UNIVERSIDADE FEDERAL DE SANTA CATARINA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA
PROFMAT

Daiane da Silva Debortoli

NÚMEROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADOS DE NÚMEROS NATURAIS

Florianópolis

2017

Daiane da Silva Debortoli

NÚMEROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADOS DE NÚMEROS NATURAIS

Dissertação submetida ao Programa de Mestrado Profissional de Matemática em rede nacional - PROFMAT da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do Grau de Mestre em Matemática.
Orientador: Profa. Dra. Alda Dayana Mattos Mortari
Universidade Federal de Santa Catarina - UFSC

Florianópolis

2017

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Debortoli, Daiane da Silva
Números que podem ser escritos como soma de dois quadrados de números naturais / Daiane da Silva Debortoli ; orientadora, Profa. Dra. Alda Dayana Mattos Mortari - Florianópolis, SC, 2017.
59 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas. Programa de Pós-Graduação em Matemática.

Inclui referências

1. Matemática. 2. Relações de equivalência. 3. Congruências. 4. Soma de dois quadrados. I. Mortari, Profa. Dra. Alda Dayana Mattos . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Matemática. III. Título.

Daiane da Silva Debortoli

NÚMEROS QUE PODEM SER ESCRITOS COMO SOMA DE DOIS QUADRADOS DE NÚMEROS NATURAIS

Esta Dissertação foi julgada aprovada para a obtenção do Título de "Mestre em Matemática", e aprovada em sua forma final pelo Programa de Mestrado Profissional de Matemática em rede nacional - PROFMAT da Universidade Federal de Santa Catarina como requisito parcial.

Florianópolis, 28 de março de 2017.

Prof. Dr. Celso Melchiades Doria
Universidade Federal de Santa Catarina - UFSC
Coordenador

Banca Examinadora:

Profa. Dra. Alda Dayana Mattos Mortari
Universidade Federal de Santa Catarina - UFSC
Orientador

Prof. Dr. Eliezer Batista
Universidade Federal de Santa Catarina - UFSC

Profa. Dra. Elisa Regina dos Santos
Universidade Federal de Uberlândia - UFU

Prof. Dr. Raphael Falcão da Hora
Universidade Federal de Santa Catarina - UFSC

AGRADECIMENTOS

A Deus, por todas as bençãos recebidas.

Aos meus pais, Terezinha e Moacir, que sempre estiveram ao meu lado, me apoiando e dando força nos momentos em que mais precisei.

Ao meu marido Ezequiel, pela paciência, pelo carinho e por estar sempre me incentivando e auxiliando nos estudos.

À professora Catiane Domingas Bortolozo Lovera, por ter sido uma inspiração para mim, sendo um exemplo de professora.

A todos os colegas da turma Profmat-2015, por todos os momentos que passamos juntos, de aprendizado e companheirismo, especialmente a minha colega Nicole Bertoluci Rodrigues, que compartilhou comigo muitos momentos felizes de estudos e lazer.

Aos professores do Profmat-UFSC, por todas as contribuições e paciência durante todo o curso.

À professora Alda Dayana Mattos Mortari, por me orientar durante a elaboração deste trabalho com esclarecimentos, correções e sugestões, e por demonstrar sempre compreensão e paciência.

Aos professores que compõem a banca examinadora: Elisa Regina dos Santos, Gilles Gonçalves de Castro e Raphael Falcão da Hora pela sua disposição em avaliar este trabalho.

À CAPES, pela ajuda financeira durante o curso.

RESUMO

Neste trabalho mostraremos uma descrição de quais números naturais possuem uma representação como soma de dois quadrados de números naturais. Para isso, estudaremos conceitos preliminares, tais como divisão euclidiana nos inteiros, números primos, relações de equivalência e congruências.
Palavras-chave: Relações de equivalência. Congruências. Soma de dois quadrados.

ABSTRACT

In this work we will show a description of natural numbers as a representation of a sum of two squares of natural numbers. For this, we will study preliminary concepts, such as Euclidean division in integers, prime numbers, equivalence relations and congruences.

Keywords: Equivalence relations. Congruences. Sum of two squares.

SUMÁRIO

INTRODUÇÃO

Que números podem ser escritos como uma soma de dois quadrados de números naturais?

Podemos concluir inicialmente que os números em questão são números naturais, já que o quadrado de um número natural é um número natural e a soma de dois números naturais é também um número natural. Assim, sempre que citarmos no decorrer deste trabalho uma expressão do tipo "números que podem ser escritos como soma de dois quadrados"estaremos nos referindo a números naturais e quadrados de números naturais.

Analisando o conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, percebemos que os números que são quadrados perfeitos $1, 4, 9, 16, \ldots$ podem ser escritos como uma soma de dois quadrados, basta considerarmos o zero ao quadrado como uma das parcelas da soma. Observando agora aqueles que não são quadrados perfeitos, notamos que alguns podem ser escritos como somas de dois quadrados, como, por exemplo:

$$\begin{aligned} 2 &= 1^2 + 1^2, \\ 5 &= 1^2 + 2^2, \\ 8 &= 2^2 + 2^2, \\ 10 &= 1^2 + 3^2, \\ 13 &= 3^2 + 2^2, \\ 17 &= 1^2 + 4^2. \end{aligned}$$

Além desses números, será que existem outros que podem ser escritos como soma de dois quadrados de números naturais? Será que eles possuem alguma característica semelhante?

Motivados a responder estas questões, nos propomos neste trabalho a mostrar que existem infinitos números naturais que podem ser escritos como uma soma de dois quadrados de números naturais e ainda, vamos determinar de que forma são estes números.

Para uma melhor compreensão do texto é importante que o leitor esteja familiarizado com a teoria básica de conjuntos, o conjunto dos números naturais, o conjunto dos números inteiros e as operações de adição e multiplicação de números naturais e inteiros.

No primeiro capítulo faremos um estudo sobre divisão euclidiana nos inteiros, números primos, relações de equivalência, congruências e

apresentaremos vários resultados que serão utilizados ao longo do trabalho. Por exemplo, mostraremos neste capítulo que todo número natural primo ímpar é da forma $4m + 1$ ou $4m + 3$, para algum $m \in \mathbb{N}$ e ainda, que existem infinitos números primos da forma $4m + 3$. Neste capítulo utilizamos como base para estudos as referências: [DOMINGUES, 2009], [HEFEZ, 2014] e [HEFEZ, 2011].

No segundo capítulo contruiremos uma relação de equivalência em um determinado conjunto, a qual nos ajudará a provar que todo número primo da forma $4m + 1$ pode ser escrito como soma de dois quadrados. Além disso, provaremos que existem infinitos números primos da forma $4m + 1$ mostrando assim que existem infinitos números naturais que podem ser escritos como soma de dois quadrados. Por fim, mostraremos de que forma são os números naturais que possuem representação como soma de dois quadrados. Neste capítulo utilizamos como base para estudos as referências: [AIGNER, 2002] e [MORGADO, 2013].

1 PRÉ-REQUISITOS

O primeiro capítulo deste trabalho será dedicado a apresentação de alguns conceitos preliminares, como divisão euclidiana nos inteiros, números primos, relações de equivalência e congruências. Estes são os principais conceitos que serão usados para demonstrar o teorema principal desde trabalho.

1.1 DIVISÃO EUCLIDIANA NOS INTEIROS

Nesta seção, apresentaremos o conceito de divisibilidade e alguns resultados sobre divisão euclidiana no conjunto dos números inteiros. Tal conjunto será denotado por $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Definição 1.1. *Dados $a, b \in \mathbb{Z}$, diremos que a* divide *b e denotaremos por $a|b$, quando existir um inteiro c tal que $b = ac$. Neste caso, diremos que a é um* divisor *de b ou um* fator *de b ou, ainda, que b é um* múltiplo *de a ou que b é* divisível *por a.*

A notação $a|b$ não representa uma operação em $\mathbb{Z}$, nem uma fração, e sim, uma sentença que diz ser verdade que existe um inteiro c tal que $b = ac$. A negação desta sentença será denotada por $a \nmid b$, representando que não existe inteiro c tal que $b = ac$.

Exemplo 1.2. $3|15$, pois $15 = 3 \cdot 5$. Já $3 \nmid 10$, pois não existe um número inteiro c tal que $10 = 3c$.

A seguir veremos dois resultados que serão utilizados várias vezes ao longo deste trabalho.

Proposição 1.3. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b + c)$. Então, se $a|b$ tem-se que $a|c$.*

Demonstração. Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b+c)$ e $a|b$. Logo, existem inteiros x e y tais que $b + c = ax$ e $b = ay$. Substituindo o valor de b na primeira igualdade obtemos

$$\begin{aligned} ay + c &= ax \\ c &= ax - ay \\ c &= a(x - y). \end{aligned}$$

Note que $x - y \in \mathbb{Z}$, pois $x, y \in \mathbb{Z}$. Logo, a divide c.

■

Exemplo 1.4. $2|[4 + (-6)]$ e $2|4$, logo $2| - 6$.

Vejamos agora um exemplo de um número inteiro que divide a soma de dois números inteiros, mas não divide nenhum deles.

Exemplo 1.5. $6|(2 + 4)$, mas $6 \nmid 2$ e $6 \nmid 4$.

Proposição 1.6. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|b$ e $a|c$. Então, para todos $x, y \in \mathbb{Z}$ tem-se que $a|(xb + yc)$.*

Demonstração. Sejam $a, b, c \in \mathbb{Z}$, tais que $a|b$ e $a|c$. Logo, existem inteiros d e e tais que $b = ad$ e $c = ae$. Logo,

$$\begin{aligned} xb + yc &= x(ad) + y(ae) \\ &= xad + yae \\ &= a(xd + ye). \end{aligned}$$

Perceba que $xd + ye \in \mathbb{Z}$, pois $x, y, d, e \in \mathbb{Z}$. Logo, a divide $xb + yc$.

■

Dados inteiros a e b, com $a \neq 0$, sempre é possível efetuar a "divisão"de b por a com resto. Este resultado é chamado *Algoritmo da Divisão Euclidiana* e será enunciado abaixo, sua demonstração pode ser consultada na página 53 de [HEFEZ, 2014].

Teorema 1.7. (Algoritmo da Divisão Euclidiana) *Sejam a e b dois números inteiros com $a \neq 0$. Então, existem dois únicos números inteiros q e r tais que*

$$b = aq + r, \quad com \quad 0 \leq r < |a|.$$

Os números q e r do teorema acima são chamados, respectivamente, de *quociente* e de *resto* da divisão euclidiana de b por a.

Exemplo 1.8. Como vimos no *Exemplo 1.2*, $3 \nmid 10$, mas podemos fazer a divisão euclidiana de 10 por 3, obtendo

$$10 = 3 \cdot 3 + 1,$$

então, temos que 3 é o quociente e 1 é o resto na divisão euclidiana de 10 por 3.

1.2 NÚMEROS PRIMOS

Nesta seção apresentaremos alguns resultados importantes sobre números primos e congruências. Estes resultados são pré-requisitos para demonstrações futuras.

Iniciaremos com a definição de número primo, pois estes números desempenham papel fundamental e a eles estão associados muitos problemas famosos, como o Postulado de Bertrand, que diz que, se $n > 3$ é um número natural, então existe pelo menos um número primo p tal que $n < p < 2n$; a Conjectura de Goldbach, proposta pelo matemático prussiano Christian Goldbach, que diz que todo número par maior ou igual a 4 é a soma de dois primos - problema este que ainda não foi demonstrado ou contradito -, e também o problema que nos propomos a demonstrar como teorema central deste trabalho. Mais informações sobre os dois primeiros problemas citados podem ser encontradas, respectivamente, na página 9 de [AIGNER, 2002] e na página 198 de [RIBENBOIM, 2012].

Definição 1.9. (Número primo em $\mathbb{N}$) *Um número natural p maior do que 1 que só possui dois divisores positivos distintos, a saber, 1 e p, é chamado de* número primo.

Exemplo 1.10. Os números $5, 13$ e 41 são números primos, já que seus únicos divisores positivos são o 1 e o próprio número. Já os números $6, 9$ e 18 não são primos, pois são divisíveis por 3, ou seja, o 1 e o próprio número não são seus únicos divisores positivos.

Definição 1.11. *Um número natural maior do que 1 e que não é primo será chamado* composto.

Observação 1.12. *Decorre da definição acima que, se um número inteiro $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Portanto, existirá um número natural n_2 tal que*

$$n = n_1 n_2 \quad com \quad 1 < n_1 < n \quad e \quad 1 < n_2 < n.$$

O resultado principal do nosso trabalho será para números naturais, portanto, a maioria dos resultados preliminares serão feitos para números naturais. Contudo, em alguns momentos precisaremos trabalhar com números inteiros, por este motivo, faremos alguns resultados para números inteiros. Desta forma, apresentaremos também a definição de número primo em $\mathbb{Z}$.

Definição 1.13. (Número primo em $\mathbb{Z}$) *Um número inteiro p que só possui quatro divisores distintos, a saber, $-p, -1, 1$ e p, é chamado de* número primo.

Exemplo 1.14. O número -5 é primo, pois seus únicos divisores são $-5, -1, 1, 5$. Já o número -6 não é primo, visto que seus divisores são $-6, -3, -2, -1, 1, 2, 3, 6$.

