),$$

teríamos

$$(c_1\beta_1^2)\beta_2^2\beta_3^2 \equiv -c_2\beta_1^4\beta_3 \equiv c_3\beta_2^2\beta_1^4 \equiv -c_1\beta_1^2\beta_2^2\beta_3^2 \equiv 0\ (mod\ p).$$

Então $(\beta_1\beta_2\beta_3)^2 \equiv 0\ (mod\ p)$, o que é uma contradição. Por isso um dos $(\beta_2, -\beta_1, 0)$, $(0, \beta_3, -\beta_2)$ e $(-\beta_3, 0, \beta_1)$ é uma solução para a congruência

$$b_1y_1^3 + b_2y_2^3 + b_3y_3^3 \equiv 0\ (mod\ p),$$

tal que $c_1y_1^2 + c_2y_2^2 + c_3y_3^2 \not\equiv 0\ (mod\ p)$.
Em qualquer dos casos (1), (2), (3), nós podemos resolver a congruência cúbica em (3-2) de tal maneira que

$$c_1y_1^2 + \cdots + c_vy_v^2 \not\equiv 0\ (mod\ p),$$

e com pelo menos uma das y_i não nula, digamos y_j. Mas pelo Corolário 2.12 do Lema 2.10, fixando os valores de y_i, nós podemos resolver a congruência quadrática

$$d_1z_1^2 + \cdots + d_wz_w^2 \equiv -(c_1y_1^2 + \cdots + c_vy_v^2) \not\equiv 0\ (mod\ p),$$

com pelo menos uma das z_i não nula, digamos z_k. Então o sistema pode ser resolvido com $\Delta^*(F, G) \geq \|6y_jz_k(b_jd_ky_j)\|_p = 1$.

(b) $w \leq 1$, pela hipótese (H) se $u \leq 1$, temos solução não singular $(mod\ p)$, nesse

caso podemos supor $u \geq 2$. Então por (3-3) $v \geq 3 - w$. Pelo Corolário 2.12 do Lema 2.10, nós podemos resolver a congruência

$$c_1 y_1^2 + \cdots + c_v y_v^2 + d_1 z_1^2 \equiv 0 \ (mod\ p)$$

não trivialmente (aqui o termo z_1 pode não aparecer caso $w = 0$). Mais do isso, nós podemos garantir que pelo menos uma das y_i é não nulas usando o Corolário 2.12, digamos y_1. Note que trocando y_i por $-y_i$ nós continuamos a ter uma solução para a congruência quadrática. Fixemos esses valores de y_i, e consideremos a forma cúbica $a_1 x_1^3 + a_2 x_2^3$. Pelo Corolário 2.11 do Lema 2.10, como $p > 7$, está forma não representa no máximo um resíduo $(mod\ p)$ não trivialmente, a saber o resíduo zero. Mas trocando os sinais $+$ e $-$ existem pelo menos dois resíduos distintos na forma

$$\pm b_1 y_1^3 \pm \cdots \pm b_v y_v^3$$

porque pelo menos um dos y_i são não nulos. Então pelo menos um desses dois resíduos fornece uma solução não trivial em x_1 e x_2 para a congruência

$$a_1 x_1^3 + a_2 x_2^3 \pm b_1 y_1^3 \pm \cdots \pm b_v y_v^3 \equiv 0 \ (mod\ p).$$

Então podemos supor que x_1 é não nulo, e dessa forma temos que o sistema pode ser resolvido com $\Delta^*(F,G) \geq \|6x_1 y_1 (a_1 c_1 x_1)\|_p = 1$.

Então nos casos (i), (ii) e (iii), nós temos que existe solução não singular $(mod\ p)$ para a congruência (3-2). Logo podemos aplicar o Lema de Hensel para garantir solução não trivial em $\mathbb{Z}_p$ para o sistema (3-1).

□

O caso $p = 7$ é um pouco mais complicado, pois $x^3 + y^3 + 4z^3 \equiv 0 \ (mod\ 7)$ só possui solução com $z \equiv 0 \ (mod\ 7)$. Nós vamos então modificar as ideias do caso anterior para lidar com essa eventualidade.

Lema 3.2 *Todo sistema 7-normalizado da forma (3-1) satisfazendo $s \geq 11$, $q_{F,0} \geq 3$, e $u > 1$ ou $w > 1$ possui uma solução não trivial sobre $\mathbb{Z}_7$.*

Prova: Vamos novamente separar em casos de acordo com o valor de v.

(i) $v = 0$. A prova segue exatamente igual ao caso $v = 0$ demonstrado no Lema 3.1.

(ii) $v = 1$. Então por (3-3), $w \geq 2$ e $u \geq 2$. Pelo Lema 2.14, nós podemos resolver a congruência

$$a_1 x_1^3 + \cdots + a_u x_u^3 + b_1 y_1^3 \equiv 0 \ (mod\ 7)$$

com $y_1 \not\equiv 0 \ (mod\ 7)$, e pelo menos um dos x_i não nulo, a menos que $u = 2$, $a_2 \equiv \pm a_1$ e $b_1 \equiv \pm 4a_1$. Se esse ultimo caso não ocorrer, a prova segue da mesma forma que o caso análogo provado no Lema 3.1. Certo, caso ocorra esse ultimo caso, por uma mudança de variáveis e uma mudança temporária da notação, nós podemos supor que o sistema é

$$\begin{aligned} F^* = &\quad x_1^3 + &\quad x_2^3 &\quad + 4y_1^3 &&\equiv 0 \ (mod\ 7) \\ G^{**} = &\quad 7b_1x_1^2 + &\quad 7b_2x_2^2 &\quad + c_1y_1^2 + d_1z_1^2 + \cdots + d_tz_t^2 &&\equiv 0 \ (mod\ 7^2), \end{aligned}$$

onde 7 não divide c_1. Além disso, por (3-2) nós temos

$$t = m_0 - q_{F,0} + q_{G,1} \geq 5.$$

Tome $y_1 = 0$. Se três ou mais dos $d_1, ..., d_t$ não são divisíveis por 7, digamos $d_1, ..., d_w$, então nós podemos resolver a congruência

$$\begin{aligned} F_0^* = x_1^3 + x_2^3 &&&\equiv 0 \ (mod\ 7) \\ G_0^* = &\quad d_1z_1^2 + \cdots + d_wz_w^2 &&\equiv 0 \ (mod\ 7) \end{aligned}$$

independentemente com $x_1 = 1$, $x_2 = -1$, e com pelo menos um dos z_i não nulos, digamos z_j. E o sistema pode ser solucionado com $\Delta^*(F,G) \geq \|6x_1z_j(d_1x_1)\|_7 = 1$.

Se apenas dois dos $d_1, ..., d_t$ não são divisíveis por 7, digamos, sem perda de generalidade, d_{t-1} e d_t, então tomamos $z_{t-1} = z_t = 0$ e dividimos toda a G por 7. Então obtemos o um sistema da forma

$$\begin{aligned} F_0^* = &\quad x_1^3 + x_2^3 &&\equiv 0 \ (mod\ 7) \\ G_0'^* = C_1x_1^2 + C_2x_2^2 &\quad + d_1z_1^2 + \cdots + d_wz_w^2 &&\equiv 0 \ (mod\ 7), \end{aligned} \tag{3-5}$$

onde 7 não divide qualquer um dos d_i, os C_i são inteiros, e $w \geq t - 2 \geq 3$. Nós podemos resolver a congruência cúbica tomando $x_1 = 1$ e $x_2 = -1$. Então pelo Corolário 2.12 do Lema 2.10, nós podemos resolver a congruência quadrática nos z_i, digamos com z_j não nulo. Logo o sistema reduzido pode ser resolvido com $\Delta^*(F,G) \geq \|6x_1z_j(d_jx_1)\|_7 = 1$.

Assim no caso $v = 1$ o sistema reduzido pode ser resolvido com uma solução não singular $(mod\ 7)$, e então o sistema (3-1) tem uma solução não trivial sobre $\mathbb{Z}_7$, pelo Lema de Hensel.

(iii) $v \geq 2$. Existem dois casos.

(a) $w \geq 2$. Nesse caso podemos proceder da mesma forma que no Lema 3.1 (iii) (a) (1).

(b) $u \geq 2$ e $w \leq 1$. Por (3-3), $v \geq 3 - w$. Observemos que por uma mudança de variáveis podemos transformar $c_1y_1^2 + c_2y_2^2 \ (mod\ 7)$ em uma das seguintes formas

$$\pm(y_1^2 + y_2^2) \text{ ou } \pm(y_1^2 - y_2^2).$$

Nessas hipóteses podemos, sem perda de generalidade, escrever

$$c_1y_1^2 + \cdots + c_vy_v^2 + d_1z_1^2 + \cdots + d_wz_w^2 = c_1y_1^2 + c_2y_2^2 + dz^2,$$

onde dz^2 representa $d_1z_1^2$ se $w = 1$, ou representa $c_3y_3^2$ se $w = 0$. Então $c_1y_1^2 + c_2y_2^2 + dz^2 \equiv 0 \ (mod\ 7)$ é equivalente a uma das seguintes congruências

$$\begin{aligned} y_1^2 + y_2^2 + z^2 &\equiv 0, \text{ com solução } (1,2,4), \\ +(y_1^2 - y_2^2) + z^2 &\equiv 0, \text{ com solução } (2,1,2), \\ -(y_1^2 - y_2^2) + z^2 &\equiv 0, \text{ com solução } (1,2,2), \\ -(y_1^2 - y_2^2) + z^2 &\equiv 0, \text{ com solução } (2,2,1). \end{aligned}$$

Vamos denotar por by^3 o termo $b_3y_3^3$ se $w = 0$, ou o termo 0 se $w = 1$. Então em cada um desses casos, a congruência quadrática é solúvel com y_1, y_2 e z diferentes de zero, de modo que para escolhas adequadas de $+$ e $-$, a expressão

$$\pm b_1y_1^3 \pm b_2y_2^3 \pm by^3$$

tem pelo menos três valores distintos. Então a congruência

$$c_1y_1^2 + c_2y_2^2 + dz^2 \equiv 0$$

pode ser resolvida de tal maneira que, pelo Lema 2.13, a congruência

$$a_1x_1^3 + a_2x_2^3 + b_1y_1^3 + b_2y_2^3 + by^3 \equiv 0$$

tem uma solução com pelo menos um dos x_i diferentes de zero, digamos x_1. Daí o sistema pode ser resolvido com $\Delta^*(F,G) \geq \|6x_1y_1(a_1c_1x_1)\|_7 = 1$.

Então nos casos (i), (ii), e (iii) deduzimos que, definindo algumas das variáveis como sendo zero, as equações (3-1) são equivalentes a um sistema com solução não singular $(mod\ 7)$, o que pelo Lema de Hensel nos garante uma solução não trivial 7-ádica.

□

Assim, sujeito a hipótese (H), e assumindo $\vartheta(F,G) \neq 0$, $s \geq 11$ e $q_{F,0} \geq 3$, nós mostramos que qualquer sistema da forma (3-1) com $p > 5$ tem um solução não trivial p-ádica. Nós agora vamos mostrar que quando $q_{F,0} = 2$, nas mesmas condições ainda temos pelo menos uma solução não trivial p-ádica.

Lema 3.3 *Seja $p > 5$, e suponha que vale a hipótese (H). Então todo sistema da forma (3-1) p-normalizado com $s \geq 11$ e $q_{F,0} = 2$ possui uma solução não trivial sobre $\mathbb{Z}_p$.*

Prova: Usaremos as desigualdades dada em (2-3) para dividir a demonstração em casos.

(i) Suponha $q_{F,0} = T_{F,0} = 2$ e $T_{F,1} \geq 5$. Podemos reagrupar as variáveis e trocar a notação para escrever

$$\begin{aligned} F^{**} = &\quad A_1X_1^3 + A_2X_2^3 + p(a_1x_1^3 + \cdots + a_ux_u^3 + b_1y_1^3 + \cdots + b_vy_v^3) &&\equiv 0 \ (mod\ p^2) \\ G^{*} = &\quad B_1X_1^2 + b_2X_2^2 + c_1y_1^2 + \cdots + c_vy_v^2 + d_1z_1^2 + \cdots + d_wz_w^2 &&\equiv 0 \ (mod\ p), \end{aligned}$$

onde p não divide qualquer um dos a_i, b_i, c_i, d_i, e A_i, os B_i são números inteiros, e por (2-3) nós temos

$$\begin{aligned} u+v &= T_{F,1} - T_{F,0} \geq 3, \\ u+v+w &= m_0 + q_{F,1} - q_{F,0} \geq 5, \\ v+w &= m_0 - q_{F,0} \geq 3. \end{aligned}$$

Independentemente de $T_{F,1}$, se $p = 7$ e $A_1 \equiv \pm A_2 \ (mod\ 7)$, então, uma vez que $v+w \geq 3$, nós temos uma solução para o sistema que é não singular $(mod\ 7)$, dada por (3-5). Dessa forma, nós podemos assumir que se $p = 7$, então $A_1 \not\equiv \pm A_2 (mod\ 7)$.

Fixemos agora $X_1 = X_2 = 0$, e considere a congruência obtida pela mudança de variáveis

$$\begin{aligned} F'^{*} = &\quad (p^{-1}F)^{*} &&\equiv 0 \ (mod\ p) \\ G'^{*} = &\quad G^{*} &&\equiv 0 \ (mod\ p). \end{aligned}$$

Este sistema de congruências ou da forma que a hipótese (H) se aplica, ou então é de algumas das formas dos sistemas que consideramos nos Lemas 3.1 e 3.2, com $q_{F',0} \geq 3$. Sendo assim o sistema possui uma solução que é não singular $(mod\ p)$, e consequentemente o sistema (3-1) possui uma solução p-ádica não trivial, a menos que pelo Lema 3.5, $p = 7$, $u = 2$, $v = 1$, $w = 2$, $a_2 \equiv \pm a_1 \ (mod\ p)$ e $b_1 \equiv \pm 4a_1 \ (mod\ 7)$.

Mas nesse último caso nós consideramos a congruência obtida ao tomar $X_1 = X_2 = y_1 = z_1 = z_2 = 0$, e fazendo a mudança de variáveis

$$\begin{aligned} F''^* = (7^{-2}F)^* &\equiv 0 \ (mod\ 7) \\ G'^* = (7^{-1}G)^* &\equiv 0 \ (mod\ 7) \end{aligned}$$

Assim, reagrupando variáveis e mudando a notação, por (2-3) o sistema vai ser da forma (3-5) com

$$w+2 = (m_0+m_1) - m_0 \geq 5.$$

Então a congruência tem uma solução que é não singular $(mod\ 7)$, logo as equações (3-1) possuem uma solução não trivial 7-ádica.

