Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Pares de Formas Aditivas e a Conjectura de Artin

por

Tertuliano Carneiro de Souza Neto

Brasília
Fevereiro de 2011

E se nos for permitido, estaremos lá, eu e você.
Ao lado, a prova de um amor incorruptível.
À nossa frente, apenas o tempo: implacável, incansável, infinito.

Agradecimentos

A Deus, em primeiro lugar. Hoje eu sei que Ele sempre esteve ao meu lado.

À minha mãe. Sei o quanto foi difícil me trazer até aqui.

À minha esposa Vanessa, por ter estado ao meu lado todo este tempo.

Ao meu filho Breno. Nada pode ser mais sincero que o seu alegre sorriso.

Aos meus irmãos, pela ajuda nos momentos difíceis e as gargalhadas de final de ano.

Ao professor Hemar Godinho, pela orientação no Mestrado e Doutorado. Devo a ele boa parte da minha formação em Teoria dos Números.

Aos membros da banca, por terem aceitado o convite.

Aos professores da UnB e da UFBA que contribuíram para a minha formação acadêmica.

Aos meus amigos. Eles são, indubitavelmente, parte importante do processo.

Ao CNPq e à CAPES, pelo suporte financeiro.

Resumo

Seja

$$\begin{aligned} f(x_1, ..., x_n) &= a_1 x_1^k + \cdots + a_n x_n^k \\ g(x_1, ..., x_n) &= b_1 x_1^k + \cdots + b_n x_n^k \end{aligned} \tag{1}$$

um par de formas aditivas de grau $p^\tau(p-1)$. Estamos interessados em obter condições que garantam a existência de zeros p-ádicos para o par (1). Uma conhecida conjectura, devida a Emil Artin, afirma que a condição $n > 2k^2$ é suficiente. Utilizando técnicas da Teoria Combinatória dos Números, provamos que a condição

$$n > 2\frac{p}{p-1}k^2 - 2k$$

é suficiente se $k = 2.3^\tau$ ou 4.5^τ, e em qualquer caso se $\tau \geq \dfrac{p-1}{2}$.

Palavras-chaves: Conjectura de Artin. Pares de formas aditivas. p-normalização. Sequências livres de zeros. Solução p-ádica.

Abstract

Let

$$\begin{aligned} f(x_1, ..., x_n) &= a_1 x_1^k + \cdots + a_n x_n^k \\ g(x_1, ..., x_n) &= b_1 x_1^k + \cdots + b_n x_n^k \end{aligned} \tag{2}$$

be a pair of additive forms of degree $p^\tau(p-1)$. We are interested in finding conditions which guarantee the existence of p-adic zeros to the pair (2). A well-known conjecture due to Emil Artin states that the condition $n > 2k^2$ is sufficient. By means of techniques of Combinatorial Number Theory, we prove that

$$n > 2\frac{p}{p-1}k^2 - 2k$$

is sufficient if $k = 2.3^\tau$ or 4.5^τ, and in any case if $\tau \geq \dfrac{p-1}{2}$.

Keywords: Artin's conjecture. Pairs of additive forms. p-normalization. p-adic solution. Zero-free sum sequences.

Sumário

Introdução

Embora não se saiba precisamente a época em que surgiram as primeiras equações algébricas, alguns registros sugerem que o seu aparecimento tenha se dado em torno de 2000 a.C. O Papiro Rhind, originário da civilização egípcia, contém problemas que, não obstante a peculiar representação matemática, equivalem ao que atualmente denominamos equações lineares. Registros da matemática babilônica mostram que esta civilização já possuía uma notável habilidade na resolução de sistemas lineares e equações quadráticas da forma $x^2 + ax + b = 0$. A despeito das complexas notações utilizadas, os babilônios eram capazes de resolver algumas equações cúbicas e perceberam que as equações $ax^4 + bx^2 = c$ não eram mais que equações quadráticas, para as quais eles já possuiam resolução (C. Boyer [2]).

Juntamente com o notável desenvolvimento científico do Renascimento, vieram as resoluções das equações cúbicas e quárticas, cuja coroação se deu com a publicação da obra Ars Magna, de Gerônimo Cardano, em 1545. Como se sabe, não pertence a Cardano a honra de tê-las resolvido. A solução da equação de 3º grau deve-se a Niccolo Tartaglia (1500-1557) e a de 4º grau é de autoria de Ludovico Ferrari (1522-1565).

Mas uma questão ainda intrigava os matemáticos da época renascentista. Ocorre que a fórmula encontrada por Tartaglia para obter as soluções da equação de 3º grau frequentemente levava à extração de raízes quadradas de números negativos, um problema que há séculos atormentava os matemáticos. De fato, tais números (ou seriam aberrações da matemática?) já apareciam quando da resolução de equações quadráticas, embora equações do tipo $x^2 + 2 = 0$ eram simplesmente ditas como não possuindo solução (G. Garbi [9]).

Os matemáticos começavam a perceber que os números reais já não mais satisfaziam às suas necessidades algébricas. Era preciso ampliar o conjunto de soluções. Surgiam, deste modo, os números complexos, investigados inicialmente por Bombelli, em meados

do século XVI, e amplamente estudados pelo genial Leonhard Euler (1707-1783). Aliás, deve-se a Euler a obtençao de uma das mais belas equações da História da Matemática, a saber:

$$e^{i\pi} + 1 = 0.$$

É provável que um imenso ciclo evolutivo no campo da Teoria das Equações Algébricas tenha se encerrado com a tese de doutorado de Carl Friedrich Gauss (1777-1855). Ele provou que todo polinômio de grau n possui exatamente n raízes no corpo complexo. Estava demonstrado o que viria a ser o Teorema Fundamental da Álgebra.

A conjectura de Artin

Com as novas ideias de estruturas matemáticas introduzidas por Abel e Galois, os matemáticos passaram a se preocupar não somente com a resolução das equações algébricas mas também com o corpo sobre o qual os polinômios estariam definidos. Mais especificamente, havia a necessidade de se descobrir novas extensões do corpo dos racionais que não fossem os já conhecidos $\mathbb{R}$ (o completamento topológico de $\mathbb{Q}$) e $\mathbb{C}$ (o fecho algébrico de $\mathbb{Q}$, conforme Gauss já havia provado um século antes).

Foi neste intuito que, em 1902, K. Hensel construiu um novo corpo de números. Utilizando uma norma não arquimediana $|\ |_p$, definida pela valoração p-ádica sobre os racionais, ele concluiu que esta norma levava a um completamento topológico diferente daquele obtido pela norma absoluta $|\ |_\infty$. Este completamento é o que atualmente denominamos corpo p-ádico, $\mathbb{Q}_p$. Vale a pena ressaltar que os únicos corpos que podem ser obtidos por completamentos topológicos de $\mathbb{Q}$ são $\mathbb{R}$ e os corpos $\mathbb{Q}_p$, para todos os números primos p. Isto se deve a um teorema de Ostrowski que garante que qualquer norma definida sobre os racionais será equivalente a $|\ |_\infty$ ou $|\ |_p$, para algum primo p.

Sendo $\mathbb{Q}_p$ um corpo, era natural perguntar-se em que condições um polinômio admitia zeros p-ádicos não triviais.

Nesta direção, Emil Artin conjecturou:

Conjectura 0.1. *Se p é um primo e $f(x_1, \ldots, x_n) \in Q_p[x_1, \ldots, x_n]$ é um polinômio homogêneo de grau k em $n > k^2$ variáveis, então a equação $f = 0$ possui ao menos uma solução não trivial em $\mathbb{Q}_p$.*

Em 1924, H. Hasse já havia provado que toda forma quadrática em 5 ou mais variáveis sempre possui zeros p-ádicos não triviais. Passados 28 anos, D. J. Lewis [13] confirmaria a Conjectura de Artin para o caso $k = 3$. No entanto, em 1966, Terjanian [17] exibiu uma forma biquadrática em 18 variáveis que não possui zeros 2-ádicos. Estava disprovada a Conjectura 0.1.

Teria Terjanian encerrado o assunto? A História da Matemática nos mostra que os problemas não se encerram, eles se renovam. Um ano antes de Terjanian construir seu contra-exemplo, Ax e Kochen [1] provaram:

Teorema 0.2. *Para todo grau k, existe um primo $p(k)$ tal que a Conjectura de Artin é verdadeira para todo primo $p > p(k)$.*

Isto mostra que, fixado o grau, a Conjectura 0.1 é verdadeira para quase todos os primos. O problema de se determinar $p(k)$ tem sido bastante investigado nos últimos anos, mas uma resposta geral (se é que existe) ainda é desconhecida.

Uma nova fonte de pesquisas foi aberta por Davenport e Lewis [5] em 1963, ao provarem:

Teorema 0.3. *Toda forma aditiva de grau k em $n > k^2$ variáveis possui um zero p-ádico não trivial.*

Uma forma aditiva (ou diagonal) de grau k em n variáveis é um polinômio do tipo $f(x_1, \ldots, x_n) = a_1 x_1^k + \cdots + a_n x_n^k$. Portanto estava provada a Conjectura de Artin para formas diagonais e surgia uma nova versão da Conjectura de Artin para sistemas de formas aditivas.

Conjectura 0.4. *Seja*

$$f_1(x_1, \ldots, x_n) = a_{11} x_1^k + \cdots + a_{1n} x_n^k$$

$$\vdots$$

$$f_r(x_1, \ldots, x_n) = a_{r1} x_1^k + \cdots + a_{rn} x_n^k$$

um sitema composto por r formas aditivas de grau k em $\mathbb{Q}_p[x_1, \ldots, x_n]$. Se $n > rk^2$, então o sistema $f_1 = \cdots = f_r = 0$ tem solução p-ádica não trivial.

O Teorema 0.3 responde afirmativamente à Conjectura 0.4 quando $r = 1$. O caso $r = 2$ é o objeto central deste nosso trabalho. O problema, como se vê, não é novo. Em verdade,

já se foram algumas décadas na tentativa de se provar que o par de equações aditivas

$$\begin{aligned} f(x_1,...,x_n) &= a_1x_1^k + \cdots + a_nx_n^k = 0 \\ g(x_1,...,x_n) &= b_1x_1^k + \cdots + b_nx_n^k = 0 \end{aligned} \tag{3}$$

possui solução p-ádica não trivial quando $n > 2k^2$.

Em 1969, Davenport e Lewis [7] provaram a validade da Conjectura de Artin em pares de formas aditivas quando o grau k é ímpar. No mesmo trabalho, foi mostrado que a condição $n \geq 7k^3$ é suficiente para se garantir a existência de solução p-ádica não trivial para o par de equações (3). Recentemente, J. Brüdern e H. Godinho [3] demonstraram que a condição $n > 2k^2$ é suficiente, a menos que o grau tenha a forma $k = p^\tau(p-1)$ para $\tau \geq 1$ e algum primo p, ou $k = 3.2^\tau$ para $\tau \geq 0$. Se $k = p^\tau(p-1)$ para algum primo $p \geq 3$ e $\tau \geq 1$, eles estabeleceram a condição $n \geq 4k^2$.

Contribuições

Concentramos nossos esforços em melhorar a condição estabelecida em [3] para o grau $p^\tau(p-1)$ quando $p \geq 3$ e $\tau \geq 1$, com o claro objetivo de aproximar-se o máximo possível da Conjectura de Artin. Para tanto, utilizamos algumas ideias da Teoria Combinatória de Números.

Faremos uso da técnica da contração de sequências para formar elementos secundários nos níveis imediatamente superiores, melhorando os resultados de [10] no que concerne à obtenção de subsequências secundárias. Utilizando um novo invariante de grupos, construímos sequências livres de zeros para nos auxiliar na obtenção de sequências não-singulares. Então finalizamos com a aplicação desta nova técnica para obter os seguintes resultados.

Teorema 0.5. *Seja (f,g) um par de formas aditivas de grau $k = p^\tau(p-1)$ para um primo $p \geq 7$. Se*

$$n > 2\frac{p}{p-1}k^2 - 2k$$

e $\tau \geq \dfrac{p-1}{2}$, então o sistema (3) possui solução p-ádica.

Teorema 0.6. *Seja (f,g) um par de formas aditivas de grau $k = p^\tau(p-1)$, com $p = 3$ ou 5. Se*

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

então o par de equações (3) *possui solução p-ádica.*

Organização do Trabalho

No Capítulo 1, abordamos um pouco da teoria que envolve pares de formas aditivas. Mais especificamente, estudamos o método da p-normalização e definimos solução não-singular.

O Capítulo 2 se inicia com as notações e definições gerais para o estudo de sequências em grupos abelianos. Em seguida, estudamos as sequências de números inteiros, com destaque para a definição de subsequências secundárias. E então finalizamos com alguns lemas combinatórios e a definição de um novo invariante de grupos.

A demonstração dos principais teoremas é feita nos capítulos 3 e 4. Inicialmente, transportamos o problema de se encontrar soluções em sistemas de congruências para o problema de se encontrar subsequências apropriadas da sequência de coeficientes do sistema (3). Em seguida, definimos os elementos primários e secundários através da contração de sequências de soma zero. E finalizamos com a demonstração dos principais resultados deste trabalho.

Capítulo 1

p-Normalização

Neste capítulo, apresentamos um pouco da teoria que trata dos pares de formas aditivas e alguns resultados que servirão de base para os capítulos subsequentes. Não abordaremos aqui a teoria concernente aos números p-ádicos. No entanto, aqueles que não estiverem familiarizados com a estrutura dos corpos p-ádicos, podem consultar Godinho [11] ou Koblitz [12].

Considere um par de formas aditivas de grau k em n variáveis

$$\begin{aligned} f(x_1, ..., x_n) &= a_1 x_1^k + \cdots + a_n x_n^k \\ g(x_1, ..., x_n) &= b_1 x_1^k + \cdots + b_n x_n^k, \end{aligned} \tag{1.1}$$

onde os coeficientes a_j, b_j são números racionais.

