Universidade Federal do Espirito Santo

Sobre o Problema de Waring para $n = 2$

e questões correlatas

Luan Carvalho Rios

São Mateus - ES

Maio

2021

Luan Carvalho Rios

Sobre o Problema de Waring para $n = 2$ e questões correlatas

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática Aplicada da Universidade Federal do Espírito Santo, Centro Universitário Norte do Espírito Santo, como requisito parcial para obtenção do Grau de Licenciado em Matemática, linha de pesquisa - Matemática Pura, sob orientação do Prof. Dr. Wescley Bonomo.

São Mateus - ES

Dezembro

2021

Luan Carvalho Rios

Sobre o Problema de Waring para $n = 2$ e questões correlatas

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática Aplicada da Universidade Federal do Espírito Santo, Centro Universitário Norte do Espírito Santo, como requisito parcial para obtenção do Grau de Licenciado em Matemática, linha de pesquisa - Matemática Pura.

BANCA EXAMINADORA

Orientador: Prof. Dr. Wescley Bonomo.

Profa. Dra. Andressa Cesana.

Prof. Dra. Fabiani Aguiar Coswosck.

Agradecimentos

À toda a minha família, especialmente à minha mãe Maria da Penha, minha irmã Luana e meus sobrinhos, por sempre estarem comigo, compreender e apoiar as minhas decisões. Agradeço também aos meu familiares e amigos que me apoiaram durante a graduação, em especial aos meus primos Jaqueline, Raphael e Tonielison, e meus amigos Genilton e Ramon. Ao meu orientador, Professor Wescley Bonomo, pela atenção e disponibilidade para me auxiliar na produção deste Trabalho por meio de orientações, sugestões bibliográficas e discussões. Aos meus amigos e colegas do curso de Licenciatura em Matemática, Filipe, Naidhila, Rômulo, Diogo, por todos os momentos alegres compartilhados e todo apoio que me deram dentro e fora da Universidade. As professoras Andressa Cesana e Fabiani Aguiar Coswosck, por aceitarem o convite para participarem da banca e por contribuírem para meu trabalho. Aos docentes do CEUNES que contribuíram para minha formação, em especial aos professores: Moysés Gonçalves Siqueira Filho, Andressa Cesana e Wescley Bonomo.

Obrigado!

ser feliz é para quem tem coragem

Da. Canô

Resumo

O conteúdo deste Trabalho de Conclusão de Curso está relacionado ao Problema de Waring, proposto em 1770, para n = 2.

Dado um número natural k qualquer, este Problema pergunta se, para cada número natural k existe, associado a ele, um número natural s = s(k), de forma que qualquer número natural n possa ser representado pela soma de no máximo s potências de ordem k.

É sabido que para k = 2, s(2) = 4, o que é consequência dos Teorema dos quatro quadrados de Lagrange, cuja demonstração foi estudada neste Trabalho, e do fato de existirem números naturais que não podem ser obtidos como soma de três quadrados perfeitos.

Neste Trabalho também estudou-se demonstrações de resultados que caracterizam quais números naturais podem ser apresentados como somas de dois e de três quadrados, bem como questões relacionadas, como ternas e quádruplas pitagóricas e outras equações diofantinas similares.

Palavras-chave: Somas de quadrados, Ternas e Quadruplas Pitagóricas, Problema de Waring, Reciprocidade quadrática.

Abstract

The content of this Course Conclusion Paper is related to the Waring's Problem, proposed in 1770, for n = 2.

Given any natural number k, this Problem asks whether, for each natural number k there is a natural number s = s (k) associated with it, so that any natural number n can be represented by the sum of, at most, s powers of order k.

It is known that for k = 2, s (2) = 4, which is a consequence of the Lagrange four squares theorem, whose demonstration was studied in this work, and the fact that there are natural numbers that cannot be obtained as a sum of three perfect squares.

In this work, we also studied demonstrations of results that characterize which natural numbers can be presented as sums of two and three squares, as well related questions, like Pythagorean terns and quadruples and other similar Diophantine equations.

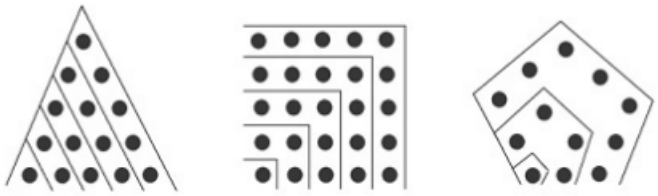
Keywords: : Sums of squares, Pythagorean Triples and Quadruples, Waring's Problem, law of quadratic reciprocity.

Sumário

Capítulo 0

Introdução

Sobre os números que podem ser escrito como soma de três quadrados, P. de Fermat aparentemente foi o primeiro a enunciar que os números da forma $3k + 1$ podem ser representados como soma de três quadrados, porém não nos forneceu demonstração alguma. Em 1774, N. Beguelin [1] notou que os números que são da forma $8n + 7$ e da forma $4n$, não podem ser representados como soma de três quadrados, porém também não demonstrou o resultado. Em 1796 Gauss provou que seu Teorema do número Poligonal, no qual diz que número inteiro positivo é uma soma de no máximo n números poligonais (vide [6]). Fermat escreveu uma nota no Livro IV da sua cópia da *Aritmética de Diofanto*, a qual afirmava que todo número natural escreve-se como soma de três números triangulares, quatro números quadrados, cinco números pentagonais e assim sucessivamente, *ad infinitum*.



Relembrando que, para cada $m \in \mathbb{N}$, o k-esimo número poligonal de ordem $m+2$, doravante $P_{m+2,\,k}$, é a soma dos primeiros k termos da progressão aritmética $(1, 1 + m, 1 + 2m, 1 + 3m, \cdots)$. Por definição, $P_{m+2,\,1} = 1$ para todo $m \in \mathbb{N}$ e, $P_{m+2,\,k+1}$ pontos, pode-se compor no plano um polígono regular de $m + 2$ lados de modo que m arestas consequtivas, sejam constituídas por $k + 1$ pontos e sejam adjacentes ao polígono de $m + 2$ lados constituído

por $P_{m+2,\,k}$ pontos. A figura a seguir ilustra os casos $m = 1$ (números triangulares), $m = 2$ (números quadrados) e $m = 3$ (números pentagonais).

Depois disso em 1797-1798 Legendre obteve a primeira demonstração do seu Teorema de Três Quadrados e em 1813 Cauchy, em [4], observou que o teorema de Legendre era equivalente a observação de N. Beguelin. Anteriormente, em 1801, C. F. Gauss havia obtido um resultado mais geral em [9], contendo o teorema de Legendre de 1797-1798 como Corolário. Gauss teria calculado o número de soluções de um inteiro como soma de três quadrados, e esta é uma generalização de mais um resultado de Legendre, cuja prova é incompleta. Este último fato deve ser a razão para argumentos incorretos anteriormente, de acordo com as quais a prova de Legendre para o teorema de Três quadrados não estava correta e teve de ser concluída por Gauss.

O Problema de Waring, publicado em 1770, questiona se todo número natural k tem um inteiro positivo s tal que todo número natural é a soma de no máximo s números naturais elevados a potência k. Atualmente é sabido que todo número natural é a soma de no máximo 4 quadrados, 9 cubos, 19 quartas potências ou 37 quintas potências.

Este Problema, pode ter sido o estopim para o estudo das somas de quadrados, visto que as publicações de Legendre, Cauchy e Gauss acima citadas são posteriores a ele.

Neste Trabalho estudou-se caracterizações dos números naturais que podem ser escritos como somas de dois e de três quadrados, bem como o Teorema dos quatro quadrados de Lagrange, o que corresponde ao Problema de Waring, para $n = 2$.

Capítulo 1

Prolegômenos

Para iniciar este trabalho achamos interessante expor alguns conceitos prelimirares de modo a propiciar uma melhor compreensão dos resultados que foram expostos nos Capítulos posteriores. Esses conceitos são os de Divisibilidades, Congruência e Resíduos Quadráticos.

1.1 Divisibilidade

Se a e b são inteiros positivos e $a \neq 0$, dizemos que a divide b e denotamos $a \mid b$, se existir um inteiro c tal que $b = ac$, caso a não divida b, denota-se por $a \nmid b$. Vale ressaltar que se $a \mid b$ e $a \mid ac$, então $a \mid c$. Um conceito importante que também será mencionado é o de máximo divisor comum (m.d.c.), que é conhecido por qualquer pessoa de nível médio. O máximo divisor comum de dois inteiros a e b é o maior inteiro que divide a e também divide b, denotaremos o m.d.c. de a e b por (a, b). Um resultado interessante e que também será utilizado sobre m.d.c. é o seguinte:

Proposição 1.1. *Seja $c = (a, b)$, então existem m e n inteiros tais que $c = am + bn$.*

1.2 Congruência

Se a e b são inteiros, dizemos que a é congruente a b módulo m se $m \mid (a - b)$ e denotamos isso por $a \equiv b \, (mod \, m)$. Se m não divide $(a - b)$ dizemos que a é incongruente a b módulo

m e denotamos por $a \not\equiv b\,(mod\, m)$. Por exemplo, $13 \equiv 1\,(mod\, 4)$ pois $4 \mid (13-1)$.

