UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
EM REDE NACIONAL

ADRIANO SILVA AVELA

O NÚMERO MÉDIO DE REPRESENTAÇÕES DE UM INTEIRO POSITIVO COMO SOMA DOS QUADRADOS DE DOIS INTEIROS

FORTALEZA
2017

ADRIANO SILVA AVELA

O NÚMERO MÉDIO DE REPRESENTAÇÕES DE UM INTEIRO POSITIVO COMO SOMA DOS QUADRADOS DE DOIS INTEIROS

Dissertação apresentada ao Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Ensino da Matemática.

Orientador: Prof. Dr.José Othon Dantas Lopes.

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A967n Avela, Adriano Silva.
O número médio de representações de um inteiro positivo como soma dos quadrados de dois inteiros / Adriano Silva Avela. – 2017.
58 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2017.
Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Soma de quadrados. 2. Números inteiros. I. Título.

CDD 510

ADRIANO SILVA AVELA

O NÚMERO MÉDIO DE REPRESENTAÇÕES DE UM INTEIRO POSITIVO COMO SOMA DOS QUADRADOS DE DOIS INTEIROS

Dissertação apresentada ao Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de concentração: Ensino da Matemática.

Orientador: Prof. Dr.José Othon Dantas Lopes.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr.José Othon Dantas Lopes (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr.José Valter Lopes Nunes
Universidade Federal do Ceará (UFC)

Prof. Dr.Ângelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

AGRADECIMENTOS

À CAPES, pelo apoio financeiro com a manutenção da bolsa de auxílio.

Ao Prof. Dr.José Othon Dantas Lopes, pela excelente orientação.

Aos professores participantes da banca examinadora José Valter Lopes Nunes e Ângelo Papa Neto pelo tempo, pelas valiosas colaborações e sugestões.

À Francisca Tainan Pereira Jesuita, pelas sugestões, críticas e reflexões.

RESUMO

Este trabalho tem como objetivo abordar dois temas: a representação de inteiros positivos como soma de quadrados e o número médio de representações de um inteiro positivo como soma de dois quadrados. Sobre o primeiro tema, provaremos diversos resultados para entender em quais condições um inteiro positivo possui uma representação como soma de dois, três ou quatro quadrados. Sobre o segundo tema, provaremos que um inteiro positivo tem, em média, π representações como soma dos quadrados de dois inteiros. Para tanto, introduziremos a função s_2, que associa um inteiro n com a cardinalidade do conjunto $X_n = \{(a, b) \in \mathbb{Z}^2; a^2 + b^2 = n\}$ e calcularemos o limite do seu valor médio. Por fim, como analogia ao resultado a respeito do valor médio de s_2, definiremos a função s_3, que associa um inteiro positivo n com a cardinalidade do conjunto $Y_n = \{(a, b, c) \in \mathbb{Z}^3; a^2 + b^2 + c^2 = n\}$ e provaremos que não existe um número médio de representações de um inteiro positivo como soma dos quadrados de três inteiros.

Palavras-chave: Números inteiros. Soma de quadrados.

ABSTRACT

This paper aims to address two themes: the representation of positive integers as sum of squares and the average number of representations of a positive integer as the sum of two squares. About the first theme, we will prove several results to understand under what conditions a positive integer has a representation as a sum of two, three or four squares. About the second theme, we will prove that the mean number of representations of a positive integer as the sum of the squares of two integers is . To do so, we will introduce the function s_2 which associates an integer n with the cardinality of the set $X_n = \{(a, b) \in \mathbb{Z}^2; a^2 + b^2 = n\}$ and we will calculate the limit of its average value. Finally, as an analogy to the result regarding the mean value of s_2, we will define the function s_3, that associates a positive integer n with the cardinality of the set $Y_n = \{(a, b, c) \in \mathbb{Z}^3; a^2 + b^2 + c^2 = n\}$ and we will prove that there is no mean number of representations of a positive integer as the sum of the squares of three integers.

Keywords: Integers. Sum of squares.

SUMÁRIO

1 INTRODUÇÃO

Procurar condições que determinem se um número pode ou não ser escrito como soma de quadrados é um problema antigo e que sempre esteve sob investigação de grandes matemáticos, desde Diofanto, no século III, até Hilbert, no século XX. Procurar tais condições é um dos objetivos deste trabalho. O outro objetivo é determinar o número médio de representações de um inteiro como soma de dois quadrados.

Na seção 2 faremos uma breve revisão de aritmética dos restos, fornecendo todas as ferramentas necessárias nas seções seguintes, desde a definição de relação de congruência até desvios quadráticos. Caso o leitor esteja familiarizado com esses assuntos, esta seção pode ser ignorada sem prejuízo para o entendimento das seções seguintes.

Na seção 3 encontra-se as principais proposições a respeito de soma de quadrados. Veremos que através da representação canônica de um número como produto de primos é possível determinar se ele pode ou não ser escrito como soma de dois quadrados.

Na seção 4 introduziremos duas funções que se associam com o número de formas que um inteiro pode ser escrito como soma de quadrados, tais funções serão essenciais nas seções 5 e 6.

Na seção 5 determinaremos o número médio de representações de inteiro como soma de dois quadrados, para tanto, usaremos um engenhoso limite provado por C.F.Gauss que, curiosamente, converge para π.

Por fim, na seção 6, em vista do que é demonstrado na seção 4, provaremos que o número médio de representações de um inteiro como soma de três quadrados não existe.

2 ARITMÉTICA DO RESTOS

Nesta seção faremos um breve estudo sobre a relação de congruência, congruências lineares e resíduos quadráticos. Serão enunciados e provados aqui todos os resultados que servirão de base para o que desenvolveremos nas próximas seções.

2.1 A relação de congruência

Seja k um número natural. Diremos que dois números inteiros a e b são congruentes, módulo k, se seus restos na divisão euclidiana por k forem iguais.

Quando a e b forem congruentes, módulo k, escreveremos

$$a \equiv b \mod k.$$

Alguns exemplos:

- $3 \equiv 5 \mod 2$, já que 3 e 5 deixam resto 1 na divisão por 2.
- $5 \equiv 11 \mod 3$, já que 5 e 11 deixam resto 2 na divisão por 3.

Quando a relação $a \equiv b \mod k$ for falsa, diremos que a e b são incongruentes, ou que não são congruentes, módulo k. Nesse caso, escreveremos,

$$a \not\equiv b \mod k.$$

Dado um número natural k, a relação de congruência, módulo k, é uma relação de equivalência, enunciaremos isso no teorema abaixo, sem as demonstrações, pois pela definição de congruência módulo k, cada um dos itens é evidente.

Teorema 2.1: Dado $k \in \mathbb{N}$. Para todos $x, y, z \in \mathbb{Z}$, tem-se que

- (Reflexividade) $x \equiv x \mod k$,
- (Simetria) Se $x \equiv y \mod k$, então $y \equiv x \mod k$,
- (Transitividade) Se $x \equiv y \mod k$ e $y \equiv z \mod k$, então $x \equiv z \mod k$.

Para deduzir que dois números são congruentes, módulo k, não é necessário efetuar a divisão euclidiana de ambos por k para depois comparar os restos obtidos. É suficiente que apliquemos o seguinte teorema:

Teorema 2.2: Suponha que $a, b, k \in \mathbb{Z}$, com $k > 1$. Tem-se que

$$k|b-a \Leftrightarrow a \equiv b \mod k.$$

Prova: Sejam $a = kq + r$, com $0 \leq r < k$ e $b = kq' + r'$, com $0 \leq r' < k$, as divisões euclidianas de a e b por k, respectivamente. Logo,

$$b - a = kq' + r' - (kq + r) = k \cdot (q' - q) + (r' - r).$$

Portanto, $a \equiv b \mod k$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $k|b-a$, já que $|r' - r| < k$.

■

Note que todo número inteiro é congruente, módulo k, ao seu resto pela divisão euclidiana por k e, portanto, é congruente, módulo k, a um dos números $0, 1, ..., k-1$. Além disso, dois desses números distintos não são congruentes módulo k.

Chamaremos de *sistema completo de resíduos módulo k* a todo conjunto de números inteiros cujos restos pela divisão por k são os números

$$0, 1, ..., k-1,$$

sem repetições e numa ordem qualquer. Ou seja, todo sistema completo de resíduos módulo k possui exatamente k elementos.

Para formar um sistema completo de resíduos módulo k, basta escolher k inteiros $a_1, a_2, ..., a_k$ dois a dois incongruentes módulo k, seus restos por k são dois a dois distintos, o que implica que são os números $0, 1, ..., k-1$ em alguma ordem. Em particular, um conjunto formado por k inteiros consecutivos é um sistema completo de resíduos módulo k.

Considere o conjunto $R = \{r \in \mathbb{Z}; -\frac{k}{2} \leq r < \frac{k}{2}\}$, em R temos k inteiros consecutivos, logo R forma um sistema de resíduos completo módulo m. Usaremos R no apêndice C, pois a soma dos módulos de seus elementos é a menor possível entre os conjuntos que formam sistemas completos de resíduos módulo k.

A relação de congruência é compatível com as operações de adição e multiplicação nos inteiros, como podemos ver nos próximos resultados.

Teorema 2.3: Sejam $a, b, c, d, k \in \mathbb{Z}$, com $k > 1$.

1. Se $a \equiv b \mod k$ e $c \equiv d \mod k$, então $a + c \equiv b + d \mod k$.
2. Se $a \equiv b \mod k$ e $c \equiv d \mod k$, então $ac \equiv bd \mod k$.

Prova: Como $a \equiv b \mod k$ e $c \equiv d \mod k$, temos que $k|b-a$ e $k|c-d$, daí $k|(b-a)+(d-c)$, ou seja, $k|(b+d)-(a+c)$, portanto $a + c \equiv b + d \mod k$.

Por outro lado, também temos que $bd - ac = d \cdot (b-a) + a \cdot (d-c)$, como $k|d \cdot (b-a) + a \cdot (d-c)$, concluímos que $k|bd - ac$ e portanto $ac \equiv bd \mod k$.

■

Corolário 2.4 Dado k um número natural, para todo n natural e a e b inteiros, se $a \equiv b \mod k$, então tem-se que $a^n \equiv b^n \mod k$.

Prova: Vamos provar este resultado por indução em n.

Para $n = 1$ é óbvio. Supondo que o resultado vale para $n = l$, temos que

$$a^{l+1} \equiv b^{l+1} \mod k \Leftrightarrow k|b^{l+1} - a^{l+1} \Leftrightarrow k|b \cdot (b^l - a^l) - a^l \cdot (a-b).$$

Como, por hipótese de indução, temos que $k|b^l - a^l$, fica provado o resultado.

■

Com a notação de congruência, o Pequeno Teorema de Fermat enuncia-se como se segue:

Teorema 2.5(Pequeno Teorema de Fermat): Se p é um número primo e se a é um inteiro, então

$$a^p \equiv a \mod p.$$

Além disso, se p não divide a, temos que

$$a^{p-1} \equiv 1 \mod p.$$

Prova: Se $p = 2$, o resultado é óbvio já que $a^2 - a = a \cdot (a-1)$ é par. Suponhamos p ímpar. Nesse caso, claramente basta mostrar o resultado para $a \geq 0$. Vamos provar o resultado por indução sobre a.

O resultado vale claramente para $a = 0$, pois $p|0$.

Supondo o resultado válido para a, ou seja, que $a^p \equiv a \mod p$, iremos prová-lo para $a+1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1} \cdot a^{p-1} + ... + \binom{p}{p-1} \cdot a.$$

Como $\binom{p}{i}$ é divisível por p, para $0 < i < p$, temos, pela hipótese de indução, que o segundo membro da igualdade acima é divisível por p, ou seja, $a^{p+1} \equiv a \mod p$.

■

Nas próximas proposições vamos mostrar como a relação de congruência interage com as operações básicas.

Proposição 2.6: Sejam $a, b, c, k \in \mathbb{Z}$, com $k > 1$. Tem-se que

$$a + c \equiv b + c \mod k \Leftrightarrow a \equiv b \mod k.$$

Prova: Se $a \equiv b \mod k$, segue-se imediatamente do Teorema 2.3 (item 1) que $a + c \equiv b + c \mod k$, pois $c \equiv c \mod k$.

Reciprocamente, se $a + c \equiv b + c \mod k$, então $k|(b + c) - (a + c)$, o que implica que $k|b - a$ e, portanto, $a \equiv b \mod k$.

■

A última proposição nos mostra que para as congruências, vale o cancelamento em relação à adição, veremos a seguir que o mesmo não ocorre, em geral, com relação à multiplicação.

Proposição 2.7: Sejam $a, b, c, k \in \mathbb{Z}$, com $k > 1$ e $mdc(c, k) = d$. Temos que

$$ac \equiv bc \mod k \Leftrightarrow a \equiv b \mod \frac{k}{d}.$$

Prova: Como $mdc\left(\frac{k}{d}, \frac{c}{d}\right) = 1$, temos que:

$$ac \equiv bc \mod k \Leftrightarrow k|(b-a) \cdot c \Leftrightarrow \frac{k}{d}|(b-a) \cdot \frac{c}{d} \Leftrightarrow \frac{k}{d}|b-a$$

onde a última expressão ocorre se, e somente se, $a \equiv b \mod \frac{k}{d}$ ocorre.