Estamos interessados em encontrar condições suficientes que garantam a existência de solução p-ádica não trivial para o par de equações

$$\begin{aligned} f(x_1, ..., x_n) &= 0 \\ g(x_1, ..., x_n) &= 0. \end{aligned} \tag{1.2}$$

Para tanto, começamos por apresentar um processo que se mostrará bastante útil nas próximas linhas. Trata-se da p-normalização, método criado por H. Davenport e D. J. Lewis [6] para auxiliar na resolução de equações que envolvam formas aditivas sobre o corpo $\mathbb{Q}_p$.

Sejam $v_1, ..., v_n$ inteiros e $\lambda, \delta, \mu, \rho$ racionais satisfazendo $\lambda\delta - \mu\rho \neq 0$. Considere as

seguintes transformações do par (1.1):

$$\begin{aligned} F_1(x_1,...,x_n) &= f(p^{v_1}x_1,...,p^{v_n}x_n) \\ G_1(x_1,...,x_n) &= g(p^{v_1}x_1,...,p^{v_n}x_n) \end{aligned} \tag{1.3}$$

$$\begin{aligned} F_2(x_1,...,x_n) &= \lambda f(x_1,...,x_n) + \mu g(x_1,...,x_n) \\ G_2(x_1,...,x_n) &= \rho f(x_1,...,x_n) + \delta g(x_1,...,x_n). \end{aligned} \tag{1.4}$$

Passamos a descrever agora como estes pares se relacionam com o par (f,g). Para cada par (1.1) vamos associar a constante

$$\vartheta(f,g) = \prod_{i\neq j}(a_ib_j - a_jb_i).$$

Lema 1.1. *Se (F_1,G_1) e (F_2,G_2) são, respectivamente, o resultado das transformações (1.3) e (1.4), então*

$$\vartheta(F_1,G_1) = p^{2k(n-1)\sum v_i}\vartheta(f,g)$$

e

$$\vartheta(F_2,G_2) = (\lambda\delta - \mu\rho)^{n(n-1)}\vartheta(f,g).$$

Demonstração. Vamos começar demonstrando a primeira igualdade. Por (1.3),

$$\begin{aligned} F_1 &= a_1'x_1^k + \cdots + a_n'x_n^k \\ G_1 &= b_1'x_1^k + \cdots + b_n'x_n^k, \end{aligned}$$

onde $a_i' = a_ip^{kv_i}$ e $b_i' = b_ip^{kv_i}$. Então

$$a_i'b_j' - a_j'b_i' = p^{k(v_i+v_j)}(a_ibj - a_jb_i)$$

e

$$\vartheta(F_1,G_1) = p^{k\sum_{i\neq j}(v_i+v_j)}\vartheta(f,g).$$

Mas

$$\sum_{i\neq j}(v_i+v_j) = 2(n-1)v_1 + \cdots + 2(n-1)v_n = 2(n-1)\sum v_i,$$

o que conclui a primeira parte da prova.

Para provar a segunda igualdade, observe que se

$$F_2 = A_1x_1^k + \cdots + A_nx_n^k$$
$$G_2 = B_1x_1^k + \cdots + B_nx_n^k,$$

então

$$\begin{aligned} A_iB_j - A_jB_i &= (\lambda a_i + \mu b_i)(\rho a_j + \delta b_j) - (\lambda a_j + \mu b_j)(\rho a_i + \delta b_i) \\ &= (\lambda\delta - \mu\rho)(a_ib_j - a_jb_i). \end{aligned}$$

Portanto

$$\vartheta(F_2, G_2) = (\lambda\delta - \mu\rho)^{n(n-1)}\vartheta(f, g).$$

◪

Definição 1.2. Dizemos que dois pares de formas aditivas são *equivalentes* (ou $p-$*equivalentes*) se eles diferem por uma combinação das operações (1.3) e (1.4).

Pode-se provar que estas operações definem uma relação de equivalência sobre o conjunto de pares de formas aditivas com coeficientes em $\mathbb{Q}_p$. Um fato importante na teoria é que a equação (1.2) terá uma solução p-ádica se, e somente se, o mesmo ocorrer com qualquer par p-equivalente a (f, g).

Considere um par (F, G) com coeficentes inteiros satisfazendo $l = \nu_p(\vartheta(F, G)) < \infty$, onde ν_p é a valoração p-ádica. Diremos que o par (F, G) é *p-normalizado* se l for a menor potência de p que divide $\vartheta(f, g)$ para todos os pares (f, g) com coeficientes inteiros e p-equivalentes a (F, G).

Lema 1.3. *Suponha que* (1.2) *tenha solução p-ádica não trivial para todos os pares p-normalizados. Então para todos os pares (f, g), a equação* (1.2) *também terá solução não trivial em $\mathbb{Q}_p$.*

Demonstração. Ver [6]. ◪

Em razão do Lema 1.3, de agora em diante só estudaremos pares de formas aditivas que sejam p-normalizados. Em particular, os coeficientes no par de formas (1.1) são números inteiros.

Vamos rearranjar as variáveis no par (1.1) como segue. Para cada variável x_j, calculamos a valoração p-ádica de a_j e b_j. Em seguida, tomamos

$$l = \min(\nu_p(a_j), \nu_p(b_j)),$$

ou seja, $p^{l+1} \nmid a_j$ ou $p^{l+1} \nmid b_j$. Então juntamos as variáveis que possuem em comum o mesmo inteiro l e formamos as subformas (f_l, g_l). Isto nos permite reescrever o par (1.1) como

$$f = \sum_{i=0}^{L} p^i f_i \ , \ g = \sum_{i=0}^{L} p^i g_i,$$

para algum inteiro L.

Um fato muito importante é que sempre podemos supor $L \in [0, k-1]$. De fato, se para alguma variável x_j tivermos $l \geq k$, então a transformação (1.3) nos dá o par p-equivalente

$$\begin{aligned} F_1(x_1, ..., x_n) &= f(x_1, \ldots, x_{j-1}, p^{-k\lfloor \frac{l}{k} \rfloor} x_j, x_{j+1}, \ldots, x_n) \\ G_1(x_1, ..., x_n) &= g(x_1, \ldots, x_{j-1}, p^{-k\lfloor \frac{l}{k} \rfloor} x_j, x_{j+1}, \ldots, x_n) \end{aligned}$$

com

$$\nu_p(\vartheta(F, G)) < \nu_p(\vartheta(f, g)).$$

Assim é que todo par p-normalizado pode ser escrito no formato

$$\begin{aligned} f &= f_0 + pf_1 + \cdots + p^{k-1} f_{k-1} \\ g &= g_0 + pg_1 + \cdots + p^{k-1} g_{k-1}. \end{aligned} \tag{1.5}$$

Por construção, os coeficientes de cada variável no par de subformas (f_l, g_l) não podem ser ambos divisíveis por p. Para cada $i \in [0, k-1]$, denotaremos por m_i o número de variáveis que ocorrem em f_i (ou g_i).

Seja $q(\lambda, \mu)$ o número mínimo de variáveis que possuem coeficientes não divisíveis por p na forma $\lambda f_0 + \mu g_0$, onde $\lambda \not\equiv 0 \bmod p$ ou $\mu \not\equiv 0 \bmod p$. Definindo $q_0 = \min(q(\lambda, \mu))$, temos o

Lema 1.4. *Se o par* (1.1) *é p-normalizado, então $q_0 \geq n/2k$ e*

$$\sum_{j=0}^{l} m_j \geq (l+1)\frac{n}{k},$$

para $l \in [0, k-1]$.

Demonstração. Ver [6], Lema 2. ◻

Definição 1.5. Uma solução $(\xi_1, \ldots, \xi_n)$ do sistema de congruências

$$\begin{aligned} a_1x_1^k + \cdots + a_nx_n^k &\equiv 0 \pmod{p^\alpha} \\ b_1x_1^k + \cdots + b_nx_n^k &\equiv 0 \pmod{p^\alpha} \end{aligned}$$

é dita *não-singular* se a matriz

$$\begin{pmatrix} a_1\xi_1 & a_2\xi_2 & \cdots & a_n\xi_n \\ b_1\xi_1 & b_2\xi_2 & \cdots & b_n\xi_n \end{pmatrix}$$

tem posto 2 módulo p.

Da definição, segue que $(\xi_1, \ldots, \xi_n)$ é uma solução não-singular se, e somente se, existe um par $i, j \in [1, n]$ tal que

$$(a_ib_j - a_jb_i)\xi_i\xi_j \not\equiv 0 \bmod p.$$

Portanto toda solução não-singular deve conter ao menos duas variáveis do par de sub-formas (f_0, g_0). Ademais, como veremos no Capítulo 3, os coeficientes destas variáveis devem possuir algumas particularidades.

Dado um primo p, defina $\tau = \nu_p(k)$ e

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

Lema 1.6. *Se o sistema*

$$\begin{aligned} a_1x_1^k + \cdots + a_nx_n^k &\equiv 0 \ (mod\ p^\gamma) \\ b_1x_1^k + \cdots + b_nx_n^k &\equiv 0 \ (mod\ p^\gamma) \end{aligned} \tag{1.6}$$

possui uma solução não-singular, então o par de equações aditivas (1.2) *possui uma solução p-ádica não trivial.*

Demonstração. A demonstração pode ser encontrada em [7], Lema 7. ◻

O Lema 1.6 é, sem dúvida, um dos mais importantes na teoria de formas aditivas e é consequência de um teorema mais geral devido a K. Hensel. Ele nos mostra que podemos

enxergar (e enfrentar) o problema da resolução de pares de equações aditivas no corpo p-ádico sob a ótica dos sistemas de congruência. Assim sendo, para determinar zeros p-ádicos para o par de formas (1.1), é suficiente encontrar uma solução não-singular para o sistema $f \equiv g \equiv 0 \bmod p^{\gamma}$, a qual, como já sabemos, deve envolver ao menos duas variáveis do par (f_0, g_0). Este será o nosso objetivo ao longo das próximas linhas.

Capítulo 2

Sequências em grupos abelianos

Neste capítulo, faremos um estudo de sequências em grupos abelianos finitos. Em particular, abordamos o problema de se encontrar subsequências secundárias em sequências inteiras (seção 2.2) e definimos um novo invariante de grupos (seção 2.3).

2.1 Definições gerais

Seja G um grupo abeliano aditivo e $S = (g_1, \ldots, g_r) = g_1 \cdot \ldots \cdot g_r$ uma sequência de elementos em G (podendo haver repetições). Para cada $g \in G$, a *multiplicidade* de g em S, $v_g(S)$, é o número de vezes que o elemento g ocorre na sequência S. Fazendo uso da notação multiplicativa de sequências, por vezes escreveremos

$$S = \prod_{g \in G} g^{v_g(S)}.$$

Dizemos que T é *subsequência* de S se $v_g(T) \leq v_g(S)$ para todo $g \in G$. Denotamos este fato por $T|S$. Se T é uma subsequência de S e $v_g(T) < v_g(S)$ para algum $g \in G$, então podemos definir a sequência ST^{-1}, construída retirando-se de S os elementos que ocorrem em T (contando-se as multiplicidades). Observe que isto equivale a

$$ST^{-1} = \prod_{g \in G} g^{(v_g(S) - v_g(T))}.$$

Ainda de posse da definição de multiplicidade de um elemento, definimos o *suporte* de

S em G, $\mathrm{supp}(S) = \{g \in G;\ v_g(S) \neq 0\}$, e o *comprimento* de S,

$$|S| = \sum_{g \in G} v_g(S).$$

Se S é a sequência vazia, então, por convenção, $|S| = 0$. Como se pode ver, o comprimento de uma sequência é a quantidade de elementos que nela ocorre (contando-se as multiplicidades), enquanto o suporte é o subconjunto de G formado pelos distintos elementos da sequência.

A *soma* de S é definida por

$$\sigma(S) = \sum_{i=1}^{r} g_i$$

e dizemos que S é uma *sequência de soma zero* se $\sigma(S) = 0$. Dizemos que S é uma *sequência curta* se ela é não vazia e seu comprimento não ultrapassa o expoente do grupo G ($\exp(G)$). Por exemplo, se G é um p-grupo abeliano elementar, então as sequências curtas em G devem possuir no máximo p elementos.

Definimos ainda o conjunto das somas de subsequências não vazias de S,

$$\Sigma(S) = \{\sigma(T);\ T|S \text{ e } T \neq \varnothing\}.$$

Observe que

$$\Sigma(S) = \{\varepsilon_1 g_1 + \cdots + \varepsilon_r g_r\},$$

onde os $\varepsilon_i \in \{0, 1\}$ não podem ser todos nulos.

A *constante de Davenport* de G (denota-se $D(G)$) é o menor inteiro positivo r tal que toda sequência S de comprimento r em G possui uma subsequência (não vazia) de soma zero. Definimos ainda o invariante $\eta(G)$ como o menor inteiro r tal que toda sequência S de comprimento r em G possui uma subsequência curta de soma zero.

Lema 2.1. *Seja p um número primo e $G = C_p \oplus C_p$. Então $D(G) = 2p-1$ e $\eta(G) = 3p-2$.*

Demonstração. A prova completa pode ser encontrada em [15] e [16]. Evidentemente, a abordagem e a notação diferem das que aqui utilizamos, mas as demonstrações são, indubitavelmente, muito elegantes. ◻

2.2 Sequências inteiras

Considere $S = (c_1, c_2, \ldots, c_r)$ uma sequência de números inteiros. Diremos, neste caso, que S é uma *sequência inteira*.

Definição 2.2. Seja p um número primo. Para cada $i \in \mathbb{N}$, definimos $\pi_i : \mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ o epimorfismo canônico, isto é,

$$\pi_i(c) = c \mod p^i.$$

O epimorfismo π_i preserva a soma de sequências, pois

$$\pi_i(\sigma(S)) = \pi_i(c_1 + c_2 + \cdots + c_r) = \sum_{j=1}^{r} \pi_i(c_j) = \sigma(\pi_i(S)).$$

Portanto, se $c_1 + \cdots + c_r \equiv 0 \mod p^i$, então $\sigma(\pi_i(S)) = 0$ e $\pi_i(S)$ é uma sequência de soma zero em $\mathbb{Z}/p^i\mathbb{Z}$.