Um resultado importante sobre congruências, que utilizaremos, é o seguinte:

Proposição 1.2. *Se a e b são inteiros, segue que $a \equiv b\,(mod\, m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Segue algumas propriedades de congruências:

Se a, b, c e m são inteiros tais que $a \equiv b(mobm)$, então:

1. $(a+c) \equiv (b+c)(\ mod\ m)$;
2. $(a-c) \equiv (b-c)\ \ (mod\ m)$;
3. $ac \equiv bc\ \ (mod\ m)$;

1.3 Resíduos quadráticos módulo p

Definição 1.3. *Sejam $m \in \mathbb{N}$ e $a \in \mathbb{Z}$ tais que $(a,m) = 1$. O "expoente de a módulo m"é o menor inteiro positivo t tal que $a^t \equiv 1\,(mod\, m)$. Notação: $t = exp_m(a)$.*

Definição 1.4. *Seja $m \in \mathbb{N}$. Denomina-se "raiz primitiva de m"a um inteiro b tal que $(b,m) = 1$ e $exp_m(b) = \varphi(m)$. Observe que este conceito particulariza a equação $exp_m(b) = t$ para o caso especial em que $t = \varphi(m)$.*

Definição 1.5. *Sejam $a, m \in \mathbb{N}, (a,m) = 1$ e g uma raiz primitiva de m. O "índice de a módulo m na base g"é o único (por 1.3) $t \in \{1,2,...,\varphi(m)\}$ satisfazendo a equação*

$$g^t \equiv a\,(mod\, m).$$

Notação: $t = ind_g(a)$.

Teorema 1.6. *Suponha que $m \in \mathbb{N}$ admite uma raiz primitiva. Sejam $a \in \mathbb{Z}, k \in \mathbb{N}$ e $d = (k, \varphi(m))$. Então a equação*

$$x^k \equiv a\,(mod\, m),$$

admite uma solução, se e somente se

$$a^{\frac{\varphi(m)}{d}} \equiv 1\,(mod\, m).$$

Demonstração. Sabemos que $x^k \equiv a\,(mod\, m)$ admite solução, se e somente se a equação

$$ind_g(x) \equiv ind_g(a)\,(mod\, \varphi(m)$$

admite solução. De outro lado, d divide $ind_g(a)$ se, e somente se,

$$ind_g(a) \equiv 0\,(mod\, d).$$

Mas como

$$ind_g(a^{\frac{\varphi(m)}{d}}) \equiv \frac{\varphi(m)}{d} ind_g(a)\,(mod\,(\varphi(m)),$$

concluímos que

$$ind_g(a) \equiv 0\,(mod\, d) \iff$$

$$ind_g(a^{\frac{\varphi(m)}{d}}) \equiv 0\,(mod\, \varphi(m)) \iff$$

$$a^{\frac{\varphi(m)}{d}} \equiv 1\,(mod\, m),$$

como queríamos demonstrar. □

Definição 1.7. *Seja p um número primo. Dizemos que $a \in \mathbb{N}$ é um* ***resíduo quadrático módulo*** *p quando a equação $x^2 \equiv a\,(mod\, p)$ admite soluções para $x \in \{1, ..., p-1\}$.*

Teorema 1.8. *[**Teste de Euler**] Sejam p primo ímpar e $a \in \mathbb{Z}$, tais que $p \nmid a$. O número a é resíduo quadrático módulo p se, e somente se,*

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

Demonstração. Basta observar que, pelo Teorema 1.6, a equação

$$x^2 \equiv a\,(mod\, m),$$

(isto é, a é resíduo quadrático módulo p) admite uma solução, se e somente se

$$a^{\frac{\varphi(p)}{(2,\varphi(p))}} = a^{\frac{p-1}{2}} \equiv 1\,(mod\, m).$$

□

Suponha que $m \in \mathbb{N}$ admite uma raiz primitiva. Sejam $a \in \mathbb{Z}, k \in \mathbb{N}$ e $d = (k, \varphi(m))$. Então a equação

$$x^k \equiv a \,(mod\, m),$$

admite uma solução, se e somente se

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \,(mod\, m).$$

Definição 1.9. *Sejam p um primo ímpar e $a \in \mathbb{N}$ tais que $(p, a) = 1$. O* ***símbolo de Legendre*** *é definido como*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é resíduo quadrático módulo p} \\ -1, & \text{caso contrário} \end{cases}$$

Teorema 1.10. *Sejam p um primo ímpar e $a, b \in \mathbb{N}$, tais que $(a, p) = (b, p) = 1$. Neste caso, as seguintes valem:*

1) Se $a \equiv b \,(mod\, p)$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Demonstração.

1) Decorre diretamente da Definição 1.9, pois,

$$a \equiv b \,(mod\, p) \Leftrightarrow b \equiv a \,(mod\, p),$$

ou seja, se a é resíduo quadrático módulo p, então b também o será. Se a não for resíduo quadrático módulo p, então b também não será.

2) Se a é resíduo quadrático módulo p, então pelo Teorema 1.8,

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

Agora suponha que a seja um resíduo quadrático módulo p. Observe que a equação

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

admite como soluções 1 e $p-1$, as quais são incongruentes módulo p (e nenhuma outra). Por outro lado, como $a^{p-1} \equiv 1 \,(mod\, p)$ (Pequeno Teorema de Fermat), segue que $a^{\frac{p-1}{2}}$ é uma solução da referida equação quadrática e com isto, $a^{\frac{p-1}{2}} \equiv \pm 1 \,(mod\, p)$, de modo que se a não é resíduo quadrático módulo p o teste de Euler (Teorema 1.8) nos diz que

$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) (mod\, p)$$

3) $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (mod\, p)$ e daí,

$$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv 0 \,(mod\, p).$$

Mas $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ é um inteiro entre -2 e 2 e como $p > 2$, resta apenas a possibilidade $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0$. □

A seguir apresenteramos o Teorema da Reciprocidade quadrática de Gauss, o qual afirma que se p e q são primos há uma relação direta entre p ser quadrado módulo q e q ser quadrado módulo p. Este Teorema fornece um rápido algoritmo para determinar se a é quadrado módulo p onde a é um inteiro e p um número primo.

Teorema 1.11. ***[Reciprocidade quadrática de Gauss]*** *Sejam p e q primos ímpares e distintos. Então*

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

Demonstração. A demonstração deste teorema pode ser encontrada em [21], p. 143. □

Capítulo 2

Soma de Dois Quadrados

Neste Capítulo apresentaremos resultados que estabelecem quais números naturais podem ser escritos como Soma de Dois Quadrados de números inteiros. A demonstração apresentada aqui baseia-se na referência [21], a qual faz uso dos conceitos de congruências, resíduos quadráticos, dentre outros. Há uma outra demostração, a qual envolve o conjunto dos inteiros gaussianos $\mathbb{Z}[i]$, e pode ser encontrada em [11].

2.1 Soma de Dois Quadrados

Lema 2.1. *Sejam m e n dois inteiros positivos que podem ser escritos como soma de dois quadrados, isto é, existem $a, b, c, d \in \mathbb{Z}$ tais que $m = a^2 + b^2$ e $n = c^2 + d^2$. Neste caso, $m \cdot n$ também pode ser escrito como soma de dois quadrados.*

Demonstração. Basta observar que

$$m \cdot n = (a^2 + b^2) \cdot (c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

□

Teorema 2.2. *Se $m \in \mathbb{Z}_+$ é da forma $m = 4k + 3$, então não existem inteiros a, b tais que $m = a^2 + b^2$.*

Demonstração. Para qualquer inteiro a,

$$a^2 \equiv 0 \ (mod\ 4)$$

ou

$$a^2 \equiv 1 \ (mod\ 4)$$

conforme a seja par ou ímpar. Logo, para quaisquer $a, b \in \mathbb{Z}$, um dos seguintes ocorre:

$$a^2 + b^2 \equiv 0 \ (mod\ 4), \quad a \text{ e } b \text{ pares;}$$
$$a^2 + b^2 \equiv 1 \ (mod\ 4), \quad a \textit{ par} \text{ e } b \text{ ímpar;}$$
$$a^2 + b^2 \equiv 1 \ (mod\ 4), \quad a \text{ ímpar e b par;}$$
$$a^2 + b^2 \equiv 2 \ (mod\ 4), \quad a \text{ e } b \text{ ímpares.}$$

Portanto, não é possível que $m = a^2 + b^2$ $(a, b \in \mathbb{Z})$ e $m \equiv 3 \ (mod\ 4)$, o que conclui a demonstração. □

Lema 2.3. *Seja p um número primo e $\lambda \in \mathbb{N}$. Se for verdade que λp pode ser escrito como soma de dois quadrados, então o mesmo é verdade para p.*

Demonstração. Seja λ_0 o menor número natural tal que $\lambda_0 p$ possa ser escrito como soma de dois quadrados. Queremos mostrar que $\lambda_0 = 1$.

Inicalmente, suponha que $\lambda_0 = 2$ e observe que 2 pode ser trivialmente escrito como soma de dois quadrados pois $2 = 1^2 + 1^2$. Logo, pelo Lema 2.1,

$$4p = 2p \cdot 2 = (x^2 + y^2) \cdot (1^2 + 1^2) = (x + y)^2 + (x - y)^2.$$

Como $2p$ é par, x e y têm a mesma paridade, ou seja, x, y são ambos pares ou x, y são ambos ímpares, logo $x + y$ e $x - y$ são pares. Portanto,

$$p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2,$$

uma contradição pois λ_0 é por hipótese o menor número natural tal que $\lambda_0 p$ pode ser escrito como soma de dois quadrados.