■

Corolário 2.8: Sejam $a, b, c, k \in \mathbb{Z}$, com $k > 1$ e $mdc(c, k) = 1$. Temos que

$$ac \equiv bc \mod k \Leftrightarrow a \equiv b \mod k.$$

Proposição 2.9: Sejam $a, l, k \in \mathbb{Z}$, com $k > 1$ e $mdc(l, k) = 1$. Se $a_1, a_2, ..., a_k$ é um sistema completo de resíduos módulo k, então

$$a + la_1, a + la_2, ..., a + la_k$$

também é um sistema completo de resíduos módulo k.

Prova: Pela Proposição 2.6 e pelo Corolário acima, para $i, j \in \{0, 1, ..., k-1\}$ temos que

$$a + la_i \equiv a + la_j \mod k \Leftrightarrow la_i \equiv la_j \mod k \Leftrightarrow a_i \equiv a_j \mod k.$$

Como $a_1, a_2, ..., a_l$ é um sistema completo de resíduos módulo k, a última equivalência acima só ocorre quando $i = j$, temos então que os números $a + la_1, a + la_2, ..., a + la_k$ são, dois a dois, incongruentes módulo k, ou seja, formam um sistema completo de resíduos módulo k.

■

A próxima proposição nos traz algumas propriedades adicionais sobre congruências que envolvem produtos.

Proposição 2.10: Sejam $a, b \in \mathbb{Z}$ e $k, n, k_1, k_2, ..., k_r$ inteiros maiores do que 1. Temos que:

1. Se $a \equiv b \mod k$ e $n|k$, então $a \equiv b \mod n$;
2. $a \equiv b \mod k_i, \forall i = 1, 2, ..., r \Leftrightarrow a \equiv b \mod [k_1, k_2, ..., k_r]$[1];
3. Se $a \equiv b \mod k$, então $mdc(a, k) = mdc(b, k)$.

Prova:

Se $a \equiv b \mod k$, então $k|b - a$. Como $n|k$, segue-se, por transitividade, que $n|b - a$, logo $a \equiv b \mod n$. Isto prova o item 1.

Se $a \equiv b \mod k_i$, $i = 1, 2, ..., r$, então $k_i|b - a$, para todo i. Sendo $b - a$ um múltiplo de cada k_i, segue-se que $[k_1, k_2, ..., k_r]|b - a$, ou seja, $a \equiv b \mod [k_1, k_2, ..., k_r]$.

Agora, se $a \equiv b \mod [k_1, k_2, ..., k_r]$, como $k_i|[k_1, k_2, ..., k_r]$ para todo $i = 1, 2, ..., r$, temos pelo item 1 que $k_i|b - a$ para todo $i = 1, 2, ..., r$, logo $a \equiv b \mod k_i$ para todo $i = 1, 2, ..., r$. Isto prova o item 2.

[1] A notação $[k_1, k_2, ..., k_r]$ representa o mínimo múltiplo comum entre os números $k_1, k_2, ..., k_r$.

Por fim, se $a \equiv b \mod k$, então $k|b-a$ e, portanto, $b = a + tk$ para algum t inteiro. Logo

$$mdc(a,k) = mdc(a+tk,k) = mdc(b,k).$$

O que prova o item 3.

■

2.2 Congruências lineares

Nesta subseção estudaremos as congruências lineares, isto é, congruências da forma

$$ax \equiv b \mod k,$$

onde $a, b, k \in \mathbb{Z}$, com $a \neq 0$, $k > 1$ e como determinar suas soluções, ou seja, os números $x \in \mathbb{Z}$ que tornam a congruência verdadeira.

Em particular, será útil no decorrer do texto determinar se uma congruência do tipo

$$aX \equiv 1 \mod k$$

possui alguma solução em X. Para tanto, o seguinte resultado nos será conveniente:

Proposição 2.11: Sejam $a, k \in \mathbb{Z}$, com $k > 1$. A congruência $aX \equiv 1 \mod k$ possui solução se, e somente se, $mdc(a,k) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0 \mod k$.

Prova: A congruência $aX \equiv 1 \mod k$ tem uma solução x_0 se, e somente se, $k|ax_0 - 1$, o que equivale a dizer que a equação diofantina $aX - kY = 1$ possui solução em números inteiros, o que ocorre, pois $mdc(a,k) = 1$.[1]

Por outro lado, se x e x_0 são soluções de $aX \equiv 1 \mod k$, então $ax \equiv ax_0 \mod k$ e $mdc(a,k) = 1$, o que implica, em virtude do Corolário 2.8, que $x \equiv x_0 \mod k$.

[1] No apêndice B está enunciado um resultado a respeito da resolubilidade de equações diofantinas de primeira ordem.

Observe que, se x_0 é solução da congruência $aX \equiv 1 \mod k$, e $x \equiv x_0 \mod k$, então x é também solução da mesma congruência, pois

$$ax \equiv ax_0 \equiv 1 \mod k.$$

■

Como aplicação do último resultado, vamos provar o Teorema de Wilson, um famoso critério de primalidade, o usaremos nas seções seguintes, mas não com esse propósito.

Teorema 2.12 (Wilson): Se p é um número primo, então

$$(p-1)! \equiv -1 \mod p.$$

Prova: O Teorema é válido para $p = 2$ e $p = 3$, pois, de fato, $(2-1)! = 1! = 1 \equiv -1 \mod 2$ e $(3-1)! = 2! = 2 \equiv -1 \mod 3$.

Suponhamos $p \geq 5$ primo. Para todo $i \in \{1, 2, ..., p-1\}$, pela Proposição 2.11, a congruência $iX \equiv 1 \mod p$ possui uma única solução módulo p; ou seja, dado $i \in \{1, 2, ..., p-1\}$, existe um único $j \in \{1, 2, ..., p-1\}$ tal que $ij \equiv 1 \mod p$.

Por outro lado, se $i \in \{1, 2, ..., p-1\}$ é tal que $i^2 \equiv 1 \mod p$, então $p|i^2 - 1$, o que equivale a dizer que $p|i-1$ ou $p|i+1$, que só podem ocorrer se $i = 1$ ou $i = p-1$.

Logo,

$$2 \cdot ... \cdot (p-2) \equiv 1 \mod p,$$

e, portanto,

$$(p-1)! = 1 \cdot 2 \cdot ... \cdot (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \mod p.$$

■

A título de curiosidade, para determinar se um número é primo ou não, através do Teorema de Wilson, basta verificar se $p|(p-1)!+1$. Trata-se de um método eficiente, mas nada eficaz, por exemplo, para determinar que 91 não é primo, teríamos de verificar que $90!+1$ não é divisível por 91, nesse caso, é mais fácil notar que $91 = 7 \cdot 13$.

A seguir, mostraremos como resolver congruências e sistemas de congruências lineares. Nossa primeira proposição a esse respeito nos dirá se uma determinada congruência admite soluções ou não.

Proposição 2.13: Dados $a, b, k \in \mathbb{Z}$, com $k > 1$ e $d = mdc(a, k)$ a congruência

$$aX \equiv b \mod k$$

possui solução se, e somente se, $d|b$.

Prova: Suponhamos que a congruência $aX \equiv b \mod k$ tenha solução x; logo, temos que $k|ax - b$, o que equivale à existência de um inteiro y tal que $ky = ax - b$. Portanto, a equação $aX - kY = b$ admite solução. Ou seja, $d|b$.

Reciprocamente, suponha que $d|b$. Logo, a equação $aX - kY = b$ admite uma solução x, y com x e y inteiros. Portanto, $ax = b + ky$ e, consequentemente, x é solução da congruência pois, $ax \equiv b \mod k$.

■

Note que, se x_0 é solução da congruência $aX \equiv b \mod k$, então todo x tal que $x \equiv x_0 \mod k$ é também solução da congruência pois,

$$ax \equiv ax_0 \equiv c \mod k.$$

Portanto, toda solução particular determina, automaticamente, uma infinidade de soluções da congruência. Doravante, essas infinitas soluções serão consideradas como uma só (módulo k), já que são congruentes entre si, e, consequentemente, se determinam mutuamente.

Estaremos, portanto, interessados em determinar uma coleção completa de soluções duas a duas incongruentes módulo k, as quais serão chamadas de sistema completo de soluções incongruentes da congruência.

No próximo teorema explicitaremos uma fórmula para determinar o sistema completo de soluções incongruentes de qualquer congruência linear.

Teorema 2.14: Sejam $a, b, k \in \mathbb{Z}$, com $k > 1$ e $d = (a, k)$, se $d|b$ e se x_0 é uma solução da congruência $aX \equiv b \mod k$, então

$$x_0, x_0 + \frac{k}{d}, x_0 + 2 \cdot \frac{k}{d}, ..., x_0 + (d-1) \cdot \frac{k}{d},$$

formam um sistema completo de soluções da congruência, duas a duas incongruentes módulo k.

Prova: Toda solução x da congruência $aX \equiv b \mod k$ é congruente, módulo k, a $x_0 + i \cdot \frac{k}{d}$ para algum $0 \leq i < d$. De fato, se x é uma solução qualquer da congruência, então,

$$ax \equiv ax_0 \mod k,$$

e, portanto, pela proposição 2.7,

$$x \equiv x_0 \mod \frac{k}{d}.$$

Logo, $x - x_0 = \frac{lk}{d}$. Pela divisão euclidiana, existe $0 \leq i < d$ tal que $l = qd + i$ e, portanto,

$$x = x_0 + qk + i \cdot \frac{k}{d} \equiv x_0 + i \cdot \frac{k}{d} \mod k.$$

Reciprocamente, os números $x_0 + i \cdot \frac{k}{d}$, com $0 \leq i < d$, são soluções da congruência, pois

$$a \cdot (x_0 + i \cdot \frac{k}{d}) = ax_0 + i \cdot \frac{a}{d} \cdot k \equiv ax_0 \equiv b \mod k.$$

Finalmente, esses números são dois a dois incongruentes, módulo k, pois, para $0 \leq i, j < d$, se

$$x_0 + i \cdot \frac{k}{d} \equiv x_0 + j \cdot \frac{k}{d} \mod k,$$

então

$$i \cdot \frac{k}{d} \equiv j \cdot \frac{k}{d} \mod k.$$

Como $0 \leq i, j < d$, então $0 \leq i \cdot \frac{k}{d}, j \cdot \frac{k}{d} < k$, e como k divide $|i \cdot \frac{k}{d} - j \cdot \frac{k}{d}|$, segue-se que $i \cdot \frac{k}{d} = j \cdot \frac{k}{d}$ e, portanto, $i = j$.

■

Corolário 2.15: Se $mdc(a, k) = 1$, então a congruência $aX \equiv b \mod k$ possui uma única solução módulo k.

Doravante, nos casos onde $b = 1$, chamaremos a solução única da congruência linear $aX \equiv 1 \mod k$ de inverso multiplicativo de a módulo k.

Para que possamos enunciar o próximo corolário, vamos precisar da definição abaixo.

Um *sistema reduzido de resíduos módulo k* é um conjunto de números inteiros $r_1, r_2, ..., r_s$ tais que para todo $i, j \in \{1, 2, ..., s\}$, temos:

1. $mdc(r_i, k) = 1$;
2. $r_i \not\equiv r_j \mod k$, se $i \neq j$;
3. Para cada $n \in \mathbb{Z}$ tal que $mdc(n, k) = 1$, existe i tal que $n \equiv r_i \mod k$.

Corolário 2.16: Sejam $k > 1$ e R' um conjunto reduzido de resíduos módulo k. Se $b \in \mathbb{Z}$, então, para todo $r \in R'$, a congruência $rX \equiv b \mod k$ possui uma única solução em R'.

Prova: De fato, como $r \in R'$, temos que $mdc(r, k) = 1$, logo a congruência tem uma única solução módulo k. Toda solução x em $\mathbb{Z}$ é tal que $mdc(x, k) = 1$, logo, tem um único representante módulo k no conjunto R'.

■

É importante notar que toda congruência linear $aX \equiv b \mod k$ que possui uma solução é equivalente a uma congruência na forma

$$X \equiv c \mod n.$$

Note que, se a congruência

$$aX \equiv b \mod k$$

possui solução, então $d = mdc(a, k)$ divide b. Pondo $\bar{a} = \frac{a}{d}, \bar{b} = \frac{b}{d}$ e $n = \frac{k}{d}$, temos que a congruência acima é equivalente à congruência

$$\bar{a}X \equiv \bar{b} \mod n,$$

com $mdc(\bar{a}, n) = 1$, que, por sua vez, é equivalente à congruência

$$X \equiv c \mod n,$$

onde $c = a'\bar{b}$, sendo a' o inverso multiplicativo de $\bar{a}$ módulo n.

Vamos agora estudar os sistemas de congruências da forma:

$$a_iX \equiv b_i \mod n_i,$$

para $i \in \{1, 2, ...m\}$.

Seja $d_i = mdc(a_i, n_i)$, para que tal sistema possua solução, é necessário que $d_i | b_i$, para todo $i \in \{1, 2, ...m\}$.

Nesse caso, pelo que foi observado logo acima, o sistema é equivalente a um na forma

$$\begin{cases} X \equiv c_1 \mod k_1 \\ X \equiv c_2 \mod k_2 \\ \vdots \\ X \equiv c_3 \mod k_m. \end{cases} \tag{1}$$

O método mais eficiente para resolver o sistema (1) é dado pelo seguinte teorema.

