Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Formas aditivas sobre corpos p-ádicos

por

Daiane Soares Veras

Orientador: Hemar Teixeira Godinho

Brasília
2017

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Soares Veras, Daiane
SD132f Formas aditivas sobre corpos p-ádicos / Daiane Soares Veras; orientador Hemar Teixeira Godinho. -- Brasília, 2017.
89 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2017.

1. Solubilidade de uma forma aditiva de grau k. I. Teixeira Godinho, Hemar , orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Formas aditivas sobre corpos p-ádicos

por

Daiane Soares Veras

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática-UnB, como requisito parcial para obtenção do grau de

DOUTORA EM MATEMÁTICA

Brasília, 31 de março de 2017.

Comissão Examinadora:

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

Profa. Dra. Daniela Amorim Amato (MAT-UnB)

Prof. Dr. Diego Marques Ferreira (MAT-UnB)

Profa. Dra. Ana Paula de Araújo Chaves (UFG)

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

*O autor foi bolsista CAPES e CNPq durante a elaboração deste trabalho.

Agradecimentos

Agradeço primeiramente a Deus por mais essa conquista.

À minha família, pelo incentivo, força e suporte que sempre me ofereceram nessa longa jornada.

Ao professor Hemar Godinho, pelo tempo dedicado, pela paciência, por compartilhar sua experiência e pelas orientações que viabilizaram esse trabalho.

Ao professor Paulo Henrique, por estar sempre presente desde a graduação, orientações no mestrado e pela colaboração na concretização de mais essa etapa.

A todos os outros professores que em todos esses anos, direta ou indiretamente, contribuíram para que eu chegasse até aqui. Em especial aos professores Ana Paula Chaves, Daniela Amato e Diego Marques, por aceitarem compor a banca, e ao Michael Knapp, por dividir comigo um pouco do seu vasto conhecimento matemático.

Aos colegas e amigos da matemática, pelos momentos de descontração, companheirismo e pelas vibrações positivas que foram de suma importância durante esse período.

"Se eu vi mais longe,
foi por estar de pé sobre os ombros de gigantes."

Isaac Newton

Resumo

Davenport e Lewis provaram uma versão da Conjectura de Artin que diz que, denotando por $\Gamma^*(k,p)$ o menor número de variáveis para o qual uma forma aditiva com coeficientes inteiros e grau k possui solução $p-$ádica não trivial, onde p é um número primo, então $\Gamma^*(k,p) \leq k^2+1$ e a igualdade acontece quando $p = k+1$. Sabe-se que, em geral, quando $k+1$ é composto essa cota é suficiente, mas não é necessária. Nessa tese obtemos uma melhora para essa cota, nos casos em que $k+1$ não é primo e, além disso, obtemos o valor exato de $\Gamma^*(k,p)$ quando $p-1$ divide k. Mais precisamente, escrevendo $k = \gamma q + r$ onde γ depende do grau k e $0 \leq r \leq \gamma - 1$, provamos que $\Gamma^*(k,p) \leq (p^\gamma - 1)q + p^r$ e a igualdade vale quando $p-1$ divide k. Como aplicação desse resultado, mostramos que, se $k = 54$, então 1049 variáveis são suficientes para garantir a solubilidade p-ádica não trivial para todo p. Para $k = 24$, M. P. Knapp mostrou que são necessárias 289 variáveis para garantir a solubilidade p-ádica não trivial para todo p, entretanto, ainda como aplicação do resultado citado acima, provamos que, se $p \neq 13$, então 140 variáveis são suficientes para garantir a solubilidade desejada. Além disso encontramos o valor exato de $\Gamma^*(10,p)$ para cada p primo.

Palavras-chave: Conjectura de Artin; Solubilidade p-ádica; Formas Aditivas

Abstract

Davenport and Lewis have proved a version of Artin's Conjecture which states that, denoting by $\Gamma^*(k,p)$ the smallest number of variables for which an additive form with integer coefficients and degree k has a nontrivial p-adic solution, where p is a prime number, then $\Gamma^*(k,p) \leq k^2+1$ and with equality when $p = k+1$. It is known that in general when $k+1$ is composite this bound is sufficient but it is not necessary. In this work we improve this bound when $k+1$ is not prime and we obtain the exact value of $\Gamma^*(k,p)$ when $p-1$ divide k. More precisely, writing $k = \gamma q + r$ with γ depending on the degree k and $0 \leq r \leq \gamma - 1$, we prove that $\Gamma^*(k,p) \leq (p^\gamma - 1)q + r$ with equality when $p-1$ divides k. As an application of this result we show that, if $k = 54$, then 1049 variables are sufficient to ensure the nontrivial p-adic solubility for all p. For $k = 24$, M. P. Knapp has proved that 289 variables are necessary to ensure the nontrivial p-adic solution for all p. However, still as an application of the previous result, we show that, if $p \neq 13$, then 140 variables are sufficient to ensure the desired solubility. Moreover, we give the exact value of $\Gamma^*(10,p)$ for each prime p.

Keywords: Artin's Conjecture, p-adic Solubility, Additive Forms

Sumário

Introdução

Existe uma conexão entre congruências e equações que é baseada no seguinte argumento: se para $F(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$ a equação

$$F(x_1, ..., x_n) = 0 \tag{1}$$

tem solução nos inteiros, então a congruência

$$F(x_1, ..., x_n) \equiv 0 \bmod(m) \tag{2}$$

tem solução para todo m.

Como a solubilidade de (1) implica na solubilidade de (2) e esta sempre pode ser decidida, já que existe uma quantidade finita de classes de resíduos módulo m, obtemos então uma sequência de condições que são necessárias para garantir a solubilidade da equação (1) nos inteiros. Entretanto, obter condições suficientes é uma tarefa mais difícil já que, em geral, não podemos afirmar que uma equação tem solução se, e somente se, tem solução como congruência módulo m para todo $m \in \mathbb{Z}$. Um exemplo disso é o polinômio $F(x) = (x^2 - 13)(x^2 - 17)(x^2 - 221)$. A congruência $F(x) \equiv 0 \pmod{m}$ tem solução para todo m como pode-se ver em [2], mas claramente $F(x) = 0$ não tem solução inteira . Por solubilidade da equação $F = 0$ entendemos a existência de uma solução não nula.

Da teoria elementar dos números sabe-se que se a congruência

$$F(x_1, \ldots, x_n) \equiv 0 (\text{mod } p_i^{k_i})$$

tem solução para todo $i = 1, \ldots, r$, onde cada p_i é primo e $m = p_1^{k_1} \ldots p_r^{k_r}$, então a congruência (2) tem solução. Assim, a solubilidade de (2) para todo $m \in \mathbb{Z}$ é equivalente à solubilidade dessa congruência módulo todas as potências de p, para todo primo p.

Em conexão com o problema de encontrar condições suficientes para garantir a solubilidade da equação a partir da solubilidade de certas congruências Hensel construiu, para cada p, um novo tipo de número chamado p-ádico. Ele mostrou que a solubilidade de um sistema de congruências módulo m para todo inteiro m era equivalente à solubilidade nos p-ádicos para todo p primo.

A primeira grande aplicação dessa teoria foi apresentada por Hasse que, baseado nos trabalhos de Minkowski, demonstrou o seguinte teorema (ver [2]):

Teorema 0.1 (Hasse-Minkowski) *Uma forma quadrática com coeficientes racionais possui zeros racionais se e somente se possuir zeros reais e p-ádicos para todo primo p.*

Esse resultado estabeleceu um princípio de atuação conhecido como princípio de Hasse, que consiste na busca de soluções inteiras através de informações p-ádicas e reais.

Sendo $\mathbb{Q}_p$ o corpo dos números p-ádicos, era natural perguntar-se sob quais condições um polinômio admitia soluções p-ádicas não triviais. Nessa direção, em 1920, Emil Artin conjecturou que qualquer polinômio homogêneo de grau k em n variáveis tem zeros p-ádicos desde que $n \geq k^2 + 1$.

Em 1924 os resultados de H. Hasse confirmaram a conjectura para formas quadráticas e em 1957, Lewis confirmou a validade da conjectura para formas de grau três, mas em 1966, Terjanian apresentou um exemplo de uma forma de grau 4 com 18 variáveis sem zeros 2-ádicos não trivais. Mais tarde, em 1963 Davenport e Lewis [5] provaram a validade da conjectura para formas aditivas. Eles mostraram ainda que quando $k + 1$ é um primo q então a cota da conjectura é a melhor possível para garantir a solubilidade q-ádica não trivial, exibindo uma forma de grau k em k^2 variáveis sem zeros q-ádicos não triviais.

Definição 0.1 *Denotamos por $\Gamma^*(k, p)$ o menor número de variáveis para o qual uma forma aditiva de grau k tem solução p-ádica não trivial, onde p é um primo fixado, e $\Gamma^*(k)$ o menor número de variáveis para o qual uma forma aditiva de grau k tem solução p-ádica não trivial para todo primo p.*

Uma grande contribuição a respeito das funções $\Gamma^*(k)$ e $\Gamma^*(k,p)$ foi dada por Dodson em [6]. Ele mostrou, entre outros resultados, que

$$\left\lfloor \frac{k}{\gamma} \right\rfloor (p^\gamma - 1) + 1 \leq \Gamma^*(k,p) \leq \left\lfloor \frac{k}{\gamma}(p^\gamma - 1) \right\rfloor + 1, \tag{3}$$

mas, como veremos, a diferença entre essas cotas pode ser muito grande dependendo dos valores de k.

Em termos da função $\Gamma^*(k,p)$ a conjectura nos diz que $\Gamma^*(k,p) \leq k^2+1$ e, apesar dessa cota ser a melhor possível quando $k+1$ é primo, em geral quando $k+1$ é composto sabe-se que o número de variáveis necessárias para garantir a solubilidade p-ádica não trivial é bem menor do que a que é dada pela conjectura. Lewis [13] mostrou que $\Gamma^*(3) = 7$. Gray [8] mostrou que formas aditivas de grau 5 em 16 variáveis tem zeros p-ádicos não triviais, exceto em $\mathbb{Q}_5$, e deu um exemplo de uma forma aditiva de grau 5 em 15 variáveis sem zeros 11-ádicos. Mais tarde, Chowla [4] mostrou que 16 variáveis são suficientes para garantir também a solubilidade não trivial em $\mathbb{Q}_5$. Juntos esses resultados mostram que $\Gamma^*(5) = 16$. Bierstedt [1] e Norton [14] mostraram independentemente que $\Gamma^*(7) = 22$ e $\Gamma^*(11) = 45$. Bovey [3] mostrou que $\Gamma^*(8) = 39$. Em [9] M. Knapp determinou os valores exatos da função $\Gamma^*(k)$ para $k = 14, 20, 24, 26, 27, 29$ e 31 e mostrou ainda que $\Gamma^*(32) = \Gamma^*(32,2)$.

Recentemente, M. Knapp [10] mostrou também o seguinte resultado:

Teorema 0.2 *Escreva $k = 2^\tau k_0$ onde k_0 é um inteiro ímpar e defina o número γ por*

$$\gamma(k) = \begin{cases} \tau + 2 \ \ se \ \ \tau > 0; \\ \\ 1 \quad se \ \ \tau = 0. \end{cases}$$

Além disso, escreva $k = \gamma q + r$, onde q e r são inteiros e $0 \leq r \leq \gamma - 1$. Então

$$\Gamma^*(k,2) = \begin{cases} 5 & se \ \ k = 2; \\ \\ (2^\gamma - 1)q + 2^r & caso \ contrário. \end{cases}$$

A maioria dos resultados citados acima foram obtidos fixando-se o primo p e encontrando um limite superior para $\Gamma^*(k,p)$, através da relação

$$\Gamma^*(k) = \max_p \Gamma^*(k,p). \tag{4}$$

Em vista desse método e com base nos resultados de M. P. Knapp e M. Dodson, é natural questionar-se sobre o estudo da função $\Gamma^*(k,p)$ para valores específicos de p. Além disso, é conhecido que $\Gamma^*(k) = k^2 + 1$ quando $k+1$ é primo, mas isso decorre do contra exemplo que é dado para o primo $p = k+1$. Portanto é natural também investigar se a cota é de fato necessária para os demais primos. Nessa direção, essa tese consiste em um estudo detalhado da função $\Gamma^*(k,p)$, e como consequência desse estudo, daremos o valor exato de $\Gamma^*(54)$ e uma estimativa para os valores de $\Gamma^*(24,p)$, para todo primo p. Além disso, daremos também o valor exato de $\Gamma^*(10,p)$ para todo primo p. Em todos esses casos em que o grau é fixado, os cálculos são feitos separando-se em dois casos: os primos que dividem o grau, e fixando esses primos utilizamos os resultados obtidos para a função $\Gamma^*(k,p)$ além de alguns resultados específicos para cada primo em questão; e os primos que não dividem o grau, e para esses casos utilizamos fortemente o MAPLE com o auxílio de algumas técnicas, como a de somas exponenciais. O conteúdo dessa tese foi divido em quatro capítulos e um apêndice, onde apresentamos tabelas com os resultados obtidos através de cálculos efetuados no MAPLE, e também as rotinas utilizadas para efetuar esses cálculos. Os quatro capítulos serão detalhados seguir.

No 1° capítulo vamos introduzir algumas definições e resultados preliminares que serão fundamentais para o entendimento do trabalho e será dividido em quatro seções. Na primeira seção apresentaremos alguns resultados relacionados à solubilidade de congruências módulo um primo p, dando algumas definições importantes e deduzindo resultados clássicos como os Teoremas de Chevalley e Warning. A segunda seção trata de somas exponenciais, método muito utilizado para obter estimativas para o número de soluções de congruências módulo p. Os resultados apresentados nas seções 3 e 4 foram dados por Davenport e Lewis [5] e dizem respeito às técnicas de p-normalização e contração de variáveis, respectivamente.

No 2° capítulo apresentamos uma melhora na cota (3) de Dodson e obtemos o valor exato de $\Gamma^*(k,p)$ quando $p-1$ divide k. Este resultado foi obtido com base nas técnicas usadas por M. P. Knapp em [10], generalizando os lemas para um primo qualquer. Mais

precisamente, definindo

$$\gamma(k) = \begin{cases} 1 & \text{se } \tau = 0; \\ \tau + 1 & \text{se } \tau > 0 \text{ e } p > 2, \\ \tau + 2 & \text{se } \tau > 0 \text{ e } p = 2. \end{cases} \tag{5}$$

provaremos o seguinte resultado:

Teorema 0.3 *Seja $k = p^\tau k_0$, com $mdc(k_0, p) = 1$ e γ como na definição acima. Escreva $k = \gamma q + r$, onde q e r são inteiros e $0 \leq r \leq \gamma - 1$. Então*

$$\Gamma^*(k, p) \leq (p^\gamma - 1)q + p^r,$$

e a igualdade ocorre quando $p - 1$ divide k.

O 3° capítulo é destinado a dar duas aplicações do teorema acima, e o faremos em duas seções. Na primeira delas daremos o valor exato para $\Gamma^*(54)$. Vamos provar o seguinte corolário

Corolário 0.1 *Seja $\Gamma^*(k)$ como na Definição 0.1. Então $\Gamma^*(54) = 1049$.*

Na segunda seção vamos obter algumas estimativas para os valores de $\Gamma^*(24, p)$. Em [9], M. Knapp mostrou que $\Gamma^*(24) = 289$. Entretanto, vamos ver que, para os primos tais que $p - 1$ não divide o grau, $\Gamma^*(24, p) < 289$. Mais precisamente mostraremos o seguinte resultado

Corolário 0.2 *Seja p um primo, $p \neq 13$. Então $\Gamma^*(24, p) \leq 140$.*

No 4° capítulo nosso objetivo é dar os valores exatos de $\Gamma^*(10, p)$ para todo primo p. Dividiremos esse capítulo em três seções, sendo as duas primeiras dedicadas aos primos que dividem o grau e a última aos primos que não dividem o grau. Ao final do capítulo ficará provado o seguinte resultado:

Teorema 0.4 . *Seja $\mathcal{P}$ o seguinte conjunto de primos*

$$\mathcal{P} = \{41, 61, 71, 101, 131, 151, 181, 191, 211, 251, 271, 281, 311, 331, 431, 491, 911\}$$

e p um primo, $p \neq 11$. Então os seguintes valores são obtidos:

- $\Gamma^*(10,p) = 23$ *e* 41*, se* $p = 2$*, e* 31*, respectivamente;*
- $\Gamma^*(10,p) = 31$*, se* $p \in \mathcal{P}$;
- $\Gamma^*(10,p) = 21$*, se* $p = 5$ *e nos casos restantes.*

Quando $p = 2$ o resultado é uma consequência do Teorema 3.1 de [10], porém faremos algumas considerações adicionais a respeito desse caso, mostrando que quase sempre o número de variáveis para garantir a solubilidade 2-ádica não trivial pode ser ainda menor do que o dado no Teorema 0.4. Como consequência dos resultados de Davenport e Lewis e da relação (4) temos que $\Gamma^*(10) = 101$, já que $\Gamma^*(10,11) = 101$. Entretanto, o Teorema 0.4 nos mostra que, mesmo em um caso onde $k+1$ é primo, o número de variáveis necessárias para garantir a solubilidade p-ádica não trivial para todo $p \neq k+1$ é bem menor do que o dado pela conjectura.

CAPÍTULO 1

Preliminares

1.1 Congruências módulo primo

As classes de resíduos módulo p formam um corpo finito com p elementos, denotado por $\mathbb{F}_p$. Neste corpo, uma congruência módulo p pode ser vista como uma equação. Assim, nossos estudos serão direcionados para resolução de equações sobre corpos finitos. Um fato relevante é que polinômios que satisfazem $F(x_1, ..., x_n) = G(x_1, ..., x_n)\ \forall x_i \in \mathbb{F}_p$ nem sempre têm coeficientes iguais.

Definição 1.1 *Sejam F e G polinômios em n variáveis, com coeficientes inteiros.*

- *Dizemos que F e G são congruentes, e escrevemos*

$$F(x_1, ..., x_n) \equiv G(x_1, ..., x_n)(mod\ p),$$

se os coeficientes dos termos correspondentes nos lados direito e esquerdo são congruentes módulo p.

- *Se para qualquer n-upla de inteiros $(c_1, ..., c_n)$ temos que*

$$F(c_1, ..., c_n) \equiv G(c_1, ..., c_n)(mod\ p),$$

então dizemos que F e G são equivalentes, e escrevemos $F \sim G$.

Definição 1.2 *O grau total de um polinômio f é o maior grau dentre os graus de seus monômios, onde o grau de um monômio é igual à soma dos graus de suas variáveis.*

Uma vez que, se $F \sim G$, as congruências $F \equiv 0(mod\ p)$ e $G \equiv 0(mod\ p)$ têm as mesmas soluções, podemos substituir um polinômio F por um equivalente a ele e que tenha uma forma mais simples. Dado um polinômio F, podemos reduzir o grau de suas variáveis através de sucessivas aplicações do Teorema de Fermat, fazendo ${x_i}^p \equiv x_i(mod\, p)$. Desse modo encontramos um polinômio equivalente a F, de grau menor do que p em cada variável x_i, que denotaremos *polinômio reduzido*. Temos portanto o seguinte resultado.

Teorema 1.1 *Todo polinômio F é equivalente a um polinômio reduzido F^*, cujo grau total é sempre menor ou igual ao grau total de F.*

Teorema 1.2 *Se dois polinômios reduzidos são equivalentes, então eles são congruentes.*

Prova. É suficiente mostrar que, se F é um polinômio reduzido e $F \sim 0$, então temos $F \equiv 0(\text{mod } p)$. A demonstração segue por indução sobre o número de variáveis.

Para $n = 1$, se $deg(F(x)) < p$ e $F(c) \equiv 0(\text{mod } p)$ para todo c, então F tem mais raizes que seu grau, o que só é possível se todos os coeficientes de F são congruentes a zero módulo p, isto é, $F \equiv 0(\text{mod } p)$.

Vamos agora supor que o teorema seja verdadeiro quando o número de variáveis é igual a $n-1$, e mostrar que é válido também para n. Para $n \geq 2$, escrevemos F na forma

$$F(x_1, ..., x_n) = A_0(x_1, ..., x_{n-1}) + A_1(x_1, ..., x_{n-1})x_n + \cdots + A_{p-1}(x_1, ..., x_{n-1})x_n^{p-1}.$$

Tome um conjunto de valores arbitrários $x_1 = c_1, ..., x_{n-1} = c_{n-1}$ e faça $A_0(c_1, ..., c_{n-1}) = a_0, ..., A_{p-1}(c_1, ..., c_{n-1}) = a_{p-1}$. Obtemos um polinômio em uma única variável, x_n, dado por

$$F(c_1, ..., c_{n-1}, x_n) = a_0 + a_1x_n + \cdots + a_{p-1}x_n^{p-1}$$

e portanto voltamos ao caso $n = 1$. Como $F \sim 0$, temos que $F(c_1, ..., c_{n-1}, x_n) \equiv 0(\text{mod } p)$. Então,

$$A_0(c_1, ..., c_{n-1}) \equiv 0(\text{mod } p)$$

$$\vdots$$

$$A_{p-1}(c_1, ..., c_{n-1}) \equiv 0(\text{mod } p)$$

isto é, $A_0 \sim 0, \ldots, A_{p-1} \sim 0$, pois $c_1, ..., c_{n-1}$ foram tomados arbitrariamente. É claro que esses polinômios são reduzidos (já que F é reduzido) e dependem de $n-1$ variáveis. Logo, por hipótese de indução, o teorema é verdadeiro para esses polinômios e, portanto, $A_0 \equiv 0(\text{mod } p), ..., A_{p-1} \equiv 0(\text{mod } p)$, ou seja, $F \equiv 0(\text{mod } p)$.

□

Dos teoremas anteriores podemos deduzir alguns resultados sobre o número de soluções de congruências.

Teorema 1.3 *Se a congruência $F(x_1, ..., x_n) \equiv 0(\text{mod } p)$ tem pelo menos uma solução, e o grau total do polinômio F é menor do que o número de variáveis, então a congruência tem pelo menos duas soluções.*

Teorema 1.4 (Teorema de Chevalley) *Se $F(x_1, ..., x_n)$ é uma forma de grau inferior a n, então a congruência $F(x_1, ..., x_n) \equiv 0(\text{mod } p)$ tem solução não nula.*

Os Teoremas 1.3 e 1.4 são consequências imediatas do teorema a seguir.