Agora, suponha que $\lambda_0 \geq 3$ e $\lambda_0 p = x^2 + y^2$. Tome a, b tais que

$$x \equiv a \ (mod\ \lambda_0)$$

e

$$y \equiv b \ (mod\ \lambda_0),$$

e

$$0 < |a|, |b| < \frac{\lambda_0}{2}.$$

Como

$$a^2 + b^2 \equiv x^2 + y^2 \equiv 0\,(mod\ \lambda_0),$$

existe $n \in \mathbb{N}$ tal que

$$n\lambda_0 = a^2 + b^2 \leq 2\left(\frac{\lambda_0}{2}\right)^2 = \frac{{\lambda_0}^2}{2},$$

e com isto, $n \leq \dfrac{\lambda_0}{2}$. Consequentemente, pelo Lema 2.1,

$$\lambda_0 p \cdot \lambda_0 n = (x^2 + y^2)(a^2 + b^2) = (ax + by)^2 + (ay - bx)^2.$$

Por outro lado, pela escolha de a e b,

$$ax + by \equiv a^2 + b^2 \equiv 0\,(mod\ \lambda_0).$$

Portanto, λ_0 também divide $ay - bx$ e com isto,

$$n \cdot p = \frac{(ax + by)^2 + (ay - bx)^2}{{\lambda_0}^2} = \left(\frac{ax + by}{\lambda_0}\right)^2 + \left(\frac{ay - bx}{\lambda_0}\right)^2,$$

mas $n < \lambda_0$, o que é uma contradição. Logo, $\lambda_0 = 1$, como queríamos demonstrar. □

Os próximos dois Teoremas caracterizam quais números primos podem ser escritos como soma de dois quadrados perfeitos e, no caso afirmativo, tal escrita é única.

Teorema 2.4. *Qualquer número primo ímpar p pode ser escrito como soma de dois quadrados se, e somente se, $p \equiv 1\,(mod\ 4)$.*

Demonstração. Pelo Teorema 2.2, se p é um primo ímpar que pode ser escrito como soma de dois quadrados, então $p \equiv 1\ (mod\ 4)$.

Consideremos a recíproca, assumindo $p \equiv 1\,(mod\ 4)$. Pelo Teorema 1.10,

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

Logo, por hipótese,

$$\left(\frac{-1}{p}\right) \equiv 1\ (mod\ p),$$

ou seja,

$$\left(\frac{-1}{p}\right) = 1.$$

Com isto, existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \ (mod\, p)$ e portanto, existe um $\lambda \in \mathbb{N}$ tal que

$$\lambda p = 1^2 + a^2.$$

Agora, a conclusão deste Teorema segue diretamente do Lema 2.3, pois se λp pode ser escrito como soma de dois quadrados, então p também pode. □

Lema 2.5. *Todo número primo p da forma $4k+1$ pode ser decomposto de maneira única como $p = a^2 + b^2$ onde, $a, b \in \mathbb{Z}$ e $0 < a, b < \sqrt{p}$.*

Demonstração. Suponha que

$$p = a^2 + b^2 = c^2 + d^2$$

com a, b, c, $d \in \mathbb{Z}_+$ e $1 < a$, b, c, $d < \sqrt{p}$. Então,

$$\begin{aligned} a^2d^2 - b^2c^2 &= (a^2 + b^2 - b^2)d^2 - b^2(c^2 + d^2 - d^2) \\ &= pd^2 - b^2d^2 - b^2p + b^2d^2 \\ &= p(d^2 - b^2) \equiv 0 \ (mod\, p), \end{aligned}$$

implicando que $ad \equiv bc \ (mod\ p)$ ou $ad \equiv -bc \ (mod\ p)$. Como $a, b, c, d < \sqrt{p}$, há duas possibilidades a considerar: $ad + bc = p$ ou $ad - bc = 0$.

Caso 1: $ad + bc = p$.

Neste caso,

$$\begin{aligned} p^2 &= (a^2 + b^2)(c^2 + d^2) \\ &= (ad + bc)^2 + (ac - bd)^2 \\ &= p^2 + (ac - db)^2, \end{aligned}$$

daí $ac - bd = 0$, logo $a \mid bd = ac$, e por outro lado, como $p = a^2 + b^2 = a \cdot a + b \cdot b$, segue que ou $(a, b) = 1$, ou $(a, b) = p$, mas essa última possibilidade não ocorre pois, por hipótese, $a, b < \sqrt{p} < p$. Logo $a \mid d$ e escrevendo $d = ka$, a condição $ac = bd$ implica em $c = kb$.

Agora,

$$p = (c^2 + d^2) = k^2(a^2 + b^2) = k^2p,$$

logo, $k = \pm 1$ e como a, b, c, $d \in \mathbb{Z}_+$, $k = 1$ e cosequentemente, $a = d$ e $b = c$.

Caso 2: Neste Caso, $a \mid bc = ad$ e como $(a, b) = 1$, $a \mid c$. Considerando $c = ka$, a condição $ad = bc$ implica que $d = kb$, e de modo análogo ao Caso 1, encontramos $a = c$ e $b = d$. □

Um resultado interessante que, em particular, assegura a infinidade de números primos da forma $4k+1$ (ou $4k+3$), é o

Teorema 2.6. *[Dirichlet, 1837] Se a, d são números naturais tal que $mdc(a,d) = 1$, então existem infinitos números primos na progressão aritmética de primeiro termo a e razão d.*

Uma demonstração deste resultado foi apresentada em [10]. Uma outra demonstração foi apresentada posteriormente por Selberg em [20], e também Hudson em [14] apresentou uma demonstração para o caso de progressões artitméticas das formas $4n \pm 1$ e $6n \pm 1$.

Finalmente, os resultados a seguir desta Seção, terminam a caracterização de quais números naturais são somas de dois quadrados perfeitos.

Teorema 2.7. *Seja $n \in \mathbb{Z}_+$, $n = N^2 m$, onde m é livre de quadrados (isto é, não existe um primo p tal que p^2 divida m). Neste caso existem inteiros a e b tais que $n = a^2 + b^2$ se, e somente se, m não tem fatores primos da forma $4k+3$.*

Demonstração. Suponha que m não tenha fatores primos da forma $4k+3$. Se $m = 1$, escreva $n = N^2 + 0^2$. Se $m > 1$, podemos escrever $m = p_1 \cdot \cdots \cdot p_r$, onde, com a excessão de um deles ser o primo 2, todos os primos são da forma $4k+1$. Como todo número da forma $4k+1$ pode ser escrito como soma de dois quadrados (Teorema 2.4) e o mesmo acontece com o número primo 2, pelo Lema 2.1, existem $u, v \in \mathbb{Z}$ tais que $m = u^2 + v^2$. Assim, tomando $a = Nu$ e $b = Nv$, obtém-se $n = a^2 + b^2$.

Reciprocamente, suponha que exista $a, b \in \mathbb{Z}$ tais que $n = N^2 m$ pode ser escrito na forma

$$n = a^2 + b^2 = N^2 m.$$

Se $m = 1$, não há nada a demonstrar (pois m não possui fatores primos da forma $4k+3$). Portanto, considerando $m > 1$, p um fator primo de m e $d = (a,b)$, existem $t, r \in \mathbb{Z}$ tais que $a = rd$, $b = td$ e $(r,t) = 1$ e daí,

$$d^2(r^2 + t^2) = a^2 + b^2 = N^2 m$$

e como m é livre de quadrados, concluí-se que $d^2 \mid N^2$ (mesmo que $d \mid N$ e $d \mid m$, $d^2 \mid N^2$). Assim,

$$r^2 + t^2 = \left(\frac{N^2}{d^2}\right) m = sp$$

para algum inteiro positivo s e desta igualdade seque que $r^2 + t^2 \equiv 0\,(mod\,p)$.

Por outro lado, como $(r,t) = 1$, devemos ter $(r,p) = 1$ ou $(t,p) = 1$, caso contrário r e t teriam um fator a em comum e a^2 dividiria sp.

Suponha inicialmente que $(r,p) = 1$ (o caso $(t,p) = 1$ é análogo), logo existem inteiros r' e r'' tais que

$$r'r + r''p = 1$$

ou, equivalentemente,

$$r'r \equiv 1\,(mod\,p).$$

Multiplicando a equação $r^2 + t^2 \equiv 0\,(mod\,p)$ por $(r')^2$, obtém-se

$$(tr')^2 + 1 \equiv 0\,(mod\,p),$$

o que é equivalente a dizer que $\left(\frac{-1}{p}\right) = 1$ (pois -1 é resíduo quadrático módulo p, pela definição 1.7). Pelo Teorema 1.8, isto só ocorre no caso $p = 2$ ou p, seja da forma $4k + 1$. Consequentemente m não possui fatores primos da forma $4k + 3$, o que conclui a demonstração. □

Corolário 2.8. *Seja $n \in \mathbb{Z}_+$. Existem $a, b \in \mathbb{Z}$ tais que $n = a^2 + b^2$ se, e somente se, todos os fatores primos de n, que são da forma $4k+3$ aparecem na forma padrão ($n = p_1 \cdot \cdots \cdot p_n$) de n com expoente par.*

O resultado deste corolário é uma consequência imediata do Teorema 2.6. A conclusão que vemos até agora é que, para decidir se um inteiro positivo n pode ou não ser escrito como soma de dois quadrados, só precisamos conhecer a decomposição de n em fatores primos.

Lema 2.9. *Seja $n \in \mathbb{Z}_+$. Existem $a, b \in \mathbb{Z}$ tais que $n = a^2 - b^2$ se, e somente se, $n \not\equiv 2\,(mod\,4)$.*

Demonstração. Para qualquer inteiro a, $a^2 \equiv 0\,(mod\ 4)$ ou $a^2 \equiv 1\,(mod\ 4)$, de modo que $a^2 - b^2 \equiv 0, 1$ ou $3\,(mod\ 4)$. Portanto, se $n \equiv 2\,(mod\ 4)$, não é verdade que $n = a^2 - b^2$, para $a, b \in \mathbb{Z}$.

