Universidade Federal de São Paulo

Instituto de Ciência e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Aritmética no Ensino Fundamental II: Um Estudo sobre os Quadrados Perfeitos

Felipe Klinger Pereira Reis

Orientadora: Prof$^{\underline{a}}$. Dr$^{\underline{a}}$. Grasiele Cristiane Jorge

São José dos Campos

Fevereiro, 2021

PROFMAT

Título: *Aritmética no Ensino Fundamental II: Um Estudo sobre os Quadrados Perfeitos*
Dissertação apresentada ao Instituto de Ciência e Tecnologia da UNIFESP, campus São José dos Campos/SP, como parte dos requisitos exigidos para a obtenção do título de Mestre pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT.

São José dos Campos
Fevereiro, 2021

Reis, Felipe Klinger Pereira

Aritmética no Ensino Fundamental II: Um Estudo sobre os Quadrados Perfeitos, Felipe Klinger Pereira Reis – São José dos Campos, 2021.

viii, 40f.

Dissertação (Mestrado) – Universidade Federal de São Paulo. Instituto de Ciência e Tecnologia. Programa de Pós-Graduação em Matemática em Rede Nacional (PROFMAT).

Title

1. Aritmética. 2. Quadrados perfeitos. 3. Ensino básico. 4. BNCC. 5. Raciocínio lógico.

UNIVERSIDADE FEDERAL DE SÃO PAULO

INSTITUTO DE CIÊNCIA E TECNOLOGIA

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

Chefe de departamento:
Prof. Dr. Marcelo Cristino Gama

Coordenador do Programa de Pós-Graduação:
Prof. Dr. Angelo Calil Bianchi

FELIPE KLINGER PEREIRA REIS

ARITMÉTICA NO ENSINO FUNDAMENTAL II: UM ESTUDO SOBRE OS QUADRADOS PERFEITOS

Presidente da banca: Prof$^{\underline{a}}$. Dr$^{\underline{a}}$. Grasiele Cristiane Jorge

Banca examinadora:

Prof. Dr. Agnaldo José Ferrari

Prof$^{\underline{a}}$. Dr$^{\underline{a}}$. Maiara Francine Bollauf

Prof. Dr. Robson Ricardo de Araujo

Data da Defesa: 25 de fevereiro de 2021

"Com a Modelagem Matemática, o objeto de conhecimento passa a ter concretude, pois o modelo matemático concretiza o que era abstrato, o que pode tornar a aprendizagem mais significativa".

(Currículo Paulista, p. 314)

AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus por ter me concedido a vida e o dom pela arte de lecionar e me permitir chegar aonde cheguei.

Agradeço aos meus professores e colegas de graduação, sem os quais eu jamais teria acreditado que, mesmo tão jovem e com muitas dificuldades em Matemática, eu teria condições plenas de me tornar professor de Matemática. Aos meus alunos de todos esses anos que me impulsionaram, me fizeram evoluir e validaram meu trabalho como professor de matemática deixo o registro da minha gratidão.

Minha irmã gêmea Michele, que, muitas vezes, foi minha companheira de estudos no Ensino Básico e no Ensino Superior, e porque, graças a ela, tive oportunidade de ter meu primeiro emprego: professor titular de Matemática do Ensino Básico, pela atual SEDUC/SP, desde 2008.

Sou muito grato aos colegas do PROFMAT, fomos - e ainda somos - uma turma muito unida: um ajudando e incentivando ao outro; aos colegas de outros polos do PROFMAT pelo Brasil, nas conversas via grupo de whatsapp, que abriram caminhos e nos deram direcionamentos; aos professores desse curso que transmitiram seus conhecimentos e experiências na educação e aos criadores do programa que sonharam, permitiram sonhos e estão contribuindo fortemente para a educação brasileira. Agradeço também a Prof.ª Dra. Grasiele Cristiane Jorge, por me orientar neste trabalho.

Agradeço também aos meus amigos, familiares e a todos aqueles que de alguma forma contribuíram para minha evolução acadêmica, profissional e pessoal. Certamente eu não conseguiria listar aqui todas essas nobres pessoas a quem eu devo gratidão.

RESUMO

Neste projeto, propomos o estudo teórico de tópicos de Teoria dos Números, a fim de produzir uma dissertação que possa ser utilizada como referência didática por professores de Matemática do Ensino Básico. O tópico principal a ser estudado é o de números inteiros que são quadrados perfeitos, destacando suas propriedades e suas principais aplicações no Ensino Básico.

Palavras-chave: 1. Aritmética. 2. Quadrados perfeitos. 3. Ensino Básico. 4. BNCC. 5. Currículo Paulista. 6. Rede Pública de Ensino. 7. Álgebra. 8. Raciocínio lógico.

ABSTRACT

In this project, we propose the theoretical study about Number Theory, for producing a dissertation to be used as didatic reference by Mathematic's teachers of the Basic Education. The main topic to be studied is integer numbers called perfect squares, emphasizing its properties and main aplications in Basic Education.

Keywords: 1. Arithmetic. 2. Perfect squares. 3. Basic education. 4. BNCC. 5. Paulista Curriculum. 6. Public Education Network. 7. Algebra. 8. Logical reasoning.

SUMÁRIO

INTRODUÇÃO

A Teoria dos Números é a parte da Matemática que se dedica ao estudo dos números inteiros e, em particular, dos números primos. O conceito de números inteiros é um dos mais antigos e fundamentais da ciência em geral, tendo acompanhado o homem desde os primórdios de sua história. Ainda hoje, a Teoria dos Números é uma área de pesquisa das mais fascinantes, tanto do ponto de vista teórico quanto do ponto de vista prático. Em especial, com o advento do computador, a Teoria dos Números ganhou muito destaque. O principal sistema criptográfico computacional utilizado atualmente, o RSA, é baseado no Teorema de Euler, que é um resultado clássico de Teoria dos Números. A segurança do RSA está baseada na atual inexistência de um algoritmo que fatore um número inteiro positivo como produto de números primos em tempo polinomial. Decidir se um número inteiro positivo é um número primo já é uma das grandes questões a serem resolvidas. O presente trabalho tem como objetivo principal estudar os números inteiros que são quadrados perfeitos. Dizemos que um número inteiro positivo n é um quadrado perfeito, quando ao fatorarmos n como um produto de números primos $n = p_1^{\alpha_1}...p_1^{\alpha_r}$, tivermos em todas as potências de α_i's números pares. O que motivou tal proposta foi que no ensino da Matemática no Brasil, principalmente na Rede Pública de Ensino, há grande defasagem quanto aos principais requisitos para a compreensão de conceitos básicos relacionados à Aritmética, inclusive quanto aos números naturais e suas propriedades, especialmente os quadrados perfeitos. Estes, por sua vez, muitas vezes deixados de lado quando o assunto é investigar e perceber suas peculiaridades e propriedades, visto que muito há a ser abordado dentro desse tema.

No primeiro capítulo, abordaremos a história dos quadrados perfeitos: história dos quadrados perfeitos, passando principalmente pela matemática do período babilônico e grego antigo; estudo sobre como os babilônicos buscavam aproximações de raízes quadradas de números inteiros e como resolviam problemas que atualmente caracterizamos como equações de segundo grau; estudo dos números figurados pitagóricos, em especial os triangulares e os quadrangulares e apresentação de algumas proposições sobre quadrados perfeitos; apresentação de propriedades sobre quadrados perfeitos. No segundo capítulo, abordaremos alguns tópicos a serem estudados como pré-requisitos importantes para a compreensão da proposta deste projeto, tais como propriedades de divisibilidade nos números inteiros, algoritmo euclidiano da divisão, conceito de máximo divisor comum, identidade de Bézout, conceito de número primo, Teorema Fundamental da Aritmética, definição e introdução sobre números quadrados perfeitos. No terceiro capítulo, serão estudadas algumas propriedades relacionadas à congruência de números inteiros e propriedades de aritmética modular; outras propriedades sobre números quadrados perfeitos; quantidades e ordenação de divisores de números quadrados perfeitos; propriedades envolvendo o máximo divisor comum entre números quadrados perfeitos; aplicações do Algoritmo de Euclides. No quarto capítulo, abordaremos o Pequeno Teorema de Fermat, enunciando-o e demonstrando-o, apresentando duas consequências do referido teorema, uma delas relacionada a quadrados perfeitos; exemplos de como calcular o resto da divisão de uma potência grande por um número primo. No quinto capítulo, abordaremos a representação de um inteiro positivo por somas de quatro quadrados (incluindo o denominado “Teorema de Lagrange”, com demonstração), de três quadrados e de dois quadrados. No sexto capítulo, apresentaremos dicas e soluções para cada um dos desafios propostos ao longo dos outros capítulos. No sétimo capítulo, trataremos de informações importantes ao docente: a importância da prática pedagógica e como ele deve desenvolver seu trabalho baseado neste projeto, tendo em vista o cumprimento de todos os pré-requisitos por parte dos alunos, enunciando e comentando algumas habilidades e objetos de conhecimento, segundo o Currículo Paulista, relacionados aos estudos desenvolvidos nesta dissertação; e uma análise generalista sobre a prática docente quando tratar das habilidades de números, álgebra e geometria no Ensino Fundamental II. E no oitavo capítulo, apresentaremos as considerações finais, contendo uma lista com fatos centrais desenvolvidos no texto.

1

A HISTÓRIA DOS QUADRADOS PERFEITOS

Neste capítulo, daremos início ao estudo de alguns conceitos estabelecidos no decorrer da história da Matemática – mais precisamente ligados à Geometria – que, de certa forma, contribuíram, de forma grandiosa, para o estudo acerca dos números inteiros, e especialmente relacionados aos quadrados perfeitos. Abordaremos estudos realizados na antiga Mesopotâmia, inclusive utilizando o sistema de numeração dos babilônios, até a Grécia antiga, por intermédio dos estudos realizados por Platão e Pitágoras.

Quando resgatamos fatos importantes ao longo da história da humanidade, em particular o que se refere à Matemática, temos diante desse estudo inúmeros conceitos e definições, bem como procedimentos que precisam estar bem claros, principalmente sobre sua origem, utilização e praticidade. A seguir, serão destacados aqueles considerados de grande importância para a compreensão de tudo o que será abordado neste capítulo e todos foram extraídos do livro "Tópicos de História da Matemática" [8].

O primeiro conceito importante é a escrita para representar os números. Logo no início do capítulo, temos a seguinte representação 1,24;51;10. Essa forma de escrita tem origem na Babilônia e seu significado tem muito a ver com o que hoje conhecemos como sistema de numeração decimal. No entanto, trata-se de um outro sistema de numeração, o sexagesimal, isto é, aquele composto por 60 símbolos ou algarismos distintos (de 0 a 59). A vírgula separa a parte inteira da parte decimal e o ponto-e-vírgula separa as casas decimais, uma a uma. Observe a seguir:

$$1,24;51;10 = 1 \cdot 60^0 + 24 \cdot 60^{-1} + 51 \cdot 60^{-2} + 10 \cdot 60^{-3}$$

Note que essa representação acima é muito similar à que utilizamos no sistema de numeração decimal.

As definições que se fazem necessárias no decorrer desse mesmo capítulo são:

(1) Coleções de bolinhas: para os pitagóricos, tratam-se de representações de números por meio de pedrinhas.

(2) Esquadro: figura em forma de L invertido, que contêm a quantidade de bolinhas acrescentadas a um dado quadrado perfeito representando geometricamente, com relação à quantidade de bolinhas contidas no quadrado imediatamente anterior.

1.1 ORIGEM DO TERMO *QUADRADO* E ALGUNS PROBLEMAS

O termo *quadrado* se deve ao fato de podermos representar, geometricamente, um número inteiro quadrado perfeito, por meio de um quadrado de área igual a esse número. Na seção

1.2, traremos mais detalhes sobre a denominação *quadrados perfeitos*. Apresentaremos, a seguir, um pouco sobre a história da Matemática, no que compete ao nosso tema.

Os quadrados foram, inicialmente, estudados na antiga Mesopotâmia onde surgiram inúmeros problemas envolvendo a área de quadrados [8, p.16-24], alguns dos quais abordaremos a seguir.

(**Problema 1**) O cálculo de raízes quadradas.

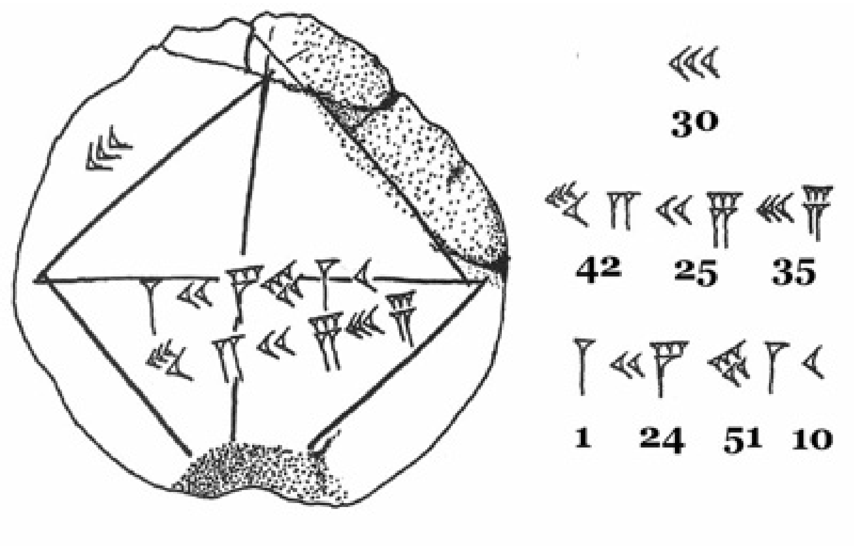

Figura 1: YBC 7289

No tablete YBC 7289, conforme a Figura 1, consta o exemplo mais famoso. Os babilônios, entre os anos 2.000 e 1.600 a.E.C., construíram, nesse tablete, um quadrado de lado l. Próximo a um dos lados do quadrado, vemos o número sexagesimal 30 ($30 \cdot 60^{-1} = 1/2$). Próximo a uma das diagonais, encontram-se os números sexagesimais 1,24;51;10 ($1 \cdot 60^0 + 24 \cdot 60^{-1} + 51 \cdot 60^{-2} + 10 \cdot 60^{-3} \simeq 1,414213$) e 42,25;35 ($42 \cdot 60^0 + 25 \cdot 60^{-1} + 35 \cdot 60^{-2} \simeq 42,426$).

A constante 1,24;51;10 encontra-se em uma tabela de coeficientes (as tabelas de coeficientes eram essenciais na Matemática da Babilônia e continham listas de constantes que ocorrem em vários tipos de problemas) e é chamada a diagonal do quadrado. Temos que 30 $\times$ 1,24;51;10 = 42;25;35. Uma das conclusões mais importantes é que a diagonal d do quadrado é igual a l $\times$ 1,24;51;10. Os escribas babilônios sabiam que $l/d \approx$ 1,24;51;10. De fato, $(1,24;51;10)^2 \approx 1,9999983$, sendo, portanto, 1,24;51;10 uma boa aproximação de $\sqrt{2}$.

Os babilônios chegaram a esta raiz quadrada usando um método bastante interessante, o qual permitia que fossem obtidos valores aproximados para raízes irracionais. Na linguagem atual, esse procedimento se baseava no cálculo da medida do lado de um quadrado de área k, representado na Figura 2.

Se o segmento AE é cortado em um ponto B, o quadrado de lado AE é igual ao quadrado de lado AB mais o quadrado de lado BE mais duas vezes o retângulo que contém

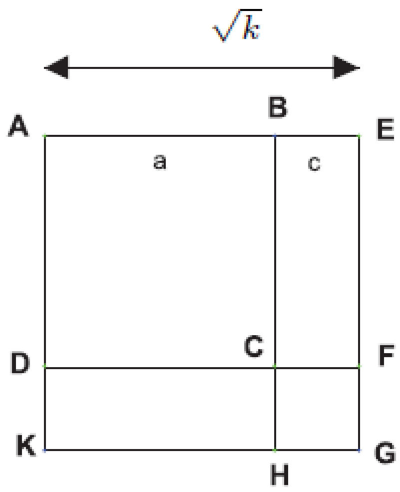

Figura 2: Medida do lado do quadrado de área k

os lados AB e BE. Se AB medir a e BE medir c, trata-se da versão geométrica da igualdade usualmente utilizada

$$(a+c)^2 = a^2 + c^2 + 2ac. \tag{1}$$

Se colocarmos, no interior do quadrado AEGK, o maior quadrado possível cuja medida do lado a é conhecida e usarmos o resultado geométrico acima, podemos aproximar a medida do lado do quadrado AEGK por a, dado que

$$\sqrt{k} = a + c. \tag{2}$$

Uma aproximação melhor do que a requer uma boa aproximação para c. Para isso, observemos a área da região poligonal BEGKDC, na Figura 2, cuja área é igual a $k - a^2$. Por outro lado, a figura poligonal DCBEGK pode ser decomposta em dois retângulos de lados a e c e em um quadrado de lado c, de sorte que

$$2ac + c^2 = k - a^2. \tag{3}$$

Note que, caso c seja bem pequeno, podemos desprezar c^2, e obtemos:

$$c \approx \frac{k - a^2}{2a}. \tag{4}$$

Consequentemente, teremos

$$a' = a + \frac{k - a^2}{2a} = \frac{1}{2}\left(a + \frac{k}{a}\right). \tag{5}$$

A partir de (23), temos que $a' \approx a + c$ é uma aproximação de $\sqrt{k}$ melhor que a, conforme podemos observar através da interpretação geométrica aqui apresentada.