Definição 2.3. Se $\pi_i(S)$ é uma sequência de soma zero e $\pi_{i+1}(S)$ não o é, diremos que S é uma *sequência secundária módulo* p^i.

Nesta seção, estamos interessados em determinar condições que garantam a existência de subsequências curtas e secundárias módulo p. Vamos considerar apenas sequências inteiras cujos elementos sejam não nulos módulo p.

Para facilitar as demonstrações, vamos escrever os elementos da sequência S como $c_i = a_i + pb_i$, com $a_i = \pi_1(c_i) \in [1, p-1]$.

Lema 2.4. *Se S é uma sequência inteira com comprimento $r \geq 3p-2$, então S possui uma subsequência curta e secundária módulo p.*

Demonstração. Pelo Lema 2.1, a sequência

$$(\pi_1(a_1), \pi_1(b_1)), (\pi_1(a_2), \pi_1(b_2)), \ldots, (\pi_1(a_r), \pi_1(b_r))$$

possui uma subsequência curta de soma zero em $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. Então existe um subconjunto $I \subset [1, r]$, com $|I| \leq p$, satisfazendo

$$\sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \mod p.$$

Portanto,

$$\sum_{i\in I} c_i \equiv \sum_{i\in I} a_i + p\sum_{i\in I} b_i \equiv 0 \mod p.$$

Como $0 < a_i < p$ para todo $i \in [1, r]$, concluímos que

$$\sum_{i\in I} c_i \not\equiv 0 \mod p^2.$$

É agora uma consequência da Definição 2.3 que a subsequência $\prod_{i\in I} c_i$ é secundária módulo p. ◪

Lema 2.5. *Se*

$$c_1 \equiv c_2 \equiv \cdots \equiv c_s \mod p$$

e $s \geq p+1$, então S possui uma subsequência curta e secundária módulo p.

Demonstração. Vamos escrever $a_i = a$, para $i \in [1, s]$. Portanto

$$\sum_{i=1}^{p} c_i = p(a + \sum_{i=1}^{p} b_i).$$

Se $\sum_{i=1}^{p} b_i \not\equiv -a \mod p$ então $\sum_{i=1}^{p} c_i \not\equiv 0 \mod p^2$ e a sequência $(c_1, \cdots, c_p)$ é secundária módulo p.
Então suponha $\sum_{i=1}^{p} b_i \equiv -a \mod p$. Neste caso, as imagens dos b_i pelo epimorfismo π_1 não podem ser todas iguais, já que $a \neq 0$. Portanto existe $j \in [1, p]$ satisfazendo

$$b_j \not\equiv b_{p+1} \mod p$$

e então

$$\sum_{\substack{i=1\\ i\neq j}}^{p} b_i + b_{p+1} \not\equiv -a \mod p,$$

o que conclui o lema. ◪

Lema 2.6. *Se S possui exatamente p elementos congruentes entre si módulo p e $|S| > p$, então S possui uma subsequência curta e secundária módulo p.*

Demonstração. Novamente, seja $a_i = a$ para $i \in [1,p]$. Se $b_1 \equiv \cdots \equiv b_p \mod p$, então

$$\sum_{i=1}^{p} b_i \not\equiv -a \mod p$$

e $(c_1, \cdots, c_p)$ é uma subsequência secundária de S. Podemos então supor que existem $i, j \in [1,p]$ tais que $b_i \not\equiv b_j \mod p$. Seja $c = c_{p+1} \in \operatorname{supp}(S)$ satisfazendo $\pi_1(c) \neq a$. Então existe um subconjunto $J \subset [1,p]$ com $|J| \leq p-1$ e (veja Lema 2.17)

$$\sum_{j \in J} c_j + c = |J|a + a_{p+1} + p\sum b_i \equiv 0 \mod p.$$

Se esta soma é zero módulo p^2, então é suficiente trocar b_i por b_j no subconjunto J, onde $b_i \not\equiv b_j \mod p$. ◻

Se $p = 3$ ou 5, o Lema 2.4 pode ser refinado, o que passamos a fazer em seguida.

Se $p = 3$, só existem dois elementos não nulos módulo p: 1 e 2. Neste caso, qualquer sequência com $2p-1$ elementos possui pelo menos três elementos repetidos e então os Lemas 2.5 e 2.6 implicam que S possui uma subsequência curta e secundária módulo p.

Vamos agora analisar o caso $p = 5$.

Lema 2.7. *Suponha que*

$$\pi_1(S) = (1,1,1,2,2).$$

Então S possui uma subsequência secundária módulo 5.

Demonstração. Consideremos duas subsequências $T_1|S$ e $T_2|S$ tais que $\pi_1(T_1) = (1,1,1,2)$ e $\pi_1(T_2) = (1,2,2)$. Então $\pi_1(T_1)$ e $\pi_1(T_2)$ são sequências de soma zero.

Sendo $p = 5$, temos $c_i = a_i + 5b_i$, com $a_i = 1$ se $i \in [1,3]$ e $a_4 = a_5 = 2$. Por argumentos já expostos nas demonstrações dos lemas 2.5 e 2.6, podemos assumir $\pi_1(b_i) = b$ se $i \in [1,3]$ e $\pi_1(b_4) = \pi_1(b_5) = b'$. Para estas subsequências,

$$\sum c_i \equiv 5 + 5(3b + b') \text{ ou } 5 + 5(b + 2b') \mod 5^2.$$

Deste modo, se $5(3b + b')$ ou $5(b + 2b')$ é incongruente a 20 módulo 25, o lema está

desmonstrado. Se não, considere o sistema de congruências

$$\begin{aligned} 5(3b+b') &\equiv 20 \mod 5^2 \\ 5(b+2b') &\equiv 20 \mod 5^2, \end{aligned}$$

que é equivalente a

$$\begin{aligned} 3b+b' &\equiv 4 \mod 5 \\ b+2b' &\equiv 4 \mod 5. \end{aligned} \tag{2.1}$$

Multiplicando a primeira equação de (2.1) por 2, obtemos $b+2b' \equiv 3 \mod 5$, o que contradiz a segunda equação. Segue que o sistema (2.1) não possui solução e as subsequências T_1 e T_2 não podem ser simultaneamente zero módulo 5^2. Portanto, ao menos uma destas subsequências é secundária módulo 5. ◪

Observação. O Lema 2.7 permanece válido se $\pi_1(S) = (1,1,3,3,3)$ ou $\pi_1(S) = (3,3,4,4,4)$. De fato, se c é inversível módulo p, então

$$\sigma(\pi_1(S)) = 0 \iff \sigma(\pi_1(cS)) = 0.$$

Lema 2.8. *Se S é uma sequência satisfazendo*

$$\pi_1(S) = (1,1,1,2,4,4),$$

então S possui uma subsequência secundária módulo 5.

Demonstração. Para provar este lema, basta considerar subsequências T_1, T_2 e T_3 tais que $\pi_1(T_1) = (1,4)$, $\pi_1(T_2) = (2,4,4)$ e $\pi_1(T_3) = (1,1,1,2)$, e proceder como na demonstração do Lema 2.7. A única diferença aqui é que obteremos um sistema de congruências módulo 25 com 3 equações, o que não chega a ser um complicador. ◪

Podemos utilizar o argumento da observação acima para concluir que o Lema 2.8 permanece válido se $\pi_1(S) = (1,1,3,4,4,4)$.

Os resultados construídos até aqui nos permitem enunciar o

Lema 2.9. *Suponha $p = 3$ ou 5. Se $|S| \geq 2p-1$, então S possui uma subsequência curta e secundária módulo p.*

Demonstração. O caso $p = 3$ já foi provado.

Suponha $p = 5$ e considere $c \in \mathrm{supp}(S)$ satisfazendo $v_c(S) = \max_{g\in G}(v_g(S))$. De acordo com os Lemas 2.5 e 2.6, podemos supor $v_c(S) = 3$ ou 4. Agora é suficiente observar que, nestas condições, a sequência $\pi_1(S)$ possui uma das seguintes subsequências

$$(1,1,1,2,2),\quad (1,1,3,3,3),\quad (3,3,4,4,4),\quad (1,1,1,2,4,4),\quad (1,1,3,4,4,4).$$

◪

O resultado do Lema 2.9 é o melhor possível. De fato, se

$$S = 1^{p-1}g^{p-1}$$

é uma sequência inteira com $\pi_2(g) = -1$ e $T|S$ é uma subsequência não vazia satisfazendo $\sigma(\pi_1(T)) = 0$, então $T = 1^u g^u$ para algum $u \in [1, p-1]$. Neste caso, $\sigma(\pi_2(T)) = 0$ e T não pode ser secundária módulo p.

2.3 Sequências livres de zeros

Uma sequência $S = (g_1, g_2, \ldots, g_r)$ em um grupo abeliano G é *livre de zeros* se, para qualquer subconjunto não vazio $I \subset [1, r]$,

$$\sum_{i\in I} g_i \neq 0.$$

Equivalentemente, S é livre de zeros se, e somente se, $0 \notin \Sigma(S)$.

Definição 2.10. Seja G um grupo abeliano finito e $p(G)$ o menor primo divisor da ordem de G. Para $t \in [1, p(G) - 1]$, definiremos $\mathfrak{s}_t = \mathfrak{s}_t(G)$ como o menor inteiro positivo tal que toda sequência S possuindo $\mathfrak{s}_t$ elementos não nulos de G possui uma subsequência livre de zeros de tamanho t.

Lema 2.11. *Para qualquer grupo G, $\mathfrak{s}_1(G) = 1$, $\mathfrak{s}_2(G) = 3$ e $\mathfrak{s}_3(G) = 5$.*

Demonstração. A primeira afirmação do lema é trivial.

Para demonstrar a segunda, considere $S = (g_1, g_2, g_3)$ em G. Como $p(G) > 2$, se $g_1 \neq -g_2$, então (g_1, g_2) é livre de zeros. Se $g_1 = -g_2$, temos (g_1, g_3) ou (g_2, g_3) livre de zeros.

Provemos agora a terceira afirmação. Seja $S = (g_1, g_2, g_3, g_4, g_5)$ uma sequência de elementos não nulos de G. Podemos supor, sem perda, que S possui no máximo dois elementos iguais.

Suponhamos que a sequência possua dois elementos iguais, digamos $S = g^2 g_3 g_4 g_5$. Se $g_i \notin \{-g, -2g\}$ para algum $i \in [3, 5]$, já temos uma subsequência livre de zeros. Se este não for o caso, teremos $S = g^2(-g)^2(-2g)$ ou $S = g^2(-2g)^2(-g)$. No primeiro caso, temos a subsequência $(-g)^2(-2g)$ e no segundo caso, a subsequência $g(-2g)^2$.

Se a sequência não possui elementos repetidos, podemos ordená-los de modo que as subsequências

$$g_1 g_2,\ g_1 g_3,\ g_1 g_4,\ g_2 g_3$$

sejam livres de zeros. Se $g_2 g_4$ é livre de zeros, então $g_1 g_2 g_3$ é livre de zeros ou $g_1 g_2 g_4$ o é. Se isto não ocorrer, então $g_3 g_4$ é livre de zeros e, portanto, ao menos uma das subsequências

$$g_1 g_2 g_3,\ g_1 g_3 g_4$$

é livre de zeros. ◪

O próximo lema fornece limites inferior e superior para o invariante $\mathfrak{s}_t(G)$, para qualquer grupo abeliano finito G.

Lema 2.12. *Para todo $t \in [1, p(G) - 1]$, vale*

$$2t - 1 \leq \mathfrak{s}_t(G) \leq (t-1)|G| - t + 2.$$

Demonstração. Se $g \neq 0$, a sequência g^t é livre de zeros em G. Por outro lado, o número de elementos não nulos no grupo G é $|G| - 1$. Segue que se uma sequência S não possui subsequência $T|S$ com $|T| = t$ e livre de zeros em G, então $|S| \leq (|G| - 1)(t - 1)$. Portanto,

$$\mathfrak{s}_t(G) \leq (t-1)|G| - t + 2.$$

Para obter a cota inferior considere a sequência

$$S = g^{t-1}(g^{-1})^{t-1},$$

onde $g \neq 0$. É simples verificar que S não possui subsequência livre de zeros de comprimento t. ◻

O Lema 2.11 nos diz que a cota inferior obtida no Lema 2.12 é atingida para $t \in [1,3]$. Vale aqui observar que a cota superior também é atingida. De fato, é possível provar que $\mathfrak{s}_{p-1}(C_p) = p^2 - 3p + 3$. Com isto e mais o Lema 2.11 determinamos completamente o invariante $\mathfrak{s}_t$ dos grupos C_3 e C_5.

Lema 2.13. *Seja S uma sequência em G e suponha $|\mathrm{supp}(S)| > t$. Se $v_g(S) \geq t-1$ para algum $g \in G$, então S possui uma subsequência livre de zeros de comprimento t.*

Demonstração. Usando a notação aditiva para relacionar os elementos no grupo G, considere as equações

$$g + x = 0$$

$$2g + x = 0$$

$$\vdots$$

$$(t-1)g + x = 0.$$

Como cada equação possui uma única solução e $|\mathrm{supp}(S)| > t$, podemos encontrar um elemento $h \in \mathrm{supp}(S)$ que não é solução de quaisquer destas equações. Segue que a subsequência curta

$$T = g^{t-1}h$$

é livre de zeros. ◻

Lema 2.14. *Suponha $G = C_p$ para um primo $p > 3$. Se $\dfrac{p-1}{2} < t < p-1$, então*

$$\mathfrak{s}_t(G) \leq (p-1)(t-2) + 1.$$

Demonstração. Seja S uma sequência em $G \setminus \{0\}$ com $|S| = (p-1)(t-2) + 1$.

Se $v_g(S) \geq t$ para algum $g \in G$, então $T = g^t$ satisfaz $|T| = t$ e é livre de zeros.