Teorema 1.5 (Teorema de Warning) *Se o grau do polinômio $F(x_1, ..., x_n)$ é menor que n, então o número de soluções da congruência $F(x_1, ..., x_n) \equiv 0(\text{mod } p)$ é divisível por p.*

Prova. Suponhamos que a congruência tenha s soluções $A_i = (a_1^{(i)}, ..., a_n^{(i)}),\ i = 1, ..., s$. Definindo $H = 1 - F^{p-1}$, então H satisfaz:

$$H(X) = \begin{cases} 1, & \text{para } X \equiv A_i(mod p), i = 1, ..., s \\ 0, & \text{caso contrário.} \end{cases}$$

onde $X = (x_1..., x_n)$. Para qualquer $A = (a_1, ..., a_n)$, defina

$$D_A(x_1, ..., x_n) = \prod_{j=1}^{n}(1 - (x_j - a_j)^{p-1}).$$

É fácil ver que

$$D_A(X) = \begin{cases} 1, & para\ X \equiv A(mod p), \\ 0, & \text{caso contrário.} \end{cases} \tag{1.1}$$

Seja

$$H^*(x_1, ..., x_n) = D_{A_1}(x_1, ..., x_n) + \cdots + D_{A_s}(x_1, ..., x_n).$$

Da equação (1.1) resulta que H^* tem a mesma solução de H $\forall x_1, ..., x_n$, isto é, $H \sim H^*$. Logo, o grau de H^* não excede o grau de H que é menor que $n(p-1)$.

Em cada D_{A_i} existe um termo de grau $n(p-1)$, a saber, o termo $(-1)^n(x_1 \dots x_n)^{p-1}$. Como o grau de H^* é estritamente menor que $n(p-1)$ necessariamante devemos ter $s \equiv 0(\text{mod } p)$, que é exatamenta o que diz o Teorema de Warning.

□

Observe que o Teorema de Warning nos fornece um resultado mais forte que o do Teorema 1.3, já que nos garante que se a congruência $F(x_1, ..., x_n) \equiv 0(mod\ p)$ tem pelo menos uma solução, e o grau total do polinômio F é menor do que o número de variáveis, então a congruência tem pelo menos p soluções.

1.2 Somas Exponenciais

Até agora os resultados apresentados investigam o número de soluções de congruências através do número de variáveis do polinômio envolvido. Os resultados apresentados a seguir utilizam somas exponenciais para estimar o número de soluções, incongruentes módulo p, dessas congruências através do primo p.

Definição 1.3 *Um polinômio $F(x_1, ..., x_n)$ com coeficientes racionais é dito absolutamente irredutível se não é possível obter uma fatoração não-trivial em qualquer extensão do corpo dos números racionais.*

Observe que para polinômios com coeficientes racionais de grau 2 com uma ou mais variáveis sempre é possível obter uma fatoração não trivial no corpo dos números complexos $\mathbb{C}$. Portanto, neste caso apenas os polinômios constantes podem ser absolutamente irredutíveis.

Teorema 1.6 *Se $F(x_1, ..., x_n)$ é um polinômio absolutamente irredutível com coeficientes inteiros, então a congruência*

$$F(x_1, ..., x_n) \equiv 0(mod\ p)$$

tem solução para todo número primo p maior que algum limite que depende somente do polinômio F.

Teorema 1.7 *O número $N(F, p)$ de soluções da congruência*

$$F(x_1, ..., x_n) \equiv 0(modp) \tag{1.2}$$

satisfaz a desigualdade

$$|N(F, p) - p^{n-1}| < C(F)p^{n-1-(1/2)}$$

onde a constante $C(F)$ não depende de p.

As demonstrações dos Teoremas 1.6 e 1.7 utilizam alguns resultados de geometria algébrica, e podem ser encontradas em [11] para $n = 2$, e em [12] para o caso geral. Neste trabalho apresentaremos apenas a demonstração de um caso particular do Teorema 1.7 em que o polinômio F é diagonal, sem o termo constante e $n \geq 3$. Neste caso, apresentaremos uma fórmula explícita para o número de soluções da congruência (1.2).

Seja ζ uma das raízes p-ésimas da unidade. Então,

$$\sum_x \zeta^{xy} = \begin{cases} p, & \text{para } y \equiv 0(\text{mod } p) \\ 0, & \text{para } y \not\equiv 0(\text{mod } p). \end{cases} \tag{1.3}$$

Usando (1.3) vamos explicitar uma fórmula para o número de soluções da congruência (1.2).

Considere a soma

$$S = \sum_{x_1,...,x_n} \sum_x \zeta^{xF(x_1,...,x_n)}.$$

Se $(x_1, ...x_n)$ é uma solução de (1.2), então

$$\sum_x \zeta^{xF(x_1,...,x_n)} = p,$$

se $F(x_1, ...x_n) \not\equiv 0(\text{mod } p)$

$$\sum_x \zeta^{xF(x_1,...,x_n)} = 0.$$

Assim, $S = Np$ onde N é o número de soluções da congruência (1.2). Desse modo fica provado o seguinte resultado:

O número de soluções da congruência (1.2) é dado por

$$N = \frac{1}{p} \sum_{x,x_1,...,x_n} \zeta^{xF(x_1,...,x_n)}. \tag{1.4}$$

Podemos ainda reescrever (1.4) na forma

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \sum_{x_1,...,x_n} \zeta^{xF(x_1,...,x_n)} \tag{1.5}$$

onde $\sum_x{}'$ denota o somatório com x percorrendo um sistema reduzido de resíduos.

Vamos agora aplicar o método anterior ao caso em que o polinômio F é dado por

$$F(x_1, ..., x_n) = a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n}, \qquad a_i \not\equiv 0(\text{mod } p)$$

e assumindo que $n \geq 3$. De (1.5) temos que o número N de soluções para a congruência $a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n} \equiv 0(\text{mod } p)$ pode ser reescrito na forma

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum \zeta^{a_i x x_i^{r_i}}. \tag{1.6}$$

Vamos portanto investigar somas da forma $\sum_y \zeta^{ay^r}$ onde $a \not\equiv 0(\text{mod } p)$. Claramente, se $m(x)$ é o número de soluções da congruência $y^r \equiv x(\text{mod } p)$, então

$$\sum_y \zeta^{ay^r} = \sum_x m(x) \zeta^{ax}. \tag{1.7}$$

Podemos encontrar uma fórmula explicita para $m(x)$ quando $x \not\equiv 0(\text{mod } p)$. Se g é uma *raíz primitiva* módulo p, então

$$x \equiv g^k(\text{mod } p), \tag{1.8}$$

onde o expoente k é determinado de maneria única módulo $p-1$. Seja $y \equiv g^u(\text{mod } p)$, a congruência $y^r \equiv x(\text{mod } p)$ é então equivalente à congruência

$$ru \equiv k(\text{mod } p-1) \tag{1.9}$$

pois

$$y^r \equiv x(\text{mod } p) \Rightarrow g^{ur} \equiv g^k(\text{mod } p) \Rightarrow g^{ur-k} \equiv 1(\text{mod } p).$$

Pelo pequeno Teorema de Fermat,

$$x^{p-1} \equiv 1(\text{mod } p) \text{ desde que } x \not\equiv 0(\text{mod } p),$$

e daí $ur - k \equiv 0(\text{mod } p-1.)$

Da teoria de congruências lineares sabemos que a congruência (1.9) tem $d = (r, p-1)$ soluções em u se, e somente se, d divide k, caso contrário não tem solução. Portanto,

$$m(x) = \begin{cases} d & \text{se } k \equiv 0(\text{mod } d) \\ 0 & \text{se } k \not\equiv 0(\text{mod } d). \end{cases} \tag{1.10}$$

Podemos ainda encontrar uma fórmula mais conveniente para $m(x)$. Seja ϵ uma raíz d-ésima primitiva da unidade, e defina as funções

$$\chi_s(x) = \epsilon^{ks}, \tag{1.11}$$

$s = 0, ..., d-1, \quad \forall x \in \mathbb{Z}$ tal que $(x, p) = 1$ e k é determindado por (1.8).

As funções χ_s que satisfazem $\chi_s(xy) = \chi_s(x)\chi_s(y)$ são chamadas de caracter módulo p. Para extendermos a todos os valores de x definimos $\chi_s(x) = 0$ se $x \equiv 0(\text{mod } p)$. O caráter $\chi_0(x)$ é chamado caráter trivial, ou caráter unidade, e assume valor 1 para todo $x \not\equiv 0(\text{mod } p)$.

Observe que se $k \equiv 0(\text{mod } d)$, então $\epsilon^{ks} = 1, \forall s \in \{0, 1, ..., d-1\}$ e portanto

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

Se $k \not\equiv 0(\text{mod } p)$, então $\epsilon^k \neq 1$ e portanto,

$$\sum_{s=0}^{d-1} \epsilon^{ks} = \frac{\epsilon^{kd} - 1}{\epsilon^k - 1} = 0.$$

Assim, comparando com (1.10) obtemos a fórmula

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

Podemos agora reescrever (1.7) na forma

$$\sum_y \zeta^{ay^r} = 1 + \sum_x{}' \sum_{s=0}^{d-1} \chi_s(x)\zeta^{ax}.$$

Como

$$1 + \sum_x{}' \zeta^{ax} = \sum_x \zeta^{ax} = 0,$$

temos

$$\sum_y \zeta^{ay^r} = \sum_{s=1}^{d-1} \sum_x \chi_s(x)\zeta^{ax} \tag{1.12}$$

onde x percorre um sistema completo de resíduos módulo p, já que para $x \equiv 0(\text{mod } p)$ definimos $\chi_s(x) = 0$.

Definição 1.4 *Sejam χ um dos caracteres χ_s e $a \in \mathbb{Z}$. A expressão*

$$\sum_x \chi(x)\zeta^{ax}$$

é chamada Soma Gaussiana, que denotamos por $\tau_a(\chi)$. Quando $a = 1$ denotamos $\tau_a(\chi)$ simplesmente por $\tau(\chi)$.

De (1.6), (1.12) e da definição acima podemos formular o seguinte teorema:

Teorema 1.8 *Seja N o número de soluções da congruência*

$$a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n} \equiv 0(\text{mod } p), \qquad a_i \not\equiv 0(\text{mod } p). \tag{1.13}$$

Então,

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} \tau_{a_i x}(\chi_{i,s}) \tag{1.14}$$

onde $d_i = (r_i, p-1)$ e o caracter $\chi_{i,s}$ é definido por (1.11) com $d = d_i$.

Teorema 1.9 *Sejam χ um caracter multiplicativo módulo p, $\chi \neq \chi_0$ e $mdc(a,p) = 1$. Então*

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

Prova. Primeiramente vamos mostrar que $\chi(a)\tau_a(\chi) = \tau(\chi)$. Da definição (1.4) temos

$$\chi(a)\tau_a(\chi) = \chi(a)\sum_{x=0}^{p-1}\chi(x)\zeta^{ax} = \sum_{x=0}^{p-1}\chi(a)\chi(x)\zeta^{ax} = \sum_{x=0}^{p-1}\chi(ax)\zeta^{ax} = \sum_{y=0}^{p-1}\chi(y)\zeta^{y} = \tau(\chi).$$

Além disso, $|\chi(a)| = \chi(a)\overline{\chi(a)} = \zeta^a\zeta^{-a} = 1$. Assim,

$$|\tau(\chi)| = |\chi(a)\tau_a(\chi)| = |\chi(a)|\,|\tau_a(\chi)| = |\tau_a(\chi)|\,.$$

Portanto é suficiente mostrar que $|\tau(\chi)|^2 = p$. Considere a soma

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

Temos que

$$\tau_a(\chi) = (\chi(a))^{-1}\tau(\chi) \Rightarrow \overline{\tau_a(\chi)} = \overline{(\chi(a))^{-1}\tau(\chi)} = \chi(a)\overline{\tau(\chi)},$$

já que $|\chi(a)| = 1 \Rightarrow \overline{\chi(a)} = (\chi(a))^{-1}$.

Assim,

$$\tau_a(\chi)\overline{\tau_a(\chi)} = \tau(\chi)\overline{\tau(\chi)} = |\tau(\chi)|^2\,.$$

Note que se $\chi \neq \chi_0$, para algum $a \in \mathbb{F}_p$ temos $\chi(a) \neq 1$ e assim

$$\chi(a)\sum_x\chi(x) = \sum_x\chi(ax) = \sum_x\chi(x) \Rightarrow (\chi(a)-1)\sum_x\chi(x) = 0 \Rightarrow \sum_x\chi(x) = 0$$

pois ax percorre $\mathbb{F}_p$ quando x percorre $\mathbb{F}_p$. Logo,

$$\tau_0(\chi) = \sum_{x=0}^{p-1}\chi(x) = 0,$$

portanto

$$\sum_{a=0}^{p-1}\tau_a(\chi)\overline{\tau_a(\chi)} = \sum_{a=1}^{p-1}\tau_a(\chi)\overline{\tau_a(\chi)} = \sum_{a=1}^{p-1}|\tau(\chi)|^2 = (p-1)\,|\tau(\chi)|^2\,. \tag{1.15}$$

Por outro lado,

$$\tau_a(\chi)\overline{\tau_a(\chi)} = \left(\sum_{x=0}^{p-1}\chi(x)\zeta^{ax}\right)\left(\sum_{y=0}^{p-1}\overline{\chi(y)}\zeta^{-ay}\right) = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\chi(x)\overline{\chi(y)}\zeta^{a(x-y)}$$

onde

$$\sum_{a=0}^{p-1}\zeta^{a(x-y)} = \begin{cases} p, \text{ se } x \equiv y(modp) \\ 0, \text{ caso contrário.} \end{cases}$$

Como $x, y \in \{0, 1, ..., p-1\}$, $x \equiv y(modp) \Rightarrow x = y$. Assim

$$\sum_{a=0}^{p-1}\tau_a(\chi)\overline{\tau_a(\chi)} = \sum_{a=0}^{p-1}\sum_{z=0}^{p-1}\chi(z)\overline{\chi(z)} = p\sum_{z=1}^{p-1}|\chi(z)|^2 = p(p-1). \tag{1.16}$$

De (1.15) e (1.16) temos $(p-1)|\tau(\chi)|^2 = p(p-1) \Rightarrow |\tau(\chi)|^2 = p$.

□

Dos Teoremas 1.8 e 1.9 obtemos o teorema a seguir.

Teorema 1.10 *Seja N o número de soluções da congruência*

$$a_1x_1^{r_1} + \cdots + a_nx_n^{r_n} \equiv 0(modp).$$

Então para cada número primo p que não divide $a_1, ..., a_n$ temos

$$|N - p^{n-1}| \leq C(p-1)p^{(n/2)-1}, \tag{1.17}$$

onde $C = (d_1 - 1)\cdots(d_n - 1)$, e $d_i = (r_i, p-1)$.

Prova. De (1.14) temos

$$\begin{aligned} \left|N - p^{n-1}\right| = \left|\frac{1}{p}\sum_{x}{}'\prod_{i=1}^{n}\sum_{s=1}^{d_i-1}\tau_{a_ix}(\chi_{i,s})\right| &\leq \frac{1}{p}\sum_{x}{}'\prod_{i=1}^{n}\sum_{s=1}^{d_i-1}|\tau_{a_ix}(\chi_{i,s})| \\ &= \frac{1}{p}\sum_{x}{}'\prod_{i=1}^{n}\sum_{s=1}^{d_i-1}\sqrt{p} \\ &= \frac{1}{p}(p-1)p^{\frac{n}{2}}\prod_{i=1}^{n}(d_i-1) \\ &= (p-1)p^{n/2-1}\prod_{i=1}^{n}(d_i-1). \end{aligned}$$

□

Quando $n \geq 3$, o Teorema 1.10 implica no Teorema 1.7 para polinômios do tipo

$$P(x) = a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n}.$$

De fato,

$$\left|N - p^{n-1}\right| \leq C(p-1)p^{(n/2)-1} \leq Cp^{n-1-(\frac{1}{2})}.$$

Além disso, sabemos que se $d_i = mdc(r_i, p-1)$ então, quanto ao número de soluções, a congruência $a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n} \equiv 0(mod\ p)$ é equivalente a $a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} \equiv 0(mod\ p)$. Assim podemos considerar que já estamos tomando o grau do polinômio como sendo o máximo divisor comum entre o grau e $p-1$, desse modo $d_i = r_i$ e, portanto, $C = \prod_{i=1}^{n}(d_i - 1)$ depende somente do polinômio $a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n}$, que é o que afirma o Teorema 1.7.

Se consideramos o caso particular em que o polinômio $F(x_1, ..., x_n)$ em (1.2) é uma forma de grau k, podemos dar uma estimativa mais refinada para o número N de soluções dessa congruência. Para isso, seja ζ uma raíz primitiva p-ésima da unidade. Definimos

$$T(u) = \sum_{y=0}^{p-1} \zeta^{uy^k}.$$

Lema 1.2.1 *Seja χ um caráter não trivial e $d = mdc(k, p-1)$. Se $u \not\equiv 0(\text{mod } p)$, então*

$$T(u) = \sum_{s=1}^{d-1} \tau_u(\chi_s).$$

Prova. Temos que

$$T(u) = \sum_{y=0}^{p-1} \zeta^{uy^k} = \sum_{x=0}^{p-1} m(x)\zeta^{ux} = m(0) + \sum_{x=1}^{p-1}\sum_{s=0}^{d-1} \chi_s(x)\zeta^{ux}.$$

Como

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

então

$$\begin{aligned} T(u) &= 1 + \sum_{x=1}^{p-1}\sum_{s=0}^{d-1} \chi_s(x)\zeta^{ux} = 1 + \sum_{x=1}^{p-1} \zeta^{ux} + \sum_{x=1}^{p-1}\sum_{s=1}^{d-1} \chi_s(x)\zeta^{ux} \\ &= \sum_{x=0}^{p-1} \zeta^{ux} + \sum_{x=1}^{p-1}\sum_{s=1}^{d-1} \chi_s(x)\zeta^{ux} = \sum_{x=1}^{p-1}\sum_{s=1}^{d-1} \chi_s(x)\zeta^{ux} \\ &= \sum_{s=1}^{p-1}\sum_{x=1}^{d-1} \chi_s(x)\zeta^{ux} = \sum_{s=1}^{d-1} \tau_u(\chi_s), \end{aligned}$$

já que $mdc(u,p)=1$ e portanto $\sum_{x=0}^{p-1}\zeta^{ux}=0$.

□

Considere o polinômio $F(x_1,...,x_n)=a_1x_1^k+\cdots+a_nx_n^k$ e defina

$$S_r=\sum_{u=1}^{p-1}|T(u)|^r$$

onde $T(u)=\sum_{x=0}^{p-1}\zeta^{ux^k}$. De (1.6) temos que

$$N=p^{n-1}+\frac{1}{p}\sum_{u=1}^{p-1}T(a_1u)\dots T(a_nu).$$

Pela desigualdade de Hölder, temos

$$\sum_{u=1}^{p-1}|T(a_1u)\dots T(a_nu)|\leq\left(\sum_{u=1}^{p-1}|T(a_1u)|^n\right)^{\frac{1}{n}}\dots\left(\sum_{u=1}^{p-1}|T(a_nu)|^n\right)^{\frac{1}{n}}.$$

Mas

$$\sum_{u=1}^{p-1}|T(au)|^n=\sum_{u=1}^{p-1}|T(u)|^n,\ \text{ se }\ a\not\equiv 0(modp),$$

o que implica que

$$\sum_{u=1}^{p-1}|T(a_1u)\dots T(a_nu)|\leq S_n.$$

Assim, o número de soluções da congruência (1.2) satisfaz

$$N\geq p^{n-1}-p^{-1}S_n.$$

Note que o número M de soluções da congruência $x^k\equiv y^k(mod\ p)$ é dado por $M=(p-1)k+1$, pois para cada $x\not\equiv 0(mod\ p)$ temos k soluções em y, e mais a solução nula.

Por outro lado, o número M de soluções pode ser dado por

$$M=p^{-1}\sum_{x,y}\sum_{v=1}^{p}\zeta^{v(x^k-y^k)}=p^{-1}\sum_{v=1}^{p}|T(v)|^2=p^{-1}\left(\sum_{v=1}^{p-1}|T(v)|^2+|T(p)|^2\right)$$

$$\Rightarrow M=p^{-1}\left(S_2+p^2\right)\Rightarrow S_2=p\left((p-1)k+1\right)-p^2=(k-1)p(p-1).$$

Além disso, do Lema 1.2.1 e Teorema 1.9

$$|T(u)|\leq\sum_{s=1}^{k-1}|\tau_u(\chi_s)|=(k-1)p^{\frac{1}{2}}\tag{1.18}$$

para $u \not\equiv 0(mod\ p)$. Segue portanto que

$$S_n = \sum_{u=1}^{p-1} |T(u)|^n = \sum_{u=1}^{p-1} |T(u)|^{n-2}|T(u)|^2 \leq (k-1)^{n-1}p^{n/2-1}p(p-1),$$

e finalmente,

$$N \geq p^{n-1} - (k-1)^{n-1}p^{n/2-1}(p-1). \tag{1.19}$$

Observe que os resultados acima nos fornecem uma condição suficiente para garantir a solubilidade não trivial de uma congruência do tipo $F(x_1, \ldots, x_n) \equiv 0(mod\ p)$, onde $F(x_1, \ldots, x_n)$ é uma forma aditiva de grau k em n variáveis. Basta mostrar que para esses valores de k, n e p tem-se $N > 1$. O próximo resultado segue da prova do Lema 2.4.1 de [6] e será uma ferramenta muito útil nos capítulos seguintes.

Lema 1.2.2 *Considere a congruência*

$$a_1x_1^k + \cdots + a_tx_t^k \equiv 0(\mathrm{mod}p). \tag{1.20}$$

Se p não divide k e $mdc(a_i, p) = 1$ para todo $i = 1, \cdots, t$, então a congruência (1.20) tem solução primitiva, sempre que

$$p > (d-1)^{(2t-2)/(t-2)},$$

onde $d = mdc(k, p-1)$.