(ii) Suponha que $T_{F,0} = 2$, $T_{F,1} = 4$, e $T_{F,2} \geq 7$. Reagrupando variáveis e mudando a notação, podemos escrever

$$\begin{aligned} F &= A_1X_1^3 + A_2X_2^3 + p(A_3X_3^3 + A_4X_4^3) \\ &\quad + p^2(a_1x_1^3 + \cdots + a_ux_u^3 + b_1y_1^3 + \cdots + b_vy_v^3) + p^3(B_1z_1^3 + \cdots + B_wz_w^3) \\ &\quad + p^{3m+n}(e_1u_1^3 + \cdots + e_ru_r^3) \\ G &= C_1X_1^2 + C_2X_2^2 + C_3X_3^2 + C_4X_4^2 \\ &\quad + p(D_1x_1^2 + \cdots + D_ux_u^2) + c_1y_1^2 + \cdots + c_vy_v^2 + d_1z_1^2 + \cdots + d_wz_w^2 \\ &\quad + p(f_1u_1^2 + \cdots + f_ru_r^2), \end{aligned}$$

onde p não divide qualquer um dos a_i, b_i, c_1, d_i, e e_1, os B_i, C_i, D_i, f_i e $e_2, ..., e_r$ são inteiros, nós temos $m \geq 1$ e $0 \leq n \leq 2$, e por (2-3),

$$\begin{aligned} u+v &= T_{F,2} - T_{F,1} \geq 3, \\ v+w &= m_0 + q_{F,1} - T_{F,1} \geq 3, \\ 4+u+v+w+r &\geq 11. \end{aligned} \tag{3-6}$$

Nós podemos supor que os f_i não são divisíveis por p, pois se $p \mid f_i$ e $p^3 \mid (p^{3m+ne_i})$ para algum i então ϑ não é minimal (nós podemos fazer uma transformação do tipo $u_i \mapsto p^{-1}u_i$ que não afeta os coeficientes).

Independentemente de $T_{F,2}$, se $p = 7$ e $A_3 \equiv \pm A_4 \ (mod\ 7)$, então fazendo $X_1 = X_2 = 0$ e dividindo o que restar de F por 7. Como $u+v \geq 3$, o sistema é da forma (3-5), e dessa forma nós temos uma solução 7-ádica não trivial para as equações (3-1). Assim vamos assumir que se $p = 7$, então $A_3 \not\equiv \pm A_4 \ (mod\ 7)$.

(a) Suponha primeiro que $u+v+w \geq 5$. Então nós fixamos $X_1 = ... = X_4 = 0$ e consideramos as congruências obtidas pela mudança de variáveis

$$\begin{aligned} F''^* = &\quad (p^{-2}F)^* &&\equiv 0 \ (mod\ p) \\ G''^* = &\quad G^* &&\equiv 0 \ (mod\ p). \end{aligned}$$

Analogamente ao que fixemos no item (i) da demonstração, este sistema de congruências ou é da forma que a hipótese (H) se aplica, ou então é igual a algum dos sistemas que consideramos nos Lemas 3.1 e 3.2 com $q_{F'',0} \geq 3$. Dessa forma o sistema tem uma solução que é não singular $(mod\ p)$, e consequentemente o sistema (3-1) tem uma solução p-ádica não trivial, a menos que pelo Lema 3.5, $p = 7$, $u = 2$, $v = 1$, $w = 2$, $a_2 \equiv \pm a_1 \ (mod\ p)$ e $b_1 \equiv \pm 4a_1 \ (mod\ 7)$.

Mas nesse último caso, nós consideramos o sistema obtido fixando $X_1 = ... = X_4 = y_1 = z_1 = z_2 = 0$, e fazendo a mudança de variáveis

$$\begin{aligned} F''^* = (7^{-2}F)^* &\equiv 0 \ (mod\ 7) \\ G''^* = (7^{-1}G)^* &\equiv 0 \ (mod\ 7). \end{aligned}$$

Onde

$$r \geq 7 - u - v - w = 2,$$

e

$$m_0 + m_1 - T_{F,1} - T_{G,0} \geq 10 - 4 - 3 = 3,$$

possivelmente fixando uma ou mais variáveis iguais a zero, nós temos um sistema da formas

$$\begin{aligned} F''^* = &\quad x_1^3 + x_2^3 &&\equiv 0 \ (mod 7) \\ G''^* = D_1 x_1^2 + a_1 x_2^2 &\quad + b_1 y_1^2 + \cdots + b_{r'} y_{r'}^2 &&\equiv 0 \ (mod 7) \end{aligned} \tag{3-7}$$

onde 7 não divide $b_1, ..., b_{r'}$, $r' \geq 2$, e se $r' = 2$, então 7 não divide a_1.

Mas nós podemos resolver a congruência cúbica colocando $(x_1, x_2) = (\alpha_1, -\alpha_2)$ para quaisquer $\alpha_1, \alpha_2 \in \{1, 2, 4\}$. Se $r' > 2$, então nós podemos resolver a congruência quadrática não trivialmente, pelo Corolário 2.12 do Lema 2.10, digamos com y_1 não nulo. Se $r' = 2$, então já que para alguma escolha de α_1 e α_2, a expressão $D_1\alpha_1^2 + a_1\alpha_2^2$ deve ser um resíduo não nulo, nós também podemos resolver a congruência quadrática para y_1 e y_2, pelo Corolário 2.12 do Lema 2.10, digamos com y_1 não nulo. Então o sistema pode ser resolvido com $\Delta^*(F'', G'') \geq \|6x_1y_1(b_1x_1)\|_7 = 1$. Daí o sistema possui uma solução que

é não singular $(mod\ p)$, e consequentemente as equações (3-1) possuem uma solução 7-ádica não trivial.

(b) Suponha agora que $u+v+w < 5$. Então por (3-6), nós temos $r \geq 3$. Se $n = 0$, fixe

$$X_3 = X_4 = x_1 = ... = x_u = y_1 = ... = y_v = z_1 = ... = z_w = 0,$$

e substituindo X_i por $p^m X_i$ para $i = 1,2$, se $n = 1$, fixe

$$X_1 = X_2 = x_1 = ... = x_u = y_1 = ... = y_v = z_1 = ... = 0,$$

e substituindo X_i por $p^m X_i$ para $i = 3,4$, se $n = 2$, fixe

$$X_1 = ... = X_4 = 0,$$

e substituindo x_i por $p^m x_i$ para $i = 1,...,u$, y_i por $p^m y_i$ para $i = 1,...,v$, e z_i por $p^m z_i$ para $i = 1,...,w$. Dividindo por p^{3m+n} o que restar de F, e por p o que restar de G, reagrupando as variáveis e mudando a notação se necessário, nós obtemos o sistema

$$\begin{array}{lllll} F'''^* = & a_1x_1^3 + \cdots + a_ux_u^3 & +b_1y_1^3 + \cdots + b_vy_v^3 & & \equiv 0 \\ G'''^* = & & +c_1y_1^2 + \cdots + c_vy_v^2 + d_1z_1^2 + \cdots + d_wz_w^2 & & \equiv 0, \end{array}$$

onde

$$u \geq 2, \qquad u+v \geq 3, \qquad v+w \geq 3,$$

e

$$u+v+w \geq \begin{cases} 5 & \text{para } n = 0,1, \\ 6 & \text{para } n = 2. \end{cases}$$

Quando $p \neq 7$, o sistema de congruências $F'''^* \equiv G'''^* \equiv 0\ (mod\ p)$ pode ser tratado da mesma forma que os sistemas considerados no Lema 3.1. Da mesma forma, quando $p = 7$, nós temos $A_{2i-1} \not\equiv A_{2i}\ (mod\ 7)$ para $i = 1,2$, e por isso quando $n = 0,1$, o sistema de congruências $F'''^* \equiv G'''^* \equiv 0\ (mod\ 7)$ pode ser tratado como os sistemas que nós fomos capazes de resolver no Lema 3.2, com $q_{F''',0} \geq 3$. Quando $p = 7$ e $n = 2$, nós temos $u+v+w \geq 6$, de modo que fixando no máximo uma variável como sendo zero, nós obtemos um sistema da forma que nós resolvemos no Lema 3.2. Dessa forma o sistema tem uma solução não singular $(mod\ p)$, e consequentemente as equações (3-1) possuem pelo menos uma solução p-ádica não trivial.

(iii) Suponha que $T_{F,0} = 2$, $T_{F,1} = 4$, e $T_{F,2} = 6$. Reagrupando variáveis e mudando a

notação. O sistema agora assume a forma

$$\begin{aligned} F &= A_1X_1^3 + A_2X_2^3 + p(A_3X_3^3 + A_4X_4^3) + p^2(A_5X_5^3 + A_6X_6^3) \\ &\quad + p^{3m+n}(a_1x_1^3 + \cdots + a_rx_r^3) \\ G &= B_1X_1^2 + B_2X_2^2 + B_3X_3^2 + B_4X_4^2 + B_5X_5^2 + B_6X_6^2 \\ &\quad + (b_1x_1^2 + \cdots + b_rx_r^2), \end{aligned} \tag{3-8}$$

onde

$$m \geq 1, \qquad 0 \geq n \geq 2, \qquad r \geq 5,$$

e onde os B_i e b_i são inteiros, e p não divide qualquer um dos A_i ou a_i. Além disso, por alguns dos argumentos que nós aplicamos para os f_i em (2), no máximo p divide algum dos b_i.

Seja $S_0 = \{i : p \nmid b_i, e\ 1 \leq i \leq r\}$, e $S_1 = \{1,...,r\}/S_0$. Então a cardinalidade de S_0 ou S_1 é pelo menos 3, uma vez que $r \geq 5$. Supondo que a cardinalidade de $S_0 \geq 3$, e renomeando qualquer três das variáveis que estão em S_0 como x_1, x_2, x_3. Fixando $x_4 = x_5 = 0$, nós temos o sistema

$$\begin{aligned} F &= A_1X_1^3 + A_2X_2^3 + p(A_3X_3^3 + A_4X_4^3) + p^2(A_5X_5^3 + A_6X_6^3) \\ &\quad + p^{3M+N}(a_1x_1^3 + a_2x_2^3 + a_3x_3^3) \\ G &= B_1X_1^2 + B_2X_2^2 + B_3X_3^2 + B_4X_4^2 + B_5X_5^2 + B_6X_6^2 \\ &\quad + p^t(b_1x_1^2 + b_2x_2^2 + b_3x_3^2), \end{aligned}$$

onde p não divide qualquer um dos A_i ou b_i, $t = 0$ ou 1, $M \geq 1$, $0 \leq N \leq 2$, e no máximo dois dos a_1, a_2, a_3 são divisíveis por p. Se $N = 0$, fixando

$$X_3 = ... = X_6 = 0,$$

e substituindo X_i por $p^M X_i$ para $i = 1,2$, se $N = 1$, fixando

$$X_1 = X_2 = X_5 = X_6 = 0,$$

e substituindo X_i por $p^M X_i$ para $i = 3,4$, se $N = 2$, fixando

$$X_1 = X_2 = X_5 = X_4 = 0,$$

e substituindo X_i por $p^M X_i$ para $i = 5,6$. Nós podemos dividir por p^{3M+N} o que restar de F, e por p^t o que restar de G, reagrupar variáveis e mudar a notação, para obter o

sistema

$$\begin{aligned} F^{IV*} &= a_1x_1^3 + \cdots + a_ux_u^3 \quad + b_1y_1^3 + \cdots + b_vy_v^3 && \equiv 0 \quad (3\text{-}9) \\ G^{IV*} &= && c_1y_1^2 + \cdots + c_vy_v^2 \quad + d_1z_1^2 + \cdots + d_wz_w^2 \equiv 0, \end{aligned}$$

onde

$$u+v \geq 3, \qquad v+w \geq 3, \qquad u+v+w \geq 5.$$

Agora nós sabemos que $A_{2i-1} \not\equiv A_{2i} \ (mod\ 7)$ para $i = 1,2$, e consequentemente, a menos que $N = 2$, $p = 7$, $u = 2$, $v = 1$, $w = 2$, $a_1 \equiv \pm a_2 \ (mod\ 7)$ e $b_1 \equiv \pm 4a_1 \ (mod\ 7)$, o sistema de congruências $F^{IV*} \equiv G^{IV*} \equiv 0 \ (mod\ 7)$ é igual a alguma dos sistemas que nós consideramos nos Lemas 3.1 e 3.2, com $q_{F^{IV},0} \geq 3$. Portanto nesses casos o sistema possui uma solução não singular $(mod\ p)$, e consequentemente as equações (3-1) possuem uma solução p-ádica não trivial.

No caso em que temos problema, retornando para a nossa notação anterior a equação (3-9), devemos ter $A_5 \equiv \pm A_6 \ (mod\ 7)$. Se B_5 e B_6 são ambos divisíveis por 7, fixando $X_1 = ... = X_4 = 0$, e dividindo o que restar de F por 7^2, e o que restar de G por 7^t. Nesse caso nós temos um sistema da forma (3-5), e consequentemente uma solução 7-ádica não trivial para as equações (3-1).

Retomando a notação introduzida na equação (3-8), assumindo que B_5 e B_6 não são ambos divisíveis por 7. Suponha também que pelo menos quatro dos b_i são divisíveis por 7, então, sem perda de generalidade, 7 divide $b_1, ..., b_4$. Então fixando $X_1 = ... = X_4 = x_5 ... = x_r = 0$, e substituindo X_i por $p^M X_i$ para $i = 5,6$. Dividindo o que restar de F por 7^{3M+2}, e o que restar de G por 7, nós obtemos um sistema da forma (3-9) com $u+v \geq 3$, $v+w \geq 4$, e $u+v+w \geq 6$. Então, possivelmente fixando uma variável com zero, nós obtemos novamente um sistema da forma (3-5), e consequentemente uma solução 7-ádica não trivial para as equações (3-1).

Então supondo que pelo menos dois dos b_i não são divisíveis por 7 (já que $r \geq 5$), e que pelo menos um entre B_5 e B_6 não é divisível por 7. Fixando $X_1 = ... = X_4 = 0$, por uma mudança de variáveis e uma mudança de notação, nós temos um sistema da forma

$$\begin{aligned} (7^{-2}F^V)^* &= \quad x_1^3 + x_2^3 && \equiv 0 \ (mod\ 7) \\ (G^V)^* &= A_1x_1^2 + a_1x_2^2 \quad + b_1y_1^2 + b_2y_2^2 && \equiv 0 \ (mod\ 7), \end{aligned}$$

onde 7 não divide a_1, b_1 ou b_2. Como para as congruências (3-7), este sistema possui solução não singular $(mod\ 7)$, e consequentemente as equações (3-1) possuem uma solução 7-ádica não trivial.