Proposição 1.15. *Seja $n \in \mathbb{N}$ um número ímpar. Então, existe $m \in \mathbb{N}$ tal que $n = 4m + 1$ ou $n = 4m + 3$.*

Demonstração. Seja $n \in \mathbb{N}$ um número ímpar, então n é da forma $2k + 1$, para algum $k \in \mathbb{N}$. Note que k é par ou é ímpar, ou seja, $k = 2m$ ou $k = 2m + 1$, para algum $m \in \mathbb{N}$. Assim, temos que n é da forma $2(2m) + 1 = 4m + 1$ ou $2(2m + 1) + 1 = 4m + 3$.

■

Corolário 1.16. *Seja $p \in \mathbb{N}$ um número primo ímpar. Então, existe $m \in \mathbb{N}$ tal que $p = 4m + 1$ ou $p = 4m + 3$.*

Usaremos em alguns resultados o máximo divisor comum de dois números inteiros, portanto, usaremos a seguinte definição.

Definição 1.17. *Um número inteiro $d > 0$ é um* máximo divisor comum *(mdc) de dois números inteiros a e b, se possuir as seguintes propriedades:*

i) d é um divisor comum de a e b, e

ii) d é divisível por todo divisor comum de a e b.

O mdc de a e b será denotado por (a, b).

Note que o máximo divisor comum de dois números inteiros sempre existe, pois o 1 é divisor de todos os números. Portanto, o máximo divisor comum é sempre um número maior que ou igual a 1. Note também que existe o maior divisor, pois o conjunto de todos os divisores de um número inteiro é limitado superiormente pelo módulo deste número.

Apresentaremos agora um resultado chamado *Princípio da Boa Ordem*, ele será importante para demonstrarmos a *Proposição 1.19*. Iremos apenas enunciá-lo, a sua demonstração pode ser encontrada na página 20 de [HEFEZ, 2011].

Teorema 1.18. (Princípio da Boa Ordem) *Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.*

Proposição 1.19. *Sejam a e b números inteiros, não ambos nulos e $d = (a, b)$. Então existem $m, n \in \mathbb{Z}$ tais que $d = ma + nb$.*

Demonstração. Seja M o conjunto de todos os números construídos usando a seguinte expressão: dados dois números inteiros m_0 e n_0, fazemos $m_0a + n_0b$, ou seja,

$$M = \{m_0a + n_0b \mid m_0, n_0 \in \mathbb{Z}\}.$$

Note que M possui números negativos, positivos e também o zero. Considere o subconjunto de M tal que todos os números sejam positivos. Este subconjunto é não vazio, pois se os inteiros a e b forem positivos basta tomar inteiros m_0 e n_0 positivos. Se a e b forem negativos basta tomar m_0 e n_0 negativos. Se a e b tiverem sinais opostos, suponhamos a positivo e b negativo, tomamos m_0 positivo e $n_0 = 0$. Se a ou b for zero, suponhamos que a seja, então escolhemos n_0 com o mesmo sinal de b. Pelo Princípio da Boa Ordem, este subconjunto de M possui um menor elemento, desta forma, escolhemos m_0 e n_0 tais que $c = m_0a+n_0b$ seja este menor elemento, ou seja, c é o menor inteiro positivo que pertence a M, e mostraremos então que $c|a$ e $c|b$. Suponha que $c \nmid a$, logo, pela divisão euclidiana, existem únicos $q_1, r_1 \in \mathbb{Z}$ tais que $a = cq_1 + r_1$, em que $0 < r_1 < c$. Assim, temos que:

$$\begin{aligned} r_1 &= a - cq_1 \\ &= a - (m_0a + n_0b)q_1 \\ &= a - m_0aq_1 - n_0bq_1 \\ &= (1 - m_0q_1)a + (-n_0q_1)b. \end{aligned}$$

Note que r_1 é da forma $m_1a + n_1b$, portanto $r_1 \in M$, mas como $0 < r_1 < c$, chegamos a uma contradição, pois supomos que c era o menor inteiro positivo que pertence a M. Logo, $c|a$. De maneira análoga, prova-se que $c|b$.

Como d é um divisor comum de a e b temos que existem inteiros m' e m'' tais que $a = m'd$ e $b = m''d$. Logo,

$$\begin{aligned} c &= m_0a + n_0b \\ &= m_0m'd + n_0m''d \\ &= d(m_0m' + n_0m''). \end{aligned}$$

Ou seja, $d|c$, portanto $d \leq c$. Como d é o máximo divisor comum de a e b, $d < c$ é impossível. Logo, $c = d$ e portanto, existem $m, n \in \mathbb{Z}$ tais

que $d = ma + nb$.

■

Exemplo 1.20. Temos que $(6, 9) = 3$. Então existem inteiros m e n tais que $3 = 6m + 9n$. Uma solução para esta equação é $m = -1$ e $n = 1$, pois

$$6(-1) + 9 \cdot 1 = 3.$$

Lema 1.21. (Lema de Gauss) *Sejam $a, b, c \in \mathbb{Z}$. Se $a|bc$, e $(a, b) = 1$, então $a|c$.*

Demonstração. Sejam $a, b, c \in \mathbb{Z}$. Suponha que $a|bc$ e que $(a, b) = 1$. Como $(a, b) = 1$, pela *Proposição 1.19*, sabemos que existem $m, n \in \mathbb{Z}$ tais que $1 = ma + nb$. Como $a|bc$, existe $k \in \mathbb{Z}$ tal que $bc = ak$. Então, temos que

$$\begin{aligned} c = 1 \cdot c &= (ma + nb)c \\ &= mac + nbc \\ &= mac + nak \\ &= a(mc + nk). \end{aligned}$$

Logo, $a|c$.

■

Exemplo 1.22. $2|(13 \cdot 4)$, logo, $2|4$ já que $(2, 13) = 1$.

A seguir, apresentamos um resultado fundamental, conhecido como *Lema de Euclides*.

Lema 1.23. (Lema de Euclides) *Sejam $a, b \in \mathbb{Z}$ e p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração. Sejam $a, b \in \mathbb{Z}$ e p um número primo. Vamos provar que, se $p|ab$ e $p \nmid a$, então $p|b$.

Suponha que $p|ab$ e $p \nmid a$, então $(p, a) = 1$, e daí pelo *Lema 1.21*, segue que $p|b$.

■

O resultado que apresentaremos a seguir será necessário para demonstrarmos o próximo teorema.

Proposição 1.24. (Segundo Princípio de Indução) *Seja $P(n)$ uma afirmação associada a todo n maior que ou igual a um certo $a \in \mathbb{Z}$, dado a priori. Suponhamos que seja possível provar as duas condições a seguir.*

i) $P(a)$ é verdadeira.

ii) Para todo $r > a$, se $P(k)$ é verdadeira sempre que $a \leq k < r$, então $P(r)$ também é verdadeira.

Então $P(n)$ é verdadeira para qualquer $n \geq a$.

A demonstração da proposição acima pode ser encontrada na página 122 de [DOMINGUES, 2009].

Veremos agora um importante resultado, conhecido como *Teorema Fundamental da Aritmética*.

Teorema 1.25. (Teorema Fundamental da Aritmética) *Todo número natural n maior do que 1 ou é primo ou pode ser representado de maneira única (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Usaremos o Segundo Princípio de Indução (*Proposição 1.24*). Se $n = 2$, o resultado é claramente verdadeiro, já que 2 é primo. Agora suponhamos que o resultado seja válido para todo número natural menor do que n e vamos mostrar que também é válido para n. Se n é primo não temos nada a provar. Suponhamos então, que n é composto. Logo, pelo que foi visto na *Observação 1.12*, existem números naturais n_1 e n_2 tais que

$$n = n_1 n_2, \quad \text{com} \quad 1 < n_1 < n \quad \text{e} \quad 1 < n_2 < n.$$

Pela hipótese de indução, temos que existem $r, s \in \mathbb{N}$ e números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto,

$$n = p_1 \cdots p_r q_1 \cdots q_s.$$

Agora mostraremos a unicidade da escrita.

Se n é primo, não há nada a provar. Vamos supor, então, que n é composto e que tenha duas fatorações distintas, isto é, existem $r, s \in \mathbb{N}$ e $p_1, \ldots, p_r, q_1, \ldots, q_s \in \mathbb{N}$ primos tais que

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Para todos $i \in \{1, \ldots, r\}$ e $j \in \{1, \ldots, s\}$ considere que os p_i não são necessariamente distintos entre si, e o mesmo vale para os q_j. Vamos provar que $r = s$ e que cada p_i é igual a algum q_j.

Como p_1 divide o produto $q_1 q_2 \ldots q_s$, pelo *Lema 1.23* temos que p_1 divide pelo menos um dos fatores q_j. Sem perda de generalidade, podemos supor que $p_1 | q_1$. Como ambos são primos, isto implica que $p_1 = q_1$. Portanto, temos

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Agora, repetindo o mesmo processo para todo $p_2, p_3, \ldots, p_r$ chegamos a conclusão de que, para todo $1 \leq i \leq r$ tem-se $p_i = q_i$, e ainda $r \leq s$.

Fazendo o mesmo para o produto $q_2 \cdots q_s$, chegamos a conclusão de que, para todo $1 \leq j \leq s$ tem-se $q_j = p_i$, e ainda $s \leq r$. Logo, $r = s$ e para todo $1 \leq i \leq r$, temos que $p_i = q_i$.

■

Existem várias formas de se provar a infinitude dos números primos, neste trabalho optamos por fazê-la por partes. Mostraremos primeiramente que existem infinitos números primos da forma $4m + 3$, em que $m \in \mathbb{N}$ e, mais adiante, mostraremos também que existem infinitos números primos da forma $4m + 1$, provando assim a infinitude dos números primos.

Proposição 1.26. *Existem infinitos números primos naturais da forma* $4m + 3$*, em que* $m \in \mathbb{N}$*.*

Demonstração. Suponhamos por absurdo, que exista uma quantidade finita de números primos naturais da forma $4m+3$, digamos $k+1$. Note que $k \in \mathbb{N}$, pois existe pelo menos um primo desta forma, o 3. Sejam $3, p_1, p_2, \ldots, p_k$ todos os números primos naturais da forma $4m + 3$. Podemos supor, sem perda de generalidade que $3 < p_1 < p_2 < \ldots < p_k$, ou seja, para todos $i, j \in \{1, \ldots, k\}$, se $i < j$, então $p_i < p_j$ e, além disso, para todo $i \in \{1, \ldots, k\}$ temos que $3 < p_i$.

Seja

$$a = 4p_1 p_2 \cdots p_k + 3.$$

Note que nenhum dos números primos $3, p_1, p_2, \ldots, p_k$ é fator primo de a, pois $3|3$, mas $3 \nmid 4p_1 p_2 \cdots p_k$ e para todo $i \in \{1, 2, \ldots, k\}$, $p_i | 4p_1 p_2 \cdots p_k$, mas $p_i \nmid 3$, pois $p_i > 3$. Portanto, a não possui fator primo da forma $4m + 3$, o que implica que a possui apenas fatores primos da forma $4m + 1$ na sua decomposição, já que a é ímpar.

Então, existe $n \in \mathbb{N}^*$ e, para todo $i \in \{1, 2, \ldots, n\}$ existem $m_i, \alpha_i \in \mathbb{N}$, com $\alpha_i \neq 0$, tais que

$$a = 4p_1p_2 \cdots p_k + 3 = (4m_1 + 1)^{\alpha_1}(4m_2 + 1)^{\alpha_2} \cdots (4m_n + 1)^{\alpha_n}.$$

Mas, para quaisquer $a, b \in \mathbb{N}$, o produto $(4a + 1)(4b + 1)$ é da forma $4x + 1$ para algum $x \in \mathbb{N}$, veja:

$$(4a + 1)(4b + 1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1.$$

Logo,

$$a = 4p_1p_2 \cdots p_k + 3 = 4y + 1,$$

para algum $y \in \mathbb{N}$, ou seja, a deixa resto 1 na divisão euclidana por 4. Mas isto é um absurdo, pois a é da forma $4m + 3$, logo, a deixa resto 3 na divisão euclidiana por 4 e pelo algoritmo da divisão euclidiana o resto é único. Portanto, existem infinitos números primos naturais da forma $4m + 3$.

■

Mais adiante no trabalho mostraremos que existem infinitos números primos naturais da forma $4m + 1$, em que $m \in \mathbb{N}$.

1.3 RELAÇÕES DE EQUIVALÊNCIA

As relações de equivalência desempenham um papel importante na Matemática, pois, por exemplo, dado um conjunto, podemos estudá-lo separando-o em classes de modo que todos os elementos de cada classe possam ser vistos como "iguais" em um certo sentido. Por exemplo, dado o conjunto de todos os seres humanos, podemos separá-lo em duas classes, a classe dos homens, que denotaremos por H e a classe das mulheres, que denotaremos por M. Desta forma, todo ser humano pertence a um dos elementos do conjunto $\{H, M\}$.

O mesmo pode ser feito em qualquer conjunto, quando desejamos tratar da mesma maneira elementos que satisfaçam determinadas propriedades. Por exemplo, no conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, podemos separar todos os números em duas classes: a classe dos números pares, que será denotada por P, e a classe dos números ímpares, que será denotada por I, formando assim um novo conjunto, o qual será da forma $\{P, I\}$, em que $P = \{x \in \mathbb{N} \mid x = 2n, \text{ para algum } n \in \mathbb{N}\}$ e $I = \{x \in \mathbb{N} \mid x = 2n + 1, \text{ para algum } n \in \mathbb{N}\}$.