Teorema 2.17(Teorema Chinês do Resto) Sejam $i, j \in \{1, 2, ...m\}$. Se $mdc(k_i, k_j) = 1$, para todo par k_i, k_j com $i \neq j$, então o sistema (1) possui uma única solução módulo $K = k_1 \cdot k_2 \cdot ... \cdot k_m$. As soluções são

$$x = K_1y_1c_1 + K_2y_2c_2 + ... + K_my_mc_m + tK,$$

onde $t \in \mathbb{Z}, K_i = \frac{K}{k_i}$ e y_i é solução de $K_iY \equiv 1 \mod k_i$.

Prova: Vamos, a priori, provar que x é solução das m equações do sistema (1).

De fato, como $k_i|K_j$, se $i \neq j$ e $K_i y_i \equiv 1 \mod k_i$, segue-se que

$$x = K_1 y_1 c_1 + K_2 y_2 c_2 + ... + K_m y_m c_m \equiv K_i y_i c_i \equiv c_i \mod k_i.$$

Por outro lado, se x' é outra solução do sistema, então

$$x \equiv x' \mod k_i, \forall i \in \{i = 1, 2, ..., m\}.$$

Como $mdc(k_i, k_j) = 1$, para $i \neq j$, segue-se que $[k_1, k_2, ..., k_m] = k_1 \cdot k_2 \cdot ... \cdot k_m = K$ e, consequentemente, pela Proposição 2.10 (item 2), temos que $x \equiv x' \mod K$.

■

2.3 Resíduos Quadráticos

Para que possamos estudar os números que podem ser escritos como soma de quadrados, será necessária a seguinte definição.

Seja r um número inteiro. Quando a congruência $X^2 \equiv r \mod p$ possui alguma solução, diz-se que r é *resíduo quadrático módulo* p, caso contrário, diz-se que r não é resíduo quadrático módulo p.

Como exemplo, temos que:

- 2 não é resíduo quadrático módulo 3;
- 1 é resíduo quadrático módulo 4;
- 4 é resíduo quadrático módulo 8.

Nosso primeiro resultado sobre resíduos quadráticos será o próximo lema.

Lema 2.18: Sejam $p > 2$ um número primo e $r \in \mathbb{Z}$ tal que $mdc(p, r) = 1$. Se $x_0 \in R^* = \{1, 2, ..., p-1\}$ é solução da congruência $X^2 \equiv r \mod p$, então $mdc(x_0, p) = 1$ e $p - x_0$ também é solução, não congruente a x_0, e essas são as únicas soluções em R^*.

Prova: Se $x_0^2 \equiv r \mod p$, então

$$mdc(x_0, p) = mdc(x_0^2, p) = mdc(r, p) = 1.$$

onde na última igualdade usamos o Teorema 2.10(item 3). Por outro lado,

$$(p - x_0)^2 = p^2 - 2px_0 + x_0^2 \equiv x_0^2 \equiv r \mod p.$$

Seja $x_1 \in R^*$ tal que $x_1^2 \equiv r \mod p$. Logo $x_0^2 \equiv x_1^2 \mod p$ e, portanto, $p|x_1^2 - x_0^2$, o que implica que $p|x_1 - x_0$ ou $p|x_1 + x_0$. Isso, por sua vez, implica que $x_1 = x_0$ ou que $x_1 = p - x_0$, dado que $x_0, x_1 \in R^*$.

Por fim, se $x_0 \equiv p - x_0 \mod p$, teríamos que $p|2x_0$ e como $p > 2$ é um número primo, teríamos que $p|x_0$, o que é absurdo.

■

Agora, suponha que $p > 2$ seja um número primo e que r seja um número inteiro tal que $mdc(p, r) = 1$. Pelo Teorema 2.5 temos

$$(r^{\frac{p-1}{2}} - 1) \cdot (r^{\frac{p-1}{2}} + 1) = r^{p-1} - 1 \equiv 0 \mod p,$$

logo $p|r^{\frac{p-1}{2}} - 1$ ou $p|r^{\frac{p-1}{2}} + 1$, não podendo ocorrer as duas situações simultaneamente, pois, caso contrário, p dividiria

$$(r^{\frac{p-1}{2}} - 1) + (r^{\frac{p-1}{2}} + 1) = 2r^{\frac{p-1}{2}},$$

o que não é possível já que $p > 2$ e $mdc(p, r) = 1$.

Agora, fica a pergunta: como saber qual das duas situações ocorre?

A resposta para isso é devida a Euler, através de um critério que deduziremos com ajuda da próxima proposição.

Proposição 2.19: Sejam p um número primo ímpar e $r \in \mathbb{Z}$ tal que $mdc(p, r) = 1$.

1. Se $X^2 \equiv r \mod p$ não tem solução, então $r^{\frac{p-1}{2}} \equiv -1 \mod p$.
2. Se $X^2 \equiv r \mod p$ tem solução, então $r^{\frac{p-1}{2}} \equiv 1 \mod p$.

Prova: Seja $A^* = \{1, 2, ..., p-1\}$.

Para provar o item 1, tome $a \in R^*$, a congruência $aX \equiv r \mod p$, pelo Corolário 2.16, possui uma única solução $a' \in A^*$. Como estamos assumindo que a congruência $X^2 \equiv r \mod p$ não tem solução, temos que $a' \neq a$. Agrupando os elementos de A^* aos pares como fizemos com a e a', temos, pelo Teorema de Wilson (Teorema 2.12), que

$$-1 \equiv (p-1)! \equiv r^{\frac{p-1}{2}} \mod p.$$

Para provar o item 2, suponha que a congruência $X^2 \equiv r \mod p$ tem solução, pelo Lema 2.18, ela possui duas soluções a e a'. Como $a' = (p-a)$ e $a^2 \equiv r \mod p$, segue-se que $aa' \equiv -r \mod p$.

Por outro lado, os outros elementos de A^* agrupam-se ao pares de elementos distintos b e b', tais que $bb' \equiv r \mod p$. Portanto, pelo Teorema de Wilson,

$$-1 \equiv (p-1)! \equiv -bb^{\frac{p-3}{2}} \equiv -r^{\frac{p-1}{2}} \mod p,$$

o que mostra que

$$r^{\frac{p-1}{2}} \equiv 1 \mod p.$$

■

Vamos agora ao Critério de Euler.

Teorema 2.20(Euler): Se p é um número primo ímpar e $r \in \mathbb{Z}$ é tal que $mdc(p, r) = 1$, então:

1. $p | r^{\frac{p-1}{2}} - 1$ se, e somente se, r é resíduo quadrático módulo p.
2. $p | r^{\frac{p-1}{2}} + 1$ se, e somente se, r não é resíduo quadrático módulo p.

Prova: Para p primo com $mdc(p, r) = 1$, já vimos que uma, e somente uma, das duas possibilidades ocorre: $p | r^{\frac{p-1}{2}} - 1$ ou $p | r^{\frac{p-1}{2}} + 1$.

Para o item 1, suponha que r é resíduo quadrático, logo $X^2 \equiv r \mod p$ tem solução, ou seja, pela Proposição 2.19 (item 2), temos que $r^{\frac{p-1}{2}} \equiv 1 \mod p$ e portanto $p|r^{\frac{p-1}{2}} - 1$.

Reciprocamente, se $p|r^{\frac{p-1}{2}} - 1$, então não ocorre $p|r^{\frac{p-1}{2}} + 1$, logo não ocorre que $r^{\frac{p-1}{2}} \equiv -1 \mod p$, ou seja, pela contra-positiva do item 1 da Proposição 2.19, $X^2 \equiv r \mod p$ deve ter pelo menos uma solução, portanto r é resíduo quadrático módulo p.

Para o item 2, suponha que r não é resíduo quadrático módulo p, logo $X^2 \equiv r \mod p$ não tem solução, ou seja, pela Proposição 2.19 (item 1), temos que $r^{\frac{p-1}{2}} \equiv -1 \mod p$ e portanto $p|r^{\frac{p-1}{2}} + 1$.

Reciprocamente, se $p|r^{\frac{p-1}{2}} + 1$, então não ocorre $p|r^{\frac{p-1}{2}} - 1$, logo não ocorre que $r^{\frac{p-1}{2}} \equiv 1 \mod p$ ou seja, pela contra-positiva do item 2 da Proposição 2.19, $X^2 \equiv r \mod p$ não tem solução, portanto r não é resíduo quadrático módulo p.

■

Em geral, determinar explicitamente os elementos de $A^* = \{1, 2, ..., p-1\}$ que são resíduos quadráticos módulo p não é simples, felizmente, o mesmo não ocorre para determinarmos a quantidade deles, na próxima proposição obtemos um resultado a respeito disso.

Proposição 2.21 Seja $p > 2$ um número primo. Os números

$$1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$$

são dois a dois não congruentes, módulo p, e representam todos os resíduos quadráticos módulo p.

Prova: Note que todo número que é resíduo quadrático módulo p é congruente, módulo p, a um dos números: $1^2, 2^2, ..., (p-1)^2$.

Nesse conjunto há repetições, pois

$$r^2 \equiv (p-r)^2 \mod p, \forall r \in \{1, 2, ..., p-1\}.$$

Portanto, os números $1^2, 2^2, ..., (\frac{p-1}{2})^2$ representam todos os resíduos quadráticos módulo p. Só nos resta mostrar que são dois a dois incongruentes.

De fato, suponha que $r, s \in \{1, 2, ..., \frac{p-1}{2}\}$, com $r \neq s$, e que $r^2 \equiv s^2 \mod p$. Logo, $p|s^2 - r^2$ e, portanto, $p|s-r$ ou $p|s+r$, ambas impossíveis, pois

$$0 < s - r < s + r < p.$$

■

Corolário 2.22 No conjunto $A^* = \{1, 2, ..., p-1\}$ existem $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ resíduos não quadráticos, módulo p.

3 SOMA DE QUADRADOS

Nesta seção, caracterizaremos os números naturais que podem ser escritos como soma dos quadrados de dois inteiros. Para começar, vamos ver quais números primos possuem essa propriedade.

Teorema 3.1(Fermat): As seguintes condições sobre um primo ímpar p são equivalentes:

1. $p \equiv 1 \mod 4$.
2. -1 é resíduo quadrático módulo p.
3. p pode ser escrito como soma de dois quadrados.

Prova:

1. $\Rightarrow$ 2. Aplicando o Teorema de Wilson (Teorema 2.12) a $p = 4k + 1$, temos que

$$\begin{aligned} -1 &\equiv (p-1)! \\ &\equiv (4k)! \\ &\equiv (1 \cdot 2 \cdot \ldots \cdot 2k) \cdot ((2k+1) \cdot (2k+2) \cdot \ldots \cdot (4k-1) \cdot (4k)) \\ &\equiv (1 \cdot 2 \cdot \ldots \cdot 2k) \cdot ((-2k) \cdot \ldots \cdot (-2)(-1)) \\ &\equiv (1 \cdot 2 \cdot \ldots \cdot 2k)^2 \cdot (-1)^{2k} \\ &\equiv (1 \cdot 2 \cdot \ldots \cdot 2k)^2 \\ &\equiv ((2k)!)^2 \mod p. \end{aligned}$$

Ou seja, existe $x = (2k)!$ tal que $x^2 \equiv -1 \mod p$.

Uma outra forma de provar que 1. $\Rightarrow$ 2. é através da Proposição 2.20 (item 1), veja:

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 \mod p$$

e daí -1 é resíduo quadrático módulo p.

2. $\Rightarrow$ 3. Sejam $h \in \mathbb{Z}$ tal que $h^2+1 \equiv 0 \mod p$, e $A = \left\{(x,y); x,y \in \mathbb{Z}, 0 \leq x,y < \sqrt{p}\right\}$, então, pelo princípio fundamental da contagem, temos

$$\#A = (\lfloor \sqrt{p} \rfloor + 1)^2 > \sqrt{p}^2 = p.$$

Como só existem p possíveis restos numa divisão por p, o princípio das gavetas garante a existência de pares ordenados distintos $(x_1, y_1), (x_2, y_2) \in A$, tais que

$$hx_1 + y_1 \equiv hx_2 + y_2 \mod p.$$

Fazendo $a = |x_1 - x_2|$ e $b = |y_1 - y_2|$, temos que a e b são ambos não nulos e, portanto,

$$0 < a^2 + b^2 = |x_1 - x_2|^2 + |y_1 - y_2|^2 < \sqrt{p}^2 + \sqrt{p}^2 = 2p.$$

Porém, como

$$a^2 + b^2 = |x_1 - x_2|^2 + |y_1 - y_2|^2 \equiv (x_1 - x_2)^2 + (hx_1 - hx_2)^2 \mod p$$

e, além disso

$$(x_1 - x_2)^2 + (hx_1 - hx_2)^2 = (h^2 + 1) \cdot (x_1 - x_2)^2 \equiv 0 \mod p,$$

a única possibilidade é que seja $a^2 + b^2 = p$.

3. $\Rightarrow$ 1. Se $p = a^2 + b^2$ com $a, b \in \mathbb{Z}$ então a é par e b é ímpar ou vice-versa (lembre-se de que p é ímpar). Supondo, sem perda de generalidade, que a é par e b é ímpar, segue que $a^2 \equiv 0 \mod 4$ e $b^2 \equiv 1 \mod 4$, logo

$$p = a^2 + b^2 \equiv 0 + 1 \equiv 1 \mod 4.$$

■

Lema 3.2: Se m e n são naturais que podem ser escritos como somas de dois quadrados, então $m \cdot n$ também pode ser escrito como soma de dois quadrados.