□

Usando os Lemas 3.1, 3.2 e 3.3 fica provado que para $p > 5$, assumindo a hipótese *(H)* e sujeito a condição $\vartheta(F,G) \neq 0$, o sistema (3-1) possui uma solução p-ádica não trivial sempre que $s \geq 11$. Nos falta provar que *(H)* de fato vale, e que o sistema (3-1) tem solução 2-ádica, 3-ádica e 5-ádica não trivial para $s \geq 11$. Na proxima seção iremos provar *(H)* para p a menos de um número finito deles.

3.2 Soluções não singulares usando somas exponenciais.

Para provar a hipótese *(H)*, que enunciamos na seção anterior, usaremos estimativas do número de soluções não singulares de um sistema da forma

$$\begin{aligned} s(x) = a_1x_1^3 + \cdots + a_5x_5^3 &\equiv 0 \ (mod\ p), \\ r(x) = b_1x_1^2 + \cdots + b_5x_5^2 &\equiv 0 \ (mod\ p), \end{aligned} \tag{3-10}$$

onde no máximo um dos a_1, e no máximo um dos b_i é nulo, e onde a_i e b_i não são nulos simultaneamente. Notemos que o sistema de congruências acima possui solução se, e somente se, $us(x) + vr(x) \equiv 0 \ (mod\ p)$ para quaisquer $w = (u,v)$ em $(\mathbb{Z}/p\mathbb{Z})^2$. Podemos mostrar que

$$\sum_{u,v \ (mod\ p)} e\left(\frac{us(x)+vr(x)}{p}\right) = \begin{cases} p^2 & \text{se } s(x) \equiv r(x) \equiv 0 \ (mod\ p), \\ 0 & \text{c.c.} \end{cases}$$

onde $e(x) = e^{2\pi ix}$.

Somando então sobre todas as quíntuplas $x = (x_1,...,x_5)$, em $(\mathbb{Z}/p\mathbb{Z})^5$ e trocando a ordem dos somatórios, temos que o número N de soluções $(mod\ p)$ das congruências (3-10) é dado pela soma exponencial

$$N = p^{-2} \cdot \sum_{u,v \ (mod\ p)} T_1(u,v) \cdots T_5(u,v), \tag{3-11}$$

onde

$$T_j(u,v) = \sum_{x \ (mod\ p)} e\left(\frac{a_jux^3 + b_jvx^2}{p}\right), \quad j = 1,...5.$$

O termo $(u,v) = (0,0)$ em (3-11) contribui com p^3 para N, que é o número esperado de soluções para as congruências (3-10). Pretendemos mostrar que os termos restantes, juntamente com a soluções singulares, não excedem $p^3 - 1$ em módulo, e dessa forma poderemos garantir que (3-10) possui uma solução não singular.

Antes de proceder com a demonstração do Lema 3.6 que nos dará uma estimativa para o número de soluções de (3-10), vamos apresentar algumas já bem conhecidas estimativas para somas exponenciais. Nos lemas que seguem usaremos por diversas vezes resultados que dizem respeito a teoria de caracteres sobre grupos abelianos finitos, que de forma resumida nada mais é do que homomorfismos do grupo nos números complexos, para mais detalhes teóricos consultar Niederreiter [9] e Schmidt [11].

Lema 3.4 *Sejam*

$$T(u) = \sum_{u \ (mod\ p)} e\left(\frac{ux^3}{p}\right), \qquad e \qquad S(u) = \sum_{u \ (mod\ p)} e\left(\frac{ux^2}{p}\right).$$

Então, quando p for um primo, tal que $p \equiv 1 \ (mod\ 3)$*, nós temos*

$$\begin{aligned}
\sum_{u=1}^{p-1} |T(u)|^2 &= 2p(p-1) \\
\sum_{u=1}^{p-1} |T(u)|^4 &= 6p^2(p-1) \\
\sum_{u=1}^{p-1} |T(u)|^6 &\leq 22p^3(p-1).
\end{aligned}$$

Quando $p \equiv 2 \ (mod\ 3)$*, cada uma dessas somas é zero. Além disso, para qualquer inteiro positivo r e primo* $p > 2$*, nós temos*

$$\sum_{u=1}^{p-1} |S(u)|^{2r} = p^r(p-1).$$

Prova: Suponha que $p \equiv 1 \ (mod\ 3)$, então existem dois caracteres, χ e $\overline{\chi}$ do grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$, diferentes do caracter principal χ_0, tais que $\chi^3 = \overline{\chi}^3 = \chi_0$. Além disso, se $p \nmid y$ temos que o número de soluções em y de

$$y^3 \equiv x \ (mod\ p)$$

é dado por

$$1 + \chi(x) + \overline{\chi}(x),$$

assim para u tal que $p \nmid u$, nós temos

$$\begin{aligned} T(u) &= \sum_{x \pmod p} e\left(\frac{ux^3}{p}\right) \\ &= \sum_{x \pmod p} \left[e\left(\frac{ux}{p}\right)(1+\chi(x)+\overline{\chi}(x)) \right] \\ &= \sum_{x \pmod p} e\left(\frac{ux}{p}\right) + \sum_{x \pmod p} e\left(\frac{ux}{p}\right)\chi(x) + \sum_{x \pmod p} e\left(\frac{ux}{p}\right)\overline{\chi}(x) \\ &= \overline{\chi}(u)\tau(\chi)+\chi(u)\tau(\overline{\chi}), \end{aligned}$$

sendo

$$\tau(\chi') = \sum_{x \pmod p} e\left(\frac{x}{p}\right)\chi'(x),$$

onde χ' um caracter.

Lembremos o fato bem conhecido que a soma de Gauss $\tau(\chi)$, satisfaz $|\tau(\chi)| = \sqrt{p}$, para qualquer caracter χ diferente do caracter principal do grupo $(\mathbb{Z}/p\mathbb{Z})^*$. Temos, então que

$$\begin{aligned} |T(u)|^2 &= T(u)\overline{T(u)} \\ &= (\overline{\chi}(u)\tau(\chi)+\chi(u)\tau(\overline{\chi}))\overline{(\overline{\chi}(u)\tau(\chi)+\chi(u)\tau(\overline{\chi}))} \\ &= 2|\tau(\chi)|^2+\chi(u)\tau(\chi)\overline{\tau(\overline{\chi})}+\overline{\chi(u)}\cdot\overline{\tau(\chi)}\tau(\overline{\chi}). \\ &= 2p+Re\left(\chi(u)\tau(\chi)\overline{\tau(\overline{\chi})}\right), \end{aligned}$$

segue então que

$$\begin{aligned} \sum_{u=1}^{p-1}\left(|T(u)|^2\right) &= \sum_{u=1}^{p-1}\left(2p+Re(\chi(u)\tau(\chi)\overline{\tau(\overline{\chi})})\right) \\ &= 2p(p-1)+Re\left(\tau(\chi)\overline{\tau(\overline{\chi})}\sum_{u=1}^{p-1}\chi(u)\right), \end{aligned}$$

como χ é um caracter diferente do caracter principal do grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$, temos que esse último somatório da zero, logo

$$\sum_{u=1}^{p-1}\left(|T(u)|^2\right) = 2p(p-1).$$

Vamos agora calcular $|T(u)|^4$ usando a expressão de $T(u)$,

$$\begin{aligned} |T(u)|^4 &= (|T(u)|^2)^2 \\ &= (2|\tau(\chi)|^2 + \chi(u)\tau(\chi)\overline{\tau(\overline{\chi})} + \overline{\chi(u)}\cdot\overline{\tau(\chi)}\tau(\overline{\chi}))^2 \\ &= 6p^2 + 8pRe(\chi(u)\tau(\chi)\overline{\tau(\overline{\chi})}) + 2Re(\chi^2(u)\tau^2(\chi)\overline{\tau^2(\overline{\chi})}), \end{aligned}$$

somando sobre u, e observando que χ e $\chi^2 = \overline{\chi}$ são caracteres diferentes do caracter principal, temos que

$$\sum_{u=1}^{p-1} |T(u)|^4 = 6p^2(p-1).$$

Seguindo o mesmo raciocínio, podemos calcular $|T(u)|^6$,

$$\begin{aligned} |T(u)|^6 &= (|T(u)|^2)^3 \\ &= (2|\tau(\chi)|^2 + \chi(u)\tau(\chi)\overline{\tau(\overline{\chi})} + \overline{\chi(u)}\cdot\overline{\tau(\chi)}\tau(\overline{\chi}))^3 \\ &= 20p^3 + 6pRe(\chi(u)\tau(\chi)\overline{\tau(\overline{\chi})}) + 15p^2Re(\chi(u)\tau(\chi)\overline{\tau(\overline{\chi})}) + 2Re(\tau^3(\chi)\overline{\tau^3(\overline{\chi})}) \end{aligned}$$

somando sobre u e aplicando a desigualdade triangular, temos

$$\begin{aligned} \sum_{u=1}^{p-1} |T(u)|^6 &= 20p^3(p-1) + \sum_{u=1}^{p-1} 2Re(\tau^3(\chi)\overline{\tau^3(\overline{\chi})}) \\ &\leq 22p^3(p-1). \end{aligned}$$

uma vez que $|\tau(\chi)| = \sqrt{p}$.

Suponha agora que $p \equiv 2 \ (mod\ 3)$, vamos mostrar que cada um dos somatórios acima são iguais a zero. Para $r \geq 1$, o número de soluções da congruência

$$x_1^3 + \cdots + x_r^3 \equiv y_1^3 + \cdots + y_r^3 \ (mod\ p) \tag{3-12}$$

é dado por

$$\begin{aligned} N &= p^{-1} \sum_{u=0}^{p-1} |T(u)|^{2r}, \\ &= p^{-1} \left(p^{2r} + \sum_{u=1}^{p-1} |T(u)|^{2r} \right), \\ &= p^{2r-1} + p^{-1} \cdot \sum_{u=1}^{p-1} |T(u)|^{2r}. \end{aligned}$$

Mas uma vez que $(3, p-1) = 1$, todo resíduo é resíduo cubico $(mod\ p)$, assim o

número de soluções para a congruência (3-12) é exatamente p^{2r-1}, e resultado segue.

Por fim, se $p > 2$ temos que $(p-1,2) = 2$, logo existe um caracter χ do grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$ diferente do caracter principal, tal que $\chi^2 = \chi_0$. Sendo assim nós temos que o número de soluções em y de $y^2 \equiv x \ (mod \ p)$ é dado por $1+\chi(x)$, assim podemos rescrever $S(u)$ da forma

$$\begin{aligned} S(u) &= \sum_{u \ (mod \ p)} e\left(\frac{ux^2}{p}\right) \\ &= \sum_{u \ (mod \ p)} \left[e\left(\frac{ux}{p}\right)(1+\chi(x))\right] \\ &= \sum_{u \ (mod \ p)} e\left(\frac{ux}{p}\right) + \sum_{u \ (mod \ p)} e\left(\frac{ux}{p}\right)\chi(x) \\ &= \chi(u)\tau(\chi), \end{aligned}$$

onde

$$\tau(\chi) = \sum_{x \ (mod \ p)} e\left(\frac{x}{p}\right)\chi(x).$$

Portanto

$$\begin{aligned} |S(u)|^{2r} &= (S(u)\cdot\overline{S(u)})^r \\ &= (\chi(u)\tau(\chi)\cdot\overline{\chi(u)\tau(\chi)})^r \\ &= |\tau(\chi)|^{2r} \\ &= p^r, \end{aligned}$$

somando sobre u, temos

$$\sum_{u=1}^{p-1} |S(u)|^{2r} = p^r(p-1).$$

□

Aqui mais um resultado bem conhecido que será importante para provar o Lema 3.6.

Lema 3.5 *Seja $f(x) = ax^2+bx+c$, onde a, b e c são números inteiros, e seja p um número primo impar que não divide a. Seja $d = b^2-4ac$ o discriminante de f. Então se denotarmos o símbolo de Legendre por $\left(\frac{\cdot}{p}\right)$, nós temos*

$$\sum_{x=1}^{p}\left(\frac{f(x)}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right), & \text{se p não divide d,} \\ (p-1)\left(\frac{a}{p}\right), & \text{se p divide d.} \end{cases}$$

Prova: Multiplicando o somatório por $\left(\frac{4a^2}{p}\right) = 1$, nós obtemos

$$\begin{aligned}\sum_{x=1}^{p}\left(\frac{f(x)}{p}\right) &= \left(\frac{a}{p}\right)\sum_{x=1}^{p}\left(\frac{4a^2x^2+4abx+4ac}{p}\right)\\ &= \left(\frac{a}{p}\right)\sum_{x=1}^{p}\left(\frac{(2ax+b)^2-d}{p}\right)\\ &= \left(\frac{a}{p}\right)\sum_{y=1}^{p}\left(\frac{y^2-d}{p}\right).\end{aligned}$$

O resultado se $p|d$ agora segue de imediato. Sendo assim suponha que $p \nmid d$, então escrevemos

$$\sum_{y=1}^{p}\left(\frac{y^2-d}{p}\right) = -p+\sum_{y=1}^{p}\left[1+\left(\frac{y^2-d}{p}\right)\right],$$

e como $1+\left(\frac{y^2-d}{p}\right)$ é o número de soluções em w da congruência $w^2 \equiv y^2-d \ (mod\ p)$, nós obtemos,

$$\sum_{y=1}^{p}\left(\frac{y^2-d}{p}\right) = -p+S(d),$$

onde $S(d)$ é o número de pares ordenados (y,w) com $y,w \in \mathbb{Z}/p\mathbb{Z}$ e $y^2-w^2=d$. Para resolver essa equação, nós tomamos $u=y+w$, $v=y-w$ e observamos que os pares (y,w) e (u,v) estão em correspondência biunívoca. Então $S(d)$ é igual ao número de pares ordenados (u,v) com $u,v \in \mathbb{Z}/p\mathbb{Z}$ e $uv=d$, ou seja, $S(d)=p-1$, donde segue o resultado.

□

Agora podemos provar de forma bastante elementar o Lema 3.6, utilizando os Lemas 3.5 e 3.4.

Lema 3.6 *Suponha que $p \neq 2$ e 3 é um número primo. Então o número de soluções, S, do sistema de equações*

$$\begin{aligned}x_1^3+x_2^3 &= y_1^3+y_2^3\\ x_1^2+x_2^2 &= y_1^2+y_2^2\end{aligned} \tag{3-13}$$

sobre $\mathbb{Z}/p\mathbb{Z}$ satisfaz $S \leq 4p^2-5p+2$.