Observação 1.1. *Através de duas iterações com a escolha* $a = \frac{3}{2}$*, presume-se que esse tenha sido o procedimento para encontrar uma aproximação para* $\sqrt{2}$*, como registrada no tablete YBC 7289.*

Os babilônios também utilizavam de tabletes contendo procedimentos, semelhantes ao que hoje chamamos de exercícios resolvidos, que resolvemos por meio de equações. Equivocadamente, muitos historiadores chegaram a acreditar que os babilônios sabiam resolver equações, através de uma certa "álgebra", que, posteriormente, teria sido expressa geometricamente pelos gregos.

A seguir, serão apresentados dois problemas do segundo grau na Babilônia.

(**Problema 2**) "Adicionei a área e o lado de um quadrado: obtive 0,45. Qual o lado?"

Solução apresentada pelos babilônios:
Passo 1 – Tome 1
Passo 2 – Fracione 1 tomando a metade $(= 0,30)$
$\Longrightarrow$ Na base decimal, metade de 1 é $\frac{1}{2}$.
Passo 3 – Multiplique 0,30 por si mesmo $(= 0,15)$
$\Longrightarrow$ Na base decimal, $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$.
Passo 4 – Some 0,15 a 0,45 $(= 1)$
$\Longrightarrow$ Na base decimal, $\frac{1}{4} + \frac{3}{4} = 1$.
Passo 5 – 1 é a raiz quadrada de 1
$\Longrightarrow$ Na base decimal, $\sqrt{1} = 1$.
Passo 6 – Subtraia os 0,30 de 1
$\Longrightarrow$Na base decimal, $1 - \frac{1}{2} = \frac{1}{2} = \frac{30}{60}$.
Passo 7 – 0,30 é o lado do quadrado

Traduzindo para a linguagem atual, queremos resolver o problema

$$x^2 + x = \frac{3}{4}.$$

Para resolver uma equação do tipo

$$x^2 + x = C$$

fazemos:

Passo 1 – Tome $B = 1$

Passo 2 – Divida B ao meio e obtenha $\dfrac{B}{2}$

Passo 3 – Eleve $\dfrac{B}{2}$ *ao quadrado e obtenha* $\left(\dfrac{B}{2}\right)^2 = \dfrac{B^2}{4}$

Passo 4 – Some C a $\dfrac{B^2}{4}$ *e obtenha* $\dfrac{B^2}{4} + C$

Passo 5 – Extraia a raiz quadrada de $\dfrac{B^2}{4} + C$ *e obtenha* $\sqrt{\dfrac{B^2}{4} + C}$

Passo 6 – Subtraia $\dfrac{B}{2}$ *de* $\sqrt{\dfrac{B^2}{4} + C}$ *e obtenha* $\sqrt{\dfrac{B^2}{4} + C} - \dfrac{B}{2}$

Passo 7 – Portanto, $\sqrt{\dfrac{B^2}{4} + C} - \dfrac{B}{2}$ *é o lado do quadrado*

(**Problema 3**) "Subtraí o terço da área e depois somei o terço do lado do quadrado à área restante: 0, 20. Qual o lado do quadrado?"

Solução apresentada pelos babilônios:

Passo 1 – Tome 1

Passo 2 – Subtraia o terço de 1, ou seja, 0,20, obtendo 0,40

Passo 3 – Multiplique 0,40 por 0,20 obtendo 0,13;20

Passo 4 – Encontre a metade de 0,20 $(\div 0, 10)$

Passo 5 – Multiplique 0,10 por 0,10 $(\div 0, 1; 40)$

Passo 6 – Adicione 0,1;40 a 0,13;20 $(\div 0, 15)$

Passo 7 – 0,30 é a raiz quadrada

Passo 8 – Subtraia 0,10 de 0,30 $(\div 0, 20)$

Passo 9 – Tome o recíproco de 0,40 $(\div 1, 30)$

Passo 10 – Multiplique 1,30 por 0,20 $(\div 0, 30)$

Passo 11 – 0,30 é o lado do quadrado

Obviamente, na época em que esses estudos foram realizados, não se escrevia uma equação geral do tipo $Ax^2 + Bx + C = 0$. No entanto, os babilônios — embora não possuíssem uma linguagem para expressar estes casos de modo genérico — eram dotados de uma natureza primordialmente algébrica, visto que o modo de enunciar o procedimento babilônio era para o caso geral de uma equação de tipo $Ax^2 + Bx = C$.

Assim, a solução de uma dada equação do tipo $Ax^2 + Bx = C$, conforme o procedimento descrito acima — para o Problema 3 — seria traduzido, algebricamente, para encontrar a raiz

$$L = \left(\sqrt{\frac{B^2}{4} + AC} - \frac{B}{2}\right) \times \frac{1}{A} \tag{6}$$

no procedimento a seguir.

Passo 1 – Multiplique A por C e obtenha AC

Passo 2 – Divida B ao meio e obtenha $\dfrac{B}{2}$

Passo 3 – Multiplique $\dfrac{B}{2}$ *por* $\dfrac{B}{2}$ *e obtenha* $\left(\dfrac{B}{2}\right)^2$

Passo 4 – Adicione AC a $\left(\dfrac{B}{2}\right)^2$ *e obtenha* $\left(\dfrac{B}{2}\right)^2 + AC$

Passo 5 – Extraia a raiz quadrada de $\left(\dfrac{B}{2}\right)^2 + AC$ *e obtenha* $\sqrt{\left(\dfrac{B}{2}\right)^2 + AC}$

Passo 6 – Subtraia $\dfrac{B}{2}$ *da raiz acima*

Passo 7 – Tome o recíproco de A e obtenha $\dfrac{1}{A}$

Passo 8 – Multiplique $\dfrac{1}{A}$ *pela raiz*

Passo 9 – O lado do quadrado é $\left(\sqrt{\dfrac{B^2}{4} + AC} - \dfrac{B}{2}\right) \times \dfrac{1}{A}$.

1.2 PRIMEIROS ESTUDOS SOBRE OS QUADRADOS PERFEITOS

Segundo acabamos de ver na seção anterior, foram grandiosas as contribuições matemáticas atribuídas aos babilônios, em especial o que se deve à origem do nosso objeto de estudo: os quadrados perfeitos. Já nesta seção, traremos uma abordagem um pouco mais específica ao nosso objeto de estudo. Estudaremos agora a Matemática grega antes de Euclides, a qual nos fornecerá a noção de número dos pitagóricos e a geometria pré-euclidiana.

Atribui-se a Pitágoras grande parte das contribuições dos gregos à Matemática e, por isso, ele é frequentemente citado como o pai da Matemática grega. Embora sua teoria tenha sido concreta — baseada em manipulações de números figurados — e sua aritmética era indutiva e sem qualquer tipo de provas, muitas generalizações sobre sequências de números podiam ser obtidas a partir de representações gráficas.

Historicamente, as regras utilizadas para obtenção dessas sequências — como as dos números quadrados, cubos e outros — eram construídas para uso prático. Estudos mostram que os gregos acreditavam que as propriedades dos números estavam associadas a forças cósmicas. De fato, a concepção de Pitágoras sobre a natureza parte da ideia de haver uma explicação global para que se possa simbolizar a totalidade do cosmos, e ela se dá através dos números. Com isso, os pitagóricos passaram a considerar que as coisas são números, elas consistem de números. Notavelmente, isso se deve ao fato de as coisas poderem ser organizadas e distinguidas. Como consequência disso, os gregos nos levam a concluir que as propriedades aritméticas das coisas constituem o seu ser propriamente dito, e o ser de todas as coisas é o número.

Os pitagóricos utilizavam de pedrinhas dispostas em uma certa configuração para representar seus números figurados. O primeiro exemplo de número figurado se dá pelos números triangulares. A Figura 3 é uma tradução, em linguagem atual, dos quatro primeiros desses números pitagóricos (coleções de bolinhas).

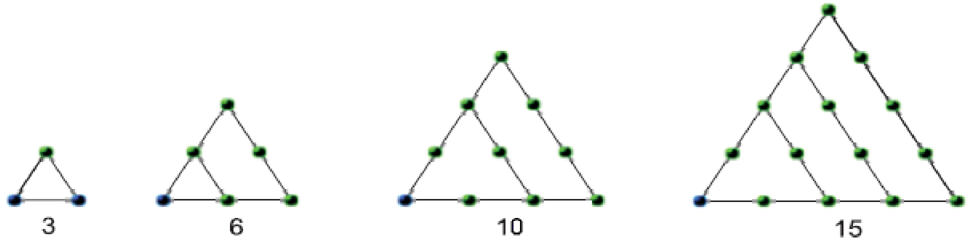

Figura 3: Os números triangulares

Os números triangulares (alguns representados na Figura 3) podem ser associados aos nossos números 1, 3, 6, 10, 15 e assim por diante. Em linguagem matemática atual, temos a seguinte definição:

Definição 1.2. *[8, p.54] O número triangular de ordem n é dado pela soma da progressão aritmética*

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

Na Figura 3, temos os números triangulares de ordem 2, 3, 4 e 5, respectivamente.

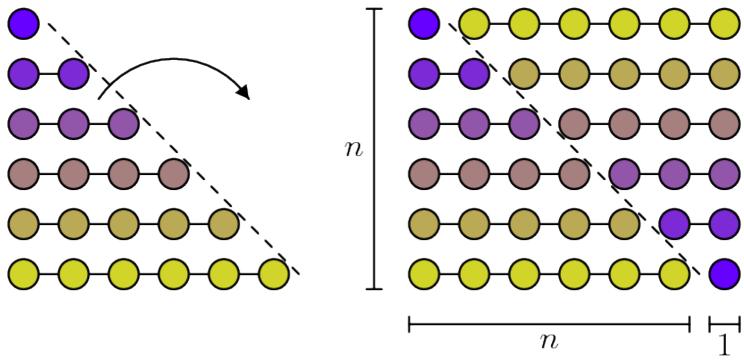

Figura 4: Soma de 1 até n

Os números quadrados (alguns representados na Figura 5) podem ser associados aos nossos números 1, 4, 9, 16, 25, 36 e assim por diante. Em linguagem matemática atual, temos a seguinte definição:

Definição 1.3. *[8, p.56] O número quadrado de ordem n é dado por n^2.*

O termo *quadrado perfeito* se deve ao fato de se construir um quadrado cuja medida do lado é representada por um número inteiro que é raiz quadrada de outro número inteiro, a área desse quadrado.

Proposição 1.4. *[8, p.56] Todo quadrado perfeito de ordem n, para $n>1$, é a soma de dois números triangulares, de ordem n e $n-1$.*

Demonstração. Considere o número natural n, tal que n^2 seja seu respectivo quadrado. Manipulando algebricamente, temos que:

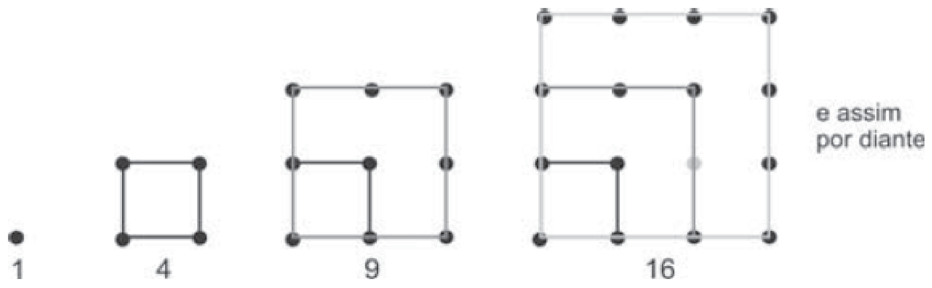

Figura 5: Os números quadrados

$$n^2 = \frac{n^2 + n^2}{2} = \frac{n^2 + n - n + n^2}{2},$$

o que nos permite reescrever n^2 da seguinte forma:

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

Logo, um quadrado perfeito de ordem $n > 1$ é a soma de um número triangular de ordem n com um número triangular de ordem $n - 1$. □

Proposição 1.5. *A diferença entre dois quadrados perfeitos consecutivos de ordem* $n+1$ *e* n *é o número ímpar* $2n + 1$.

Demonstração. Temos que

$$(n+1)^2 = n^2 + (2n+1) \Longleftrightarrow (n+1)^2 - n^2 = 2n + 1. \tag{7}$$

□

As *triplas pitagóricas* ou *ternas pitagóricas*, como chamamos hoje, estão associadas a problemas cujo objetivo é determinar dois números quadrados perfeitos cuja soma seja também um número quadrado perfeito. Esses três números inteiros podem ser associados às medidas dos lados de um triângulo retângulo. Os pitagóricos chegaram a estas triplas por meio do gnómon que era sinônimo dos números ímpares, formados pelas diferenças entre números quadrados sucessivos. A Figura 6 nos permite calcular a sequência dos quadrados perfeitos por meio de um deslocamento do esquadro, o que, em outras palavras, significa que devemos somar a sequência dos números ímpares.

Observando a Figura 6 e a igualdade (25), podemos concluir que *a diferença entre dois quadrados perfeitos consecutivos* será um quadrado perfeito, se, e somente se, o maior dos esquadros contiver um quadrado perfeito ímpar.

Embora tenhamos, geometricamente, uma boa explicação para a abordagem dos quadrados perfeitos como *números figurados*, vamos demonstrar que a soma dos n primeiros ímpares é o quadrado perfeito n^2.

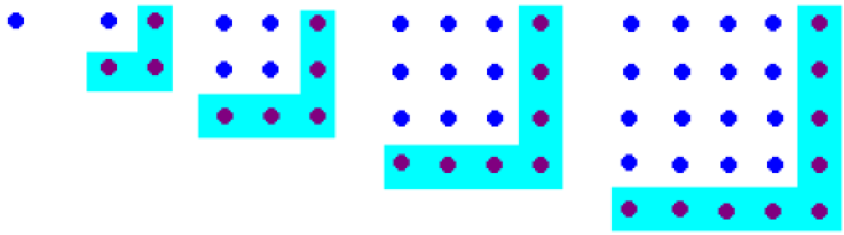

Figura 6: Esquadro de ímpares ao redor de $(n-1)^2$

Antes, vejamos alguns exemplos:

$1^2 = 1$
$2^2 = 1+3$
$3^2 = 1+3+5$
$4^2 = 1+3+5+7$
$5^2 = 1+3+5+7+9$
$6^2 = 1+3+5+7+9+11$
$7^2 = 1+3+5+7+9+11+13$
$8^2 = 1+3+5+7+9+11+13+15$
$9^2 = 1+3+5+7+9+11+13+15+17$
$10^2 = 1+3+5+7+9+11+13+15+17+19$
$11^2 = 1+3+5+7+9+11+13+15+17+19+21$
$12^2 = 1+3+5+7+9+11+13+15+17+19+21+23$
$13^2 = 1+3+5+7+9+11+13+15+17+19+21+23+25.$

Proposição 1.6. *A soma dos n primeiros números ímpares é o quadrado perfeito n^2.*

Demonstração. Temos que todo número ímpar pode ser escrito como $2n+1$ com $n \in \mathbb{N}$. Agora a soma dos n primeiros números ímpares é

$$\begin{aligned} 1+3+\cdots+(2(n-1)+1) &= \sum_{i=0}^{n-1}(2i+1) \\ &= 2\left(\sum_{i=0}^{n-1} i\right) + (\underbrace{1+\cdots+1}_{n \text{ vezes}}) \\ &= 2\frac{(n-1)n}{2} + n \\ &= n^2 - n + n = n^2, \end{aligned}$$

como queríamos. Note que $\sum_{i=0}^{n-1} i$ é a soma dos termos de uma progressão aritmética com razão 1. $\square$

Para instigar ainda mais o estudo sobre os números figurados de Pitágoras, sugerimos a você leitor que tente resolver os desafios a seguir.