1.3 p-Normalização

Nesta seção descreveremos o método de p-normalização, bem como apresentaremos alguns resultados sobre a solubilidade p-ádica de uma equação aditiva. O Lema a seguir pode ser encontrado em [5] Lema 2.

Lema 1.3.1 *Sejam $v_0, v_1, \cdots, v_{k-1} \in \mathbb{R}$ e $n = v_0 + \cdots + v_{k-1}$. Vamos assumir que $v_{k+i} = v_i$ para todo $i \in \mathbb{N} \cup \{0\}$. Então existe $r \in \mathbb{N}$ tal que*

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

Dizemos que duas formas aditivas em n variáveis são equivalentes se uma pode ser obtida da outra através de uma substituição $x_i = l_i x_i^{'}$, onde $l_1, \ldots, l_n$ são inteiros não nulos. É fácil ver que essa relação é simétrica, transitiva e reflexiva. A equivalência é tal que, se duas formas são equivalentes e uma representa zeros p-ádicos, então o mesmo ocorre com a outra. Como veremos a seguir, uma forma aditiva é sempre equivalente a uma cujos coeficientes se encontram em níveis menores do que o grau k e que tem propriedades especiais, dadas no resultado a seguir. Uma forma satisfazendo tais propriedades é dita *p-normalizada.*

Lema 1.3.2 *Seja $F = a_1 x_1^k + \cdots + a_n x_n^k$ uma forma aditiva de grau k em n variáveis. Então F pode ser escrita como*

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

onde F_j é uma subforma em v_j variáveis, para $j = 0, 1, \ldots, k-1$, com todos os coeficientes não divisíveis por p e com $v_0, v_1, \ldots, v_{k-1}$ satisfazendo

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

Prova. Escreva

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

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

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

pois, para os índices $i > k-1$, digamos $i = kt + r$ com $r < k$, podemos fazer a substituição das variáveis x_j de F_i por $p^t x_j$ e então as incluímos à subforma F_r, e estas novas variáveis ainda possuem unidades p-ádicas como coeficientes.

Seja v_i o núnero de variáveis de F_i. Assim, $v_0 + v_1 + \cdots + v_{k-1} = n$ e pelo Lema anterior existe um r tal que $v_r + \cdots + v_{r-1+t} \geq \frac{tn}{k}$ para $t = 1, 2, ..., k$. Vamos fazer uma

permutação cíclica das variáveis de F, substituindo todas as variáveis das subformas F_j's, com $j < r$, por $x = px^{'}$ e depois dividindo F por p^r, obtendo

$$F^{'} = p^{-r}F = F_r + pF_{r+1} + \cdots + p^{k-1-r}F_{k-1} + p^{k-r}F_0 + \cdots + p^{k-1}F_{r-1}.$$

Assim, reindexando as subformas obtemos

$$\begin{aligned} F^{'} &= F_0^{'} + pF_1^{'} + \cdots + p^{k-1}F_{k-1}^{'}, \text{ e} \\ & v_0^{'} + \cdots + v_{t-1}^{'} \geq \frac{tn}{k} \end{aligned}$$

para $t = 1, 2, ..., k$. Claramente se a forma $F^{'}$ possuir zeros p-ádicos não triviais, o mesmo ocorre com F. Portanto, podemos supor que F tem a forma descrita acima e assim

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

□

Devido a essa equivalência, podemos sempre supor que estamos trabalhando com uma forma p-normalizada e utilizar as propriedades descritas no Lema **??**. Dizemos que uma variável está no nível j se seu coeficiente é divisível por p^j mas não é divisível por p^{j+1}, isto é, as variáveis das subformas F_j descritas no Lema **??** estão no nível j. O próximo resultado é uma condição necessária e suficiente para garantir a solubilidade p-ádica não trivial de uma forma aditiva.

Lema 1.3.3 *Seja $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. A congruência*

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

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

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

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

Definição 1.5 *Seja k um número natural e p um número primo. Escreva $k = p^{\tau}k_0$ com $mdc(k_0, p) = 1$. Vamos definir o número γ como*

$$\gamma = \begin{cases} \tau + 1 \ \ se \ \ p > 2 \\ \tau + 2 \ \ se \ \ p = 2 \\ 1 \quad se \ \ \tau = 0. \end{cases}$$

Lema 1.3.4 *Se a congruência*

$$x^k \equiv m \,(\mathrm{mod}\ p^\gamma)$$

tem solução, onde $mdc(m,p) = 1$, *então a congruência*

$$y^k \equiv m \,(\mathrm{mod}\ p^\nu)$$

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

O resultado acima encontra-se em [7]. Sejam F uma forma aditiva como no Lema 1.3.2 e γ como na Definição 1.5. Denotaremos por *solução primitiva* uma solução da congruência $F \equiv 0(\mathrm{mod}\ p^\gamma)$ com pelo menos uma das variáveis em F_0 não divisível por p.

A seguir veremos que para garantir a solubilidade não trivial de uma forma aditiva em $\mathbb{Q}_p$, basta estabelecer uma cota n que garanta a existência de uma solução primitiva para a congruência módulo uma potência específica de p.

Lema 1.3.5 *Suponha que a congruência*

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

tenha solução primitiva. Então a equação

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

tem solução p-ádica não trivial.

1.4 Contração de variáveis

Nesta seção vamos apresentar a operação de *contração de variáveis*, que consiste basicamente em substituir uma soma de um determinado número de termos de F por um único termo. O resultado a seguir é uma ferramenta fundamental para esse método e pode ser encontrado em [5].

Lema 1.4.1 *Seja* $\delta = (k, p-1)$ *e suponha que* $c_1 c_2 \ldots c_{\delta+1} \not\equiv 0(\mathrm{mod}\ p)$.

Então a congruência

$$c_1 x_1^k + \cdots + c_{\delta+1} x_{\delta+1}^k \equiv 0 (\text{mod } p) \tag{1.21}$$

tem solução com $x_1 \not\equiv 0 (\text{mod } p)$.

Prova. Desde que $x^k \equiv m(\text{ mod } p)$ tem solução em x se, e somente se, o mesmo ocorre para $x^\delta \equiv m(\text{mod } p)$, podemos substituir k por δ em (1.21). Suponha, por absurdo, que a conclusão do Lema não é verdadeira. Então

$$c_1 + c_2 x_2^\delta + \cdots + c_{\delta+1} x_{\delta+1}^\delta \not\equiv 0 (\text{mod } p),$$

para todo $x_2, ..., x_{\delta+1}$. Assim,

$$\left(c_1 + c_2 x_2^\delta + \cdots + c_{\delta+1} x_{\delta+1}^\delta\right)^{p-1} \equiv 1 (\text{mod } p)$$

para todo $x_2, ..., x_{\delta+1}$, o que significa que o produto do lado esquerdo da congruência é o polinômio identicamente 1.

Expandindo esse produto e substituindo x_j^p por x_j para cada j, obtemos termos com expoentes no máximo $p-1$. Entretanto, na expansão aparece um termo

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

com $a \not\equiv 0(\text{ mod } p)$, que não é afetado por tal substiuição e todos os outros termos contém pelo menos uma das variáveis $x_2, ..., x_{\delta+1}$ com uma potência menor do que $p-1$. Portanto, esse polinômio não pode ser reduzido ao polinômio identicamente 1, o que é um absurdo.

□

Para $\tau > 0$, nós definimos a **operação de contração** como sendo a substituição de um conjunto de $\delta + 1$ termos em algum F_j por um único termo em algum F_i, onde $i > j$.

Considere uma soma

$$d_1 y_1^k + \cdots + d_{\delta+1} y_{\delta+1}^k$$

onde $d_1 \ldots d_{\delta+1} \not\equiv 0 (mod\ p)$.

Uma das variáveis $y_1, \ldots, y_{\delta+1}$ é distinta das outras, e tomamos essa variável distinta como sendo y_1.

Pelo Lema 1.4.1, existe uma solução

$$d_1a_1^k + \cdots + d_{\delta+1}a_{\delta+1}^k \equiv 0(mod\ p)$$

com $a_1 \not\equiv 0(mod\ p)$.

Escolhendo a solução de maneira conveniente, podemos supor que

$$d_1a_1^k + \cdots + d_{\delta+1}a_{\delta+1}^k = p^\sigma e,$$

onde $\sigma \geq 1$, e $e \not\equiv 0(mod\ p)$.

A substituição $y_i = a_i z$ transforma a soma $d_1y_1^k + \cdots + d_{\delta+1}y_{\delta+1}^k$ em um único termo

$$p^\sigma e z^k.$$

Note que $z \not\equiv 0(mod\ p)$ implica em $y_1 \not\equiv 0(mod\ p)$.

Operações de contração de variáveis serão primeiramente aplicadas a conjuntos de $\delta+1$ termos de F_0, e aqui qualquer uma das variáveis pode ser tomada como sendo a variável distinta.

O restante das variáveis de F_0 que não estão nesses conjuntos são igualadas a zero, e isso resulta numa forma do tipo

$$pG_1 + p^2G_2 + \ldots,$$

onde a forma G_j contém os v_j termos originais de F_j mais os possíveis termos adicionais resultantes do processo de contração.

As variáveis obtidas pelo processo de contração são chamadas **variáveis primárias.** Além disso, a congruência $d_1x_1^k + \cdots + d_sx_s^k \equiv 0(\ \mathrm{mod}\ \ p)$ possui sempre solução, mesmo que seja a solução trivial. Isso também gera novas variáveis em níveis superiores. Denotamos por **variáveis secundárias** as variáveis obtidas através de soluções triviais de somas de um determinado número de termos de F. Aplicamos novamente o processo de contração, agora a grupos de $\delta + 1$ termos de G_1, sujeitos à condição de que cada grupo contém pelo menos uma variável primária. Tal variável é escolhida como sendo a variável distinta na contração.

Suponha que após um número permissível de contrações obtemos uma forma H tal que

$$H \equiv 0(mod\ p^\gamma)$$

tem solução com pelo menos uma das variáveis primárias não nulas módulo p. Esse é o caso se obtemos a forma

$$H = p^{\mu} H_{\mu} + p^{\mu+1} H_{\mu+1} + \dots$$

onde as subformas $H_{\gamma}, H_{\gamma+1}$ contêm uma variável primária. Podemos tomar essa variável primária igual a 1 e as outras variáveis iguais a zero. Como a variável primária foi obtida de sucessivas contrações a partir de variáveis de F_0, isto implica em uma solução de

$$F \equiv 0 (mod\ p^{\gamma})$$

com pelo menos uma das variáveis em F_0 não divisível por p. Como já vimos na seção anterior, isso é suficiente para garantir a solubilidade p-ádica não trivial de $F = 0$ e esse é chamado o *caso solúvel.*

CAPÍTULO 2

Valor exato de $\Gamma^*(k,p)$ quando $p-1$ divide k

Neste capítulo vamos considerar

$$F(x_1,\ldots,x_n) = a_1x_1^k + \cdots + a_nx_n^k \tag{2.1}$$

com coeficientes inteiros e determinar o menor número de variáveis, em função do grau k, que garantem a solubilidade p-ádica não trivial de $F=0$ quando $p-1$ divide k. Os resultados apresentados aqui são baseados em [10], onde M. Knapp apresenta o menor número de variáveis para garantir que uma forma aditiva com coeficientes inteiros tem zeros p-ádicos não triviais, no caso em que $p=2$.

Em 1966 Dodson mostrou que

$$\left\lfloor \frac{k}{\gamma} \right\rfloor (p^\gamma - 1) + 1 \leq \Gamma^*(k,p) \leq \left\lfloor \frac{k}{\gamma}(p^\gamma - 1) \right\rfloor + 1. \tag{2.2}$$

Observe que quando γ divide k os limitantes acima coincidem. Por outro lado, quando k cresce, a diferença entre eles tende ao infinito.

Lema 2.0.2 *Sejam p um número primo, $k = p^\tau k_0$ onde $p \nmid k_0$, e $\gamma = \tau + 1$. Defina $A_k = \left\lfloor \frac{k}{\gamma} \right\rfloor (p^\gamma - 1) + 1$ e $B_k = \left\lfloor \frac{k}{\gamma}(p^\gamma - 1) \right\rfloor + 1$, então $\lim\limits_{k\to\infty}(B_k - A_k) = \infty$.*

Prova. Escreva $k = \gamma q + r$, $(p^\gamma - 1) = \gamma l + s$ e $rs = \gamma u + w$, onde $0 \leq r, s, w < \gamma$. Assim,

$$\begin{aligned} A_k &= \left\lfloor \frac{k(p^\gamma - 1)}{\gamma} \right\rfloor = \left\lfloor \frac{(\gamma q + r)(\gamma l + s)}{\gamma} \right\rfloor = \left\lfloor \frac{\gamma^2 ql + \gamma qs + \gamma lr + rs}{\gamma} \right\rfloor \\ &= \gamma ql + qs + lr + \left\lfloor \frac{rs}{\gamma} \right\rfloor = \gamma ql + qs + lr + u \end{aligned}$$

$$B_k = \left\lfloor \frac{k}{\gamma} \right\rfloor (p^\gamma - 1) = \left\lfloor \frac{\gamma q + r}{\gamma} \right\rfloor (\gamma l + s) = \gamma ql + qs$$

de onde obtemos que $A - B = lr + u$, com $0 \leq r < \gamma$.

Observe que $\gamma u + w = rs \leq (\gamma - 1)^2$. Se $u > \gamma - 1$, então

$$\gamma u > \gamma(\gamma - 1) \Rightarrow \gamma u + w > \gamma(\gamma - 1) > (\gamma - 1)^2,$$

absurdo. Logo, $u \leq \gamma - 1$. Assim, desde que r e u estão limitados, é suficiente mostrarmos que $l = l(\gamma)$ não é limitado, e $lr + u \to \infty$ quando $l \to \infty$.

Suponha que exista um $M > 0$ tal que $l \leq M$, para todo γ. Então

$$(p^\gamma - 1) = \gamma l + s \leq M\gamma + s \Rightarrow p^\gamma \leq M\gamma + s + 1 \Rightarrow \frac{p^\gamma}{\gamma} \leq M + \frac{s}{\gamma} + \frac{1}{\gamma} < M + 2,$$

contrariando o fato de que $\lim_{\gamma \to \infty} \frac{p^\gamma}{\gamma} = \infty$. O absurdo surgiu do fato de supormos que l é limitado por um inteiro M. Portanto, l não é limitado e quando $l \to \infty$ o resultado segue.

□

Do lema acima podemos ver que, para valores grandes de k, nem sempre é possível obter uma boa estimativa para $\Gamma^*(k, p)$ usando (2.2) já que a diferença entre as cotas superior e inferior pode ser significativamente grande.

O próximo resultado nos fornece o valor exato de $\Gamma^*(k, p)$ dependendo de k, para os primos tais que $p - 1 \mid k$, que é o objetivo principal deste capítulo.

Teorema 2.1 *Seja $k = p^\tau k_0$, com $mdc(k_0, p) = 1$ e γ como na Definição 1.5. Escreva $k = \gamma q + r$, onde q e r são inteiros e $0 \leq r \leq \gamma - 1$. Então*

$$\Gamma^*(k, p) \leq (p^\gamma - 1)q + p^r,$$

e a igualdade ocorre quando $p - 1$ divide k.

A seguir apresentamos alguns lemas que serão peças fundamentais na demonstração do Teorema 2.1.

2.1 Lemas preliminares

O próximo lema pode ser encontrado em [9] e é uma generalização do Lema 1 de [3].

Lema 2.1.1 *Seja n um inteiro positivo e suponha que para $i = 0, ..., n$ tem-se*

$$F_i = \sum_{j=1}^{m_i} a_{ij}x_{ij} \text{ com } p \nmid a_{ij} \ \forall i, j$$

e com v_i satisfazendo $\sum_{i=0}^{l-1} v_i \geq p^l$, para cada $l = 1, ..., n$.

Então para todo inteiro positivo $N > n$, a forma $\sum_{i=0}^{n} p^i F_i$ representa pelo menos $\min(\sum_{i=0}^{n} v_i, p^N)$ classes de resíduos $(\text{mod } p^N)$, onde os x_{ij} são 0 ou 1 e com pelo menos um dos $x_{0j} = 1$.

Lema 2.1.2 *Sejam β, a inteiros positivos tais que $\beta > p - 1$ e $a\beta > p^a - 1$. Então $t\beta > p^t - 1$ sempre que $2 \leq t \leq a - 1$.*

Prova. Defina $f(t) = t\beta - p^t + 1$. O lema é equivalente à afirmação de que $f(t) > 0$ para todo $1 \leq t \leq a$ e , por hipótese, isso é verdadeiro para $t = 1$ e $t = a$. Como f é uma função de uma variável real t, então $f'(t) = \beta - p^t \ln p$.

Desde que

$$f'(t) = 0 \Leftrightarrow \beta - p^t \ln p = 0 \Leftrightarrow t = \log_p \left(\frac{\beta}{\ln p} \right),$$

existe um único ponto crítico, digamos $t_0 = \log_p \left(\frac{\beta}{\ln p} \right)$ tal que $f'(t_0) = 0$. Além disso, $f'(t) > 0$ para $t < t_0$ e $f'(t) < 0$ para $t > t_0$. Isto significa que t_0 é um ponto de máximo local e f é uma função decrescente a partir de t_0. Suponha por absurdo que exista um número t_1 entre 1 e a tal que $f(t_1) < 0$. Por hipótese temos $f(1) > 0$ e $f(a) > 0$, e portanto f decresce antes de t_1 e cresce depois de t_1, isto é, $f'(t) < 0$ para $t < t_1$ e $f'(t) > 0$ para $t > t_1$. Mas isso nos diz que t_1 é ponto de mínimo local, contrariando existência de um único ponto crítico.

□

Lema 2.1.3 *Suponha que r, γ e $q \in \mathbb{N}$, com $\gamma \geq 2$ e p um primo ímpar, $0 \leq r \leq \gamma - 1$, e seja $k = \gamma q + r$. Além disso, suponha que $v_0, ..., v_{\gamma-2}$ são inteiros tais que*

$$v_0 + \cdots + v_{t-1} \geq t\frac{(p^\gamma - 1)q + p^r}{k}, \quad 1 \leq t \leq \gamma - 1.$$

Então temos que

$$v_0 + \cdots + v_{t-1} > p^t - 1, \quad 1 \leq t \leq \gamma - 1.$$

Prova. Do Lema 2.1.2 é suficiente mostrar que, para $t = 1$ e $t = \gamma - 1$ tem-se

$$t\frac{(p^\gamma - 1)q + p^r}{k} > p^t - 1.$$

Suponhamos inicialmente que $t = 1$. Queremos provar que

$$\frac{(p^\gamma - 1)q + p^r}{k} > p - 1$$

Note que a desigualdade acima equivale a

$$(p^\gamma - 1)q + p^r > (p - 1)\gamma q + (p - 1)r$$

e isso ocorre desde que $p^r > (p-1)r$. Se $r = 0$ ou $r = 1$ o resultado vale. Suponha como hipótese de indução que o resultado seja válido para um r fixado, vamos mostrar que vale para $r + 1$. De fato,

$$p^{r+1} = p \cdot\ p^r > p(p-1)r = (p-1)r + (p-1)(p-1)r > (p-1)r + (p-1) = (p-1)(r+1).$$

Agora suponha que $t = \gamma - 1$ e, neste caso, podemos considerar $\gamma \geq 3$. Queremos provar que

$$(\gamma - 1)\frac{(p^\gamma - 1)q + p^r}{k} > p^{\gamma-1} - 1. \tag{2.3}$$

Note que isso é verdade se, e somente se,

$$\begin{aligned}
(\gamma - 1)((p^\gamma - 1)q + p^r) &> (p^{\gamma-1} - 1)k \Leftrightarrow \\
(\gamma - 1)((p^\gamma - 1)q + p^r) &> (p^{\gamma-1} - 1)(\gamma q + r) \Leftrightarrow \\
(\gamma - 1)((p^\gamma - 1)q + p^r) &> p^{\gamma-1}(\gamma q + r) - \gamma q - r
\end{aligned}$$

onde a última desigualdade equivale a mostrar que

$$\begin{aligned}(\gamma-1)((p^\gamma-1)q+p^r)-p^{\gamma-1}(\gamma q+r)+\gamma q+r &> 0 \Leftrightarrow\\ (\gamma-1)((p^\gamma-1)q+(\gamma-1)p^r)-p^{\gamma-1}(\gamma q+r)+\gamma q+r &> 0 \Leftrightarrow\\ (\gamma p^\gamma-\gamma-p^\gamma+1)q+(\gamma-1)p^r-p^{\gamma-1}(\gamma q+r)+\gamma q+r &> 0 \Leftrightarrow\\ p^{\gamma-1}(\gamma q(p-1)-pq-r)+((\gamma-1)p^r+q+r) &> 0. \qquad (2.4)\end{aligned}$$

Desde que $(\gamma-1)p^r+q+r>0$, para mostrar que (2.4) vale, é suficiente mostrar que $\gamma q(p-1)-pq-r\geq 0$ e isso ocorre sempre que $r\leq \gamma q(p-1)-pq$. Observe que, como $r\leq \gamma-1$, então (2.4) falha se

$$\gamma q(p-1)-pq<r\leq \gamma-1,$$

o que implica que

$$q\leq \frac{\gamma-1}{\gamma(p-1)-p}=1+\frac{\gamma(2-p)+p-1}{\gamma(p-1)-p}.$$

Por outro lado,

$$\frac{\gamma(2-p)+p-1}{\gamma(p-1)-p}<1,$$

para $p\geq 3$ e $\gamma\geq 3$. Assim, o único problema seria quando $q=1$ e , neste caso, mostrar que (2.3) vale é equivalente a mostrar que

$$\frac{(\gamma-1)(p^\gamma+p^r-1)}{(\gamma+r)(p^{\gamma-1}-1)}>1.$$

Note que a desigualdade acima é verdadeira, pois

$$\begin{aligned}\frac{(\gamma-1)(p^\gamma+p^r-1)}{(\gamma+r)(p^{\gamma-1}-1)} &\geq \frac{(\gamma-1)(p^\gamma+p^r-1)}{(2\gamma-1)(p^{\gamma-1}-1)}\\ &> \frac{2}{5}\frac{p^\gamma+p^r-1}{p^{\gamma-1}-1}>1,\end{aligned}$$

desde que p é um primo ímpar e $\gamma\geq 3$.