Prova: Suponha que (x_1,x_2,y_1,y_2) satisfazem (3-13), e seja

$$\lambda = x_1+x_2-y_1-y_2. \tag{3-14}$$

Denotamos por $s_k(z) = z_1^k + z_2^k$ para $k \geq 1$. Então notando que

$$\begin{aligned} s_1(z)^3 - 3s_2(z)s_1(z) + 2s_3(z) &= (z_1+z_2)^3 - 3(z_1^2+z_2^2)(z_1+z_2) + 2(z_1^3+z_2^3) \\ &= (z_1+z_2)^3 - z_1^3 - 3z_1^2z_2 - 3z_1z_2^2 - z_2^3 \\ &= 0, \end{aligned}$$

é fácil ver que

$$(\lambda + s_1(y))^3 - 3s_2(y)(\lambda + s_1(y)) + 2s_3(y) = s_1(x)^3 - 3s_2(y)s_1(x) + 2s_3(y),$$

porém por (3-13) $s_2(y) = s_2(x)$ e $s_3(y) = s_3(x)$, donde

$$(\lambda + s_1(y))^3 - 3s_2(y)(\lambda + s_1(y)) + 2s_3(y) = 0.$$

Se as equações (3-13) possuem uma solução, então λ deve satisfazer a equação cúbica

$$\begin{aligned} 0 &= (\lambda + s_1(y))^3 - 3s_2(y)(\lambda + s_1(y)) + 2s_3(y) \\ 0 &= \lambda^3 + 3\lambda^2 s_1(y) + 3\lambda s_1^2(y) + s_1^3(y) - 3s_2(y)s_1(t) - 3\lambda s_2(y) + 2s_3(y) \\ 0 &= \lambda^3 + 3\lambda^2 s_1(y) + 3\lambda(s_1^2(y) - s_2(y)) \\ 0 &= \lambda(\lambda^2 + 3\lambda(y_1+y_2)6y_1y_2). \end{aligned} \tag{3-15}$$

e para isso existem dois caso:

(i) $\lambda = 0$. Então nós temos por (3-14) que $x_1 + x_2 = y_1 + y_2$, e por (3-13) e (3-14) que $x_1x_2 = y_1y_2$. Sendo assim para qualquer $s \in \mathbb{Z}/p\mathbb{Z}$,

$$(s - x_1)(s - x_2) = (s - y_1)(s - y_2).$$

Logo $(x_1 - y_1)(x_1 - y_2) = 0$, e consequentemente ou $x_1 = y_1$, ou $x_1 = y_2$. Assim $\lambda = 0$ dá exatamente duas soluções para (3-13) e (3-14) para cada par (y_1, y_2) em $\mathbb{Z}/p\mathbb{Z}^2$ com $y_1 \neq y_2$, a saber $(x_1, x_2) = (y_1, y_2)$ e $(x_1, x_2) = (y_2, y_1)$. Mas quando $y_1 = y_2$, nós claramente temos a solução única $x_1 = x_2 = y_1$, então o número total de soluções distintas correspondentes à $\lambda = 0$ é $2p(p-1) + p = 2p^2 - p$.

(ii) $\lambda \neq 0$. Então por (3-15), λ satisfaz

$$\lambda^2 + 3\lambda(y_1 + y_2) + 6y_1y_2 = 0. \tag{3-16}$$

Para um dado (y_1, y_2), o número de soluções em λ dessa equação quadrática é

$1+\left(\frac{\Delta}{p}\right)$, onde $\Delta = 9y_1^2 - 6y_1y_2 + 9y_2^2$ é o discriminante da equação quadrática em (3-16). Então o número, T, de triplas (y_1, y_2, λ) satisfazendo (3-16) é

$$\sum_{y_1=1}^{p}\sum_{y_2=1}^{p}\left[\left(\frac{9y_1^2-6y_1y_2+9y_2^2}{p}\right)+1\right] = p^2 + \sum_{y_1=1}^{p}\sum_{y_2=1}^{p}\left(\frac{9y_1^2-6y_1y_2+9y_2^2}{p}\right).$$

Fixemos y_1 e consideremos $9y_1^2 - 6y_1y_2 + 9y_2^2$ como uma equação quadrática em y_2 tendo discriminante $-288y_1^2$, que é divisível por p se, e somente se, $p = 2$ ou 3, ou se p dividi y_1. Então usando o Lema 3.5, nós deduzimos que

$$\sum_{y_1=1}^{p}\sum_{y_2=1}^{p}\left(\frac{9y_1^2-6y_1y_2+9y_2^2}{p}\right) = \sum_{y_1=1}^{p-1}\left[-\left(\frac{9}{p}\right)\right] + (p-1)\left(\frac{9}{p}\right) = 0$$

Ou seja $T = p^2$. Mas $\lambda = 0$ é uma solução (3-16) sempre que p dividi $6y_1y_2$, que é quando $y_1 = p$ ou $y_2 = p$, e nós já contamos as soluções com $\lambda = 0$. Então o número de triplas (y_1, y_2, λ) satisfazendo (3-15) com $\lambda \neq 0$ é $p^2 - (2p-1)$.

Dada uma tripla (y_1, y_2, λ), substituindo (3-14) na equação quadrática (3-13). Nós deduzimos que x_2 satisfaz a equação quadrática

$$2y_1y_2 + 2\lambda(y_1+y_2) + \lambda^2 + 2x_2^2 = 2x_2(y_1+y_2+\lambda). \tag{3-17}$$

Dada uma solução x_2 para (3-17) , x_1 está determinado unicamente por (3-13), então para cada tripla (y_1, y_2, λ), existem no máximo dois pares (x_1, x_2) satisfazendo (3-13) e (3-14).

O número total de soluções para a equação (3-14) é dessa forma limitado por

$$S \leq 2(p^2 - 2p + 1) + 2p^2 - p = 4p^2 - 5p + 2.$$

□

Um resultado imediato que diz o que estamos interessados de fato é o corolário.

Corolário 3.7 *Escrevendo*

$$T(u,v) = \sum_{x \bmod p} e\left(\frac{ux^3+vx^2}{p}\right),$$

nós temos

$$p^{-2}\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T(u,v)|^4 \leq \begin{cases} 3p^2-12p+9, & \text{se } 3|(p-1), \\ 3p^2-6p+3, & \text{se } 3|(p-2). \end{cases}$$

Prova: A soma exponencial

$$p^{-2}\sum_{u=0}^{p-1}\sum_{v=0}^{p-1}|T(u,v)|^4,$$

é o número de soluções do sistema de congruências

$$\begin{aligned} x_1^3+x_2^3 &\equiv x_3^3+x_4^3 \ (mod\ p),\\ x_1^2+x_2^2 &\equiv x_3^2+x_4^2 \ (mod\ p), \end{aligned}$$

que é limitado superiormente por $4p^2-5p+2$ pelo Lema 3.6. Além disso, pelo Lema 3.4, temos que

$$\sum_{u=0}^{p-1}\sum_{v=0}^{p-1}|T(u,v)|^4=|T(0,0)|^4+\sum_{u=1}^{p-1}|T(u,0)|^4+\sum_{v=1}^{p-1}|T(0,v)|^4+\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T(u,v)|^4,$$

onde

$$p^{-2}\left(|T(0,0)|^4+\sum_{u=1}^{p-1}|T(u,0)|^4+\sum_{v=1}^{p-1}|T(0,v)|^4\right)=\begin{cases} p^2+7(p-1),\ 3|(p-1),\\ p^2+(p-1),\ 3|(p-2). \end{cases}$$

Então

$$p^{-2}\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T(u,v)|^4\leq\begin{cases} 3p^2-12p+9,\ \text{se } 3|(p-1),\\ 3p^2-6p+3,\ \text{se } 3|(p-2). \end{cases}$$

□

Agora podemos estimar o número de soluções da congruência (3-10), esta estimativa será dividida em quatro partes, como mostra o resultado a seguir, provando este resultado ainda teremos que estimar o número de soluções singulares, então poderemos garantir a existência de solução não singular.

Lema 3.8 *Nós temos:*

(i) se nenhum a_i assim como nenhum b_i é igual a zero, então

$$|N-p^3|\leq\begin{cases} 6p^{\frac{5}{2}}+(2\cdot 33^{\frac{1}{2}}-23)p^{\frac{3}{2}}+(17-2\cdot 33^{\frac{1}{2}})p^{\frac{1}{2}}, & 3|(p-1),\\ 6p^{\frac{5}{2}}-11p^{\frac{3}{2}}+5p^{\frac{1}{2}}, & 3|(p-2); \end{cases}$$

(ii) se existe um i tal que a_i é zero, mas nenhum b_j é igual a zero, então

$$|N-p^3| \leq \begin{cases} 3p^{\frac{5}{2}} - 11p^{\frac{3}{2}} + 8p^{\frac{1}{2}} + 6p^2 - 6p, & 3|(p-1)), \\ 3p^{\frac{5}{2}} - 5p^{\frac{3}{2}} + 2p^{\frac{1}{2}}, & 3|(p-2); \end{cases}$$

(iii) se existe um i tal que b_i é zero, mas nenhum a_j é igual a zero, então

$$|N-p^3| \leq \begin{cases} 6p^{\frac{5}{2}} + (2\cdot 33^{\frac{1}{2}} - 24)p^{\frac{3}{2}} + (18 - 2\cdot 33^{\frac{1}{2}})p^{\frac{1}{2}} + p^2 - p, & 3|(p-1), \\ 6p^{\frac{5}{2}} - 12p^{\frac{3}{2}} + 6p^{\frac{1}{2}} + p^2 - p, & 3|(p-2); \end{cases}$$

(iv) se existe um i tal que a_i é zero, e um $j \neq i$ tal que b_j é zero, então

$$|N-p^3| \leq \begin{cases} (12p^5 - 96p^4 + 263p^3 - 288p^2 + 108p)^{\frac{1}{2}} + 7p^2 - 7p, & 3|(p-1), \\ (12p^5 - 48p^4 + 72p^3 - 48p^2 + 12p)^{\frac{1}{2}} + p^2 - p, & 3|(p-2). \end{cases}$$

Prova: Separando os termos principais e renomeando, nós obtemos

$$\begin{aligned} N-p^3 &= p^{-2}\left(\sum_{u=1}^{p-1}\sum_{v=1}^{p-1} T_1(u,v)\cdots T_5(u,v)\right) + p^{-2}\left(\sum_{v=1}^{p-1} T_1(0,v)\cdots T_5(0,v)\right) \\ &\quad + p^{-2}\left(\sum_{u=1}^{p-1} T_1(u,0)\cdots T_5(u,0)\right) \\ &= S_1 + S_2 + S_3. \end{aligned}$$

Existem quatro casos.

(i) Nenhum a_i assim com nenhum b_i é iguais zero. Então pela desigualdade de Hölder,

$$\begin{aligned} |S_1| &= p^{-2}\left|\sum_{u=1}^{p-1}\sum_{v=1}^{p-1} T_1(u,v)\cdots T_5(u,v)\right| \\ &\leq p^{-2}\prod_{i=1}^{5}\left(\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T_i(u,v)|^5\right)^{\frac{1}{5}} \\ &\leq p^{-2}\left(\sup_{(u,v)}|T_I(u,v)|\right)\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T_I(u,v)|^4, \end{aligned}$$

para algum I em $\{1,...,5\}$, onde o *sup* é sobre $u \neq 0$ e $v \neq 0$. Pela Hipótese de Riemann para corpos finitos (ver Schmidt [11]), temos para qualquer polinômio $f(x)$ de grau k com

coeficientes inteiros, tal que p não dividi o conteúdo de $f(x)-f(0)$, a estimativa

$$\left| \sum_{x \pmod p} e\left(\frac{f(x)}{p}\right) \right| \leq (k-1)p^{\frac{1}{2}}.$$

Usando esta estimativa, fazendo uma mudança de variáveis, e aplicando o Corolário 3.7, nós obtemos

$$|S_1| \leq \begin{cases} 6p^{\frac{5}{2}} - 24p^{\frac{3}{2}} + 18p^{\frac{1}{2}} & \text{se } 3|(p-1), \\ 6p^{\frac{5}{2}} - 12p^{\frac{3}{2}} + 6p^{\frac{1}{2}} & \text{se } 3|(p-2). \end{cases}$$

Por um argumento similar ao dado acima, existe um J tal que

$$\begin{aligned} |S_2| &= p^{-2} \left| \sum_{v=1}^{p-1} T_1(0,v) \cdots T_5(0,v) \right| \\ &\leq p^{-2} \prod_{i=1}^{5} \left(\sum_{v=1}^{p-1} |T_i(0,v)|^5 \right)^{\frac{1}{5}} \\ &\leq p^{-2} \sum_{v=1}^{p-1} |T_J(0,v)|^5, \end{aligned}$$

Pelo Lema 3.4 e pela desigualdade de Cauchy, fazendo uma mudança de variáveis, temos

$$|S_2| \leq p^{\frac{1}{2}}(p-1).$$

Aqui novamente como feito para $|S_1|$ e $|S_2|$, existe K tal que

$$|S_3| \leq p^{-2} \cdot \sum_{u=1}^{p-1} |T_K(u,0)|^5.$$

Se $p \equiv 2 \pmod 3$, então o somatório é zero. Caso contrário, pela desigualdade de Cauchy e o Lema 3.4,

$$\begin{aligned} |S_3| &\leq p^{-2} \cdot \left(\sum_{u=1}^{p-1} |T_K(u,0)|^6 \right)^{\frac{1}{2}} \left(\sum_{u=1}^{p-1} |T_K(u,0)|^4 \right)^{\frac{1}{2}} \\ &\leq p^{-2} (22p^3(p-1) \cdot 6p^2(p-1))^{\frac{1}{2}} \\ &= 2 \cdot 33^{\frac{1}{2}} p^{\frac{1}{2}} (p-1). \end{aligned}$$

O resultado agora segue somando as estimativas acima para $|S_1|$, $|S_2|$ e $|S_3|$.