Apresentaremos nesta seção a definição de uma relação de equivalência, de uma classe de equivalência e também de um conjunto quociente. Estes conceitos serão importantes para o desenvolvimento dos resultados que apresentaremos neste trabalho.

Antes de definirmos uma relação de equivalência, veremos a definição de *relação* entre conjuntos.

Definição 1.27. *Dados os conjuntos A e B, uma* relação *de A em B, que será denotada por $\sim$, é um subconjunto de $A \times B$, ou seja, é um conjunto de pares ordenados de $A \times B$. Quando $(x, y) \in \sim$ dizemos que x e y* estão relacionados *segundo $\sim$. E, neste caso, escrevemos $x \sim y$, que lê-se x* está relacionado com *y.*

Quando $\sim$ for uma relação de A em A, escreveremos que $\sim$ é uma relação sobre A.

Veja o seguinte exemplo:

Exemplo 1.28. Dado o conjunto $A = \{1, 2, 3\}$. A relação $\sim = \{(x, y) \in A \times A \mid x - y \text{ é } par\}$ é:

$$\sim = \{(1,1), (1,3), (2,2), (3,1), (3,3)\},$$

pois

$$\begin{aligned} 1-1 &= \ \ 0, \\ 1-3 &= -2, \\ 2-2 &= \ \ 0, \\ 3-1 &= \ \ 2, \\ 3-3 &= \ \ 0. \end{aligned}$$

Já os pares $(1,2), (2,1), (2,3)$ e $(3,2)$ não pertentem a $\sim$, pois

$$\begin{aligned} 1-2 &= -1, \\ 2-1 &= \ \ 1, \\ 2-3 &= -1, \\ 3-2 &= \ \ 1. \end{aligned}$$

Mais adiante no trabalho precisaremos mostrar que uma determinada relação é uma função, por este motivo, apresentaremos a seguir a definição de função. Existem muitas coisas a serem estudadas sobre funções, mas como este não é o objetivo deste trabalho, vamos nos ater

apenas a definição e a um exemplo simples.

Definição 1.29. *Dados os conjuntos A e B, uma* função *f de A em B, denotada por $f : A \to B$, é uma relação $f \subseteq A \times B$ que satisfaz as seguintes condições:*

i) todo elemento de A está relacionado a um elemento de B;

ii) todo elemento de A está relacionado a um único elemento de B.

Exemplo 1.30. No *Exemplo 1.28*, definimos uma relação, note que a relação definida não é uma função, pois o elemento 1 se relaciona com os elementos 1 e 3. Para ser função, ele deveria estar relacionado a um único elemento. Note que o mesmo ocorre com o elemento 3.

Exemplo 1.31. Vamos verificar se a relação de $A = \{3, 8, 15, 24\}$ em $B = \{2, 3, 4, 5\}$, definida por $\sim = \{(a, b) \in A \times B \mid b = \sqrt{a+1}\}$ é uma função.

Temos que

$$\sim = \{(3, 2), (8, 3), (15, 4), (24, 5)\},$$

pois

$$\begin{aligned} \sqrt{3+1} &= 2, \\ \sqrt{8+1} &= 3, \\ \sqrt{15+1} &= 4, \\ \sqrt{24+1} &= 5. \end{aligned}$$

Perceba que cada elemento de A está relacionado a um único elemento de B. Logo, $\sim$ é uma função.

Apresentaremos agora um tipo de relação chamada *relação de equivalência*. Este tipo de relação será de extrema importância, pois nos ajudará a demonstrar o principal lema do nosso trabalho, *Lema 2.3*.

Definição 1.32. *Sejam X um conjunto e $\sim$ uma relação sobre X. Dizemos que $\sim$ é uma relação de equivalência se, para todos $x, y, z \in X$ valem as seguintes propriedades:*

- ***Reflexiva:*** *$x \sim x$.*
- ***Simétrica:*** *se $x \sim y$, então $y \sim x$.*
- ***Transitiva:*** *se $x \sim y$ e $y \sim z$, então $x \sim z$.*

Exemplo 1.33. Em $\mathbb{Z}$, a relação definida para quaisquer $a, b \in \mathbb{Z}$ por "$a \sim b$ se, e somente se, $a - b$ é um múltiplo de 3", é uma relação de equivalência, pois:

- (Reflexiva) para todo $a \in \mathbb{Z}$, temos que $a - a = 0 = 3 \cdot 0$. Logo, $a \sim a$.
- (Simétrica) sejam $a, b \in \mathbb{Z}$ tais que $a \sim b$. Logo $a - b = 3k$, para algum $k \in \mathbb{Z}$, então $b - a = 3(-k)$. Portanto, se $a \sim b$, então $b \sim a$.
- (Transitiva) sejam $a, b, c \in \mathbb{Z}$ tais que $a \sim b$ e $b \sim c$, então $a - b = 3k$ e $b - c = 3m$ para algum $k, m \in \mathbb{Z}$, logo, $a - c = (a - b) + (b - c) = 3k + 3m = 3(k + m)$. Portanto, se $a \sim b$ e $b \sim c$, então $a \sim c$.

Como $\sim$ é reflexiva, simétrica e transitiva, concluímos que $\sim$ é de fato uma relação de equivalência.

No início desta seção falamos que dado um conjunto, podemos separar seus elementos em classes de modo que todos os elementos de cada classe satisfaçam determinada propriedade. Veremos abaixo como são estas classes e qual sua denominação.

Definição 1.34. *Seja $\sim$ uma relação de equivalência sobre um conjunto X. Dado $x \in X$, chama-se* classe de equivalência *determinada por x, e indica-se por $\overline{x}$, o subconjunto de X formado por todos os elementos de X que se relacionam com x segundo a relação $\sim$, ou seja,*

$$\overline{x} = \{a \in X \mid a \sim x\}.$$

E neste caso, x será denominado um representante *da classe de equivalência $\overline{x}$.*

Note que na definição acima podemos usar tanto $a \sim x$ quanto $x \sim a$, pois como $\sim$ é simétrica, as duas relações são equivalentes.

A seguir, veremos um teorema que mostra que qualquer elemento de uma classe pode ser um representante dela.

Teorema 1.35. *Seja $\sim$ uma relação de equivalência em um conjunto X e sejam $a, b \in X$. As seguintes afirmações são equivalentes:*

(i) $a \sim b$,

(ii) $a \in \overline{b}$,

(iii) $b \in \overline{a}$,

(iv) $\overline{a} = \overline{b}$.

Demonstração. (i) $\Rightarrow$ (ii) $\overline{b} = \{x \in X \mid x \sim b\}$. Como $a \sim b$, temos que, $a \in \overline{b}$.
(ii) $\Rightarrow$ (iii) Se $a \in \overline{b}$, então $a \sim b$. Como $\sim$ é uma relação de equivalência, e portanto, é simétrica, temos que $b \sim a$. Logo, $b \in \overline{a}$.
(iii) $\Rightarrow$ (iv) Para mostrar que $\overline{a} = \overline{b}$, temos que mostrar que $\overline{a} \subseteq \overline{b}$ e $\overline{b} \subseteq \overline{a}$. Vamos iniciar mostrando que $\overline{a} \subseteq \overline{b}$.

Seja x um elemento qualquer de $\overline{a}$, então $x \sim a$. Mas, por hipótese, $b \in \overline{a}$, então $a \sim b$. Assim, pela transitividade da relação $\sim$ temos que $x \sim b$, ou seja, $x \in \overline{b}$. Portanto, $\overline{a} \subseteq \overline{b}$.

De modo análogo, mostra-se que $\overline{b} \subseteq \overline{a}$.

Portanto, como $\overline{a} \subseteq \overline{b}$ e $\overline{b} \subseteq \overline{a}$, temos que $\overline{a} = \overline{b}$.
(iv) $\Rightarrow$ (i) Como $\sim$ é uma relação de equivalência, é portanto, reflexiva. Assim, $a \sim a$, logo $a \in \overline{a} = \overline{b}$. Portanto, $a \sim b$.

■

Exemplo 1.36. Considere a relação de equivalência definida no *Exemplo 1.33*, vamos analisar quais são as classes de equivalência segundo $\sim$.

Seja a um número inteiro qualquer. Considere a divisão euclidiana de a por 3, então sabemos que existem únicos inteiros q e r tais que $a = 3q + r$, com $0 \leq r < 3$, ou seja, r pode assumir apenas os valores $0, 1$ ou 2.

Sendo $a = 3q + r$, segue que $a - r = 3q$. Se $r = 0$, temos $a = 3q$ logo, $a \sim 0$; se $r = 1$, temos $a - 1 = 3q$, logo, $a \sim 1$; e se $r = 2$, temos $a - 2 = 3q$, portanto $a \sim 2$. Desta forma as classes de equivalência de $\sim$ são:

$$\begin{aligned} \overline{0} &= \{3q \mid q \in \mathbb{Z}\}, \\ \overline{1} &= \{3q + 1 \mid q \in \mathbb{Z}\}, \\ \overline{2} &= \{3q + 2 \mid q \in \mathbb{Z}\}. \end{aligned}$$

O *Teorema 1.35* mostra que qualquer elemento da classe pode ser um representante da classe. Assim, no exemplo acima, temos que, por exemplo, $\overline{1} = \overline{4} = \overline{7} = \overline{10}$, etc.

Até aqui vimos que, dados um conjunto e uma relação $\sim$ sobre ele, podemos particioná-lo em classes de equivalência. Agora veremos que o conjunto formado por estas classes de equivalência recebe uma denominação específica.

Definição 1.37. *Seja $\sim$ uma relação de equivalência sobre um con-*

junto X. O conjunto de todas as classes de equivalência segundo $\sim$ é chamado de conjunto quociente *e é denotado por $X/\sim$. Portanto,*

$$X/\sim = \{\overline{x} \mid x \in X\}.$$

Exemplo 1.38. Vamos determinar o conjunto quociente da relação definida no *Exemplo 1.33*.

Vimos no *Exemplo 1.36* que as classes de equivalência segundo $\sim$ são $\overline{0}, \overline{1}, \overline{2}$, logo

$$X/\sim = \{\overline{0}, \overline{1}, \overline{2}\}.$$

1.4 CONGRUÊNCIAS

O conceito de congruência será muito utilizado neste trabalho, portanto, faremos uma seção dedicada a este tema para apresentarmos algumas definições e resultados importantes.

Definição 1.39. *Seja m um número natural maior que zero. Diremos que dois números inteiros a e b são* congruentes *módulo m, se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escrevemos*

$$a \equiv b \pmod{m}.$$

Exemplo 1.40. Temos que $15 \equiv 21 \pmod{2}$, já que os restos da divisão euclidiana de 15 e 21 por 2 são iguais a 1.

Definição 1.41. *Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que a e b* não são congruentes *módulo m. Escreveremos, neste caso,*

$$a \not\equiv b \pmod{m}.$$

Exemplo 1.42. $30 \not\equiv 18 \pmod{15}$, pois o resto da divisão euclidiana de 30 por 15 é 0 e o resto da divisão euclidiana de 18 por 15 é 3, ou seja, os restos são diferentes.

Para verificar se um número é congruente a outro módulo m, não é necessário realizar a divisão euclidiana desses números para comparar os restos obtidos. É suficiente aplicar o resultado a seguir:

Proposição 1.43. *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 0$. Tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m|b - a$.*

Demonstração. ($\Rightarrow$) Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$ tais que $a \equiv b \pmod{m}$. Então, a e b deixam o mesmo resto na divisão euclidiana por m, logo, existem únicos inteiros q_1, q_2, r tais que $a = mq_1 + r$ e $b = mq_2 + r$, com $0 \leq r < m$. Desta forma,

$$\begin{aligned} b - a &= mq_2 + r - (mq_1 + r) \\ &= m(q_2 - q_1). \end{aligned}$$

Ou seja, $m|(b-a)$.

($\Leftarrow$) Suponha que $m|(b-a)$. Pelo Algoritmo da Divisão Euclidiana, existem inteiros q_1, q_2, r_1, r_2 tais que $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leq r_1, r_2 < m$. Logo,

$$\begin{aligned} b - a &= mq_2 + r_2 - (mq_1 + r_1) \\ &= m(q_2 - q_1) + (r_2 - r_1). \end{aligned}$$

Pela hipótese, temos que $m|(b-a)$. Então pela *Proposição 1.3* $m|(r_2 - r_1)$, ou seja $r_2 - r_1$ é um múltiplo de m, mas $|r_2 - r_1| < m$. Logo $r_2 - r_1 = 0$ e portanto $r_2 = r_1$. Segue que, $a \equiv b \pmod{m}$.

■

Observe que se m divide $b-a$ então m divide também $a-b$, pois se $m|(b-a)$ então existe um inteiro k tal que $b - a = mk$, daí segue que $a - b = m(-k)$, ou seja, $m|(a-b)$. Do mesmo modo, prova-se que se $m|(a-b)$, então $m|(b-a)$.

Vamos agora mostrar que a congruência módulo um número natural fixado m, é uma *relação de equivalência*.

Proposição 1.44. *Seja m um número natural maior que zero. Para todos $a, b, c \in \mathbb{Z}$, tem-se as seguintes propriedades.*

(i) Reflexiva: $a \equiv a \pmod{m}$.