□

Agora temos todas as ferramentas necessárias para demonstrar o Teorema 2.1.

2.2 Prova do Teorema 2.1

O caso $p = 2$ foi provado por M. Knapp em [10], então podemos assumir que p é um primo ímpar. Além disso, quando $\gamma \mid k$, o resultado segue de (2.2). Assim, podemos também asumir que $\gamma \nmid k$ e portanto $\tau > 0$. Observe que neste caso temos $\left\lfloor \frac{k}{\gamma} \right\rfloor > 0$ pois, se $\left\lfloor \frac{k}{\gamma} \right\rfloor = 0$, como $k = \left\lfloor \frac{k}{\gamma} \right\rfloor \gamma + r$ teríamos $k = p^{\tau} k_0 = r < \gamma = \tau + 1$, o que é impossível para $p \geq 3$.

Como já vimos, se F é uma forma aditiva de grau k com coeficientes inteiros, então podemos escrever F separando suas variáveis em k níveis, e obtemos

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

Suponha que o número de variáveis de F seja $n = (p^{\gamma} - 1)q + p^r$. Pelo Lema 1.3.2 temos

$$v_0 + \cdots + v_{t-1} \geq t\frac{(p^{\gamma} - 1)q + p^r}{k}, \quad 1 \leq t \leq \gamma - 1 = \tau,$$

e o Lema 2.1.3 nos garante que

$$v_0 + \cdots + v_{t-1} \geq p^t \quad 1 \leq t \leq \tau.$$

Se além disso tivermos $v_0 + \cdots + v_{\tau} \geq p^{\tau+1} = p^{\gamma}$, o resultado segue do Lema 2.1.1. Portanto, sem perda de generalidade, podemos supor que

$$v_0 + \cdots + v_{\tau} \leq p^{\gamma} - 1.$$

Desde que $k = \gamma q + r$ e $0 < r < \gamma$, se separarmos os índices das subformas F_j em conjuntos de $\tau + 1 = \gamma$ elementos, então q é o número máximo de conjuntos que podemos formar.

Suponha que exista um número h, com $1 \leq h \leq q - 1$, para o qual podemos encontrar h conjuntos $S_1, \cdots, S_h \subset \{0, 1, \cdots, k - 1\}$ satisfazendo:

1. $|S_i| = \tau + 1$ para cada i;

2. $S_i = \{s_i, s_i + 1, \cdots, s_i + \tau\}$;

3. $v_{s_i} + \cdots + v_{s_i+t-1} \geq p^t$, para todo $1 \leq t \leq \tau$ e para cada conjunto S_i;

4. $v_{s_i} + \cdots + v_{s_i+\tau} \leq p^{\tau+1} - 1$, para cada conjunto S_i.

Note que $S_1 = \{0, 1, ..., \tau\}$ satisfaz as propriedades $(1) - (4)$. Portanto existe pelo menos um conjunto satisfazendo tais propriedades.

Lema 2.2.1 *Nas notações acima, ou F tem zeros p-ádicos não trivais ou podemos obter um conjunto S_{h+1} disjunto de $S_1 \cup \cdots \cup S_h$ satisfazendo as propriedades $(1) - (4)$.*

Prova. Sejam F_j as subformas como no Lema 1.3.2, onde $j \notin \cup S_i$. Como existem h subconjuntos S_i de índices, cada $|S_i| = \tau + 1$ e existem $k = \gamma q + r$ subformas F_j no total, então existem pelo menos $\alpha = \gamma q + r - h(\tau + 1) = (\tau + 1)(q - h) + r$ subformas F_j, onde $j \notin \cup S_i$. Além disso, como $v_{s_i} + \cdots + v_{s_i+\tau} \leq p^{\tau+1} - 1$, e temos um total de $(p^\gamma - 1)q + p^r$ variáveis, então o número de variáveis nas subformas F_j com $j \notin \cup S_i$ é pelo menos

$$(p^\gamma - 1)q + p^r - (p^{\tau+1} - 1)h = (p^{\tau+1} - 1)(q - h) + p^r.$$

Sejam $F_{i_0}, F_{i_1}, \cdots, F_{i_{\alpha-1}}$ tais subformas, onde $1 \leq i_0 < i_1 < \cdots < i_{\alpha-1} \leq k - 1$. Observe que $v_0, v_1, \cdots, v_{k-1}$ satisfazem $v_{(j+k)} = v_j, \ \forall j$. Além disso,

$$\begin{aligned} v_0 + v_1 + \cdots + v_{k-1} &= (p^{\tau+1} - 1)q + p^r \\ v_{i_0} + v_{i_1} + \cdots + v_{i_{\alpha-1}} &\geq (p^{\tau+1} - 1)(q - h) + p^r. \end{aligned}$$

Pelo Lema 1.3.1, existe um número r tal que

$$v_r + \cdots + v_{r+t-1} \geq t\frac{(p^{\tau+1} - 1)(q - h) + p^r}{(\tau + 1)(q - h) + r},$$

para cada t com $1 \leq t \leq \alpha$, onde $r, ..., r + t - 1 \in \{i_0, \cdots, i_{\alpha-1}\}$.

Seja $(w_0, w_1, \cdots, w_{\alpha-1})$ uma permutação cíclica de $(i_0, \cdots, i_{\alpha-1})$ tal que, para cada t, com $1 \leq t \leq \alpha$ vale

$$v_{w_0} + \cdots + v_{w_{t-1}} \geq t\frac{(p^{\tau+1} - 1)(q - h) + p^r}{(\tau + 1)(q - h) + r},$$

Pelo Lema 2.1.3 temos que

$$v_{w_0} + \cdots + v_{w_{t-1}} \geq p^t, \quad 1 \leq t \leq \tau.$$

Suponha primeiramente que os índices $w_0, ..., w_\tau$ não são consecutivos. Este seria o caso, por exemplo, se $S_1 = \{0, ..., \tau\}$ e existe um conjunto S_2, mas $\tau+1$ não seja o primeiro elemento desse conjunto, e assim sucessivamente, onde F é escrita da forma

$$F_0 + \cdots + p^\tau F_\tau + p^{\tau+1} F_{\tau+1} + \cdots + p^{s_2} F_{s_2} + p^{s_2+1} F_{s_2+1} + \cdots + p^{s_2+\tau} F_{s_2+\tau} + \cdots + p^{k-1} F_{k-1}.$$

Então existe um menor número $z \leq \tau$ tal que $w_z = w_0 + z$, mas $w_{z+1} \neq w_z + 1 = w_0 + z + 1$ e $w_z + 1$ é o menor elemento de um dos conjuntos S_i definidos anteriormente. Por exemplo, se $w_z = k - 1$, $w_{z+1} \neq k$ (ou $w_{z+1} \neq 0$) e $w_z + 1 = k$, então $w_{z+1} \geq \tau + 1$, pois $S_1 = \{0, ..., \tau\}$ e portanto, se $s_2 \neq \tau + 1$, então $w_{z+1} = \tau + 1$, se $s_2 = \tau + 1$, então $w_{z+1} = 2\tau+1$, etc. Nesse caso, podemos fazer uma mudança de variáveis $x = yp$ nos níveis $0, 1, ..., \tau$, levando as variáveis desses níveis para os níveis $k, k + 1, ..., k + \tau$ e considerar $s_1 = k$ e $S_1 = \{k, k + 1, ..., k + \tau\}$, isto é, de fato $w_z + 1 = s_i$ para algum i, mas $w_0, ..., w_z$ são consecutivos, $1 \leq z \leq \tau$. Pelo Lema 2.1.1, temos que

$$F_{w_0} + pF_{w_1} + \cdots + p^z F_{w_z} \equiv 0 (\text{mod } p^{z+1})$$

tem solução com alguma variável de F_{w_0} ímpar, o que implica que

$$\begin{aligned} p^{w_0}(F_{w_0} + pF_{w_1} + \cdots + p^z F_{w_z}) &\equiv 0 (\text{mod } p^{w_0+z+1}) \\ &\equiv 0 (\text{mod } p^{w_z+1}) \end{aligned}$$

tem solução com uma variável em F_{w_0} coprima com p.

Se essa solução é de fato uma solução módulo $p^{w_0+\tau+1}$, isto é, se estamos no caso em que $z = \tau$, o Lema 1.3.5 nos garante a solubilidade p-ádica não trivial.

Caso contrário, podemos contrair as variáveis utilizadas nessa solução para gerar uma variável primária em algum nível p^{w_0+z+l}, $z + 1 \leq z + l \leq \tau$. Digamos que a variável primária seja y com coeficiente a_y, onde $a_y \equiv 0 (\text{mod } p^{w_z+1})$.

Vamos agora considerar a forma

$$p^{s_i} F_{s_i} + \cdots + p^{s_i+\tau-1} F_{s_i+\tau-1}.$$

Das propriedades de S_i, temos que

$$\begin{aligned} v_{s_i} + \cdots + v_{s_i+\tau-2} &\geq p^{\tau-1} \\ v_{s_i} + \cdots + v_{s_i+\tau-1} &\geq p^\tau \end{aligned}$$

e novamente o Lema 2.1.1 nos garante que $\sum_{j=0}^{\tau-1} p^j F_{s_i+j}$ representa $\min\left(\sum_{j=0}^{\tau-1} v_{s_i+j}, p^\tau\right) = p^\tau$ classes de resíduos módulo p^τ. Portanto a forma $p^{s_i}(F_{s_i} + \cdots + p^{\tau-1}F_{s_i+\tau-1})$ representa todos os múltiplos de p^{s_i} módulo $p^{s_i+\tau}$.

Como $w_z+1 = s_i$ para algum i, e $p^{w_z+1} \mid ay$, se fizermos $y = 1$, desde que a_y é múltiplo de p^{s_i}, podemos resolver não trivialmente a congruência

$$a_y + p^{s_i}F_{s_i} + \cdots + p^{s_i+\tau-1}F_{s_i+\tau-1} \equiv 0 (\text{mod } p^{s_i+\tau}).$$

Isso nos fornece uma solução para $F \equiv 0 (\text{mod } p^{s_i+\tau})$ com uma variável coprima com p no nível w_0. Desde que $s_i + \tau \geq w_0 + 1 + \tau = w_0 + (\tau + 1)$, o Lema 1.3.5 nos garante a solubilidade p-ádica não trivial para $F = 0$.

Portanto, no caso em que os números $w_0, ..., w_\tau$ não são consecutivos temos a solubilidade desejada.

Suponha agora que os índices $w_0, ..., w_\tau$ são consecutivos e defina $S_{\tau+1} = \{w_0, ..., w_\tau\}$. Já vimos que este conjunto satisfaz as propriedades $(1) - (3)$ anteriores. Se além disso tivermos $v_{w_0} + \cdots + v_{w_\tau} \geq p^{\tau+1}$, o Lema 2.1.1 nos garante que podemos resolver

$$p^{w_0}F_{w_0} + \cdots + p^{w_\tau}F_{w_\tau} \equiv 0 (\text{mod } p^{w_0+\tau+1})$$

com pelo menos uma variável ímpar em F_0, e isto nos fornece uma solução p-ádica não trivial pelo Lema 1.3.5.

Portanto, podemos assumir que $v_{w_0} + \cdots + v_{w_\tau} \leq p^{\tau+1} - 1$ e daí $S_{\tau+1}$ satisfaz as propriedades $(1) - (4)$.

□

Lema 2.2.2 *Se existirem $S_1, ..., S_q$ conjuntos disjuntos satisfazendo as propriedades* (1), (2), (3) *e* (4) *acima, então a forma F tem zeros p-ádicos não triviais.*

Prova. Suponha que existam q conjuntos disjuntos $S_1, ..., S_q$ com as propriedades listadas anteriormente. Então existem exatamente r índices j das subformas F_j tais que $j \notin S_i$.

Suponhamos que essas formas sejam $F_{i_0}, \cdots, F_{i_{r-1}}$, com $0 \leq i_0 < i_1 < \cdots < i_{r-1} \leq k - 1$. Pelo Lema 1.3.1, podemos reescrever essas subformas como $F_{m_0}, \cdots, F_{m_{r-1}}$, de

modo que $(m_0, \cdots, m_{r-1})$ é uma permutação cíclica de $i_0, \cdots, i_{r-1}$ e para cada t com $1 \leq t \leq r$, temos

$$v_{m_0} + \cdots + v_{m_{t-1}} \geq t\frac{p^r}{r}.$$

Observe que

- para $t = 1$, $v_{m_0} \geq \frac{p^r}{r} \geq p$;
- para $t = r$, $v_{m_0} + \cdots + v_{m_{r-1}} \geq p^r$.

Logo, pelo Lema 2.1.2, temos que

$$t\frac{p^r}{r} > p^t - 1, \quad 1 \leq t \leq r.$$

Em particular,

$$v_{m_0} + \cdots + v_{m_{t-1}} \geq p^t, \quad 1 \leq t \leq r.$$

Seja z o menor inteiro tal que $m_z = m_0 + z$, mas $m_{z+1} \neq m_z + 1 = m_0 + z + 1$. Então $m_z + 1$ é o menor elemento de um dos conjuntos S_i e temos que $m_z + 1 = s_i$ para algum índice i. Novamente, se $m_z = k - 1$, então por uma mudança de variáveis podemos considerar S_1 como sendo o conjunto $\{k, k+1, \cdots, k+\tau\}$ e $s_1 = k$. Observe que não há problema se todos os $m_0, m_1, \cdots, m_{r-1}$ forem consecutivos, pois voltaríamos ao caso em que $m_z = k - 1$.

Pelo Lema 2.1.1, como $v_{m_0} + \cdots + v_{m_{t-1}} \geq p^t$, $1 \leq t \leq r$, então

$$F_{m_0} + pF_{m_1} + \cdots + p^z F_z \equiv 0 (\text{mod } p^{z+1})$$

tem solução com pelo menos uma variável coprima com p em F_{m_0}, o que implica em uma solução primitiva para

$$p^{m_0}\left(F_{m_0} + pF_{m_1} + \cdots + p^z F_{m_z}\right) \equiv 0 (\text{mod } p^{m_0+z+1})$$

e portanto podemos resolver

$$p^{m_0}F_{m_0} + p^{m_0+1}F_{m_1} + \cdots + p^{m_0+z}F_z \equiv 0 (\text{mod } p^{m_z+1})$$

com alguma variável de F_{m_0} coprima com p.

Se a solução acima for de fato uma solução módulo $p^{m_0+\tau+1}$ isso nos fornece uma solução p-ádica não trivial pelo Lema 1.3.5.

Caso contrário, podemos fazer uma contração com as variáveis usadas nessa solução e gerar uma variável y, com coeficiente a_y, em algum nível p^{m_0+z+l}, onde $z+1 \leq z+l \leq \tau$ e $a_y \equiv 0(\text{mod } p^{m_0+z+1})$ ou ainda, $a_y \equiv 0(\text{mod } p^{s_i})$ para algum i.

Considere a forma

$$p^{s_i}F_i + \cdots + p^{s_i+\tau-1}F_{s_i+\tau-1}.$$

Da definição dos conjuntos S_i, temos que

$$v_{s_i} + \cdots + v_{s_i+j-1} \geq p^j,\ 1 \leq j \leq \tau,$$

e do Lema 2.1.1 isso implica que

$$p^{s_i}\left(F_i + \cdots + p^{\tau-1}F_{s_i+\tau-1}\right)$$

representa todos os múltiplos de p^{s_i} módulo $p^{s_i+\tau}$. Como p^{s_i} divide a_y, fazendo $y = 1$, podemos resolver a congruência

$$a_y + p^{s_i}F_{s_i} + \cdots + p^{s_i+\tau-1}F_{s_i+\tau-1} \equiv 0(\text{mod } p^{s_i+\tau}).$$

Essa solução leva a uma solução de $F \equiv 0(\text{mod } p^{s_i+\tau})$ que envolve uma variável no nível m_0 que é coprima com p. Desde que $s_i+\tau \geq m_0+1+\tau$, pelo Lema 1.3.5 isso nos fornece uma solução p-ádica não trivial.

□

Pelo Lema 2.2.1 vimos que, ou $F = 0$ tem solução p-ádica não trivial, ou podemos obter q subconjuntos disjuntos $S_1, ..., S_q$, e nesse caso o Lema 2.2.2 nos garante a solubilidade desejada.

Como de costume, a solubilidade p-ádica não trivial foi garantida via Lema 1.3.5. Ficou provado que $\Gamma^*(k,p) \leq (p^\gamma - 1)q + p^r$. Para concluirmos a prova do Teorema precisamos ainda mostrar que a cota apresentada é a melhor possível quando $p-1$ divide k. Para isso, nas condições anteriores, observe que se x é um múltiplo de p, então

$$x^k = x^{p^\tau k_0} \equiv 0(\text{mod } p^\gamma).$$

Se p não divide x, desde que $\varphi(p^\gamma) = p^{\gamma-1}(p-1)$, então $x^{p^\tau(p-1)} \equiv 1(\text{mod } p^\gamma)$. Como $k = p^\tau k_0$ e $p-1 \mid k_0$, segue que $k_0 = (p-1)k_1$ e

$$x^k = (x^{p^\tau(p-1)})^{k_1} \equiv 1(\text{mod } p^\gamma).$$

Considere a forma aditiva

$$F = \sum_{i=1}^{p^\gamma-1} x_i^k + p^\gamma \sum_{i=p^\gamma}^{2(p^\gamma-1)} x_i^k + \cdots + p^{(q-1)\gamma} \sum_{i=(q-1)(p^\gamma-1)+1}^{q(p^\gamma-1)} x_i^k + p^{q\gamma} \sum_{i=q(p^\gamma-1)+1}^{q(p^\gamma-1)+p^r-1} x_i^k. \quad (2.5)$$

O próximo lema é trivial, e omitiremos a prova.

Lema 2.2.3 *Seja* $H = \sum_{i=1}^{p^t-1} x_i^k$, *onde* $p-1 \mid k$. *Então* $H \equiv 0(\text{mod } p^t)$ *não possui solução não trivial,* $\forall\ t \leq \gamma$.

Agora, suponha que $F(\xi) = 0$ em $\mathbb{Z}_p$. Como é homogêneo, podemos supor que alguma entrada de ξ é uma unidade em $\mathbb{Z}_p$, em particular, essa entrada é coprima com p. Seja $m = p^\gamma - 1$ e escreva

$$\begin{aligned} F_j &= F_j(x_{1j}, \cdots, x_{mj}), \quad \text{para } \ j = 0, \cdots, q-1, \\ \xi &= (\xi_{10}, \cdots, \xi_{m0}, \cdots, \xi_{1(q-1)} \cdots, \xi_{m(q-1)}, \eta_1, \cdots, \eta_{p^r-1}) \end{aligned}$$

e suponha que a primeira entrada de ξ coprima com p corresponda a uma variável de F_j, para algum j fixado. Sem perda de generalidade podemos supor que a primeira unidade é ξ_{1j}. Assim, temos que $\xi_{uv} = p\xi_{uv}^*,\ \forall\ v \leq j-1$. Logo,

$$\begin{aligned} F(\xi) &= p^k \left(\sum_{i=0}^{j-1} p^{i\gamma} F_i(\xi_i^*) \right) + p^{\gamma j} F_j(\xi_j^*) + p^{\gamma(j+1)} G = 0 \\ p^{-\gamma j} F(\xi) &= F_j(\xi_j^*) + p^\gamma G + p^{k-\gamma j} H = 0, \end{aligned}$$

onde $H = \sum_{i=0}^{j-1} p^{i\gamma} F_i(\xi_i^*)$. Em particular,

$$p^{-\gamma j} F(\xi) = F_j(\xi_j^*) \equiv 0(\text{mod } p^\gamma),$$

o que é impossível.

Suponha então que a primeira unidade esteja entre os $\eta_1, ..., \eta_{p^r-1}$. De maneira inteiramente análoga obtemos

$$p^{-q\gamma}F(\xi) = \sum_{i=1}^{p^r-1} \eta_i^k + p^{k-\gamma q}G' = 0,$$

e em particular, como $k - \gamma q = r$

$$p^{-q\gamma}F(\xi) = \sum_{i=1}^{p^r-1} \eta_i^k \equiv 0(\text{mod } p^r)$$

o que também é impossível. Daí, segue que, se $p-1$ divide k, então

$$\Gamma^*(k,p) \geq (p^\gamma - 1)q + p^r. \tag{2.6}$$

CAPÍTULO 3

Aplicações do Teorema 2.1

Neste capítulo daremos duas aplicações do Teorema 2.1, que serão apresentadas em duas seções. Mas antes faremos algumas considerações.

Seja $d = \text{mdc}(k, p-1)$. Sabe-se que a congruência $x^d \equiv a(\text{mod } p)$ tem solução se, e somente se, o mesmo ocorre para $x^k \equiv a(\text{mod } p)$. Isto implica que o conjunto das k-ésimas potências e o conjunto das d-ésimas potências em $\mathbb{F}_p$ coincidem. Desde que estamos asumindo que k é um número natural, sem perda de generalidade podemos trocar k por d nas congruências do tipo

$$a_1 x_1^k + \cdots + a_n x_n^k \equiv 0(\text{mod } p),$$

e assim, de agora em diante vamos assumir que $p \equiv 1(\text{mod } k)$.

Seja $\mathbb{F}_p^*$ o grupo dos elementos não nulos de $\mathbb{F}_p$, e seja $\mathbb{K}$ o subgrupo de $\mathbb{F}_p^*$ de todas as k-ésimas potências. Existe um $\delta \in \left(\mathbb{F}_p^* - \mathbb{K}\right)$ tal que

$$\mathbb{F}_p^* = \mathbb{K} \cup \delta\mathbb{K} \cup \delta^2\mathbb{K} \cup \cdots \cup \delta^{k-1}\mathbb{K} \text{ (união disjunta).} \tag{3.1}$$

Vamos denotar por $\mathbb{S}$ o seguinte conjunto de representantes das k classes acima

$$\mathbb{S} = \{1, \delta, ..., \delta^{k-1}\}. \tag{3.2}$$

Segue portanto que qualquer elemento $\alpha \in \mathbb{F}_p^*$ pode ser escrito da forma $\alpha = \delta^i a^k$ para algum $a \in \mathbb{F}_p^*$ e $\delta^i \in \mathbb{S}$.