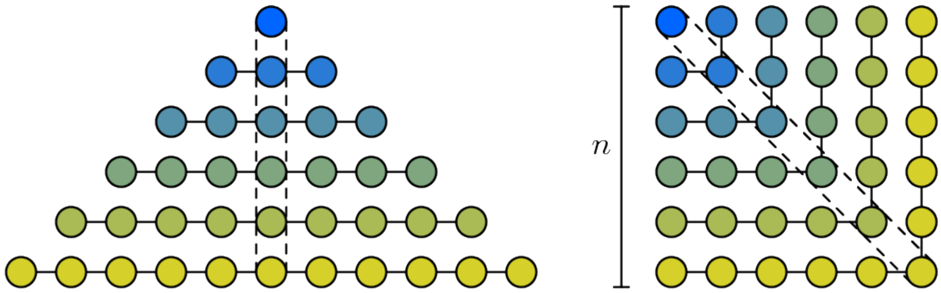

Figura 7: Soma dos n primeiros números ímpares

Desafio 1.7. *Mostre que, se* $k^2 < 100$ *é um número triangular, então* $k = 1$ *ou* $k = 6$.

Desafio 1.8. *Mostre, sem utilizar aritmética ou álgebra, simplesmente reorganizando diagramas de números figurados, que oito vezes um número triangular mais um é igual a um número quadrado. Se o número triangular tem ordem* n*, qual a ordem do número quadrado obtido pelo processo acima? [8, p.64]*

2

PRÉ-REQUISITOS IMPORTANTES

Neste capítulo, introduziremos conceitos e definições importantes que tornarão o leitor mais familiarizado com o tema proposto. É de extrema importância que toda a abordagem dada aos quadrados perfeitos nos capítulos subsequentes torne a leitura mais agradável, de forma a facilitar a compreensão e, consequentemente, despertar o interesse nesse estudo. Os conceitos e as definições apresentados encontram-se no livro "Aritmética" [3].

2.1 DIVISÃO NOS INTEIROS

Definição 2.1. *[3, p.2] Dados dois números inteiros a e b, dizemos que a divide b e escrevemos $a|b$ quando existir um número inteiro c tal que $b = c \cdot a$.*

Os inteiros gozam das seguintes propriedades:

Proposição 2.2. *[3, p.3] Dado $a \in \mathbb{Z}$, temos que $1|a$, $a|a$ e $a|0$.*

Demonstração. Temos que:

$$0 = 0 \cdot a,$$

$$a = 1 \cdot a \quad \text{e}$$

$$a = a \cdot 1.$$

□

Proposição 2.3. *Dado $a \in \mathbb{Z}$, se $a \mid 1$, então $|a| = 1$.*

Demonstração. Se $a \mid 1$, então existe k $\in \mathbb{Z}$ tal que $1 = k \cdot a$. Assim, temos que $k = 1$ e $a = 1$ ou $k = -1$ e $a = -1$. Portanto, $|a| = 1$. □

Proposição 2.4. *[3, p.3] Dados $a, b, c \in \mathbb{Z}$, se $a \mid b$ e $c \mid d$, então $a \cdot c \mid b \cdot d$.*

Demonstração. Como $a \mid b$ e $c \mid d$, temos que existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$a \mid b \Rightarrow b = k_1 \cdot a \tag{8}$$

e

$$c \mid d \Rightarrow d = k_2 \cdot c. \tag{9}$$

Multiplicando (1) e (2), obtemos:

$$b \cdot d = (k_1 \cdot a) \cdot (k_2 \cdot c) = (k_1 \cdot k_2) \cdot (a \cdot c).$$

Portanto, $a \cdot c \mid b \cdot d$. □

Proposição 2.5. *[3, p.3] Dados $a, b, c \in \mathbb{Z}$, se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Como $a \mid b$ e $b \mid c$, temos que existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$a \mid b \Rightarrow b = k_1 \cdot a \tag{10}$$

e

$$b \mid c \Rightarrow c = k_2 \cdot b. \tag{11}$$

Substituindo (3) em (4), obtemos:

$$c = (k_1 \cdot k_2) \cdot a.$$

Portanto, $a \mid c$. □

Proposição 2.6. *Dados $a, b \in \mathbb{Z}$, se $a \mid b$ e $b \mid a$, então $|a| = |b|$.*

Demonstração. Como $a \mid b$ e $b \mid a$, temos que existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$a \mid b \Rightarrow b = k_1 \cdot a \tag{12}$$

e

$$b \mid a \Rightarrow a = k_2 \cdot b. \tag{13}$$

Substituindo (5) em (6), obtemos:

$$a = (k_1 \cdot k_2) \cdot a \Rightarrow k_1 \cdot k_2 = 1.$$

Logo, temos que:

$$k_2 \mid 1 \Rightarrow |k_2| = 1.$$

Como $a \mid b$ e $b \mid a$, temos $|a| = |b|$. □

Proposição 2.7. *[3, p.4] Dados $a, b \in \mathbb{Z}$, se $a \mid b$ e $b \neq 0$, então $|a| \leq |b|$.*

Demonstração. Como $a \mid b$, temos que existe $k_1 \in \mathbb{Z}$ tal que

$$a \mid b \Rightarrow b = k_1 \cdot a.$$

Dessa forma,

$$|b| = |k_1| \cdot |a|.$$

Como, por hipótese, $k_1 \neq 0$, então $|k_1| \geq 1$. Portanto, $|a| \leq |b|$. □

Proposição 2.8. *[3, p.4] Dados $a, b \in \mathbb{Z}$, se $a \mid b$ e $a \mid c$, então $a \mid (b \cdot x + c \cdot y)$, $\forall x, y \in \mathbb{Z}$.*

Demonstração. Como $a \mid b$ e $a \mid c$, temos que existem $k_1, k_2 \in \mathbb{Z}$ tais que

$$a \mid b \Rightarrow b = k_1 \cdot a \tag{14}$$

e

$$a \mid c \Rightarrow c = k_2 \cdot a. \tag{15}$$

Quaisquer que sejam os inteiros x e y, temos, de (7) e (8), que:

$$b \cdot x + c \cdot y = (k_1 \cdot a) \cdot x + (k_2 \cdot a) \cdot y = (k_1 \cdot x + k_2 \cdot y) \cdot a.$$

Portanto, $a \mid (b \cdot x + c \cdot y)$, $\forall x, y \in \mathbb{Z}$. □

Teorema 2.9. *[3, p.10]* **Algoritmo euclidiano da divisão**
Dados a e b inteiros e $b > 0$, existem um único q e um único r inteiros, tais que $a = b \cdot q + r$ e $0 \leq r < b$, onde a é o dividendo, b é o divisor, q é o quociente e r é o resto.

Demonstração. (1) A existência de q e r.

Seja S o conjunto de todos os inteiros não-negativos da forma $a - b \cdot x$, com x inteiro. Como $b > 0$, S possui ao menos um elemento. De fato, basta tomar $x = -|a|$ e notar que $b \geq 1$. Assim,

$$a - b \cdot x = a + b \cdot |a| \geq a + |a| \geq 0.$$

Usando o Princípio da Boa Ordenação, existe o elemento mínimo $r \in S$, tal que:

$$r \geq 0 \text{ e } r = a - b \cdot q \text{ para algum } q \in \mathbb{Z}, \text{ ou seja, } a = b \cdot q + r.$$

Note que $r < b$, pois, caso contrário, r não seria o elemento mínimo de S, pois:

$$0 \leq r - b = (a - b \cdot q) - b = a - b \cdot (q + 1) < r.$$

Essa parte da demonstração nos leva a concluir que, se $r > b$, então não usamos q suficiente para a divisão de a por b.

(2) A unicidade de q e r.

Suponhamos que existam outros inteiros q_1 e r_1, tais que:

$$a = b \cdot q_1 + r_1, \text{ com } 0 \leq r_1 < b.$$

Nesse caso, temos que:

$$a = b \cdot q_1 + r_1 = b \cdot q + r \Rightarrow r_1 - r = b \cdot (q - q_1).$$

Note que:

$$-b < -r \leq 0 \quad \text{e} \quad 0 \leq r_1 < b.$$

Assim:

$$-b < r - r_1 < b \Leftrightarrow |r - r_1| < b.$$

Como $b \mid (r - r_1)$ e $|r - r_1| < b$, então $r - r_1 = 0$. Como $b > 0$, então $q - q_1 = 0$. Logo, $r_1 = r$ e $q_1 = q$. Portanto, q e r existem e são únicos. □

Definição 2.10. *[3, p.33] Dados dois números inteiros a e b não simultaneamente nulos, o maior divisor comum de a e b será chamado de máximo divisor comum de a e b e denotado por $mdc(a, b)$.*

Teorema 2.11. *[3, p.41] (Identidade de Bézout). Dados dois inteiros a e b não simultaneamente nulos, existem dois inteiros s e t tais que*

$$mdc(a, b) = a \cdot s + b \cdot t.$$

Demonstração. Seja $D = \{n \cdot a + m \cdot b;\ m, n \in \mathbb{Z}\}$. Temos que D contém números positivos, números negativos e também o zero. Sejam s e t inteiros tais que $d = s \cdot a + t \cdot b$ seja o menor inteiro positivo de D. Vamos provar que d é o máximo divisor comum de a e b. Mostremos que $d \mid a$ e $d \mid b$. Suponhamos que d não divide a. Neste caso, pelo algoritmo euclidiano da divisão, existem q e r inteiros tais que $a = q \cdot d + r$ com $0 < r < d$. Daí,

$$r = a - q \cdot d = a - q \cdot (s \cdot a + t \cdot b) = a \cdot (1 - q \cdot s) + (-q \cdot t) \cdot b.$$

Disso segue que $r \in D$, pois $1 - q \cdot s$ e $-q \cdot t$ são inteiros. Como $0 < r < d$ e d é o menor elemento positivo do conjunto D, temos uma contradição. Portanto, $d \mid a$. De forma similar mostramos que $d \mid b$. Portanto, d é um divisor comum de a e b. Seja d' um divisor comum de a e b. Temos que existem números inteiros x e y tais que $a = x \cdot d'$ e $b = y \cdot d'$. Daí,

$$d = s \cdot a + t \cdot b = s \cdot (x \cdot d') + t \cdot (y \cdot d') = (s \cdot x + t \cdot y) \cdot d'.$$

Logo, $d' \mid d$. Portanto, $d = mdc(a, b)$. □

Definição 2.12. *Dois inteiros a e b são ditos coprimos se $mdc(a, b) = 1$.*

Proposição 2.13. *[3, p.43] Dois números inteiros a e b são coprimos se, e somente se, existem inteiros s e t tais que*

$$a \cdot s + b \cdot t = 1.$$

Demonstração. Suponhamos que $mdc(a, b) = 1$. Pela Identidade de Bézout, existem inteiros s e t tais que $a \cdot s + b \cdot t = mdc(a, b) = 1$. Reciprocamente, suponha que existam inteiros s e t tais que $a \cdot s + b \cdot t = 1$ e seja $d = mdc(a, b)$. Como $d \mid a$ e $d \mid b$, então $d \mid (a \cdot s + b \cdot t) = 1$. Logo, $d = 1$, pois $d = mdc(a, b) \geq 1$. □

2.2 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Definição 2.14. *[3, p.79] Um número inteiro n, com $|n| \neq 1$, possuindo somente como divisores positivos 1 e $|n|$, é chamado primo. Se n não é primo, dizemos que é composto.*

Proposição 2.15. *[3, p.79] Sejam p, a, b inteiros. Se p é primo e $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se p não divide a, então $mdc(a, p) = 1$. De fato, se $d = mdc(a, p)$, então $d \mid a$ e $d \mid p$. Como p é primo e $d \mid p$, então $d = 1$ ou $d = p$. Como p não divide a, então $d = 1$. Pela Identidade de Bézout, existem s e t inteiros tais que $1 = a \cdot s + p \cdot t$. Disto segue que $b = b \cdot (a \cdot s) + b \cdot (p \cdot t)$. Temos que $p \mid p$ e $p \mid a \cdot b$ por hipótese. Logo, $p \mid ((a \cdot b) \cdot s + p \cdot (b \cdot t)) = b$.

□

Corolário 2.16. *[3, p.80] Sejam $p, a_1, \ldots, a_n$ inteiros. Se p é primo e $p \mid a_1 \cdots a_n$, então $p \mid a_i$ para algum i.*

Teorema 2.17. *[3, p.80] (Teorema Fundamental da Aritmética) Todo inteiro n maior do que 1 pode ser representado de maneira única, a menos da ordem, como um produto de fatores primos positivos.*

Demonstração. Se n é primo não há nada a ser demonstrado. Suponhamos n composto. Seja p_1 o menor dos divisores positivos de n diferente de 1. Afirmamos que p_1 é primo. Isto é verdade, pois caso contrário existiria p com $1 < p < p_1$ e $p \mid p_1$. Então, $p \mid n$, contradizendo a escolha de p_1. Logo, $n = p_1 \cdot n_1$ com p_1 primo. Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1 diferente de 1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 \cdot p_2 \cdot n_2$ com p_1, p_2 primos. Repetindo esse procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, \ldots$. Como todos estes inteiros são maiores do que 1, este processo deve terminar e então $n = p_1 \cdot p_2 \cdots p_k$ para algum $k \geq 2$. Como os primos $p_1, p_2, \ldots, p_k$ não são, necessariamente, distintos, n terá a forma

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}.$$

Para mostrarmos a unicidade usamos indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 \cdot p_2 \cdots p_s = q_1 \cdot q_2 \cdots q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 é primo e divide o produto $q_1 \cdot q_2 \cdots q_r$, pelo Corolário 2.16 ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \mid q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 \cdot p_2 \cdots p_s$ e $q_1 \cdot q_2 \cdots q_r$ são iguais. □

2.3 QUADRADOS PERFEITOS - ABORDAGEM POR MEIO DA OBSERVAÇÃO

No caso de termos que identificar características específicas de um dado conjunto numérico, é necessário, primeiro, que estejamos familiarizados com o que ele representa. Observe a seguinte sequência numérica[1]:

$$4, 9, 16, 25, 49, 64, 81, 100, 121, 400$$

O que esses números têm em comum?

Para responder isso, vamos escrevê-los de outra maneira. Observe:

$$\begin{aligned} 4 &= 2^2; \\ 9 &= 3^2; \\ 16 &= 4^2; \\ 25 &= 5^2; \\ 49 &= 7^2; \\ 64 &= 8^2; \\ 81 &= 9^2; \\ 100 &= 10^2; \\ 121 &= 11^2; \\ 400 &= 20^2. \end{aligned}$$

Dessa forma, é possível percebermos que esses números são, na verdade, quadrados de outros números. Em outras palavras, são denominados quadrados perfeitos.

Definição 2.18. *Seja $n \in \mathbb{N}$. Dizemos que n é um quadrado perfeito se, e somente se, existe $a \in \mathbb{N}$ tal que $n = a^2$.*

Uma característica interessante desse tipo de número natural é que todos eles possuem raízes quadradas exatas, o que só é possível quando todos os primos que o compõem possuem expoente par.

Assim, para que possamos identificar, por exemplo, que $\sqrt{5787}$ e $\sqrt{14722}$ não são números naturais, devemos realizar as decomposições de 5787 e 14722 em fatores primos.

[1] Disponível em: http://clubes.obmep.org.br/blog/quadrado-perfeito/

Nestes casos, temos que há pelo menos um primo em cada decomposição que não possui expoente par. De fato,

$$5787 = 3^2 \cdot 643^1$$

e

$$14722 = 2^1 \cdot 17^1 \cdot 433^1.$$

Além disso, no decorrer dos capítulos, estudaremos algumas propriedades relacionadas aos quadrados perfeitos. Inclusive, apresentando proposições, teoremas e suas respectivas demonstrações. Ao final de cada seção, traremos um desafio para o leitor. E no último capítulo, apresentaremos uma possível solução para cada um desses desafios propostos.

3 ALGUMAS PROPRIEDADES DOS QUADRADOS PERFEITOS

Neste capítulo, traremos estudos que complementam, de certa forma, o que estudamos no capítulo anterior. Nosso objetivo é investigar as propriedades dos quadrados perfeitos, quanto à sua divisibilidade. Todas as informações aqui contidas encontram-se no livro "Aritmética" [3]. A princípio, separamos algumas assertivas para serem demonstradas com rigor matemático, utilizando, como referência, algumas propriedades do Máximo Divisor Comum e do Mínimo Múltiplo Comum e alguns critérios de divisibilidade. A prioridade neste estudo também é investigar os quadrados perfeitos com ênfase no conjunto dos números naturais (incluindo o zero). No entanto, é totalmente possível expandirmos para os inteiros tudo o que é apresentado e demonstrado.