(ii) Existe um i tal que a_i é zero, mas nenhum b_j é igual a zero. Reagrupando

variáveis, podemos supor que $a_1 = 0$. Então pela desigualdade de Hölder e pela Hipótese de Riemann para corpos finitos,

$$\begin{aligned}\left|\sum_{u=1}^{p-1}\sum_{v=1}^{p-1} T_1(u,v)\cdots T_5(u,v)\right| &\leq \left(\sup_{(u,v)}|T_I(u,v)|\right)\prod_{i=2}^{5}\left(\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T_i(u,v)|^4\right)^{\frac{1}{2}} \\ &\leq p^{\frac{1}{2}}\cdot\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T_I(u,v)|^4\end{aligned}$$

para algum $I \in \{2,...,5\}$. Fazendo uma mudança de variáveis e usando o Corolário 3.7, concluímos novamente que

$$|S_1| \leq \begin{cases} 3p^{\frac{5}{2}} - 12p^{\frac{3}{2}} + 9p^{\frac{1}{2}} & \text{se } 3|(p-1), \\ 3p^{\frac{5}{2}} - 6p^{\frac{3}{2}} + 3p^{\frac{1}{2}} & \text{se } 3|(p-2). \end{cases}$$

Também, de forma similar a que foi feita em *(i)*, temos

$$|S_2| \leq p^{\frac{1}{2}}(p-1),$$

e notando que $T_1(u,0) = p$, segue que

$$|S_3| \leq p^{-2}\left(p\cdot\sum_{u=1}^{p-1}|T_K(u,0)|^4\right),$$

para algum K, e consequentemente,

$$|S_3| \begin{cases} \leq 6p(p-1) & \text{se } 3|(p-1), \\ = 0 & \text{se } 3|(p-2). \end{cases}$$

O resultado agora segue somando as estimativas acima para $|S_1|$, $|S_2|$ e $|S_3|$.

(iii) Existe um i tal que b_i é zero, mas nenhum a_j é igual a zero. Procedendo de forma similar a que foi feita em *(i)* e *(ii)*,

$$|N - p^3| \leq \begin{cases} 6p^{\frac{5}{2}} + (2\cdot 33^{\frac{1}{2}} - 24)p^{\frac{3}{2}} + (18 - 2\cdot 33^{\frac{1}{2}})p^{\frac{1}{2}} + p^2 - p, & 3|(p-1), \\ 6p^{\frac{5}{2}} - 12p^{\frac{3}{2}} + 6p^{\frac{1}{2}} + p^2 - p, & 3|(p-2). \end{cases}$$

(iv) Existe um i tal que a_i é zero, e um j tal que b_j é zero. Reagrupando variáveis podemos supor que $a_1 = 0$ e que $b_2 = 0$. Temos mais uma vez que

$$p^{-2}\cdot\left|\sum_{u=1}^{p-1}\sum_{v=1}^{p-1} T_1 1(u,v)\cdots T_5(u,v)\right| \leq (2p^{\frac{1}{2}})\cdot(p^{\frac{1}{2}})\cdot p^{-2}\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}|T_I(W)|^3,$$

para algum I, e consequentemente, pela desigualdade de Cauchy

$$|S_1| \leq 2p \left(p^{-2} \cdot \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} |T_I(u,v)|^2 \right)^{\frac{1}{2}} \left(p^{-2} \cdot \sum_{u=1}^{p-1} \sum_{v=1}^{p-1} |T_I(u,v)|^4 \right)^{\frac{1}{2}}. \tag{3-18}$$

Mas

$$p^{-2} \cdot \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} |T_I(u,v)|^2$$

é o número de soluções do sistema de congruências

$$\begin{aligned} a_1 x_1^3 &\equiv a_1 x_2^3 \ (mod\ p) \\ b_1 x_1^2 &\equiv b_1 x_2^2 \ (mod\ p), \end{aligned}$$

que é claramente p, consequentemente a_I e b_I são ambos não nulos. Então usando o Lema 3.4, nós deduzimos que

$$\sum_{u=1}^{p-1} \sum_{v=1}^{p-1} |T_I(u,v)|^2 = \begin{cases} p^3 - p^2 - 2p(p-1) - p(p-1) & \text{se } 3|(p-1), \\ p^3 - p^2 - p(p-1) & \text{se } 3|(p-2). \end{cases}$$

Como em *(i)* e *(ii)*,

$$|S_2| \leq p(p-1),$$

e

$$|S_3| \begin{cases} \leq 6p(p-1) & \text{se } 3|(p-1), \\ = 0 & \text{se } 3|(p-2). \end{cases}$$

O resultado agora segue somando nossas estimativas para $|S_1|$, $|S_2|$ e $|S_3|$.

□

Antes de estimarmos o número de soluções singulares para as congruências (3-10), nós precisamos de um lema contando o número de soluções para um certo problema de partição. Embora a estimativa trivial seja adequada para o que queremos, o argumento elegante de R. C. Vaughan que segue nos dá uma resposta mais precisa.

Lema 3.9 *Sejam* $\alpha_1, ..., \alpha_{2k}$ *resíduos* $(mod\ q)$*, e* $N(q;\alpha)$ *o número de escolhas de* $\varepsilon_1, ..., \varepsilon_{2k}$*, com* $\varepsilon = 1$ *ou 0, tal que*

$$\sum_{i=1}^{2k} \varepsilon_i x_i \equiv 0 \ (mod\ q).$$

Se $(q,\alpha_i)=1$ *para todo i, e* $q>k$, *então*

$$N(q;\alpha)\leq\binom{2k}{k}.$$

Fixando

$$\gamma_i\begin{cases}1 & \text{para } 1\leq i\leq k,\\ -1 & \text{para } k+1\leq i\leq 2k,\end{cases}$$

temos $N(q;\gamma)=\binom{2k}{k}$.

Prova: Seja

$$S(\beta)=\sum_{\varepsilon=0}^{1}e(\varepsilon\beta).$$

Então,

$$\begin{aligned}N(q;\alpha) &= \sum_{\varepsilon_1=0}^{1}\cdots\sum_{\varepsilon_{2k}=0}^{1}q^{-1}\sum_{r=1}^{q}e\left(\frac{r}{q}\sum_{i=1}^{2k}\varepsilon_i\alpha_i\right)\\ &= q^{-1}\sum_{r=1}^{q}\prod_{i=1}^{2k}S\left(\frac{r\alpha_i}{q}\right)\\ &\leq \prod_{i=1}^{2k}\left(q^{-1}\sum_{r=1}^{q}\left|S\left(\frac{r\alpha_i}{q}\right)\right|^{2k}\right)^{1/(2k)},\end{aligned}$$

pela desigualdade de Hölder. Daí, por uma mudança de variáveis,

$$N(q;\alpha)\leq N(q;\gamma)=\sum_{j=0}^{k}\binom{k}{j}^2=\binom{2k}{k}.$$

□

Corolário 3.10 *Sejam* $\alpha_1,\ldots,\alpha_{2k+1}$ *resíduos* (mod q), *e seja* $N(q;\alpha)$ *o número de escolhas de* $\varepsilon_1,\ldots,\varepsilon_{2k+1}$, *com* $\varepsilon_i=0$ *ou* 1, *tal que*

$$\sum_{i=1}^{2k+1}\varepsilon_i\alpha_i\equiv 0\ (mod\ q).$$

Se $(q,\alpha_i)=1$ *para todo i, e* $q>k+1$, *então*

$$N(q;\alpha)\leq\left(\frac{2k+2}{2k+1}\right)^{\frac{1}{2}}\binom{2k+1}{k}.$$

prova: Assim como na prova do Lema 3.9,

$$N(q;\alpha_1,...,\alpha_{2k+1}) = q^{-1}\cdot\sum_{r=1}^{q}\prod_{i=1}^{2k+1} S\left(\frac{r\alpha_i}{q}\right),$$

então pela desigualdade de Hölder,

$$N(q;\alpha) \leq \prod_{i=1}^{2k+1}\left(\left(q^{-1}\cdot\sum_{r=1}^{q}\left|S\left(\frac{r\alpha_i}{q}\right)\right|^{2k+2}\right)^{\frac{1}{2}}\left(q^{-1}\cdot\sum_{r=1}^{q}\left|S\left(\frac{r\alpha_i}{q}\right)\right|^{2k}\right)^{\frac{1}{2}}\right)^{\frac{1}{2k+1}}.$$

Então por uma mudança de variáveis e usando o Lema 3.9, nós temos

$$N(q;\alpha) \leq \left(\binom{2k+2}{k+1}\binom{2k}{k}\right)^{\frac{1}{2}}.$$

□

Devemos notar que para n resíduos $\alpha_1,...,\alpha_n$, e $q > \frac{1}{2}(n+1)$ satisfazendo $(q,\alpha_i) = 1$ para todo i, nós esperamos que $N(q;\alpha) \leq \binom{n}{\lfloor\frac{1}{2}n\rfloor}$.

Lema 3.11 *Suponha que $p \neq 2,3$. Então o número de soluções singulares distintas da congruência (3-10) é no máximo*

(i) $9p-8$ *se nenhum dos a_i, e nenhum dos b_i é igual a zero,*

(ii) $5p-4$ *se existe um i tal que ou $a_i \equiv 0$ ou $b_i \equiv 0$, mas não existem i e j, com $i \neq j$, e $a_i \equiv b_j \equiv 0$,*

(iii) $2p-1$ *se existe um i tal que a_i é zero, e um j tal que b_j é zero.*

Prova: Suponha que $(\alpha_1,...,\alpha_5)$ é uma solução da congruência (3-10) que é singular $(mod\ p)$. Suponha também que precisamente v dos α_i são não nulos, podemos reordenar variáveis de forma que $\alpha_i \not\equiv 0$ para $i = 1,...,v$. Claramente, como a_i e b_i não são simultaneamente nulos, nós temos $v = 0$ ou $v \geq 2$. Uma vez que α é uma solução singular e $p \neq 2,3$, nós devemos ter para quaisquer $i,j \in \{1,...,5\}$,

$$\alpha_i\alpha_j(a_ib_j\alpha_i - a_jb_i\alpha_j) \equiv 0\ (mod\ p),$$

e assim $a_ib_j\alpha_i \equiv a_jb_i\alpha_j\ (mod\ p)$ para todo $i,j \in \{1,...,v\}$. Suponha que $v \geq 2$. Existem dos casos

(i) Não existe $i \in \{1,...,v\}$ tal que ou $a_i \equiv 0$ ou $b_i \equiv 0$. Então

$$\alpha_j \equiv \begin{cases} \dfrac{a_1 b_j}{b_1 a_j}\alpha_1 & \text{para } j = 1,...,v, \\ 0 & \text{para } j = v+1,...,5. \end{cases}$$

Existem então $p-1$ soluções não triviais, tomando $\alpha_1 \equiv 1,...,p-1$.

(ii) Existem $i, j \in \{1,...,v\}$ tais que $a_i \equiv 0$ ou $b_j \equiv 0$. Então nós podemos encontrar $i, j \in \{1,...,v\}$ tal que a_j e b_i são ambos não nulos, mas $a_j b_i \alpha_j \equiv a_i b_j \alpha_i \equiv 0 \ (mod\ p)$. Então $\alpha_j \equiv 0$, o que é uma contradição.

Então nós concluímos que *i)* vale sempre que $v \neq 0$, e por

$$\begin{aligned} a_1\alpha_1^3 + \cdots + a_5\alpha_5^3 &\equiv 0 \ (mod\ p), \\ b_1\alpha_1^2 + \cdots + b_5\alpha_5^2 &\equiv 0 \ (mod\ p), \end{aligned}$$

nós obtemos

$$\left(\frac{b_1^3}{a_1^2} + \cdots + \frac{b_v^3}{a_v^2}\right)\alpha_1^3 \equiv 0 \ (mod\ p).$$

Reordenando as variáveis de modo que $a_1 \not\equiv 0$ e $b-i \not\equiv 0$ para $i = 1,...,n$, e ou $a_i \equiv 0$ ou $b_i \equiv 0$ para $n < i \leq 5$. Seja $\beta \equiv\ b_i^3/a_i^2$ para $i = 1,...,n$. Usando a notação do Lema 3.9, podemos ver que pelo menos $N(p;\beta)$ congruências distintas da forma

$$\beta_{i_1} + \cdots + \beta_{i_t} \equiv 0 \ (mod\ p),$$

com $1 \leq i_1 < \cdots < i_t \leq n$ e $0 \leq t \leq n$, e $0 \leq t \leq n$ uma das quais é a congruência trivial. Para cada congruência não trivial, nós temos $p-1$ soluções não singulares (dadas pelos $p-1$ valores não nulos de α_1). Então, pelo Corolário 3.10 (notando que $N(p;\beta)$ é um número inteiro), nós observamos que o número de soluções singulares, incluindo 0, para a congruência (3-10) é no máximo

(i) $(10-1)(p-1)+1 = 9p-8$ se nenhum dos a_i e nenhum dos b_i é igual a 0.

(ii) $(6-1)(p-1)+1 = 5p-4$ se existe um i tal que ou $a_i \equiv 0$ ou $b_i \equiv 0$, mas não existe $j \neq i$, com $a_i \equiv b_j \equiv 0$.

(iii) $(3-1)(p-1)+1 = 2p-1$ se existem i e j tais que $a_i \equiv b_j \equiv 0$.

□

Finalmente temos que pelos Lemas 3.11 e 3.8 o número, N^* de soluções não singulares $(mod\ p)$ para a congruência (3-10), satisfaz $|N^* - p^3| \leq E$, onde E satisfaz:

(i) se nenhum a_i assim como nenhum b_i é igual a zero, então

$$E \leq \begin{cases} 6p^{\frac{5}{2}} + (2\cdot 33^{\frac{1}{2}} - 23)p^{\frac{3}{2}} + (17 - 2\cdot 33^{\frac{1}{2}})p^{\frac{1}{2}} + 9p - 8, & 3|(p-1), \\ 6p^{\frac{5}{2}} - 11p^{\frac{3}{2}} + 5p^{\frac{1}{2}} + 9p - 8, & 3|(p-2); \end{cases}$$

(ii) se existe um i tal que a_i é zero, mas nenhum b_j é igual a zero, então

$$E \leq \begin{cases} 3p^{\frac{5}{2}} - 11p^{\frac{3}{2}} + 8p^{\frac{1}{2}} + 6p^2 - 6p - p - 4, & 3|(p-1), \\ 3p^{\frac{5}{2}} - 5p^{\frac{3}{2}} + 2p^{\frac{1}{2}} + 5p - 4, & 3|(p-2); \end{cases}$$

(iii) se existe um i tal que b_i é zero, mas nenhum a_j é igual a zero, então

$$E \leq \begin{cases} 6p^{\frac{5}{2}} + (2\cdot 33^{\frac{1}{2}} - 24)p^{\frac{3}{2}} + (18 - 2\cdot 33^{\frac{1}{2}})p^{\frac{1}{2}} + p^2 + 4p - 4, & 3|(p-1), \\ 6p^{\frac{5}{2}} - 12p^{\frac{3}{2}} + 6p^{\frac{1}{2}} + p^2 + 4p - 4, & 3|(p-2); \end{cases}$$

(iv) se existe um i tal que a_i é zero, e um $j \neq i$ tal que b_j é zero, então

$$E \leq \begin{cases} (12p^5 - 96p^4 + 263p^3 - 288p^2 + 108p)^{\frac{1}{2}} + 7p^2 - 7p, & 3|(p-1), \\ (12p^5 - 48p^4 + 72p^3 - 48p^2 + 12p)^{\frac{1}{2}} + p^2 - p, & 3|(p-2). \end{cases}$$

Agora podemos facilmente verificar que a desigualdades *(i)-(iv)* implicam que $|N^* - p^3| < p^3$ para todos número primo satisfazendo:

$$\text{quando nenhum } a_i \text{ é igual a zero} \begin{cases} p > 31 & \text{se } 3|(p-1), \\ p > 29 & \text{se } 3|(p-2); \end{cases}$$

$$\text{quando um } a_i \text{ é igual a zero} \begin{cases} p > 13 & \text{se } 3|(p-1), \\ p > 5 & \text{se } 3|(p-2). \end{cases}$$

Ou seja, para todos os números primos, exceto possivelmente

$$\begin{cases} \text{quando nenhum dos } a_i \text{ é zero}, & 2,3,5,7,11,13,17,19,23,29,31, \\ \text{quando um } a_i \text{ é zero}, & 2,3,5,7,13. \end{cases}$$

o sistema de congruências (3-10) possui uma solução que não é singular $(mod\ p)$.