Definição 3.1 *Definimos $\gamma^*(k,p)$ como sendo o menor inteiro positivo s para o qual a congruência*

$$a_1 x_1^k + \cdots + a_s x_s^k \equiv 0 (\text{mod } p)$$

tem solução primitiva, onde $a_1, ..., a_s$ são inteiros não divisíveis por p.

A seguir apresentamos uma série resultados sobre a função $\gamma^*(k,p)$, que podem ser encontrados em [6], e serão ferramentas importantes nas seções que seguem. Denotaremos por d o $\text{mdc}(k, p-1)$.

Lema 3.0.4 *Se $\frac{1}{2}(p-1)$ é múltiplo de d, então*

$$\gamma^*(d,p) \leq \left\lfloor \frac{\log p}{\log 2} \right\rfloor + 1.$$

Se $d = \frac{1}{2}(p-1)$ vale a igualdade.

Lema 3.0.5 *Temos que $\gamma^*(d,p) \leq d+1$ e $\gamma^*(p-1,p) = p$.*

Lema 3.0.6 *Se d satisfaz $d < \frac{1}{2}(p-1)$, então*

$$\gamma^*(d,p) \leq \left\lfloor \frac{1}{2}(d+4) \right\rfloor.$$

Lema 3.0.7 *Se $p > d^4$, então $\gamma^*(d,p) \leq 3$ e se $p > 2d^2$, então*

$$\gamma^*(d,p) \leq \left\lfloor \frac{2\log 2d}{\log 2} \right\rfloor + 1.$$

Das considerações feitas no início do capítulo, é fácil ver que $\gamma^*(k,p) = \gamma^*(d,p)$, e portanto podemos trocar $\gamma^*(k,d)$ por $\gamma^*(k,p)$ nos lemas acima. O lema a seguir relaciona as funções $\gamma^*(k,p)$ e $\Gamma^*(k,p)$ e também pode ser encontrado em [6].

Lema 3.0.8 *Sejam $\Gamma^*(k,p)$ e $\gamma^*(k,p)$ como nas definições anteriores. Então*

$$\Gamma^*(k,p) \leq k\left(\gamma^*(k,p^\gamma) - 1\right) + 1.$$

3.1 Valor exato de $\Gamma^*(54)$

Nosso objetivo nessa seção é provar o seguinte corolário do Teorema 2.1:

Corolário 3.1 *Seja $\Gamma^*(k)$ como na Definição 0.1. Então $\Gamma^*(54) = 1049$.*

Prova. Vamos utilizar a relação entre as funções $\Gamma^*(k)$ e $\Gamma^*(k,p)$ dada em (4) e investigar os valores de $\Gamma^*(k,p)$ para cada p primo.

Primeiramente considere $p = 2$. Desde que $54 = 3^3 \cdot 2$, temos que que $\gamma = 3$ e do Teorema 2.1 (ou de (2.2), já que nesse caso γ divide 54) segue que $\Gamma^*(54, 2) = 127$.

Agora considere $p = 3$. Então $\gamma = 4$, e desde que 2 divide o grau, estamos nas hipóteses do Teorema 2.1. Escrevendo $54 = 4 \cdot 13 + 2$ segue que $\Gamma^*(54, 3) = (3^4 - 1)13 + 3^2 = 1049$. Assim, é suficiente mostrar que $\Gamma^*(k, p) \leq 1049$ para todos os outros primos.

Devido às considerações no início do capítulo, para os primos p que não dividem 54, podemos assumir $p \equiv 1 (\bmod 54)$ e analisar cada $d = \text{mdc}(54, p-1)$. Note que os divisores de 54 são $2, 3, 6, 9, 18, 27$ e 54. Como p é um primo ímpar, então 2 sempre divide $p - 1$. Assim, se $3 \mid p - 1$, então $6 \mid p - 1$, se $9 \mid p - 1$ então $18 \mid p - 1$ e se $27 \mid p - 1$, então $54 \mid p - 1$. Portanto, $d \in \{2, 6, 18, 54\}$.

Pelo Teorema de Chevalley, se $d = 2, 6$ ou 18 para garantir a solubilidade desejada são suficientes $3, 7$ e 19 variáveis no nível zero. Mas, pelo Lema 1.3.2 isso ocorre desde que o número total de variáveis seja $109, 379$ e 1027, respectivamente. Portanto temos os seguintes valores:

- $\Gamma^*(54, p) \leq 109$, se $\text{mdc}(54, p - 1) = 2$;
- $\Gamma^*(54, p) \leq 379$, se $\text{mdc}(54, p - 1) = 6$;
- $\Gamma^*(54, p) \leq 1027$, se $\text{mdc}(54, p - 1) = 18$.

Vamos agora analisar os primos tais que $\text{mdc}(54, p - 1) = 54$.

Assumindo que o número total de variáveis é 1049, do Lema 1.3.2 temos que existem pelo menos vinte variáveis na subforma do nível zero. Assim, tomando $t = 20$ e $d = 54$ no Lema 1.2.2, a solução primitiva é garantida para todo primo $p > (53)^{38/18}$. Portanto,

para os primos $p > 6215$ temos que

$$\Gamma^*(54, p) \leq 1049.$$

Resta agora analisar o que ocorre com os primos $p < 6215$. Para isso vamos utilizar um resultado devido a Bovey. Esse resultado é essencialmente o Lema 5 de [3], e o detalharemos aqui com o intuito de deixar o trabalho mais autossuficiente.

Lema 3.1.1 *Sejam N um inteiro positivo e f uma função real, positiva, definida sobre os inteiros* (mod N)*, e $c_1, ..., c_s$ inteiros relativamente primos com N. Então,*

$$\sum_{n=1}^{N} f(nc_1) \cdots f(nc_s) \leq \sum_{n=1}^{N} f(n)^s.$$

A demonstração desse lema segue basicamente da desigualdade de Hölder e de indução sobre s.

Suponha que $c_1x_1^k + \cdots + c_sx_s^k \equiv 0 (\text{mod } p)$ tem somente a solução trivial. Então,

$$\sum_{x_1,...,x_s=0}^{p-1} \sum_{t=0}^{p-1} \mathrm{e}_p(c_1x_1^kt) \cdots \mathrm{e}_p(c_sx_s^kt) = p,$$

isto é,

$$\sum_{t=1}^{p-1} S(c_1t) \cdots S(c_st) = p - p^s,$$

onde $\mathrm{e}_p(x) = \exp(2\pi ix/p)$ e $S(b) = \sum\limits_{x=0}^{p-1} \mathrm{e}_p(x^kb)$. Tomando módulo e aplicando o Lema (3.1.1) obtemos:

$$\sum_{t=1}^{p-1} |S(t)|^s \geq (p^s - p).$$

Defina, para $s > 1$ a seguinte função

$$Q(k, p, s) = \sum_{t=1}^{p-1} |S(t)|^s/(p^s - p).$$

Fica portanto provado o seguinte resultado:

Lema 3.1.2 (Bovey) *Se $Q(k, p, s) < 1$, então $\gamma^*(k, p) \leq s$.*

Do Lema acima, com o auxílio do MAPLE, calculamos o valor da função $Q(54, p, 20)$ para os primos $p < 6215$ tais que $\text{mdc}(54, p-1) = 54$ e obtemos

$$Q(54, p, 20) < 1 \quad \forall\ p \neq 109, 163.$$

Os valores de $Q(54, p, 20)$ para cada primo p podem ser encontrados na tabela 4.3 do Apêndice.

Lema 3.1.3 *Se* $d = \frac{1}{2}(p-1)$, *então* $\gamma^*(d,p) = \left\lfloor \frac{\ln p}{\ln 2} \right\rfloor + 1$.

O resultado acima é o Lema 2.2.1 de [6]. Desde que estamos considerando os casos em que $d = 54$, e $54 = (109-1)/2$, segue dos Lemas 3.1.3 e 3.0.8 que $\gamma^*(54, 109) = 7$ e portanto,

$$\Gamma^*(54, 109) \leq 325.$$

Finalmente vamos investigar o valor de $\Gamma^*(54, 163)$. Com auxílio de um computador, é fácil verificar que $x^{54} \equiv 0, 1, 58$ ou $104 (\text{mod } 163)$ e utilizando o MAPLE verificamos que $ax + by + cz \equiv 0 (\text{mod } 163)$ tem sempre solução não trivial, com $x, y, z \in \{1, 58, 104\}$. Além disso, seja $\mathbb{K}$ como nas considerações do início do capítulo, tomando $k = 54$. Desde que $ax^{54} - by^{54} \equiv 0 (\text{mod } 163)$, com a e b não divisíveis por 163 e $a \notin \mathbb{K}$, não tem solução não trivial, segue que $\gamma^*(54, 163) = 3$ e portanto,

$$\Gamma^*(54, 163) = 109,$$

o que completa a prova do corolário.

□

3.2 Um estudo da função $\Gamma^*(k,p)$ com $k = p^3(p-1)$ e $p > 3$

Da seção anterior ficou provado que $\Gamma^*(p^3(p-1), q) \leq \Gamma^*(p^3(p-1), p)$ para todo primo q e $p = 3$. A seguir veremos que, de um modo mais geral, quando $p > 3$ e k pode ser escrito da forma $k = p^3(p-1)$, quase sempre temos $\Gamma^*(k, q) \leq \Gamma^*(k, p)$, onde p e q são primos distintos.

Lema 3.2.1 *Seja $p \geq 5$ um primo tal que $k = p^3(p-1)$, $k \not\equiv 0 (\mod 4)$ e $k+1$ é composto. Se $q \neq p$ é um primo tal que $q \nmid k$, $d = mdc(k, q-1) \leq k/2$ e $d \neq q-1$. Então*

$$\Gamma^*(k,q) \leq \Gamma^*(k,p).$$

Prova. Suponha inicialmente que $d < (q-1)/2$. Do Lema 3.0.6, da hipótese de que $d \leq k/2$ e do Lema 3.0.8, segue que $\gamma^*(k,q) \leq \frac{k}{4} + 2$ e portanto

$$\Gamma^*(k,q) \leq k\left(\frac{k}{4} + 2 - 1\right) + 1 = \frac{k^2}{4} + k + 1.$$

Por outro lado, do Teorema 2.1 temos que

$$\begin{aligned} \Gamma^*(k,p) &= (p^4-1)\left\lfloor \frac{k}{4} \right\rfloor + p^r \\ &= (p^4-1)\left\lfloor \frac{p^3(p-1)}{4} \right\rfloor + p^r \\ &> \frac{p^6(p-1)^2}{4} + p^3(p-1) \end{aligned}$$

pois, para $p \geq 3$ vale

$$\frac{1}{p^6(p-1)}\left\lfloor \frac{p^3(p-1)}{4} \right\rfloor + \frac{p^r}{p^6(p-1)^2} > \frac{1}{4} + \frac{1}{p^3(p-1)}.$$

Suponha agora que $d = \frac{q-1}{2}$. Do Lema 3.0.4 segue que

$$\begin{aligned} \gamma^*(d,q) &= \lfloor \log_2 q \rfloor + 1 \\ &= \lfloor \log_2(2d+1) \rfloor + 1 \\ &< \log_2 d + 2 < \frac{d}{2}, \end{aligned}$$

para $d \geq 11$. Portanto, do Lema 3.0.8

$$\Gamma^*(k,q) \leq k\left(\frac{d}{2} - 1\right) + 1 \leq k\left(\frac{k}{4} - 1\right) + 1 = \frac{k^2}{4} - k + 1 < \Gamma^*(k,p).$$

Finalmente, se $d \leq 10$, desde que $\gamma^*(d,q) \leq d + 1 \leq 11$, segue que

$$\Gamma^*(k,q) \leq 10k + 1 = 10p^3(p-1) + 1 \leq (p^4-1)\left\lfloor \frac{p^3(p-1)}{4} \right\rfloor + p^r = \Gamma^*(k,p).$$

□

O próximo Lema melhora o resultado do Lema 1.2.2 quando k é da forma $k = p^3(p-1)$ com $p > 3$.

Lema 3.2.2 *Nas notações do Lema 3.2.1, sejam q e p primos distintos, $q > 2d^2$. Então*

$$\Gamma^*(k,q) \leq \Gamma^*(k,p).$$

Prova. Suponha inicialmente que $d > 20$. Como

$$\log_2 d + 2 < \frac{d}{4},$$

segue do Lema 3.0.7 que

$$\gamma^*(d,q) \leq \lfloor 2\log_2 2d \rfloor + 1 < \frac{d}{2},$$

e nesse caso já vimos que $\Gamma^*(k,q) \leq \Gamma^*(k,p)$.

Se $d \leq 20$, do Lema 3.0.5 temos $\gamma^*(d,q) \leq d+1 \leq 21$. Assim, pelo Lema 3.0.8 obtemos

$$\Gamma^*(k,q) \leq 20k + 1 \leq (p^4-1)\left\lfloor \frac{p^3(p-1)}{4} \right\rfloor + p^r = \Gamma^*(k,p),$$

para $p \geq 5$.

□

3.3 Um estudo da função $\Gamma^*(24,p)$

Nesta seção estamos interessados em encontrar, para cada p, o número mínimo de variáveis para o qual a equação $F = 0$ tem zeros p-ádicos não triviais, onde

$$F = a_1x_1^{24} + \cdots + a_nx_n^{24}. \tag{3.3}$$

Mais uma vez, isso será feito via Lema 1.3.5, garantindo-se uma solução primitiva para a congruência

$$F = a_1x_1^{24} + \cdots + a_nx_n^{24} \equiv 0 (\text{mod } p^\gamma). \tag{3.4}$$

Em [9], Michael Knapp mostrou que $\Gamma^*(24) = 289$. Por outro lado, vamos mostrar que se $p \neq 13$ é um primo, então $\Gamma^*(24,p) < 289$. Mais precisamente, nosso objetivo aqui é provar o seguinte resultado:

Corolário 3.2 *Seja p um primo, $p \neq 13$. Então $\Gamma^*(24, p) \leq 140$.*

Prova. Os valores exatos de $\Gamma^*(24, p)$ quando p divide o grau, isto é, quando $p = 2$ e $p = 3$, seguem diretamente do Teorema 2.1.

Considere inicialmente $p = 2$. Desde que $k = 24 = 2^3 \cdot 3$, então $\gamma = 5$ e podemos escrever $k = 5 \cdot 4 + 4$ como na notação do Teorema 2.1 onde $r = 4$ e $q = 4$ para obter

$$\Gamma^*(24, 2) = (2^5 - 1) \cdot 4 + 2^4 = 140.$$

Agora considere $p = 3$, e nesse caso temos $\gamma = 2$. Podemos escrever $k = 2 \cdot 12 + 0$ como na notação do Teorema 2.1 onde $q = 12$ e $r = 0$. Segue que

$$\Gamma^*(24, 3) = (3^2 - 1) \cdot 12 + 3^0 = 97.$$

Para os primos que não dividem o grau, como $\gamma = 1$, o Lema 1.3.5 nos garante que é suficiente encontrar soluções primitvas módulo p. Como vimos nas considerações no início desse capítulo, podemos substituir 24 por d na congruência (3.4) com $\gamma = 1$, e de agora em diante vamos assumir que $p \equiv 1 (\text{mod } 24)$. Aqui, $\mathbb{K}$ denota o subgrupo das vigésimas quartas potências de $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Para concluir a demonstração, vamos dividir nas próximas subseções cada um dos casos de d, onde $d \in \{2, 4, 6, 8, 12, 24\}$.

3.3.1 $\mathbf{mdc}(24, p - 1) = 2$

Primeiramente, suponha $d = 2$. Pelo Teorema 1.4, se $v_0 = 3$, então a solubilidade desejada é garantida, e isso decorre do Lema 1.3.2 quando o número n de variáveis em (3.3) é $n = 49$. Disso segue que $\Gamma^*(24, p) \leq 49$. Considere agora a forma aditiva em 48 variáveis

$$F = (ax_0^{24} - by_0^{24}) + p(ax_1^{24} - by_1^{24}) + \cdots + p^{23}(ax_{23}^{24} - by_{23}^{24}),$$

onde $a \cdot b \not\equiv 0 (\text{mod } p)$ e $a \notin \mathbb{K}$. É fácil ver que a equação $F = 0$ não possui zeros p-ádicos não triviais, e portanto $\Gamma^*(24, p) = 49$.

3.3.2 $\mathbf{mdc}(24, p - 1) = 4$

Como estamos no caso em que $d = 4$, as hipóteses do Lema 3.0.6 são satisfeitas e $\gamma^*(4, p) \leq 4$.

Do Lema 1.3.2 temos que, quando o número de variáveis é $n = 49$, então $v_0 \geq 3$. Assim, podemos usar o Lema 1.2.2 com $t = 3$ e $d = 4$, e então a solução desejada é garantida para todo $p > 3^4 = 81$.

Vamos analisar o que ocorre com os primos menores que 81 e $\text{mdc}(24, p-1) = 4$, isto é, os primos no conjunto $\{5, 29, 53\}$.

Suponha $p = 5$. Desde que $p - 1 = 4$ divide 24, podemos utilizar o Teorema 2.1 e obtemos $\Gamma^*(24, 5) = 97$.

Suponha agora que $p = 29$. Neste caso, pelas considerações feitas anteriormente, temos que cada elemento $a \in \mathbb{F}_p^*$ pode ser escrito na forma $a = \delta^i \alpha^{24}$, para algum $\alpha \in \mathbb{F}_p^*$. Portanto, podemos considerar que os coeficientes da forma aditiva variam no conjunto $\mathbb{S}$ dos representantes das 24 classes, como na notação do início do capítulo.

Para $p = 29$ temos $\delta = 2$ e com auxílio do MAPLE verifica-se que

$$x^{24} + y^{24} + z^{24} \equiv 0 (\text{mod } 29)$$

não tem solução não trivial. Portanto,

$$F = \left(x_0^{24} + y_0^{24} + z_0^{24}\right) + 29\left(x_1^{24} + y_1^{24} + z_1^{24}\right) + \cdots + 29^{23}\left(x_{23}^{24} + y_{23}^{24} + z_{23}^{24}\right)$$

é uma forma em 72 variáveis com coeficientes inteiros e não possui zeros $29-$ádicos não triviais, o que implica que $\Gamma^*(24, 29) \geq 73$.

Considere agora a forma (3.3) com $n = 73$. Pelo Lema 1.3.2 temos que $v_0 \geq 4$. Com as considerações acima e com auxílio do MAPLE, verifica-se que

$$a_1 x_1^{24} + a_2 x_2^{24} + a_3 x_3^{24} + a_4 x_4^{24} \equiv 0 (\text{mod } 29)$$

tem solução não trivial, para todo a_1, a_2, a_3, a_4 não divisíveis por 29 e obtemos $\Gamma^*(24, 29) = 73$.

Finalmente, suponha $p = 53$. De maneira inteiramente análoga ao caso anterior, com o auxílio do MAPLE verificamos que

$$ax^{24} + by^{24} + cz^{24} \equiv 0 (\text{mod } 53)$$

tem solução não trivial para todo a, b, c não divisíveis por 53.

Logo, se considerarmos em (3.3) o número n de variáveis igual a 49, do Lema 1.3.2 segue que $v_0 \geq 3$ e portanto $\Gamma^*(24,53) \leq 49$. Desde que $ax^{24} - by^{24} \equiv 0(\text{ mod } 53)$ não tem solução não trivial onde 53 não divide a e b, e $a \notin \mathbb{K}$, segue que

$$F = \left(ax_0^{24} - by_0^{24}\right) + 53\left(ax_1^{24} - by_1^{24}\right) + \cdots + 53^{23}\left(ax_{23}^{24} - by_{23}^{24}\right)$$

é uma forma em 48 variáveis sem zeros 53-ádicos não triviais, daí $\Gamma^*(24,53) \geq 49$. Das duas desigualdades segue que $\Gamma^*(24,53) = 49$.

3.3.3 $\mathbf{mdc}(24, p-1) = 6$

Mais uma vez vamos utilizar o Lema 1.2.2, dessa vez com $d = 6$. Fazendo $t = 3$ temos que a congruência

$$ax^{24} + by^{24} + cz^{24} \equiv 0(\text{mod } p) \tag{3.5}$$

tem solução não trivial para todos a, b, c não divisíveis por p, desde que $p > 5^4 = 625$.

Resta analisar o que ocorre com os primos menores que 625 tais que $\text{mdc}(24, p-1) = 6$. Denotando por $\mathbb{P}$ o conjunto desses primos, segue que

$$\mathbb{P} = \{7, 19, 31, 43, 67, 79, 103, 127, 139, 151, 163, 199, 211, 223, 271, 283, 307, 331, 367, 379, 439,$$
$$463, 487, 499, 523, 547, 571, 607, 619, 631, 643\}$$

Com o auxílio do MAPLE verifica-se que, com exceção dos primos

$$\mathbb{P}' = \{19, 31, 43, 67, 79, 139, 223\},$$

sempre é possível resolver a congruência (3.5) não trivialmente. Se $a \notin \mathbb{K}$ e p não divide b, então $ax^{24} - by^{24} \equiv 0(\text{mod } p)$ não tem solução não trivial e portanto

$$F = \left(ax_0^{24} - by_0^{24}\right) + \cdots + p^{23}\left(ax_{23}^{24} - by_{23}^{24}\right) \tag{3.6}$$

não possui zeros p-ádicos não triviais. Daí,

$$\Gamma^*(24,p) = 49, \quad \text{para todo } p \notin \mathbb{P}'.$$

Para os primos em $\mathbb{P}'$, utilizamos o MAPLE, dessa vez com quatro variáveis no nível zero e, com exceção de $p = 31$, verifica-se que sempre é possível resolver

$$a_1x_1^{24} + a_2x_2^{24} + a_3x_3^{24} + a_4x_4^{24} \equiv 0(\text{mod } p)$$

com os coeficientes a_1, a_2, a_3, a_4 não divisíveis por p. Para $p = 31$ são necessárias cinco variáveis no nível zero, e portanto obtemos a seguinte tabela de valores e contra exemplos. As formas apresentadas na tabela abaixo, assim como nas demais tabelas daqui em diante, representam apenas os coeficientes que aparecem na subforma do nível zero.