Prova: Se $m = a^2 + b^2$ e $n = c^2 + d^2$, então

$$\begin{aligned} m \cdot n &= (a^2 + b^2) \cdot (c^2 + d^2) \\ &= a^2 \cdot c^2 + a^2 \cdot d^2 + b^2 \cdot c^2 + b^2 \cdot d^2 \\ &= ((ac)^2 + (bd)^2) + ((ad)^2 + (bc)^2) \\ &= ((ac)^2 + 2acbd + (bd)^2) + ((ad)^2 - 2adbc + (bc)^2) \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

■

Teorema 3.3(Fermat): Um natural n pode ser escrito como soma de dois quadrados se, e só se, $n = 1$ ou n é tal que todo primo congruente a 3 módulo 4 e que comparece na fatoração canônica de n o faz com expoente par.

Prova: No que segue, seja

$$n = 2^a \cdot p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} \cdot q_1^{b_1} \cdot \ldots \cdot q_l^{b_l}$$

a decomposição de n em fatores primos, com $a, a_i, b_j \geq 0, p_i \equiv 1 \mod 4$ e $q_j \equiv 3 \mod 4$, para todos $1 \leq i \leq k$ e $1 \leq j \leq l$.

Suponhamos inicialmente que cada b_j seja par, vamos mostrar que n pode ser escrito como soma de dois quadrados.

Note inicialmente que, pelo teorema 3.1, cada p_i pode ser escrito como soma de dois quadrados; por outro lado, temos $2^a = (2^{\frac{a}{2}})^2 + 0^2$ se a for par e $2^a = (2^{\frac{a-1}{2}})^2 + (2^{\frac{a-1}{2}})^2$ se a for ímpar; por fim, se $b_j = 2c_j$, com $c_j \in \mathbb{Z}$ para $1 \leq j \leq l$, então $q_j^{b_j} = (q_j^{c_j})^2 + 0^2$. Portanto, aplicando repetidamente o Lema 3.2, concluímos que n pode ser escrito como soma de dois quadrados.

Reciprocamente, suponha que n pode ser escrito como soma de dois quadrados, vamos mostrar que cada b_j é par.

Vamos, primeiramente, provar que se n pode ser escrito como soma de dois quadrados e $b_j \geq 1$, então $b_j \geq 2$ e $\frac{n}{q_j^2}$ também pode ser escrito como soma de dois quadrados. Para tanto, se $n = c^2 + d^2$, com $c, d \in \mathbb{Z}$, então $c^2 + d^2 \equiv 0 \mod q_j$. Se $d \not\equiv 0 \mod q_j$, então q_j não divide d e portanto $mdc(d, q_j) = 1$, de sorte que d, pelo corolário 2.15, é invertível módulo q_j; sendo f seu inverso módulo q_j, obtemos

$$(c^2 + d^2) \cdot f^2 \equiv 0 \cdot f^2 \mod q_j$$

$$\Rightarrow (cf)^2 + 1 \equiv 0 \mod q_j,$$

em contradição ao teorema 3.1, uma vez que $q_j \equiv 3 \mod 4$, portanto, $d \equiv 0 \mod q_j$ e, daí, $c \equiv 0 \mod q_j$. Logo, $n = c^2 + d^2 \equiv 0 \mod q_j^2$, de forma que $b_j \geq 2$ e

$$\frac{n}{q_j^2} = \left(\frac{c}{q_j}\right)^2 + \left(\frac{d}{q_j}\right)^2.$$

Agora, suponha que exista $1 \leq j \leq l$ tal que b_j é ímpar, ou seja, que $b_j = 2a + 1$ para algum a inteiro positivo. Se n puder ser escrito como soma de dois quadrados, então $b_j \geq 2$ e $\frac{n}{q_j^2}$ também pode ser escrito como soma de dois quadrados, note que se $a = 0$ chegamos a um absurdo, daí $a > 0$ e $b_j - 2 \geq 1$, ou seja, pelo que provamos, $b_j - 2 \geq 2$ e $\frac{n}{q_j^4}$ pode ser escrito como soma de dois quadrados, logo, para $a = 1$, obtemos outro absurdo, daí $a > 1$. Aplicando recorrentemente esse raciocínio, obtemos que $b_j - 2a > 2$, o que é absurdo, logo b_j não pode ser ímpar.

■

Teorema 3.4: Se p é um primo da forma $4k + 1$, então existem únicos $x, y \in \mathbb{N}$ tais que $x < y$ e $x^2 + y^2 = p$.

Prova: Já sabemos que existe ao menos um par de naturais x, y tais que $x^2 + y^2 = p$. Seja, então, a, b um outro tal par e observe que a, b, x e y são todos primos com p e menores que $\sqrt{p}$. Escolha inteiros $1 \leq c, z < p$ tais que $xz \equiv y$ e $ac \equiv b \mod p$.

Afirmamos que $c = z$ ou $c + z = p$. De fato, módulo p, temos

$$x^2 + y^2 \equiv x^2 + (xz)^2 = x^2 \cdot (z^2 + 1),$$

de maneira que $z^2 \equiv -1 \mod p$. Analogamente, $c^2 \equiv -1 \mod p$, de modo que p divide $z^2 - c^2 = (z - c) \cdot (z + c)$ e, daí, p divide $z - c$ ou $z + c$. Porém, como $1 \leq c, z < p$, segue que $-p < z - c < z + c < 2p$, acarretando em $z - c = 0$ ou $z + c = p$.

Suponha, agora, que $c = z$. As escolhas de c e z garantem que

$$bxz \equiv acy \equiv ayz \mod p$$

e, daí, $bx \equiv ay \mod p$. Porém, uma vez que $0 < a, b, x, y < \sqrt{p}$, temos que $0 < bx, ay < p$ e, por conseguinte, $bx = ay$. Assim,

$$p = x^2 + y^2 = \left(\frac{ay}{b}\right)^2 + y^2 = \left(\frac{y}{b}\right)^2 \cdot (a^2 + b^2) = \left(\frac{y}{b}\right)^2 \cdot p$$

e, daí, $y = p$ e $x = a$.

Se $z + c = p$, então, como $bxz \equiv acy \equiv ayz \mod p$, chegamos a $bx \equiv -ay \mod p$ e, daí, a $bx + ay = p$. Logo, pelo Lema 3.2, temos

$$p^2 = (a^2 + b^2) \cdot (x^2 + y^2) = (bx + ay)^2 + (by - ax)^2 = p^2 + (by - ax)^2,$$

ou seja, $by = ax$. Novamente, concluímos que $x = b$ e $y = a$.

■

4 FUNÇÃO s_2 E FUNÇÃO s_3

Nesta seção, definiremos duas funções, elas serão essenciais nas demonstrações dos resultados envolvendo o número médio de representações de um inteiro como soma de dois ou três quadrados.

4.1 Função s_2

Antes de definir s_2, vamos definir um importante conjunto associado à função.

Seja $X_n = \{(a,b) \in \mathbb{Z}^2; a^2 + b^2 = n\}$. X_n é o conjunto de todos os pares ordenados com coordenadas inteiras que se elevadas ao quadrado e somadas, resultam em n.

Alguns exemplos são:

- $X_0 = \{(0,0)\}$
- $X_1 = \{(1,0),(0,1),(-1,0),(0,-1)\}$
- $X_2 = \{(1,1),(1,-1)(-1,1),(-1,-1)\}$
- $X_3 = \varnothing$
- $X_4 = \{(2,0),(0,2),(-2,0),(0,-2)\}$
- $X_5 = \{(2,1),(1,2),(-2,1),(1,-2),(2,-1),(-1,2),(-2,-1),(-1,-2)\}$
- $X_6 = \varnothing$
- $X_7 = \varnothing$

Note que X_3, X_6 e X_7 são vazios, o que era de se esperar, em vista do Teorema 3.3.

Vamos definir a função s_2 da seguinte forma: $s_2(n) = \#X_n$, ou seja, s_2 é a função que associa um inteiro positivo n a cardinalidade de X_n.

Para calcular $s_2(n)$, basta encontrarmos todos os elementos de X_n, com isso e os exemplos dados acima, podemos concluir que: $s_2(0) = 1$, $s_2(2) = 4$, $s_2(3) = 0$, $s_2(4) = 4$, $s_2(5) = 8$, $s_2(6) = 0$ e $s_2(7) = 0$.

Podemos interpretar $s_2(n)$ como o número de maneiras que um inteiro positivo n pode ser escrito como soma dos quadrados de dois inteiros, contando com a permutação dos números.

Vamos agora provar alguns resultados sobre a função s_2.

Proposição 4.1 $s_2(4k+3) = 0$ para todo k inteiro.

Prova: De fato, como os resíduos quadráticos módulo 4 são 0 e 1, então para dois inteiros x, y só podemos ter $x^2 \equiv 0 \mod 4$ ou $x^2 \equiv 1 \mod 4$ e $y^2 \equiv 0 \mod 4$ ou $y^2 \equiv 1 \mod 4$, ou seja, $x^2 + y^2 \equiv 0 \mod 4$, $x^2 + y^2 \equiv 1 \mod 4$ ou $x^2 + y^2 \equiv 2 \mod 4$.

Como não temos $x^2 + y^2 \equiv 3 \mod 4$ para todos x, y inteiros, concluímos que não existe inteiro k tal que $4k + 3$ possa ser escrito como soma de dois quadrados, daí $s_2(4k+3) = 0$ para todo k inteiro.

■

Teorema 4.2: A função s_2 não é limitada superiormente.

Queremos mostrar que para $m \in \mathbb{Z}_+$ dado, existe $n \in \mathbb{Z}_+$ tal que $s_2(n) > m$.

Através de uma longa inspeção, pode-se perceber a formação de uma conjectura a respeito dos números cujos fatores primos são, somente, da forma $4k + 1$.

Para não estender demasiadamente os cálculos, analisaremos números livres de quadrados cujos fatores primos são 5,13,17 ou 29. Observe:

$$5 = 1^2 + 2^2$$

$$13 = 2^2 + 3^2$$

$$17 = 1^2 + 4^2$$

$$29 = 2^2 + 5^2$$

$$65 = 5 \cdot 13 = 1^2 + 8^2 = 4^2 + 7^2$$

$$85 = 5 \cdot 17 = 2^2 + 9^2 = 6^2 + 7^2$$

$$221 = 13 \cdot 17 = 10^2 + 11^2 = 14^2 + 5^2$$

$$145 = 5 \cdot 29 = 12^2 + 1^2 = 9^2 + 8^2$$

$$377 = 13 \cdot 29 = 19^2 + 4^2 = 16^2 + 11^2$$

$$493 = 17 \cdot 29 = 22^2 + 3^2 = 13^2 + 18^2$$

$$1105 = 5 \cdot 13 \cdot 17 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2$$

$$1885 = 5 \cdot 13 \cdot 29 = 34^2 + 27^2 = 42^2 + 11^2 = 43^2 + 6^2 = 38^2 + 21^2$$

$$2465 = 5 \cdot 17 \cdot 29 = 28^2 + 41^2 = 47^2 + 16^2 = 44^2 + 23^2 = 49^2 + 8^2$$

$$6409 = 13 \cdot 17 \cdot 29 = 53^2 + 60^2 = 72^2 + 35^2 = 80^2 + 3^2 = 75^2 + 28^2$$

$$32045 = 5 \cdot 13 \cdot 17 \cdot 19 = 179^2 + 1^2 = 178^2 + 19^2 = 173^2 + 46^2 = 166^2 + 67^2$$
$$= 163^2 + 74^2 = 157^2 + 86^2 = 142^2 + 109^2 = 131^2 + 122^2.$$

Os cálculos acima nos sugerem que números que são produtos de n primos da forma $4k+1$ distintos podem ser escritos de 2^{n-1} formas como soma de dois quadrados, ou seja, que $s_2(n) = 2^{n+2}$, já que no cálculo de $s_2(n)$ distinguimos $a^2 + b^2$ de $b^2 + a^2$ e também distinguimos $(-a)^2 + b^2$ de $a^2 + b^2$.

Não vamos provar que vale a igualdade, nos restringiremos a provar que

$$s_2(n) \geq 2^{n-1},$$

pois essa desigualdade é suficiente para a prova da proposição.

Prova: Considere o número $m = p_1 \cdot p_2 \cdot ... \cdot p_n$, onde $p_1, p_2, ..., p_n$ são primos distintos da forma $4k + 1$. Afirmamos que m pode ser escrito de pelo menos 2^{n-1} formas como soma dos quadrados de dois inteiros positivos

Vamos provar por indução em n que a última afirmação é verdadeira. O Teorema 3.4 nos garante o caso $n = 1$, já que para todo primo $p = 4k + 1$ existem únicos inteiros positivos $y > x > 0$ tais que $x^2 + y^2 = p$.

Supondo o resultado válido para n, vamos provar que o resultado também vale para $n+1$.