Vamos então assumir $v_g(S) \leq t-1$ para todo $g \in G$. Como

$$(t-2)(p-1) < |S|,$$

existe um elemento $h \in \mathrm{supp}(S)$ satisfazendo $v_h(S) = t-1$. Pelo Lema 2.13, podemos supor $|\mathrm{supp}(S)| \leq t$. Por outro lado,

$$|S| - (t-1)^2 = pt - 2p - (t^2 - t - 2) = (t-2)(p-t-1) > 0,$$

por hipótese. Assim, concluímos que $|\mathrm{supp}(S)| = t$. Mas

$$|S| - [t(t-1) - 1] = pt - 2p - t^2 + 4$$

e como $p \geq t+2$,

$$pt - 2p - t^2 + 4 \geq (t+2)(t-2) - t^2 + 4 \geq 0.$$

Portanto,

$$t(t-1) - 1 \leq |S| \leq t(t-1).$$

Sendo $t > \dfrac{p-1}{2}$, concluímos que existe $a \in \mathrm{supp}(S)$ tal que $v_a(S) = t-1$ e $2a \in \mathrm{supp}(S)$. Todos estes fatos nos levam a concluir que a subsequência

$$a^{t-1}(2a)$$

é livre de zeros. ◪

2.4 Outros resultados

Sejam A, B subconjuntos não vazios de um grupo abeliano G. O *conjunto-soma* de A e B é definido por

$$A + B = \{a + b; a \in A \ e \ b \in B\}.$$

Por exemplo, se $G = \mathbb{Z}/5\mathbb{Z}$, $A = \{1, 3\}$ e $B = \{1, 2, 4\}$, então $A + B = \{0, 2, 3, 4\}$.

Se $n \geq 3$ é um inteiro, podemos definir o conjunto-soma de n subconjuntos de um

grupo G de forma recursiva, isto é,

$$A_1 + \cdots + A_n = (A_1 + \cdots + A_{n-1}) + A_n.$$

Equivalentemente,

$$A_1 + \cdots + A_n = \{\sum_{i=1}^{n} a_i \ ; \ a_i \in A_i\}.$$

O próximo lema é o conhecido Teorema de Cauchy-Davenport. Ele fornece um limite inferior para a cardinalidade do conjunto-soma de subconjuntos de $\mathbb{Z}/p\mathbb{Z}$.

Lema 2.15 (Cauchy-Davenport)**.** *Seja p um primo e A, B subconjuntos não-vazios de $\mathbb{Z}/p\mathbb{Z}$. Então*

$$|A + B| \geq \min(p, |A| + |B| - 1).$$

Demonstração. Este é um resultado clássico e sua demonstração pode ser encontrada em inúmeras referências. Indicamos [4] para a prova exibida por Davenport e [14] para uma demonstração mais moderna. ◪

O Teorema de Cauchy-Davenport pode ser generalizado como segue.

Lema 2.16. *Seja $n \geq 2$, p um primo e $A_1, \ldots, A_n$ subconjuntos não-vazios de $\mathbb{Z}/p\mathbb{Z}$. Então*

$$|A_1 + \cdots + A_n| \geq \min(p, \sum_{i=1}^{n} |A_i| - n + 1).$$

Demonstração. A prova é por indução. O caso $n = 2$ é o Teorema de Cauchy-Davenport. Suponha que o resultado seja válido para n subconjuntos de $\mathbb{Z}/p\mathbb{Z}$ e escreva $A = A_1 + \cdots + A_n$. Pela hipótese de indução, temos

$$|A| \geq \min(p, \sum_{i=1}^{n} |A_i| - n + 1).$$

Aplicando novamente o Teorema de Cauchy-Davenport, vamos obter

$$\begin{aligned} |A_1 + \cdots + A_n + A_{n+1}| &= |A + A_{n+1}| \\ &\geq \min(p, |A| + |A_{n+1}| - 1) \\ &\geq \min(p, \sum_{\substack{i=1 \\ n+1}}^{n} |A_i| - n + 1 + |A_{n+1}| - 1) \\ &\geq \min(p, \sum_{i=1}^{n} |A_i| - (n+1) + 1), \end{aligned}$$

o que prova o lema. ◪

Lema 2.17. *Considere uma sequência $S = (a_1, ..., a_{p-1})$ de elementos não-nulos em $\mathbb{Z}/p\mathbb{Z}$. Então*

$$\mathbb{Z}/p\mathbb{Z} \setminus \{0\} \subset \Sigma(S).$$

Demonstração. Defina os conjuntos

$$A_i = \{0, a_i\},\ i \in [1, p-1].$$

Pelo Lema 2.16,

$$\begin{aligned} |A_1 + A_2 + \cdots + A_{p-1}| &\geq \min\{p, \sum_{i=1}^{p-1} |A_i| - (p-1) + 1\} \\ &= \min\{p, (p-1).2 - (p-1) + 1\} \\ &= p. \end{aligned}$$

Segue que, exceto possivelmente o zero, todo elemento de $\mathbb{Z}/p\mathbb{Z}$ pode ser obtido utilizando-se ao menos um elemento de S. ◪

Lema 2.18. *Se definirmos recursivamente*

$$\left\lfloor \frac{a}{m} \right\rfloor_{(1)} = \left\lfloor \frac{a}{m} \right\rfloor \quad e \quad \left\lfloor \frac{a}{m} \right\rfloor_{(k+1)} = \left\lfloor \frac{\left\lfloor \frac{a}{m} \right\rfloor_{(k)}}{m} \right\rfloor$$

com a, m, k números naturais, então

$$\left\lfloor \frac{a}{m} \right\rfloor_{(k)} = \left\lfloor \frac{a}{m^k} \right\rfloor.$$

Demonstração. Vamos definir a sequência

$$X_1 = \left\lfloor \frac{X}{m} \right\rfloor, X_2 = \left\lfloor \frac{X_1}{m} \right\rfloor, ..., X_l = \left\lfloor \frac{X_{l-1}}{m} \right\rfloor.$$

Para demonstrar o lema, é suficiente provar que $X_l = \left\lfloor \frac{X}{m^l} \right\rfloor$.

Temos

$$\begin{gathered} X = X_1 m + r_1, 0 \leq r_1 < m \\ X_1 = X_2 m + r_2, 0 \leq r_2 < m \\ \vdots \\ X_{l-1} = X_l m + r_l, 0 \leq r_l < m. \end{gathered}$$

Então

$$X = (X_2 m + r_2)m + r_1 = X_2 m^2 + R_2, \tag{2.2}$$

onde $R_2 = r_2 m + r_1$. Como $r_1, r_2 \leq m - 1$, temos

$$R_2 = r_2 m + r_1 \leq m(m-1) + m - 1 = m^2 - 1.$$

Portanto, $0 \leq R_2 < m^2$.

Usando (2.2), obtemos

$$X = (X_3 m + r_3)m^2 + R_2 = X_3 m^3 + R_3,$$

com $R_3 = r_3 m^2 + R_2$.
Analogamente ao que fizemos acima, temos $0 \leq R_3 < m^3$.

Uma indução simples nos dá

$$X = X_i m^i + R_i,$$

para todo $i \in [1, l]$, sendo

$$R_i = \begin{cases} r_1, & \text{se } i = 1. \\ r_i m^{i-1} + R_{i-1}, & \text{se } i > 1. \end{cases}$$

Assim,

$$R_l = r_l m^{l-1} + r_{l-1} \leq (m-1)m^{l-1} + m^{l-1} - 1 = m^l - 1.$$

Portanto $X = X_l m^l + R_l$, com $0 \leq R_l < m^l$, o que prova o lema. ◪

Capítulo 3

Pares de Formas de Grau $p^\tau(p-1)$

Doravante vamos supor que o par (1.1) tem grau $k = p^\tau(p-1)$. O principal resultado deste capítulo é o

Teorema 3.1. *Seja (f, g) um par de formas aditivas de grau $k = p^\tau(p-1)$ para um primo $p \geq 7$. Se*

$$n > 2\frac{p}{p-1}k^2 - 2k$$

e $\tau \geq \dfrac{p-1}{2}$, então o sistema (1.2) possui solução q-ádica para todo primo q.

Segundo [3], precisamos analisar apenas os casos em que $q = p$, pois para os outros primos $q \neq p$, a condição $n > 2k^2$ é suficiente para se obter solubilidade q-ádica.

3.1 Sequências em $\mathbb{Z}/p^m\mathbb{Z} \oplus \mathbb{Z}/p^m\mathbb{Z}$

Seja

$$\mathscr{A} = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_n \\ b_n \end{pmatrix}$$

a sequência dos coeficientes do sistema (1.1). Iniciamos esta seção definindo uma aplicação que nos permita olhar para os elementos de $\mathscr{A}$ quando inseridos no grupo $\mathbb{Z}/p^m\mathbb{Z} \oplus \mathbb{Z}/p^m\mathbb{Z}$.

Definição 3.2. Para cada natural i, definimos o homomorfismo

$$\varphi_i : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z} \oplus \mathbb{Z}/p^i\mathbb{Z}$$

com o auxílio do homomorfismo canônico π_i (Definição 2.2), como segue:

$$\varphi_i\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \pi_i(a) \\ \pi_i(b) \end{pmatrix}.$$

Uma subsequência $S|\mathscr{A}$ é dita *de soma zero módulo* p^m se $\sigma(\varphi_m(S)) = 0$. Além disso, inspirados na Definição 2.3, diremos que S é *secundária módulo* p^m se ela é uma sequência de soma zero módulo p^m mas não é de soma zero módulo p^{m+1}.

Suponha que (f, g) tenha a forma descrita em (1.5). Denote por M_i a subsequência de $\mathscr{A}$ constituída dos coeficientes que aparecem no par de subformas $(p^i f_i, p^i g_i)$. Dizemos que um elemento $\begin{pmatrix} a_j \\ b_j \end{pmatrix} \in \mathrm{supp}(\mathscr{A})$ está no nível l se ele está no par de subformas $(p^l f_l, p^l g_l)$.

Frequentemente nos será útil dividir os elementos de cada nível em classes de equivalência. Para tanto, vamos visualizar $\mathbb{F}_p^2 \setminus \{(0,0)\}$ como a união de $p+1$ subconjuntos $L_0, L_1, \ldots, L_p$, sendo

$$L_0 = \{\lambda\begin{pmatrix} 1 \\ 0 \end{pmatrix} |\ \ \lambda \in [1, p-1]\}$$

e

$$L_i = \{\lambda\begin{pmatrix} i \\ 1 \end{pmatrix} |\ \ \lambda \in [1, p-1]\}$$

para $i \in [1, p]$. Os conjuntos L_i são disjuntos e possuem um total de $(p-1)(p+1) = p^2 - 1$ elementos. Portanto

$$\mathbb{F}_p^2 \setminus \{(0,0)\} = \bigsqcup_{i=0}^{p} L_i. \tag{3.1}$$

Seja S uma subsequência de M_0. Em virtude de (3.1), cada elemento de $\varphi_1(S)$ estará em um (e somente um) dos conjuntos L_i. Neste contexto, vamos definir, para cada $j \in [0, p]$, a sequência

$$I_j(S) = \prod_{g \in B_j} g^{v_g(S)},$$

onde $B_j = \{g \in M_0\ ;\ \varphi_1(g) \in L_j\}$. Vamos escrever $i_j(S) = |I_j(S)|$ e diremos que um elemento $a \in M_0$ *é de classe* j se ele está no suporte de $I_j(M_0)$. Observe que podemos escrever a sequência S como o produto disjunto

$$S = \prod_{j=0}^{p} I_j(S).$$

De maneira completamente análoga, podemos dividir em classes os elementos que estão em níveis superiores. Se S é uma subsequência de M_l, definiremos

$$I_j(S) = \prod_{g \in C_j} g^{v_g(S)},$$

sendo $C_j = \{g \in M_l \ ; \ \varphi_1(p^{-l}g) \in L_j\}$, e diremos que g é de classe j.

Vamos definir também a sequência

$$Q_0(S) = SI_0(S)^{-1} = \prod_{j=1}^{p} I_j(S),$$

que é, obviamente, uma subsequência de S. Escreveremos ainda $q_0(S) = |Q_0(S)|$ e, por razões históricas, adotaremos $q_0 = q_0(M_0)$ (vide Lema 1.4).

Diremos que uma sequência $S|\mathscr{A}$ é *não-singular* se o conjunto $S \bigcap M_0$ possuir ao menos dois elementos em classes distintas. Se isto não ocorrer, diremos que S é singular.

Utilizando a transformação (1.4) e recorrendo ao Lema 1.1, podemos transformar qualquer par p-normalizado em outro p-equivalente de modo que, para uma subsequência $S|M_i$, vale

$$i_0(S) \geq i_p(S) \geq i_j(S)$$

para todo $j \in [1, p]$.

Com o intuito de garantir a existência de zeros p-ádicos para o sistema (1.1), o Lema 1.6 afirma que é suficiente provar a existência de uma solução não-singular para o sistema de congruências

$$\begin{aligned} a_1x_1^k + \cdots + a_nx_n^k &\equiv 0 \bmod p^\gamma \\ b_1x_1^k + \cdots + b_nx_n^k &\equiv 0 \bmod p^\gamma, \end{aligned} \tag{3.2}$$

sendo $\gamma = \tau + 1$. Mas

$$\phi(p^\gamma) = \phi(p^{\tau+1}) = (p-1)p^\tau = k,$$

onde ϕ é a função de Euler. Isto significa que obter uma solução não-singular para o sistema de congruências (3.2) é equivalente a encontrar uma solução para a equação

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}\varepsilon_1 + \cdots + \begin{pmatrix} a_n \\ b_n \end{pmatrix}\varepsilon_n = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \tag{3.3}$$

em $\mathbb{Z}/p^\gamma\mathbb{Z} \oplus \mathbb{Z}/p^\gamma\mathbb{Z}$, com pelo menos duas entradas não nulas $\varepsilon_u = \varepsilon_v = 1$, $u, v \in [1, m_0]$,

tais que $\begin{pmatrix} a_u \\ b_u \end{pmatrix}$ e $\begin{pmatrix} a_v \\ b_v \end{pmatrix}$ pertençam a classes distintas. Por outro lado, a equação (3.3) tem uma solução em $\mathbb{Z}/p^\gamma\mathbb{Z} \oplus \mathbb{Z}/p^\gamma\mathbb{Z}$ com esta propriedade se, e somente se, a sequência $\mathscr{A}$ possui uma subsequência não-singular de soma zero módulo p^γ.