Primo p	$\Gamma^*(24,p)$	**Contra exemplo**
19	73	$x_1^{24} + x_2^{24} + 2x_3^{24}$
31	97	$x_1^{24} + x_2^{24} + x_3^{24} + x_4^{24}$
43	73	$x_1^{24} + x_2^{24} + 3x_3^{24}$
67	73	$x_1^{24} + x_2^{24} + x_3^{24}$
79	73	$x_1^{24} + x_2^{24} + x_3^{24}$
139	73	$x_1^{24} + x_2^{24} + x_3^{24}$
223	73	$x_1^{24} + x_2^{24} + x_3^{24}$

Tabela 3.1: Valores de $\Gamma^*(24,p)$ e contra exemplos.

3.3.4 $\mathbf{mdc}(24, p-1) = 8$

Usando o Lema 1.2.2 com $t = 3$ e $d = 8$ segue que a congruência (3.5) tem solução não trivial para todo $p > 7^4 = 2401$. De maneira inteiramente análoga aos casos anteriores, vamos analisar o que acontece com os primos menores que 2401 cujo $\mathrm{mdc}(24, p-1) = 8$. Denotando por $\mathbb{P}$ o conjunto desses primos, temos:

$$\begin{aligned}\mathbb{P} = \{&17, 41, 89, 113, 137, 233, 257, 281, 353, 401, 449, 521, 569, 593, 617, 641, 761, 809, 857,\\ &881, 929, 953, 977, 1049, 1097, 1193, 1217, 1289, 1361, 1409, 1433, 1481, 1553, 1601, 1967,\\ &1721, 1889, 1913, 2081, 2129, 2153, 2273, 2297, 2393\}.\end{aligned}$$

Usando o MAPLE podemos verificar que, com exceção dos primos

$$p \in \mathbb{P}' = \{17, 41, 89, 137, 233, 761\}$$

é possível resolver a congruência (3.5) não trivialmente, e utilizando o contra exemplo (3.6), para $p \notin \mathbb{P}'$ obtemos

$$\Gamma^*(24,p) = 49.$$

Para os primos $p \in \mathbb{P}'$, como na seção anterior utilizamos mais uma vez o MAPLE, dessa vez verificando com quatro variáveis no nível zero, e obtemos os seguintes valores e contra exemplos:

Primo p	$\Gamma^*(24,p)$	**Contra exemplo**
17	97	$x_1^{24} + 9x_2^{24} + 13x_3^{24} + 15x_4^{24}$
41	97	$x_1^{24} + x_2^{24} + x_3^{24} + x_4^{24}$
89	73	$x_1^{24} + x_2^{24} + x_3^{24}$
137	73	$x_1^{24} + x_2^{24} + x_3^{24}$
233	73	$x_1^{24} + x_2^{24} + x_3^{24}$
761	73	$x_1^{24} + x_2^{24} + x_3^{24}$

Tabela 3.2: Valores de $\Gamma^*(24,p)$, com $p \in \mathbb{P}'$ e contra exemplos.

3.3.5 $\mathbf{mdc}(24, p-1) = 12$

Nas notações do Lema 1.2.2 considere $t = 3$ e $d = 12$, e então a solubilidade não trivial de (3.5) é garantida para todo primo $p > 11^4 = 14641$. Usando o contra exemplo (3.6) segue que, para esses primos, $\Gamma^*(24,p) = 49$. Vamos avaliar $\Gamma^*(24,p)$ para os primos menores que 14641 satisfazendo $\text{mdc}(24, p-1) = 12$.

Quando $p = 13$, então $(p-1) \mid 24$ e do Teorema 2.1 segue que $\Gamma^*(24,13) = 289$.

Para todos os outros primos satisfazendo $\text{mdc}(24, p-1) = 12$, temos que $p \geq 37$ e portanto $(p-1) \nmid 24$. Além disso, $d = 12 < \frac{36}{2} < \frac{(p-1)}{2}$ e podemos mais uma vez utilizar o Lema 3.0.6 para nos dar uma cota superior para o número de variáveis no nível zero. Nas notações desse Lema, $\gamma^*(24,p) \leq 8$, e dessa vez a cota superior não se mostrou muito eficiente. Por outro lado, utilizando o Lema 4.2.1 com $t = 4$ e $d = 12$, então temos que $\gamma^*(24,p) \leq 4$, para todo primo $p > 11^3 = 1331$. Com o auxílio do MAPLE, vamos analisar o que ocorre com os primos $13 < p < 1331$ e $1331 < p < 14641$, respectivamente.

- $13 < p < 1331$.

  Vamos denotar por $\mathbb{P}$ o conjunto desses primos. Então

  $$\begin{aligned}\mathbb{P} &= \{37, 61, 109, 157, 181, 229, 277, 349, 373, 397, 421, 541, 613, 661, 709, 733, 757,\\ &\quad 829, 853, 877, 997, 1021, 1069, 1093, 1117, 1213, 1237\}.\end{aligned}$$

  Novamente utilizaremos o fato já descrito anteriormente de que para cada p podemos encontrar uma raiz primitiva δ e então $\mathbb{F}_p^*$ pode ser escrito como a união disjunta de 24 classes laterais

  $$\mathbb{F}_p^* = \mathbb{K} \cup \delta\mathbb{K} \cup \cdots \cup \delta^{23}\mathbb{K}.$$

  Isto nos garante que todo elemento de $\mathbb{F}_p^*$ pode ser escrito da forma $\delta^i\alpha$, para algum $i = 0, ..., 23$ e $\alpha \in \mathbb{K}$, e portanto podemos considerar os coeficientes das formas percorrem o seguinte conjunto de representantes das classes acima $\mathbb{S} = \{1, \delta, ..., \delta^{23}\}$.

  Dessas considerações e com auxílio do MAPLE concluímos que, com exceção dos primos

  $$\mathbb{P}_1^{'} = \{37, 61, 109, 157, 181, 277, 349, 373, 397, 421, 541, 661, 733, 877, 1069\},$$

  tem-se $\Gamma^*(24,p) = 49$. Para os primos $p \in \mathbb{P}_1^{'}$ temos os seguintes valores e respectivos contra exemplos:

Primo p	$\Gamma^*(24,p)$	**Contra exemplo**
37	97	$x_1^{24} + x_2^{24} + 2x_3^{24} + 4x_4^{24}$
61	97	$x_1^{24} + x_2^{24} + x_3^{24} + 4x_4^{24}$
109	73	$x_1^{24} + x_2^{24} + 6x_3^{24}$
157	73	$x_1^{24} + x_2^{24} + x_3^{24}$
181	73	$x_1^{24} + x_2^{24} + x_3^{24}$
229	97	$x_1^{24} + x_2^{24} + x_3^{24} + x_4^{24}$
277	73	$x_1^{24} + x_2^{24} + x_3^{24}$
349	73	$x_1^{24} + x_2^{24} + x_3^{24}$

373	73	$x_1^{24} + x_2^{24} + 32x_3^{24}$
397	73	$x_1^{24} + x_2^{24} + 5x_3^{24}$
421	73	$x_1^{24} + x_2^{24} + x_3^{24}$
541	73	$x_1^{24} + x_2^{24} + 2x_3^{24}$
661	73	$x_1^{24} + x_2^{24} + x_3^{24}$
733	73	$x_1^{24} + x_2^{24} + x_3^{24}$
877	73	$x_1^{24} + x_2^{24} + x_3^{24}$
1069	73	$x_1^{24} + x_2^{24} + x_3^{24}$

Tabela 3.3: Valores de $\Gamma^*(24, p)$ e contra exemplos.

- $1331 < p < 14641$.

Para os primos nesse intervalo, vamos utilizar o resultado do Lema 3.1.2.

Com o auxílio do MAPLE verificamos os valores da função $Q(k, p, s)$. Para $k = 24$, $s = 3$ e $1331 < p < 14641$, com $p \neq 1453, 1669$ e 1741 , verifica-se que $Q(24, p, 3) < 1$. Para cada um dos primos nesse intervalo, os valores de $Q(24, p, 3)$ encontram-se na Tabela 4.4 do Apêndice. Para todos os primos $p \neq 1453, 1669$ e 1741, considerando-se o contra exemplo (3.6), vale que $\Gamma^*(24, p) = 49$.

Para $p = 1453, 1669$ e 1741 verificamos mais uma vez, como o auxílio do MAPLE, o valor da função $Q(24, p, s)$, agora com $s = 4$. A tabela a seguir contém os respectivos valores e contra exemplos.

Primo p	$Q(24, p, 4)$	$\Gamma^*(24, p)$	**Contra exemplo**
1453	0,136	73	$x_1^{24} + x_2^{24} + x_3^{24}$
1669	0,121	73	$x_1^{24} + x_2^{24} + x_3^{24}$
1741	0,159	73	$x_1^{24} + x_2^{24} + x_3^{24}$

Tabela 3.4: Valores $\Gamma^*(24, p)$ e contra exemplos.

3.3.6 $\mathbf{mdc}(24, p-1) = 24$

Vamos proceder de maneira inteiramente análoga à seção anterior para estimar os valores de $\Gamma^*(24,p)$, agora para os primos cujo $\text{mdc}(24, p-1) = 24$. Primeiramente, vamos utilizar o Lema 1.2.2 para estabelecer cotas superiores para o valor de $\gamma^*(24,p)$, e juntamente com o Lema 3.0.8, estimar os valores de $\Gamma^*(24,p)$ para intervalos de primos.

- Inicialmente, considere $s = 3$. Então temos que $\gamma^*(24,p) \leq 3$ para os primos satisfazendo $p > (23)^4 = 279841$. Disso e do contra exemplo (3.6) segue que

$$\Gamma^*(24,p) = 49, \text{ para todo primo } p > 279841.$$

- Tome agora $s = 4$, então $\gamma^*(24,p) \leq 4$ para todo primo $p > (23)^3 = 12167$. Portanto,

$$\Gamma^*(24,p) \leq 73, \text{ para os primos } 12167 < p < 279841.$$

- Para $s = 5$ temos que $\gamma^*(24,p) \leq 5$ para todo primo satisfazendo $p^{3/2} > (23)^4$, e portanto isso é verdade para os primos $p > 4279$. Assim,

$$\Gamma^*(24,p) \leq 97 \text{ para os primos } 4279 < p < 12167.$$

Para os primos $p < 4279$, vamos utilizar mais uma vez o Lema 3.1.2 e calcular o valor de $Q(24,p,5)$. Com o auxílio do MAPLE calculamos $Q(24,p,5)$ para os primos em questão e, com exceção dos primos no conjunto $\mathbb{P} = \{73, 97, 193, 241, 313, 337, 433, 457\}$, obtemos $Q(24,p,5) < 1$ [ver tabela 4.5 do Apêndice]. Assim, se $p \notin \mathbb{P}$ temos que $\gamma^*(24,p) \leq 5$ e portanto, $\Gamma^*(24,p) \leq 97$. Para $p \in \mathbb{P}$ mais uma vez com o auxílio do MAPLE obtemos os seguintes valores e contra exemplos:

Primo p	$\Gamma^*(24,p)$	**Contra exemplo**
73	121	$x_1^{24} + x_2^{24} + 5x_3^{24} + 5x_4^{24} + 10x_5^{24}$
97	97	$x_1^{24} + 5x_2^{24} + 25x_3^{24} + 40x_4^{24}$

193	97	$x_1^{24} + 5x_2^{24} + 153x_3^{24} + 56x_4^{24}$
241	73	$x_1^{24} + 7x_2^{24} + 49x_3^{24}$
313	97	$x_1^{24} + x_2^{24} + x_3^{24} + x_4^{24}$
337	73	$x_1^{24} + 10x_2^{24} + 100x_3^{24}$
433	73	$x_1^{24} + 5x_2^{24} + 25x_3^{24}$
457	73	$x_1^{24} + x_2^{24} + 13x_3^{24}$

Tabela 3.5: Valores de $\Gamma^*(24, p)$ e contra exemplos.

Desse modo, fica provado que, apesar de $\Gamma^*(24) = 289$ (já que $\Gamma^*(24, 13) = 289$), para todos os demais primos vale que $\Gamma^*(24, p) \leq 140$, que era o resultado desejado.

□

CAPÍTULO 4

Valores exatos da função $\Gamma^*(10, p)$

Neste capítulo faremos um estudo detalhado da função $\Gamma^*(k, p)$ no caso em que $k = 10$. Usando as técnicas introduzidas no Capítulo 1 vamos provar o seguinte resultado:

Teorema 4.1 . *Sejam p um primo diferente de 11 e $\mathcal{P}$ o seguinte conjunto de primos:*

$$\mathcal{P} = \{41, 61, 71, 101, 131, 151, 181, 191, 211, 251, 271, 281, 311, 331, 431, 491, 911\}.$$

Então os seguintes valores são obtidos:

1. $\Gamma^*(10, p) = 23$ *e* 41, *se* $p = 2$, *e* 31, *respectivamente;*

2. $\Gamma^*(10, p) = 31$, *se* $p \in \mathcal{P}$;

3. $\Gamma^*(10, p) = 21$, *para* $p = 5$ *e para os primos restantes.*

A demonstração desse teorema será dividida em três casos que serão detalhados nas próximas seções. Em todas elas F é uma forma aditiva do tipo $F = a_1x_1^{10} + \cdots + a_nx_n^{10}$.

4.1 Uma observação sobre o caso $p = 2$

Pela definição 1.5 segue que $\tau = 1$ e $\gamma = 3$. Portanto, nosso objetivo nesta seção é encontrar um número n de variáveis para o qual a congruência

$$a_1x_1^{10} + \cdots + a_nx_n^{10} \equiv 0(mod\ 8)$$

tenha solução primitiva. Segue do Teorema 2.1 que $\Gamma^*(10, 2) = 23$. Entretanto veremos a seguir que, a menos de alguns casos particulares, o número de variáveis necessárias para garantir a solubilidade 2-ádica é menor que 23. Mais precisamente mostraremos que, para quase toda forma aditiva de grau 10, a solubilidade 2-ádica é garantida com apenas 21 variáveis.

Lema 4.1.1 *Seja $F = a_1x_1^{10} + \cdots + a_{21}x_{21}^{10}$ uma forma aditiva equivalente a uma do tipo $F = F_0 + 2F_1 + 2^2F_2 + \cdots + 2^9F_9$. Então F possui zeros 2-ádicos, a menos que tenhamos simultaneamente*

1. *$F_0 = ax_1^{10} + \cdots + ax_7^{10}$, com $a = 1, 3, 5$ ou 7;*

2. *$v_0 + v_1 + v_2 = 7$.*

Prova. Como F é uma forma em 21 variáveis, segue do Lema 1.3.2 que

$$v_0 \geq 3,\ v_0 + v_1 \geq 5 \ \text{ e } \ v_0 + v_1 + v_2 \geq 7. \tag{4.1}$$

Além disso, como $mdc(10, 1) = 1$, do Lema 1.4.1, sempre podemos resolver $ax^{10} + by^{10} \equiv 0(\text{mod } 2)$ com $x \not\equiv 0(\text{mod } 2)$, onde $a \cdot b \not\equiv 0(\text{mod } 2)$. Portanto, podemos iniciar o método de contração agrupando duas a duas as variáveis da subforma F_0 para tentar chegar ao caso solúvel.

Denote por π o número total de variáveis primárias geradas através do processo de contração de variáveis do nível zero, e por π_i a quantidade de variáveis primárias que alcançam o nível $i > 0$. Vamos analisar separadamente os casos em que $v_0 = 3$, $v_0 = 4$, $v_0 = 5$, $v_0 = 6$ e $v_0 = 7$.

Caso 1 - $v_0 = 3$.

Neste caso $\pi = 1$, e de (4.1) temos que $v_1 \geq 2$. Se $v_1 = 2$, então $v_2 \geq 2$ e se $v_1 = 3$, temos $v_2 \geq 1$. Em todo caso temos pelo menos duas variáveis no nível 1 e uma variável no nível 2. Assim, se $\pi_1 = 1$ e $\pi_2 = 0$ ou $\pi_1 = 0$ e $\pi_2 = 1$ a quantidade de variáveis é suficiente para garantir que chegamos ao caso solúvel.

Se $v_1 \geq 4$, então $v_2 \geq 0$. Sem perda de generalidade podemos supor $v_1 = 4$ e $v_2 = 0$. Se $\pi_1 = 1$ e $\pi_2 = 0$, repetimos o processo de contração utilizando a variável primária proveniente do processo de contração das variáveis do nível zero e mais uma das quatro variáveis do nível 1 para gerar uma nova variável primária no nível superior. Se essa nova variável alcançar exatamente o nível 2, utilizamos duas das três variáveis restantes no nível 1 para produzir uma variável secundária no nível 2 e repetir mais uma vez o processo de contração, chegando ao caso solúvel. Se $\pi_1 = 0$ e $\pi_2 = 1$, basta utilizar as variáveis do nível 1 para gerar uma variável secundária no nível 2. Com essa variável e a variável primária podemos repetir o processo de contração chegando ao caso solúvel.

Caso 2 - $v_0 = 4$.

Neste caso $v_1 \geq 1$ e $\pi = 2$. A tabela a seguir mostra o número mínimo de variáveis nos níveis 1 e 2 quando $v_0 = 4$:

v_0	v_1	v_2
4	1	2
4	2	1
4	3	0

Temos três possibilidades para a distribuição das duas variáveis primárias geradas pelo processo de contração: $\pi_1 = 2$ e $\pi_2 = 0$; $\pi_1 = \pi_2 = 1$; e $\pi_1 = 0$ e $\pi_2 = 2$. De acordo com a tabela acima é fácil ver que em todos os casos o número de variáveis nos níveis 1 e 2 é suficiente para chegar ao caso solúvel.

Caso 3 - $v_0 = 5$.

Temos $\pi = 2$ e por (4.1) $v_1 \geq 0$. Se $\pi_2 = 2$ o resultado é imediato. Assim, podemos supor que $\pi_1 \geq 1$. Temos duas possibilidades: $\pi_1 = 1$ e $\pi_2 = 1$ ou $\pi_1 = 2$ e $\pi_2 = 0$.

Como já vimos anteriormente, uma vez iniciado o processo de contração, cada nível i contém as v_i variáveis iniciais, mais as possíveis variáveis primárias resultantes da contração. Suponhamos $\pi_1 = 1$ e $\pi_2 = 1$. A tabela a seguir nos fornece o número mínimo de

variáveis contidas inicialmente em cada um dos níveis, e o número de variáveis já contando as possíveis variáveis primárias.

v_0	v_1	v_2	$v_1 + \pi_1$	$v_2 + \pi_2$
5	0	2	0+1	2+1
5	1	1	1+1	1+1
5	2	0	2+1	0+1

Se $v_2 \geq 1$ o resultado é imediato. Se $v_2 = 0$, a tabela acima nos mostra que temos pelo menos duas variáveis no nível 1, logo é possível agrupar uma variável com a variável primária e repetir o processo de contração gerando uma nova variável primária em um nível superior. Se essa variável sobe exatamente um nível, como $\pi_2 = 1$, podemos repetir mais uma vez o processo de contração e chegamos ao caso solúvel.

Analogamente, no caso em que $\pi_1 = 2$ e $\pi_2 = 0$ temos a seguinte tabela:

v_0	v_1	v_2	$v_1 + \pi_1$	$v_2 + \pi_2$
5	0	2	0+2	2
5	1	1	1+2	1
5	2	0	2+2	0

Como $\pi_2 = 2$, sempre é possível gerar pelo menos uma variável primária em um nível superior. Assim, se $v_2 \geq 1$ o resultado é imediato. Quando $v_2 = 0$ temos $v_1 = 2$, portanto podemos gerar duas variáveis primárias em níveis superiores. Se ambas alcançam exatamente o nível 2, basta repetir o processo de contração e chegamos ao caso solúvel.

Caso 4 - $v_0 = 6$.

Neste caso, agrupando duas a duas as variáveis do nível zero, podemos gerar três variáveis primárias em níveis superiores. Se $\pi_2 \geq 2$ basta realizar a contração utilizando essas variáveis e o resultado segue. Assim, sem perda de generalidade podemos supor $\pi_2 \leq 1$ e portanto temos duas possibilidades para a distribuição das variáveis primárias: $\pi_1 = 2$ e $\pi_2 = 1$ ou $\pi_1 = 3$ e $\pi_2 = 0$.

Primeiramente suponha $\pi_1 = 2$ e $\pi_2 = 1$. Nesse caso, é suficiente considerar somente as variáveis primárias. Como $\pi_1 = 2$, podemos gerar uma variável primária no nível 2

ou acima. Se essa variável alcança exatamente o nível 2, como $\pi_2 = 1$ temos variáveis suficientes para repetir mais uma vez o processo de contração e chegamos ao caso solúvel.

Na tabela a seguir temos o número mínimo de variáveis contidas inicialmente nos níveis 0, 1 e 2, e o número de variáveis nesses níveis com as possíveis variáveis primárias provenientes das contrações das variáveis do nível zero no caso em que $\pi_1 = 3$ e $\pi_2 = 0$.

v_0	v_1	v_2	$v_1 + \pi_1$	$v_2 + \pi_2$
6	0	1	0+3	1
6	1	0	1+3	0

Se $\pi_1 = 3$ e $v_1 = 0$, então produzimos uma variável primária em algum nível superior. Suponhamos que essa variável alcance exatamente o nível 2. Como $v_2 = 1$, podemos repetir o processo de contração e chegamos ao caso solúvel.

Se $v_1 = 1$, como $\pi_1 = 3$, ficamos com quatro variáveis no nível um, das quais três são variáveis primárias. Assim, podemos gerar duas variáveis primárias em níveis superiores. Se alguma delas alcança um nível superior ao nível 2, nada temos a fazer. Se ambas alcançam o nível 2, repetimos o processo de contração e chegamos ao caso solúvel.

Caso 5 - $v_0 = 7$.

Finalmente vamos supor $v_0 = 7$, e mais uma vez temos $\pi = 3$. De (4.1) segue que $v_1 \geq 0$ e $v_2 \geq 0$. Sem perda de generalidade podemos supor $\pi_2 \leq 1$, $v_1 = 0$ e $v_2 = 0$. Esse é exatamente o caso em que temos $v_0 + v_1 + v_2 = 7$.

Se $\pi_2 = 1$ e $\pi_1 = 2$, de maneira análoga ao caso $v_0 = 6$, é suficiente considerar as variáveis primárias para garantir que chegamos ao caso solúvel. Assim, o único problema seria $\pi_1 = 3$ e $\pi_2 = 0$, com $v_1 = v_2 = 0$. Vamos analisar o que acontece nesse caso.