Seja $m = p_1 \cdot p_2 \cdot ... \cdot p_n$, se $s_2(m) \geq 2^{n-1}$, sejam

$$x_1^2 + y_1^2 = x_2^2 + y_2^2 = ... = x_{2^{n-1}}^2 + y_{2^{n-1}}^2$$

2^{n-1} formas de se escrever m como soma de dois quadrados, temos então que $m \cdot p_{n+1}$ pode ser escrito das seguintes formas:

$$(x_1^2 + y_1^2) \cdot p_{n+1} = (x_2^2 + y_2^2) \cdot p_{n+1} = ... = (x_{2^{n-1}}^2 + y_{2^{n-1}}^2) \cdot p_{n+1}.$$

Sejam $a, b \in \mathbb{Z}_+$ tais que $p_{n+1} = a^2 + b^2$, pelo Teorema 3.4, temos que a e b são únicos com essa propriedade.

Agora, temos para todo $i \in \{1, 2, ..., 2^{n-1}\}$ que

$$(x_i^2 + y_i^2) \cdot p_{n+1} = (x_i^2 + y_i^2) \cdot (a^2 + b^2) = (x_i a - y_i b)^2 + (x_i b + y_i a)^2$$

e, que

$$(x_i^2 + y_i^2) \cdot p_{n+1} = (x_i^2 + y_i^2) \cdot (b^2 + a^2) = (x_i b - y_i a)^2 + (x_i a + y_i b)^2.$$

Note que usamos o Lema 3.2 nas últimas igualdades das duas expressões acima.

Vamos provar agora que $x_i a - y_i b \neq x_i b - y_i a$ e que $x_i a - y_i b \neq x_i a + y_i b$.

De fato, se $x_i a - y_i b = x_i b - y_i a$, então $x_i(a-b) = -y_i(a-b)$. Se $a-b = 0$, então $p_{n+1} = 2a^2$, absurdo, pois este é um primo ímpar, daí $x_i = -y_i$, o que é outro absurdo, pois x_i e y_i são inteiros positivos. Agora, se $x_i a - y_i b = x_i a + y_i b$, então $2y_i b = 0$ e daí $y_i = 0$ ou $b = 0$, absurdo, pois m e p_{n+1} não são quadrados perfeitos.

Com os resultados do parágrafo anterior, podemos concluir que $m \cdot p_{n+1}$ possui pelo menos $2 \cdot 2^{n-1} = 2^n$ formas de ser escrito como soma de dois quadrados, ou seja, $s_2(m \cdot p_{n+1}) \geq 2^n$.

Como os primos ímpares da forma $4k+1$ são infinitos, temos como consequência que a função s_2 não é limitada superiormente.

■

Proposição 4.3: Dado n natural, existem n naturais consecutivos $a_1, a_2, ..., a_n$ tais que

$$s_2(a_1) = s_2(a_2) = ... = s_2(a_n) = 0.$$

Prova: Como os primos da forma $4k+3$ são infinitos, sejam $p_1, p_2, ..., p_n$ n primos da forma $4k+3$, pelo Teorema 2.17(Teorema Chinês do Resto), o sistema

$$\begin{cases} x \equiv -1 + p_1 & \mod p_1^2 \\ x \equiv -2 + p_2 & \mod p_2^2 \\ \vdots & \\ x \equiv -n + p_n & \mod p_n^2 \end{cases} \tag{2}$$

tem solução, já que $mdc(p_i^2, p_j^2) = 1$ para $1 \leq i \neq j \leq n$.

Seja x a solução do sistema (2), temos que p_i^2 divide $x + i - p_i$ para todo $1 \leq i \leq n$, daí existe $m_i \in \mathbb{Z}$ tal que $m_i p_i^2 = x + i - p_i$, ou seja, $x + i = m_i p_i^2 + p_i = p_i \cdot (m_i p_i + 1)$, como p_i não divide $m_i p_i + 1$ para todo $1 \leq i \leq n$, temos que o expoente de p_i na fatoração canônica de $x + i$ é 1, ou seja, pelo Teorema 3.3, $s_2(x + i) = 0$ para $1 \leq i \leq n$.

■

4.2 Função s_3

Antes de definir s_3, vamos definir um importante conjunto associado à função.

Seja $Y_n = \{(a, b, c) \in \mathbb{Z}^3; a^2 + b^2 + c^2 = n\}$. Y_n é o conjunto de todos os ternos ordenados com coordenadas inteiras que se elevadas ao quadrado e somadas, resultam em n.

Alguns exemplos são:

- $Y_0 = \{(0,0,0)\}$
- $Y_1 = \{(1,0,0),(-1,0,0),(0,1,0),(0,-1,0),(0,0,1),(0,0,-1)\}$
- $Y_2 = \{(1,1,0),(1,0,1),(0,1,1),(-1,-1,0),(-1,0,-1),(0,-1,-1),$ $(1,-1,0),(-1,1,0),(-1,0,1),(1,0,-1),(0,1,-1),(0,-1,1)\}$
- $Y_3 = \{(1,1,1),(1,1,-1),(1,-1,1),(-1,1,1),(1,-1,-1),$ $(-1,1,-1),(-1,-1,1),(-1,-1,-1)\}$
- $Y_4 = \{(2,0,0),(-2,0,0),(0,2,0),(0,-2,0),(0,0,2),(0,0,-2)\}$

Vamos definir a função s_3 da seguinte forma: $s_3(n) = \#Y_n$, ou seja, s_3 é a função que associa um inteiro positivo n com a cardinalidade de Y_n.

Para calcular $s_3(n)$, basta encontrarmos todos os elementos de Y_n, com isso e os exemplos dados acima, podemos concluir que: $s_3(0) = 1$, $s_3(2) = 6$, $s_3(3) = 8$ e $s_2(4) = 6$.

Podemos interpretar $s_3(n)$ como o número de maneiras que um inteiro positivo n pode ser escrito como soma de três quadrados de inteiros, contando com a permutação dos números.

Vamos agora provar alguns resultados sobre a função s_3.

Teorema 4.4: A função s_3 não é limitada superiormente.

Prova: Como s_2 é ilimitada superiormente, temos que para todo m inteiro positivo, existe k inteiro positivo tal que $s_2(k) > m$, ou seja, o conjunto $X_k = (a,b) \in Z^2; a^2 + b^2 = k$ tem mais que m elementos. Seja (a_i, b_i) um desses elementos, temos que $a_i^2 + b_i^2 = k$, ou seja, $0^2 + a_i^2 + b_i^2 = k$ e portanto $(0, a_i, b_i) \in Y_k$, com isso concluímos que a cardinalidade do conjunto Y_k é maior ou igual a cardinalidade do conjunto X_k, ou seja,

$$s_3(k) \geq s_2(k), \forall k \in Z_+$$

Ora, como s_2 é ilimitada superiormente, temos da desigualdade acima que s_3 também é ilimitada superiormente.

■

Proposição 4.5: Não existem inteiros k, l tais que $l \geq 0$ e $s_3(4^l \cdot (8k+7)) > 0$.

Prova: Vamos provar por indução em l.

Seja $X = \{l \in \mathbb{Z}_+; x^2 + y^2 + z^2 \neq 4^l \cdot (8k+7), \forall x, y, z, k \in \mathbb{Z}\}$.

$0 \in X$, pois os resíduos quadráticos módulo 8 são 0,1 e 4, daí $x^2 + y^2 + z^2$ não pode ser congruente a 7, módulo 8, ou seja, $x^2 + y^2 + z^2$ não pode ser da forma $8k + 7 = 4^0(8k + 7)$, portanto $s_3(8k + 7) = 0$ para todo k inteiro.

Suponha que $n \in X$, $n > 0$, se tivermos inteiros x, y, z e k tais que $x^2 + y^2 + z^2 = 4^{n+1} \cdot (8k + 7)$, então também temos que $x^2 + y^2 + z^2 \equiv 0 \mod 8$, se um entre x, y ou z for ímpar, digamos que seja x, teremos que $x^2 \equiv 1 \mod 8$, logo $y^2 + z^2 \equiv 7 \mod 8$, o que não pode ocorrer, já que $y^2, z^2 \equiv 0, 1, 4 \mod 8$, daí x, y e z são pares e portanto existem a, b e c inteiros tais que $x = 2a, y = 2b$ e $z = 2c$, daí, de $x^2 + y^2 + z^2 = 4^{n+1} \cdot (8k+7)$ temos $4a^2 + 4b^2 + 4c^2 = 4^{n+1} \cdot (8k+7)$ e, portanto, $a^2 + b^2 + c^2 = 4^n \cdot (8k+7)$, o que é absurdo, pois $n \in X$, logo $n+1 \in X$ e portanto

$$X = \mathbb{Z}_+.$$

Da última igualdade podemos concluir nossa tese.

■

5 O NÚMERO MÉDIO DE REPRESENTAÇÕES DE UM INTEIRO POSITIVO COMO SOMA DE DOIS QUADRADOS

Nesta seção temos como objetivo determinar um interessante limite que envolve a função aritmética s_2, para tanto, considere a sequência

$$\alpha = (s_2(0), s_2(1), s_2(2), s_2(3), ...)$$

Vimos na seção anterior que $s_2(4k+3) = 0$ para todo k inteiro e que s_2 é ilimitada superiormente. Unindo esses dois fatos, podemos notar que α é uma sequência bastante irregular, pois cresce arbitrariamente e, também, volta a zero periodicamente.[1]

Apesar do comportamento caótico de α não nos indicar muito, se definirmos a função

$$S_2(z) = s_2(0) + s_2(1) + s_2(2) + ... + s_2(z-1)$$

ao analisarmos a sequência

$$\alpha' = \left(\frac{S_2(1)}{1}, \frac{S_2(2)}{2}, \frac{S_2(3)}{3}, \frac{S_2(4)}{4}, ...\right)$$

podemos ver que ela vai oscilando em torno de um número a medida que z cresce e que esse número, surpreendentemente, é π.[2]

Vamos à prova do resultado.

No plano cartesiano considere o círculo $C(\sqrt{z}) : x^2 + y^2 = z$ de centro $(0,0)$ e raio $\sqrt{z}$. Chamaremos de ponto de rede todo ponto $P = (a,b)$ tal que a e b sejam números inteiros, temos que todo ponto de rede interior a $C(\sqrt{z})$ tem coordenadas satisfazendo a inequação $a^2 + b^2 < z$, pois a distância de P até a origem é menor do que o raio de $C(\sqrt{z})$, ou seja: $\sqrt{a^2+b^2} < \sqrt{z}$.

Além disso, como a e b são inteiros, $n = a^2 + b^2$ também é inteiro e daí o par ordenado (a,b) nos dá uma expressão para n como a soma dos quadrados de dois inteiros: $a^2 + b^2 = n < z$.

[1] No apêndice A encontra-se os cem primeiros valores de α.
[2] No apêndice A encontra-se os cem primeiros valores de α'.

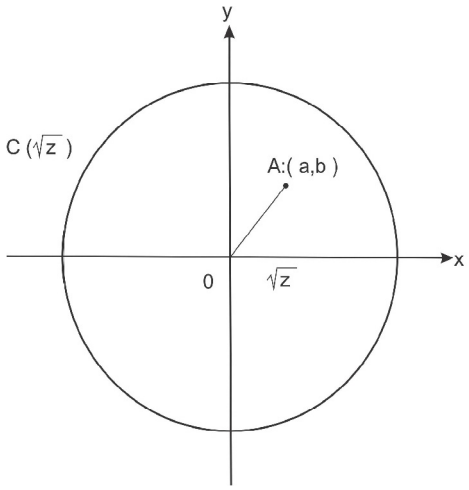


Figura 1: O círculo $C\left(\sqrt{z}\right)$

Cada ponto de rede dentro de $C(\sqrt{z})$ contribui em 1 para a soma

$$S_2(z) = s_2(0) + s_1(1) + s_2(2) + ... + s_2(z-1)$$

uma vez que cada ponto (x, y) desses é tal que $x^2 + y^2 = n$ para algum $n \in \{0, 1, 2, ..., z-1\}$.

Reciprocamente, todo par de inteiros (p, q) tal que $p^2 + q^2 = n < z$, isto é, todo par ordenado contado em $S_2(z)$ deverá ser um ponto de rede dentro de $C(\sqrt{z})$, consequentemente, $S_2(z)$ é igual ao número de pontos de rede interiores a $C(\sqrt{z})$.

Agora, em torno de cada ponto de rede $P = (a, b)$ no plano, considere um quadrado de lado 1 e centro P, conforme a Figura 2. Nos é interessante diferenciar os quadrados cujo centro é um ponto de rede interior a $C(\sqrt{z})$, para tanto, vamos colorir tais quadrados de azul e todos os outros de vermelho, consequentemente, a maior parte do interior de $C(\sqrt{z})$ é azul e a maior parte de seu exterior é vermelha, conforme a Figura 3.

Observe que alguns quadrados azuis se projetam para fora de $C(\sqrt{z})$, enquanto alguns quadrados vermelhos fazem justamente o contrário.