(ii) Simétrica: se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

(iii) Transitiva: se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração. (i) Tome $a \in \mathbb{Z}$ qualquer, como $m|(a-a) = 0$, temos que $a \equiv a \pmod{m}$.

(ii) Sejam $a, b \in \mathbb{Z}$ tais que $a \equiv b \pmod{m}$, então temos que $m|(b-a)$, logo $m|(a-b)$. Portanto, $b \equiv a \pmod{m}$.

(iii) Sejam $a, b, c \in \mathbb{Z}$ tais que $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então segue que $m|(a-b)$ e $m|(b-c)$, logo $m|[(a-b)+(b-c)]$, ou seja, $m|(a-c)$. Portanto, $a \equiv c \pmod{m}$.

■

Esta proposição nos diz que a congruência módulo m, definida no conjunto dos números inteiros, é uma relação de equivalência, pois acabamos de ver que ela é reflexiva, simétrica e transitiva.

Assim, $\mathbb{Z}$ pode ser particionado em classes de equivalências com respeito a esta relação de equivalência.

Sendo assim, para cada natural a tal que $0 \leq a \leq m-1$, define-se a classe de congruência módulo m determinada por a como sendo o conjunto

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\}.$$

O conjunto formado pelas classes de equivalência dos elementos de $\mathbb{Z}$ será denotado por $\mathbb{Z}_m$. Desta forma, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

Observe que o número total de classes para todo natural m é igual a m, pois os restos possíveis na divisão euclidiana por m são: $0, 1, 2, \ldots, m-1$.

Exemplo 1.45. Como os restos possíveis na divisão euclidiana por 5 são 0, 1, 2, 3 e 4, temos que $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

A seguir, iremos enunciar e demonstrar uma série de resultados que serão utilizados no próximo capítulo. Em todos estes resultados, considere m um número natural maior que 1.

Proposição 1.46. *Sejam $a, b, c, d \in \mathbb{Z}$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.*

Demonstração. Sejam $a, b, c, d \in \mathbb{Z}$ tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $m|(b-a)$ e $m|(d-c)$. Logo, pela *Proposição 1.6*, segue que $m|[(b-a)+(d-c)]$, ou seja, $m|[(b+d)-(a+c)]$. Portanto, $a + c \equiv b + d \pmod{m}$.

■

Proposição 1.47. *Sejam $a, b, c, d \in \mathbb{Z}$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.*

Demonstração. Sejam $a, b, c, d \in \mathbb{Z}$ tais que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $m|(b-a)$ e $m|(d-c)$.

Note que $bd - ac = d(b-a) + a(d-c)$. Como m divide as duas parcelas do segundo membro da igualdade, temos que $m|(bd-ac)$. Portanto, $ac \equiv bd \pmod{m}$.

■

Enunciaremos a seguir um resultado que será necessário para demonstrarmos a *Proposição 1.49*, a demonstração deste resultado pode ser consultada na página 43 de [DOMINGUES, 2009].

Proposição 1.48. (Princípio da Indução Finita) *Seja $a \in \mathbb{N}$ e suponha que a cada número natural $n \geq a$ esteja associada uma afirmação $P(n)$. Admita ainda que seja possível provar o seguinte:*

i) $P(a)$ é verdadeira.

ii) Para todo $r \geq a$, se $P(r)$ é verdadeira, então $P(r+1)$ também é verdadeira.

Então $P(n)$ é verdadeira para todo $n \geq a$.

Proposição 1.49. *Sejam $n \in \mathbb{N}^*$ e $a, b \in \mathbb{Z}$. Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.*

Demonstração. Esta demonstração será feita por indução. Sejam $a, b \in \mathbb{Z}$ tais que $a \equiv b \pmod{m}$.

Para $n = 1$, temos que $a^1 \equiv b^1 \pmod{m}$ é verdadeira.

Suponhamos que $a^n \equiv b^n \pmod{m}$, para algum natural n. Vamos verificar se $a^{n+1} \equiv b^{n+1} \pmod{m}$.

Temos que

$$a^n \equiv b^n \pmod{m}$$

e

$$a \equiv b \pmod{m}.$$

Então, pela *Proposição 1.47* temos que

$$a^n \,.\, a \equiv b^n \,.\, b \pmod{m}.$$

Logo,

$$a^{n+1} \equiv b^{n+1} \pmod{m}.$$

Portanto, pelo Princípio da Indução Finita, a proposição é verdadeira.

■

Proposição 1.50. *Sejam $a, b, c \in \mathbb{Z}$. Tem-se que*

$$a + c \equiv b + c \pmod{m} \iff a \equiv b \pmod{m}.$$

Demonstração. Sejam $a, b, c \in \mathbb{Z}$.

($\Rightarrow$) Suponha que $a + c \equiv b + c \pmod{m}$, então $m|[(b + c) - (a + c)]$, ou seja, $m|(b - a)$. Logo $a \equiv b \pmod{m}$.

($\Leftarrow$) Suponha $a \equiv b \pmod{m}$. Sabe-se que $c \equiv c \pmod{m}$. Portanto, pela *Proposição 1.46*, segue que $a + c \equiv b + c \pmod{m}$.

■

A proposição acima nos diz que vale o cancelamento com relação à adição para congruências. Contudo, veremos que, em geral, não vale o cancelamento para a multiplicação.

Exemplo 1.51. Note que $6 \cdot 7 \equiv 6 \cdot 3 \pmod{3}$, porém, $7 \not\equiv 3 \pmod{3}$, pois $3 \nmid (7 - 3)$. Assim, neste caso, não vale o cancelamento do fator 6.

A seguir, enunciaremos um resultado relacionado ao cancelamento multiplicativo, sua demonstração pode ser encontrada na página 196 de [HEFEZ, 2014].

Proposição 1.52. *Sejam $a, b, c \in \mathbb{Z}$. Temos que*

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{(c, m)}}.$$

Vimos anteriormente que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$. Agora veremos que podem ser definidas operações de adição e multiplicação em $\mathbb{Z}_m$. Primeiramente definiremos duas relações sobre $\mathbb{Z}_m$, que serão denotadas pelos símbolos $+$ e $\cdot$, tais relações serão um subconjunto de $(\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$. Depois, mostraremos que estas relações são funções.

Definição 1.53. *Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_m$, vamos definir duas relações:*

$$\begin{aligned} + &= \left\{ \left((\overline{a}, \overline{b}), \overline{a+b} \right) \mid (\overline{a}, \overline{b}) \in \mathbb{Z}_m \times \mathbb{Z}_m \right\}; \\ \cdot &= \left\{ \left((\overline{a}, \overline{b}), \overline{a \cdot b} \right) \mid (\overline{a}, \overline{b}) \in \mathbb{Z}_m \times \mathbb{Z}_m \right\}. \end{aligned}$$

Se $\left((\overline{a}, \overline{b}), \overline{c} \right) \in +$ representaremos isto usando a seguinte notação

$$\overline{a} + \overline{b} = \overline{c},$$

ou seja,

$$\overline{a} + \overline{b} = \overline{a + b},$$

pois se $\big((\overline{a},\overline{b}),\overline{c}\big) \in +$ *isso significa que*

$$\overline{c} = \overline{a+b}.$$

Se $\big((\overline{a},\overline{b}),\overline{c}\big) \in \cdot$ *representaremos isto usando a seguinte notação*

$$\overline{a} \cdot \overline{b} = \overline{c},$$

ou seja,

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b},$$

pois se $\big((\overline{a},\overline{b}),\overline{c}\big) \in \cdot$ *isso significa que*

$$\overline{c} = \overline{a \cdot b}.$$

Exemplo 1.54. Considere $m = 7$.
$\big((\overline{2},\overline{3}),\overline{5}\big) \in +$, já que $\overline{2+3} = \overline{5}$. O fato que $\big((\overline{2},\overline{3}),\overline{5}\big) \in +$ é denotado da seguinte forma

$$\overline{2} + \overline{3} = \overline{5}.$$

$\big((\overline{2},\overline{3}),\overline{6}\big) \in \cdot$, pois $\overline{2 \cdot 3} = \overline{6}$. O fato que $\big((\overline{2},\overline{3}),\overline{6}\big) \in \cdot$ é denotado da seguinte forma

$$\overline{2} \cdot \overline{3} = \overline{6}.$$

Proposição 1.55. *As relações definidas em* 1.53 *são funções. Ou seja, para* $\overline{a},\overline{a'},\overline{b},\overline{b'} \in \mathbb{Z}_m$, *se* $\overline{a} = \overline{a'}$ *e* $\overline{b} = \overline{b'}$ *então* $\overline{a+b} = \overline{a'+b'}$ *e* $\overline{ab} = \overline{a'b'}$.

Demonstração. Sejam $\overline{a},\overline{a'},\overline{b},\overline{b'} \in \mathbb{Z}_m$ tais que $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Então, $a \equiv a' \pmod m$ e $b \equiv b' \pmod m$, logo, $m|(a-a')$ e $m|(b-b')$. Portanto, existem $x, y \in \mathbb{Z}$ tais que $a - a' = mx$ e $b - b' = my$. Somando estas duas equações temos que

$$\begin{aligned} (a-a') + (b-b') &= mx + my \\ (a+b) - (a'+b') &= m(x+y). \end{aligned}$$

Logo, $a + b \equiv a' + b' \pmod m$. Portanto, $\overline{a+b} = \overline{a'+b'}$.

Vamos mostrar agora que $\overline{ab} = \overline{a'b'}$.

Sendo $a - a' = mx$ e $b - b' = my$, temos que $a = a' + mx$ e $b = b' + my$. Assim,

$$\begin{aligned} ab &= (a'+mx)(b'+my) \\ &= a'b' + a'my + b'mx + m^2xy \\ &= a'b' + m(a'y + b'x + mxy). \end{aligned}$$

Logo, $ab - a'b' = m(a'y + b'x + mxy)$. Desta forma, $ab \equiv a'b' \pmod{m}$. Portanto, $\overline{ab} = \overline{a'b'}$.

■

Acabamos de provar que as relações definidas em *1.53* são funções. Estas funções são chamadas, respectivamente, de *operação de adição* e *operação de multiplicação* em $\mathbb{Z}_m$.

Observação 1.56. *Seja $\overline{a} \in \mathbb{Z}_m$, temos que:*

- $\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$;
- $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}$.

Logo, $\overline{0}$ é o *elemento neutro* da operação de adição e $\overline{1}$ é o *elemento neutro* da operação de multiplicação em $\mathbb{Z}_m$.

Definiremos agora, o inverso aditivo e o inverso multiplicativo em $\mathbb{Z}_m$.

Definição 1.57. *Seja $a \in \mathbb{Z}$. Um* inverso aditivo *de a módulo m é o inteiro b tal que*

$$a \equiv -b \pmod{m},$$

ou seja,

$$a + b \equiv 0 \pmod{m}.$$

Note que, se b é um inverso aditivo de a, então todo b' tal que $b' \equiv b \pmod{m}$ é também o inverso aditivo de a, pois se

$$b' \equiv b \pmod{m}$$

somando a nos dois membros da congruência obtemos

$$a + b' \equiv a + b \pmod{m} \Rightarrow a + b' \equiv 0 \pmod{m}.$$

Logo, se b é o inverso aditivo de a, podemos concluir que, $\overline{b}$ é a classe do inverso aditivo da classe $\overline{a}$ em $\mathbb{Z}_m$.

Portanto, podemos enunciar novamente esta definição, mas agora usando as classes de equivalência módulo m.

Definição 1.58. *Seja $\overline{a} \in \mathbb{Z}_m$. O* inverso aditivo *de $\overline{a}$ em $\mathbb{Z}_m$ é a classe $\overline{b}$ tal que*

$$\overline{a} + \overline{b} = \overline{0} = \overline{b} + \overline{a}.$$

Exemplo 1.59.

a) A classe do inverso aditivo de $\overline{2}$ em $\mathbb{Z}_7$ é $\overline{5}$, pois:

$$\overline{2} + \overline{5} = \overline{2+5} = \overline{7} = \overline{0}.$$

b) $\overline{1}$ é a classe do inverso aditivo de $\overline{6}$ em $\mathbb{Z}_7$, pois:

$$\overline{1} + \overline{6} = \overline{1+6} = \overline{7} = \overline{0}.$$

Definição 1.60. *Seja $a \in \mathbb{Z}$. Um* inverso multiplicativo *de a módulo m é o inteiro b tal que*

$$a \cdot b \equiv 1 \pmod{m}.$$

Note que, assim como no inverso aditivo, se b é o inverso multiplicativo de a, então todo b' tal que $b' \equiv b \pmod{m}$ é também o inverso multiplicativo de a, pois se

$$b' \equiv b \pmod{m},$$

multiplicando por a os dois membros da congruência obtemos

$$a \cdot b' \equiv a \cdot b \pmod{m} \Rightarrow a \cdot b' \equiv 1 \pmod{m}.$$

Logo, se b é o inverso multiplicativo de a, podemos concluir que, $\overline{b}$ é a classe do inverso multiplicativo da classe $\overline{a}$ em $\mathbb{Z}_m$.

Assim, podemos enunciar novamente esta definição, agora usando as classes de equivalência módulo m.