Em resumo, para provar a existência de zeros p-ádicos não triviais para o par (f, g) no Teorema 3.1 é suficiente encontrar uma subsequênca não-singular de soma zero módulo p^γ da sequência $\mathscr{A}$.

3.2 Elementos primários e secundários

Considere a sequência

$$M_0 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \ldots, \begin{pmatrix} a_{m_0} \\ b_{m_0} \end{pmatrix}$$

dos elementos do nível zero e seja S uma subsequência de soma zero módulo p em M_0. Por definição,

$$\varphi_1(\sigma(S)) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Assim, ao somar os elementos de S, obtemos um novo elemento $\sigma(S) = \begin{pmatrix} A \\ B \end{pmatrix}$ no nível $l \geq 1$, já que $A \equiv B \equiv 0 \pmod{p}$. A este processo daremos o nome de *contração*.

No que fizemos acima nada há de especial com o nível zero. Assim é que se a sequência $\mathscr{A}$ possui uma subsequência S de soma zero módulo p^l, então

$$\varphi_l(\sigma(S)) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

e $\sigma(S) = \begin{pmatrix} A \\ B \end{pmatrix}$ passa a ser um elemento do nível l ou superior.

O processo de contração de uma sequência pode nos ajudar a obter elementos em níveis mais elevados, bastando, para tanto, que se tenha uma sequência de soma zero. O elemento resultante da contração será um *elemento primário* no nível l (ou superior) se ele for obtido pela contração de uma sequência não-singular de soma zero módulo p^l. Se S é uma sequência singular e secundária módulo p^l, diremos que o elemento resultante da

contração é um *elemento secundário* no nível l.

Vamos utilizar a notação P_l para denotar a sequência de elementos primários no nível l (ou superior) e S_l denotará a sequência dos elementos secundários no nível l. Utilizaremos ainda

$$p_l = |P_l| \quad \text{e} \quad s_l = |S_l|.$$

Em vista da definição acima, podemos considerar que os elementos que já se encontram naturalmente no nível l são, igualmente, elementos secundários do nível l. Portanto, a sequência S_l é formada pela sequência M_l e os elementos formados pela contração de sequências secundárias em níveis imediatamente inferiores.

O próximo teorema, provado em [7], nos fornece uma cota inferior para o comprimento da sequência P_1.

Teorema 3.3. *Se (f,g) é um par p-normalizado, então*

$$p_1 \geq \min\left(\left\lfloor \frac{m_0}{2p-1} \right\rfloor, \left\lfloor \frac{q_0}{p} \right\rfloor\right).$$

Vamos agora utilizar o Teorema 3.3 para calcular o número mínimo de elementos primários que podem ser obtidos no primeiro nível.

Pelo Lema 1.4,

$$q_0 \geq \frac{n}{2k} > k\frac{p}{p-1} - 1.$$

Portanto

$$q_0 \geq p^{\tau+1}. \tag{3.4}$$

Ainda pelo mesmo lema,

$$\sum_{i=0}^{l} m_i \geq (l+1)\frac{n}{k} > 2(l+1)(k\frac{p}{p-1} - 1)$$

e então

$$\sum_{i=0}^{l} m_i > 2(l+1)(p^{\tau+1} - 1). \tag{3.5}$$

Em particular, $m_0 > 2(p^{\tau+1} - 1)$.

Deste modo,

$$\frac{m_0}{2p-1} \geq \frac{2(p^{\tau+1}-1)+1}{2p-1}$$

e então o Teorema 3.3 fornece

$$p_1 \geq p^\tau. \tag{3.6}$$

A desigualdade (3.4) nos mostra o tamanho mínimo de Q_0. No entanto, para formar os elementos primários no nível 1 vamos utilizar apenas a quantidade mínima de elementos estabelecida por esta desigualdade. A razão para este procedimento é que restarão muito mais sequências para serem contraídas na forma de elementos secundários para o nível 1. Em decorrência disto, para produzir os p_1 elementos primários no nível 1 estaremos contraindo, no nível $l = 0$, no máximo p^τ sequências de comprimento máximo $2p$ cada uma. É por esta razão que definiremos

$$s_0 = m_0 - 2p^{\tau+1}. \tag{3.7}$$

Concluímos esta seção com três lemas que serão bastante úteis no restante do trabalho.

Lema 3.4. *Seja S uma subsequência de S_l. Se $i_j(S) \geq 3p-2$ para algum $j \in [0,p]$, então S possui uma subsequência curta e secundária módulo p^{l+1}.*

Demonstração. Pelo que já foi observado quando da definição das classes I_j, podemos supor

$$i_0(S) = \max_{j\in[0,p]}(i_j(S)) \geq 3p-2.$$

Seja

$$T = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_{3p-2} \\ b_{3p-2} \end{pmatrix}$$

uma subsequência de $I_0(S)$ de comprimento $3p-2$. Então

$$\varphi_{l+1}(T) = \begin{pmatrix} A_1 \\ 0 \end{pmatrix} \cdots \begin{pmatrix} A_{3p-2} \\ 0 \end{pmatrix},$$

com $A_i \neq 0$ para todo $i \in [1, 3p-2]$. Pelo Lema 2.4, a sequência inteira $(p^{-l}a_1, \ldots, p^{-l}a_{2p-1})$ possui uma subsequência curta e secundária módulo p. Segue que T (e consequentemente S) possui uma subsequência curta e secundária módulo p^{l+1}. ◪

Lema 3.5. *Se $p_l \geq p$ e $i_j(S_l) \geq p-1$ para algum $j \in [0,p]$, então podemos obter um elemento primário no nível $l+1$ utilizando no máximo $p-1$ elementos secundários.*

Demonstração. Se algum elemento primário já estiver em um nível maior que l, o resultado é trivial. Vamos então supor que os p_l elementos primários encontram-se exatamente no nível l.

Como já observado, podemos supor $i_0(S_l) \geq p-1$. Seja

$$T = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_p \\ b_p \end{pmatrix} \begin{pmatrix} c_1 \\ d_1 \end{pmatrix} \cdots \begin{pmatrix} c_{p-1} \\ d_{p-1} \end{pmatrix}$$

uma subsequência de S_l formada por p elementos primários e $p-1$ elementos de $I_0(S)$. Então

$$\varphi_1(p^{-l}T) = \begin{pmatrix} A_1 \\ B_1 \end{pmatrix} \cdots \begin{pmatrix} A_p \\ B_p \end{pmatrix} \begin{pmatrix} C_1 \\ 0 \end{pmatrix} \cdots \begin{pmatrix} C_{p-1} \\ 0 \end{pmatrix}.$$

Se $B_i = 0$ para algum $i \in [1,p]$, o Lema 2.17 garante que existe um subconjunto $J \subset [1,p-1]$ tal que

$$-A_i = \sum_{j \in J} C_j$$

e, portanto,

$$\varphi_{l+1}\left(\begin{pmatrix} a_i \\ b_i \end{pmatrix} + \sum_{j \in J} \begin{pmatrix} c_j \\ d_j \end{pmatrix} \right) = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

o que dá um elemento primário no nível $l+1$.

Suponhamos $B_i \neq 0$ para todo $i \in [1,p]$. Ainda utilizando o Lema 2.17, existe um subconjunto $J \subset [1,p]$ tal que

$$\sum_{j \in J} \begin{pmatrix} A_j \\ B_j \end{pmatrix} = \begin{pmatrix} A \\ 0 \end{pmatrix}.$$

Deste modo, se $A = 0$, já temos um elemento primário no nível $l+1$. Se não, procedemos como no caso anterior e concluímos o resultado. ◻

Lema 3.6. *Seja S uma subsequência de S_l. Se $i_0(S) \geq \mathfrak{s}_u(\mathbb{Z}/p\mathbb{Z})$ e $q_0(S) \geq \mathfrak{s}_v(\mathbb{Z}/p\mathbb{Z})$, então $\varphi_{l+1}(S)$ possui uma subsequência livre de zeros em $\mathbb{Z}/p^{l+1}\mathbb{Z} \oplus \mathbb{Z}/p^{l+1}\mathbb{Z}$ com comprimento $u+v$.*

Demonstração. Consideremos

$$T = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_r \\ b_r \end{pmatrix} \begin{pmatrix} c_1 \\ d_1 \end{pmatrix} \cdots \begin{pmatrix} c_s \\ d_s \end{pmatrix}$$

uma subsequência de S formada por $r = \mathfrak{s}_u(\mathbb{Z}/p\mathbb{Z})$ elementos de $I_0(S)$ e $s = \mathfrak{s}_v(\mathbb{Z}/p\mathbb{Z})$ elementos de $Q_0(S)$. Então

$$\varphi_1(p^{-l}T) = \begin{pmatrix} A_1 \\ 0 \end{pmatrix} \cdots \begin{pmatrix} A_r \\ 0 \end{pmatrix} \begin{pmatrix} C_1 \\ D_1 \end{pmatrix} \cdots \begin{pmatrix} C_s \\ D_s \end{pmatrix}.$$

Da definição 2.10, a sequência $(A_1, \ldots, A_r)$ possui uma subsequência livre de zeros em $\mathbb{Z}/p\mathbb{Z}$ de comprimento u. Do mesmo modo, podemos obter uma subsequência de $(D_1, \ldots, D_s)$ com comprimento v e livre de zeros em $\mathbb{Z}/p\mathbb{Z}$. Reenumerando os índices, se necessário for, podemos assumir que tais subsequências livres de zeros são, respectivamente, $(A_1, \ldots, A_u)$ e $(D_1, \ldots, D_v)$.

Segue que

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \notin \Sigma\left(\begin{pmatrix} A_1 \\ 0 \end{pmatrix} \cdots \begin{pmatrix} A_u \\ 0 \end{pmatrix} \begin{pmatrix} C_1 \\ D_1 \end{pmatrix} \cdots \begin{pmatrix} C_v \\ D_v \end{pmatrix}\right),$$

o que prova o lema. ◻

3.3 Demonstração do teorema principal

Pelo que já observamos, para demonstrar o Teorema 3.1 é suficiente provar que a sequência $\mathscr{A}$ dos coeficientes do sistema (1.1) possui uma subsequência não-singular de soma zero módulo p^γ. Como consequência da definição de elementos primários, isto equivale a provar que a sequência P_γ é não vazia, isto é, $p_\gamma \neq 0$.

Lema 3.7. *Seja $l \geq 0$. Então*

$$s_{l+1} \geq m_{l+1} + \left\lfloor \frac{s_l}{p} \right\rfloor - 3p.$$

Demonstração. Seguindo o processo de contração descrito na demonstração do Lema 3.4, o número de elementos em cada nível l que não poderão ser contraídos para formar um

elemento secundário no nível $l+1$ é no máximo

$$3(p^2-1).$$

Portanto,

$$s_{l+1} \geq m_{l+1} + \left\lfloor \frac{s_l - 3(p^2-1)}{p} \right\rfloor \geq m_{l+1} + \left\lfloor \frac{s_l}{p} \right\rfloor - 3p.$$

◪

De posse do Lema 3.7, vamos estabelecer uma desigualdade que nos permita saber o número de elementos secundários no nível l, independentemente do número de elementos no nível anterior. Doravante estaremos supondo $p \geq 7$.

Pelo Lema 3.7,

$$s_1 \geq m_1 + \left\lfloor \frac{s_0}{p} \right\rfloor - 3p,$$

sendo (conforme observado anteriormente) $s_0 = m_0 - 2p^{\tau+1}$. Podemos ainda reescrever a desigualdade acima como

$$s_1 \geq \left\lfloor \frac{pm_1 + s_0}{p} \right\rfloor - 3p. \tag{3.8}$$

Pelo mesmo lema,

$$s_2 \geq m_2 + \left\lfloor \frac{s_1}{p} \right\rfloor - 3p,$$

o que, em razão de (3.8), nos dá

$$s_2 \geq m_2 + \left\lfloor \frac{\left\lfloor \frac{pm_1 + s_0}{p} \right\rfloor - 3p}{p} \right\rfloor - 3p.$$

Então podemos aplicar o Lema 2.18 e obter

$$\begin{aligned} s_2 &\geq m_2 + \left\lfloor \frac{\left\lfloor \frac{pm_1 + s_0}{p} \right\rfloor}{p} \right\rfloor - 3p - 3 \\ &= m_2 + \left\lfloor \frac{pm_1 + s_0}{p^2} \right\rfloor - 3p - 3 \\ &= \left\lfloor \frac{p^2 m_2 + pm_1 + s_0}{p^2} \right\rfloor - 3p - 3. \end{aligned}$$

Procedendo de maneira análoga, temos

$$s_3 \geq m_3 + \left\lfloor \frac{\left\lfloor \frac{p^2m_2 + pm_1 + s_0}{p^2} \right\rfloor - 3p - 3}{p} \right\rfloor - 3p.$$

Como estamos supondo $p \geq 7$, temos

$$\begin{aligned} s_3 &\geq m_3 + \left\lfloor \frac{\left\lfloor \frac{p^2m_2 + pm_1 + s_0}{p^2} \right\rfloor - 4p}{p} \right\rfloor - 3p \\ &\geq \left\lfloor \frac{p^3m_3 + p^2m_2 + pm_1 + s_0}{p^3} \right\rfloor - 3p - 4. \end{aligned}$$

Todo este raciocínio nos leva ao

Lema 3.8. *Se $l \geq 1$, então*

$$s_l \geq \left\lfloor \frac{\sum_{i=0}^{l} p^i m_i}{p^l} \right\rfloor - 2p^{\tau-l+1} - 3p - 4.$$