3.3 Algumas demonstrações diretas do teorema para os primos 2, 3 e congruentes a $5\ (mod 12)$.

Nas seções anteriores estudamos os pares de formas de graus 2 e 3 passando a um sistema p-normalizado, garantindo solução não singular $(mod\ p)$, e aplicando o Lema de Hensel para garantir solução não trivial em $\mathbb{Z}_p$, com esse método conseguimos provar o resultado principal, a menos de um número finito de primos, que estão listados no final da seção 3.2, nessa seção vamos provar que para alguns primos p em particular, podemos provar que $\Gamma_p(3,2) \leq 11$ de uma forma mais direta, encontrando explicitamente soluções para o sistema em função dos seus coeficientes. Com isso diminuiremos ainda mais a lista de números de primos restantes para a demonstração final do resultado. Nessa direção trataremos primeiramente os primos p tais que $p \equiv 5\ (mod\ 12)$.

Lema 3.12 $\Gamma_p(3,2) \leq 11$ *para todo primo p, tal que* $p \equiv 5\ (mod\ 12)$.

Prova: Vamos começar fazendo algumas considerações que serão importantes na demonstração, primeiramente se $p \equiv 5\ (mod\ 12)$, então -1 é um resíduo quadrático $(mod\ p)$, e qualquer $a \in \mathbb{Z}/p\mathbb{Z}$ não nulo é um resíduo cúbico $(mod\ p)$. Considere um sistema da forma (3-1) em $s \geq 11$ variáveis.

Suponha que c não é resíduo quadrático $(mod\ p)$, e seja $K = \{0,1,c,p,pc\}$. Para qualquer $b \in \mathbb{Z}_p/\{0\}$ existem $u \in \mathbb{Z}_p$, e $\delta \geq 0 \in \mathbb{Z}$, tais que, $b = p^{\delta}u$, onde $u \equiv u_0 \not\equiv 0\ (mod\ p)$, sendo assim nós podemos encontrar $g \in K/\{0\}$ e $x_0 \in \mathbb{Z}_p$ tais que $gx_0^2 - b \equiv 0\ (mod\ p^{\delta+1})$, mas $(2gx_0)^2 \not\equiv 0\ (mod\ p^{\delta+1})$, onde

$$g = \begin{cases} 1, & \text{se } u_0 \text{ é resíduo quadrático e } \delta+1 \text{ é par;} \\ p, & \text{se } u_0 \text{ é resíduo quadrático e } \delta+1 \text{ é ímpar;} \\ c, & \text{se } u_0 \text{ não é resíduo quadrático e } \delta+1 \text{ é par;} \\ pc, & \text{se } u_0 \text{ não é resíduo quadrático e } \delta+1 \text{ é ímpar,} \end{cases}$$

logo o polinômio $f(x) = gx^2 - b$ é tal que $\|f(x_0)\|_p < \|f'(x_0)\|_p^2$, e pelo Lema de Hensel existe um $a \in \mathbb{Z}_p/\{0\}$ tal que $b = ga^2$.

Considere agora um sistema da forma (3-1) em $s \geq 11$ variáveis, das observações feitas acima podemos dividir o conjunto $\{1,...,s\}$ em cinco subconjuntos dependendo dos coeficientes d_i de G, a saber

$$\mathfrak{U}_g = \{i : d_i = ga^2 \text{ para algum } a \in \mathbb{Z}_p/\{0\}\} \qquad (g \in K),$$

assim temos que

$$\sum_{g\in K}|\mathfrak{U}_g| = s.$$

Seja M o número de $g \in K/\{0\}$ tais que $\mathfrak{U}_g \neq \varnothing$. Então $M \leq 4$, escrevendo $[x]$ para denotar a parte inteira de x, temos que

$$\begin{aligned}
|\mathfrak{U}_0| + \sum_{g\in K/\{0\}}\left[\frac{1}{2}|\mathfrak{U}_g|\right] &\geq |\mathfrak{U}_0| + \sum_{\substack{g\in K/\{0\},\\ \mathfrak{U}_g\neq\varnothing.}}\frac{1}{2}(|\mathfrak{U}_g|-1)\\
&\geq \frac{1}{2}\sum_{g\in K}|\mathfrak{U}_g| - \frac{1}{2}M\\
&\geq \frac{1}{2}(s-4)\\
&\geq 4.
\end{aligned}$$

Então reordenando as variáveis de modo que para $i = 1,2,3,4$, ou $2i-1, 2i \in \mathfrak{U}_q$ para algum $q \in K/\{0\}$, ou então $2i-1 \in \mathfrak{U}_0$. Nesse último caso $d_{2i-1}x^2 + d_{2i}y^2 = 0$ possui a solução não trivial $(1,0)$. No primeiro caso $d_{2i-1}x^2 + d_{2i}y^2 = q((ax)^2 + (by)^2)$ com $a,b \in \mathbb{Z}_p/\{0\}$, e temos a solução não singular $(x,y) = (\rho b, a)$, onde ρ satisfaz $\rho^2 = -1$ que existe pelo Lema de Hensel, pois é possível encontrar ρ' tal que $\rho'^2 \equiv -1 \ (mod\ p)$. Então escrevemos

$$G = (d_1x_1^2 + d_2x_2^2) + \cdots + (d_7x_7^2 + d_8x_8^2) + d_9x_9^2 + \cdots + d_sx_s^2,$$

onde podemos zerar as expressões entre parênteses tomando $(x_{2i-1}, x_{2i}) = (a_{2i-1}, a_{2i})$, sendo as escolhas de (a_{2i-1}, a_{2i}) feitas de forma conveniente, de acordo com as observações feitas acima. Fixamos $a_9 = ... = a_s = 0$, e para $i = 1,2,3,4$ tomamos

$$C_i = c_{2i-1}a_{2i-1}^3 + c_{2i}a_{2i}^3.$$

Como $p \equiv 2 \ (mod\ 3)$, todo resíduo é resíduo cúbico $(mod\ p)$, então é um exercício simples de Lema de Hensel, semelhante as considerações feitas no começo da demonstrar, mostrar que para cada i, existem um $g \in L = \{0,1,p,p^2\}$ e um $a \in \mathbb{Z}_p$ tal que $C_i = ga^3$ (para mais detalhes veja, por exemplo, Cassels [1] Capítulo 4, Lema 3.4).

Considere a equação

$$C_1X_1^3 + C_2X_2^3 + C_3X_3^3 + C_4X_4^3 = 0 \quad \text{sobre } \mathbb{Z}_p. \tag{3-19}$$

Se algum dos C_i é zero, então temos a solução não trivial $X_i = 1$, e $X_j = 0$ se $j \neq i$. Então podemos assumir que nenhum dos C_i é igual a zero, e consequentemente que existe um reordenamento de variáveis tal que $C_1 = ga^3$ e $C_2 = gb^3$ com $a,b \in \mathbb{Z}_p$ e

$g \in L/\{0\}$. Então (3-19) possui a solução não singular

$$(X_1,...,X_4) = (b,-a,0,0).$$

Em ambos os casos a equação (3-19) possui uma solução não trivial $(b_1,...,b_4)$ sobre $\mathbb{Z}_p$, e consequentemente o sistema (3-1) possui a solução não trivial

$$(x_1,...,x_s) = (a_1b_1,a_2b_1,a_3b_2,a_4b_2,a_5b_3,a_6b_3,a_7b_4,a_8b_4,0,...,0).$$

□

Vamos agora tratar do caso $p = 2$, veremos na prova do próximo lema que para provar a existência de solução para o sistema (3-1) sobre o inteiros 2-ádicos em alguns casos será preciso encontrar a "solução não singular", que garantirá existência de solução não trivial em $\mathbb{Z}_2$ explicitamente, são contas simples, e que podem ser facilmente verificadas com um computador ou mesmo a mão.

Lema 3.13 $\Gamma_2(3,2) \leq 11$.

Prova: Considere o sistema (3-1) com $s \geq 11$. Nós podemos assumir que para qualquer i, no máximo um entre c_i e d_i é igual a zero (caso contrário nós temos claramente uma solução não trivial). Seja $K = \{0,1,2,4\}$, dado $b \in \mathbb{Z}_2/\{0\}$ é possível encontrar $x \in \mathbb{Z}_2/\{0\}$ e $g \in K/\{0\}$, aplicando o Lema de Hensel ao polinômio $f(x) = gx^3 - b$, tais que $b = gx^3$, donde podemos particionar os índices $1,...,s$ entre os quatro conjuntos

$$\mathfrak{U}_g = \{i : c_i = ga^3 \text{ para algum } a \in \mathbb{Z}_2/\{0\}\} \qquad (g \in K),$$

assim temos

$$\sum_{g\in K} |\mathfrak{U}_g| = s.$$

Seja M o número de $g \in K/\{0\}$ para os quais $\mathfrak{U}_g \neq \varnothing$, e seja $r = |\mathfrak{U}_0|$. Então $M \leq 3$ e

$$\begin{aligned} S &= |\mathfrak{U}_0| + \sum_{g\in K/\{0\}} \left\lfloor \frac{1}{2}|\mathfrak{U}_g| \right\rfloor \\ &\geq r + \sum_{\substack{g\in K/\{0\},\\ \mathfrak{U}\neq\varnothing.}} \frac{1}{2}(|\mathfrak{U}_g| - 1) \\ &\geq \frac{1}{2}(s + r - 3). \end{aligned}$$

Existem dois caso.

i) Suponha que $r > 0$. Então $S \geq 5$, daí nós podemos reorganizar variáveis de forma que, para $i = 1,...,5$, ou $2i-1 \in \mathfrak{U}_q$ e $2i \in \mathfrak{U}_q$ para algum $q \in K/\{0\}$, ou então $2i-1 \in \mathfrak{U}_0$. Em cada caso, de maneira análoga a que fizemos na demonstração do lema anterior, $c_{2i-1}x^3 + c_{2i}y^3 = 0$ possui uma solução não singular sobre $\mathbb{Z}_2$, digamos (a_{2i-1}, a_{2i}). Defina $D_i = d_{2i-1}a_{2i-1}^2 + d_{2i}a_{2i}^2$ para $i = 1,...,5$. Então como sabemos que $\Gamma(2) = 5$, podemos encontrar uma solução não trivial para a equação

$$D_1u_1^2 + \cdots + D_5u_5^2 = 0,$$

digamos $(b_1,...,b_5)$, e consequentemente

$$(a_1b_1, a_2b_1, ..., a_9b_5, a_{10}b_5, 0, ..., 0)$$

é uma solução não trivial para o sistema (3-1) sobre $\mathbb{Z}_2$.

ii) Suponha que $r = 0$. Então $S \geq 4$, se tivermos $S \geq 5$, o mesmo argumento usado no item anterior pode ser aplicado, então vamos supor que $S = 4$. Reordenando e fazendo uma mudança de variáveis se for preciso, podemos assumir que $c_{2i-1} = c_{2i} \in K/\{0\}$ para $i = 1,2,3,4$. Além disso, também podemos assumir que pelo menos um dos três índices restantes, sem perda de generalidade $i = 9$, é tal que $c_7 = c_8 = c_9$. Seja $\mathfrak{B}_i = \{2i, 2i-1\}$ para $i \in \{1,2,3\}$, e $\mathfrak{B}_4 = \{7,8,9\}$.

Considere a equação cúbica correspondente a cada conjunto $\mathfrak{B}_i$. A equação $x^3 + y^3 = 0$ possui a solução não trivial $(u,-u)$ para qualquer $u \in \mathbb{Z}_2/\{0\}$. Também, a equação $x^3 + y^3 + z^3 = 0$ possui a solução não trivial (au, bu, cu) para qualquer $u \in \mathbb{Z}_2/\{0\}$, com $c = 2^r$ para qualquer $r \geq 1$ e algum $(a,b) \equiv (1,-1)$ $(mod\ 8)$ usando o Lema de Hensel.

Escreva $D_i = d_{2i-1} + d_{2i}$ para $i = 1,2,3$, $D_4 = d_7a^2 + d_8b^2 + d_9c^2$, e considere a equação

$$Q(D_1, D_2, D_3, D_4) = D_1u_1^2 + \cdots + D_4u_4^2 = 0. \tag{3-20}$$

Se for possível encontra uma solução não trivial $(u_1,...,u_4)$ para a equação (3-20) sobre $\mathbb{Z}_2$, então vista da nossa mudança de variáveis, as equações (3-1) possui a solução não trivial $(u_1, -u_1, u_2, -u_2, u_3, -u_3, au_4, bu_4, cu_4, 0, ..., 0)$.

Agora vamos considerar para quais quadráticas $Q(D)$ existe solução não trivial, claramente temos uma solução não trivial para a quadrática $Q(D)$ se algum D_i é zero, então nós podemos supor que nenhum dos D_i é igual a zero. Fazendo uma mudança de variáveis, podemos assumir que $(D_i, 8) \leq 2$ para cada i, que $(D_1, D_2, 2) = 1$, e que $D_1 \equiv 1$ $(mod\ 8)$. Além disso, se para quaisquer i e j nós temos $D_i \equiv D_j$ $(mod\ 8)$, e $(D_i, D_j, 2) = 1$, então podemos supor que $D_1 \equiv D_2$ $(mod\ 8)$. Se podermos agora encontrar uma solução para a equação quadrática $(mod\ 8)$ tais que D_i e u_i são ambos relativamente

primos com 2 para algum i, que chamaremos de uma solução "não singular $(mod\ 8)$", então pelo Lema de Hensel existe uma solução não trivial para a quadrática sobre $\mathbb{Z}_2$.

Reorganizando os D_i, podemos facilmente verificar que a Tabela 1 lista todos os casos distintos possíveis, e consequentemente nós podemos nos concentrar naquelas cinco quadráticas para as quais não se pode encontrar solução que é não singular $(mod\ 8)$.