Definição 1.61. *Seja $\overline{a} \in \mathbb{Z}_m$. O* inverso multiplicativo *de $\overline{a}$ em $\mathbb{Z}_m$ é a classe $\overline{b}$ tal que*

$$\overline{a} \cdot \overline{b} = \overline{1} = \overline{b} \cdot \overline{a}.$$

Exemplo 1.62.

a) A classe do inverso multiplicativo de $\overline{2}$ em $\mathbb{Z}_7$ é $\overline{4}$, pois:

$$\overline{2} \cdot \overline{4} = \overline{2 \cdot 4} = \overline{8} = \overline{1}.$$

b) $\overline{5}$ é a classe do inverso multiplicativo de $\overline{3}$ em $\mathbb{Z}_7$, pois:

$$\overline{5} \cdot \overline{3} = \overline{5 \cdot 3} = \overline{15} = \overline{1}.$$

Observação 1.63. *Nem todo* $\overline{a} \in \mathbb{Z}_m$ *possui inverso multiplicativo. Por exemplo,* $\overline{2} \in \mathbb{Z}_4$ *não possui.*

2 NÚMEROS REPRESENTÁVEIS

Seja p um número primo ímpar e $X = \{0, 1, 2, \ldots, p-1\}$ o conjunto formado pelos restos possíveis na divisão euclidiana por p. Vamos construir uma relação de equivalência neste conjunto que nos permitirá particioná-lo, uma vez que ele ficará dividido em subconjuntos denominados classes de equivalência, formadas pelos elementos que estão relacionados. Essa partição será importante para a demonstração do *Lema 2.3*.

Definiremos uma relação $\sim$ no conjunto X. Para isso, tomaremos dois elementos $x, y \in X$ e utilizaremos o símbolo $\sim$, inserido entre eles $(x \sim y)$, indicando que x se relaciona com y caso satisfaçam pelo menos uma das quatro condições descritas abaixo:

$$\begin{array}{rcrll} x & \equiv & y & (mod\ \ p), & ou \\ x & \equiv & -y & (mod\ \ p), & ou \\ x \cdot y & \equiv & 1 & (mod\ \ p), & ou \\ x \cdot -y & \equiv & 1 & (mod\ \ p). & \end{array}$$

Usaremos a notação $[x]$ para representar a classe dos elementos pertencentes a X que se relacionam com x segundo a relação de equivalência definida acima.

Dessa forma, a classe $[x]$ irá conter os elementos $\{x, -x, \widehat{x}, -\widehat{x}\} \subseteq X$, em que $-x$ denota um representante da classe do inverso aditivo de $\overline{x}$ em $\mathbb{Z}_p$, $\widehat{x}$ um representante da classe do inverso multiplicativo de $\overline{x}$ em $\mathbb{Z}_p$ e $-\widehat{x}$ um representante da classe do inverso multiplicativo do inverso aditivo de $\overline{x}$ em $\mathbb{Z}_p$.

Antes de mostrarmos que $\sim$ é uma relação de equivalência vamos analisar um exemplo para compreender melhor esta relação.

Exemplo 2.1. Seja $p = 7$, então nesse caso $X = \{0, 1, 2, 3, 4, 5, 6\}$. Vamos analisar quem são as classes de equivalência em X.

- $[0] = \{0\}$: O elemento zero só se relaciona com ele mesmo, pois:

$$\begin{array}{rcrll} 0 & \equiv & 0 & (mod\ \ 7), \\ 0 & \equiv & -0 & (mod\ \ 7), \end{array}$$

e não existe $y \in X$ que satisfaça as equações:

$$\begin{array}{rcrll} 0 \cdot y & \equiv & 1 & (mod\ \ 7) & \text{e} \\ 0 \cdot -y & \equiv & 1 & (mod\ \ 7), & \end{array}$$

pois a classe do zero não possui inverso multiplicativo em $\mathbb{Z}_p$.

- $[1] = \{1, 6\}$: O elemento 1 se relaciona com os elementos 1 e 6, pois:

$$\begin{aligned} 1 \cdot 1 &\equiv 1 \pmod{7} \quad \text{e} \\ 1 &\equiv -6 \pmod{7}. \end{aligned}$$

Note que o elemento 6 também se relaciona com 1 e 6:

$$\begin{aligned} 6 &\equiv -1 \pmod{7} \quad \text{e} \\ 6 \cdot 6 &\equiv 1 \pmod{7}, \end{aligned}$$

portanto o 1 e o 6 são elementos de [1]. Vamos mostrar agora que o elemento 1 não se relaciona com nenhum outro elemento de X. Ou seja, que 1 não se relaciona com $0, 2, 3, 4$ e 5. Veja:

$$\begin{aligned} 1 &\not\equiv 0 \pmod{7}, \\ 1 &\not\equiv -0 \pmod{7}, \\ 1 \cdot 0 &\not\equiv 1 \pmod{7}, \\ 1 \cdot -0 &\not\equiv 1 \pmod{7}, \end{aligned}$$

$$\begin{aligned} 1 &\not\equiv 2 \pmod{7}, \\ 1 &\not\equiv -2 \pmod{7}, \\ 1 \cdot 2 &\not\equiv 1 \pmod{7}, \\ 1 \cdot -2 &\not\equiv 1 \pmod{7}, \end{aligned}$$

$$\begin{aligned} 1 &\not\equiv 3 \pmod{7}, \\ 1 &\not\equiv -3 \pmod{7}, \\ 1 \cdot 3 &\not\equiv 1 \pmod{7}, \\ 1 \cdot -3 &\not\equiv 1 \pmod{7}, \end{aligned}$$

$$\begin{aligned} 1 &\not\equiv 4 \pmod{7}, \\ 1 &\not\equiv -4 \pmod{7}, \\ 1 \cdot 4 &\not\equiv 1 \pmod{7}, \\ 1 \cdot -4 &\not\equiv 1 \pmod{7}, \end{aligned}$$

$$\begin{aligned} 1 &\not\equiv 5 \pmod{7}, \\ 1 &\not\equiv -5 \pmod{7}, \\ 1 \cdot 5 &\not\equiv 1 \pmod{7}, \\ 1 \cdot -5 &\not\equiv 1 \pmod{7}. \end{aligned}$$

Pelas contas feitas, vemos que de fato, 1 não se relaciona com $0, 2, 3, 4$ e 5. Agora vamos mostrar que o elemento 6 também não

se relaciona com os elementos $0, 2, 3, 4$ e 5.

$$\begin{aligned}
6 &\not\equiv 0 \pmod 7,\\
6 &\not\equiv -0 \pmod 7,\\
6 \cdot 0 &\not\equiv 1 \pmod 7,\\
6 \cdot -0 &\not\equiv 1 \pmod 7,
\end{aligned}$$

$$\begin{aligned}
6 &\not\equiv 2 \pmod 7,\\
6 &\not\equiv -2 \pmod 7,\\
6 \cdot 2 &\not\equiv 1 \pmod 7,\\
6 \cdot -2 &\not\equiv 1 \pmod 7,
\end{aligned}$$

$$\begin{aligned}
6 &\not\equiv 3 \pmod 7,\\
6 &\not\equiv -3 \pmod 7,\\
6 \cdot 3 &\not\equiv 1 \pmod 7,\\
6 \cdot -3 &\not\equiv 1 \pmod 7,
\end{aligned}$$

$$\begin{aligned}
6 &\not\equiv 4 \pmod 7,\\
6 &\not\equiv -4 \pmod 7,\\
6 \cdot 4 &\not\equiv 1 \pmod 7,\\
6 \cdot -4 &\not\equiv 1 \pmod 7,
\end{aligned}$$

$$\begin{aligned}
6 &\not\equiv 5 \pmod 7,\\
6 &\not\equiv -5 \pmod 7,\\
6 \cdot 5 &\not\equiv 1 \pmod 7,\\
6 \cdot -5 &\not\equiv 1 \pmod 7.
\end{aligned}$$

Pelas contas feitas, provamos que 6 não se relaciona com $0, 2, 3, 4$ e 5. Portanto, $[1] = \{1, 6\}$. Neste caso, observe que $-x = 6$, $\widehat{x} = 1$ e $-\widehat{x} = 6$.

- $[2] = \{2, 3, 4, 5\}$: Vimos nos itens anteriores que os elementos $2, 3, 4$ e 5 não se relacionam com os elementos $0, 1$ e 6. Agora iremos mostrar que o elemento 2 se relaciona com os elementos 2, 3, 4, 5, veja:

$$\begin{aligned}
2 &\equiv 2 \pmod 7,\\
2 \cdot -3 &\equiv 1 \pmod 7,\\
2 \cdot 4 &\equiv 1 \pmod 7,\\
2 &\equiv -5 \pmod 7.
\end{aligned}$$

Temos também que o elemento 3 se relaciona com os elementos 2, 3, 4, 5; o elemento 4 se relaciona com os elementos 2, 3, 4, 5 e, por fim, o elemento 5 se relaciona com os elementos 2, 3, 4, 5.

Veja:

$$\begin{array}{rcrl} 3 \cdot -2 & \equiv & 1 & (mod \quad 7), \\ 3 & \equiv & 3 & (mod \quad 7), \\ 3 & \equiv & -4 & (mod \quad 7), \\ 3 \cdot 5 & \equiv & 1 & (mod \quad 7), \end{array}$$

$$\begin{array}{rcrl} 4 \cdot 2 & \equiv & 1 & (mod \quad 7), \\ 4 & \equiv & -3 & (mod \quad 7), \\ 4 & \equiv & 4 & (mod \quad 7), \\ 4 \cdot -5 & \equiv & 1 & (mod \quad 7), \end{array}$$

$$\begin{array}{rcrl} 5 & \equiv & -2 & (mod \quad 7), \\ 5 \cdot 3 & \equiv & 1 & (mod \quad 7), \\ 5 \cdot -4 & \equiv & 1 & (mod \quad 7), \\ 5 & \equiv & 5 & (mod \quad 7). \end{array}$$

Portanto, $[2] = \{2, 3, 4, 5\}$ e neste caso, observe que $-x = 5$, $\widehat{x} = 4$ e $-\widehat{x} = 3$. Como podemos ver, em todas as classes $[x]$ os elementos se relacionam entre si segundo a relação $\sim$ definida. Note que o conjunto $X = \{0, 1, 2, 3, 4, 5, 6\}$ foi particionado em três subconjuntos disjuntos: $[0]$, $[1]$ e $[2]$, pois se fizermos a união desses três conjuntos obteremos X e a intersecção de quaisquer dois deles, desde que sejam distintos, é vazia.

Proposição 2.2. *A relação $\sim$ definida anteriormente é uma relação de equivalência.*

Demonstração. Para provarmos que $\sim$ é uma relação de equivalência, precisaremos mostrar que $\sim$ é reflexiva, simétrica e transitiva. Vamos fazer a prova de cada caso.
i) Reflexiva: Seja $x \in X$. Como $x = x$, então, $x \equiv x \pmod p$, logo $x \sim x$.
ii) Simétrica: Vamos mostrar que para todos $x, y \in X$, se $x \sim y$, então $y \sim x$. Vamos dividir esta demonstração em casos. Tome $x, y \in X$, tais que $x \sim y$, então temos que:

- $x \equiv y \pmod p \Rightarrow y \equiv x \pmod p \Rightarrow y \sim x$.
- $x \equiv -y \pmod p \Rightarrow -x \equiv y \pmod p \Rightarrow y \equiv -x \pmod p \Rightarrow y \sim x$.
- $x \cdot y \equiv 1 \pmod p \Rightarrow y \cdot x \equiv 1 \pmod p \Rightarrow y \sim x$.
- $x \cdot -y \equiv 1 \pmod p \Rightarrow -x \cdot y \equiv 1 \pmod p \Rightarrow y \cdot -x \equiv 1 \pmod p \Rightarrow y \sim x$.

iii) Transitiva: Vamos mostrar que para todos $x, y, z \in X$, se $x \sim y$ e $y \sim z$, então $x \sim z$. Também dividiremos esta demonstração em casos. Tome $x, y, z \in X$, tais que $x \sim y$ e $y \sim z$, então temos que:

- se $x \equiv y \pmod p$ e $y \equiv z \pmod p$, então, $x \equiv z \pmod p$. Logo, $x \sim z$.

- se $x \equiv y \pmod p$ e $y \equiv -z \pmod p$, então, $x \equiv -z \pmod p$. Portanto, $x \sim z$.

- se $x \equiv y \pmod p$ e $y \cdot z \equiv 1 \pmod p$, multiplicando a primeira congruência por z obtemos que $x \cdot z \equiv y \cdot z \pmod p$. Assim, $x \cdot z \equiv 1 \pmod p$. Logo, $x \sim z$.

- se $x \equiv y \pmod p$ e $y \cdot -z \equiv 1 \pmod p$, multiplicando a primeira congruência por $-z$ obtemos que $x \cdot -z \equiv y \cdot -z \pmod p$. Assim, $x \cdot -z \equiv 1 \pmod p$. Portanto, $x \sim z$.

- se $x \equiv -y \pmod p$ e $y \equiv z \pmod p$, então, $-y \equiv -z \pmod p$. Logo, $x \equiv -z \pmod p$. Portanto, $x \sim z$.

- se $x \equiv -y \pmod p$ e $y \equiv -z \pmod p$, então, $-y \equiv z \pmod p$. Assim, $x \equiv z \pmod p$. Logo, $x \sim z$.