Demonstração. A prova é por indução. Pela desigualdade (3.8), temos

$$s_1 \geq \left\lfloor \frac{pm_1 + m_0 - 2p^{\tau+1}}{p} \right\rfloor - 3p \geq \left\lfloor \frac{pm_1 + m_0}{p} \right\rfloor - 2p^\tau - 3p,$$

provando que o lema é válido se $l = 1$. Suponhamos que o resultado seja válido para algum

natural l. Então o Lema 3.7 nos dá

$$\begin{aligned} s_{l+1} &\geq m_{l+1} + \left\lfloor \frac{s_l}{p} \right\rfloor - 3p \\ &\geq m_{l+1} + \left\lfloor \frac{\left\lfloor \frac{\sum_{i=0}^{l} p^i m_i}{p^l} \right\rfloor - 2p^{\tau-l+1} - 3p - 4}{p} \right\rfloor - 3p \\ &\geq m_{l+1} + \left\lfloor \frac{\left\lfloor \frac{\sum_{i=0}^{l} p^i m_i}{p^l} \right\rfloor}{p} \right\rfloor - 2p^{\tau-l} - 4 - 3p. \end{aligned}$$

Agora podemos utilizar o Lema 2.18 para obter

$$\begin{aligned} s_{l+1} &\geq m_{l+1} + \left\lfloor \frac{\sum_{i=0}^{l} p^i m_i}{p^{l+1}} \right\rfloor - 2p^{\tau-l} - 3p - 4 \\ &= \left\lfloor \frac{\sum_{i=0}^{l+1} p^i m_i}{p^{l+1}} \right\rfloor - 2p^{\tau-(l+1)+1} - 3p - 4, \end{aligned}$$

o que mostra a validade do lema para $l+1$. ◪

Pela desigualdade (3.5),

$$\sum_{i=0}^{l} p^i m_i \geq \sum_{i=0}^{l} m_i > 2(l+1)(p^{\tau+1}-1)$$

e então

$$s_l \geq \left\lfloor \frac{2(l+1)p^{\tau+1} - 2(l+1)}{p^l} \right\rfloor - 2p^{\tau-l+1} - 3p - 4.$$

Sendo $l > 0$ e $p > 3$, a desigualdade acima fica

$$\begin{aligned} s_l &\geq \left\lfloor \frac{2(l+1)p^{\tau+1} - p^l}{p^l} \right\rfloor - 2p^{\tau-l+1} - 3p - 4 \\ &= 2(l+1)p^{\tau-l+1} - 1 - 2p^{\tau-l+1} - 3p - 4 \\ &= 2lp^{\tau-l+1} - 3p - 5, \end{aligned}$$

o que nos fornece uma cota inferior para o número de elementos secundários s_l em função do nível l, do primo p e da potência τ.

Se $l \in [1, \tau-1]$, então

$$s_l \geq 2lp^2 - 3p - 5. \tag{3.9}$$

Se $l = \tau$, temos

$$s_l \geq 2\tau p - 3p - 5$$

e como $\tau \geq \dfrac{p-1}{2}$, obtemos

$$s_\tau \geq p^2 - 4p - 5. \tag{3.10}$$

3.3.1 O caso $p \geq 11$

Lema 3.9. *Suponha $l \geq 1$. Se $p_l = p$ e $s_l \geq p^2 - 6p + 5$, então podemos obter um elemento primário no nível $l+1$ utilizando no máximo $p-1$ elementos secundários.*

Demonstração. Temos

$$i_0(S_l) \geq \left\lceil \frac{s_l}{p+1} \right\rceil \geq p - 6.$$

Além disso, o Lema 3.5 nos permite assumir $i_0(S_l) \leq p-2$. Como estamos supondo $p \geq 11$, temos $i_0(S_l) \geq \mathfrak{s}_3(\mathbb{Z}/p\mathbb{Z})$, de acordo com o Lema 2.11. Por outro lado, o Lema 2.14 nos dá

$$\begin{aligned} q_0(S_l) &\geq p^2 - 6p + 5 - (p-2) \\ &= p^2 - 7p + 7 \\ &= (p-1)(p-6) + 1 \\ &\geq \mathfrak{s}_{p-4}(\mathbb{Z}/p\mathbb{Z}). \end{aligned}$$

Segue do Lema 3.6 que S_l possui uma subsequência T livre de zeros em $\mathbb{Z}/p^{l+1}\mathbb{Z} \oplus \mathbb{Z}/p^{l+1}\mathbb{Z}$ tal que $|T| = p-1$.

Mas o Lema 2.1 garante que a sequência TP_l possui uma subsequência de soma zero módulo p^{l+1}, pois $|TP_l| = 2p-1$. Como T é livre de zeros em $\mathbb{Z}/p^{l+1}\mathbb{Z} \oplus \mathbb{Z}/p^{l+1}\mathbb{Z}$, tal subsequência deve conter ao menos um elemento de P_l e é, por este motivo, não-singular. A contração desta subsequência nos fornece um novo elemento primário no nível $l+1$, o que prova o lema. ◪

Lema 3.10. *Se $s_l \geq p^2 - 5p + 4$, então*

$$p_{l+1} \geq \left\lfloor \frac{p_l}{p} \right\rfloor.$$

Demonstração. Suponha $p_l \geq 3p$. Como $\eta(\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}) = 3p-2$, podemos construir um novo elemento primário no nível $l+1$ pela contração de uma subsequência $T|P_l$ enquanto $p_l \geq 3p-2$. Então

$$\begin{aligned} p_{l+1} &\geq \left\lfloor \frac{p_l - (2p-2)}{p} \right\rfloor \\ &\geq \left\lfloor \frac{p_l - 2p}{p} \right\rfloor \\ &= \left\lfloor \frac{p_l}{p} \right\rfloor - 2. \end{aligned}$$

Ou seja, com os p_l elementos primários no nível l é possível obter pelo menos $\left\lfloor \frac{p_l}{p} \right\rfloor - 2$ elementos primários no nível $l+1$, restando ao menos $2p$ elementos primários não contraídos. Como

$$s_l \geq p^2 - 5p + 4 = p^2 - 6p + 5 + p - 1,$$

podemos aplicar duas vezes o Lema 3.9 e obter outros dois elementos primários no nível $l+1$, o que nos dá o resultado.

Para concluir, suponha $p_l < 3p$. O resultado é imediato se $p_l < p$ e o Lema 3.9 nos dá pelo menos um elemento primário (ou pelo menos dois elementos primários) no nível $l+1$, conforme $p \leq p_l < 2p$ (ou $2p \leq p_l < 3p$). Em qualquer caso, teremos

$$p_{l+1} \geq \left\lfloor \frac{p_l}{p} \right\rfloor,$$

o que conclui o lema. ◪

Podemos agora concluir a prova do Teorema 3.1 no caso $p \geq 11$.

Por (3.9), temos $s_l \geq 2p^2 - 3p - 5$ para $0 < l < \tau$. Usando o Lema 3.10 e a equação (3.6), concluímos que $p_l \geq p^{\tau-l+1}$. Em particular, $p_\tau \geq p$. Por sua vez, a equação (3.10) nos dá

$$s_\tau \geq p^2 - 4p - 5 \geq p^2 - 6p + 5$$

e então o Lema 3.9 garante que $p_\gamma \neq 0$. Isto prova o Teorema 3.1 no caso $p \geq 11$, conforme

observação feita no início desta seção.

3.3.2 O caso $p = 7$

Lema 3.11. *Se $G = \mathbb{Z}/7\mathbb{Z}$, então $\mathfrak{s}_4(G) \leq 12$.*

Demonstração. Seja S uma sequência de elementos não nulos em $\mathbb{Z}/7\mathbb{Z}$ e suponha $|S| \geq 12$. O objetivo é provar que S possui uma subsequência livre de zeros em $\mathbb{Z}/7\mathbb{Z}$ de comprimento 4.

Se $v_g(S) \geq 4$ para algum $g \in \mathbb{Z}/7\mathbb{Z}$, o resultado segue trivialmente. Se $v_g(S) = 3$ para algum $g \in \mathbb{Z}/7\mathbb{Z}$, podemos usar o Lema 2.13 e supor $\text{supp}(S) \leq 4$, o que implica em $|S| \leq 12$. Se $v_g(S) \leq 2$ para todo elemento não nulo g, então novamente $|S| \leq 12$. Em qualquer caso, teremos $|S| \leq 12$.

Podemos supor (mas não provaremos) que

$$v_1(S) = \max_{g \in \mathbb{Z}/7\mathbb{Z}} (v_g(S)).$$

Com esta observação e as considerações anteriormente expostas, podemos afirmar que

$$S = (1,1,2,2,3,3,4,4,5,5,6,6) \text{ ou } S = (1,1,1,a,a,a,b,b,b,c,c,c).$$

No primeiro caso, temos a subsequência $(1,1,2,2)$ e o resultado segue. No segundo caso, se

$$\{a,b,c\} \cap \{2,3\} \neq \varnothing,$$

temos as subsequências $(1,1,1,2)$ ou $(1,1,1,3)$, que são claramente livres de zeros em $\mathbb{Z}/7\mathbb{Z}$. A última possibilidade é ter $S = (1,1,1,4,4,4,5,5,5,6,6,6)$ e, neste caso, podemos extrair a subsequência $(1,4,4,4)$.

Concluímos, portanto, que se S não possui subsequência livre de zeros de comprimento 4 em $\mathbb{Z}/7\mathbb{Z}$, então $|S| \leq 11$. ◰

Vamos à demonstração do Teorema 3.1 quando $p = 7$.

Da desigualdade (3.9), temos $s_l \geq 2p^2 - 3p - 5 = 72$ se $l \in [0, \tau - 1]$. Então

$$i_0(S_l) \geq \left\lceil \frac{72}{8} \right\rceil = 9.$$

Com isto, podemos aplicar os Lemas 2.1 e 3.5 e proceder como no caso $p \geq 11$ para obter

$$p_{l+1} \geq \left\lfloor \frac{p_l}{7} \right\rfloor.$$

Como $p_1 \geq 7^\tau$, concluímos que $p_\tau \geq 7$.

Por (3.10), temos $s_\tau \geq p^2 - 4p - 5 = 16$, o que dá $i_0(S_\tau) \geq 2$, pois $S_\tau = \prod_{j=0}^{p} I_j(S_\tau)$ e $i_0(S_\tau) = \max_{j\in[0,p]}(i_j(S_\tau))$.

Passamos agora à demonstração de que $p^\gamma \neq 0$. A prova é dividida em quatro casos.

Se $i_0(S_\tau) \geq 6$, o resultado segue diretamente do Lema 3.5.

Se $i_0(S_\tau) = 5$, então $i_0(S_\tau) = \mathfrak{s}_3(\mathbb{Z}/7\mathbb{Z}) \leq q_0(S_\tau)$. Segue do Lema 3.6 que S_τ possui uma subsequência T livre de zeros em $\mathbb{Z}/7^{\tau+1}\mathbb{Z} \oplus \mathbb{Z}/7^{\tau+1}\mathbb{Z}$ satisfazendo $|T| = 6$. Como $p_\tau \geq 7$, o Lema 2.1 garante que a sequência TP_l possui uma subsequência de soma zero módulo p^τ. Como T é livre de zeros, esta subsequência deve ser, necessariamente, não-singular módulo p^γ, como queríamos.

Se $3 \leq i_0(S_\tau) \leq 4$, então $q_0(S_\tau) \geq 12$. Pelo Lema 3.11, temos $q_0(S_\tau) \geq \mathfrak{s}_4(\mathbb{Z}/7\mathbb{Z})$ e como $i_0(S_\tau) \geq \mathfrak{s}_2(\mathbb{Z}/7\mathbb{Z})$, o Lema 3.6 garante que S_τ possui uma subsequência T de comprimento 6 que é livre de zeros em $\mathbb{Z}/7^{\tau+1}\mathbb{Z} \oplus \mathbb{Z}/7^{\tau+1}\mathbb{Z}$. A partir daqui, basta proceder como no caso anterior.

Finalmente, analisemos o caso $i_0(S_\tau) = 2$. Neste caso, $s_\tau = 16$ e $i_j(S_\tau) = 2$ para todo $j \in [0, 7]$.

Suponha que $I_0(S_\tau)$ é uma sequência livre de zeros em $\mathbb{Z}/7^{\tau+1}\mathbb{Z} \oplus \mathbb{Z}/7^{\tau+1}\mathbb{Z}$. Como $q_0(S_\tau) = 14 > \mathfrak{s}_4(\mathbb{Z}/7\mathbb{Z})$, podemos obter uma subsequência livre de zeros em $\mathbb{Z}/7^{\tau+1}\mathbb{Z} \oplus \mathbb{Z}/7^{\tau+1}\mathbb{Z}$ de comprimento 6, pois $i_0(S_\tau) = 2$ e estamos supondo $I_0(S_\tau)$ livre de zeros em $\mathbb{Z}/7^{\tau+1}\mathbb{Z} \oplus \mathbb{Z}/7^{\tau+1}\mathbb{Z}$. Isto nos dá $p_\gamma \neq 0$. O mesmo argumento se aplica se, para algum $j \in [1, 7]$, a sequência $I_j(S_\tau)$ for livre de zeros em $\mathbb{Z}/7^{\tau+1}\mathbb{Z} \oplus \mathbb{Z}/7^{\tau+1}\mathbb{Z}$.

Portanto podemos supor que para todo $j \in [0, 7]$, $I_j(S_\tau)$ é uma sequência de soma zero

módulo 7^γ. Seja

$$Q_0(S_\tau) = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_{14} \\ b_{14} \end{pmatrix}$$

e

$$\varphi_1(p^{-\tau}Q_0(S_\tau)) = \begin{pmatrix} A_1 \\ B_1 \end{pmatrix} \cdots \begin{pmatrix} A_{14} \\ B_{14} \end{pmatrix}.$$

Pelo que observamos anteriormente, se $\begin{pmatrix} a_i \\ b_i \end{pmatrix}$ e $\begin{pmatrix} a_j \\ b_j \end{pmatrix}$ pertencem à mesma classe, então $B_i + B_j = 0$. Ou seja, $(B_i, B_j) = (1,6), (2,5)$ ou $(3,4)$. Como existem 7 classes em $Q_0(S_\tau)$, concluímos que existem B_u, B_v em classes distintas tais que $B_u + B_v = 0$ e $A_u + A_v \neq 0$. Portanto

$$\begin{pmatrix} a_u \\ b_u \end{pmatrix} + \begin{pmatrix} a_v \\ b_v \end{pmatrix} \in I_0(S_\tau)$$

e passamos a ter $i_0(S_\tau) \geq \mathfrak{s}_2(\mathbb{Z}/7\mathbb{Z})$. Como

$$\left| \begin{pmatrix} a_u \\ b_u \end{pmatrix}^{-1} \begin{pmatrix} a_v \\ b_v \end{pmatrix}^{-1} Q_0 \right| = 12 \geq \mathfrak{s}_4(\mathbb{Z}/7\mathbb{Z}),$$

podemos aplicar o Lema 3.6 para concluir a demonstração do Teorema 3.1.