3.1 ALGUMAS DEFINIÇÕES EM ARITMÉTICA MODULAR

Definição 3.1. *[3, p.126] Seja $m > 1$ um número inteiro. Dizemos que dois números inteiros a e b são congruentes módulo m se a e b possuírem mesmo resto quando divididos por m e simbolizaremos por*

$$a \equiv b \ mod \ m.$$

Quando a e b não forem congruentes módulo m, escreveremos

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

A menos que se diga o contrário, no que se segue m será um número inteiro maior do que 1.

Proposição 3.2. *[3, p.127] Sejam a e b dois números inteiros. Temos que $a \equiv b \ mod \ m$ se, e somente se, m divide $b - a$.*

Demonstração. De fato, pelo algoritmo euclidiano da divisão, podemos escrever

$$a = mq_1 + r_1 \text{ e } b = mq_2 + r_2,$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor $r_1 \leq r_2$ (se o contrário ocorrer, basta considerar $a - b$ ao invés de $b - a$ na equação a seguir). Assim, podemos escrever

$$b - a = m(q_2 - q_1) + r_2 - r_1.$$

Logo, temos que m divide $b-a$ se, e somente se, m divide $r_2 - r_1$. Por ser $0 \leq r_2 - r_1 < m$, segue que m divide $b-a$ se, e somente se, $r_2 - r_1 = 0$, ou seja, se, e somente se, $r_2 = r_1$. □

Proposição 3.3. *Se a e b são inteiros, temos que $a \equiv b \mod m$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração. Se $a \equiv b \mod m$, então $m \mid (a-b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial pois na existência de k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m \mid (a-b)$ isto é, $a \equiv b \mod m$. □

Proposição 3.4. *[3, p.127] Sejam a_1, a_2, b_1 e b_2 inteiros quaisquer. Se $a_1 \equiv b_1 \mod m$ e $a_2 \equiv b_2 \mod m$, então $a_1 + a_2 \equiv b_1 + b_2 \mod m$ e $a_1 - a_2 \equiv b_1 - b_2 \mod m$.*

Demonstração. De fato, como $a_1 \equiv b_1 \mod m$ e $a_2 \equiv b_2 \mod m$, então m divide $b_1 - a_1$ e divide $b_2 - a_2$. Logo,

$$m \text{ divide } (b_1 - a_1) + (b_2 - a_2) = (b_1 + b_2) - (a_1 + a_2),$$

mostrando que $b_1 + b_2 \equiv a_1 + a_2 \mod m$. O caso $a_1 - a_2 \equiv b_1 - b_2 \mod m$ é similar. □

Proposição 3.5. *[3, p.129] Sejam $a, b, c, m \in \mathbb{Z}$. Temos que:*

$$a + c \equiv b + c \mod m \text{ se, e somente se, } a \equiv b \mod m.$$

Demonstração. Se $a \equiv b \mod m$, segue imediatamente da Proposição 3.4 que $a + c \equiv b + c \mod m$, pois $c \equiv c \mod m$. Reciprocamente, se $a + c \equiv b + c \mod m$, então m divide $(b + c) - (a + c)$, o que implica que m divide $b - a$ e, consequentemente, $a \equiv b \mod m$. □

Proposição 3.6. *[3, p.130] Sejam a_1, a_2, b_1 e b_2 inteiros quaisquer. Se $a_1 \equiv b_1 \mod m$ e $a_2 \equiv b_2 \mod m$, então $a_1 a_2 \equiv b_1 b_2 \mod m$.*

Demonstração. De fato, como $a_1 \equiv b_1 \mod m$ e $a_2 \equiv b_2 \mod m$, então m divide $a_1 - b_1$ e $a_2 - b_2$. Por outro lado, como

$$a_1 a_2 - b_1 b_2 = a_1 a_2 - b_1 b_2 + a_1 b_2 - a_1 b_2 = a_1(a_2 - b_2) + b_2(a_1 - b_1),$$

segue que m divide $a_1 a_2 - b_1 b_2$, o que prova o resultado. □

Corolário 3.7. *[3, p.128] Se $a \equiv b \mod m$, então $a^n \equiv b^n \mod m$, para todo n natural.*

Essas definições são importantes para tornar claras e objetivas as investigações necessárias para compreensão deste capítulo e do capítulo 4, inclusive para tratar sobre o Pequeno Teorema de Fermat.

Propriedade 3.8. *Nenhum quadrado perfeito termina em 2, 3, 7 ou 8.*

Demonstração. Consideremos inicialmente que a terminação de um número natural significa exatamente sua congruência módulo 10, isto é, o resto da sua divisão por 10. Queremos, portanto, provar que nenhum quadrado perfeito é congruente a 2, 3, 7 ou 8, módulo 10. Para isso, consideremos que todo número natural pode ser escrito na forma:

$$\begin{gathered}10k, 10k+1, 10k+2, 10k+3, 10k+4,\\ 10k+5, 10k+6, 10k+7, 10k+8 \text{ ou } 10k+9,\\ \text{com } k \in \mathbb{N} \cup \{0\}.\end{gathered}$$

Efetuando o quadrado de cada uma dessas formas, obtemos:

$$\begin{gathered}(10k)^2 \equiv 0 \ (mod\ 10), \text{ ou seja, termina em 0.}\\ (10k+1)^2 = 100k^2 + 20k + 1 \equiv 1 \ (mod\ 10), \text{ ou seja, termina em 1.}\\ (10k+2)^2 = 100k^2 + 40k + 4 \equiv 4 \ (mod\ 10), \text{ ou seja, termina em 4.}\\ (10k+3)^2 = 100k^2 + 60k + 9 \equiv 9 \ (mod\ 10), \text{ ou seja, termina em 9.}\\ (10k+4)^2 = 100k^2 + 80k + 16 \equiv 16 \equiv 6 \ (mod\ 10), \text{ ou seja, termina em 6.}\\ (10k+5)^2 = 100k^2 + 100k + 25 \equiv 25 \equiv 5 \ (mod\ 10), \text{ ou seja, termina em 5.}\\ (10k+6)^2 = 100k^2 + 120k + 36 \equiv 36 \equiv 6 \ (mod\ 10), \text{ ou seja, termina em 6.}\\ (10k+7)^2 = 100k^2 + 140k + 49 \equiv 49 \equiv 9 \ (mod\ 10), \text{ ou seja, termina em 9.}\\ (10k+8)^2 = 100k^2 + 160k + 64 \equiv 64 \equiv 4 \ (mod\ 10), \text{ ou seja, termina em 4.}\\ (10k+9)^2 = 100k^2 + 180k + 81 \equiv 81 \equiv 1 \ (mod\ 10), \text{ ou seja, termina em 1.}\end{gathered}$$

Portanto, nenhum quadrado perfeito termina em 2, 3, 7 ou 8. □

Propriedade 3.9. *Todo quadrado perfeito ímpar deixa resto 1 na divisão por 8.*

Demonstração. Qualquer número natural, quando dividido por 8, pode deixar os seguintes restos: 0, 1, 2, 3, 4, 5, 6 ou 7. Escrevendo-o de acordo com a divisão euclidiana, temos naturais da forma:

$$\begin{gathered}8k, 8k+1, 8k+2, 8k+3,\\ 8k+4, 8k+5, 8k+6 \text{ ou } 8k+7,\\ \text{com } k \in \mathbb{N} \cup \{0\}.\end{gathered}$$

Como queremos apenas os ímpares, utilizaremos somente os inteiros da forma:

$$8k+1, 8k+3, 8k+5 \text{ ou } 8k+7.$$

Efetuando o quadrado de cada uma dessas formas, obtemos:

$$\begin{gathered}(8k+1)^2 = 64k^2 + 16k + 1 \equiv 1 \ (mod\ 8)\\(8k+3)^2 = 64k^2 + 48k + 9 \equiv 9 \equiv 1 \ (mod\ 8)\\(8k+5)^2 = 64k^2 + 80k + 25 \equiv 25 \equiv 1 \ (mod\ 8)\\(8k+7)^2 \equiv 49 \equiv 1 \ (mod\ 8).\end{gathered}$$

Portanto, todo quadrado perfeito ímpar deixa resto 1 na divisão por 8. □

Propriedade 3.10. *Se m e 3 são coprimos, então m^2 deixa resto 1 na divisão por 3.*

Demonstração. Se m e 3 são coprimos, então m é da forma $3k+1$ ou $3k+2$, com $k \in \mathbb{N} \cup \{0\}$. Efetuando o quadrado de cada uma dessas formas, obtemos:

$$\begin{gathered}(3k+1)^2 = 9k^2 + 6k + 1 \equiv 1 \ (mod\ 3)\\(3k+2)^2 = 9k^2 + 12k + 4 \equiv 4 \equiv 1 \ (mod\ 3)\end{gathered}$$

Portanto, se m e 3 são coprimos, então m^2 deixa resto 1 na divisão por 3. □

No que segue, vamos utilizar a notação $\boxed{\text{x}}\ \boxed{\text{y}}$ para representar o número $x \cdot 10 + y$, com $0 \leq y \leq 9$.

Propriedade 3.11. *Dado um número natural $N = 10 \cdot a + b$, com $0 \leq b \leq 9$, temos que:*

1. *Se $b^2 \leq 9$, então*
$$N^2 = [a \cdot (10 \cdot a + 2 \cdot b)] \cdot 10 + b^2.$$

2. *Se $b^2 > 9$ e $b^2 = 10 \cdot c + d$, então*
$$N^2 = [a \cdot (10 \cdot a + 2 \cdot b) + c] \cdot 10 + d.$$

Demonstração. Temos que

$$\begin{aligned}(10 \cdot a + b)^2 &= 100 \cdot a^2 + 2 \cdot 10 \cdot a \cdot b + b^2\\&= 10 \cdot a \cdot (10 \cdot a + 2 \cdot b) + b^2.\end{aligned} \tag{16}$$

Note que, a partir de (16), podemos concluir que $(10 \cdot a + b)^2 \equiv b^2 \ (mod\ 10)$ e de forma geral, temos que qualquer quadrado perfeito é congruente ao quadrado de suas unidades módulo 10. Vamos considerar dois casos:

- Caso $b^2 \leq 9$ (o que ocorre se, e somente se, $b \leq 3$). Neste caso, temos:

$$(10 \cdot a + b)^2 = \boxed{a \cdot (10 \cdot a + 2 \cdot b)}\ \boxed{b^2}. \tag{17}$$

  onde o primeiro quadro representa as dezenas e o segundo, as unidades.

- Caso $b^2 > 9$ (o que acontece se, e somente se, $b > 3$). Neste caso temos que $b^2 = 10 \cdot c + d$, pois qualquer número natural maior que 9, possui, no mínimo, uma dezena e isso deve ser considerado no primeiro quadro, dado que ele representa exatamente as dezenas de $N^2 = (10 \cdot a + b)^2$. Reescrevendo N^2, teremos:

$$\begin{aligned}(10 \cdot a + b)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot b) + 10 \cdot c + d \\ &= 10 \cdot [a \cdot (10 \cdot a + 2 \cdot b) + c] + d \\ &= \boxed{a \cdot (10 \cdot a + 2 \cdot b) + c.}\ \boxed{d}\end{aligned} \tag{18}$$

$\square$

Conforme mencionado na Propriedade 3.11, os dígitos de um quadrado perfeito N^2 têm relação com os algarismos que formam N.

Vamos analisar a seguir todas as possibilidades para o algarismo das unidades:

- Note que um número terminado em 0 é da forma $10k$. Logo, seu quadrado é da forma

$$(10k)^2 = 100 \cdot k^2. \tag{19}$$

- Para a forma $10k + 1$ temos

$$\begin{aligned}(10 \cdot a + 1)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 1) + 1^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 2) + 1^2.\end{aligned}$$

Portanto, quando o número original terminar em 1, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 2)}\ \boxed{1}. \tag{20}$$

- Para a forma $10k + 2$, teremos:

$$\begin{aligned}(10 \cdot a + 2)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 2) + 2^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 4) + 4.\end{aligned}$$

Portanto, quando o número original terminar em 2, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 4)}\ \boxed{4}. \tag{21}$$

- Para a forma $10k + 3$, teremos:

$$\begin{aligned}(10 \cdot a + 3)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 3) + 3^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 6) + 9.\end{aligned}$$

Portanto, quando o número original terminar em 3, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 6)}\ \boxed{9}. \tag{22}$$

- Para a forma $10k + 4$, teremos:

$$\begin{aligned}(10 \cdot a + 4)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 4) + 4^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 8) + 16 \\ &= 10 \cdot a \cdot (10 \cdot a + 8) + 10 + 6 \\ &= 10 \cdot [a \cdot (10 \cdot a + 8) + 1] + 6.\end{aligned}$$

Portanto, quando o número original terminar em 4, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 8) + 1}\ \boxed{6}. \tag{23}$$

- Para a forma $10k + 5$, teremos:

$$\begin{aligned}(10 \cdot a + 5)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 5) + 5^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 10) + 25 \\ &= 100 \cdot [a \cdot (a + 1)] + 10 \cdot 2 + 5.\end{aligned}$$

Portanto, quando o número original terminar em 5, seu quadrado será:

$$\boxed{a \cdot (a + 1) + 2}\ \boxed{5}. \tag{24}$$

- Para a forma $10k + 6$, teremos:

$$\begin{aligned}(10 \cdot a + 6)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 6) + 6^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 12) + 36 \\ &= 10 \cdot a \cdot (10 \cdot a + 12) + 30 + 6 \\ &= 10 \cdot [a \cdot (10 \cdot a + 12) + 3] + 6.\end{aligned}$$

Portanto, quando o número original terminar em 6, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 12) + 3}\ \boxed{6}. \tag{25}$$

- Para a forma $10k + 7$, teremos:

$$\begin{aligned}(10 \cdot a + 7)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 7) + 7^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 14) + 49 \\ &= 10 \cdot a \cdot (10 \cdot a + 14) + 40 + 9 \\ &= 10 \cdot [a \cdot (10 \cdot a + 14) + 4] + 9.\end{aligned}$$

Portanto, quando o número original terminar em 7, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 14) + 4}\,\boxed{9}. \tag{26}$$

- Para a forma $10k + 8$, teremos:

$$\begin{aligned}(10 \cdot a + 8)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 8) + 8^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 16) + 64 \\ &= 10 \cdot a \cdot (10 \cdot a + 16) + 60 + 4 \\ &= 10 \cdot [a \cdot (10 \cdot a + 16) + 6] + 4.\end{aligned}$$

Portanto, quando o número original terminar em 8, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 16) + 6}\,\boxed{4}. \tag{27}$$

- Para a forma $10k + 9$, teremos:

$$\begin{aligned}(10 \cdot a + 9)^2 &= 10 \cdot a \cdot (10 \cdot a + 2 \cdot 9) + 9^2 \\ &= 10 \cdot a \cdot (10 \cdot a + 18) + 81 \\ &= 10 \cdot a \cdot (10 \cdot a + 18) + 80 + 1 \\ &= 10 \cdot [a \cdot (10 \cdot a + 18) + 8] + 1.\end{aligned}$$

Portanto, quando o número original terminar em 9, seu quadrado será:

$$\boxed{a \cdot (10 \cdot a + 18) + 8}\,\boxed{1}. \tag{28}$$

A partir das duas últimas propriedades apresentadas e demonstradas, propomos a você leitor um pequeno desafio.

Desafio 3.12. *Usando as propriedades observadas, calcule o quadrado de:*

(a) 61

(b) 92

(c) 113

(d) 54

(e) 85

(f) 106

(g) 87

(h) 98

(i) 119

(j) 750

No item (j), você pode desprezar as unidades do número original e utilizar a Propriedade 3.11 somente para as dezenas do número informado, bastando acrescentar ao final os dois zeros correspondentes às unidades e dezenas do quadrado.

3.2 ALGUMAS CURIOSIDADES SOBRE OS QUADRADOS PERFEITOS

Os dois próximos resultados, atribuídos a Platão, elencam uma família de quadrados perfeitos que pode ser escrita como soma de outros dois quadrados perfeitos.

Proposição 3.13. *[2, p.8] Dados $x = n > 1$ ímpar, $y = \dfrac{n^2-1}{2}$ e $z = \dfrac{n^2+1}{2}$, temos que*

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

Demonstração. Temos que

$$\begin{aligned} y^2 - z^2 &= \frac{n^4 - 2n^2 + 1}{4} - \frac{n^4 + 2n^2 + 1}{4} \\ &= \frac{n^4 - 2n^2 + 1 - n^4 - 2n^2 - 1}{4} \\ &= \frac{-4n^2}{4} \\ &= -n^2 = -x^2. \end{aligned}$$

Portanto, $x^2 + y^2 = z^2$. □

Proposição 3.14. *[2, p.8] Dados $x = n > 1$ par, $y = \dfrac{n^2}{4} - 1$ e $z = \dfrac{n^2}{4} + 1$, temos que*

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

Demonstração. Temos que

$$\begin{aligned} y^2 - z^2 &= \frac{n^4}{16} - \frac{n^2}{2} + 1 - \left(\frac{n^4}{16} + \frac{n^2}{2} + 1\right) \\ &= \frac{n^4}{16} - \frac{n^2}{2} + 1 - \frac{n^4}{16} - \frac{n^2}{2} - 1 \\ &= \frac{-2n^2}{2} \\ &= -n^2 = -x^2. \end{aligned}$$

Portanto, $x^2 + y^2 = z^2$. □

Através dessa proposição, é possível gerar os chamados *ternos pitagóricos primitivos.*

O próximo resultado, atribuído aos pitagóricos, elenca todos os quadrados perfeitos que podem ser escritos como soma de outros dois quadrados perfeitos.