Reciprocamente, suponha que uma das três situações ocorra:

$$n \equiv 0\,(mod\ 4),$$

$$n \equiv 1\,(mod\ 4)$$

ou

$$n \equiv 3\,(mod\ 4).$$

Se $n \equiv 1\,(mod\ 4)$ ou $n \equiv 3\,(mod\ 4)$, então $n+1$ e $n-1$ são ambos pares e neste caso:

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2.$$

Quando $n \equiv 0\,(mod\ 4)$, podemos escrever:

$$n = \left(\frac{n}{4}+1\right)^2 - \left(\frac{n}{4}-1\right)^2,$$

logo, em qualquer caso, encontramos $a, b \in \mathbb{Z}$ tais que $n = a^2 - b^2$, como queríamos. □

2.2 Ternas Pitagóricas

Uma observação interessante a se fazer é que a ***equação pitagórica****, quando consideramos só o conjunto dos inteiros, é um caso particular de soma de dois quadrados.*

Teorema 2.10. ***[Teorema de Pitágoras]*** *Em um triângulo retângulo, a hipotenusa (a) ao quadrado é igual a soma dos quadrados dos catetos, (b e c), isto é*

$$a^2 = b^2 + c^2.$$

Na segunda edição do livro ***"The Pythagorean Proposition"*** *[15] de E. S. Loomis, consta 370 demonstrações desse Teorema. As soluções $(a, b, c) \in \mathbb{Z}$ que satisfazem a equação $a^2 = b^2 + c^2$ são denominadas ternas pitagóricas, e, naturalmente somos conduzidos a duas perguntas:*

1. *Existem infinitas ternas pitagóricas?*
2. *Se a resposta de 1. for positiva, é possível determinar uma fórmula geral que descreva todas as ternas pitagóricas?*

as quais estas foram respondidas afirmativamente. De fato, Um resultado interessante é a ***Proposição XXIX*** *do Livro X de* ***"Os Elementos de Euclides"*** *[7] e que aponta*

a solução geral desta equação, expõe que toda solução inteira da equação $a^2 + b^2 = c^2$ *é da forma*

$$a = \pm(m^2 - n^2),\ b = \pm(2\,m\,n),\ c = \pm(m^2 + n^2).$$

Neste contexto, (a, b, c) *é denominado terna pitagórica e se* (a, b, c) *são coprimos (ou seja, o único divisor comum deles é o* 1*),* (a, b, c) *é denominada terna pitagórica primitiva. Aparentemente, já havia entre os babilônios algum conhecimento sobre ternas pitagóricas, considerando análises feitas no tablete de argila conhecido como Plimpton 322 (sec. XVIII a. c.).*

Segue alguns exemplos de ternas pitagóricas:

$3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $20^2 + 21^2 = 29^2$, $7^2 + 24^2 = 25^2$, *etc...*

2.2.1 Outro Belo Teorema de Fermat

Pierre de Fermat (*Beaumont - Fr,* $1601 - 1665$) *não era formado em matemática, mas em direito, e fez inúmeras "descobertas" em diversos campos da Matemática, principalmente na Teoria dos Números. O "Último Teorema de Fermat" é a sua descoberta mais conhecida e foi demonstrado pelo Inglês Andrew Willes apenas em* 1993*, três séculos após a sua morte.*

Fermat também percebeu algo que daria origem ao assunto principal dessa Sessão: os números primos da forma $4k + 1$ *podem ser sempre, e de modo único, decompostos como Soma de Dois Quadrados, enquanto os primos da forma* $4k+3$ *não podem ser decompostos como Soma de Dois Quadrados (Fato já demonstrado anteriormente neste Capítulo). Já os números ímpares não primos podem ter mais de uma forma de decomposição em soma de dois quadrados. Por exemplo,* $65 = 49 + 16$ *ou* $65 = 64 + 1$.

Segundo Garbi [8], uma descoberta de Fermat em relação a isso foi que se elevarmos qualquer número primo a uma potência inteira t*, o resultado obtido é hipotenusa de* t *diferentes triângulos retângulos de lados inteiros. O autor, no entanto não apresenta justificativa ou referências do porquê isso ocorre. No entanto, em [3] (Cap. 14, p. 116), encontramos o seguinte resultado:*

Teorema 2.11. *Para encontrar o número de maneiras* H_p *pelas quais um número* s *pode ser hipotenusa de triângulos retângulos primitivos , escreva sua fatoração como*

$$s = 2^{a_0} \cdot (p_1^{a_1} \cdots p_n^{a_n}) \cdot (q_1^{b_1} \cdots q_r^{b_r}),$$

onde os p_n são da forma $4k+3$ e os q_r são da forma $4k+1$. O número de tais triângulos retângulos primitivos possíveis é então

$$H_p(s) = \begin{cases} 2^{r-1} \text{ se } n = 0 \text{ e } a_0 = 0 \\ 0 \text{ caso contrário} \end{cases}$$

Por exemplo, $H_p(65) = 2$ e os dois triângulos pitágóricos primitivos com hipotenusa 65 são

$$\begin{aligned} 65^2 &= 16^2 + 63^2 \\ &= 33^2 + 56^2 \end{aligned}$$

Este resultado de Fermat, citado pelo Garbi, pode ser obtido como consequência do Teorema 2.11. Por exemplo, considere o menor número primo da forma $4k+1$, ou seja, o número 5. Sua potência de ordem 1, $5^1 = 5$, é hipotenusa de apenas um triângulo retângulo de lados inteiros, o triângulo $(5,4,3)$, sua potência de ordem 2, $5^2 = 25$, é hipotenusa de dois triângulos retângulos de lados inteiros, são eles os triângulos $(25,20,15)$ e $(25,24,7)$ e sua potência de ordem 3, $5^3 = 125$, é hipotenusa de três triângulos retângulos de lados inteiros, são eles $(125,100,75)$, $(125,120,35)$ e $(125,117,44)$, e assim sucessivamente.

Algo a se pensar é como são gerados todos os triângulos retângulos com lados inteiros, ou seja, quais são as soluções inteiras para a equação $a^2+b^2 = c^2$. A idéia é procurar ternos a,b,c que sejam solução para a equação $a^2+b^2 = c^2$ de modo que não possuam divisores em comum, estas são chamadas de ***soluções primitivas****, assim poderíamos encontrar todas as outras soluções multiplicando as por um número inteiro qualquer r. Por exemplo, dada a solução $(5,4,3)$, todas as $(5r,4r,3r)$ também serão soluções da equação. Observe que a,b não podem ser ambos pares, pois assim c também seria par e teríamos o número 2 como divisor comum de (a,b,c). Se ambos forem ímpares, eles seriam da forma $a = 2q_1+1$ e $b = 2q_2+1$ para q_1, q_2 inteiros e $c^2 = 4(q_1^2+q_2^2)+4(q_1+q_2)+2$. Assim, não existe um inteiro c que seja par, mas seu quadrado não seja divisivel por 4, pois deixa resto 2. Logo, de a,b, podemos concluir que um tem que ser par e outro ímpar, o que implica em c também ser ímpar. Suponha que a seja par e b seja ímpar. Se a é par, ele é da forma $2^\alpha p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, onde $p_1, p_2, \cdots, p_n$ são primos diferentes de 2 e $\beta_1, \beta_2 \cdots \beta_n$ são seus expoentes na decomposição de c.*

Como

$$a^2 + b^2 = c^2$$

$$a^2 = c^2 - b^2$$

$$a^2 = (c+b)(c-b)$$

Como visto anteriormente, b, c *são ímpares, então*

$$c = 2q_1 + 1$$

e

$$b = 2q_2 + 1.$$

Logo

$$(c+b) = 2(q_1 + q_2 + 1)$$

e

$$(c-b) = 2(q_1 - q_2).$$

Observe que a soma e a diferença tem o fator 2 *em comum mas, se* q_1 *e* q_2 *forem de mesma paridade,* $(c+b)$ *será divisivel por* 2 *apenas uma vez, entretanto, se* q_1 *e* q_2 *são de paridades diferentes,* $(c-b)$ *é divisivel por* 2 *apenas uma vez. Portanto, a soma ou a diferença de dois números ímpares é divisivel por* 2 *apenas uma vez.*
Se a contém α *vezes o divisor* 2*, então*

$$a^2 = (c+b)(c-b) = 2^{2\alpha} p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_n^{2\beta_n}$$

Para acharmos $(c+b)$ *e* $(c-b)$ *vamos dividir a equação em duas partes, uma das partes terá o fator* 2 *aparecendo apenas uma vez e nenhum fator primo que aparecer em uma das partes poderá aparecer na outra.*

$$(c+b)(c-b) = (2p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k})(2^{\alpha-1} p_{k+1}^{2\beta_{k+1}} p_{k+2}^{2\beta_{k+2}} \cdots p_n^{2\beta_n})$$

Assim, ou

$$(c+b) = 2p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k}$$

$$(c-b) = 2^{\alpha-1} p_{k+1}^{2\beta_{k+1}} p_{k+2}^{2\beta_{k+2}} \cdots p_n^{2\beta_n}$$

ou,

$$(c+b) = 2^{\alpha-1} p_{k+1}^{2\beta_{k+1}} p_{k+2}^{2\beta_{k+2}} \cdots p_n^{2\beta_n}$$

$$(c-b) = 2p_1^{2\beta_1}p_2^{2\beta_2}\cdots p_k^{2\beta_k}$$

No primeiro caso temos,

$$c = p_1^{2\beta_1}p_2^{2\beta_2}\cdots p_k^{2\beta_k} + 2^{\alpha-2}p_{k+1}^{2\beta_{k+1}}p_{k+2}^{2\beta_{k+2}}\cdots p_n^{2\beta_n}$$

$$b = p_1^{2\beta_1}p_2^{2\beta_2}\cdots p_k^{2\beta_k} - 2^{\alpha-2}p_{k+1}^{2\beta_{k+1}}p_{k+2}^{2\beta_{k+2}}\cdots p_n^{2\beta_n}$$

$$a = 2\left(p_1^{2\beta_1}p_2^{2\beta_2}\cdots p_k^{2\beta_k}\right)\cdot\left(2^{\alpha-1}p_{k+1}^{2\beta_{k+1}}p_{k+2}^{2\beta_{k+2}}\cdots p_n^{2\beta_n}\right)$$

Chamando $p_1^{2\beta_1}p_2^{2\beta_2}\cdots p_k^{2\beta_k} = m$ *e* $2^{\alpha-1}p_{k+1}^{2\beta_{k+1}}p_{k+2}^{2\beta_{k+2}}\cdots p_n^{2\beta_n} = n$ *temos,*

$$c = m^2 + n^2, \qquad b = m^2 - n^2, \qquad a = 2mn,$$

com m *e* n *primos entre si e de paridades diferentes.*
O segundo caso é análogo ao primeiro. Desta forma encontramos todos os ternos de números inteiros correspondentes aos lados de triângulos retângulos.