- se $x \equiv -y \pmod p$ e $y \cdot z \equiv 1 \pmod p$, então, $-y \cdot -z \equiv 1 \pmod p$ e multiplicando a primeira congruência por $-z$ obtemos que $x \cdot -z \equiv -y \cdot -z \pmod p$. Portanto, $x \cdot -z \equiv 1 \pmod p$, e disto segue que $x \sim z$.

- se $x \equiv -y \pmod p$ e $y \cdot -z \equiv 1 \pmod p$, então, $-y \cdot z \equiv 1 \pmod p$, multiplicando a primeira congruência por z obtemos que $x \cdot z \equiv -y \cdot z \pmod p$. Assim, $x \cdot z \equiv 1 \pmod p$. Portanto, $x \sim z$.

- se $x \cdot y \equiv 1 \pmod p$ e $y \equiv z \pmod p$, multiplicando a segunda congruência por x obtemos que $x \cdot y \equiv x \cdot z \pmod p$, assim, $1 \equiv x \cdot z \pmod p$, que é equivalente a $x \cdot z \equiv 1 \pmod p$. Logo, $x \sim z$.

- se $x \cdot y \equiv 1 \pmod p$ e $y \equiv -z \pmod p$, multiplicando a segunda congruência por x obtemos que $x \cdot y \equiv x \cdot -z \pmod p$. Logo, $1 \equiv x \cdot -z \pmod p$, ou seja, $x \cdot -z \equiv 1 \pmod p$. Portanto, $x \sim z$.

- se $x \cdot y \equiv 1 \pmod{p}$ e $y \cdot z \equiv 1 \pmod{p}$, então, $x \cdot y \equiv y \cdot z \pmod{p}$, como o $(y,p) = 1$, pois $y \in \{0,1,2,\ldots,p-1\}$ e $1|p$, temos que, $x \equiv z \pmod{p}$. Portanto, $x \sim z$.

- se $x \cdot y \equiv 1 \pmod{p}$ e $y \cdot -z \equiv 1 \pmod{p}$, então, $x \cdot y \equiv y \cdot -z \pmod{p}$, usando o mesmo argumento do item acima, temos que $x \equiv -z \pmod{p}$. Logo, $x \sim z$.

- se $x \cdot -y \equiv 1 \pmod{p}$ e $y \equiv z \pmod{p}$, então, $-y \equiv -z \pmod{p}$, e assim, multiplicando por x esta última congruência obtemos que $x \cdot -y \equiv x \cdot -z \pmod{p}$. Logo, $1 \equiv x \cdot -z \pmod{p}$, ou seja, $x \cdot -z \equiv 1 \pmod{p}$. Portanto, $x \sim z$.

- se $x \cdot -y \equiv 1 \pmod{p}$ e $y \equiv -z \pmod{p}$, então, $-y \equiv z \pmod{p}$, multiplicando por x esta última congruência obtemos que $x \cdot -y \equiv x \cdot z \pmod{p}$. Logo, $1 \equiv x \cdot z \pmod{p}$, portanto $x \cdot z \equiv 1 \pmod{p}$. Logo, $x \sim z$.

- se $x \cdot -y \equiv 1 \pmod{p}$ e $y \cdot z \equiv 1 \pmod{p}$, então, $-x \cdot y \equiv 1 \pmod{p}$, logo, $-x \cdot y \equiv y \cdot z \pmod{p}$. Como o $(y,p) = 1$, pois $y \in \{0,1,2,\ldots,p-1\}$ e $1|p$, temos que $-x \equiv z \pmod{p}$, assim, $x \equiv -z \pmod{p}$. Portanto, $x \sim z$.

- se $x \,.\, -y \equiv 1 \pmod{p}$ e $y \cdot -z \equiv 1 \pmod{p}$, então, $-x \cdot y \equiv 1 \pmod{p}$ e assim, $-x \cdot y \equiv y \cdot -z \pmod{p}$. Usando o mesmo argumento do item acima, temos que $-x \equiv -z \pmod{p}$, ou seja, $x \equiv z \pmod{p}$. Portanto, $x \sim z$.

Logo, $\sim$ é reflexiva, simétrica e transitiva, portanto, $\sim$ é uma relação de equivalência.

■

Sendo $\sim$ uma relação de equivalência, então, X será particionado em classes de equivalências $[x]$, onde estas classes serão da forma $[x] = \{x, -x, \widehat{x}, -\widehat{x}\}$. Note que a cardinalidade (que representaremos por $\#$) de $[x]$ é menor que ou igual a quatro, isto é, $\#\,[x] \leq 4$, já que é possível que alguns destes elementos sejam iguais. Por exemplo, vimos no *Exemplo 2.1* que se $p = 7$, $[1] = \{1, 6\}$.

Se $x = 0$, a cardinalidade de $[x]$ será um, pois a classe do inverso aditivo do $\overline{0}$ em $\mathbb{Z}_p$ é ela mesma e a classe do zero não possui inverso multiplicativo em $\mathbb{Z}_p$.

Se $x \neq 0$, então $2 \leq \#\,[x] \leq 4$, pois se $x = -x$, então $x \equiv -x \pmod{p}$, o que implica que $p|2x$. Como p é primo ímpar, isso

implica que $p|x$, o que não ocorre, pois estamos considerando $x \neq 0$ e como sabemos, $x \in \{1, 2, \ldots, p-1\}$. Portanto, $[x]$ possui pelo menos dois elementos.

Será importante provar que a cardinalidade de $[x]$ sempre é diferente de três, pois este fato será usado em demonstrações futuras. Para isso, vamos supor que a cardinalidade de $[x]$ é menor que ou igual a 3 e vamos provar que ela deve ser igual a 2 se $x \neq 0$. Para que a cardinalidade de $[x]$ seja menor que ou igual a 3 pelo menos um dos elementos $x, -x, \widehat{x}$ e $-\widehat{x}$ deve ser igual a outro. Vamos supor, sem perda de generalidade que $x = -x$ ou $x = \widehat{x}$ ou $x = -\widehat{x}$. Vamos analisar cada um dos casos.

- Se $x = -x$, então $x \equiv -x \pmod{p}$, portanto $p|2x$, mas como p é primo ímpar, isso implica que $p|x$, logo $x \equiv 0 \pmod{p}$, o que não ocorre, pois $0 < x < p$.
  Conclusão: $x \neq -x$.

- Se $x = \widehat{x}$, então $-x = -\widehat{x}$. Logo, $[x] = \{x, -x, \widehat{x}, -\widehat{x}\} = \{x, -x\}$. Note que $x \neq -x$ pelo que vimos anteriormente. Então a cardinalidade de $[x]$ é dois.

  Agora vamos procurar quais elementos $X \setminus \{0\}$ satisfazem $x = \widehat{x}$. Para tanto, observe que $x = \widehat{x}$ se, e somente se, $x \cdot x \equiv 1 \pmod{p}$, ou seja, $x^2 \equiv 1 \pmod{p}$. Logo, basta procurar quais elementos $X \setminus \{0\}$ satisfazem $x^2 \equiv 1 \pmod{p}$. Estes números nós chamaremos de solução desta congruência.
  Os números 1 e $p-1$ são soluções da congruência, pois:

$$1^2 \equiv 1 \pmod{p} \quad \text{e}$$

$$(p-1)^2 = p^2 - 2p + 1 = p(p-2) + 1 \equiv 1 \pmod{p}.$$

  Será que existe uma terceira solução?

  Suponha que existe outra solução, então ela é da forma $x = p - c$, em que $1 < c < p-1$, pois $x \in \{1, 2, \ldots, p-1\}$.
  Se $x = p - c$ é uma solução de $x^2 \equiv 1 \pmod{p}$ então:

$$(p-c)^2 = p^2 - 2pc + c^2 = p(p-2c) + c^2 \equiv 1 \pmod{p}.$$

  Logo,

$$c^2 \equiv 1 \pmod{p} \Rightarrow p|(c^2 - 1),$$

  ou seja,

$$p|(c+1)(c-1).$$

Isso implica que, $p|(c+1)$ ou $p|(c-1)$, já que p é primo. Veja que $p \nmid (c+1)$, pois $1 < c < p-1$, logo $2 < c+1 < p$. E também, $p \nmid (c-1)$, pois $1 < c < p-1$, logo $0 < c-1 < p-2 < p$. Sendo assim, $p \nmid (c+1)(c-1)$, portanto, não existe uma terceira solução.

Logo, as únicas possibilidades são $x = 1$ ou $x = p-1$. Agora, perceba que $p-1$ é o inverso aditivo de 1 em $\mathbb{Z}_p$. Portanto, 1 e $p-1$ pertencem a mesma classe na relação $\sim$. Desta forma, obtemos $[x] = \{1, p-1\}$.

- Se $x = -\widehat{x}$, então $-x = \widehat{x}$. Logo $[x] = \{x, -x, \widehat{x}, -\widehat{x}\} = \{x, -x\}$. Note novamente que $x \neq -x$ pelo que vimos anteriormente. Assim, a cardinalidade de $[x]$ é dois.

  Agora vamos procurar quais elementos $X \setminus \{0\}$ satisfazem $x = -\widehat{x}$. Para tanto, observe que $x = -\widehat{x}$ se, e somente se, $x \cdot -x \equiv 1 \pmod{p}$, ou seja, $x^2 \equiv -1 \pmod{p}$. Veremos que existem duas possibilidades para esta última congruência: não existe solução ou existem duas soluções. Vamos analisar as duas possibilidades.

  i) $x^2 \equiv -1 \pmod{p}$ não tem solução. Vamos mostrar que isso é possível, tomando por exemplo $p = 3$. Assim teremos $X = \{0, 1, 2\}$. Veja:

  $$0^2 \equiv 0 \pmod{3},$$

  $$1^2 \equiv 1 \pmod{3},$$

  $$2^2 \equiv 1 \pmod{3}.$$

  Note que $0 \not\equiv -1 \pmod{3}$ e $1 \not\equiv -1 \pmod{3}$. Ou seja, a congruência $x^2 \equiv -1 \pmod{p}$ não possui solução quando $p = 3$.

  ii) Se tiver solução, digamos x_0, então mostraremos que necessariamente terá outra solução que será $p - x_0$. Além disso, estas serão as únicas duas soluções.

  Seja x_0 solução de $x^2 \equiv -1 \pmod{p}$, então $x_0^2 \equiv -1 \pmod{p}$. Temos que

  $$(p - x_0)^2 = p^2 - 2px_0 + x_0^2 = p(p - 2x_0) + x_0^2.$$

  Assim,

  $$(p - x_0)^2 \equiv x_0^2 \pmod{p}.$$

Pela hipótese,

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

logo,

$$(p - x_0)^2 \equiv -1 \quad (mod\ p).$$

Portanto, se x_0 é solução de $x^2 \equiv -1 \quad (mod\ p)$, então $p - x_0$ também é solução.

Vamos mostrar agora que não existem outras soluções. Suponha que existe uma terceira solução, digamos x_1, em que $0 < x_1 < p$. Então

$$x_1^2 \equiv -1 \quad (mod\ p).$$

Como x_0 também é solução, temos que

$$x_0^2 \equiv -1 \quad (mod\ p).$$

Portanto,

$$x_0^2 \equiv x_1^2 \quad (mod\ p) \ \Rightarrow\ p | x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1).$$

Dessa forma,

$$p|(x_0 + x_1) \tag{2.1}$$

ou

$$p|(x_0 - x_1). \tag{2.2}$$

Temos que $0 < x_0 < p$ e $0 < x_1 < p$. Logo, $0 < x_0 + x_1 < 2p$, portanto, para que (2.1) seja verdadeira, devemos ter $x_0 + x_1 = p$ o que implica que $x_1 = p - x_0$. Então nesse caso não temos uma terceira solução.

Sendo $0 < x_0 < p \quad$ e $\quad 0 < x_1 < p \quad$ temos que

$$x_0 - x_1 < p. \tag{2.3}$$

Como $x_1 < p$, temos que $-x_1 > -p$, logo, somando x_0 nos dois membros da desigualdade obtemos:

$$x_0 - x_1 > x_0 - p \ \Rightarrow\ x_0 - x_1 > -p. \tag{2.4}$$

De (2.3) e (2.4) temos que $-p < x_0 - x_1 < p$. Portanto, para que (2.2) aconteça, devemos ter $x_0 - x_1 = 0$, ou seja, $x_1 = x_0$. Nesse caso também não temos uma terceira solução. Logo, quando a congruência $x^2 \equiv -1 \quad (mod\ p)$ possui solução ela será um elemento de $\{x_0, p - x_0\}$.

Concluímos então que se existe solução para $x = -\widehat{x}$, digamos

x_0, então $[x] = \{x_0, p - x_0\}$, pois x_0 e $p - x_0$ são inversos aditivos em $\mathbb{Z}_p$. Além disso, esta é a única classe onde $x = -\widehat{x}$.

Conclusão:

- $x = -x$ nunca ocorre.
- se $x = \widehat{x}$ então $[x] = \{1, p - 1\}$.
- se $x = -\widehat{x}$ então $[x] = \{x_0, p - x_0\}$.

Portanto, $[x] = \{x, -x, \widehat{x}, -\widehat{x}\}$ ou tem 4 elementos ou tem 2 elementos. Além disso, concluímos que temos no máximo duas classes com 2 elementos, sendo elas: $\{1, p - 1\}$ e $\{x_0, p - x_0\}$ e ainda, sempre temos a classe $\{1, p - 1\}$.