Proposição 3.15. *[2, p.7] Dados $x = 2luv$, $y = l(u^2 - v^2)$ e $z = l(u^2 + v^2)$, temos que $x^2 + y^2 = z^2$.*

Demonstração. Para essa demonstração, basta efetuarmos $x^2 + y^2$ e compararmos o resultado obtido, em função de u e v, com $z = l(u^2 + v^2)$. Temos que

$$x = 2luv \Longrightarrow x^2 = l^2(4uv)^2 \text{ e}$$
$$y = l(u^2 - v^2) \Longrightarrow y^2 = l^2[u^4 - 2(uv)^2 + v^4].$$

Assim:

$$\begin{aligned} x^2 + y^2 &= l^2[(4uv)^2 + (u^4 - 2(uv)^2 + v^4)] \\ &= l^2[u^4 + 2(uv)^2 + v^4] \\ &= l^2(u^2 + v^2)^2 = z^2. \end{aligned}$$

Portanto, $x^2 + y^2 = z^2$, dadas as condições iniciais. □

Após os resultados anteriores, propomos a você leitor um pequeno desafio:

Desafio 3.16. *Escreva sete exemplos de quadrados perfeitos que podem ser escritos como soma de dois outros quadrados perfeitos.*

Proposição 3.17. *Se entre os infinitos termos de uma progressão aritmética de inteiros positivos existe um quadrado perfeito, então infinitos termos dessa progressão são também quadrados perfeitos*[2]*.*

Demonstração. Seja

$$S = (a_1, a_1 + r, a_1 + 2r, a_1 + 3r, \dots)$$

uma PA infinita de inteiros positivos com razão $r \in \mathbb{N}$, $r > 0$.

Dado a um número natural, suponha que a^2 seja um termo dessa PA, ou seja

$$S = (a_1, a_1 + r, a_1 + 2r, a_1 + 3r, \dots, \mathbf{a^2}, \dots)$$

Considere o número $m = (a + r)^2$ e observe que:

(i) m é um número inteiro; (ii) m é um quadrado perfeito; (iii) $m = (a + r)^2 = a^2 + 2ar + r^2 = a^2 + (2a + r)r$.

Note que $(2a + r)$ é um número natural.

Ao observarmos (i), (ii) e (iii), podemos concluir que m é um quadrado perfeito e é um termo da sequência considerada.

Note que $m > a^2$. Assim, temos

[2] Disponível em: https://www.tutorbrasil.com.br/forum/viewtopic.php?t=27313

$$S = (a_1, a_1 + r, a_1 + 2r, a_1 + 3r, \ldots, \mathbf{a^2}, \ldots, (\mathbf{a} + \mathbf{r})^{\mathbf{2}}, \ldots)$$

Podemos, inclusive, determinar mais alguns quadrados perfeitos dessa sequência S. Observe:

$$\begin{aligned} a^2 &\longrightarrow (a+r)^2 \\ (a+r)^2 &\longrightarrow ((a+r)+r)^2 = (a+2r)^2 \\ (a+2r)^2 &\longrightarrow ((a+2r)+r)^2 = (a+3r)^2 \\ (a+3r)^2 &\longrightarrow ((a+3r)+r)^2 = (a+4r)^2 \\ (a+4r)^2 &\longrightarrow ((a+4r)+r)^2 = (a+5r)^2 \\ &\vdots \end{aligned}$$

Logo, temos

$$\begin{gathered} S = (a_1, a_1 + r, a_1 + 2r, a_1 + 3r, \ldots, a^2, \ldots, (a+r)^2, \ldots, (a+2r)^2, \ldots, \\ (a+3r)^2, \ldots, (a+4r)^2, \ldots, (a+5r)^2, \ldots) \end{gathered}$$

Portanto, se uma dada PA infinita possui um quadrado perfeito, ela possuirá infinitos quadrados perfeitos. □

Proposição 3.18. *[6, p.18] A soma dos $n+1$ primeiros quadrados perfeitos é dada pela fórmula*

$$\sum_{n=0}^{N} n^2 = \frac{N \cdot (N+1) \cdot (2N+1)}{6} = 0^2 + 1^2 + 2^2 + \cdots + N^2.$$

Demonstração. Essa demonstração se dará por meio do Princípio de Indução Finita.

Caso-base: para $n = 0$, temos:

$$\frac{0 \cdot (0+1) \cdot (2 \cdot 0 + 1)}{6} = 0.$$

Suponhamos que essa propriedade seja válida para N, isto é:

$$\sum_{n=0}^{N} n^2 = \frac{N \cdot (N+1) \cdot (2N+1)}{6}$$

e essa será nossa Hipótese de Indução.

Queremos demonstrar que essa propriedade é válida para $N+1$.

Primeiro, observemos que:

$$\begin{aligned}
\sum_{n=0}^{N+1} n^2 &= \sum_{n=0}^{N} n^2 + (N+1)^2 \\
&= \frac{N \cdot (N+1) \cdot (2N+1)}{6} + (N+1)^2 \\
&= \frac{N \cdot (N+1) \cdot (2N+1) + 6 \cdot (N+1)^2}{6} \\
&= \frac{(N+1) \cdot [N \cdot (2N+1) + 6 \cdot (N+1)]}{6} \\
&= \frac{(N+1) \cdot (2N^2 + N + 6N + 6)}{6} \\
&= \frac{(N+1) \cdot [(N+1)+1] \cdot [2 \cdot (N+1) + 1]}{6}
\end{aligned}$$

Logo, a propriedade é válida para $N+1$.

Portanto, a soma dos n primeiros quadrados perfeitos é dada pela fórmula de recorrência

$$\sum_{n=0}^{N} n^2 = \frac{N \cdot (N+1) \cdot (2N+1)}{6}.$$

□

Proposição 3.19. *O número 3 é o único número primo antecessor de um quadrado perfeito.*

Demonstração. Se m é um quadrado perfeito, então $m = n^2$ para algum natural n. Daí,

$$m - 1 = n^2 - 1 = (n-1)(n+1).$$

Temos que $m-1$ é primo se, e somente se, $n-1 = 1$ ou $n+1 = 1$. Agora, $n-1 = 1$ se, e somente se, $n = 2$ e $n+1 = 1$ se, e somente se, $n = 0$. Logo, de $n = 2$ temos $m = 4$ e $m - 1 = 3$. De $n = 0$ temos $m = 0$ e neste caso, seu antecessor não é um número natural. □

No que segue, vamos definir o que é número feliz.

(1) Inicia-se com qualquer número inteiro positivo.

(2) Esse número é substituído pela soma dos quadrados dos seus dígitos.

(3) Repete-se o processo (2) até que o número seja igual a 1 ou ocorra num ciclo infinito sem incluir um.

Os números no fim do processo de extremidade com 1, são conhecidos como números feliz [3]e aqueles que não terminam com um 1 são números chamados infelizes.

[3] Disponível em: https://pt.wikipedia.org/wiki/Número_feliz

Definição 3.20. *Dado um número* $n = n_0$*, define-se uma sequência* $n_1, n_2, \ldots,$ *em que* n_{i+1} *é a soma dos quadrados dos dígitos* n_i*. Então* n *é um número feliz se e somente se existe* i *tal que* $n_i = 1$*.*

Exemplo 3.21. *7 é um número feliz, pois:*

$$\begin{gathered} 7^2 = 49 \\ 4^2 + 9^2 = 97 \\ 9^2 + 7^2 = 130 \\ 1^2 + 3^2 + 0^2 = 10 \\ 1^2 + 0^2 = 1. \end{gathered}$$

Exemplo 3.22. *10 é um número feliz, pois:*

$$\begin{gathered} 10^2 = 100 \\ 1^2 + 0^2 + 0^2 = 1. \end{gathered}$$

Exemplo 3.23. *3 não é um número feliz, pois:*

$$\begin{gathered} 3^2 = 9 \\ 9^2 = 81 \\ 8^2 + 1^2 = 65 \\ 6^2 + 5^2 = 61 \\ 6^2 + 1^2 = 37 \\ 3^2 + 7^2 = 58 \\ 5^2 + 8^2 = 89 \\ 8^2 + 9^2 = 153 \\ 1^2 + 5^2 + 3^2 = 35 \\ 3^2 + 5^2 = 34 \\ 3^2 + 4^2 = 25 \\ 2^2 + 5^2 = 29 \\ 2^2 + 9^2 = 85 \\ 8^2 + 5^2 = 89 \\ \vdots \end{gathered}$$

A partir da última linha dos cálculos efetuados, teremos uma repetição infinita de 153*,* 35*,* 34*,* 25*,* 29 *e* 85*, nesta ordem.*

Desafio 3.24. *Verifique se os números* 28*,* 30 *e* 98 *são números felizes.*

3.3 DIVISORES DE UM QUADRADO PERFEITO

Nesta seção, estudaremos exclusivamente as propriedades dos números quadrados perfeitos relacionadas a seus divisores. Para isso, utilizaremos, como base, o Teorema Fundamental da Aritmética e os principais teoremas que tratam dos divisores. Sem perda de generalidade, consideraremos apenas os divisores inteiros não negativos.

Proposição 3.25. *[3, p.81] Seja $N = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ um número natural, onde p_i's são números primos positivos distintos e $\alpha_i \in \mathbb{N}$ para todo i. Se N' é um divisor de N, então*

$$N' = p_1^{\beta_1} \cdots p_n^{\beta_n},$$

onde $0 \leq \beta_i \leq \alpha_i$ para todo $i = 1, \ldots, r$. Mais ainda, a quantidade de divisores de N é $(\alpha_1 + 1) \cdots (\alpha_n + 1)$.

Demonstração. Se N' é um divisor de N e p^β é a maior potência de um primo p que aparece na decomposição de N', então p^β divide $N = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Como os primos p_i's são distintos e p é primo, então p^β divide $p_i^{\alpha_i}$ para algum i e é coprimo com $p_j^{\alpha_j}$ para todo $j \neq i$. Logo, $\beta \leq \alpha_i$. Como os primos p_i's são distintos, pelo princípio multiplicativo, temos que a quantidade de divisores de N é $(\alpha_1 + 1) \cdots (\alpha_n + 1)$. □

Propriedade 3.26. *[3, p.82] Todo quadrado perfeito $N = (p_1)^{2\alpha_1} \cdot (p_2)^{2\alpha_2} \cdots (p_k)^{2\alpha_k}$, possui uma quantidade ímpar de divisores positivos.*

Demonstração. Basta notar que neste caso a quantidade de divisores positivos de N é

$$(2\alpha_1 + 1) \cdots (2\alpha_k + 1).$$

Como $2\alpha_i + 1$ é ímpar para todo i, temos que $(2\alpha_1 + 1) \cdots (2\alpha_k + 1)$ é ímpar. □

Corolário 3.27. *Seja N um número inteiro positivo formado pelo produto de quadrados de números primos positivos distintos entre si, ou seja, $N = (p_1)^2 \cdot (p_2)^2 \cdots (p_k)^2$, com $p_i \neq p_j$, $i \neq j$. O número de divisores positivos de N é 3^k.*

Demonstração. Neste caso, basta notar que $\alpha_i = 2$ para todo i e, então, $\alpha_i + 1 = 3$. □

Observação 3.28. *Se considerarmos todos os divisores inteiros, basta multiplicar por 2 a quantidade de divisores que acabamos de determinar, ou seja:*

$$d_Z = 2 \cdot (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_i + 1),$$

onde d_Z é a quantidade de divisores inteiros de N.

Proposição 3.29. *Para ordenarmos os divisores positivos d_N de um quadrado perfeito N em ordem crescente, basta sabermos ordenar os primeiros $\frac{d_N-1}{2}$ divisores.*

Demonstração. Consideremos o quadrado perfeito

$$N = (p_1)^{2\alpha_1} \cdot (p_2)^{2\alpha_2} \cdots (p_k)^{2\alpha_k},$$

onde $\alpha_i \in \mathbb{N}$ e $p_i \neq p_j$, para $i \neq j$ e $i, j \in \{1, 2, 3, \ldots, k\}$. Temos que $N = n^2$, onde

$$n = (p_1)^{\alpha_1} \cdot (p_2)^{\alpha_2} \cdots (p_k)^{\alpha_k}.$$

Temos também que se t é um divisor de N, então $\dfrac{N}{t}$ também o é.

Como a quantidade de divisores naturais de N é ímpar, então n ocupa a posição central da lista de divisores naturais, ordenada em ordem crescente, pois ele é o único dos divisores naturais de N que pode ser combinado com ele mesmo ($N = n \cdot n$), não podendo, portanto, aparecer mais de uma vez na lista, dado que o quociente de N por n é o próprio n. Logo, antes e depois de n, há exatamente $\dfrac{d_N - 1}{2}$ divisores naturais ambos.

Suponha que já ordenamos os $\frac{d_N-1}{2}$ menores divisores de N como

$$d_1 < d_2 < \cdots < d_{\frac{d_N-1}{2}}.$$

Perceba que o menor divisor natural de N é 1 e o maior de todos, é o próprio N. Dessa forma, temos que $d_1 = 1$ e $d_{d_N} = N$. Para escrevermos em ordem crescente cada um dos divisores de um quadrado perfeito, basta considerarmos que as posições equidistantes ao centro sempre serão d_k e $\dfrac{N}{d_k}$, para $k \in \mathbb{N}$ e $1 \leq k \leq \dfrac{d_N - 1}{2}$.

Portanto, temos que

$$d_1 < d_2 < d_3 < \cdots < d_{\frac{d_N-1}{2}} < n < \frac{N}{\frac{d_N-1}{2}} < \cdots < \frac{N}{d_3} < \frac{N}{d_2} < \frac{N}{d_1}.$$

é uma ordenação para os divisores de N. □

Exemplo 3.30. *Agora, vamos determinar a quantidade de divisores naturais de 225 e, posteriormente, escreveremos, em ordem crescente, cada um deles.*

Decompondo 225 em fatores primos, temos que $225 = 3^2 \cdot 5^2$. *Note que* $N = 225$ *e* $\alpha_1 = \alpha_2 = 2$. *Logo:*

$$\begin{aligned} d_N &= (\alpha_1 + 1) \cdot (\alpha_2 + 1) \\ &= (2 + 1) \cdot (2 + 1) \\ &= 3 \cdot 3 \\ &= 9 \end{aligned}$$

Para escrevermos cada um dos divisores naturais de 225, consideraremos primeiro que qualquer número natural, primo ou composto, é divisível por 1 e por ele mesmo. Usando a ideia proposta anteriormente, sabemos que os divisores naturais de N são todos os números possíveis de serem formados através combinação pelo princípio multiplicativo de todas as potências $(p_i)^{s_i}$, com $s_i \in \{0, 1, 2, \ldots, \alpha_i\}$ e $i = 1, 2, \ldots, k$. Para $N = 225$, temos os seguintes divisores:

$$
\begin{gathered}
3^0 \cdot 5^0,\ 3^0 \cdot 5^1,\ 3^0 \cdot 5^2, \\
3^1 \cdot 5^0,\ \boxed{3^1 \cdot 5^1},\ 3^1 \cdot 5^2, \\
3^2 \cdot 5^0,\ 3^2 \cdot 5^1,\ 3^2 \cdot 5^2.
\end{gathered}
$$

*Isto é: 1, 5, 25, 3, **15**, 75, 9, 45, 225.*

O termo destacado em negrito é $n = \sqrt{225}$.

É possível escrevermos, de forma ordenada, cada um desses divisores. Nesse caso, consideraremos $N = 225$ e $n = \sqrt{225} = 15$5. Assim, o menor divisor natural de 225 é 1; o divisor que ocupa a posição central da lista é 15; e o maior divisor, o próprio 225. Assim, nossa lista ordenada de divisores de 225 é:

1, ___, ___, ___, 15, ___, ___, ___, 225.