2.2.2 A equação diofantina $a^2 + b^2 = c^{2n}$

Nesta Subseção, fixado $n > 1$*, será abordada a existência de soluções inteiras para a equação diofantina* $a^2 + b^2 = c^{2n}$*, sendo que isto está relacionado a Subseção anterior, na qual analisou-se a quantidade de triângulos pitagóricos cuja hipotenusa é uma potência de número primo.*

Note que, como vimos anteriormente, é fácil encontrar uma solução quando $a^2+b^2 = c^2$*, mas quando multiplicamos a equação por* c^{2n-2}*, obtemos* $(ac^{n-1})^2 + (bc^{n-1})^2 = c^{2n}$ *e isso nos leva a fazer a seguinte pergunta:*
Existem soluções de $a^2 + b^2 = c^{2n}$ ***com*** a, b, c ***primos entre si?*** *A resposta para essa pergunta é afirmativa.*

Segundo alguns resultados demonstrados anteriormente neste Capítulo, sabemos que quaisquer número inteiro maior do que 1 *pode ser representado como soma de dois quadrados* $a^2 + b^2$ *de números inteiros, desde que sua decomposição em fatores primos não contenha nenhum primo da forma* $4k + 3$ *elevado a um expoente ímpar.*

Considere c *primo, tal que* $c \equiv 1 \pmod 4$*. Devido a resultados demonstrados anteriormente, existem inteiros* a *e* b *tais que* $c^{2n} = a^2 + b^2$*, entretanto, não sabemos a priori se* a, b, c *são primos entre si. Mas, considerando os Inteiros de Gauss* $\mathbb{Z}[\imath]$*, temos a seguinte solução:*

$$c = a^2 + b^2 = (a + b\imath)(a - b\imath),$$

onde $a+bi$ *e* $a-bi$ *são inteiros Gaussianos com norma igual a* c.

Considere,

$$a_0 = (a+bi)^{2n} \text{ e } b_0 = (a-bi)^{2n}.$$

Se $c \mid a_0$ *e* $c \mid b_0$, *então* $c \mid (a+bi)^{2n}$, *contradizendo o fato de* c *ser primo. Com isto,* $c^{2n} = a_0^2 + b_0^2$ *com* c, a_0, b_0 *sendo primos entre si.*

Exemplo: *Considere* $n = 3$ *e* $c = 5$. *Neste caso,*

$$5 = 1^2 + 2^2 = (1+2i)(1-2i) \Rightarrow (1+2i)^6 = 117 + 44i \Rightarrow 5^6 = 117^2 + 44^2.$$

é uma solução primitiva para $a^2 + b^2 = c^{2n}$.

2.3 números de Fibonacci como soma de dois quadrados

A sequência de Fibonacci (F_n) *ou* $(0, 1, 1, 2, 3, 5, 8, 13, 21, \cdots)$ *é caracterizada por*

$$\begin{cases} F_{n+2} = F_{n+1} + F_n \\ F_0 = 0 \\ F_1 = 1 \end{cases},$$

a qual, para todo $k \in \mathbb{N}$, *satisfaz*

$$F_{2k+1} = F_k^2 + F_{k+1}^2.$$

Notras palavras, todo termo F_n, *com* n *ímpar, é soma de dois quadrados. No entanto, nem todo* F_n, *com* n *par, é soma de dois quadrados. Por exemplo,* $F_4 = 3$ *e* $F_8 = 21$ *não o são. Na verdade, em [2] os autores provam que a equação* $x^2 + y^2 = F_{2n}$ *não admite soluções, exceto para valores de* n *em um subconjunto de* N *com densidade assintótica nula, isto é*

$$\lim_{n\to\infty} \frac{1}{n+1} \cdot Card\{0 \le i \le n \mid \exists\, a, b \in \mathbb{N},\ a^2 + b^2 = F_{2n}\} = 0.$$

Capítulo 3

Soma de Três Quadrados

Neste Capítulo apresentaremos resultados que estabelecem quais números naturais podem ser escritos como Soma de Três Quadrados de números inteiros, sendo que, a demonstração apresentada aqui baseia-se na referência [16].

Teorema 3.1. ***(Teorema dos Três Quadrados de Gauss):*** *Se um inteiro positivo $n \geq 0$ é soma de três quadrados, então n não é da forma $4^a(8b+7)$, com $a, b \in \mathbb{N}$.*

Demonstração. Dado $k \in \mathbb{N}$ qualquer, observe que

$$k^2 \equiv 0,\ 1 \text{ ou } 4 \ (mod 8)$$

e consequentemente, um número que é soma de três quadrados não pode ser da forma $8b+7$.

Completando esta análise, observe que se $x^2+y^2+z^2 \equiv 0 \ (mod\ 4)$, então x, y, z devem ser pares, caso contrário, se um deles fosse ímpar, teriamos $x^2+y^2+z^2 \equiv 1 \ (mod\ 4)$; se dois deles fossem ímpares, teríamos $x^2+y^2+z^2 \equiv 2 \ (mod\ 4)$ e se os três fossem ímpares, teríamos $x^2+y^2+z^2 \equiv 3 \ (mod\ 4)$. Agora, supondo por contradição que $x^2+y^2+z^2 = 4^a(8b+7)$, seja $a \in \mathbb{N}$ tal que $2^a \mid \text{mdc}(x,y,z)$ e $2^{a+1} \nmid \text{mdc}(x,y,z)$. Neste caso, $\left(\frac{x}{2^a}\right)^2 + \left(\frac{y}{2^a}\right)^2 + \left(\frac{z}{2^a}\right)^2 = 8b+7$, o que é um absurdo, pelo fato provado no parágrafo anterior.

□

A recíproca do Teorema 3.1 também é verdadeira e será provada a seguir, no Teorema 3.4. Antes, será apresentado alguns resultados técnicos, necessários para a conclusão desta recíproca.

Lema 3.2. *Se $n \in \mathbb{N}$ é soma de três quadrados de números racionais, então n é soma de três quadrados de números inteiros.*

Demonstração. Se $n = x_1^2 + x_2^2 + x_3^2$ e $x_1 = \frac{p_1}{q}, x_2 = \frac{p_2}{q}, x_3 = \frac{p_3}{q} \in \mathbb{Q}$, sendo $q \in \mathbb{N}$ um denominador comum para x_1, x_2, x_3, então $q^2 n = p_1^2 + p_2^2 + p_3^2$, onde $p_1 = q \cdot x_1$, $p_2 = q \cdot x_2$ e $p_3 = q \cdot x_3$ são inteiros.

Com base nesta observação, seja $d > 0$ o menor inteiro positivo para o qual existem $y_1, y_2, y_3 \in \mathbb{N}$ tais que

$$d^2 n = y_1^2 + y_2^2 + y_3^2. \tag{3.1}$$

Queremos concluir que $d = 1$ (e com isto o Lema 3.2) e para isso, inicialmente suponha por absurdo que $d > 1$. Neste caso, considere $y_1 = dy_1' + z_1$, $y_2 = dy_2' + z_2$ e $y_3 = dy_3' + z_3$, com $y_i', z_i \in \mathbb{Z}$, $|z_i| \leq \frac{d}{2}, i = 1, 2, 3$, e também

$$\begin{aligned}
a &= y_1'^2 + y_2'^2 + y_3'^2 - n, \\
b &= 2(nd - y_1 y_1' - y_2 y_2' - y_3 y_3') \\
d' &= ad + b, \\
y_i'' &= a y_i + b y_i', \ i = 1, 2, 3.
\end{aligned}$$