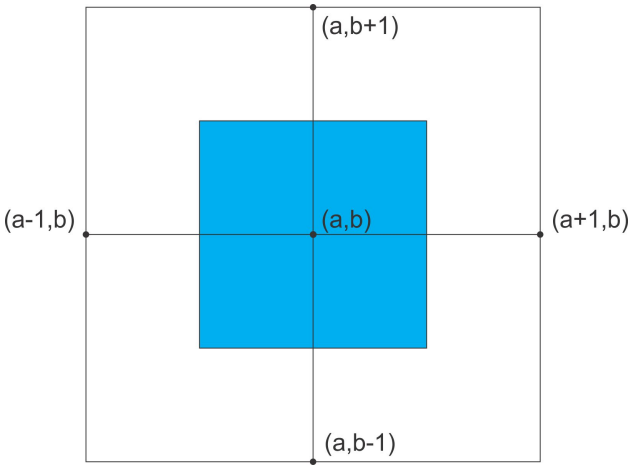


Figura 2: Quadrado azul em torno do ponto de rede (a, b)

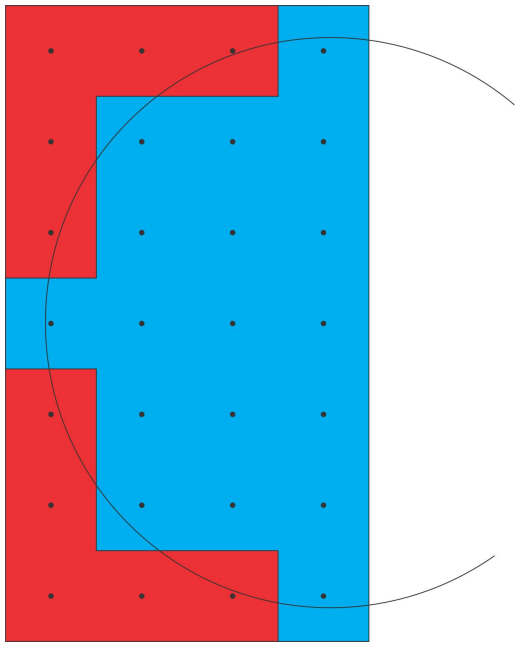


Figura 3: Área azul e $C\left(\sqrt{z}\right)$

Como o número de quadrados azuis é igual ao número de pontos de rede dentro de $C(\sqrt{z})$, que por sua vez é igual a $S_2(z)$ e como cada quadrado tem área 1, concluímos que $S_2(z)$ é igual a área do polígono formado pelos

quadrados azuis, que denotaremos por A, assim $S_2(z) = A$. Ou seja, nosso trabalho se resume a calcular o valor de A.

Se Q é um ponto de rede exterior a $C(\sqrt{z})$ ou sobre $C(\sqrt{z})$, e se R é qualquer ponto pertencente ao quadrado de centro Q, então $\overline{OQ} \geq \sqrt{z}$ e $\overline{RQ} \leq \frac{1}{\sqrt{2}}$. Pela desigualdade triangular temos $\overline{OR} + \overline{RQ} \geq \overline{OQ}$, logo

$$\overline{OR} \geq \overline{OQ} - \overline{RQ} \geq \sqrt{z} - \frac{1}{\sqrt{2}}$$

ou seja, não existem pontos pertencentes a quadrados vermelhos dentro do círculo $C(\sqrt{z} - \frac{1}{\sqrt{2}})$ de centro na origem e raio $\sqrt{z} - \frac{1}{\sqrt{2}}$.

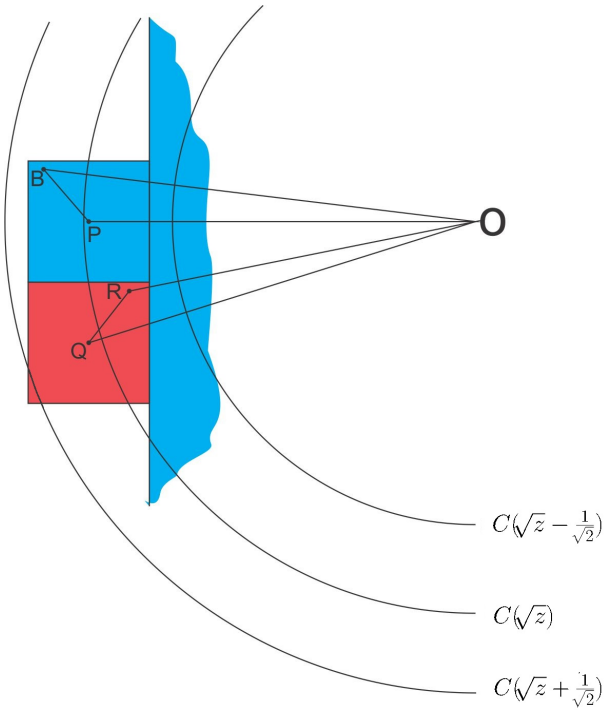


Figura 4: $C\left(\sqrt{z}\right)$, $C\left(\sqrt{z} + \frac{1}{\sqrt{2}}\right)$ e $C\left(\sqrt{z} - \frac{1}{\sqrt{2}}\right)$

Analogamente, seja B um ponto pertencente a um quadrado azul cujo centro é o ponto de rede P, temos que $\overline{OP} < \sqrt{z}$ e $\overline{PB} \leq \frac{1}{\sqrt{2}}$, logo

$$\overline{OB} \leq \overline{OP} + \overline{PB} < \sqrt{z} + \frac{1}{\sqrt{2}}$$

de forma que nenhum ponto pertencente a um quadrado azul é exterior ou pertencente ao círculo $C\left(\sqrt{z} + \frac{1}{\sqrt{2}}\right)$ de centro na origem e raio $\sqrt{z} + \frac{1}{\sqrt{2}}$.

Como todo ponto de $C\left(\sqrt{z} - \frac{1}{\sqrt{2}}\right)$ é interior ao polígono formado pelos quadrados azuis, podemos concluir que A é maior do que a área de $C\left(\sqrt{z} - \frac{1}{\sqrt{2}}\right)$, além disso, como nenhum ponto de um quadrado azul é externo a $C\left(\sqrt{z} + \frac{1}{\sqrt{2}}\right)$, podemos concluir que A é menor do que a área de $C\left(\sqrt{z} + \frac{1}{\sqrt{2}}\right)$. Juntando esses dois fatos, temos que:

$$\pi \cdot \left(\sqrt{z} - \frac{1}{\sqrt{2}}\right)^2 < A = S_2(z) < \pi \cdot \left(\sqrt{z} + \frac{1}{\sqrt{2}}\right)^2$$

$$\Rightarrow \pi \cdot \left(z - \sqrt{2z} + \frac{1}{2}\right) < S_2(z) < \pi \cdot \left(z + \sqrt{2z} + \frac{1}{2}\right)$$

$$\Rightarrow \pi z - \pi \cdot \sqrt{2z} + \frac{\pi}{2} < S_2(z) < \pi z + \pi \cdot \sqrt{2z} + \frac{\pi}{2}$$

$$\Rightarrow \frac{\pi}{2} - \pi \cdot \sqrt{2z} < S_2(z) - \pi z < \frac{\pi}{2} + \pi \cdot \sqrt{2z}$$

$$\Rightarrow \frac{\pi}{2z} - \frac{\pi \cdot \sqrt{2}}{\sqrt{z}} < \frac{S_2(z)}{z} - \pi < \frac{\pi}{2z} + \frac{\pi \cdot \sqrt{2}}{\sqrt{z}}$$

$$\Rightarrow \lim_{z \to +\infty} \frac{\pi}{2z} - \frac{\pi \cdot \sqrt{2}}{\sqrt{z}} \leq \lim_{z \to +\infty} \frac{S_2(z)}{z} - \pi \leq \lim_{z \to +\infty} \frac{\pi}{2z} + \frac{\pi \cdot \sqrt{2}}{\sqrt{z}}$$

$$\Rightarrow 0 \leq \lim_{z \to +\infty} \frac{S_2(z)}{z} - \pi \leq 0$$

$$\Rightarrow \lim_{z \to +\infty} \frac{S_2(z)}{z} - \pi = 0$$

$$\Rightarrow \lim_{z \to +\infty} \frac{S_2(z)}{z} = \pi$$

Com o último limite acima, podemos concluir que um inteiro positivo n tem, em média, π representações como soma dos quadrados de dois inteiros.

6 O NÚMERO MÉDIO DE REPRESENTAÇÕES DE UM INTEIRO POSITIVO COMO SOMA DE TRÊS QUADRADOS

Em vista do que vimos na seção 4, é natural se perguntar se existe um número médio de representações de um inteiro positivo como soma de três quadrados, ou seja, se o limite

$$\lim_{k \to +\infty} \frac{S_3(k)}{k} = L \tag{3}$$

existe para algum $L \in \mathbb{R}$. Nosso objetivo nesta seção é responder essa pergunta.

Para tanto, vamos fazer agora um resultado análogo ao que vimos na seção anterior. Faremos s_3 exercer o papel que s_2 exerceu, usaremos o espaço euclidiano tridimensional ao invés do plano cartesiano e seguiremos os mesmos passos, com as devidas adaptações, que seguimos na seção anterior.

Seja $E(\sqrt{k})$ a esfera de centro $O = (0,0,0)$ e raio $\sqrt{k}$, sua equação é

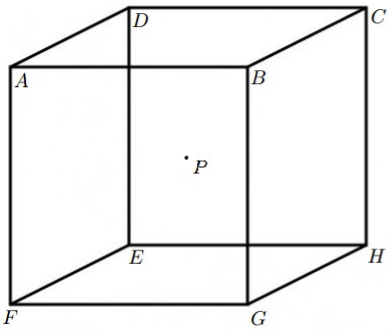
$$x^2 + y^2 + z^2 = k$$

Seja $S_3(k) = s_3(0) + s_3(1) + ... + s_3(k-1)$, vamos associar essa função a $E(\sqrt{k})$.

Vamos chamar de ponto de rede $3D$ todo terno $P = (a,b,c) \in \mathbb{Z}^3$ e por um cubo de aresta 1 centrado em cada ponto de rede $3D$ como indicado na Figura 6.

Temos que $S_3(k)$ equivale ao volume do sólido formado pelos cubos centrados em pontos de rede $3D$ interiores a $E(\sqrt{k})$.

De fato, se $P = (a,b,c) \in Y_l$ para $l < k$, então $a^2 + b^2 + c^2 = l < k$ e, daí, $d(P,O) = \sqrt{a^2 + b^2 + c^2} = \sqrt{l} < \sqrt{k}$, ou seja, P é um ponto de rede $3D$ interior a $E(\sqrt{k})$.



$A = (a - \frac{1}{2}, b + \frac{1}{2}, c + \frac{1}{2})$ $E = (a - \frac{1}{2}, b - \frac{1}{2}, c - \frac{1}{2})$

$B = (a + \frac{1}{2}, b + \frac{1}{2}, c + \frac{1}{2})$ $F = (a - \frac{1}{2}, b + \frac{1}{2}, c - \frac{1}{2})$

$C = (a + \frac{1}{2}, b - \frac{1}{2}, c + \frac{1}{2})$ $G = (a + \frac{1}{2}, b + \frac{1}{2}, c - \frac{1}{2})$

$D = (a - \frac{1}{2}, b - \frac{1}{2}, c + \frac{1}{2})$ $H = (a + \frac{1}{2}, b - \frac{1}{2}, c - \frac{1}{2})$

Figura 5: Cubo em torno de um ponto de rede $3D$

Agora, se $P = (a, b, c)$ é um ponto de rede $3D$ interior a $E(\sqrt{k})$, então $a, b, c \in \mathbb{Z}$ e $d(P, O) = \sqrt{a^2 + b^2 + c^2} < \sqrt{k}$, ou seja, $a^2 + b^2 + c^2$ é um número inteiro l menor do que k, logo $P \in Y_l$ e portanto P contribui em um no valor de $S_3(k)$.

Vamos colorir de azul os cubos centralizados em pontos de rede $3D$ interiores a $E(\sqrt{k})$ e de vermelho os cubos centralizados em pontos de rede $3D$ exteriores ou sobre $E(\sqrt{k})$. Dessa forma, o cálculo de $S_3(k)$ se resume a calcular o volume V do sólido formado pelos cubos azuis.

Seja C_1 o centro de um cubo azul e P um ponto pertencente a esse cubo, temos que $\overline{OC_1} < \sqrt{k}$ e $\overline{PC_1} \leq \frac{\sqrt{3}}{2}$, pois a máxima distância de um ponto interior a um cubo de aresta 1 para seu centro é $\frac{\sqrt{3}}{2}$.

Pela desigualdade triangular, temos:

$$\overline{OP} < \overline{OC_1} + \overline{PC_1} < \sqrt{k} + \frac{\sqrt{3}}{2}$$

ou seja, P é interior à esfera $E\left(\sqrt{k} + \frac{\sqrt{3}}{2}\right)$. Como P é um ponto arbitrário de um cubo azul, podemos concluir que V é menor do que o volume da esfera $E\left(\sqrt{k} + \frac{\sqrt{3}}{2}\right)$.

Seja C_2 o centro de um cubo vermelho e Q um ponto pertencente a esse cubo, temos que $\overline{OC_2} \geq \sqrt{k}$ e $\overline{QC_2} \leq \frac{\sqrt{3}}{2}$.

Pela desigualdade triangular, temos

$$\overline{OQ} > \overline{OC_2} - \overline{QC_2} \geq \sqrt{k} - \frac{\sqrt{3}}{2}$$

ou seja, Q é exterior à esfera $E\left(\sqrt{k} - \frac{\sqrt{3}}{2}\right)$. Como Q é um ponto arbitrário de um cubo vermelho, podemos concluir que a esfera $E\left(\sqrt{k} - \frac{\sqrt{3}}{2}\right)$ está completamente contida no sólido formado pelos cubos azuis, logo seu volume é menor do que V.