É fácil perceber que 3 e 5 também são divisores naturais de 225 pois são os fatores primos, distintos entre si, que aparecem na sua decomposição. Isto é:

*1, 3, 5, ___, **15**, ___, ___, ___, 225.*

Para descobrirmos outros dois divisores de 225, basta obtermos os quocientes de 225 por 3 e de 225 por 5, ou seja, respectivamente, 75 e 45. Desse modo, temos já os seguintes divisores naturais de 225:

*1, 3, 5, ___, **15**, ___, 45, 75, 225.*

Para completar as duas lacunas da lista, basta observarmos que ainda não utilizamos $3^2 \cdot 5^0 = 9$. *Logo, os dois divisores naturais que faltam para completar essa lista são: 9 e o quociente de 225 por 9, que é 25. Portanto, a lista ordenada dos divisores naturais de 225 é a seguinte:*

*1, 3, 5, 9, **15**, 25, 45, 75, 225.*

*Note que, antes e depois de **15**, há exatamente 4 divisores ambos.*

Usando a Propriedade 3.26, é possível determinar a quantidade de divisores naturais de qualquer quadrado perfeito. Por isso, propomos a você leitor o desafio a seguir.

Desafio 3.31. *Determine a quantidade de divisores naturais de 400 e 441 e escreva cada um deles.*

3.4 MÁXIMO DIVISOR COMUM ENVOLVENDO QUADRADOS PERFEITOS

Como vimos na seção anterior, é possível determinarmos a quantidade de divisores de um dado número quadrado perfeito, inclusive escrevermos, de forma ordenada, cada um deles. Nesta seção, estudaremos todas as propriedades referentes ao máximo divisor comum envolvendo quadrados perfeitos.

Proposição 3.32. *[3, p.34] Dados a, b e n inteiros, temos que*

$$mdc(a, b) = mdc(a, b - n \cdot a).$$

Demonstração. Consideremos $d = mdc(a, b - n \cdot a)$. Como $d \mid a$ e $d \mid b - n \cdot a$, temos que $d \mid b = b - n \cdot a + n \cdot a$. Consideremos agora que c seja um divisor comum de a e b. Logo, $c \mid a$ e $c \mid b - n \cdot a$. Isso garante que $c \mid d$ e, portanto, $d = mdc(a, b)$.

Portanto, satisfeitas as condições iniciais, $mdc(a, b) = mdc(a, b - n \cdot a)$. □

Teorema 3.33. *[3, p.36] (***Algoritmo de Euclides***)*
Sejam $r_{-1} = a$, $r_0 = b$ inteiros não negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter

$$r_{j-1} = q_{j+1} r_j + r_{j+1}, \ \ 0 \leq r_{j+1} < r_j$$

para $j = 0, 1, 2, \cdots, n-1$ e r_{n+1} for o primeiro resto igual a zero, então $mdc(a, b) = r_n$.

Demonstração. Suponhamos que $1 < b < a$ e que b não divide a. Pela divisão euclidiana, temos que

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b.$$

(1) Se r_1 divide b, então $r_1 = mdc(b, r_1)$ e, Pela Proposição 3.32, temos que

$$r_1 = mdc(b, r_1) = mdc(b, a - q_1 b) = mdc(b, a) = mdc(a, b),$$

e assim se encerra o algoritmo.

(2) Se r_1 não divide b, pela divisão euclidiana, temos que

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1.$$

(a) Se r_2 divide r_1, então $r_2 = mdc(r_1, r_2)$ e, pela Proposição 3.32, temos que

$$r_2 = mdc(r_1, r_2) = mdc(r_1, b - q_2 r_1) = mdc(r_1, b) = mdc(a - q_1 b, b) = mdc(a, b),$$

e assim se encerra o algoritmo.

(b) Se r_2 não divide r_1, pela divisão euclidiana, temos que que

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

Utilizando sucessivas vezes esse procedimento, é certo que, em algum dado momento, ele cessará, pois, caso contrário, teríamos uma sequência infinita de naturais tais que $b > r_1 > r_2 > r_3 > \dots$, o que não é possível por conta do Princípio da Boa Ordenação. Isso significa que, para algum dado n, existirá $r_n \mid r_{n-1}$, ou seja:

$$mdc(a,b) = r_n.$$

□

Propriedade 3.34. *Dois números naturais coprimos têm seus quadrados também coprimos.*

Demonstração. Suponha que existisse um número primo positivo p tal que $p|a^2$ e $p|b^2$. Como p é primo, então $p|a$ e $p|b$. Logo, $mdc(a,b) \neq 1$. Como temos, por hipótese, $mdc(a,b) = 1$, então não existe tal primo positivo p. Portanto, $mdc(a^2,b^2) = 1$. □

Propriedade 3.35. *O máximo divisor comum entre dois quadrados perfeitos é um quadrado perfeito.*

Demonstração. Sejam a e b dois quadrados perfeitos. Temos que

$$a = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$$

e

$$b = p_1^{2\beta_1} \cdots p_k^{2\beta_k},$$

onde p_i's são números primos positivos distintos e $0 \leq \alpha_i, \beta_i$ são números naturais para todo $i = 1, \dots, k$. Temos que

$$mdc(a,b) = p_1^{2 \cdot min\{\alpha_1,\beta_1\}} \cdots p_k^{2 \cdot min\{\alpha_k,\beta_k\}} = \left(p_1^{min\{\alpha_1,\beta_1\}} \cdots p_k^{min\{\alpha_k,\beta_k\}}\right)^2,$$

que é um quadrado perfeito. □

Propriedade 3.36. *Os quadrados de dois números naturais consecutivos são coprimos.*

Demonstração. Sejam a e b dois números naturais consecutivos. Sem perda de generalidade, tomemos $b > a$, isto é, $b = a + 1$. Calculemos agora o mdc(a,b), dadas as condições iniciais, ou seja:

$$mdc(a,b) = mdc(a, a+1)$$

Usando a Proposição 3.32, temos que:

$$mdc(a,b) = mdc(a, a+1) = mdc(a, a+1-a) = mdc(a,1) = 1.$$

Portanto, os quadrados perfeitos de dois números consecutivos são coprimos. □

Para calcularmos o máximo divisor comum entre dois números inteiros, podemos utilizar a decomposição em fatores primos e o Algoritmo de Euclides.

Exemplo 3.37. ***(1)*** *Usando a decomposição em fatores primos.*

(a) Vamos calcular o máximo divisor comum de 36 e 81.
Note que $36 = 2^2 \cdot 3^2$ *e* $81 = 3^4 = 3^2 \cdot 3^2$. *Logo, o* $mdc(36, 81) = 3^2 = 9$.

(b) Vamos calcular o máximo divisor comum de 49 e 196.
Note que $49 = 7^2$ *e* $196 = 2^2 \cdot 7^2$. *Logo, o* $mdc(49, 196) = 7^2 = 49$.

(c) Vamos calcular o máximo divisor comum de 64 e 100.
Note que $64 = 2^6 = 2^2 \cdot 2^2 \cdot 2^2$ *e* $100 = 2^2 \cdot 5^2$. *Logo, o* $mdc(64, 100) = 2^2 = 4$.

(d) Vamos calcular o máximo divisor comum de 225 e 441.
Note que $225 = 3^2 \cdot 5^2$ *e* $441 = 3^2 \cdot 7^2$. *Logo, o* $mdc(225, 441) = 3^2 = 9$.

(e) Vamos calcular o máximo divisor comum de 25 e 144.
Note que $25 = 5^2$ *e* $144 = 2^4 \cdot 3^2 = 2^2 \cdot 2^2 \cdot 3^2$. *Logo, o* $mdc(25, 144) = 1$.

(2) *Usando o Algoritmo de Euclides (Proposição 3.33)*
Para o Algoritmo de Euclides, vamos utilizar também a Proposição 3.32, desta seção.
(a) $mdc(36, 81) = 9$. *De fato, temos que*

$$81 = 2 \cdot 36 + 9 \text{ e}$$
$$36 = 4 \cdot 9.$$

Portanto,

$$mdc(36, 81) = mdc(36, 81 - 2 \cdot 36) = mdc(36, 9).$$

(b) $mdc(49, 196) = 49$. *De fato, temos que*

$$196 = 4 \cdot 49.$$

(c) $mdc(64, 100) = 4$. *De fato, temos que*

$$100 = 1 \cdot 64 + 36$$
$$64 = 1 \cdot 36 + 28$$
$$36 = 1 \cdot 28 + 8$$
$$28 = 3 \cdot 8 + 4 \text{ e}$$
$$8 = 2 \cdot 4.$$

Portanto,

$$\begin{aligned} mdc(64,100) &= mdc(64,100-1\cdot 64) = mdc(64,36) \\ mdc(36,64) &= mdc(36,64-1\cdot 36) = mdc(36,28) \\ mdc(28,36) &= mdc(28,36-1\cdot 28) = mdc(28,8) \ \ e \\ mdc(8,28) &= mdc(8,28-3\cdot 8) = mdc(8,4). \end{aligned}$$

(d) $mdc(225,441)=9$. *De fato, temos que*

$$\begin{aligned} 441 &= 1\cdot 225+216 \\ 225 &= 1\cdot 216+9 \ \ e \\ 216 &= 24\cdot 9. \end{aligned}$$

Portanto,

$$\begin{aligned} mdc(225,441) &= mdc(225,441-1\cdot 225) = mdc(225,216) \ \ e \\ mdc(216,225) &= mdc(216,225-1\cdot 216) = mdc(216,9). \end{aligned}$$

(e) $mdc(144,25)=1$. *De fato, temos que*

$$\begin{aligned} 144 &= 5\cdot 25+19 \\ 25 &= 1\cdot 19+6 \\ 19 &= 3\cdot 6+1 \ \ e \\ 6 &= 6\cdot 1. \end{aligned}$$

Portanto,

$$\begin{aligned} mdc(144,25) &= mdc(25,144-5\cdot 25) = mdc(25,19) \\ mdc(19,25) &= mdc(19,25-1\cdot 19) = mdc(19,6) \ \ e \\ mdc(6,19) &= mdc(6,19-3\cdot 6) = mdc(6,1). \end{aligned}$$

Ao utilizarmos o Algoritmo de Euclides para o cálculo do máximo divisor comum entre dois ou mais números inteiros, estamos, na verdade, utilizando a divisão euclidiana e a Proposição 3.32 desta seção, dado que é necessário identificar a existência e a unicidade da escrita de um número inteiro, quando dividido por outro inteiro.

Para facilitar os cálculos, sugerimos que as divisões sejam realizadas na chave e sejam destacados o resto e o quociente, em cada uma delas, conforme se pode observar na figura a seguir.

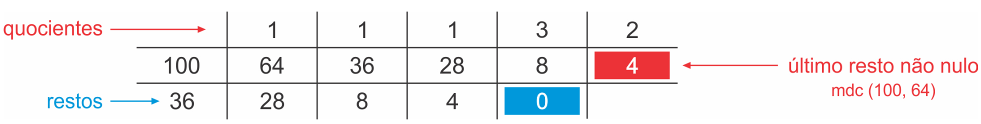

Figura 10. Algoritmo de Euclides

Primeiro, dividimos (na chave) 100 por 64 e obtemos 1 como quociente e 36 como resto. Anotamos abaixo de 100 o resto e o quociente, acima de 64. Copiamos, ao lado direito de 64, o primeiro resto obtido (36) e efetuamos a divisão de 64 por 36, anotando, abaixo de 64, o resto obtido (28) e o quociente (1) acima de 36. E vamos repetindo esse procedimento, até que, em um dado momento, a divisão, na chave, deixe resto zero e cessamos as sucessivas divisões. Note que o **último quociente** utilizado é, na verdade, o **último resto não nulo** obtido por meio das divisões sucessivas efetuadas. Esse valor obtido é o máximo divisor comum entre os dois primeiros números utilizados, ou seja, o $mdc(100, 64)$. Na verdade, esse valor é o *mdc* entre quaisquer dos números que aparecem na linha central (100, 64, 36, 28, 8, 4).

Propomos a você leitor o seguinte desafio:

Desafio 3.38. *Calcule, utilizando o Algoritmo de Euclides, o mdc de 196 e 1.225; de 484 e 900; e de 625 e 1.089.*

4 TÓPICOS AVANÇADOS DE ARITMÉTICA

Neste capítulo, traremos estudos mais aprofundados realizados durante o curso do PROFMAT, na disciplina de Aritmética. Este capítulo tem, como objetivo, apresentar peculiaridades dos quadrados perfeitos não citadas, evidenciadas e demonstradas no capítulo anterior. Todas as informações aqui contidas encontram-se no livro "Aritmética", da SBM [3]. A princípio, separamos algumas assertivas para serem demonstradas com rigor matemático, utilizando, como referência, o Pequeno Teorema de Fermat. Deixamos para este capítulo um estudo sobre sentenças que, embora envolvam características diretamente ligadas aos quadrados perfeitos, precisam de maior cuidado e de um grande conjunto de teorias elementares, para suas respectivas demonstrações. A prioridade neste estudo também é investigar os quadrados perfeitos com ênfase no conjunto dos números naturais, incluindo o zero. No entanto, é totalmente possível expandirmos para os inteiros tudo o que é apresentado e demonstrado aqui.

Apresentamos, logo a seguir, os mais importantes teoremas que envolvem aritmética modular e os quadrados perfeitos.

4.1 O PEQUENO TEOREMA DE FERMAT

Desde pelo menos 500 anos antes de Cristo os chineses sabiam que se p é um número primo positivo, então o número $2^p - 2$ é divisível por p. Pierre de Fermat generalizou este resultado no século XVII, provando que p divide $a^p - a$ para todo inteiro a.

Para o caso $p = 2$, temos que $2 \mid 2^p - 2 = 2 \cdot (2^{p-1} - 1)$, pois, embora 2 não divida $(2^{p-1} - 1)$, é certo que $2 \mid 2$.

Agora, se $p > 2$, embora p não divida 2, podemos demonstrar que p divide $(2^{p-1} - 1)$. Vamos apresentar nesta seção.

Antes vamos enunciar e demonstrar o Pequeno Teorema de Fermat vamos precisar do lema a seguir.

Lema 4.1. *[3, p.94] Seja p um número primo. Os números $\begin{pmatrix} p \\ i \end{pmatrix}$, com $0 < i < p$, são todos divisíveis por p.*

Demonstração. Note que o resultado vale para $i = 1$, pois $\begin{pmatrix} p \\ 1 \end{pmatrix} = p$.

Vamos supor $1 < i < p$. Como $\begin{pmatrix} p \\ i \end{pmatrix} = \dfrac{p \cdot (p-1) \cdot (p-2) \cdots (p-i+1)}{i!} \in \mathbb{N}$ e $mdc(i, p) = 1$, então

$$i! \mid (p-1)\cdot(p-2)\cdots(p-i+1)$$

e portanto

$$\binom{p}{i} = p \cdot \frac{(p-1)\cdot(p-2)\cdots(p-i+1)}{i!}.$$

Logo, $\binom{p}{i}$ é divisível por p.

$\square$

Teorema 4.2. *[3, p.94] (***Pequeno Teorema de Fermat)** *Dados dois inteiros a e p, com p primo, vale a seguinte propriedade:*

$$a^p \equiv a(mod\ p),\ \textit{ou seja},\ p \mid a^p - a.$$

Demonstração. Se $p = 2$, o resultado é trivial, pois $a^2 - a = a\cdot(a-1)$ é um número par.

Por isso, vamos supor que p seja um primo ímpar e, sem perda de generalidade, que $a \geq 0$. Para essa demonstração, utilizaremos o Princípio de Indução Finita (PIF) sobre a. Para $a = 0$, temos

$$0^p \equiv 0(mod\ p) \Longleftrightarrow p \mid 0,$$

ou seja, a propriedade é válida para $a = 0$.

Essa será a nossa Hipótese de Indução.

Queremos demonstrar que a propriedade é válida para $a + 1$.

Considere que:

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1$$

Subtraiamos, em ambos os lados, $a + 1$. Logo:

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

Queremos mostrar que $p \mid (a+1)^p - (a+1)$, o que implica que teremos que mostrar que $p \mid a^p - a + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$.

Vamos dividir em duas partes essa demonstração. Por HI temos que p divide $a^p - a$. Assim, precisamos provar que:

$$p \mid \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a$$

Pelo Lema 4.1, temos que os números $\binom{p}{i}$, com $0 < i < p$, são todos divisíveis por p. Logo,

$$p \mid \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-2} a^2 + \binom{p}{p-1} a$$

Portanto, demonstramos que $p|(a+1)^p - (a+1)$. E o resultado do Pequeno Teorema de Fermat segue. □

O que pretendemos demonstrar nesta seção e que contribui para nosso estudo acerca dos quadrados perfeitos é uma particularidade do Pequeno Teorema de Fermat:

Proposição 4.3. *[3, p.95] Toda vez que $mdc(a,p) = 1$, teremos que*

$$a^p \equiv a (mod\ p) \ \ e\ p \mid a^{p-1} - 1.$$

Demonstração. Já sabemos pelo Pequeno Teorema de Fermat que p divide $a^p - a$. Portanto, existe $k \in \mathbb{N}$ tal que

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

Como p é primo e $mdc(a,p) = 1$, então p divide $a^{p-1} - 1$ (Corolário 2.16).