Com isto, por (3.1),

$$\begin{aligned}
\sum_{1 \leq i \leq 3} y_i''^2 &= \sum_{1 \leq i \leq 3} (a y_i + b y_i')^2 \\
&= \sum_{1 \leq i \leq 3} \left(a^2 y_i^2 + 2ab y_i y_i' + b^2 y_i'^2 \right) \\
&= a^2 \sum_{1 \leq i \leq 3} y_i^2 + ab \left(2 \sum_{1 \leq i \leq 3} y_i y_i' \right) + b^2 \sum_{1 \leq i \leq 3} y_i'^2 \\
&= a^2 d^2 n + ab(2nd - b) + b^2 (a + n) \\
&= (ad + b)^2 n \\
&= d'^2 n,
\end{aligned}$$

ou seja, $d'^2 n = y_1''^2 + y_2''^2 + y_3''^2$, e além disso,

$$\begin{aligned} dd' &= d(ad+b) \\ &= ad^2 + db \\ &= d^2\left(\sum_{1\le i\le 3} y_i'^2 - n\right) + d\cdot 2\left(nd - \sum_{1\le i\le 3} y_i y_i'\right) \\ &= nd^2 - 2d\sum_{1\le i\le 3} y_i y_i' + d^2\sum_{1\le i\le 3} y_i'^2 \\ &= \sum_{1\le i\le 3} y_i^2 - 2d\sum_{1\le i\le 3} y_i y_i' + d^2\sum_{1\le i\le 3} y_i'^2 \\ &= \sum_{1\le i\le 3} (y_i - dy_i')^2 \\ &= \sum_{1\le i\le 3} z_i^2 \le \frac{3}{4}d^2, \end{aligned}$$

donde conclui-se que $0 \le d' \le \frac{3}{4}d < d$, contradizendo a minimalidade de d. Agora, observe que se $d' = 0$, então

$$\sum_{1\le i\le 3} z_i^2 = dd' = 0,$$

donde se conclui que $z_1 = z_2 = z_3 = 0$ e consequentemente,

$$y_1'^2 + y_2'^2 + y_3'^2 = \left(\frac{y_1}{d}\right)^2 + \left(\frac{y_2}{d}\right)^2 + \left(\frac{y_3}{d}\right)^2 = \frac{y_1^2 + y_2^2 + y_3^2}{d^2} = \frac{d^2 n}{d^2} = n,$$

o que é absurdo. □

Teorema 3.3. ***(Legendre)*** *Seja a, b, c inteiros livres de quadrados, primos entre si, dois a dois, e não todos com o mesmo sinal. A equação $ax^2 + by^2 + cy^2 = 0$ admite solução $(x, y, z) \neq (0, 0, 0)$ com x, y, z inteiros se, e somente se, $-bc$ é quadrado módulo a, $-ac$ é quadrado módulo b e $-ab$ é quadrado módulo c.*

Demonstração. Inicialmente, demonstremos a necessidade. Podemos supor que x, y, z são primos relativos dois a dois, pois se $d \mid mdc(x, y)$ então d^2 divide cz^2, mas c é livre de quadrados, portanto $d \mid z$. Agora, como $by^2 + cz^2 \equiv 0\,(mod\ a)$, segue que $b^2y^2 \equiv -bcz^2 (mod\ a)$. Note que z deve ser primo com a, pois se p é primo tal que $p \mid a$ e $p \mid z$, então $p \mid by^2$, mas como $mdc(a, b) = 1$, segue que $p \mid y$, o que contradiz o fato de y e z serem primos entre si. Assim, z é invertível módulo a e, consequentemente, $(byz^{-1})^2 \equiv -bc (mod\ a)$.

Provemos agora a suficiência. Podemos supor, sem perda de generalidade, que $a < 0, b < 0$ e $c < 0$. Por hipótese, existe $u \in \mathbb{Z}$ tal que $u^2 \equiv -bc(mod\ a)$. Assim,

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \\ &\equiv b^{-1}((by)^2 + bcz^2) \\ &\equiv b^{-1}((by)^2 - u^2z^2) \\ &\equiv b^{-1}(by - uz)(by + uz) \\ &\equiv (y - b^{-1}uz)(by + uz) \\ &\equiv L_1(x,y,z)M_1(x,y,z)(mod\ a), \end{aligned}$$

onde $L_1(x,y,z) = d_1x + e_1y + f_1z$, $M_1(x,y,z) = g_1x + h_1y + i_1z$, com $d_1 = g_1 = 0$, $e_1 = 1$, $f_1 = -b^{-1}u$, $h_1 = b$ e $i_1 = u$. Do mesmo modo,

$$ax^2 + by^2 + cz^2 \equiv L_2(x,y,z)M_2(x,y,z)(mod\ b)$$

e

$$ax^2 + by^2 + cz^2 \equiv L_3(x,y,z)M_3(x,y,z)(mod\ c),$$

onde $L_k(x,y,z) = d_kx + e_ky + f_kz$, $M_k(x,y,z) = g_kx + h_ky + i_kz$, $k = 2,3$. Como a, b e c são primos entresi dois a dois, podemos, pelo Teorema chinês dos restos, encontrar duas formas lineares $L(x,y,z) = dx + ey + fz$, $M(x,y,z) = gx + hy + iz$ tais que $L \equiv L_1(mod\ a)$, $L \equiv L_2(mod\ b)$ e $L \equiv L_3(mod\ c)$, e $M \equiv M_1(mod\ a)$, $M \equiv M_2(mod\ b)$ e $M \equiv M_3(mod\ c)$ (basta resolver o sistema de congruências coeficiente a coeficiente). Logo,

$$ax^2 + by^2 + cz^2 \equiv L(x,y,z)M(x,y,z)(mod\ abc).$$

Consideremos agora todas as triplas $x,y,z \in \mathbb{Z}^3$ com $0 \le x \le \sqrt{|bc|}, 0 \le y \le \sqrt{|ac|}$ e $0 \le z \le \sqrt{|ab|}$.

Para tais triplas,

$$\left(\left\lfloor\sqrt{|bc|}\right\rfloor + 1\right)\left(\left\lfloor\sqrt{|ac|}\right\rfloor + 1\right)\left(\left\lfloor\sqrt{|ab|}\right\rfloor + 1\right) > abc,$$

donde, pelo Princípio de Dirichlet, existem duas triplas distintas dentre elas, (x_1,y_1,z_1) e (x_2,y_2,z_2), com $L(x_1,y_1,z_1) \equiv L(x_2,y_2,z_2)(mod\ abc)$ ou, equivalemtnemente, $L(x_1 - x_2, y_1 - y_2, z_1 - z_2) \equiv 0(mod\ abc)$, donde, fazendo $\tilde{x} = x_1 - x_2, \tilde{y} = y_1 - y_2$ e $\tilde{z} = z_1 - z_2$, obtém-se

$$a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \equiv L(\tilde{x},\tilde{y},\tilde{z}) \cdot M(\tilde{x},\tilde{y},\tilde{z}) \equiv 0(mod\ abc).$$

Note que $(\tilde{x},\tilde{y},\tilde{z}) \neq (0,0,0), |\tilde{x}| < \sqrt{|bc|}, |\tilde{y}| < \sqrt{|ac|}$ e $|\tilde{z}| < \sqrt{|ab|}$ (de fato, como a,b,c são dois a dois coprimos e livre de quadrados, estas desigualdades são de fato estritas). Como $a,b<0$ e $c>0$, obtemos

$$-2abc = a|bc| + b|ac| < a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \leq c\tilde{z}^2 < |ab|c = abc.$$

Como $abc \mid a\tilde{x}^2+b\tilde{y}^2+c\tilde{z}^2$, necessariamente $a\tilde{x}^2+b\tilde{y}^2+c\tilde{z}^2=0$, o que ou resolve o problema, ou $a\tilde{x}^2+b\tilde{y}^2+c\tilde{z}^2=-abc$. Mas, nesse segundo caso,

$$\begin{aligned} 0 &= (a\tilde{x}^2+b\tilde{y}^2+c\tilde{z}^2+abc)(c\tilde{z}^2+ab) \\ &= a(\tilde{x}\tilde{z}+b\tilde{y})^2 + b(\tilde{y}\tilde{z}-a\tilde{x})^2 + c(\tilde{z}^2+ab)^2, \end{aligned}$$

o que nos dá a solução

$$(\tilde{x}\tilde{z}+b\tilde{y}, \tilde{y}\tilde{z}-a\tilde{x}, \tilde{z}^2+ab),$$

com $\tilde{z}^2+ab \neq 0$. □

Teorema 3.4. ***(Recíproca do Teorema 3.1):*** *Se um inteiro positivo $n \geq 0$ não é da forma $4^a(8b+7)$ com $a,b \in \mathbb{N}$, então n é soma de três quadrados.*

Demonstração. Dado $n \in \mathbb{N}$ que não seja da forma $4^a(8b+7)$, dividindo-o por uma potência de 4 conveniente, pode-se supor que $n\,(mod\ 8) \in \{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$ e com isto, basta provar que existem $m \in \mathbb{Z}$ e $x,y,z,t \in \mathbb{Q}$ com $t \neq 0$ tais que $x^2+y^2=m$ e $nt^2-z^2=m$, pois

$$n = \left(\frac{x}{t}\right)^2 + \left(\frac{y}{t}\right)^2 + \left(\frac{z}{t}\right)^2$$

será soma de três quadrados de racionais e, como provado anteriormente, soma de três quadrados de inteiros.

Podemos supor que n é livre de quadrados (um inteiro é livre de quadrados se ele não é divisível pelo quadrado de nenhum número inteiro maior do que 1), pois sempre podemos escrever $n = a^2 \cdot \tilde{n}$, onde $\tilde{n}$ é livre de quadrados, e se $\tilde{n} = x^2+y^2+z^2$, então

$$n = (ax)^2 + (ay)^2 + (az)^2.$$

Em particular, n não é múltiplo de 4 e a é ímpar, logo $a^2 \equiv 1\,(mod\ 8)$, donde

$$n = a^2\tilde{n} \equiv \tilde{n}\,(mod\ 8).$$

Temos agora os seguintes casos:

1. Se $n \equiv 1\,(mod\ 4)$, ou seja $n\,(mod\ 8) \in \{\bar{1}, \bar{5}\}$, tomando m primo, obtemos $m \equiv 1\,(mod\ 4)$ e $m \equiv -1\,(mod\ n)$. Tal primo existe, pois pelo **Teorema Chinês do Resto**, existe um a com $a \equiv 1\,(mod\ 4)$ e $a \equiv -1\,(mod\ n)$ e pelo **Teorema de Dirichlet** existem infinitos primos congruentes com $a\ \ (mod\ 4)$. Como $m \equiv 1\,(mod\ 4)$ e m é primo, existem x, y tais que $x^2 + y^2 = m$.