Juntando as desigualdades obtidas acima, temos a seguinte relação entre os volumes das esferas e $S_3(k)$:

$$\frac{4\pi}{3} \cdot \left(\sqrt{k} - \frac{\sqrt{3}}{2}\right)^3 < S_3(k) = V < \frac{4\pi}{3} \cdot \left(\sqrt{k} + \frac{\sqrt{3}}{2}\right)^3$$

$$\Rightarrow \frac{4\pi}{3} \cdot \left(k \cdot \sqrt{k} - 3k\frac{\sqrt{3}}{2} + \frac{9 \cdot \sqrt{k}}{4} - \frac{3 \cdot \sqrt{3}}{8}\right) < S_3(k) < \frac{4\pi}{3} \cdot \left(k \cdot \sqrt{k} + 3k\frac{\sqrt{3}}{2} + \frac{9 \cdot \sqrt{k}}{4} + \frac{3 \cdot \sqrt{3}}{8}\right)$$

$$\Rightarrow \frac{4\pi}{3}k\sqrt{k} - 2\sqrt{3}\pi k + 3\pi\sqrt{k} - \frac{\pi \cdot \sqrt{3}}{2} < S_3(k) < \frac{4\pi}{3}k\sqrt{k} + 2\sqrt{3}\pi k + 3\pi\sqrt{k} + \frac{\pi \cdot \sqrt{3}}{2}$$

$$\Rightarrow 3\pi \cdot \sqrt{k} - 2 \cdot \sqrt{3}\pi k - \frac{\pi \cdot \sqrt{3}}{2} < S_3(k) - \frac{4\pi}{3}k \cdot \sqrt{k} < 3\pi \cdot \sqrt{k} + 2 \cdot \sqrt{3}\pi k + \frac{\pi \cdot \sqrt{3}}{2}$$

$$\Rightarrow \frac{3\pi}{k} - \frac{2 \cdot \sqrt{3}\pi}{\sqrt{k}} - \frac{\pi \cdot \sqrt{3}}{2k \cdot \sqrt{k}} < \frac{S_3(k)}{k \cdot \sqrt{k}} - \frac{4\pi}{3} < \frac{3\pi}{k} + \frac{2 \cdot \sqrt{3}\pi}{\sqrt{k}} + \frac{\pi \cdot \sqrt{3}}{2k \cdot \sqrt{k}}$$

$$\Rightarrow \lim_{k \to +\infty} \frac{3\pi}{k} - \frac{2 \cdot \sqrt{3}\pi}{\sqrt{k}} - \frac{\pi \cdot \sqrt{3}}{2k \cdot \sqrt{k}} \leq \lim_{k \to +\infty} \frac{S_3(k)}{k \cdot \sqrt{k}} - \frac{4\pi}{3} \leq \lim_{k \to +\infty} \frac{3\pi}{k} + \frac{2 \cdot \sqrt{3}\pi}{\sqrt{k}} + \frac{\pi \cdot \sqrt{3}}{2k \cdot \sqrt{k}}$$

$$\Rightarrow 0 \leq \lim_{k \to +\infty} \frac{S_3(k)}{k \cdot \sqrt{k}} - \frac{4\pi}{3} \leq 0$$

$$\Rightarrow \lim_{k \to +\infty} \frac{S_3(k)}{k \cdot \sqrt{k}} - \frac{4\pi}{3} = 0$$

$$\Rightarrow \lim_{k \to +\infty} \frac{S_3(k)}{k \cdot \sqrt{k}} = \frac{4\pi}{3}. \tag{4}$$

Para a pergunta feita no começo da seção, a respeito de (3), vamos provar que a resposta para ela é não. Para isso, suponha que L exista, como $\lim_{k\to+\infty} \frac{1}{\sqrt{k}} = 0$, temos que

$$\lim_{k\to+\infty} \frac{S_3(k)}{k\cdot\sqrt{k}} = \left(\lim_{k\to+\infty} \frac{S_3(k)}{k}\right)\cdot\left(\lim_{k\to+\infty}\frac{1}{\sqrt{k}}\right) = L\cdot 0 = 0$$

o que é absurdo, em vista de (4).

7 CONCLUSÃO

Neste trabalho, enunciamos e demonstramos os principais teoremas a respeito de congruências e somas de quadrados, definimos as funções s_2 e s_3, demonstramos que, em média, o número de representações de um inteiro positivo como soma dos quadrados de dois inteiros é π e, por fim, definimos e provamos que não existe o número médio de representações de um inteiro positivo como soma dos quadrados de três inteiros.

Além desses resultados, ao demonstrarmos o limite (4), não somente provamos que não existe o número médio de representações de um inteiro positivo como soma de três quadrados, também descobrimos que a função S_3 tem mesma magnitude que a função $f(k) = k \cdot \sqrt{k}$.

Com base no que foi feito neste trabalho, considere as funções s_k e S_k, onde k é um número natural, definidas de forma análoga as funções s_2 e S_2. É fácil provar que s_k é ilimitada superiormente, e que, por isso, o número médio de representações de um inteiro positivo como soma de k quadrados não existe. Todavia, o que se pode dizer sobre a magnitude de S_k? Existe um resultado análogo ao limite (4)?

REFERÊNCIAS

HEFEZ, A. **Aritmética**. Rio de Janeiro: SBM, 2013.

HONSBERGER, R. **Ingenuity in Mathematics**. Random House: Singer School Division, 1970.

MUNIZ NETO, A. C. **Tópicos de Matemática Elementar: teoria dos números- 2.ed.** Rio de Janeiro: SBM, 2012.

SANTOS, J. P. **Introdução à Teoria dos Números 3ed.** Rio de Janeiro: IMPA, 2011.

APÊNDICE A - TABELAS DE VALORES

Neste apêndice veremos os cem primeiros valores de $s_2(n)$ e também os cem primeiros termos da sequência α', o objetivo aqui é convencer, mesmo que por empirismo, o leitor de que α' converge para π.

Os cem primeiros valores de $s_2(n)$ são:

$s_2(0) = 1$	$s_2(1) = 4$	$s_2(2) = 4$	$s_2(3) = 0$	$s_2(4) = 4$
$s_2(5) = 8$	$s_2(6) = 0$	$s_2(7) = 0$	$s_2(8) = 4$	$s_2(9) = 4$
$s_2(10) = 8$	$s_2(11) = 0$	$s_2(12) = 0$	$s_2(13) = 8$	$s_2(14) = 0$
$s_2(15) = 0$	$s_2(16) = 4$	$s_2(17) = 8$	$s_2(18) = 4$	$s_2(19) = 0$
$s_2(20) = 8$	$s_2(21) = 0$	$s_2(22) = 0$	$s_2(23) = 0$	$s_2(24) = 0$
$s_2(25) = 12$	$s_2(26) = 8$	$s_2(27) = 0$	$s_2(28) = 0$	$s_2(29) = 8$
$s_2(30) = 0$	$s_2(31) = 0$	$s_2(32) = 4$	$s_2(33) = 0$	$s_2(34) = 8$
$s_2(35) = 0$	$s_2(36) = 4$	$s_2(37) = 8$	$s_2(38) = 0$	$s_2(39) = 0$
$s_2(40) = 8$	$s_2(41) = 8$	$s_2(42) = 0$	$s_2(43) = 0$	$s_2(44) = 0$
$s_2(45) = 8$	$s_2(46) = 0$	$s_2(47) = 0$	$s_2(48) = 0$	$s_2(49) = 4$
$s_2(50) = 12$	$s_2(51) = 0$	$s_2(52) = 8$	$s_2(53) = 8$	$s_2(54) = 0$
$s_2(55) = 0$	$s_2(56) = 0$	$s_2(57) = 0$	$s_2(58) = 8$	$s_2(59) = 0$
$s_2(60) = 0$	$s_2(61) = 8$	$s_2(62) = 0$	$s_2(63) = 0$	$s_2(64) = 4$
$s_2(65) = 16$	$s_2(66) = 0$	$s_2(67) = 0$	$s_2(68) = 8$	$s_2(69) = 0$
$s_2(70) = 0$	$s_2(71) = 0$	$s_2(72) = 4$	$s_2(73) = 8$	$s_2(74) = 8$
$s_2(75) = 0$	$s_2(76) = 0$	$s_2(77) = 0$	$s_2(78) = 0$	$s_2(79) = 0$
$s_2(80) = 8$	$s_2(81) = 4$	$s_2(82) = 8$	$s_2(83) = 0$	$s_2(84) = 0$
$s_2(85) = 16$	$s_2(86) = 0$	$s_2(87) = 0$	$s_2(88) = 0$	$s_2(89) = 8$
$s_2(90) = 8$	$s_2(91) = 0$	$s_2(92) = 0$	$s_2(93) = 0$	$s_2(94) = 0$
$s_2(95) = 0$	$s_2(96) = 0$	$s_2(97) = 8$	$s_2(98) = 4$	$s_2(99) = 0$

Tabela 1: Valores de $s_2(n)$

Por simplicidade, aqui denotaremos $\frac{S_2(n)}{n}$ por a_n.

Os cem primeiros termos de α' são:

$a_0 = 1$	$a_1 = 2,5$	$a_2 = 3$	$a_3 = 2,25$
$a_4 = 2,6$	$a_5 = 3,5$	$a_6 = 3$	$a_7 = 2,625$
$a_8 = 2,7778$	$a_9 = 2,9$	$a_{10} = 3,36364$	$a_{11} = 3,08333$
$a_{12} = 2,84615$	$a_{13} = 3,42857$	$a_{14} = 3$	$a_{15} = 2,81250$
$a_{16} = 2,88235$	$a_{17} = 3,16667$	$a_{18} = 3,21053$	$a_{19} = 3,05$
$a_{20} = 3,28571$	$a_{21} = 3,13636$	$a_{22} = 3$	$a_{23} = 2,875$
$a_{24} = 2,76$	$a_{25} = 3,11538$	$a_{26} = 3,2963$	$a_{27} = 3,17857$
$a_{28} = 3,06897$	$a_{29} = 3,23333$	$a_{30} = 3,12903$	$a_{31} = 3,03125$
$a_{32} = 3,06061$	$a_{33} = 2,97059$	$a_{34} = 3,11429$	$a_{35} = 3,02778$
$a_{36} = 3,05405$	$a_{37} = 3,18421$	$a_{38} = 3,10256$	$a_{39} = 3,025$
$a_{40} = 3,14634$	$a_{41} = 3,2691$	$a_{42} = 3,18605$	$a_{43} = 3,11364$
$a_{44} = 3,04444$	$a_{45} = 3,15217$	$a_{46} = 3,08511$	$a_{47} = 3,02083$
$a_{48} = 2,95918$	$a_{49} = 2,98$	$a_{50} = 3,15686$	$a_{51} = 3,09615$
$a_{52} = 3,18868$	$a_{53} = 3,27778$	$a_{54} = 3,21818$	$a_{55} = 3,16071$
$a_{56} = 3,10526$	$a_{57} = 3,05172$	$a_{58} = 3,13559$	$a_{59} = 3,08333$
$a_{60} = 3,03279$	$a_{61} = 3,11290$	$a_{62} = 3,06349$	$a_{63} = 3,01563$
$a_{64} = 3,03077$	$a_{65} = 3,22727$	$a_{66} = 3,1791$	$a_{67} = 3,13235$
$a_{68} = 3,2029$	$a_{69} = 3,15714$	$a_{70} = 3,11268$	$a_{71} = 3,06944$
$a_{72} = 3,08219$	$a_{73} = 3,14865$	$a_{74} = 3,21333$	$a_{75} = 3,17105$
$a_{76} = 3,12987$	$a_{77} = 3,08974$	$a_{78} = 3,05063$	$a_{79} = 3,01250$
$a_{80} = 3,07407$	$a_{81} = 3,08537$	$a_{82} = 3,14458$	$a_{83} = 3,10714$
$a_{84} = 3,07059$	$a_{85} = 3,22093$	$a_{86} = 3,18391$	$a_{87} = 3,14773$
$a_{88} = 3,11236$	$a_{89} = 3,16667$	$a_{90} = 3,21978$	$a_{91} = 3,18478$
$a_{92} = 3,15054$	$a_{93} = 3,11702$	$a_{94} = 3,08421$	$a_{95} = 3,05208$
$a_{96} = 3,02062$	$a_{97} = 3,07143$	$a_{98} = 3,08081$	$a_{99} = 3,05$

Tabela 2: Termos da sequência α'

APÊNDICE B - RESULTADOS COMPLEMENTARES

Nesta seção enunciaremos diversos teoremas que, de algum modo, servem de base para os conceitos elaborados no texto principal.

Princípio da boa ordenação: Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Princípio da indução finita: Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que

- $a \in S$.
- Para todo n inteiro, $n \in S \Rightarrow n+1 \in S$.

Então, $\{x \in \mathbb{Z}; x \geq a\} \in S$.

Binômio de Newton: Sendo n um número natural e a, b reais, temos:

$$(a+b)^n = \binom{n}{0} \cdot a^n + \binom{n}{1} \cdot a^{n-1} \cdot b + \binom{n}{2} \cdot a^{n-2} \cdot b^2 + ... + \binom{n}{n} \cdot b^n.$$

Princípio das gavetas: Se $n+1$ ou mais objetos são colocados em n ou menos gavetas, então pelo menos uma gaveta recebe mais de um objeto.