Agora vamos enunciar e demonstrar um lema que será importante para a demonstração do teorema principal do nosso trabalho.

Lema 2.3. *Sejam p um número primo, $m \in \mathbb{N}$ e $s \in \{1, 2, \ldots, p - 1\}$. A congruência $s^2 \equiv -1 \pmod{p}$ tem uma solução quando $p = 2$; tem duas soluções quando $p = 4m+1$ e não tem solução quando $p = 4m+3$.*

Demonstração. A congruência $s^2 \equiv -1 \pmod{p}$ possui uma solução quando $p = 2$, a saber, quando $s = 1$:

$$1^2 \equiv -1 \pmod{2}, \text{ pois } 2|(1 + 1).$$

Suponhamos agora que p é primo ímpar.

Já vimos que quando p é primo ímpar, p é da forma $4m + 1$ ou $4m + 3$.

Agora vamos mostrar que para $p = 4m + 1$ a congruência $s^2 \equiv -1 \pmod{p}$ terá duas soluções. Veja:

$$p = 4m + 1 \Rightarrow p - 1 = 4m.$$

Vimos anteriormente que $X = \{1, 2, \ldots, p - 1\}$ pode ser particionado em classes $[x]$ cuja cardinalidade é dois ou é quatro. Portanto, como $p - 1 = 4m$, existem duas possibilidades: ou existem apenas classes com quatro elementos, o que não ocorre, pois sempre temos a classe $\{1, p - 1\}$, ou existem classes com quatro elementos e no máximo duas classes com dois elementos, a saber, $\{1, p - 1\}$ e $\{x_0, p - x_0\}$.

Perceba que não podemos ter mais classes com dois elementos, pois como já vimos, existem no máximo duas classes com dois elementos, $\{1, p - 1\}$ e $\{x_0, p - x_0\}$.

Vamos verificar em qual ou quais classes estão os s que são solução de $s^2 \equiv -1 \pmod{p}$.

Já sabemos que o s que procuramos não está na classe $\{1, p-1\}$, pois:

$$1^2 \equiv -1 \pmod{p} \Rightarrow p|2,$$

o que não ocorre, pois p é primo ímpar. E,

$$(p-1)^2 \equiv -1 \pmod{p} \Rightarrow p|(p^2 - 2p + 2),$$

como $p|(p^2 - 2p)$ isso implica que $p|2$, o que não ocorre, por p ser um primo ímpar. Portanto, não há solução s na classe $\{1, p-1\}$.

Pelas contas que fizemos anteriormente, sabemos que $s = x_0$ ou $s = p - x_0$ é solução, portanto, na classe $\{x_0, p - x_0\}$ há duas soluções.

Agora vamos mostrar que nas classes com 4 elementos não temos nenhuma solução de $s^2 \equiv -1 \pmod{p}$.

Suponha que exista uma classe $[x] = \{x, -x, \widehat{x}, -\widehat{x}\}$ com elementos todos distintos, ou seja, a cardinalidade de $[x]$ é quatro, que contenha uma solução s. Então, já sabemos que $p - s$ também é solução. Agora vamos mostrar que $p - s \in [x]$.

Como $s + (p - s) \equiv 0 \pmod{p}$, temos que em $\mathbb{Z}_p$, $p - s$ é um representante da classe do inverso aditivo de $\overline{s}$, logo $p - s \in [x]$.

Por outro lado,

$$(p-s) \cdot s = ps - s^2 \equiv 1 \pmod{p} \Rightarrow p - s = \widehat{s}.$$

Se $p - s$ é o inverso aditivo e também o inverso multiplicativo de $\overline{x}$ em $\mathbb{Z}_p$, então, $[x]$ tem menos de 4 elementos, o que é uma contradição.

Logo, não existe solução s em classes com 4 elementos.

Portanto, quando $p = 4m+1$ há duas soluções para a congruência $s^2 \equiv -1 \pmod{p}$.

Por fim, vamos mostrar que para $p = 4m + 3$ a congruência $s^2 \equiv -1 \pmod{p}$ não terá solução. Veja:

$$p = 4m + 3 \Rightarrow p - 1 = 4m + 2.$$

Disto, vemos que $\{1, 2, \ldots, p-1\}$ foi particionado em classes com quatro elementos e uma classe com dois elementos, pois só existem duas classes com dois elementos. E mais, esta classe tem que ser a classe $\{1, p-1\}$ que ocorre sempre.

Portanto, pelas contas feitas no caso de $p = 4m + 1$ segue que não temos nenhum s no conjunto $\{1, 2, \ldots, p-1\}$ que satisfaz $s^2 \equiv -1 \pmod{p}$.

■

Apresentaremos agora um resultado conhecido como *Princípio da Casa dos Pombos*, que será útil na demonstração da próxima proposição.

Teorema 2.4. (Princípio da Casa dos Pombos) *Seja $n \in \mathbb{N}^*$. Se colocarmos $n+1$ pombos em n casas, pelo menos uma casa deverá conter pelo menos dois pombos.*

Demonstração. Seja $n+1$ o número de pombos e n a quantidade de casas disponíveis para colocar os pombos. Na pior das hipóteses, se distribuirmos exatamente um pombo para cada casa, sobrará um pombo para ser colocado em qualquer casa. Logo, uma das casa deverá conter pelo menos dois pombos.

■

Este princípio é também conhecido como *Princípio das Gavetas de Dirichlet*, e pode ser enunciado da seguinte forma: "Se $n+1$ objetos são colocados em n gavetas, então pelo menos uma gaveta deverá conter, pelo menos, dois objetos". Mais informações sobre este princípio podem ser encontradas na página 176 de [MORGADO, 2013].

Na sequência apresentaremos a definição que dá nome ao capítulo.

Definição 2.5. *Um número natural n é chamado de* representável *se ele for a soma de dois quadrados de números naturais, isto é, se existirem $x, y \in \mathbb{N}$ tais que*

$$n = x^2 + y^2.$$

Exemplo 2.6. O número 98 é representável, pois $7^2 + 7^2 = 98$. Já o número 14 não é representável, pois não existe $x \in \mathbb{N}$ que satisfaz uma das equações:

$$x^2 + 0^2 = 14,$$
$$x^2 + 1^2 = 14,$$
$$x^2 + 2^2 = 14,$$
$$x^2 + 3^2 = 14.$$

Veja:

$$x^2 + 0^2 = 14 \Rightarrow x = \sqrt{14},$$
$$x^2 + 1^2 = 14 \Rightarrow x = \sqrt{13},$$
$$x^2 + 2^2 = 14 \Rightarrow x = \sqrt{10},$$

$$x^2 + 3^2 = 14 \Rightarrow x = \sqrt{5}.$$

Note que as raízes das equações não são números naturais, portanto 14 não é representável. Perceba que fizemos os cálculos apenas com os números $0, 1, 2$ e 3, pois para todo natural $y > 3$ a equação $x^2 + y^2 = 14$ não possui solução em $\mathbb{N}$.

Nosso objetivo neste trabalho é verificar quais números naturais são representáveis. Para isso, inicialmente vamos apresentar um resultado no qual identificamos os números primos que são representáveis.

Lema 2.7. *Todo número primo p, tal que $p = 2$ ou $p = 4m + 1$, em que $m \in \mathbb{N}^*$, é representável, isto é, pode ser escrito como $p = x^2 + y^2$ para números naturais x e y.*

Demonstração. Note que $2 = 1^2 + 1^2$, logo 2 é representável.

Agora considere p um número primo da forma $p = 4m + 1$, e tome $q = \lfloor \sqrt{p} \rfloor$, ou seja, q é o maior inteiro menor que ou igual a $\sqrt{p}$. Como $\sqrt{p}$ não é inteiro, pois p é primo, temos que $q < \sqrt{p} < q + 1$.

Considere os pares (x', y') de inteiros, em que $0 \leq x' \leq q$ e $0 \leq y' \leq q$. Dessa forma, vemos que x' pode assumir $q + 1$ valores e y' também pode assumir $q + 1$ valores, portanto, o número total de pares (x', y') é $(q + 1)^2$.

Como $\sqrt{p} < q+1$, temos que $p < (q+1)^2$, isto é, o total de pares (x', y') é superior a p.

Seja s um número inteiro fixado. A partir dos pares (x', y') vamos construir números usando a seguinte expressão: dado um par (x', y') da lista, fazemos $x' - sy'$. Assim, obtemos uma lista de números inteiros. Nesta lista de números duas coisas podem acontecer com $(x', y'), (x'', y'') \in \{0, 1, \ldots, q\} \times \{0, 1, \ldots, q\}$:

1. sempre que $(x', y') \neq (x'', y'')$ temos $x' - sy' \neq x'' - sy''$;

2. existem pelo menos dois pares com $(x', y') \neq (x'', y'')$ tais que $x' - sy' = x'' - sy''$.

Se (1) ocorrer, então teremos uma lista com mais de p elementos e daí, como existem apenas p restos distintos na divisão euclidiana por p, pelo Princípio da Casa dos Pombos, dois destes números terão o mesmo resto na divisão euclidiana por p.

Se (2) ocorrer, então $x' - sy'$ e $x'' - sy''$ deixam o mesmo resto na divisão euclidiana por p, já que são iguais.

Deste modo, concluímos que existem $(x', y'), (x'', y'') \in \{0, 1, \ldots, q\} \times \{0, 1, \ldots, q\}$ distintos, tais que $x' - sy' \equiv x'' - sy'' \pmod{p}$, o

que equivale a:

$$x' - x'' \equiv s \cdot (y' - y'') \pmod{p}.$$

Elevando os dois membros da congruência ao quadrado, temos:

$$(x' - x'')^2 \equiv s^2 \cdot (y' - y'')^2 \pmod{p}.$$

Agora, seja s uma solução de $s^2 \equiv -1 \pmod{p}$, que sabemos que existe pelo *Lema 2.3*, pois $p = 4m + 1$. Então:

$$(x' - x'')^2 \equiv -(y' - y'')^2 \pmod{p}.$$

Logo,

$$(x' - x'')^2 + (y' - y'')^2 \equiv 0 \pmod{p}.$$

Assim, se definirmos $a = |x' - x''|$ e $b = |y' - y''|$ teremos:

$$a^2 + b^2 \equiv 0 \pmod{p}.$$

Ou seja,

$$p|(a^2 + b^2). \tag{2.5}$$

Como os pares (x', y') e (x'', y'') são distintos, a e b não são ambos zero, portanto $(a^2+b^2) > 0$. Sendo $a = |x'-x''|$, então $a \leq q$ e sendo $b = |y' - y''|$, então $b \leq q$, já que $x', x'', y', y'' \in \{0, 1, \ldots, q\} \times \{0, 1, \ldots, q\}$. Como $q < \sqrt{p}$, concluímos que $a < \sqrt{p}$ e $b < \sqrt{p}$, o que implica que $a^2 < p$ e $b^2 < p$, logo, $a^2 + b^2 < 2p$, portanto,

$$0 < a^2 + b^2 < 2p. \tag{2.6}$$

De (2.5) e (2.6) temos que $p|(a^2+b^2)$ e $0 < a^2+b^2 < 2p$. Mas p é o único número entre 0 e $2p$ que é divisível por p. Logo, $a^2 + b^2 = p$, ou seja, $p = 4m + 1$ pode ser escrito como soma de dois quadrados.

■

O lema que apresentaremos a seguir será importante para a demonstração do resultado principal deste trabalho.

Lema 2.8. *O produto de dois números representáveis é representável.*

Demonstração. Sejam $n_1, n_2 \in \mathbb{N}$ números representáveis quaisquer,

então existem $a, b, c, d \in \mathbb{N}$ tais que $n_1 = a^2 + b^2$ e $n_2 = c^2 + d^2$. Logo

$$\begin{aligned} n_1 \,.\, n_2 &= (a^2 + b^2)(c^2 + d^2) \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 + 2abcd - 2abcd \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

Logo, $n_1 \,.\, n_2$ é representável.

■

Vimos anteriormente que os números primos da forma $p = 4m+1$ e também o número primo 2 são representáveis, agora vamos identificar de que forma são os números naturais representáveis. Para isso, vamos enunciar e demonstrar o teorema principal do nosso trabalho.

Teorema 2.9. *Um número natural n é representável se, e somente se, n não possui nenhum fator primo da forma $p = 4m+3$, em que $m \in \mathbb{N}$, ou se possuir, então o expoente de todo fator da forma $p = 4m + 3$ é par.*

Demonstração. ($\Rightarrow$) Seja n um número representável. Se n não possui nenhum fator primo da forma $p = 4m + 3$ não temos nada a provar. Suponha que n possui fator primo da forma $p = 4m + 3$, então, vamos provar que o expoente de todo fator desta forma é par. Usaremos duas afirmações para fazer esta prova.

Afirmação 1: Se $p = 4m+3$ é um primo que divide um número representável $n = x^2 + y^2$, então $p|x$ e $p|y$, e assim $p^2|n$.

Prova. Suponha que $p|n$ e que $p \nmid x$. Se $p \nmid x$, temos que $x \not\equiv 0 \pmod{p}$, portanto, existe a classe do inverso multiplicativo de $\overline{x}$, ou seja, existe $\widehat{x} \in \mathbb{N}$ tal que $x \cdot \widehat{x} \equiv 1 \pmod{p}$.