Por outro lado, existem $t, z \in \mathbb{Q}$ com $nt^2 - z^2 = m$ se, e somente se, existem $u, v, w \in \mathbb{Z}$ não nulos tais que $nu^2 - v^2 - mw^2 = 0$. Pelo Teorema de Legendre 3.3 , isso equivale a n ser quadrado módulo m e $-m$ ser quadrado módulo n, mas $-m \equiv 1 = 1^2\,(mod\ n)$. Além disso, se $n = p_1\,p_2 \cdots p_k$, com p_i primos, usando o fato que $m \equiv 1\,(mod\ 4)$ e pela lei da reciprocidade quadrática 1.11 obtemos

$$\left(\frac{n}{m}\right) = \prod_{1\le i\le k}\left(\frac{p_i}{m}\right) = \prod_{1\le i\le k}\left(\frac{m}{p_i}\right).$$

Mas $m \equiv -1\,(mod\ n)$, em particular $m \equiv -1\,(mod\ p_i)$ e assim,

$$\left(\frac{m}{p_i}\right) = \left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i-1}{2}}.$$

Mas o número de fatores p_i de n, congruentes com $3\,(mod\ 4)$, é par pois $n \equiv 1\,(mod\ 4)$, portanto $\left(\frac{n}{m}\right) = 1$.

2. Se n é par, então, $n\ mod\ 8 \in \{\bar{2}, \bar{6}\}$ e além disso, $n = 2p_1 \cdot p_2 \cdot \cdots \cdot p_k$, onde os p_i são primos ímpares distintos. Tomemos m como primo, então $m \equiv 1\,(mod\ 4)$ e $m \equiv -1\ \left(mod\ \frac{n}{2}\right)$; ainda, a classe de congruência de m módulo 8 pode ser 1 ou 5. Lembrando que se $m \equiv 1\,(mod\ 8)$, então $\left(\frac{2}{m} = 1\right)$ e se $m \equiv 5\,(mod\ 8)$, então $\left(\frac{2}{m}\right) = -1$. Como antes, $-m \equiv 1\,(mod\ n)$, onde $-m$ é um quadrado módulo n. Basta mostrar que m pode ser escolhido de modo que n seja quadrado módulo m. Temos

$$\left(\frac{n}{m}\right) = \left(\frac{2}{m}\right)\prod_{1\le i\le k}\left(\frac{p_i}{m}\right) = \left(\frac{2}{m}\right)\prod_{1\le i\le k}\left(\frac{m}{p_i}\right) = \left(\frac{2}{m}\right)\prod_{1\le i\le k}\left(\frac{-1}{p_i}\right).$$

Basta então escolher a classe de congruência de $m\ (mod\ 8)$ de modo que

$$\frac{2}{m} = \prod_{1\le i\le k}\left(\frac{-1}{p_i}\right)$$

para que tenhamos $\left(\frac{n}{m}\right) = 1$, como queríamos.

3. Se $n \equiv 3\,(mod\ 8)$, tomamos $m = 2q$, com q primo, $q \equiv 1\,(mod\ 4)$ e $2q \equiv -1\,(mod\ n)$. Como antes, $-m \equiv 1\,(mod\ n)$, donde $-m$ é um quadrado módulo n. Mostremos que n é quadrado módulo m. Como n é quadrado módulo 2, basta mostrar que ele é quadrado módulo q. Sendo $n = p_1 p_2 \cdots p_k$, com p_i primos,

$$\left(\frac{n}{q}\right) = \prod_{1\le i\le k}\left(\frac{p_i}{q}\right) = \prod_{1\le i\le k}\left(\frac{q}{p_i}\right) = \prod_{1\le i\le k}\left(\frac{2}{p_i}\right)\left(\frac{2q}{p_i}\right) = \prod_{1\le i\le k}\left(\frac{2}{p_i}\right)\left(\frac{-1}{p_i}\right)$$

e

$$\left(\frac{2}{p_i}\right)\left(\frac{-1}{p_i}\right) = \begin{cases} 1 \text{ se } p_i \ mod\ 8 \in \{\bar{1}, \bar{3}\} \\ -1 \text{ se } p_i \ mod\ 8 \in \{\bar{5}, \bar{7}\} \end{cases}.$$

Como $1.1 \equiv 3\cdot 3 \equiv 5\cdot 5 \equiv 7\cdot 7 \equiv 1\,(mod\ 8)$, $1\cdot 3 \equiv 5\cdot 7 \equiv 3\,(mod\ 8)$, $1\cdot 5 \equiv 3\cdot 7 \equiv 5\,(mod\ 8)$ e $1\cdot 7 \equiv 3\cdot 5 \equiv 7\,(mod\ 8)$, n deve ter uma quantidade par de fatores pertencentes a $\{\bar{5}, \bar{7}\}\,(mod\ 8)$, pois caso contrário, $n\ (mod\ 8) \in \{\bar{5}, \bar{7}\}$. Assim, $\left(\frac{n}{q} = 1\right)$.

□

3.1 Algumas generalizações e resultados

Em [17] é apresentado os dois seguintes resultados e suas respectivas demonstrações.

Teorema 3.5. *Considere inteiros a, b, c que satisfaçam a seguinte desigualdade $1 \le a \le b \le c$. Para cada número natural n ímpar não negativo existe x, y, z tais que*

$$n = ax^2 + by^2 + cz^2$$

se, e somente se, (a, b, c) é $(1, 1, 2)$, $(1, 2, 3)$ ou $(1, 2, 4)$.

Teorema 3.6. *Não existem números naturais a, b, c de modo que todo n natural par seja da forma*

$$n = ax^2 + by^2 + cz^2$$

com x, y, z inteiros.

3.2 Quadruplas Pitagóricas

Definição 3.7 (**Quadruplas Pitagóricas**). *Dado* x, y, z, $m \in \mathbb{Z}$ *se a equação* $x^2 + y^2 + z^2 = m^2$ *for satisfeita* x, y, z, m *é denominado como "quadrupla pitagórica".*

Um resultado antigo sobre as quadruplas pitagóricas é o seguinte:

Exemplo 3.8. *Dado* $x^2 + y^2 + z^2 = m^2$ *com* z *ímpar e* $(x, y, z) = 1$, *pode-se encontrar números* u, v, w *e* t *tais que*

$$x = 2(uw - t),$$

$$y = 2(ut + vw),$$

$$z = u^2 + v^2 - w^2 - t^2$$

e

$$m = u^2 + v^2 + w^2 + t^2.$$

A primeira demonstração satisfatória para esse resultado foi apresentada por L. Dickson [5] em 1920, para outra demonstração deste resultado, veja [22].

Capítulo 4

Soma de Quatro Quadrados

Neste Capítulo será abordado o Teorema de Lagrange, o qual afirma que todo número inteiro positivo que pode ser escrito como soma de quatro quadrados de números inteiros. A prova que apresentaremos aqui, baseia-se na referência [21]. Encontramos na literatura um outro modo de demonstração do Teorema dos Quatro Quadrados difrente da que apresentaremos aqui, a qual faz uso do conceito de quatérnios hamiltonianos inteiros, e pode ser encontrada em [12].

Lema 4.1. *Se os inteiros positivos m e n podem ser escritos como soma de quatro quadrados, então o produto mn também satisfaz essa propriedade.*

Demonstração. Se $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Z}$ são tais que

$$m = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

e

$$n = b_1^2 + b_2^2 + b_3^2 + b_4^2,$$

então

$$\begin{aligned} mn &= (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ &= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + \\ &+ (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 + \\ &+ (a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + \\ &+ (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2. \end{aligned}$$

□

Para o próximo Lema usaremos um resultado conhecido como ***Princípio de Dirichlet****.*

Lema 4.2. *Se $p > 2$ é um número primo, então a equação*

$$x^2 + y^2 + 1 \equiv 0 \,(mod\, p)$$

admite uma solução $x_0, y_0 \in \mathbb{Z}$ tal que

$$0 \leq x_0 \leq \frac{p-1}{2},\ 0 \leq y_0 \leq \frac{p-1}{2}.$$

Demonstração. Sejam

$$s_1 = \left\{1 + k^2 : k = 0, 1, 2, ..., \frac{p-1}{2}\right\},$$

$$s_2 = \left\{-l^2 : l = 0, 1, 2, ..., \frac{p-1}{2}\right\}.$$

Quaisquer dois elementos distintos de S_1 são incongruentes módulo p, pois, caso contrário, teríamos $1 + k_1^2, 1 + k_2^2 \in S_1$ e

$$1 + k_1^2 \equiv 1 + k_2^2 \,(mod\, p)$$

e daí,

$$(k_1 + k_2)(k_1 - k_2) \equiv 0 \,(mod\, p).$$

Logo,

$$k_1 + k_2 \equiv 0 \,(mod\, p) \text{ ou } k_1 - k_2 \equiv 0 \,(mod\, p).$$

Já que $0 \leq k_1 \leq \frac{p-1}{2}$ e $0 \leq k_2 \leq \frac{p-1}{2}$, segue que $0 \leq k_1 + k_2 \leq p-1$. Logo, a única maneira de ocorrer $k_1 + k_2 \equiv 0 \,(mod\, p)$ é $k_1 = -k_2$ e isto acarreta $1 + k_1^2 = 1 + k_2^2$. Por outro lado, $-\frac{p-1}{2} \leq k_1 - k_2 \leq \frac{p-1}{2}$, de onde segue que o único modo de termos $k_1 - k_2 \equiv 0 \,(mod\, p)$ é $k_1 = k_2$ e isto também implica em $1 + k_1^2 = 1 + k_2^2$. Da mesma forma, quaisquer dois elementos distintos de S_2 são incongruentes módulo p. Como S_1 e S_2 são disjuntos, o número de elementos de $S_1 \cup S_2$ é $2\left[1 + \frac{1}{2}(p-1)\right] = p + 1$. Logo, pelo Princípio de Dirichlet, algum elemento $1 + x_0 \in S_1$ deve ser congruente módulo p com algum elemento $-y_0^2 \in S_2$, isto é,

$$1 + x_0 \equiv -y_0^2 \,(mod\, p)$$

e

$$0 \leq x_0 \leq \frac{p-1}{2},\ 0 \leq y_0 \leq \frac{p-1}{2},$$

como queríamos demonstrar. □

Lema 4.3. *Se p é um primo ímpar, então existe um inteiro positivo k tal que $k \leq p$ e kp é soma de quatro quadrados.*