Tabela 1. (Aqui γ e δ denotam inteiros arbitrários.)

Quadrática Q				Solução não singular $(mod\ 8)$				Quadrática Q				Solução não singular $(mod\ 8)$			
D_1	D_2	D_3	D_4	u_1	u_2	u_3	u_4	D_1	D_2	D_3	D_4	u_1	u_2	u_3	u_4
1	7	γ	δ	1	1	0	0	1	1	5	5	nenhuma			
3	5	γ	δ	1	1	0	0	1	1	1	2	1	1	2	1
1	1	6	γ	1	1	1	0	1	1	3	2	1	1	2	1
1	5	2	γ	1	1	1	0	1	1	2	2	nenhuma			
1	1	1	1	nenhuma				1	3	2	2	1	1	1	1
1	1	1	3	1	0	2	1	1	3	2	6	nenhuma			
1	1	1	5	1	1	1	1	1	3	6	6	1	1	1	1
1	1	3	3	1	1	1	1	1	5	6	6	nenhuma			

Agora pretendemos mostrar que usando uma escolha alternativa admissível de (a,b,c), nós podemos mudar o valor de D_4 de modo a evitar as cinco quadráticas problemáticas. Considere o coeficiente $D_4 = d_7a^2 + d_8b^2 + d_9c^2$. Reorganizando as variáveis, escrevemos $D_4 = d\mathcal{R}(a,b,c)$, com $\mathcal{R}(a,b,c) = a^2 + \alpha b^2 + \beta c^2$ onde $d, \alpha, \beta \in \mathbb{Z}_2$. Também podemos supor que se $\alpha \equiv \beta\ (mod\ 8)$, e $(\alpha\beta, 2) = 1$, então $\alpha \equiv 1\ (mod\ 8)$. Então verificamos que a Tabela 2 lista as únicas possibilidades distintas para (α, β) onde um deles não é divisível por 2. Daí encontramos (a_1,b_1,c_1) e (a_2,b_2,c_2), de modo que, ao fazer a mudança de variáveis que nos permite assumir que $(D_4, 8) \leq 2$, temos dois valores que são distintos $(mod\ 8)$ para esse coeficiente reduzido.

Tabela 2

α $(mod\ 8)$	β	a_1	b_1	c_1	$\mathcal{R}(a_1,b_1,c_1)$ $(mod\ 8)$	a_2	b_2	c_2	$\mathcal{R}(a_2,b_2,c_2)$ $(mod\ 8)$
1	1	1	-1	0	2	1	-1	2	6
1	3	1	-1	0	2	1	0	-1	4
1	5	1	-1	0	2	1	0	-1	6
1	7	1	-1	0	2	1	-1	2	6
3	5	1	-1	0	4	1	0	-1	6
3	5	1	-1	0	4	0	1	-1	2
5	7	1	-1	0	6	0	1	-1	4
1	2	1	-1	0	2	1	0	-1	3
1	4	1	-1	0	2	1	0	-1	5
1	6	1	-1	0	2	1	0	-1	7
1	0	1	-1	0	2	1	0	-1	1
3	2	1	0	-1	3	0	1	-1	5
3	4	1	0	-1	5	0	1	-1	7
3	6	1	0	-1	7	0	1	-1	1
3	0	1	0	-1	1	0	1	-1	3
5	2	1	-1	0	6	1	0	-1	3
5	4	1	-1	0	6	1	0	-1	5
5	6	1	-1	0	6	1	0	-1	7
5	0	1	-1	0	6	1	0	-1	1
7	2	0	1	-1	1	1	0	-1	3
7	4	0	1	-1	3	1	0	-1	5
7	6	0	1	-1	5	1	0	-1	7
7	0	0	1	-1	7	1	0	-1	1

Além disso, usando γ e δ para denotar inteiros relativamente primos com 2 arbitrários, temos os casos que $(\alpha,\beta) = (\gamma 2^r, \delta 2^s)$ para algum $s \geq r \geq 1$. Aqui nós obtemos

$$\mathcal{R}(1,-1,0) = 1+\gamma 2^r \qquad \text{e} \qquad \mathcal{R}(0,1,-1) = \gamma 2^r + \delta 2^s.$$

Escrevemos $\gamma 2^r + \delta 2^s = \eta 2^t$ com η não divisível por 2 (se $\eta = 0$, então podemos facilmente resolver não trivialmente a quadrática). Então a menos que t seja par, considerando a mudança de variáveis que permita-nos assumir que $(D_4, 8) \leq 2$, o coeficiente representado por $\mathcal{R}(1,-1,0)$ e $\mathcal{R}(0,1,-1)$ são distintos $(mod\ 8)$. Mas se $t = 2v$ é par, então

$$2^{-t}\mathcal{R}(0,1,-1) \equiv \eta\ (mod\ 8), \qquad 2^{-t}\mathcal{R}(2^{v+1},1,-1) \equiv \eta + 4\ (mod\ 8),$$

e esses resíduos são distintos $(mod\ 8)$. Além disso η não é divisível por 2, então considerando a mudança de variáveis que permita-nos assumir que $(D_4, 8) \leq 2$, nós vemos que os coeficientes D_4 dados pos essas soluções são distintos.

Em todos esses casos nós obtemos uma escolha de valores para D_4. Fazendo a mudança de variáveis que nos permite assumir que $(D_4, 8) \leq 2$, observamos que existem dois valores que são distintos $(mod\ 8)$ para esse coeficiente reduzido. Mas examinado a Tabela 1, podemos facilmente ver que uma escolha, pelo menos, dos coeficientes disponíveis nos dá uma quadrática que podemos resolver, não importando como o coeficiente D_4 tenha sido reorganizado.

Então podemos encontra uma solução que é não singular $(mod\ 8)$ para a equação quadrática reduzida, e consequentemente existe uma solução não trivial para a equação (3-1) sobre $\mathbb{Z}_2$.

□

Na direção de encontrar solução para o caso $p = 3$ vamos começar com o o seguinte lema

Lema 3.14 *Suponha que nós temos uma solução x para a congruência*

$$\begin{aligned} F(x) = c_1x_1^3 + \cdots + c_sx_s^3 &\equiv 0\ (mod\ 9), \\ G(x) = d_1x_1^2 + \cdots + d_sx_s^2 &\equiv 0\ (mod\ 3), \end{aligned}$$

tal que existem indices i e j com $x_ix_j(c_id_jx_i - c_jd_ix_j) \not\equiv 0\ (mod\ 3)$. *Então existe uma solução não trivial 3-ádica para as equações (3-1).*

Prova: A prova será feita por indução. Suponha que para algum $\mu \geq 2$, nós temos uma solução para o sistema de congruências

$$\begin{aligned} F(x) &\equiv 0\ (mod\ 3^\mu), \\ G(x) &\equiv 0\ (mod\ 3^{\mu-1}), \end{aligned}$$

satisfazendo, para algum i e j,

$$x_ix_j(c_id_jx_i - c_jd_ix_j) \not\equiv 0\ (mod\ 3). \tag{3-21}$$

Escrevendo $y_i = x_i + k_i3^{\mu-1}$, para algum k_i a ser determinado. Então

$$\begin{aligned} F(y) &\equiv F(x) + 3^\mu(c_1k_1x_1^2 + \cdots + c_sk_sx_s^2) \quad (mod\ 3^{\mu+1}), \\ G(y) &\equiv G(x) + 3^{\mu-1}(2d_1k_1x_1 + \cdots + 2d_sk_sx_s) \quad (mod\ 3^\mu). \end{aligned}$$

Se nós podemos resolver o sistema de congruências

$$\begin{aligned} 3^{-\mu}F(x) + c_1k_1x_1^2 + \cdots + c_sk_sx_s^2 &\equiv 0 \ (mod\ 3), \\ 3^{1-\mu}G(x) + 2d_1k_1x_1 + \cdots + 2d_sk_sx_s &\equiv 0 \ (mod\ 3), \end{aligned} \tag{3-22}$$

então teremos uma solução y para o sistema de congruências

$$\begin{aligned} F(y) &\equiv 0 \ (mod\ 3^{\mu+1}), \\ G(y) &\equiv 0 \ (mod\ 3^{\mu}) \end{aligned}$$

satisfazendo

$$y_iy_j(c_id_jy_i - c_jd_iy_j) \equiv x_ix_j(c_id_jx_i - c_jd_ix_j) \not\equiv 0 \ (mod\ 3).$$

Mas as formas lineares em $(k_1, ..., k_s)$ no sistema de congruências (3-22) não são proporcionais $(mod\ 3)$, por (3-21). Logo nós podemos resolver para k_i, e consequentemente a hipótese de indução para μ implica $\mu + 1$. Mas, por hipótese, o resultado vale para $\mu = 2$, ou seja, o resultado vale para todo $\mu \geq 2$. Então temos uma solução não trivial x para a congruência $F(x) \equiv G(x) \equiv 0 \ (mod\ 3^{\mu})$ para todo μ, e consequentemente uma solução 3-ádica não trivial para o sistema (3-1).

□

Pelo que fizemos na seção 2.3, nós podemos escrever as equações (3-1) numa forma 3-normalizada $F = G = 0$, com

$$\begin{aligned} F^{**} = a_1x_1^3 + \cdots + a_ux_u^3 + \quad & b_1y_1^3 + \cdots + b_vy_v^3 && \equiv 0 \ (mod\ 9), \\ G^* = \quad & c_1y_1^2 + \cdots + c_vy_v^2 \quad + d_1z_1^2 + \cdots + d_wz_w^2 && \equiv 0 \ (mod\ 3), \end{aligned} \tag{3-23}$$

onde c_i e d_i são relativamente primos com 3, cada a_i e b_i é divisível no máximo por 3, e onde F^{**} denota as variáveis explicitas em $F \ (mod\ 9)$, e G^* denota aquelas explicitas em $G \ (mod\ 3)$.

Seja u_1 o número de a_i não divisíveis por 3, e v_1 o número de b_i não divisíveis por 3. Então por (2-3), nós temos

$$m_0 + q_{F,1} = u + v + w \geq 7, \quad q_{G,0} = v + w \geq, 3 \quad T_{F,1} = u + v \geq 4,$$

$$m_0 = u_1 + v + w \geq 5, \qquad q_{F,0} = u_1 + v_1 \geq 2.$$

Lema 3.15 *Suponha que $w \geq 3$. Então existe uma solução para a congruência (3-23) satisfazendo a condição (3-21) do Lema 3.14.*

Prova: Primeiro resolvemos a equação cúbica

$$a_1x_1^3+\cdots+a_ux_u^3+b_1y_1^3+\cdots+b_vy_v^3\equiv 0\ (mod\ 9).$$

Isso é possível não trivialmente, uma vez que $u+v\geq 4$, e $u_1+v_1\geq 2$ juntas implicam que por uma mudança de variáveis, a congruência acima consiste de uma das seguintes congruências

$$x^3+y^3\equiv 0\ (mod\ 9)\text{ ou }x^3+2y^3+3z^3\equiv 0\ (mod\ 9).$$

Ambas as congruências podem ser resolvidas não trivialmente, e mais, resolvidas com uma variável que é não nula $(mod\ 3)$ tendo um um coeficiente cubico não nulo $(mod\ 3)$. Fixando a solução para a cúbica, nós podemos então resolver independentemente a congruência

$$d_1z_1^2+\cdots+d_wz_w^2\equiv -(c_1y_1^2+\cdots+c_vy_v^2)\ (mod\ 3).$$

Como $w\geq 3$, está congruência sempre pode ser resolvida não trivialmente, pelo Corolário 2.12. Mas agora, como os coeficientes cúbicos de z_i são congruentes a zero $(mod\ 3)$, a condição (3-21) do Lema 3.14 é satisfeita.

□

Lema 3.16 *Supondo verdadeira a hipótese (H3),*

(H3) para toda congruência da forma (3-23) com $u+v+w\geq 7$, $u+v\geq 4$, $v+w\geq 3$, $u_1+v+w\geq 5$, $u_1+v_1\geq 2$, e $w<3$, nós temos uma solução uma solução satisfazendo (3-21),

todo sistema da forma (3-1) 3-normalizado com $s\geq 11$ possui uma solução não trivial 3-ádica.

Prova: Para $w\geq 3$ o Lema 3.11 garante uma solução não singular para o sistema (3-1), aplicando o Lema de Hensel, temos uma solução 3-ádica não trivial, para $w<3$ é a hipótese (H3), que provaremos na próxima seção, que garante solução a solução.

□

3.4 O método computacional para os primos 3, 7, 11, 13, 19, 23 e 31.

Agora só nos falta encontrar solução não singular para um pequeno número de primos e verificar a hipótese $(H3)$ para $p=3$, que supomos ter solução não singular sobre

algumas condições na seção passada, e ainda não provamos. Para esses casos descreveremos como verificar a existência dessa solução computacionalmente, apresentaremos como implementar os cálculos necessários primeiro para os primos 7, 11, 13, 19, 23 e 31, e depois para o 3.

(a) Primos diferentes de 3.

Considere o sistema de congruências

$$\begin{aligned} a_1x_1^3+\cdots+a_5x_5^3 &\equiv 0 \ (mod\ p) \\ b_1x_1^2+\cdots+b_5x_5^2 &\equiv 0 \ (mod\ p) \end{aligned} \tag{3-24}$$

onde $0 \leq a_i, b_i \leq p-1$, e no máximo um entre a_i e b_i é diferente de zero. Para estabelecer a validade da hipótese *(H)*, seguindo as conclusões das duas seções anteriores, nós temos apenas que checar que as congruências (3-24) possuem uma solução não singular $(mod\ p)$ para quaisquer escolhas possíveis de a_i e b_i. Além disso, se $p \equiv 1\ (mod\ 3)$ e $p > 13$, ou se $p \equiv 2\ (mod\ 3)$, então nós podemos também assumir que nenhum dos a_i é igual a zero.

Mas com a mudança de variáveis $x_i \to \omega x_i$, para um adequado ω, nós podemos assumir que cada b_i é 0, 1 ou c, onde c é algum resíduo não quadrático $(mod\ p)$. Também, pela mudança de variáveis $x_i \to -x_i$, nós podemos assumir que $0 \leq a_i \leq \frac{1}{2}(p-1)$. Ainda mais que isso, multiplicando por um fator não nulo adequado e reorganizando as variáveis, nós podemos assumir que $b_1 \leq b_2 \leq \cdots \leq b_5$, $b_1 = 0$ ou 1, e $b_2 = b_3 = 1$. Finalmente, se para algum j nós temos $b_j = b_{j+1}$, então nós podemos assumir que $a_j \leq a_{j+1}$.