Capítulo 4

Pares de Formas de Grau 2.3^τ e 4.5^τ

No Capítulo 3, vimos que se $p \geq 7$ e

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

a hipótese $\tau \geq \dfrac{p-1}{2}$ é suficiente para se garantir zeros p-ádicos para o sistema (1.1). Neste capítulo, provaremos este resultado para os primos 3 e 5, sem hipóteses adicionais sobre a potência τ. Mais especificamente,

Teorema 4.1. *Seja (f, g) um par de formas aditivas de grau $k = p^\tau(p-1)$, com coeficientes racionais e $p = 3$ ou 5. Se*

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

então o par de equações (1.2) *possui solução p-ádica.*

O próximo lema nos auxiliará na tarefa de demonstrar o Teorema 4.1

Lema 4.2. *Suponhamos $p = 3$ ou 5 e S uma subsequência de S_l. Se $i_j(S) \geq 2p-1$ para algum $j \in [0, p]$, então S possui uma subsequência curta e secundária módulo p^{l+1}.*

Demonstração. Sem perda de generalidade, podemos assumir $i_0(S) \geq 2p-1$. Seja

$$T = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_{2p-1} \\ b_{2p-1} \end{pmatrix}$$

uma subsequência de $I_0(S)$ de comprimento $2p-1$. Então

$$\varphi_1(p^{-l}T) = \begin{pmatrix} A_1 \\ 0 \end{pmatrix} \ldots \begin{pmatrix} A_{2p-1} \\ 0 \end{pmatrix},$$

com $A_i \neq 0$ para todo $i \in [1, 2p-1]$. Pelo Lema 2.9, a sequência $(p^{-l}a_1, \ldots, p^{-l}a_{2p-1})$ possui uma subsequência curta e secundária módulo p. Segue que T possui uma subsequência curta e secundária módulo p^{l+1}. ◪

4.1 O caso $p = 3$

No capítulo anterior, construímos os elementos secundários em um nível l através da contração de subsequências secundárias da sequência S_{l-1}. Podemos notar, entretanto, que os elementos destas subsequências secundárias estavam sempre em uma mesma classe. Para provar o Teorema 4.1 quando $p = 3$, precisamos avançar um pouco mais. Ao se esgotar o procedimento descrito, será necessário combinar elementos de classes distintas a fim de se obter elementos secundários adicionais.

Vale salientar que, diferentemente do que ocorreu no Capítulo 3, as subsequências secundárias obtidas através deste novo processo não são sequências curtas. Porém como os elementos secundários obtidos são adicionais, o método é útil e tem algumas vantagens.

Seja S uma subsequência de S_l. Já sabemos que é possível escrever S como o produto (disjunto)

$$S = I_0 I_1 I_2 I_3, \tag{4.1}$$

onde $I_j = I_j(S)$.

O seguinte lema reúne simples observações acerca da estrutura das classes módulo 3 e, por esta razão, sua demonstração será omitida.

Lema 4.3. *Supondo S como acima, temos*

(i) Se $u \in \mathrm{supp}(I_1)$ e $v \in \mathrm{supp}(I_2)$, então $u + v \in \mathrm{supp}(I_0 I_3)$.

(ii) Se $u, v \in \mathrm{supp}(I_1 I_2)$ e $w \in \mathrm{supp}(I_3)$, então existem $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{0, 1\}$ de modo que $\varepsilon_1 u + \varepsilon_2 v + \varepsilon_3 w \in \mathrm{supp}(I_0)$.

O Lema 4.3 continua válido se trocarmos I_0 por I_3 no item (ii).

Lema 4.4. *Seja S uma subsequência de S_l de comprimento r.*
(i) *Se $r \geq 10$, então S possui pelo menos uma subsequência secundária módulo p^{l+1}.*
(ii) *Se $r \geq 14$, então S possui pelo menos duas subsequências secundárias módulo p^{l+1}.*

Demonstração. Escreva

$$S = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_r \\ b_r \end{pmatrix}.$$

(i) Observe que $i_0(S) \geq 3$.

Se $i_0(S) \geq 5$, o resultado segue do Lema 4.2.

Suponhamos então $i_0(S) = 4$. Sem perda, podemos supor que

$$I_0(S) = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_4 \\ b_4 \end{pmatrix}.$$

Temos $i_3(S) \geq 2$ e então podemos obter $J \subset [5, r]$ com $|J| \leq 3$ e

$$\sum_{j \in J} \begin{pmatrix} a_j \\ b_j \end{pmatrix} \varepsilon_j \in \mathrm{supp}(I_0(S)),$$

de acordo com o Lema 4.3 (ii). Agora, aplicamos o Lema 4.2 à sequência

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_4 \\ b_4 \end{pmatrix} \begin{pmatrix} \sum_{j \in J} a_j \\ \sum_{j \in J} b_j \end{pmatrix}$$

e obtemos a subsequência desejada.

Agora suponha $i_0(S) = 3$. Então $\mathrm{supp}(S)$ possui elementos de todas as 4 classes e, pelo item (i) do Lema 4.3, concluímos que existem 2 elementos cuja soma é de classe 0 ou 3. Mas $i_3(S) = 3 = i_0(S)$, de sorte que podemos supor, sem perda,

$$\begin{pmatrix} a_9 \\ b_9 \end{pmatrix} + \begin{pmatrix} a_{10} \\ b_{10} \end{pmatrix} \in \mathrm{supp}(I_0(S)).$$

Além disso, pelo item (ii) do mesmo lema, podemos obter $J \subset [4,8]$ com $|J| \leq 3$ e

$$\sum_{j\in J}\begin{pmatrix} a_j \\ b_j \end{pmatrix}\varepsilon_j \in \mathrm{supp}(I_0(S)).$$

Então aplique novamente o Lema 4.2 à sequência

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}\begin{pmatrix} a_2 \\ b_2 \end{pmatrix}\begin{pmatrix} a_3 \\ b_3 \end{pmatrix}\begin{pmatrix} a_9+a_{10} \\ b_9+b_{10} \end{pmatrix}\begin{pmatrix} \sum_{j\in J} a_j \\ \sum_{j\in J} b_j \end{pmatrix}.$$

Isto conclui (i).

(ii) Neste caso, temos $i_0(S) \geq 4$. Pelo que já vimos, só precisamos nos preocupar com o caso $i_0(S) = 4$.
Novamente, $\mathrm{supp}(S)$ possui as 4 classes representadas, de modo que existem dois elementos cuja soma é de classe 0. Isto nos permite obter uma subsequência secundária módulo p^{l+1} com comprimento máximo 4. Ficamos então com uma subsequência $T|S$ com $|T| = r^* \geq 10$, o que nos permite aplicar o item (i) para obter a outra subsequência. ◲

Lema 4.5. *Seja S uma subsequência de S_l de comprimento $r \geq 11$. Então S possui pelo menos*

$$\left\lfloor \frac{r-8}{3} \right\rfloor$$

subsequências secundárias módulo p^{l+1}.

Demonstração. Se $11 \leq r \leq 16$, o resultado segue do Lema 4.4.

Suponha então $r \geq 17$. Como só existem 4 classes módulo 3, ao menos uma classe possui mais que 4 elementos em $\mathrm{supp}(S)$. Sem perda, podemos supor $i_0(S) \geq 5$ e, pelo Lema 4.2, a sequência S possui uma subsequência T que é curta e secundária módulo p^{l+1}. Este raciocínio pode ser aplicado sempre que $|ST^{-1}| \geq 17$. Usando esta ideia, podemos obter elementos secundários módulo p^{l+1} até a sequência S possuir menos que 17 elementos (e mais que 13, obviamente). Resta-nos então uma subsequência $T'|S$ com $|T'| \geq 14$. Então o item (ii) do Lema 4.4 nos diz que o número de subsequências secundárias módulo p^{l+1} contidas em S é no mínimo

$$\left\lfloor \frac{r-14}{3} \right\rfloor + 2 = \left\lfloor \frac{r-8}{3} \right\rfloor.$$

◲

Lema 4.6. *Para todo $l \geq 1$, vale*

$$s_{l+1} \geq m_{l+1} + \left\lfloor \frac{s_l}{3} \right\rfloor - 3.$$

Demonstração. A sequência dos elementos secundários do nível $l+1$ é composta pelos elementos secundários que lá estão mais os elementos secundários que provenham da contração de subsequências secundárias do nível l. Deste modo, podemos usar o Lema 4.5 para obter

$$s_{l+1} \geq m_{l+1} + \left\lfloor \frac{s_l - 8}{3} \right\rfloor \geq m_{l+1} + \left\lfloor \frac{s_l}{3} \right\rfloor - 3.$$

◪

Embora seja útil, o Lema 4.6 apenas estabelece uma relação entre as quantidades de elementos secundários de um determinado nível e do anterior. Seria interessante (e ainda mais útil) obtermos a quantidade de elementos secundários no nível l, tendo como referência apenas a variável envolvida (neste caso, l) e não os níveis anteriores. Para tanto, vamos usar os Lemas 2.18 e 4.6.

O Lema 4.6 fornece

$$s_1 \geq m_1 + \left\lfloor \frac{s_0}{3} \right\rfloor - 3,$$

o que pode ser reescrito como

$$s_1 \geq \left\lfloor \frac{3m_1 + s_0}{3} \right\rfloor - 3. \tag{4.2}$$

Novamente, o Lema 4.6 nos dá

$$\begin{aligned} s_2 &\geq m_2 + \left\lfloor \frac{s_1}{3} \right\rfloor - 3 \\ &= m_2 + \left\lfloor \frac{\left\lfloor \frac{3m_1 + s_0}{3} \right\rfloor - 3}{3} \right\rfloor - 3 \\ &\geq m_2 + \left\lfloor \frac{\left\lfloor \frac{3m_1 + s_0}{3} \right\rfloor}{3} \right\rfloor - 1 - 3. \end{aligned}$$

Usando o Lema 2.18, obtemos

$$s_2 \geq \left\lfloor \frac{9m_2 + 3m_1 + s_0}{9} \right\rfloor - 4.$$

Sucessivas aplicações dos Lemas 2.18 e 4.6 e o fato de que $s_0 = m_0 - 2.3^{\tau+1}$ nos dá o

Lema 4.7. *Para $l \in [1, \tau]$, temos*

$$s_l \geq \left\lfloor \frac{\sum_{i=0}^{l} 3^i m_i}{3^l} \right\rfloor - 2.3^{\tau-l+1} - 5.$$

Demonstração. Já demonstramos o caso $l = 1$. Suponhamos que o lema seja válido para $l > 1$. Usando os Lemas 2.18 e 4.6, teremos

$$\begin{aligned}
s_{l+1} &\geq m_{l+1} + \left\lfloor \frac{s_l}{3} \right\rfloor - 3 \\
&\geq m_{l+1} + \left\lfloor \frac{\left\lfloor \frac{\sum_{i=0}^{l} 3^i m_i}{3^l} \right\rfloor - 2.3^{\tau-l+1} - 5}{3} \right\rfloor - 3 \\
&\geq m_{l+1} + \left\lfloor \frac{\sum_{i=0}^{l} 3^i m_i}{3^{l+1}} \right\rfloor - 2.3^{\tau-l-1+1} - 2 - 3 \\
&= \left\lfloor \frac{\sum_{i=0}^{l+1} 3^i m_i}{3^{l+1}} \right\rfloor - 2.3^{\tau-(l+1)+1} - 5,
\end{aligned}$$

o que conclui o lema. ◪

Lema 4.8. *Suponha $l \geq 1$. Se $p_l \geq 3$ e $s_l \geq 2$, então podemos obter um elemento primário no nível $l+1$ utilizando no máximo 2 elementos secundários.*

Demonstração. Considere a sequência

$$S = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \begin{pmatrix} a_3 \\ b_3 \end{pmatrix} \begin{pmatrix} c_1 \\ d_1 \end{pmatrix} \begin{pmatrix} c_2 \\ d_2 \end{pmatrix},$$

onde os três primeiros elementos são primários e os outros dois são elementos secundários módulo p^l. Se algum destes elementos primários está além do nível l, não há mais nada a ser feito. Vamos então supor que os elementos $\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$, $\begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$ e $\begin{pmatrix} a_3 \\ b_3 \end{pmatrix}$ estejam precisamente no nível l. Se os dois elementos secundários pertencem à mesma classe, podemos aplicar o Lema 3.5 e finalizar a demonstração. Então podemos supor que

$$\varphi_{l+1}\left(\begin{pmatrix} c_1 \\ d_1 \end{pmatrix} + \begin{pmatrix} c_2 \\ d_2 \end{pmatrix} \right) \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

pois elementos de classes distintas não podem ter soma zero. Mas o Lema 2.1 afirma que a sequência $\varphi_{l+1}(S)$ possui uma subsequência de soma zero e, portanto, tal subsequência deve incluir ao menos um dos elementos primários. ◪

Lema 4.9. *Se $s_l \geq 4$, então*

$$p_{l+1} \geq \left\lfloor \frac{p_l}{3} \right\rfloor.$$

Demonstração. Suponha inicialmente $p_l \geq 9$. Como $\eta(C_3 \oplus C_3) = 3p - 2 = 7$ (Lema 2.1), concluímos que os elementos primários no nível $l+1$ podem ser construídos contraindo-se subsequências curtas de soma zero em P_l, enquanto for válida a condição $p_l \geq 7$. Portanto

$$p_{l+1} \geq \left\lfloor \frac{p_l - 6}{3} \right\rfloor.$$

Com os 6 elementos primários restantes e mais 4 elementos secundários, podemos aplicar duas vezes o Lema 4.8 e obter mais dois elementos primários no nível $l+1$. Ou seja,

$$p_{l+1} \geq \left\lfloor \frac{p_l - 6}{3} \right\rfloor + 2 = \left\lfloor \frac{p_l}{3} \right\rfloor.$$

Agora, suponha $p_l < 9$. Se $p_l < 3$, o resultado é imediato, e se $3 \leq p_l \leq 8$, a aplicação do Lema 4.8, uma ou duas vezes, já garante a validade do resultado. ◪

Estamos agora em posição de demonstrar o Teorema 4.1 para $p = 3$.