Observe que, como $\varphi(8) = 4$, então $x^{10} \equiv x^2 (\text{mod } 8)$. Disso segue que $x^{10} \equiv 1 (\text{mod } 8)$, para todo x ímpar. Caso contrário, $x^{10} \equiv 0 (\text{mod } 8)$. Vamos separar em casos considerando os coeficientes da subforma F_0.

Caso 5.1 - F_0 possui todos os coeficientes iguais.

É fácil ver que se $F_0' = x_1^{10} + \cdots + x_7^{10}$, então $F_0' \equiv 0 (\text{mod } 8)$ não tem solução não trivial e portanto o mesmo ocorre para $F_0 = a \cdot F_0' \equiv 0 (\text{ mod } 8)$, onde $a = 3, 5$ ou 7. Como os únicos coeficientes que podem aparecer em $F_0 (\text{ mod } 8)$ são $1, 3, 5$ e 7, se a subforma F_0

possui todos os coeficientes iguais, então $F \equiv 0(\text{mod } 8)$ não possui zeros 2-ádicos não triviais.

Caso 5.2 - F_0 possui quatro coeficientes distintos.

Quando F_0 possui exatamente quatro coeficientes distintos, então esses coeficientes são $\{1, 3, 5, 7\}$. Os coeficientes 1 e 7, 3 e 5 estão em classes opostas módulo 8. Portanto é fácil ver que $F_0 \equiv 0(\text{mod } 8)$ tem solução não trivial. Basta fazer as entradas correspondentes aos coeficientes nas classes opostas como sendo 1 e o restante igualamos a zero.

Caso 5.3 - F_0 possui três coeficientes distintos.

Neste caso as únicas possibilidades para os coeficientes distintos são $\{1, 3, 5\}$, $\{1, 3, 7\}$, $\{1, 5, 7\}$ ou $\{3, 5, 7\}$. Note que, em todos os casos, dois dos coeficientes estão em classes opostas módulo 8 e novamente $F_0 \equiv 0(\text{mod } 8)$ tem solução não trivial.

Caso 5.4 - F_0 possui dois coeficientes distintos.

Finalmente, se F_0 possui apenas dois coeficientes distintos e eles estão em classes opostas, a solubilidade não trivial da congruência $F_0 \equiv 0(\text{mod } 8)$ segue de maneira inteiramente análoga aos casos anteriores. Vamos então considerar os casos em que aparecem os seguintes pares de coeficientes: $\{1, 3\}$, $\{1, 5\}$, $\{3, 7\}$ e $\{5, 7\}$. Observe que os pares $\{1, 3\}$ e $\{5, 7\}$ geram variáveis primárias no nível 2, o que nos daria $\pi_2 \geq 1$, e nesse caso já vimos que existe solução. Portanto, basta analisar os casos em que aparecem os pares de coeficientes $\{1, 5\}$ e $\{3, 7\}$:

- Se os coeficientes distintos são 1 e 5, e F_0 possui pelo menos um coeficiente igual a 5 e pelo menos três coeficientes iguais a 1, suponhamos $a_1 = 5, a_2 = a_3 = a_4 = 1$, então $(1, 1, 1, 1, 0, 0, 0)$ é uma solução não trivial. Caso F_0 possua no máximo dois coeficientes iguais a 1, então temos pelo menos cinco coeficientes iguais a 5, e é fácil ver que existe solução não trivial. Basta tomar três entradas x_i com coeficiente cinco e uma entrada x_j com coeficiente um como sendo $x_i = x_j = 1$, e o restante das entradas igualamos a zero.

- Se os coeficientes distintos são 3 e 7, e F_0 possui pelo menos três coeficientes iguais a 3 e um coeficiente igual a 7, basta tomar as entradas correspondentes a esses coeficientes como sendo 1 e o restante igualamos a zero para obter a solução de-

sejada. Mais precisamente, suponhamos que sejam $a_1 = 7$ e $a_2 = a_3 = a_4 = 3$, então $(1, 1, 1, 1, 0, 0, 0)$ é uma solução não trivial. Se F_0 possui, no máximo, dois coeficientes iguais a 3, então F tem pelo menos cinco coeficientes iguais e 7. Logo, basta tomar três das entradas correspondentes aos coeficientes 7 e uma entrada correspondente ao coeficiente 3 como sendo 1 e obtemos a solução desejada.

Portanto, a menos que tenhamos $F_0 = ax_1^{10} + \cdots + ax_7^{10}$, onde $a = 1, 3, 5$ ou 7 e $v_0 + v_1 + v_2 = 7$ simultaneamente, $F_0 \equiv 0 (\text{mod } 8)$ tem solução não trivial, o que pelo Lema 1.3.5 é suficiente para garantir que $F = 0$ tem zeros 2-ádicos.

□

Do Lema anterior fica provado que, apesar de termos $\Gamma^*(10, 2) = 23$, a menos de alguns casos particulares, 21 variáveis são suficientes para garantir a solubilidade 2-ádica não trivial de uma forma aditiva de grau 10.

4.2 Caso $p = 5$

Nesta seção vamos investigar a solubilidade 5-ádica de uma forma aditiva de grau 10. Da Definição 1.5 segue que $\tau = 1$ e portanto $\gamma = 2$. Assim, do Lema 1.3.5 temos que, para garantir que F possui zeros 5-ádicos não triviais, é suficiente provar que

$$F \equiv 0 (\text{mod } 25)$$

tem solução primitiva.

É fácil ver que, se 5 divide x, então $x^{10} \equiv 0 (\text{mod } 5)$. Caso contrário, desde que $\varphi(5) = 4$, então $x^4 \equiv 1 (\text{mod } 5)$. Daí,

$$x^4 \equiv 1 (\text{mod } 5) \Rightarrow x^8 \equiv 1 (\text{mod } 5) \Rightarrow x^{10} \equiv x^2 (\text{mod } 5).$$

Portanto, as décimas potências módulo 5 são os resíduos quadráticos módulo 5, isto é,

$$x^{10} \equiv -1, 0 \text{ ou } 1 (\text{mod } 5).$$

É fácil verificar que esse também é o conjunto das décimas potências módulo 25.

Lema 4.2.1 *A congruência* $F = ax_1^{10} + bx_2^{10} \equiv 0(\text{mod } 5)$ *tem solução não trivial se, e somente se,* $a + b \equiv 0(\text{mod } 5)$ *ou* $a - b \equiv 0(\text{mod } 5)$, *onde* $a \cdot b \not\equiv 0(\text{mod } 5)$.

Prova. De fato, como $x^{10} \equiv -1, 0$ ou $1(\text{mod } 5)$, então $ax_1^{10} + bx_2^{10} \equiv 0(\text{mod } 5) \Leftrightarrow ax_1^{10} \equiv -bx_2^{10}(\text{mod } 5) \Leftrightarrow ax^{10} \equiv 0, b$ ou $-b(\text{mod } 5)$ tem solução.

A solução existe sempre que $a \equiv b(\text{ mod } 5)$ ou $a \equiv -b(\text{ mod } 5)$, a menos que tenhamos a solução trivial $x_1 \equiv x_2 \equiv 0(\text{mod } 5)$.

□

Corolário 4.1 *Considere a forma aditiva*

$$F = (x_1^{10} + 3x_2^{10}) + 5(x_3^{10} + 3x_4^{10}) + \cdots + 5^9(x_{19}^{10} + 3x_{20}^{10}).$$

Então F *não possui zeros* 5*-ádicos não triviais.*

Prova. De fato, como $1 \not\equiv \pm 3(\text{mod } 5)$, então $x_i^{10} + 3x_{i+1}^{10} \equiv 0(\text{mod } 5)$ não tem solução não trivial, para todo $i = 1, ..., 19$. Pelo Lema 1.3.3 isso é suficiente para garantir que $F = 0$ não possui solução 5-ádica não trivial.

□

Dos resultados acima podemos deduzir que $\Gamma^*(10, 5) \geq 21$. O próximo resultado nos fornece uma cota superior.

Lema 4.2.2 *Seja* F *uma forma aditiva de grau* 10 *em* 21 *variáveis com coeficientes inteiros. Então* F *possui zeros* 5*-ádicos não triviais.*

Prova. Pelo Lema 1.3.5 é suficiente provar que $F \equiv 0(\text{mod } 25)$ tem solução primitiva. Como F possui 21 variáveis, do Lema 1.3.2 temos

$$v_0 \geq 3 \text{ e } v_0 + v_1 \geq 5. \tag{4.2}$$

Vamos analisar separadamente os casos em que $v_0 = 3$, $v_0 = 4$ e $v_0 = 5$, e mais uma vez a contração de variáveis será a ferramenta principal da demonstração.

Como mdc(10,4)=2, o Lema 1.4.1 nos garante que três variáveis são suficientes para gerar variáveis primárias. No entanto veremos que, em alguns casos, essa quantidade não é necessária.

Desde que -1 é uma décima potência módulo 25, sem perda de generalidade podemos supor que todos os coeficientes no nível zero são distintos módulo 25.

Caso A - $v_0 = 3$

Nesse caso podemos gerar uma variável primária através da contração das variáveis do nível zero. Se essa nova variável alcançar exatamente o nível seguinte, como por (4.2) temos $v_1 \geq 2$, podemos repetir o processo de contração e chegamos ao caso solúvel.

Caso B - $v_0 = 4$

Novamente, por (4.2) temos $v_1 \geq 1$. Como temos variáveis suficientes no nível zero para produzir uma variável primária, se $v_1 \geq 2$ podemos repetir o processo de contração e chegamos ao caso solúvel. Logo, sem perda de generalidade podemos supor $v_1 = 1$. Vale ressaltar que os coeficientes das variáveis do nível zero são distintos módulo 25, mas não necessariamente distintos módulo 5.

B.1 - Os coeficientes estão em classes distintas módulo 5

Como existem apenas quatro classes não nulas e estamos considerando $v_0 = 4$ então, nesse caso, duas variáveis são suficientes para produzir uma variável primária em algum nível superior. De fato, se a_1 e a_2 são dois coeficientes em classes opostas módulo 5 então $a_1 + a_2 \equiv 0 (\text{mod } 5)$, e portanto a congruência $a_1 x_1^{10} + a_2 x_2^{10} \equiv 0 (\text{mod } 5)$ sempre tem solução não trivial, basta tomar $x_1 = x_2 = 1$. Assim, podemos gerar duas variáveis primárias e, sem perda de generalidade, supor que ambas alcançam o nível 1. Como $v_1 = 1$, pelo Lema 1.4.1, com três variáveis sempre podemos gerar uma nova variável primária, e chegamos ao caso solúvel.

B.2 - Nem todos os coeficientes estão em classes distintas módulo 5.

Na tabela a seguir temos todos os resíduos módulo 25 que são não nulos módulo 5. Cada coluna contém os elementos que estão na mesma classe módulo 5. Note que o elemento a_{ij} que está na linha i e coluna j satisfaz a relação $a_{ij} = j + 5(i - 1)$.

Tabela 4.1: Resíduos módulo 25 coprimos com 5.

	1	**2**	**3**	**4**
1	1	2	3	4
2	6	7	8	9
3	11	12	13	24
4	16	17	18	19
5	21	22	23	24

Existem três possibilidades para a distribuição coeficientes nas classes módulo 5, de modo que em alguma classe tenha sempre pelo menos dois coeficientes:

1. Pelo menos três coeficientes estão numa mesma classe j;
2. Dois coeficientes estão na classe j e dois na classe $i \neq j$;
3. Dois coeficientes estão na classe j, um coeficiente na classe i e o outro na classe k, com $i \neq j \neq k$.

Vamos analisar cada uma das possibilidades acima.

B.2.1 - Pelo menos três coeficientes estão na mesma coluna.

Vamos mostrar que, com três coeficientes em uma mesma coluna j, podemos gerar qualquer classe de resíduo módulo 5 no nível um, isto é, se a_1 é o coeficiente da variável no nível 1, mostraremos que, com três variáveis do nível zero cujos coeficientes estão na mesma classe módulo 5, podemos gerar uma variável primária no nível 1 cujo coeficiente está em uma classe oposta à classe de a_1 módulo 5. Nesse caso, essas duas variáveis são suficientes para repetir o processo de contração e, uma vez que $\gamma = 2$, chegamos ao caso solúvel.

De fato, considere o conjunto de coeficientes $\{a_{ij}, a_{kj}, a_{tj}\}$, onde $i \neq k \neq t$ e defina

$$\begin{aligned} A &= a_{tj} - a_{ij} = 5(t-i), \\ B &= a_{tj} - a_{kj} = 5(t-k), \\ C &= a_{kj} - a_{ij} = 5(k-i). \end{aligned}$$

Como -1 é uma décima potência módulo 25, podemos fazer contrações desse tipo e essas contrações nos permitem gerar variáveis no nível 1 cujos coeficientes são

$$A^{'} = (t-i), B^{'} = (t-k), \text{ e } C^{'} = (k-i).$$

Vamos mostrar que esses coeficientes representam pelo menos duas classes distintas e não opostas módulo 5.

Note que $A^{'} \equiv B^{'}(\text{mod } 5) \Leftrightarrow i \equiv k(\text{mod } 5)$, e $A^{'} \equiv C^{'}(\text{mod } 5) \Leftrightarrow t \equiv k(\text{mod } 5)$, o que é um absurdo. Logo, $A^{'} \not\equiv B^{'}(\text{mod } 5)$ e $A^{'} \not\equiv C^{'}(\text{mod } 5)$. Além disso,

$$\begin{aligned} A^{'} + B^{'} &\equiv 0(\text{mod } 5) \Leftrightarrow t - i \equiv k - t(\text{mod } 5), \\ A^{'} + C^{'} &\equiv 0(\text{mod } 5) \Leftrightarrow t - i \equiv i - k(\text{mod } 5). \end{aligned}$$

Suponha que tenhamos simultaneamente $A^{'} + B^{'} \equiv 0(\text{mod } 5)$ e $A^{'} + C^{'} \equiv 0(\text{mod } 5)$. Então,

$$\begin{aligned} A^{'} + B^{'} \equiv A^{'} + C^{'} \equiv 0(\text{mod } 5) &\Leftrightarrow i - k \equiv k - t(\text{mod } 5) \\ &\Leftrightarrow 2k \equiv t + i(\text{mod } 5). \end{aligned}$$

Desde que $i, t, k \in \{1, 2, 3, 4, 5\}$, onde $i \neq t \neq k$, as únicas soluções para a congruência $2k \equiv t + i(\text{mod } 5)$ seriam

$$(i, t, k) \in \{(1,3,2), (1,5,3), (2,4,3), (3,5,4), (3,1,2), (5,1,3), (4,2,3), (5,3,4)\}.$$

Em todos os casos essas soluções nos dariam, respectivamente

$$\begin{aligned} A^{'} &\equiv \pm 2(\text{mod } 5) \text{ e } B^{'} \equiv C^{'} \equiv \pm 1(\text{mod } 5), \text{ ou} \\ A^{'} &\equiv \pm 4(\text{mod } 5) \text{ e } B^{'} \equiv C^{'} \equiv \pm 2(\text{mod } 5) \end{aligned}$$

o que contradiz o fato de que $A^{'} + B^{'} \equiv A^{'} + C^{'} \equiv 0(\text{mod } 5)$.

Portanto, se $A' + B' \equiv 0(\text{mod } 5)$, então $A' + C' \not\equiv 0(\text{mod } 5)$ e isso é suficiente para garantirmos que podemos representar todas as classes não nulas módulo 5 no nível um.

De fato, se $A' + B' \not\equiv 0(\text{mod } 5)$, como $A' \not\equiv B'(\text{mod } 5)$ então podemos representar quatro classes distintas módulo 5, a saber, $\{A', B', -A', -B'\}$.

Caso contrário, se $A' + B' \equiv 0(\text{mod } 5)$, então $A' + C' \not\equiv 0(\text{mod } 5)$. Desde que $A' \not\equiv C'(\text{mod } 5)$, podemos representar as quatro classes distintas $\{A', C', -A', -C'\}$.

B.2.2 - Dois coeficientes em uma coluna j e os outros dois em uma coluna $i \neq j$.

Observando a tabela (2.1) é fácil ver que se os coeficientes estão dois a dois na mesma coluna, duas variáveis são suficientes para gerar uma variável primária no nível um, já que se a e b são coeficientes em uma mesma coluna, então $a - b \equiv 0(\text{mod } 5)$. Portanto, com as variáveis do nível zero podemos gerar duas variáveis primárias. Se essas variáveis vão para o nível 1, como $v_1 = 1$, repetimos mais uma vez o processo de contração e chegamos ao caso solúvel.

B.2.3 - Dois coeficientes em uma coluna j, um coeficiente em uma coluna i e outro na coluna k, com $j \neq i \neq k$.

Nesse caso, temos três colunas que contêm os coeficientes. Como existem apenas quatro classes não nulas módulo 5, então duas colunas estão em classes opostas. Já vimos que, com duas variáveis na mesma coluna, podemos gerar uma variável primária no nível um. Vimos também que, se as colunas i e k representam classes opostas módulo 5, então duas variáveis são suficientes para gerar uma variável primária no nível um. Supondo que essas variáveis alcançam exatamente o nível 1, desde que $v_1 = 1$, com essas três variáveis podemos repetir mais uma vez o processo de contração e chegamos ao caso solúvel.

Suponha agora que $i + k \neq 5$, isto é, que i e k não representam classes opostas módulo 5. Então $i + j = 5$ ou $k + j = 5$. Sem perda de generalidade, podemos supor que $i + j = 5$.

Considere os seguintes coeficientes: a_{kj}, a_{nj} e a_{ri}, onde $n \neq k$. De maneira interiamente análoga ao que fizemos no caso B.2.1, vamos mostrar que com esses três coeficientes

podemos representar qualquer classe módulo 5 no nível um. De fato, defina

$$\begin{aligned} A &= a_{kj} - a_{nj} = 5(k-n) \\ B &= a_{kj} + a_{ri} = 5(k+r-1) \\ C &= a_{nj} + a_{ri} = 5(n+r-1). \end{aligned}$$

Então podemos gerar, no nível um, os seguintes coeficientes

$$A^{'} = k - n, B^{'} = k + r - 1 \text{ e } C^{'} = n + r - 1.$$

Note que $B^{'} \equiv C^{'}(\text{mod } 5) \Leftrightarrow k \equiv n(\text{mod } 5),$ o que é um absurdo. Além disso,

$$A^{'} \equiv B^{'} \Leftrightarrow n + r - 1 \equiv 0(\text{mod } 5) \Leftrightarrow C \equiv 0(\text{mod } 25)$$

e nesse caso já teríamos uma solução primitiva módulo 25. Portanto, sem perda de generalidade podemos supor que

$$A^{'} \not\equiv B^{'}(\text{mod } 5) \text{ e } B^{'} \not\equiv C^{'}(\text{mod } 5).$$

Note também que $A^{'} + B^{'} \equiv 0(\text{mod } 5) \Leftrightarrow n \equiv 2k + r - 1(\text{mod } 5)$. Se além disso tivermos $A^{'} \equiv C^{'}(\text{mod } 5)$, desde que

$$A^{'} \equiv C^{'}(\text{mod } 5) \Leftrightarrow k \equiv 2n + r - 1(\text{mod } 5)$$

e $n \equiv 2k + r - 1(\text{mod } 5)$, segue que $n \equiv 2(2n + r - 1) + r - 1(\text{mod } 5)$, e isso ocorre se, e somente se, $n + r - 1 \equiv 0(\text{mod } 5)$, o que equivale a dizer que $C \equiv 0(\text{mod } 25)$ e novamente já teríamos uma solução primitiva módulo 25. Podemos então, sem perda de generalidade, assumir que se $A^{'} + B^{'} \equiv 0(\text{mod } 5)$, então $A^{'} \not\equiv C^{'}(\text{mod } 5)$.

Veja que isso é suficiente para garantir que conseguimos representar todas as classes não nulas módulo 5 no nível um.

De fato, se $A^{'} + B^{'} \not\equiv 0(\text{mod } 5)$, como $A^{'} \not\equiv B'(\text{mod } 5)$, então podemos representar quatro classes distinas, a saber $\{A^{'}, B^{'}, -A^{'}, -B^{'}\}$.

Se $A^{'} + B^{'} \equiv 0(\text{ mod } 5)$, então $A^{'} \not\equiv C^{'}(\text{ mod } 5)$ e $A^{'} + C^{'} \not\equiv 0(\text{ mod } 5)$, ou do contrário teríamos $B^{'} \equiv C^{'}(\text{mod } 5)$, o que é um absurdo. Portanto, nesse caso também podemos representar quatro classes distintas, $\{A^{'}, C^{'}, -A^{'}, -C^{'}\}$, e com isso fechamos o caso em que $v_0 = 4$.

Caso C - $v_0 \geq 5$

Nesse caso, de (4.2) temos que $v_1 \geq 0$. Sem perda de generalidade podemos supor $v_1 = 0$. O resultado a seguir é uma consequência do Lema 3.2.1 de [6] e pode ser encontrado em [9].

Lema 4.2.3 *Considere a congruência*

$$a_1 x_1^k + \cdots + a_t x_t^k \equiv 0 (\text{mod } p^\gamma).$$

Se -1 *é uma* k*-ésima potência módulo* p^γ *e* p *não divide nenhum dos coeficientes* a_i*, então a congruência acima tem solução primitiva sempre que* $2^t > p^\gamma$.

No nosso caso temos $k = 10$, $\gamma = 2$ e $p = 5$. Além disso, como $v_0 = 5$ e $v_1 = 0$, então $t = 5$ e nenhum dos coeficientes $a_1, ..., a_5$ é divisível por 5. Como -1 é uma décima potência módulo 25, todas as hipóteses do lema acima são satisfeitas, o que nos garante a solubilidade desejada, já que $2^{v_0+v_1} \geq 2^5 > 5^2$.

4.3 Primos que não dividem o grau

Considere agora os primos que não dividem o grau. Nesse caso $\gamma = 1$ e portanto é suficiente encontrar soluções primitivas para a congruência

$$F = a_1 x_{10} + \cdots + a_n x_n^{10} \equiv 0 (\text{mod} p), \tag{4.3}$$

onde $p \neq 2, 5,$ e 11.