□

Observação 4.4. *Se $p \mid a$, então $p \mid a^{p-1}$.*

A partir de agora, devemos ter todo o cuidado ao validarmos essa propriedade, pois ela não é válida para qualquer a. Note que, por exemplo, no caso em que

$$10^5 \equiv 10 (\text{mod}\, 5).$$

Temos que 5 não divide $10^4 - 1$. Isso acontece pois $mdc(10,5) = 5 > 1$.

4.2 ALGUMAS APLICAÇÕES DO PEQUENO TEOREMA DE FERMAT

Na seção anterior, enunciamos e demonstramos um teorema de grande importância para o nosso estudo sobre os quadrados perfeitos. O Pequeno Teorema de Fermat nos fornece duas informações importantes:

(1) Se m é coprimo com 3, o quadrado de m deixa resto 1 na divisão por 3.

Em outras palavras:

$$mdc(m,3) = 1 \Longrightarrow m^2 \equiv 1 \ (mod\ 3).$$

E mais ainda:

(2) Se m é coprimo com p, existirão infinitas potências pares de m que deixam resto 1 na divisão por qualquer primo ímpar p.

Isso se deve ao fato de, pelo Pequeno Teorema de Fermat, termos que:

$$mdc(m,p) = 1 \Longrightarrow m^{p-1} \equiv 1 \ (mod\ p).$$

Assim, como p não divide m, podemos garantir que:

$$\begin{gathered} m^{p-1} \equiv 1 \ (mod\ p) \\ [m^{p-1}]^2 \equiv 1 \ (mod\ p) \\ [m^{p-1}]^3 \equiv 1 \ (mod\ p) \\ \vdots \\ [m^{p-1}]^k \equiv 1 \ (mod\ p). \end{gathered}$$

Note que, como p é um primo ímpar, então $p-1$ é par.

A seguir, temos um exemplo de como isso funciona na prática para potências pares e ímpares.

Vamos calcular o resto de 2^{2021} na divisão por 17.

1º passo: $p = 17 \Longrightarrow p - 1 = 16$.

2º passo: Pelo Pequeno Teorema de Fermat, temos que:

$$\begin{gathered} 2^{16} \equiv 1 \ (mod\ 17) \\ [2^{16}]^2 = 2^{32} \equiv 1 \ (mod\ 17) \\ [2^{16}]^3 = 2^{48} \equiv 1 \ (mod\ 17) \\ [2^{16}]^4 = 2^{64} \equiv 1 \ (mod\ 17) \\ \vdots \\ [2^{16}]^k \equiv 1 \ (mod\ p). \end{gathered}$$

3º passo: Dividir 2021 por 16 para determinar o maior expoente de 2, mas menor do que 2021, cujo resto na divisão por 17 é também igual a 1.

$$2021 = 126 \cdot 16 + 5.$$

Logo, temos que:

$$[2^{16}]^{126} = 2^{2016} \equiv 1 \ (mod\ 17).$$

Note que:

$$2^{2021} = [2^{16}]^{126} \cdot 2^5.$$

4º passo: Calcular o resto de 2^5 na divisão por 17.

Como $2^{2021} = 2^{2016} \cdot 2^5$ e já sabemos o resto de 2^{2016} na divisão por 17, vamos então calcular o resto de 2^5 na divisão por 17.

Note que, usando a divisão euclidiana, $2^5 = 32 = 1 \cdot 17 + 15$.

Logo, 2^5 deixa resto 15 na divisão por 17.

5º passo: Calcular o resto de 2^{2021} na divisão por 17.
Para esse último passo, basta lembrarmos que:

$$2^{2021} = [2^{16}]^{126} \cdot 2^5.$$

Assim:

$$2^{2021} \equiv 2^{2016} \cdot 2^5 \,(mod\ 17).$$

De fato, como $2^{2016} \equiv 1(mod\ 17)$ e $2^5 \equiv 15\,(mod\ 17)$, então:

$$2^{2021} \equiv 1 \cdot 15 \equiv 15\,(mod\ 17).$$

Portanto, o resto da divisão de 2^{2021} por 17 é 15.

Propomos a você, leitor, o seguinte desafio:

Desafio 4.5. *Calcule o resto de* 2020^{2021} *na divisão por* 37*.*

5

REPRESENTAÇÃO DE UM INTEIRO POSITIVO POR SOMAS DE QUADRADOS

Em um trabalho publicado em 1770, Waring[3] afirmou que todo inteiro positivo é a soma de no máximo 4 quadrados, no máximo 9 cubos e no máximo 19 quartas potências. Ele não demonstrou tais afirmações e provavelmente as deduziu pela observação de muitos exemplos.

No mesmo ano de 1770, Lagrange demonstrou que todo inteiro positivo é a soma de no máximo 4 quadrados.

Exemplo 5.1. *Vamos ver alguns exemplos antes da demonstração. Temos que*

$$57 = 7^2 + 2^2 + 2^2 + 0^2,$$

$$218 = 14^2 + 3^2 + 3^2 + 2^2 \ \ e$$

$$539 = 23^2 + 3^2 + 1^2 + 0^2.$$

Notemos que a decomposição de um inteiro positivo como soma de 4 quadrados não é única, pois

$$20 = 4^2 + 2^2 + 0^2 + 0^2 \ \ e$$

$$20 = 3^2 + 3^2 + 1^2 + 1^2.$$

Proposição 5.2. *[9, p.131] (Identidade de Euler) O produto de números possuindo representação como soma de quatro quadrados possui, também, representação como soma de quatro quadrados.*

Demonstração. Dados a, b, c, d, r, s, t e v números inteiros, temos que

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2) \cdot (r^2 + s^2 + t^2 + v^2) = {} & (ar + bs + ct + dv)^2 \\ & + (as - br - cv + dt)^2 \\ & + (at + bv - cr - ds)^2 \\ & + (av - bt + cs - dr)^2.\end{aligned}$$

[3] Disponível em: https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/EA_2011_MONOII.pdf

De fato, expandindo cada lado da igualdade, temos que

$$\begin{aligned}(a^2+b^2+c^2+d^2)\cdot(r^2+s^2+t^2+v^2) &= a^2r^2+a^2s^2+a^2t^2+a^2v^2+b^2r^2+b^2s^2\\ &+b^2t^2+b^2v^2+c^2r^2+c^2s^2+c^2t^2+c^2v^2\\ &+d^2r^2+d^2s^2+d^2t^2+d^2v^2\end{aligned}$$

e que

$$\begin{aligned}&(ar+bs+ct+dv)^2+(as-br-cv+dt)^2+(at+bv-cr-ds)^2+(av-bt+cs-dr)^2\\ &=a^2r^2+a^2s^2+a^2t^2+a^2v^2+b^2r^2+b^2s^2+b^2t^2+b^2v^2+c^2r^2+c^2s^2+c^2t^2+c^2v^2\\ &+d^2r^2+d^2s^2+d^2t^2+d^2v^2.\end{aligned}$$

□

Precisaremos dos lemas seguintes para demonstrar o teorema.

Lema 5.3. *[9, p.95] Seja p um primo ímpar. O conjunto*

$$\left\{1^2\,(mod\,p), 2^2\,(mod\,p), \ldots, (p-1)^2\,(mod\,p)\right\}$$

contém exatamente $\frac{p-1}{2}$ elementos distintos.

Demonstração. Consideremos os quadrados

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

Vamos mostrar que estes quadrados são incongruentes módulo p. Sejam x e y tais que $1 \leq x, y \leq \frac{p-1}{2}$ e suponhamos $x^2 \equiv y^2\,(mod\,p)$. Daí, $x^2-y^2 \equiv 0\,(mod\,p)$. Como $x^2-y^2 = (x-y)(x+y)$, temos que $(x-y)(x+y) \equiv 0\,(mod\,p)$, ou seja, p divide $(x-y)(x+y)$. Como p é primo, então p divide uma das duas parcelas do produto, ou seja, $p|(x-y)$ ou $p|(x+y)$. Temos que p não divide $x+y$, pois $2 < x+y < p$. Logo, $p|(x-y)$. Portanto, $x \equiv y\,(mod\,p)$. Com isso, concluímos que os quadrados $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ são dois a dois incongruentes módulo p. Agora, notemos que

$$(p-k)^2 \equiv k^2\,(mod\,p).$$

Portanto, $1^2 \equiv (p-1)^2\,(mod\,p)$, $2^2 \equiv (p-2)^2\,(mod\,p), \ldots$, $\left(\frac{p-1}{2}\right)^2 \equiv \left(p-\frac{p-1}{1}\right)^2 \equiv \left(\frac{p+1}{1}\right)^2\,(mod\,p)$. □

Lema 5.4. *[5, p.144] Para todo primo ímpar p existem inteiros a e b tais que*

$$a^2+b^2+1 \equiv 0\,(mod\,p)$$

Demonstração. Considere os conjuntos

$$A = \left\{a^2\,(mod\,p);\ 0 \leq a \leq \frac{p-1}{2}\right\}$$

e

$$B = \left\{-b^2 - 1\,(mod\,p);\ 0 \leq b \leq \frac{p-1}{2}\right\}.$$

De acordo com a demonstração do lema anterior, temos que os quadrados

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

são incongruentes módulo p. Além disso, eles são incongruentes a 0 módulo p, pois se $a^2 \equiv 0\,(mod\,p)$, então $p|(a^2 - 0)$, ou seja, $p|a$. Como $1 \leq a \leq \frac{p-1}{2}$, temos que p não divide a. Portanto, o conjunto A contém exatamente $\frac{p+1}{2}$ elementos distintos. Mostremos agora que os elementos de B são dois a dois incongruentes módulo p. Se $-b_1^2 - 1 \equiv -b_2^2 - 1\,(mod\,p)$, então $b_1^2 \equiv b_2^2\,(mod\,p)$. Como $0 \leq b_1, b_2 \leq \frac{p-1}{2}$, temos que b_1^2 não é congruente a b_2^2 módulo p. Portanto, o conjunto B contém exatamente $\frac{p+1}{2}$ elementos distintos. Como cada conjunto possui $\frac{p+1}{2}$ elementos, então $A \cap B \neq \emptyset$, pois existem exatamente p elementos incongruentes módulo p. Portanto, existem a e b tais que $a^2 \equiv -b^2 - 1\,(mod\,p)$. □

Teorema 5.5. *[9, p.131] [5, p.144] (Teorema de Lagrange) Todo inteiro positivo pode ser escrito como soma de 4 quadrados.*

Demonstração. Vamos demostrar que todo número primo pode ser representado como soma de quatro quadrados. Então, usando o Teorema Fundamental da Aritmética e a Identidade de Euler, é fácil ver que todo número inteiro positivo pode ser representado como soma de quatro quadrados. Primeiramente, notemos que $2 = 1^2 + 1^2 + 0^2 + 0^2$. Seja p um primo ímpar. Pelo Lema 5.4, existem inteiros a, b e c tais que

$$a^2 + b^2 + c^2 \equiv 0\,(mod\,p)$$

(tome $c = 1$, por exemplo). Logo, existem inteiros a, b, c e $d = 0$ e um inteiro positivo M tais que

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

Pelo Princípio da Boa Ordem, temos que existe um menor inteiro positivo m tal que existem inteiros a, b, c e d tais que

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

Queremos provar que $m = 1$. Vamos supor primeiro m par. É fácil ver que para m par necessariamente os inteiros a, b, c e d devem ser todos pares, dois pares e dois ímpares ou todos ímpares. Em qualquer um destes três casos podemos escolher a, b, c e d satisfazendo que a e b possuem a mesma paridade e que c e d também possuem a mesma paridade. Assim,

$$p\frac{m}{2} = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2.$$

Portanto, tomando $m'' = \frac{m}{2} < m$, obtemos uma expressão para $m''p$ como soma de quatro quadrados, o que contraria a minimalidade de m. Temos então que m é ímpar. Vamos mostrar que a suposição $m > 1$ nos leva à obtenção de um inteiro $0 \leq n < m$ o qual, também nos fornece uma representação para np como soma de quatro quadrados, o que contradiz a minimalidade de m. Seja $m > 1$ ímpar. Sejam x, y, z, w inteiros tais que

$$\begin{aligned} w &\equiv a \,(mod\, m) \\ x &\equiv b \,(mod\, m) \\ y &\equiv c \,(mod\, m) \\ z &\equiv d \,(mod\, m) \end{aligned}$$

onde $x, y, z, w \in \left(-\frac{m}{2}, \frac{m}{2}\right)$. Logo,

$$w^2 + x^2 + y^2 + z^2 < 4 \cdot \frac{m^2}{4} = m^2 \quad \text{e} \quad w^2 + x^2 + y^2 + z^2 \equiv 0 \,(mod\, m).$$

Portanto,

$$w^2 + x^2 + y^2 + z^2 = nm \quad \text{com } 0 < n < m.$$

Pela escolha de w, x, y, z, temos que os números $ax - bw - cz + dy$, $ay + bz - cw - dx$ e $az - by + cx - dw$ são divisíveis por m e

$$aw + bx + cy + dz \equiv a^2 + b^2 + c^2 + d^2 \; (mod\ m).$$

Portanto, pela proposição 5.2, temos que

$$\begin{aligned} np = \frac{1}{m^2} \cdot mp \cdot nm &= \frac{1}{m^2}(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) \\ &= \left(\frac{aw + bx + cy + dz}{m}\right)^2 + \left(\frac{ax - bw - cz + dy}{m}\right)^2 \\ &+ \left(\frac{ay + bz - cw - dx}{m}\right)^2 + \left(\frac{az - by + cx - dw}{m}\right)^2 \end{aligned}$$

é a soma de quatro quadrados. Concluímos então que $m = 1$, ou seja, o primo p pode ser representado como soma de quatro quadrados de inteiros.

$\square$

Os próximos resultados, que serão apenas enunciados, nos dizem sob quais condições um inteiro positivo m pode ser escrito como soma de 3 ou 2 quadrados apenas.

Teorema 5.6. *[5, p.146] Um inteiro* $m \geq 0$ *é soma de três quadrados se, e somente se,* m *não é da forma* $4^a(8b+7)$, *com* $a, b \in \mathbb{N}$.

Exemplo 5.7. *O inteiro* $m = 48$ *pode ser escrito como soma de* 3 *quadrados, pois* $48 = 4^2 \cdot (8 \cdot 0 + 3)$. *Temos que* $48 = 4^2 + 4^2 + 4^2$.

Teorema 5.8. *[5, p.140][9, p.130] Um inteiro* m *pode ser representado como a soma de dois quadrados se, e somente se, tiver fatoração da forma*

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

onde $p_i \equiv 1 \ (mod\ 4)$ *e* $q_j \equiv 3 \mod 4$, $i = 1, 2, \dots, r$, $j = 1, 2, \dots, s$ *e todos os expoentes* β_j *são pares.*

Exemplo 5.9. *O inteiro* $m = 218 = 2 \cdot 109$ *pode ser escrito como soma de* 2 *quadrados, pois* $109 \equiv 1 \, (mod\, 4)$. *Temos que* $218 = 13^2 + 7^2$.

Propomos a você, leitor, o seguinte desafio:

Desafio 5.10. *Escreva como soma de quatro quadrados os números* 31, 54, 93 *e* 119.

6 DICAS E RESOLUÇÕES DOS DESAFIOS PROPOSTOS

Neste capítulo, encontram-se dicas e resoluções para cada um dos desafios propostos ao longo dos capítulos. É de extrema importância para a compreensão do passo a passo que envolve, por exemplo, a decomposição de um número na base sexagesimal, o cálculo de um máximo divisor comum, entre outras aplicações.

- **Seção 2.2**

  (1) Mostre que, se $k^2 < 100$ é um número triangular, então $k = 1$ ou $k = 6$.

  Basta calcular o valor de 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2 e 9^2 e perceber que os únicos números triangulares serão 1 e 36.

  (2) Mostre, sem utilizar aritmética ou álgebra, simplesmente reorganizando diagramas de números figurados, que oito vezes um número triangular mais um é igual a um número quadrado. Se o número triangular tem ordem n, qual a ordem do número quadrado obtido pelo processo acima?

  Esse problema se resolve basicamente a partir da ideia de completar quadrados ao reorganizar, em filas de mesmo comprimento, o óctuplo de bolinhas de um número triangular. Esse processo é facilitado quando os números triangulares estão dispostos de maneira a formarem triângulos retângulos isósceles. Assim, ao encaixá-los convenientemente, teremos um quadrado quase perfeito, faltando apenas uma bolinha para completá-lo.