Suponha que I é o conjunto de todos $(a_1,...,a_5,b_1,...,b_5)$, satisfazendo os critérios acima. Se para algum $(\alpha,\beta,\gamma,\kappa,\lambda,\mu)$ nós podemos encontrar uma solução não singular para as congruências

$$\begin{aligned} \alpha x^3+\beta y^3+\gamma z^3 &\equiv 0 \quad (mod\ p) \\ \kappa x^2+\lambda y^2+\mu z^2 &\equiv 0 \quad (mod\ p), \end{aligned}$$

então qualquer sistema de congruências da forma (3-24) com

$$(a_i,a_j,a_k,b_i,b_j,b_k) \equiv (\alpha,\beta,\gamma,\kappa,\lambda,\mu)\ (mod\ p),$$

para algum $(i,j,k) \in \{1,...,5\}^3$, com i,j,k distintos, admite uma solução não singular $(mod\ p)$. Nós usamos essa ideia para economizar mais o número de casos para serem checados, começamos testando todas as formas em três variáveis satisfazendo os critérios acima, e armazenamos as que nós não podemos encontrar nenhuma solução que seja não singular $(mod\ p)$. Nós então tomamos cada uma dessas formas, e testamos todas as formas em 4 variáveis satisfazendo o critério acima obtido considerando qualquer

coeficiente possível para a quarta variável, novamente armazenamos todas as formas que não possuem solução não singular. Se necessário, nós então procedemos semelhantemente pa a quinta variável.

Podemos implementar esse método em um computador para verificar que todo sistema de congruências da forma (2-24) possui uma solução que não é singular $(mod\ p)$.

(b) O primo 3.

Considere o sistema de congruências

$$\begin{aligned} a_1x_1^3+\cdots+a_7x_7^3 &\equiv 0(mod\ 9), \\ b_1x_1^2+\cdots+b_7x_7^2 &\equiv 0(mod\ 3), \end{aligned} \tag{3-25}$$

onde $0 \leq a_i \leq 8$, $0 \leq b_i \leq 2$, e os coeficientes satisfazem a condição da $(H3)$. Para estabelecer $(H3)$, seguindo as conclusões da seção anterior, nós temos apenas que checar que as congruências (3-24) possuem uma solução satisfazendo (3-21), para quaisquer escolhas possíveis de a_i e b_i. Pela mudança de variáveis $x_i \to -x_i$, nós podemos assumir que $0 \leq a_i \leq 4$. Multiplicando a congruência quadrática por uma fator não nulo adequado e reorganizando variáveis, nós podemos então assumir que o número de b_i iguais a 1 é pelo menos tão grande quanto o número iguais a 2. Também, reorganizando variáveis, nós podemos assumir que $b_1 \leq b_2 \leq \cdots \leq b_7$. Finalmente, se para algum j nós temos $b_j = b_{j+1}$, então nós podemos assumir que $a_j \leq a_{j+1}$.

Como o sistema de congruências (3-25) é mais complicado que o (3-24), o método não é tão bem sucedido. Mesmo assim, notando que $0, 1^3$ e 2^3 representam todos os resíduos cúbicos $(mod\ 9)$, somos capazes de economizar computação de soluções (3-25) usando $x_i \in \{0,1,2\}$. Nós podemos então usar um computador para verificar que todo sistema da forma (3-25) possui solução satisfazendo (3-21).

3.5 Garantindo soluções p-ádica.

Os cálculos computacional verificados na seção anterior completa a prova que as hipóteses (H) e $(H3)$ são verdadeiras, e consequentemente mostramos que, sujeito as condições $s \geq 11$ e $\vartheta(F,G) \neq 0$, um dos itens a seguir é verdadeiro:

(i) o sistema $F = G = 0$ possui uma solução não trivial sobre $\mathbb{Z}_p$,

(ii) o sistema $F \equiv G \equiv 0\ (mod\ p)$ tem uma solução não singular $(mod\ p)$.

Nesse último caso, argumentando pelo Lema de Hensel nós também podemos obter uma solução p-ádica não trivial. Nós agora vamos retirar a condição $\vartheta(F,G) \neq 0$.

Lema 3.17 *Para qualquer sistema da forma (3-1) em pelo menos onze variáveis (independentemente do valor de $\vartheta(F,G)$) possui uma solução p-ádica não trivial.*

Prova: Nós temos provado que $F = G = 0$ possui uma solução p-ádica não trivial quando $\vartheta(F,G) \neq 0$. Suponha agora que $\vartheta(F,G) = 0$. Para qualquer inteiro μ existem formas

$$\begin{aligned} F^{(\mu)} &= c_1^{(\mu)} x_1^3 + \cdots + c_s^{(\mu)} x_s^3, \\ G^{(\mu)} &= d_1^{(\mu)} x_1^2 + \cdots + d_s^{(\mu)} x_s^2, \end{aligned}$$

com coeficientes inteiros tal que $\vartheta(F^{(\mu)}, G^{(\mu)}) \neq 0$ e tal que

$$c_i^{(\mu)} - c_i \equiv d_i^{(\mu)} - d_i \equiv 0 \ (mod\ p^{(\mu)}) \text{ para } i = 1, ..., s.$$

Mas então a equação $F^{(\mu)} \equiv G^{(\mu)} \equiv 0$ possui uma solução p-ádica não trivial $\xi^{(\mu)} = (\xi_1^{(\mu)}, ..., \xi_s^{(\mu)})$. Por homogeneidade, nós podemos supor que os $\xi_i^{(\mu)}$ são inteiros p-ádicos, e que pelo menos um não é divisível por p. Pela compacidade dos inteiros p-ádicos, o conjunto $\{\xi^{(\mu)}\}$ tem um ponto de acumulação $\xi \neq 0$, Então mandando μ para o infinito em uma sequência adequada, nós temos que

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

existe no sentido p-ádico, e

$$\begin{aligned} \|F(\xi^{(\mu)})\|_p &= \|F(\xi^{(\mu)}) - F^{(\mu)}(\xi^{(\mu)})\|_p \\ &= \left\| \sum_i (c_i^{(\mu)} - c_i) \xi_i^{(\mu)3} \right\|_p \\ &\leq p^{-\mu}. \end{aligned}$$

Pela continuidade, nós temos $F(\xi) = 0$, e de forma similar $G(\xi) = 0$. Dessa forma o sistema (3-1) possui uma solução p-ádica não trivial.

□

Então todo sistema em pelo menos onze variáveis possui, para todo p primo, uma solução nos inteiros p-ádica não trivial, ou seja, $\Gamma(3,2) \leq 11$. Nós agora mostraremos que $\Gamma(3,2) \geq 11$.

Lema 3.18 $\Gamma(3,2) \geq 11$ *para todo primo* $p \equiv 1\ (mod\ 3)$.

Prova: Seja $p \equiv 1\ (mod\ 3)$ um primo, c um resíduo que não é resíduo cúbico $(mod\ p)$, e ω um resíduo que não é resíduo quadrático $(mod\ p)$. Considere o sistema de equações em dez variáveis:

$$\begin{aligned}(x_1^3+cx_2^3)+p(x_3^3+cx_4^3)+p^2(x_5+cx_6^3) &= 0,\\ (x_7-\omega x_8^2)+p(x_9^2-\omega x_{10}^2) &= 0.\end{aligned}$$

A equação cúbica não possui solução não trivial sobre $\mathbb{Z}_p$, pois c não é resíduo cúbico $(mod\ p)$. Além disso, a equação quadrática não possui solução não trivial em $\mathbb{Z}_p$, pois ω não é um resíduo quadrático $(mod\ p)$. Consequentemente o sistema acima não possui solução não trivial em $\mathbb{Z}_p$.

□

Com isso concluímos esse trabalho apresentando o teorema a seguir, que não só confirma a Conjectura de Artin para $\Gamma(3,2)$, como dá uma valor ainda mais baixo para o número de variáveis do que o proposto pela conjectura que seria 14.

Teorema 3.19 $\Gamma(3,2) = 11$.

CAPÍTULO 4

Apêndice: Rotina para encontrar soluções não singulares $(mod\ p)$.

Faremos aqui uma breve rotina, que pode ser facilmente implementada para encontrar as soluções não singulares $(mod\ p)$ para os primos listados na seção 3.4.

Iniciamos com o primo p e um resíduo c não quadrático $(mod\ p)$ (que também pode ser obtido computacionalmente);

Passo 1 (solução não singular com três variáveis): Nesse passo teremos seis parâmetros (coeficientes), $(a_1,a_2,a_3,b_1,b_2,b_3)$ que pelas considerações feitas na seção 3.4, se $p \equiv 2\ (mod 3)$ ou se $p \equiv 1\ (mod\ 3)$ e $p > 13$, então $0 < a_1,a_2,a_3 \leq \frac{p-1}{2}$, caso contrário $0 \leq a_1,a_2,a_3 \leq \frac{p-1}{2}$, nos dois casos $b_1,b_2,b_3 \in \{0,1,c\}$, e teremos três variáveis $0 \leq x_1,x_2,x_3 \leq p-1$.

Passo 1.a: Para cada escolha fixada dos parâmetros $(a_1,a_2,a_3,b_1,b_2,b_3)$, fazemos x_1,x_2,x_3 variar nos resíduos $(mod\ p)$ testando em cada caso as congruências:

$$\begin{aligned} a_1x_1^3 + a_2x_2^3 + a_3x_3^3 &\equiv 0 \quad (mod\ p) \\ b_1x_1^2 + b_2x_2^2 + b_3x_3^2 &\equiv 0 \quad (mod\ p), \end{aligned} \tag{4-1}$$

se para algum $(\alpha_1,\alpha_2,\alpha_3)$ as congruências acima forem verdadeiras passamos para o passo seguinte 1.b, senão, damos um incremento nas variáveis (que deve ser feito de forma a passar por todas as combinações possíveis dos resíduos) e testamos novamente, se esgotarem as possibilidade para x_1,x_2,x_3 vamos para o passo 2.

Passo 1.b: dada a solução $(\alpha_1,\alpha_2,\alpha_3)$ da congruência (4-1) do passo 1.a testamos a congruência

$$6\alpha_i\alpha_j(a_ib_j\alpha_i - a_jb_i\alpha_j) \equiv 0\ (mod\ p)\ \text{para} i \neq j, \tag{4-2}$$

onde $i,j \in \{1,2,3\}$, se a congruência (4-2) é verdadeira para todos os i,j voltamos ao passo 1.a (a solução é singular $(mod\ p)$), se (4-2) é falsa para algum i,j então a rotina para

e informamos que para os parâmetros $(a_1, a_2, a_3, b_1, b_2, b_3)$ corresponde a uma sistema com solução não singular.

Passo 2(solução não singular com quatro variáveis): Nesse passo teremos como entradas os parâmetros $(a_1, a_2, a_3, b_1, b_2, b_3)$ do passo 1 para os quais não foi possível encontrar solução não singular, fixaremos esses parâmetros e introduziremos dois novos (a_4, b_4) e uma nova variável x_4.

Passo 2.a: Para cada escolha fixada dos parâmetros (a_4, b_4), fazemos x_1, x_2, x_3, x_4 variar nos resíduos $(mod\ p)$ testando em cada caso as congruências:

$$\begin{aligned} a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 &\equiv 0 \pmod p \\ b_1x_1^2 + b_2x_2^2 + b_3x_3^2 + b_4x_4^2 &\equiv 0 \pmod p, \end{aligned} \tag{4-3}$$

se para algum $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ as congruências acima forem verdadeiras passamos para o passo seguinte 2.b, senão, damos um incremento nas variáveis (que deve ser feito de forma a passar por todas as combinações possíveis dos resíduos) e testamos novamente, se esgotarem as possibilidade para x_1, x_2, x_3, x_4 vamos para o passo 3.

Passo 2.b: dada a solução $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ da congruência (4-3) do passo 2.a testamos a congruência

$$6\alpha_i\alpha_j(a_ib_j\alpha_i - a_jb_i\alpha_j) \equiv 0 \pmod p \text{ para } i \neq j, \tag{4-4}$$

onde $i, j \in \{1, 2, 3, 4\}$, se a congruência (4-4) é verdadeira para todos os i, j voltamos ao passo 2.a (a solução é singular $(mod\ p)$), se (4-4) é falsa para algum i, j então a rotina para e informamos que para os parâmetros $(a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4)$ corresponde a uma sistema com solução não singular.

Passo 3 (solução não singular com cinco variáveis): Esse passo é análogo ao passo anterior da rotina, teremos como entradas os parâmetros para os quais não foi possível encontrar solução não singular no passo 2, acrescentaremos a eles os parâmetros (a_5, b_5) e uma variável x_5, executaremos os passo 3.a e 3.b, que nada mais são, do que os passos 2.a e 2.b, agora com cinco variáveis.

Wooley mostrou que para $p \in \{7, 11, 13, 19, 23, 31\}$ a rotina termina no máximo no passo 3, comprovando a hipótese (H) para esse primos e concluindo a demonstração do teorema principal.

Referências Bibliográficas

[1] Cassels, W. S. , *Local Fields*, London Mathematical Society Student (3), London, 1986.

[2] Cook, R. J., *Pairs of Additive Congruences: Cubic Congruences*, Mathematika (32) 286-300, 1985.

[3] Davenport, H., Lewis, D. J., *Homogeneous Additive Equations*, Proc. Roy. Soc. London Ser. A (274) 443-460, London, 1963.

[4] Davenport, H., Lewis, D. J. , *Cubic Equations of Additive Type*, Philosophical Transactions of the Royal Society of London, (261) 97-136, London, 1966.

[5] Davenport, H., Lewis, D. J., *Two Additive Equations*, Proceedings of Symposia in Pure Mathematics, (12) 74-98, Houston, 19.67.

[6] Davenport, H., Lewis, D. J., *Simultaneous Equations of Additive Type*, Philosophical Transactions of the Royal Society of London, (264) 557-595, London, 1969.

[7] Godinho, H., Soares, M., Shokranian, S. *Teoria dos Números*, Editora Universidade de Brasília, 2º edição, 1999.

[8] Lewis, D. J., *Cubic Congruences*, Michigan Math J., (4) 85-95, 1976.

[9] Lidl, R., Niederreiter, H., *Finite Fields*. Cambridge University Press, 1997.

[10] Nathanson, M. B., *Additive Number Theory - Inverse Problems and Geometry of Sumsets*, Graduate Texts in Mathematics vol. 165, Springer, 1996.

[11] Schmidt, W. M., *Equations over finite fields. An elementary approach, Lecture Notes in Mathematics 536*, Springer, Berlin, 1976.

[12] Wooley, Trevor D., *On Simultaneous Additive Equations I*, Proceedings of the London Mathematical Society. (3) 63 (1991), 1-34.