Como já mencionamos anteriormente, se $d = \text{mdc}(10, p-1)$, então a congruência $x^d \equiv a (\text{mod } p)$ tem solução se, e somente se, o mesmo ocorre para $x^{10} \equiv a (\text{mod } p)$, o que significa que o conjunto das d-ésimas potências e o conjunto das décimas potências de $\mathbb{F}_p$ é o mesmo. Portanto, sem perda de generalidade, vamos substituir 10 por d na congruência (4.3), e de agora em diante vamos assumir que $p \equiv 1 (\text{mod } 10)$.

Observe que, como $p - 1$ é par, se $5 \mid (p-1)$, então $\text{mdc}(10, p-1) = 10$. Assim, os únicos valores possíveis para d são 2 ou 10.

Primeiramente, suponha que $d = 2$. Se $n = 21$, pelo Lema 1.3.2 temos que $v_0 \geq 3$, e pelo Teorema 1.4 a congruência (4.3) tem solução primitiva. Isso nos garante que $\Gamma^*(10, p) \leq 21$. Por outro lado, como $f_i = ax_i^{10} - by_i^{10} \equiv 0 (\text{mod } p)$ não tem solução não trivial sempre que $a \notin \mathbb{K}$, onde $\mathbb{K}$ denota o subgrupo das décimas potências de $\mathbb{F}_p^*$, então

$$F = f_0 + pf_1 + \cdots + p^9 f_9 \tag{4.4}$$

é uma forma aditiva com coeficientes inteiros em 20 variáveis sem zeros p-ádicos não triviais. Segue que $\Gamma^*(10, p) = 21$ para os primos p que satisfazem $\text{mdc}(10, p-1) = 2$.

Suponha de agora que $d = 10$. Seja N o número de soluções da congruência

$$a_1 x_1^k + \cdots + a_t x_t^k \equiv 0 (\text{mod } p),$$

onde $\text{mdc}(a_i, p) = 1$ para $i = 1, ..., t$.

Dos resultados da seção 1.2 sabe-se que

$$N \geq p^{t-1} - (k-1)^{t-1} p^{t/2-1}(p-1),$$

e a congruência acima tem solução não trivial desde que

$$p^{\frac{t}{2}-1} > (k-1)^{t-1}.$$

Fazendo $k = 10$ e $t = v_0 = 3$ segue que, se $n = 21$, então a congruência (4.3) tem solução não trivial para todo primo $p > 81^2$, e novamente usando (4.4) temos $\Gamma^*(10, p) = 21$.

Resta agora analisar o que ocorre com os primos menores que 81^2. Como já vimos, existe $\delta \in (\mathbb{F}_p^* - \mathbb{K})$ tal que

$$\mathbb{F}_p^* = \mathbb{K} \cup \delta\mathbb{K} \cup \cdots \cup \delta^9\mathbb{K} \quad \text{(união disjunta)}.$$

Denote por $\mathbb{S}$ o seguinte conjunto de representantes das 10 classes anteriores:

$$\mathbb{S} = \{1, \delta, \delta^2, \ldots, \delta^9\}. \tag{4.5}$$

Segue dessas considerações que para cada $p \equiv 1 (\text{mod } 10)$ podemos determinar uma raiz primitiva δ de $\mathbb{F}_p^*$ e através da mudança de variáveis $x_i^{10} \leftrightarrow \alpha_i^{10} x_i^{10}$ considerar que os coeficientes a_i da forma F na congruência (4.3) são elementos de $\mathbb{S}$.

Feito isso, com auxílio do MAPLE, obtemos os valores exatos de $\Gamma^*(10,p)$ para os primos menores que 81^2 com $\text{mdc}(10,p-1)=10$. Verifica-se que nesse caso, $\Gamma^*(10,p)\leq 21$, exceto para o seguinte conjunto de primos

$$\mathbb{P}=\{31,42,61,71,101,131,151,181,191,211,251,271,281,311,331,431,491,911\}.$$

Para $p\in\mathbb{P}$, com $p\neq 31$ temos que $\Gamma^*(10,p)=31$, e $\Gamma^*(10,31)=41$.

A tabela 4.2 contém os valores de $\Gamma^*(10,p)$ para $p\in\mathbb{P}$ e os respectivos contra exemplos. Para os primos que não estão na tabela abaixo, podemos utilizar mais uma vez o contra exemplo dado por (4.4) para afirmar que $\Gamma^*(10,p)=21$. Na tabela, f representa a subforma que aparece no nível zero, isto é, o contra exemplo propriamente dito é a forma dada por

$$f_0+pf_1+\cdots+p^9f_9.$$

Primo p	$\Gamma^*(10,p)$	**Contra exemplo**
31	41	$f_i=x_{i1}^{10}+19x_{i2}^{10}+17x_{i3}^{10}+17x_{i4}^{10}$
41	31	$f_i=x_{i1}^{10}+6x_{i2}^{10}+6x_{i3}^{10}$
61	31	$f_i=x_{i1}^{10}+6x_{i2}^{10}+12x_{i3}^{10}$
71	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+x_{i3}^{10}$
101	31	$f_i=x_{i1}^{10}+27x_{i2}^{10}+7x_{i3}^{10}$
131	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+x_{i3}^{10}$
151	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+6x_{i3}^{10}$
181	31	$f_i=x_{i1}^{10}+2x_{i2}^{10}+32x_{i3}^{10}$
191	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+174x_{i3}^{10}$
211	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+2x_{i3}^{10}$
251	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+41x_{i3}^{10}$
271	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+264x_{i3}^{10}$
281	31	$f_i=x_{i1}^{10}+9x_{i2}^{10}+13x_{i3}^{10}$
311	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+x_{i3}^{10}$
331	31	$f_i=x_{i1}^{10}+x_{i2}^{10}+9x_{i3}^{10}$

431	31	$f_i = x_{i1}^{10} + x_{i2}^{10} + x_{i3}^{10}$
491	31	$f_i = x_{i1}^{10} + x_{i2}^{10} + x_{i3}^{10}$
911	31	$f_i = x_{i1}^{10} + x_{i2}^{10} + x_{i3}^{10}$

Tabela 4.3: Valores da função $\Gamma^*(10, p)$ para $p \in \mathbb{P}$.

Apêndice

Tabelas de valores da função $Q(k, p, s)$

- Valores de $Q(54, p, 20)$ para os primos $p < 6215$ com $p \equiv 1 (\text{mod } 54)$.

Primo p	109	163	271	379	433
$Q(54, p, 20)$	15,246914	4,839553	0,210817	0,013238	0,163891
Primo p	487	541	757	811	919
$Q(54, p, 20)$	0,000753	0,024424	0,000560	$1,70 \cdot 10^{-5}$	$6,52 \cdot 10^{-5}$
Primo p	1297	1459	1567	1621	1783
$Q(54, p, 20)$	$2,17 \cdot 10^{-5}$	$1,03 \cdot 10^{-8}$	$2,08 \cdot 10^{-7}$	$3,40 \cdot 10^{-6}$	$9,83 \cdot 10^{-10}$
Primo p	1999	2053	2161	2269	2377
$Q(54, p, 20)$	$1,14 \cdot 10^{-8}$	$2,36 \cdot 10^{-6}$	$2,01 \cdot 10^{-5}$	$3,17 \cdot 10^{-3}$	$1,57 \cdot 10^{-8}$
Primo p	2539	2593	2647	2917	2971
$Q(54, p, 20)$	$9,60 \cdot 10^{-10}$	$2,19 \cdot 10^{-8}$	$1,30 \cdot 10^{-10}$	$1,54 \cdot 10^{-8}$	$7,49 \cdot 10^{-10}$
Primo p	3079	3187	3457	3511	3673
$Q(54, p, 20)$	$1,81 \cdot 10^{-9}$	$8,98 \cdot 10^{-10}$	$7,30 \cdot 10^{-9}$	$6,11 \cdot 10^{-12}$	$6,09 \cdot 10^{-9}$

Primo p	3727	3889	3943	4051	4159
$Q(54, p, 20)$	$3,83 \cdot 10^{-11}$	$3,74 \cdot 10^{-11}$	$3,58 \cdot 10^{-10}$	$3,86 \cdot 10^{-11}$	$1,35 \cdot 10^{-11}$
Primo p	4483	4591	4861	4969	5023
$Q(54, p, 20)$	$5,10 \cdot 10^{-12}$	$7,22 \cdot 10^{-13}$	$7,82 \cdot 10^{-12}$	$2,56 \cdot 10^{-11}$	$8,99 \cdot 10^{-12}$
Primo p	5077	5347	5563	5779	6211
$Q(54, p, 20)$	$4,77 \cdot 10^{-10}$	$1,01 \cdot 10^{-13}$	$2,45 \cdot 10^{-13}$	$7,08 \cdot 10^{-12}$	$5,71 \cdot 10^{-14}$

Tabela 4.4: Valores da função $Q(54, p, 20)$.

- Valores de $Q(24, p, 3)$ para os primos $1331 < p < 14641$ tais que $\text{mdc}(24, p-1) = 12$.

Primo p	1381	1429	1453	1549	1597	1621
$Q(54, p, 20)$	1,168704	1,079652	1,189131	1,278479	1,353699	1,001930
Primo p	1669	1693	1741	1789	1861	1933
$Q(54, p, 20)$	1,134802	1,361682	1,236107	1,393699	1,223988	1,025771
Primo p	2029	2053	2221	2269	2293	2341
$Q(54, p, 20)$	0,908686	0,936806	0,870568	1,132039	0,878164	1,156145
Primo p	2389	2437	2557	2677	2749	2797
$Q(54, p, 20)$	0,874374	0,912778	0,906612	0,823078	1,134643	0,834566
Primo p	2917	3037	3061	3109	3181	3229
$Q(54, p, 20)$	0,855282	0,819732	1,185364	0,777529	0,727160	0,897403
Primo p	3253	3301	3373	3469	3517	3541
$Q(54, p, 20)$	0,721154	0,712027	1,005670	0,704565	0,880999	0,709586
Primo p	3613	3637	3709	3733	3853	3877
$Q(54, p, 20)$	0,881751	0,659784	0,806446	0,745588	0,763950	0,790618
Primo p	4021	4093	4261	4357	4549	4597
$Q(54, p, 20)$	0,704596	0,625141	0,892970	0,616605	0,746403	0,727035

Primo p	4621	4789	4813	4861	4909	4933
$Q(54, p, 20)$	0,758888	0,761537	0,756351	0,593607	0,614458	0,609454
Primo p	4957	5077	5101	5197	5413	5437
$Q(54, p, 20)$	0,588418	0,777498	0,577099	0,881455	0,630921	0,679860
Primo p	5557	5581	5653	5701	5749	5821
$Q(54, p, 20)$	0,540145	0,574757	0,659833	0,515653	0,574889	0,614798
Primo p	5869	6037	6133	6229	6277	6301
$Q(54, p, 20)$	0,599331	0,868885	0,686615	0,694991	0,552033	0,532641
Primo p	6373	6397	6421	6469	6637	6661
$Q(54, p, 20)$	0,565258	0,596767	0,681156	0,541468	0,524802	0,587919
Primo p	6709	6733	6781	6829	6949	6997
$Q(54, p, 20)$	0,488161	0,542410	0,50057	0,568212	0,498797	0,730042
Primo p	7069	7213	7237	7309	7333	7477
$Q(54, p, 20)$	0,518066	0,578421	0,536701	0,527514	0,631498	0,506334
Primo p	7549	7573	7621	7669	7717	7741
$Q(54, p, 20)$	0,578684	0,482922	0,444008	0,432922	0,452310	0,541524
Primo p	7789	7933	8053	8101	8221	8269
$Q(54, p, 20)$	0,484530	0,528887	0,426600	0,472238	0,470741	0,460259
Primo p	8293	8317	8389	8461	8581	8629
$Q(54, p, 20)$	0,537487	0,778157	0,592613	0,490062	0,529233	0,496030
Primo p	8677	8821	8893	8941	9013	9109
$Q(54, p, 20)$	0,475819	0,465658	0,716265	0,554894	0,443537	0,604699
Primo p	9133	9157	9181	9277	9349	9397
$Q(54, p, 20)$	0,450661	0,442645	0,575023	0,463569	0,493958	0,446124
Primo p	9421	9613	9661	9733	9781	9829
$Q(54, p, 20)$	0,477373	0,451009	0,459485	0,433517	0,522802	0,453618

Primo p	9901	9949	9973	10069	10093	10141
$Q(54, p, 20)$	0,376236	0,485263	0,430868	0,431411	0,395413	0,419938
Primo p	10333	10357	10429	10453	10477	10501
$Q(54, p, 20)$	0,551747	0,424119	0,535587	0,426764	0,440688	0,466952
Primo p	10597	10789	10837	10861	10909	10957
$Q(54, p, 20)$	0,612942	0,410819	0,511198	0,425831	0,457851	0,446067
Primo p	11149	11173	11197	11317	11437	11677
$Q(54, p, 20)$	0,439635	0,458912	0,522949	0,364925	0,401430	0,385263
Primo p	11701	11821	11941	12037	12109	12157
$Q(54, p, 20)$	0,376299	0,420910	0,478454	0,382098	0,383891	0,36501
Primo p	12253	12277	12301	12373	12421	12517
$Q(54, p, 20)$	0,436246	0,488480	0,390761	0,493637	0,465395	0,389229
Primo p	12541	12589	12613	12637	12757	12781
$Q(54, p, 20)$	0,366963	4,0,420895	0,395920	0,485542	0,401577	0,605134
Primo p	12829	12853	12973	13093	13309	13381
$Q(54, p, 20)$	0,349506	0,400369	0,425450	0,525312	0,455705	0,386230
Primo p	13477	13597	13669	13693	13789	13933
$Q(54, p, 20)$	0,390672	0,378344	0,493235	0,393135	0,372313	0,3774109
Primo p	14029	14149	14173	14197	14221	14293
$Q(54, p, 20)$	0,452746	0,361351	0,345112	0,416700	0,352063	0,384585
Primo p	14341	14389	14437	14461	14533	14557
$Q(54, p, 20)$	0,423550	0,361028	0,384178	0,381699	0,434259	0,349571
Primo p	14629					
$Q(54, p, 20)$	0,408768					

Tabela 4.5: Valores da função $Q(24, p, 3)$.

- Valores de $Q(24, p, 5)$ para os primos $p < 4279$ com $\text{mdc}(24, p-1) = 24$.

Primo p	73	97	193	241	313	337
$Q(54, p, 20)$	9,311379	9,635629	4,137281	2,926953	1,607933	1,685126
Primo p	409	433	457	577	601	673
$Q(54, p, 20)$	0,846525	1,038054	1,465216	0,880781	0,287312	0,595368
Primo p	769	937	1009	1033	1129	1153
$Q(54, p, 20)$	0,289392	0,214829	0,437653	0,211357	0,157440	0,363106
Primo p	1201	1249	1297	1321	1489	1609
$Q(54, p, 20)$	0,330636	0,374836	0,323911	0,148426	0,272803	0,106982
Primo p	1657	1753	1777	1801	1873	1993
$Q(54, p, 20)$	0,094653	0,070370	0,119343	0,096470	0,117971	0,064525
Primo p	2017	2089	2113	2137	2161	2281
$Q(54, p, 20)$	0,141232	0,061149	0,173414	0,091854	0,150028	0,087963
Primo p	2377	2473	2521	2593	26617	2689
$Q(54, p, 20)$	0,114354	0,040805	0,063243	0,076074	0,0485361	0,076641
Primo p	2713	2833	2857	2953	3001	3049
$Q(54, p, 20)$	0,059636	0,083748	0,035718	0,064884	0,051677	0,064697
Primo p	3121	3169	3217	3313	3361	3433
$Q(54, p, 20)$	0,143931	0,083652	0,081932	0,100121	0,126128	0,033945
Primo p	3457	3529	3673	3697	3769	3793
$Q(54, p, 20)$	0,083957	0,033945	0,040457	0,047168	0,044149	0,068628
Primo p	3889	4057	4129	4153	4177	4201
$Q(54, p, 20)$	0,143931	0,083652	0,081932	0,100121	0,126128	0,033945
Primo p	4273					
$Q(54, p, 20)$	0,041331					

Tabela 4.6: Valores da função $Q(24, p, 5)$.

Rotina 1

Para calcular os valores da função $Q(k, p, s)$ do Lema 3.1.2, utilizamos a seguinte rotina no MAPLE, que será dividida em três partes detalhadas a seguir. Primeiramente declaramos a função $S(b)$ da Seção 3.1 como 'bigess'.

```
maple> bigess:= proc(k,p,t)
S:=0;
for x from 0 to p-1 do
S:= S+evalf(exp(2*Pi*sqrt(-1)*x^d*t/p));
end do;
S;
end proc
bigess:=proc(k,p,t)
local S,x:
S:=0;
for x from 0 to p-1 do
S:=S+evalf(exp(2*Pi*sqrt(-1)*x^d*t/p))
end do;
S
end proc
```

Em seguida declaramos a função $Q(k, p, s)$ do Lema 3.1.2 como 'bigq':

```
maple>bigq:=proc(k,p,s)
Q:=0;
for t from 1 to p-1 do
Q:=Q+abs(bigess(k,p,t))^s;
```

```
end do;
Q:=Q/(p^s-p);
end proc
bigq:=proc(k,p,s)
local Q,t;
Q:=0;
for t to p-1 do
Q:=Q+abs(bigess(k,p,t))^s
end do;
Q:=Q/(p^s-p)
end proc
```

Por último encontramos os valores de $Q(k,p,s)$ fixando-se $k=k_0$ e $s=s_0$ para os casos específicos, deixando apenas que o primo p percorra um intervalo conveniente de primos satisfazendo $p \equiv 1(\bmod\ k)$, e daí $Q(k_0,p,s_0)=Q(p)$. Em particular, na Tabela 4.3 foram obtidos os valores da função quando $k=54$ e $s=20$ com p um primo satisfazendo $p \equiv 1(\bmod\ 54)$ e $p<6215$. Nesse caso a rotina fica:

```
maple> for p from 55 by 54 to 6215 do
if isprime(p)=true then
m:=bigq(54,p,20);
print("p=",p,"Q(54,p,20)=",m);
end if;
end do
```

Ao final, o programa retorna para cada valor de p o respectivo $Q(54,p,20)=m$.

Rotina 2

A seguir detalharemos a rotina utilizada para verificar se uma forma aditiva

$$a_1x_1^k+\cdots+a_nx_n^k \equiv 0(\bmod\ p) \tag{4.6}$$

tem solução não trivial ou gerar os contra-exemplos (mod p). A estratégia é utilizar as considerações feitas no início do Capítulo 3, onde vimos que para cada p primo podemos encontrar uma raiz primitiva δ de modo que todo elemento de $\mathbb{F}_p^*$ pode ser escrito na forma $\alpha = \delta^i a^k$ para algum $a \in \mathbb{F}_p^*$ e $i \in \{0, 1, ..., k-1\}$. Assim, podemos considerar que os coeficientes das formas aditivas percorrem o conjunto $S = \{1, \delta, ..., \delta^{k-1}\}$. Mais ainda, como estamos resolvendo congruências módulo p, podemos sempre considerar que $a_1 = 1$.

Primeiramente carregamos o pacote de teoria dos números e, em seguida, definimos um conjunto P como uma sequência de primos satisfazendo $p \equiv 1(\text{mod } k)$. Para os primos nesse conjunto encontramos a raiz primitiva δ, consideramos $a_1 = 1$ e os demais coeficientes no conjunto S. Ao final, o programa nos retorna "FIM, p" se a congruência (4.6) tem solução não trivial módulo p, para todos os coeficientes $1, a_2, ..., a_n$. Se existem coeficientes para os quais a congruência (4.6) não tem solução não trivial, o programa nos retorna a frase "não tem solução não trivial" e em seguida os coeficientes $[1, a_2, ..., a_n]$ para os quais isso acontece, gerando os contra exemplos.

A rotina a seguir verifica a solubilidade não trivial da forma (4.6) com $k = 10$ e $n = 3$ para os primos $41, ..., 541$ com $p \equiv 1(\text{mod } 10)$:

```
maple> with(numtheory);
maple> Primos := {seq(ithprime(n), n = 12 ..100 )};
 P := {};
for q in Primos do
if q-1 mod 10 = 0 then
P := P union{q}:
fi: od:
P := P;
for p in P do
t := primroot(p);
K := {seq(x^10 mod p, x = 0 .. p-1))};
T := {seq(t^m mod p, m = 0 .. 9)};
for i from 0 to 9 do
for k from i to 9 do
```

```
N[i, k] := 0:
for x in K do
for y in K do
for z in K do
if 0 = x+t^i*y+t^k*z mod p then
N[i, k] := N[i, k]+1;
fi: od: od: od:
if N[i, k] = 1 then print("nao tem solucao nao-trivial"):
print([1, t^i mod p, t^k mod p]);
fi: od: od:
print("FIM", p);
od:
```

Referências

[1] Bierstedt, R.G. *Some problems on the distribution of kth power residues modulo a prime*, PhD thesis, University of Colorado, 1963.

[2] Borevich, Z. I. and Shafarevich, I. R. *Number Theory*, Academic Press Inc. (1973).

[3] Bovey, J. D. $\Gamma^*(8)$, Acta Arith. 25 (1974), 145-150.

[4] Chowla, S. *On conjecture of J.F. Gray,* Norske Vid. Selk. Forh. Trondheim 33 (1960), 58-59.

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

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

[7] Godinho, H. *Polinômios Homogêneos sobre Números p-ádicos*. MAT-UL-2000- 01. Universidade de Lisboa, (1999).

[8] Gray, J.F. *Diagonal forms of prime degree*, PhD thesis, University of Notre Dame, 1958.

[9] Knapp, M.P. *Exact values of the function* $\Gamma^*(k)$, J. Number Theory 131 (2011), 1901-1911.

[10] Knapp, M.P. 2-*Adic zeros of diagonal forms and distance pebbling of graphs*, preprint (2012).

[11] Lang, S. *Abelian Varieties*, Wiley (Interscience), 1959.

[12] Lang, S. e Weil, A. *Number of points of varieties in finite fields*, Amer. J. Math. 76 (1954), 819-827.

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

[14] Norton, K.K. *On homogeneous diagonal congruences of odd degree*, PhD thesis, University of Illiones, 1966.