Princípio fundamental da contagem: Um evento que ocorre em n situações independentes e sucessivas, tendo a primeira situação ocorrendo de m_1 maneiras, a segunda situação ocorrendo de m_2 maneiras e assim sucessivamente até a n-ésima situação ocorrendo de m_n maneiras, temos que o número total de ocorrências para o evento será dado pelo produto:

$$m_1 \cdot m_2 \cdot ... \cdot m_n.$$

Desigualdade triangular: Dado um triângulo cujos lados medem a, b e c, tem-se que:

- $a < b + c$
- $b < a + c$
- $c < a + b$

Resolução de uma equação diofantina de primeira ordem: Sejam a, b e c números inteiros não nulos dados. A equação $ax + by = c$ admite soluções $x, y \in \mathbb{Z}$ se, e só se, $d|c$, onde $d = mdc(a, b)$. Nesse caso, se $x = x_0$ e $y = y_0$ for uma solução inteira qualquer da equação, então as fórmulas

$$x = x_0 + \frac{bt}{d}, y = y_0 + \frac{at}{d},$$

$t \in \mathbb{Z}$, dão todas as soluções inteiras possíveis. Em particular, podemos supor que seja $x > 0 > y$ ou, ainda $x < 0 < y$.

APÊNDICE C - TEOREMA DOS QUATRO QUADRADOS

Nesta seção provaremos o Teorema dos Quatro Quadrados, ou seja, mostraremos que todo inteiro positivo pode ser escrito como soma de quatro quadrados. Para tanto, precisaremos dos seguintes lemas:

Lema 1: Se m e n são naturais que podem ser escritos como soma de quatro quadrados, então o produto $m \cdot n$ também pode ser escrito como soma de quatro quadrados.

Prova: Sejam $m = a^2 + b^2 + c^2 + d^2$ e $n = w^2 + x^2 + y^2 + z^2$, temos que:

$$m \cdot n = (a^2 + b^2 + c^2 + d^2) \cdot (w^2 + x^2 + y^2 + z^2) =$$
$$(aw)^2 + (ax)^2 + (ay)^2 + (az)^2 + (bw)^2 + (bx)^2 + (by)^2 + (bz)^2 +$$
$$(cw)^2 + (cx)^2 + (cy)^2 + (cz)^2 + (dw)^2 + (dx)^2 + (dy)^2 + (dz)^2.$$

Por outro lado, temos que:

$$(aw - bx - cy - dz)^2 = (aw - bx - cy - dz) \cdot (aw - bx - cy - dz)$$
$$= (aw)^2 - awbx - awcy - awdz - awbx + (bx)^2 + bxcy + bxdz -$$
$$awcy + cybx + (cy)^2 + cydz - awdz + bxdz + dzcy + (dz)^2,$$

$$(ax + bw + cz - dy)^2 = (ax + bw + cz - dy) \cdot (ax + bw + cz - dy)$$
$$= (ax)^2 + axbw + axcz - axdy + bwax + (bw)^2 + bwcz - bwdy +$$
$$czax + czbw + (cz)^2 - czdy - axdy - bwdy - czdy + (dy)^2,$$

$$(ay - bz + cw + dx)^2 = (ay - bz + cw + dx) \cdot (ay - bz + cw + dx)$$
$$= (ay)^2 - aybz + aycw + aydx - bzay + (bz)^2 - bzcw - bzdx +$$
$$cway - cwbz + (cw)^2 + cwdx + dxay - dxbz + dxcw + (dx)^2$$

e, por fim:

$$(az + by - cx + dw)^2 = (az + by - cx + dw) \cdot (az + by - cx + dw)$$
$$= (az)^2 + azby - azcx + azdw + byaz + (by)^2 - bycx + bydw -$$
$$cxaz - cxby + (cx)^2 - cxdw + dwaz + dwby - cxdw + (dw)^2.$$

Somando os quatro quadrados acima, ocorrerão diversos cancelamentos e então obteremos que:

$$(aw-bx-cy-dz)^2+(ax+bw+cz-dy)^2+$$

$$(ay-bz+cw+dx)^2+(az+by-cx+dw)^2$$

$$=(aw)^2+(ax)^2+(ay)^2+(az)^2+(bw)^2+(bx)^2+(by)^2+(bz)^2+$$

$$(cw)^2+(cx)^2+(cy)^2+(cz)^2+(dw)^2+(dx)^2+(dy)^2+(dz)^2=m\cdot n.$$

■

Lema 2: Dado p primo, existe um par de inteiros positivos a, b que satisfazem $a^2+b^2 \equiv -1 \mod p$.

Prova: Sejam $x, y \in \{0, 1, ..., \frac{p-1}{2}\}$ com $x > y$. Temos, pela Proposição 2.21, que os quadrados x^2 e y^2 são incongruentes módulo p, assim, o conjunto $A = \{0^2, 1^2, ..., \left(\frac{p-1}{2}\right)^2\}$ tem todos seus elementos incongruentes módulo p, o mesmo ocorre com o conjunto $B = \{-0^2, -1^2, ..., -\left(\frac{p-1}{2}\right)^2\}$ e também com o conjunto $C = \{-1-0^2, -1-1^2, ..., -1-\left(\frac{p-1}{2}\right)^2\}$.

A e C possuem $\frac{p+1}{2}$ elementos, como só existem p possíveis restos na divisão por p, pelo principio das gavetas, pelo menos um dos elementos de A deixa o mesmo resto na divisão por p que algum dos elementos de C , ou seja, existem a, b inteiros positivos tais que $a^2 \equiv -1-b^2 \mod p$.

■

Teorema: Todo inteiro pode ser escrito como uma soma de quatro quadrados.

Prova: Como $2 = 1^2+1^2+0^2+0^2$ e como o Lema 1 garante que o produto de dois números que podem ser escritos como uma soma de quatro quadrados também pode ser escrito como uma soma de quatro quadrados, nos basta mostrar que todo primo ímpar pode ser escrito como soma de quatro quadrados.

Dado p primo ímpar, pelo Lema 2 existem $x, y \in \mathbb{Z}_+$ tais que

$$x^2 \equiv -(1 + y^2) \mod p,$$

ou seja, existe $m \geq 1$ inteiro tal que $mp = x^2 + y^2 + 1$, ora, isso nos diz que mp pode ser escrito como $x^2 + y^2 + 1^2 + 0^2$, uma soma de quatro quadrados. Considere o conjunto A dos inteiros positivos k tais que kp pode ser escrito como soma de quatro quadrados. $m \in A$, logo A é não vazio, portanto, pelo princípio da boa ordenação, existe um elemento $b \in A$ que é mínimo.

Sejam $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ tais que $bp = a_1^2 + a_2^2 + a_3^2 + a_4^2$, podemos tomar $a_1, a_2, a_3, a_4 \in [0, \frac{p}{2})$, pois todo número $v \in \mathbb{Z}$ é tal que v^2 é congruente, módulo p, a um elemento de $\{0^2, 1^2, 2^2, ..., (\frac{p-1}{2})^2\}$.

De $a_1 < \frac{p}{2}, a_2 < \frac{p}{2}, a_3 < \frac{p}{2}$ e $a_4 < \frac{p}{2}$, temos que $a_1^2 < \frac{p^2}{4}, a_2^2 < \frac{p^2}{4}, a_3^2 < \frac{p^2}{4}$ e $a_4^2 < \frac{p^2}{4}$, logo $a_1^2 + a_2^2 + a_3^2 + a_4^2 < p^2$, daí $bp < p^2$ e portanto $b < p$.

Vamos mostrar que b não pode ser maior do que 1.

Se b for par, então bp também é par, logo $a_1^2 + a_2^2 + a_3^2 + a_4^2$ é a soma de quatro pares ou a soma de quatro ímpares ou a soma de dois pares e de dois ímpares, ou seja, os números a_1, a_2, a_3, a_4 são todos pares ou todos ímpares ou dois deles são pares enquanto os outros dois são ímpares. Em todo caso, podemos supor, sem perda de generalidade, que $a_1 \equiv a_2 \mod 2$ e $a_3 \equiv a_4 \mod 2$.

De $a_1^2 + a_2^2 + a_3^2 + a_4^2 = bp$ temos que

$$\frac{bp}{2} = \frac{a_1^2 + a_2^2 + a_3^2 + a_4^2}{2} = \frac{2 \cdot (a_1^2 + a_2^2) + 2 \cdot (a_3^2 + a_4^2)}{4} =$$

$$\frac{a_1^2 + 2a_1a_2 + a_2^2 + a_1^2 - 2a_1a_2 + a_2^2 + a_3^2 + 2a_3a_4 + a_4^2 + a_3^2 - 2a_3a_4 + a_4^2}{4} =$$

$$\left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2$$

ou seja, $\frac{bp}{2}$ é soma de quatro quadrados. Como $\frac{b}{2} < b$, temos um absurdo, pois b é mínimo com tal propriedade.

Agora, se b for ímpar, sejam $b_1, b_2, b_3, b_4 \in \left[-\frac{b}{2}, \frac{b}{2}\right]$ os números tais que

$$\begin{cases} b_1 \equiv a_1 \mod b \\ b_2 \equiv a_2 \mod b \\ b_3 \equiv a_3 \mod b \\ b_4 \equiv a_4 \mod b \end{cases} \tag{5}$$

Temos que

$$b_1^2 + b_2^2 + b_3^2 + b_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \mod b$$

ou seja, existe b' inteiro positivo tal que

$$bb' = b_1^2 + b_2^2 + b_3^2 + b_4^2.$$

Como $|b_1| < \frac{b}{2}, |b_2| < \frac{b}{2}, |b_3| < \frac{b}{2}$ e $|b_4| < \frac{b}{2}$, temos que

$$b_1^2 + b_2^2 + b_3^2 + b_4^2 < 4 \cdot \frac{b^2}{4} = b^2,$$

logo $bb' < b^2$ e daí $b' < b$.

Se $b' = 0$, então $b_1^2 + b_2^2 + b_3^2 + b_4^2 = 0 \Rightarrow b_1 = b_2 = b_3 = b_4 = 0 \Rightarrow a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv 0 \mod b \Rightarrow a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \mod b^2$, ou seja, b^2 divide bp, portanto b divide p, absurdo, pois como p é primo, seus únicos divisores são 1 e p, além disso, supomos $b > 1$ e já provamos que $b < p$.

Se $b' > 0$, então $bb' = b_1^2 + b_2^2 + b_3^2 + b_4^2 > 0$, como $bp = a_1^2 + a_2^2 + a_3^2 + a_4^2$, temos, pelo Lema 2, que

$$bpb'b = \left(a_1^2 + a_2^2 + a_3^2 + a_4^2\right) \cdot \left(b_1^2 + b_2^2 + b_3^2 + b_4^2\right)$$

$$= \left(a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4\right)^2 + \left(a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3\right)^2 +$$

$$\left(a_1b_3 + a_2b_4 - a_3b_1 - a_4b_2\right)^2 + \left(a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1\right)^2$$

Por (5) temos que

$$\begin{cases} a_1^2 \equiv a_1b_1 \mod b \\ a_2^2 \equiv a_2b_2 \mod b \\ a_3^2 \equiv a_3b_3 \mod b \\ a_4^2 \equiv a_4b_4 \mod b \end{cases} \tag{6}$$

Logo $a_1^2+a_2^2+a_3^2+a_4^2 \equiv a_1b_1+a_2b_2+a_3b_3+a_4b_4 \equiv 0 \mod b$ e portanto b divide $a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4$.

Sejam $0 \leq r_1, r_2, r_3, r_4 < b$ os inteiros tais que

$$\begin{cases} b_1 \equiv a_1 \equiv r_1 \mod b \\ b_2 \equiv a_2 \equiv r_2 \mod b \\ b_3 \equiv a_3 \equiv r_3 \mod b \\ b_4 \equiv a_4 \equiv r_4 \mod b \end{cases} \tag{7}$$

De (7) temos que

$$a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3 \equiv r_1r_2 - r_2r_1 - r_3r_4 + r_4r_3 \equiv 0 \mod b$$

$$a_1b_3 + a_2b_4 - a_3b_1 - a_4b_2 \equiv r_1r_3 + r_2r_4 - r_3r_1 - r_4r_2 \equiv 0 \mod b$$

e, por fim,

$$a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1 \equiv r_1r_4 - r_2r_3 + r_3r_2 - r_4r_1 \equiv 0 \mod b.$$

Ou seja, b divide $a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3, a_1b_3 + a_2b_4 - a_3b_1 - a_4b_2$ e $a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1$.

Sejam c_1, c_2, c_3 e c_4 os inteiros tais que

$$\begin{cases} c_1b = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4 \\ c_2b = a_1b_2 - a_2b_1 - a_3b_4 + a_4b_3 \\ c_3b = a_1b_3 + a_2b_4 - a_3b_1 - a_4b_2 \\ c_4b = a_1b_4 - a_2b_3 + a_3b_2 - a_4b_1 \end{cases} \tag{8}$$

Temos então, por (8), que

$$bpb'b = (c_1b)^2 + (c_2b)^2 + (c_3b)^2 + (c_4b)^2 = b^2 \cdot (c_1^2 + c_2^2 + c_3^2 + c_4^2),$$

ou seja, $b'p = c_1^2 + c_2^2 + c_3^2 + c_4^2$. Como $b' < b$, temos mais um absurdo quanto a minimalidade de b.

Concluímos que $b = 1$ e, portanto, p pode ser escrito como soma de quatro quadrados.

■