Demonstração. Pelo Teorema 3.3,

$$p_1 \geq \min\left(\left\lfloor \frac{2(3^{\tau+1} - 1)}{5} \right\rfloor, \left\lfloor \frac{3^{\tau+1}}{3} \right\rfloor\right) = 3^\tau. \tag{4.3}$$

O nosso objetivo é provar que $p_\gamma \neq 0$. Para tanto, o Lema 4.8 afirma que é suficiente provar que

$$p_\tau \geq 3 \text{ e } s_\tau \geq 2.$$

Para obter a primeira desigualdade, vamos utilizar os Lemas 4.9 e 4.7.

Para $l \geq 1$, já vimos que

$$s_l \geq \left\lfloor \frac{\sum_{i=0}^{l} 3^i m_i}{3^l} \right\rfloor - 2.3^{\tau-l+1} - 5.$$

Por outro lado, segue da desigualdade (3.5) que

$$\sum_{i=0}^{l} 3^i m_i \geq \sum_{i=0}^{l} m_i > 2(l+1).(3^{\tau+1}-1).$$

Agora, o Lema 4.7 dá

$$s_l \geq \left\lfloor \frac{2(l+1).3^{\tau+1} - 2l - 1}{3^l} \right\rfloor - 2.3^{\tau-l+1} - 5$$

e como $2l + 1 \leq 3^l$ para todo inteiro l, obtemos

$$s_l \geq \left\lfloor \frac{2(l+1).3^{\tau+1} - 3^l}{3^l} \right\rfloor - 2.3^{\tau-l+1} - 5 = 2(l+1).3^{\tau-l+1} - 1 - 2.3^{\tau-l+1} - 5.$$

Portanto

$$s_l \geq 2l.3^{\tau-l+1} - 6. \tag{4.4}$$

Segue que se $l \in [1, \tau-1]$, então

$$s_l \geq 2.1.3^{\tau-(\tau-1)+1} - 6 = 2.3^2 - 6 = 12.$$

Utilizando (4.3) e aplicando repetidamente o Lema 4.9, podemos obter $p_{l+1} \geq 3^{\tau-l}$ para $l \in [1, \tau-1]$. Em particular, $p_\tau \geq 3$. Agora o Lema 4.8 nos diz que para concluir nossa demonstração é suficiente provar que $s_\tau \geq 2$.

Pela desigualdade (4.4), se $l = \tau$, obtemos $s_\tau \geq 6\tau - 6$, o que dá $s_\tau \geq 6$ se $\tau \geq 2$. Se $\tau = 1$, podemos utilizar a desigualdade (4.2) e o fato de que $s_0 = m_0 - 2.3^{\tau+1}$ para obter

$$s_1 \geq \left\lfloor \frac{3m_1 + m_0 - 2.3^2}{3} \right\rfloor - 3 = \left\lfloor \frac{3m_1 + m_0}{3} \right\rfloor - 9.$$

Por outro lado, já vimos que

$$\sum_{i=0}^{l} m_i > 2(l+1).(3^{\tau+1}-1),$$

o que implica em $m_0 + 3m_1 \geq 33$. Logo $s_1 \geq 11 - 9 = 2$, o que conclui a demonstração do Teorema 4.1 para $p = 3$. ◪

4.2 O caso $p = 5$

Vamos agora finalizar a demonstração do Teorema 4.1, provando-o quando $p = 5$. É importante salientar que as ideias aqui contidas em muito se assemelham àquelas utilizadas na demonstração do Teorema 3.1.

Lema 4.10. *Seja $l \geq 1$. Se $p_l \geq 5$ e $s_l \geq 7$, então podemos obter um elemento primário no nível $l+1$ utilizando no máximo 4 elementos secundários.*

Demonstração. Seja S uma subsequência de S_l composta por 5 elementos primários e 7 elementos secundários. Vamos escrever $S = T_1T_2$, sendo T_1 a subsequência dos elementos primários e

$$T_2 = \prod_{i=1}^{7} \begin{pmatrix} c_i \\ d_i \end{pmatrix}$$

a subsequência dos elementos secundários.

Pelo que já observamos anteriormente, podemos supor que os 5 elementos primários encontram-se exatamente no nível l. Também podemos supor $i_0(T_2) \leq 4$, de acordo com o Lema 3.5. Além disso, o fato de só existirem 6 classes módulo 5 garante que $i_0(T_2) \geq 2$. Temos, desse modo, 2 casos para serem analisados.

Suponha inicialmente $i_0(T_2) = 3$. Neste caso, temos $q_0(T_2) = 4$ e pelo fato do Lema 2.11 nos garantir que $\mathfrak{s}_2(C_5) = 3$, podemos retirar de T_2 uma subsequência T_2' livre de zeros em $\mathbb{Z}/5^{l+1}\mathbb{Z} \oplus \mathbb{Z}/5^{l+1}\mathbb{Z}$ de comprimento 4 (veja o Lema 3.6). Como a sequência T_1T_2' deve ter, necessariamente, uma subsequência de soma zero módulo p^{l+1}, concluímos que S possui uma subsequência cuja contração fornece um elemento primário no nível $l+1$.

Suponha agora $i_0(T_2) = 2$. Então $q_0(T_2) = 5 \geq \mathfrak{s}_3(C_5)$ e podemos novamente obter uma

subsequência $T_2'|T_2$ com 4 elementos e livre de zeros em $\mathbb{Z}/5^{l+1}\mathbb{Z}\oplus\mathbb{Z}/5^{l+1}\mathbb{Z}$. A demonstração agora é análoga ao caso anterior. ◪

Lema 4.11. *Se $s_l \geq 11$, então*

$$p_{l+1} \geq \left\lfloor \frac{p_l}{5} \right\rfloor.$$

Demonstração. Suponha $p_l \geq 15$. Utilizando o Lema 2.1, obtemos

$$p_{l+1} \geq \left\lfloor \frac{p_l - 15}{5} \right\rfloor = \left\lfloor \frac{p_l}{5} \right\rfloor - 3.$$

Com estes 15 elementos primários restantes, podemos novamente aplicar o Lema 2.1 e formar um outro elemento primário no nível $l+1$, utilizando no máximo cinco elementos do nível l. Como ainda restarão 10 elementos primários no nível l e estamos supondo $s_l \geq 11$, podemos aplicar o Lema 4.10 e obter mais dois elementos primários.

Para concluir, se $5 \leq p_l < 15$, o resultado segue do Lema 4.10, e se $p_l < 5$, o resultado segue trivialmente. ◪

Se aplicarmos recursivamente o Lema 4.2 na contração de subsequências secundárias módulo p^{l+1}, os elementos secundários restantes somarão no máximo

$$(p+1)(2p-2) = 48.$$

Ou seja,

$$\begin{aligned} s_{l+1} &\geq m_{l+1} + \left\lfloor \frac{s_l - 48}{5} \right\rfloor \\ &\geq m_{l+1} + \left\lfloor \frac{s_l - 50}{5} \right\rfloor \\ &= m_{l+1} + \left\lfloor \frac{s_l}{5} \right\rfloor - 10. \end{aligned}$$

Utilizando a desigualdade acima, obtemos

$$s_1 \geq \left\lfloor \frac{5m_1 + s_0}{5} \right\rfloor - 10$$

e então

$$s_2 \geq m_2 + \left\lfloor \frac{\left\lfloor \frac{5m_1 + s_0}{5} \right\rfloor - 10}{5} \right\rfloor - 10.$$

Podemos então utilizar o Lema 2.18 para obter

$$s_2 \geq \left\lfloor \frac{25m_2 + 5m_1 + s_0}{25} \right\rfloor - 12. \tag{4.5}$$

Aplicando as desigualdades anteriores e o Lema 2.18 repetidas vezes, podemos utilizar um argumento de indução para obter

$$s_l \geq \left\lfloor \frac{\sum_{i=1}^{l} 5^i m_i + s_0}{5^l} \right\rfloor - 13$$

se $l \in [3, \tau]$. Segue que

$$s_l \geq \left\lfloor \frac{\sum_{i=0}^{l} 5^i m_i}{5^l} \right\rfloor - 2.5^{\tau-l+1} - 13.$$

Por outro lado, a desigualdade (3.5) garante que

$$\sum_{i=0}^{l} 5^i m_i > 2(l+1)(5^{\tau+1} - 1)$$

e então

$$s_l \geq \left\lfloor \frac{2(l+1).5^{\tau+1} - 2(l+1)}{5^l} \right\rfloor - 2.5^{\tau-l+1} - 13.$$

Como $2(l+1) < 5^l$ se $l \geq 1$, concluímos que

$$s_l \geq \left\lfloor \frac{2(l+1).5^{\tau+1} - 5^l}{5^l} \right\rfloor - 2.5^{\tau-l+1} - 13 = 2l.5^{\tau-l+1} - 14.$$

Se $l \in [1, \tau-1]$, temos $s_l \geq 2.1.5^2 - 14 = 36$. Como $p_1 \geq 5^\tau$ (desigualdade (3.6)), podemos usar os lemas 4.11 e 2.18 para obter $p_{l+1} \geq 5^{\tau-l}$, se $l \in [0, \tau-1]$. Em particular, $p_\tau \geq 5$. Deste modo, se $l = \tau \geq 3$, temos $s_\tau \geq 2.3.5 - 14 = 16$ e o Lema 4.10 garante que $p_\gamma \neq 0$. Se $l = \tau = 2$, podemos utilizar as desigualdades (4.5) e (3.5) para obter $s_\tau \geq 10\tau - 13 \geq 7$, e novamente o Lema 4.10 garante que $p_\gamma \neq 0$.

Vale observar que o argumento acima não se aplica se $l = \tau = 1$. Em vez disso, vamos proceder de uma forma um pouco diferente para provar que $p_2 \neq 0$. Se $p_1 \geq 9$, o Teorema

4.1 segue diretamente do Lema 2.1. Isto nos permite supor $5 \leq p_1 \leq 8$. Temos $m_0+m_1 \geq 97$. Se $m_1 \geq 7$, então $s_1 \geq 7$ e a demonstração termina. Logo $m_0 \geq 91$. Ora,

$$p_1 \geq \min\left(\left\lfloor \frac{q_0}{5} \right\rfloor, \left\lfloor \frac{m_0}{9} \right\rfloor\right),$$

donde $q_0 \leq 44$ e então

$$\left\lfloor \frac{q_0}{5} \right\rfloor < \left\lfloor \frac{m_0}{9} \right\rfloor.$$

Logo

$$p_1 \geq \left\lfloor \frac{q_0}{5} \right\rfloor.$$

Vamos escrever $q_0 = 5q + r$, com $r \in [0, 4]$. Então, como visto acima, podemos supor $p_1 \geq q$. Com isto, o número de elementos secundários no primeiro nível é

$$s_1 \geq m_1 + \left\lfloor \frac{m_0 - 2.5.q - r}{5} \right\rfloor = \left\lfloor \frac{5m_1 + m_0 - r}{5} \right\rfloor - 2q.$$

Como $-2q \geq -2p_1$, concluímos que $s_1 \geq \left\lfloor \frac{93}{5} \right\rfloor - 2p_1$, ou seja, $s_1 \geq 18 - 2p_1$. Portanto, se $p_1 \in [6, 8]$, os Lemas 2.1 e 2.11 garantem que $p_2 \neq 0$ e se $p_1 = 5$, basta aplicar o Lema 4.10 para obter o mesmo resultado.

Referências Bibliográficas

[1] J. Ax and S. Kochen, *Diophantine problems over local fields I*, Amer. J. Math. **87** (1965), 605-630.

[2] C. B. Boyer, *História da Matemática*, Ed. Edgar Blücher (1996).

[3] J. Brüdern and H. Godinho, *On Artin's Conjecture, II: Pairs of Additive Forms*, Proc. Lond. Math. Soc. (3) **84** (2002), 513-538.

[4] H. Davenport, *On the addition of residue classes*, J. Lond. Math. Soc. (2) **10** (1935), 30-32.

[5] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **274** (1963), 443-460.

[6] H. Davenport and D. J. Lewis, *Cubic equations of additive type*, Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **261** (1966), 97-136.

[7] H. Davenport and D. J. Lewis, *Two Additive Equations*, Proc. Sympos. Pure Math. **12** (1967), 74-98.

[8] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math. **24** (2006), 337-369.

[9] G. Garbi, *O Romance das Equações Algébricas*, Ed. Livraria da Física (2007).

[10] H. Godinho, *On p-adic zeros of additive forms of even degree*, J. Number Theory **68** (1998), 1-20.

[11] H. Godinho, M. Soares, S. Shokranian, *Teoria dos Números*, Ed. UnB (1999), 2nd ed.

[12] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag (1977).

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

[14] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, New York (1996).

[15] J. E. Olson, *A combinatorial problem on finite abelian groups, I*, J. Number Theory **1** (1969), 8-10.

[16] J. E. Olson, *A combinatorial problem on finite abelian groups, II*, J. Number Theory **1** (1969), 195-199.

[17] G. Terjanian, *Une contre-example à une conjecture d'Artin*, C. R. Math. Acad. Sci. Paris **262** (1966), A612.