Demonstração. Pelo Lema 4.2, existem $0 \leq x_0 < \frac{p}{2}$ e $0 \leq y_0 < \frac{p}{2}$ tais que

$$x_0^2 + y_0^2 + 1^2 + 0^2 = kp$$

para algum $k \in \mathbb{Z}$, $k > 0$. Por outro lado, destas condições sobre x_0 e y_0, segue que

$$kp = x_0^2 + y_0^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2$$

e consequentemente $k < p$, como afirmamos. □

Teorema 4.4. *Para qualquer número primo positivo p, existem $x, y, z, w \in \mathbb{Z}$ tais que $p = x^2 + y^2 + z^2 + w^2$.*

Demonstração. O caso $p = 2$ é trivial, pois

$$2 = 1^2 + 1^2 + 0^2 + 0^2.$$

Agora, seja p um primo ímpar. Pelo Lema 4.3, existe $k \in \mathbb{Z}$ tal que $1 \leq k < p$ e k é o menor inteiro possível tal que existam $x, y, z, w \in \mathbb{Z}$ satisfazendo

$$kp = x^2 + y^2 + z^2 + w^2. \tag{4.1}$$

Queremos mostrar que $k = 1$. Para isso, note que se k fosse par, x, y, z, w seriam todos pares ou todos ímpares, ou dois pares e dois ímpares. Em qualquer caso, pode-se supor $x \equiv y \,(mod\, 2)$ e $z \equiv w \,(mod\, 2)$. Com isto, os números

$$\frac{1}{2}(x-y), \frac{1}{2}(x+y), \frac{1}{2}(z-w), \frac{1}{2}(z+w)$$

são todos inteiros e além disso,

$$\left(\frac{1}{2}k\right)p = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2,$$

contradizendo a mínimalidade de k, pois $\frac{1}{2}k \in \mathbb{Z}$ visto que k é par. Portanto, k é ímpar. Se $k > 1$, então $k \geq 3$ e assim existiriam $a, b, c, d \in \mathbb{Z}$ tais que

$$a \equiv x \pmod{k},$$

$$b \equiv y \pmod{k},$$

$$c \equiv z \pmod{k},$$

$$d \equiv w \pmod{k}$$

e

$$|a|, |b|, |c|, |d| < \frac{k}{2}$$

(para obter x, considere o resto da divisão de x por k e tome $a = r$ ou $a = r - k$ conforme tenhamos $r < \frac{k}{2}$ ou $r > \frac{k}{2}$).

Daí,

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k} \tag{4.2}$$

e portanto, $a^2 + b^2 + c^2 + d^2 = nk$, para algum $n \in \mathbb{Z}$. Por outro lado, das condições impostas sobre a, b, c, d, segue que

$$0 \leq nk = a^2 + b^2 + c^2 + d^2 \leq 4\left(\frac{k}{2}\right)^2 = k^2.$$

Também, $n \neq 0$, pois $n = 0$ acarreta $a = b = c = d = 0$ e daí, $k \mid x, y, z, w$ (Por 4.2), de onde se conclui que $k^2 \mid kp$ (por 4.1) e portanto, $k \mid p$, o que é impossível, já que $1 < k < p$ e p é primo.

Assim,

$$0 < nk < k^2,$$

o que implica em

$$0 < n < k.$$

Agora, pelo Lema 4.1,

$$\begin{aligned} k^2np &= (kp)(kn) \\ &= (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) \\ &= r^2 + s^2 + t^2 + u^2 \end{aligned}$$

onde

$$r = xa + yb + zc + wd,$$
$$s = xb - ya + zd - wc,$$
$$t = xc - yd - za + wb,$$
$$u = xd + yc - zb - wa.$$

Essas equações nos mostram que cada um dos inteiros r, s, t, u são múltiplos de k. Por exemplo,

$$r = xa + yb + zc + dw \equiv a^2 + b^2 + c^2 + d^2 = nk \equiv 0(mod\ k)$$

e analogamente para s, t, u. Portanto,

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2,$$

onde $\frac{r}{k}, \frac{s}{k}, \frac{t}{k}, \frac{u}{k} \in \mathbb{Z}$. Como $0 < n < k$, chegamos a uma contradição sobre a minimalidade de k e com isto, só resta a possibilidade $k = 1$, como queríamos demonstrar. □

4.1 Generalizações

Em [18], Ramanujan provou, como generalização do Teorema dos 4 quadrados, que existem exatamente cinquenta e quatro 4-uplas $(a, b, c, d) \in \mathbb{N}$ para as quais a equação

$$ax^2 + by^2 + cz^2 + du^2 = n$$

admite soluções para todo n natural.

Neste Trabalho, também são comentadas generalizações similares para o caso da soma de três quadrados.

Referências Bibliográficas

[1] *ACADEMIA DE BERLIM.* ***Nouveaux Mémoires de l'Académie de Berlin****, p. 313–369, 1776.*

[2] *BALLOT C.; LUCA F.,* ***On the equation*** $x^2 + dy^2 = F_n$*. ACTA ARITHMETICA, vol 127, n. 2, p. 145–155, 2007.*

[3] *BEILER, Albert H.,* ***Recreations in The Theory of Numbers:*** *The Queen of Mathematics Entertains, 2 ed. New York: Dover Publications Inc, 1964.*

[4] *CAUCHY, A. L.* ***Mém. Sci. Math. Phys. de l'Institut de France****, vol. 14, n. 1, p. 1813–1815, 1777.*

[5] *DICKSON, L.* ***Some relations between the theory of numbers and other branches of mathematics****, Comptes rendus du congrès international des mathématiciens, p.41-56, 1920.*

[6] *DICKSON, L.* ***History of the theory of Numbers****, Carnegie Institute of Washington, vol. 2, p. 15, 1992.*

[7] *EUCLIDES.* ***Os Elementos.*** *Traduçãdo por Irineu Bicudo, 1 ed. São Paulo: UNESP, 2009.*

[8] *GARBI, G. Outro Belo Teorema de Fermat;* ***Revista do Professor de Matemática****, vol. 38; set./ dez. 1998, S.B.M. Disponível em:* ⟨*https://www.rpm.org.br/cdrpm/38/1.htm*⟩.

[9] *GAUSS, Carl.* ***Disquisitiones Arithmeticae****, Yale University Press, art. 291 et 292, 1965.*

[10] HASSE, H. ***Vorlesungen über Zahlentheorie****. Springer, 1964.*

[11] HEFEZ, I. N. ***Curso de Álgebra****, vol 1. 3. ed. Rio de Janeiro: IMPA, 2002.*

[12] HERSTEIN, I. N. ***Tópicos de álgebra****. tradução de Adalberto P. Bergamasco, L. H. Jacy Monteiro; São Paulo: EDUSP, 1970.*

[13] HILBERT, David, ***Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahln ter Potenzen (Waringsches Problem)****, Mathematische Annalen, 1909.*

[14] HUDSON, R. H.; Brauer, A. On the exact number of primes in the arithmetic progression $4n \pm 1$ *and* $6n \pm 1$*.* ***Journal für die reine und angewandte Mathematik****. Vol. 291, p. 23–29, 1977.*

[15] LOOMIS, Elisha. ***The Pythagorean Proposition****; 2. ed; Michigan: The Nacional Conncil of Teachers of Mathematics, 1940.*

*[16] MARTINEZ, F. et al.****Teoria dos Números:*** *um passeio com primos e outros números familiares pelo mundo inteiro, 5 ed. Rio de Janeiro: IMPA, 2018.*

[17] PANAITOPOL, L. ***On the Representation of Natural Numbers as Sums of Squares****. Mathematical Association of America, vol. 112, n. 2, p.168-171, fev. 2005.*

[18] RAMANUJAN, S. ***On the expression a number in the form*** $ax^2+by^2+cz^2+du^2$*. [Proc. Cambridge Philos. Soc. 19 (1917), 11-21]*

[19] RIBENBOIM, P. ***Números Primos : mistérios e recordes****; 1. ed; IMPA, 2001;*

[20] SELBERG, A. An Elementary Proof of Dirichlet's Theorem About Primes in an Arithmetic Progression; ***Annals of Mathematics****, vol. 50, n. 2; Princeton University, Apr., 1949.*

[21] SHOKRANIAN , S. SOARES , M.; GODINHO , H. ***Teoria dos Números****. 2. ed. Brasília: Editora Universidade de Brasília, 1999.*

[22] SPIRA, R. ***The Diophantine Equation*** $x^2 + y^2 + z^2 = m^2$ *. The American Mathematical Monthly, v.69, p.360-365, 2013.*

Índice Remissivo