Como $p|n$, isto é, $p|(x^2 + y^2)$, temos que $x^2 + y^2 \equiv 0 \pmod{p}$, multiplicando a congruência por $\widehat{x}^2$ obtemos:

$$\begin{aligned} & x^2 \cdot \widehat{x}^2 + y^2 \cdot \widehat{x}^2 && \equiv && 0 && (mod && p) \\ \Rightarrow\ & (x \cdot \widehat{x})^2 + (y \cdot \widehat{x})^2 && \equiv && 0 && (mod && p) \\ \Rightarrow\ & 1 + (y \cdot \widehat{x})^2 && \equiv && 0 && (mod && p) \\ \Rightarrow\ & (y \cdot \widehat{x})^2 && \equiv && -1 && (mod && p). \end{aligned}$$

Sabemos que $y \cdot \widehat{x}$ deixa um resto $s \in \{0, 1, 2, \ldots, p-1\}$ na divisão euclidiana por p. Então, podemos reescrever a última congruência, obtendo:

$$s^2 \equiv -1 \pmod{p}.$$

Perceba que s deve ser diferente de zero, então pelo *Lema 2.3*, esta congruência não possui solução para $p = 4m + 3$. Portanto a afirmação $p \nmid x$ não ocorre, logo, $p|x$.

Se $p|x$, então $p|x^2$. Como $p|(x^2+y^2)$ e $p|x^2$, isso implica que $p|y^2$ e portanto, pela *Proposição 1.23*, $p|y$. Logo, $p|x$ e $p|y$. Assim, existem $a, b \in \mathbb{N}$ tais que $x = pa$ e $y = pb$. Daí, $n = x^2 + y^2$ pode ser escrito como:

$$\begin{array}{rcl} & n & = & (pa)^2 + (pb)^2 \\ \Rightarrow & n & = & p^2a^2 + p^2b^2 \\ \Rightarrow & n & = & p^2(a^2 + b^2). \end{array}$$

Portanto, $p^2|n$ e $n = p^2k$, em que $k = a^2 + b^2 \in \mathbb{N}$.

Afirmação 2: Seja n um número representável. Se $n = p^2k$, em que p é um primo da forma $4m+3$ e $k \in \mathbb{N}$, então k é representável.

Prova. Sendo $n = p^2k$, então $k = \dfrac{n}{p^2}$.

Temos que $n = x^2 + y^2$, para algum $x, y \in \mathbb{N}$ e também $n = p^2k$, então:

$$x^2 + y^2 = p^2k \quad \Rightarrow k = \frac{x^2 + y^2}{p^2} \quad \Rightarrow k = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2.$$

Como $p|x$ e $p|y$ (provado na Afirmação 1), concluímos que k é representável, ou seja, existem $k_1, k_2 \in \mathbb{N}$ tais que $k = (k_1)^2 + (k_2)^2$.

Note que:

- Se $p \nmid k$ na Afirmação 1, então apenas $p^2|n$, e provamos que p aparece com expoente par na decomposição em primos de n.
- Se $p|k$ na Afirmação 1, então, pela Afirmação 2, temos que k é representável e pela Afirmação 1 temos que $p^2|k$. Daí, existe $k' \in \mathbb{N}$ tal que $k = p^2k'$ e k' é representável pois k é representável. Como $n = p^2k$, obtemos $n = p^4k'$. Agora se $p \nmid k'$ provamos que p aparece com expoente 4 (par) na decomposição em primos de n e se $p|k'$ usamos o argumento inicial para mostrar que então $p^2|k'$ e assim também p aparece com expoente par na decomposição em primos de n. Repetindo essa análise, pela finitude dos expoentes de p na decomposição em primos de n, concluímos que se $p|n$ então p aparece com expoente par na sua decomposição em primos.

($\Leftarrow$) Vamos separar esta demonstração em dois casos. O primeiro quando n não possui fatores da forma $p = 4m + 3$ e o segundo quando n possui fatores da forma $p = 4m + 3$ e estes aparecem com expoente par na sua decomposição em primos.

- Suponha que n não possui nenhum fator primo da forma $p = 4m + 3$. Logo, pelo *Teorema Fundamental da Aritmética 1.25*, existem $r \in \mathbb{N}$, primos ímpares $p_1, p_2 \ldots, p_r$ e números naturais $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_r$, tais que

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

é a decomposição de n em primos e, como n não possui nenhum fator primo da forma $p = 4m + 3$, temos que para todo $i \in \{1, \ldots, r\}$, $p_i = 4m + 1$ para algum $m \in \mathbb{N}$.

Pelo *Lema 2.7*, temos que o fator 2 é representável e os fatores p_i são representáveis. E, pelo *Lema 2.8*, temos que, produto de números representáveis é representável. Desta forma, concluímos que n é um número representável.

- Suponha que n possua na sua decomposição em primos fatores da forma $p = 4m + 3$, além disso, suponha que os expoentes de todos estes fatores sejam pares. Logo, novamente pelo *Teorema Fundamental da Aritmética 1.25*, existem $r, s \in \mathbb{N}$, primos $p_1, p_2 \ldots, p_r, q_1, q_2 \ldots, q_s$ e números naturais $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_r$, $\beta_1, \beta_2, \ldots, \beta_s$ tais que

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$

é a decomposição de n em primos, onde para todos $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s\}$, $p_i \equiv 1 \pmod 4$, $q_j \equiv 3 \pmod 4$ e β_j é par.

Pela hipótese, para todo $j \in \{1, \ldots, s\}$, β_j é par, então existe $\beta_j' \in \mathbb{N}$, tal que $\beta_j = 2\beta_j'$. Portanto,

$$q_j^{\beta_j} = q_j^{2\beta_j'} = (q_j^{\beta_j'})^2 + 0^2,$$

logo $q_j^{2\beta_j'}$ é um número representável, e assim temos que $q_j^{\beta_j}$ é um número representável.

Vimos no item anterior desta demonstração que $2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ é um número representável e como todo $q_j^{\beta_j}$ também é um número representável, segue, pelo *Lema 2.8* que n é um número representável.

■

Note que este teorema nos mostra como verificar se um número

é representável ou não, mas não nos diz como descobrir a sua representação como soma de dois quadrados.

No *Exemplo 2.6*, vimos que 98 é um número representável e 14 não. Vamos novamente verificar isto, agora, usando o teorema que acabamos de demonstrar.

Perceba que a decomposição em primos do número 98 é $2 \cdot 7^2$. Ainda, $7 = 4 \cdot 1 + 3$, ou seja, o fator primo 7 é da forma $p = 4m + 3$. E, além disso, é o único desta forma. Como ele aparece com expoente par na decomposição em primos de 98, pelo teorema principal deste trabalho, concluímos que 98 é um número representável.

Temos que $2 \cdot 7$ é a decomposição em primos do número 14 e, além disso, vimos acima que o fator 7 é da forma $p = 4m+3$. Este fator aparece com expoente 1, ou seja, com expoente ímpar na decomposição em primos do 14. Logo, pelo teorema que acabamos de provar 14 não é representável.

Na sequência veremos que a infinitude dos números primos da forma $4m+1$, em que $m \in \mathbb{N}$ pode ser provada usando o *Teorema 2.9*.

Corolário 2.10. *Existem infinitos números primos naturais da forma* $4m + 1$*, em que* $m \in \mathbb{N}$*.*

Demonstração. Suponhamos que exista uma quantidade finita de números primos naturais da forma $4m+1$, digamos $k+1$. Note que $k \in \mathbb{N}$, pois existe pelo menos um número primo natural desta forma, o 5, inclusive ele é o primeiro número primo desta forma. Sejam $5, p_1, p_2, \ldots, p_k$ todos os números primos naturais da forma $4m + 1$. Podemos supor, sem perda de generalidade que $5 < p_1 < p_2 < \ldots < p_k$, ou seja, para todos $i, j \in \{1, \ldots, k\}$, se $i < j$, então $p_i < p_j$ e, ainda, para todo $i \in \{1, \ldots, k\}$ temos que $5 < p_i$.

Considere o número natural M_k, tal que M_k é a soma do quadrado do produto de todos os números primos naturais ímpares menores que ou iguais a p_k com o quadrado do número 2. Ou seja,

$$M_k = (3 \cdot 5 \cdot 7 \cdot \cdots \cdot p_k)^2 + 2^2,$$

logo M_k é um número representável. Vamos mostrar que M_k é um número da forma $4m + 1$.

Seja $a = 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p_k$. Pela *Proposição 1.15*, temos que todos os fatores de a são da forma $4m+1$ ou $4m+3$ e, portanto, a é da forma $4m + 1$ ou $4m + 3$. De fato, veja que, para quaisquer $b, c \in \mathbb{N}$ tem-se que:

i) $(4b+1)(4c+1)$ é da forma $4m+1$, fato visto na *Proposição 1.26*;

ii) $(4b+1)(4c+3) = 16bc + 12b + 4c + 3 = 4(4bc + 3b + c) + 3$;

iii) $(4b+3)(4c+3) = 16bc + 12b + 12c + 9 = 4(4bc + 3b + 3c + 2) + 1$.

Logo, a é da forma $4m+1$ ou $4m+3$ e, pelos itens i) e iii) acima, temos que a^2 é da forma $4m+1$.

Temos que $M_k = (3 \cdot 5 \cdot 7 \cdot \cdots p_k)^2 + 2^2$, logo, $M_k = a^2 + 2^2$. Como a^2 é da forma $4m+1$, existe $x \in \mathbb{N}$ tal que $a^2 = 4x + 1$ e como $2^2 = 4 \cdot 1 + 0$ segue que

$$M_k = (4x + 1) + (4 \cdot 1 + 0) = 4(x + 1) + 1,$$

ou seja, M_k é da forma $4m + 1$.

Sabemos que M_k é um número representável. Desta forma, pela Afirmação 1 do *Teorema 2.9*, segue que, M_k não possui fatores primos da forma $4m+3$, pois se possuísse, então este fator dividiria 2, o que não ocorre, já que dois é primo e não é da forma $4m + 3$. Logo, concluímos que, os fatores primos de M_k são da forma $4m + 1$.

Supomos inicialmente que os únicos números primos da forma $4m + 1$ são $5, p_1, p_2, p_3, \ldots, p_k$. Note que nenhum desses números é fator primo de M_k, pois $5|(3 \cdot 5 \cdot 7 \cdot \cdots p_k)^2$, mas $5 \nmid 2^2$ e para todo $i \in \{1, \ldots, k\}$, $p_i|(3 \cdot 5 \cdot 7 \cdot \cdots p_k)^2$, mas $p_i \nmid 2^2$, então pela *Proposição 1.3* nenhum dos números primos $5, p_1, p_2, \ldots, p_k$ é fator de M_k. Assim, M_k tem um fator primo da forma $4m+1$ que é maior que p_k, o que é uma contradição, pois supomos que $5, p_1, p_2, \ldots, p_k$ são os únicos números primos da forma $4m + 1$ e ainda que p_k é o maior deles. Portanto, existem infinitos números primos naturais da forma $4m + 1$.

■

Uma consequência imediata deste resultado é que existem infinitos números naturais que podem ser escritos como soma de dois quadrados de números naturais.

CONCLUSÃO

Nosso objetivo neste trabalho era apresentar uma resposta para a pergunta "que números podem ser escritos como uma soma de dois quadrados de números naturais?", ou seja, determinar de que forma são os números que possuem representação como uma soma de dois quadrados de números naturais.

Para chegar a esta resposta primeiramente mostramos que existem infinitos números primos da forma $4m + 3$, em que $m \in \mathbb{N}$. Mostramos também que o número primo 2 e os números primos da forma $4m + 1$, em que $m \in \mathbb{N}$, podem ser escritos como soma de dois quadrados. Na sequência provamos que o produto de números que possuem representação como soma de dois quadrados também possui esta representação. E ainda, provamos que existem infinitos números primos da forma $4m+1$, e portanto, concluímos que existem infinitos números naturais que podem ser escritos como soma de dois quadrados de números naturais.

Assim, após obtermos alguns resultados importantes e fundamentais, relacionados aos conceitos de divisão eucliana nos inteiros, números primos, relações de equivalência e congruências, conseguimos alcançar o objetivo proposto, pois mostramos que um número natural que não possui fator primo da forma $4m+3$ em sua decomposição, com $m \in \mathbb{N}$, ou o possui com expoente par, pode ser escrito como soma de dois quadrados.

Contudo, é importante destacar que o teorema principal deste trabalho, o qual apresenta a resposta para a pergunda dada, nos mostra como verificar se um número é soma de dois quadrados ou não, mas não nos diz como descobrir a sua representação como soma de dois quadrados.

REFERÊNCIAS

[1] AIGNER, Martin; ZIEGLER, Günter M. **As provas estão n'O LIVRO**. São Paulo: Edgard Blücher, 2002.

[2] DOMINGUES, Hygino H. **Fundamentos de aritmética**. Florianópolis: Ed. da UFSC, 2009.

[3] HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2014.

[4] HEFEZ, Abramo. **Elementos de aritmética**. 2. ed. Rio de Janeiro: SBM, 2011.

[5] MORGADO, Augusto C.; CARVALHO, Paulo C. P. **Matemática Discreta**. Rio de Janeiro: SBM, 2013.

[6] RIBENBOIM, Paulo. **Números primos: Velhos mistérios e novos recordes**. Rio de Janeiro: IMPA, 2012.