  Listamos a seguir quadrados construídos através desse processo.

$$\begin{gathered}8 \cdot 1 + 1 = 9 \\ 8 \cdot 3 + 1 = 25 \\ 8 \cdot 6 + 1 = 49 \\ 8 \cdot 10 + 1 = 81 \\ 8 \cdot 15 + 1 = 121 \\ \vdots \\ 8 \cdot \frac{n \cdot (n+1)}{2} + 1 = (2n+1)^2.\end{gathered}$$

  Se o número triangular tem ordem n, o número quadrado obtido por esse processo tem ordem $2n + 1$.

- **Seção 3.1**

Usando as propriedades observadas, calcule o quadrado de:

(a) 61

1º passo: $61 = 10 \cdot 6 + 1$, onde $a = 6$.

2º passo: Usando a fórmula (20), temos que:

$$\begin{aligned} 61^2 &= 6 \cdot (10 \cdot 6 + 2)\ \boxed{1} \\ &= 6 \cdot 62\ \boxed{1} \\ &= 372\ \boxed{1} \\ &= 3721. \end{aligned}$$

(b) 92

1º passo: $92 = 10 \cdot 9 + 2$, onde $a = 9$.

2º passo: Usando a fórmula (21), temos que:

$$\begin{aligned} 92^2 &= 9 \cdot (10 \cdot 9 + 4)\ \boxed{4} \\ &= 9 \cdot 94\ \boxed{4} \\ &= 846\ \boxed{4} \\ &= 8464. \end{aligned}$$

(c) 113

1º passo: $113 = 10 \cdot 11 + 3$, onde $a = 11$.

2º passo: Usando a fórmula (22), temos que:

$$\begin{aligned} 113^2 &= 11 \cdot (10 \cdot 11 + 6)\ \boxed{9} \\ &= 11 \cdot 116\ \boxed{9} \\ &= 1276\ \boxed{9} \\ &= 12769. \end{aligned}$$

(d) 54

1º passo: $54 = 10 \cdot 5 + 4$, onde $a = 5$.

2º passo: Usando a fórmula (23), temos que:

$$
\begin{aligned}
54^2 &= 5 \cdot (10 \cdot 5 + 8) + 1\ \boxed{6} \\
&= 5 \cdot 58 + 1\ \boxed{6} \\
&= 291\ \boxed{6} \\
&= 2916.
\end{aligned}
$$

(e) 85

1º passo: $85 = 10 \cdot 8 + 5$, onde $a = 8$.

2º passo: Usando a fórmula (24), temos que:

$$
\begin{aligned}
85^2 &= 8 \cdot (8 + 1)\ \boxed{25} \\
&= 72\ \boxed{25} \\
&= 7225.
\end{aligned}
$$

(f) 106

1º passo: $106 = 10 \cdot 10 + 6$, onde $a = 10$.

2º passo: Usando a fórmula (25), temos que:

$$
\begin{aligned}
106^2 &= 10 \cdot (10 \cdot 10 + 12) + 3\ \boxed{6} \\
&= 10 \cdot 112 + 3\ \boxed{6} \\
&= 372\ \boxed{6} \\
&= 11236.
\end{aligned}
$$

(g) 87

1º passo: $87 = 10 \cdot 8 + 7$, onde $a = 8$.

2º passo: Usando a fórmula (26), temos que:

$$
\begin{aligned}
87^2 &= 8 \cdot (10 \cdot 8 + 14) + 4\ \boxed{9} \\
&= 8 \cdot 94 + 4\ \boxed{9} \\
&= 756\ \boxed{9} \\
&= 7569.
\end{aligned}
$$

(h) 98

1º passo: $98 = 10 \cdot 9 + 8$, onde $a = 9$.

2º passo: Usando a fórmula (27), temos que:

$$
\begin{aligned}
98^2 &= 9 \cdot (10 \cdot 9 + 16) + 6\ \boxed{4} \\
&= 9 \cdot 106 + 6\ \boxed{9} \\
&= 960\ \boxed{4} \\
&= 9604.
\end{aligned}
$$

(i) 119

1º passo: $119 = 10 \cdot 11 + 9$, onde $a = 11$.

2º passo: Usando a fórmula (28), temos que:

$$
\begin{aligned}
119^2 &= 11 \cdot (10 \cdot 11 + 18) + 8\ \boxed{1} \\
&= 11 \cdot 128 + 8\ \boxed{1} \\
&= 1416\ \boxed{1} \\
&= 14161.
\end{aligned}
$$

(j) 750

1º passo: $750 = 10 \cdot 75$, onde $a = 75$.

2º passo: Usando a fórmula (19), temos que:

$$750^2 = 100 \cdot (75^2).$$

3º passo: Como $70 = 10 \cdot 7 + 5$, conforme a fórmula (F), temos que:

$$
\begin{aligned}
75^2 &= 7 \cdot (7 + 1)\ \boxed{25} \\
&= 56\ \boxed{25} \\
&= 5625.
\end{aligned}
$$

Portanto:

$$
\begin{aligned}
750^2 &= 100 \cdot 5625 \\
&= 562500.
\end{aligned}
$$

- **Seção 3.2**

  Desafio: *Verifique se os números* 28, 30 *e* 98 *são números felizes.*

  (1) O número 28 é um número feliz, pois:

$$28^2 = 784$$
$$7^2 + 8^2 + 4^2 = 129$$
$$1^2 + 2^2 + 9^2 = 86$$
$$8^2 + 6^2 = 100$$
$$1^2 + 0^2 + 0^2 = 1$$

(2) O número 30 não é um número feliz, pois:

$$98^2 = 9064$$
$$9^2 + 0^2 + 6^2 + 4^2 = 133$$
$$1^2 + 3^2 + 3^2 = 19$$
$$1^2 + 9^2 = 82$$
$$8^2 + 2^2 = 68$$
$$6^2 + 8^2 = 100$$
$$1^2 + 0^2 + 0^2 = 1$$

(3) O número 98 é um número feliz, pois:

$$30^2 = 900$$
$$9^2 + 0^2 + 0^2 = 81$$
$$8^2 + 1^2 = 65$$
$$6^2 + 5^2 = 61$$
$$6^2 + 1^2 = 37$$
$$3^2 + 7^2 = 58$$
$$5^2 + 8^2 = 89$$
$$8^2 + 9^2 = 153$$
$$1^2 + 5^2 + 3^2 = 35$$
$$3^2 + 5^2 = 34$$
$$3^2 + 4^2 = 25$$
$$2^2 + 5^2 = 29$$
$$2^2 + 9^2 = 85$$
$$8^2 + 5^2 = 89$$
$$\vdots$$

Note que, no caso do número 30, a partir da última linha da resolução, teremos uma repetição infinita de somas de quadrados iguais a 89, 153, 35, 34, 25, 29 e 85, nesta ordem.

Desafio: *Escreva sete exemplos de quadrados perfeitos que podem ser escritos como soma de dois outros quadrados perfeitos.*

Utilizando o primeiro método pitagórico, temos:

Exemplo 1: Tomemos $x = 3$. Assim:

$$x = 3$$
$$y = \frac{3^2 - 1}{2} = 4$$
$$z = \frac{3^2 + 1}{2} = 5.$$

Logo, temos que $3^2 + 4^2 = 5^2$.

Exemplo 2: Tomemos $x = 5$. Assim:

$$x = 5$$
$$y = \frac{5^2 - 1}{2} = 12 \text{ e}$$
$$z = \frac{5^2 + 1}{2} = 13.$$

Logo, temos que $5^2 + 12^2 = 13^2$.

Exemplo 3: Tomemos $x = 7$. Assim:

$$x = 7$$
$$y = \frac{7^2 - 1}{2} = 24 \text{ e}$$
$$z = \frac{7^2 + 1}{2} = 25.$$

Logo, temos que $7^2 + 24^2 = 25^2$.

Exemplo 4: Tomemos $x = 9$. Assim:

$$x = 9$$
$$y = \frac{9^2 - 1}{2} = 40 \text{ e}$$
$$z = \frac{9^2 + 1}{2} = 41.$$

Logo, temos que $9^2 + 40^2 = 41^2$.

Utilizando o segundo método pitagórico, temos:

Exemplo 5: Tomemos $l = 2$, $u = 3$ e $v = 2$. Assim:

$$x = 2 \cdot 2 \cdot 3 \cdot 2 = 12$$
$$y = 2 \cdot (3^2 - 2^2) = 10 \text{ e}$$
$$z = 2 \cdot (3^2 + 2^2) = 26.$$

Logo, temos que $24^2 + 10^2 = 26^2$.

Exemplo 6: Tomemos $l = 2$, $u = 5$ e $v = 2$. Assim:

$$x = 2 \cdot 2 \cdot 5 \cdot 2 = 40$$
$$y = 2 \cdot (5^2 - 2^2) = 42 \text{ e}$$
$$z = 2 \cdot (5^2 + 2^2) = 58.$$

Logo, temos que $40^2 + 42^2 = 58^2$.

Exemplo 7: O exemplo a seguir é chamado de *terno pitagórico raro*, pois trata-se de um quadrado perfeito que pode ser obtido a partir da soma dos quadrados de dois números inteiros consecutivos.

$$119^2 + 120^2 = 169^2.$$

- **Seção 3.3**

Para calcular a quantidade de divisores naturais de 400, note que $400 = 2^4 \cdot 5^2$. Assim:

$$d_{400} = (4 + 1) \cdot (2 + 1) = 5 \cdot 3 = 15.$$

Portanto, 400 possui 15 divisores naturais: 1, 2, 4, 5, 8, 10, 16, 20, 25, 40, 50, 80, 100, 200 e 400.

Para calcular a quantidade de divisores naturais de 441, note que $441 = 3^2 \cdot 7^2$. Assim:

$$d_{441} = (2 + 1) \cdot (2 + 1) = 3 \cdot 3 = 9.$$

Portanto, 441 possui 9 divisores naturais: 1, 3, 7, 9, 21, 49, 63, 147 e 441.

- **Seção 3.4**

  Calcule, utilizando o Algoritmo de Euclides, o mdc de 196 e 1.225; de 484 e 900; e de 625 e 1.089.

  (1) Usando o algoritmo de Euclides para calcular o $mdc(196, 1225)$:

$$1225 = 6 \cdot 196 + 49 \text{ e}$$
$$196 = 4 \cdot 49.$$

  Portanto, $mdc(196, 1225) = 49$.

  (2) Usando o algoritmo de Euclides para calcular o $mdc(484, 900)$:

$$900 = 1 \cdot 484 + 416$$
$$484 = 1 \cdot 416 + 68$$
$$416 = 6 \cdot 68 + 8$$
$$68 = 8 \cdot 8 + 4 \text{ e}$$
$$8 = 2 \cdot 4.$$

  Portanto, $mdc(484, 900) = 4$.

  (3) Usando o algoritmo de Euclides para calcular o $mdc(625, 1089)$:

$$1089 = 1 \cdot 625 + 464$$
$$625 = 1 \cdot 464 + 161$$
$$464 = 2 \cdot 161 + 142$$
$$161 = 1 \cdot 142 + 19$$
$$142 = 7 \cdot 19 + 9$$
$$19 = 2 \cdot 9 + 1 \text{ e}$$
$$9 = 9 \cdot 1.$$

  Portanto, $mdc(625, 1089) = 1$.

- **Seção 4.3**

  Calcule o resto de 2020^{2021} *na divisão por* 37.

  Como o número 37 é primo, podemos utilizar o Pequeno Teorema de Fermat. Assim:

$$2020^{37} \equiv 2020 \ (mod\ 37).$$

Note que $mdc(2020, 37) = 1$. Logo, podemos escrever que:

$$2020^{36} \equiv 1 \ (mod\ 37).$$

Como $2021 = 56 \cdot 36 + 5$, então $2020^{2021} = [2020^{56}]^{36} \cdot 2020^{5}$.

Como $2020^{36} \equiv 1 \ (mod\ 37)$, então $[2020^{56}]^{36} \equiv 1 \ (mod\ 37)$.

Usando o algoritmo de Euclides, temos que:

$$2020 = 54 \cdot 37 + 22.$$

Logo, temos que:

$$2020 \equiv 22 \ (mod\ 37).$$

Desse modo, reescrevemos:

$$2020^{5} \equiv 22^{5} \equiv 22^{2} \cdot 22^{2} \cdot 22 \ (mod\ 37).$$

Note que $22^2 = 484 = 13 \cdot 37 + 3$.

Logo, temos que:

$$22^{2} \equiv 3 \ (mod\ 37).$$

Assim:

$$22^{5} \equiv 3 \cdot 3 \cdot 22 \ (mod\ 37) \text{ e}$$
$$22^{5} \equiv 198 \ (mod\ 37).$$

Usando o algoritmo de Euclides, temos $198 = 5 \cdot 37 + 13$.

Logo:

$$2020^{2021} \equiv 13 \ (mod\ 37).$$

Portanto, o resto da divisão de 2020^{2021} por 37 é 13.

- **Capítulo 5**

  Desafio: *Escreva como soma de quatro quadrados os números* 31, 54, 93 *e* 119.

  Uma possível solução:

$$31 = 1^2 + 1^2 + 2^2 + 5^2$$
$$54 = 0^2 + 2^2 + 5^2 + 5^2$$
$$93 = 2^2 + 2^2 + 2^2 + 9^2$$
$$119 = 1^2 + 3^2 + 3^2 + 10^2$$

  Note que, em ambos os casos, houve repetição de quadrados.

7

INFORMAÇÕES IMPORTANTES AO DOCENTE

Este capítulo servirá de guia para a prática de ensino sobre o que trata o presente projeto. Para isso, serão apresentadas informações contidas no "Currículo Paulista" [1]. Cabe ao docente dosar todas as informações aqui transmitidas, inclusive no que diz respeito ao desenvolvimento do seu trabalho em sala de aula. Deve-se ter muita cautela no momento de introduzir uma nova abordagem sobre os números inteiros não negativos, tendo em vista que muitos alunos possuem grandes dificuldades na escrita matemática, principalmente quando se trata da representação desses números. Por isso, antes de iniciar qualquer estudo a respeito dos números quadrados perfeitos e suas propriedades, o docente deve trabalhar, como pré-requisito, algumas habilidades importantes, assim que o aluno ingressa para o Ensino Fundamental II.

7.1 HABILIDADES A SEREM TRABALHADAS COMO PRÉ-REQUISITO

Segundo o "Currículo Paulista" [1], de 26 de julho de 2019, na área de conhecimento que trata sobre a Matemática e suas tecnologias, o docente deve ter seu trabalho, em sala de aula, respaldado nas seguintes habilidades e seus respectivos objetos do conhecimento:

$\Longrightarrow$ **6º ano do Ensino Fundamental**

(1) Habilidade EF06MA02 (lê-se Ensino Fundamental, 6º ano, Matemática, habilidade 02) (Números): reconhecer o sistema de numeração decimal como fruto de um processo histórico e identificar suas principais características.

Objeto do conhecimento: características, leitura, escrita e comparação de números naturais e de números racionais representados na forma decimal.

(2) Habilidade EF06MA03 (Números): solucionar problemas que envolvam cálculos com números naturais.

Objeto do conhecimento: adição, subtração, multiplicação, divisão e potenciação com números naturais; Divisão euclidiana.

(3) Habilidade EF06MA04A (Números): reconhecer um fluxograma tendo, como referência, sua estrutura e de seus elementos.

Objeto do conhecimento: determinar a paridade de um número natural; múltiplos e divisores de um número natural; números primos e compostos.

(4) Habilidade EF06MA05 (Números): classificar números naturais em primos e compostos, identificar múltiplos e divisores e estabelecer alguns critérios de divisibilidade.

Objeto do conhecimento: determinar a paridade de um número natural; múltiplos e divisores de um número natural; números primos e compostos.

(5) Habilidade EF06MA06 (Números): resolver e elaborar situações-problema acerca da ideia de múltiplo e de divisor.

Objeto do conhecimento: determinar a paridade de um número natural; múltiplos e divisores de um número natural; números primos e compostos.

(6) Habilidade EF06MA14 (Álgebra): reconhecer que a relação de igualdade matemática permanece inalterável, quanto ao fato de adicionar, subtrair, multiplicar ou dividir os seus dois membros por um mesmo número e, com isso, ser possível determinar valores desconhecidos na resolução de problemas.

Objeto do conhecimento: Propriedades da igualdade.

(7) Habilidade EF06MA29 (Grandezas e medidas): analisar e descrever mudanças no lado, no perímetro e na área de um quadrado, por meio da ampliação/redução.

Objeto do conhecimento: Perímetro de um quadrado como grandeza proporcional à medida do lado.

No 6º ano do Ensino Fundamental, os números inteiros são abordados a partir da história da matemática, tendo como referência o sistema de numeração decimal, os números primos, a divisão euclidiana, as principais operações aritméticas e a resolução de problemas que envolvem paridade, múltiplos e divisores.

⟹ 7º ano do Ensino Fundamental

(1) Habilidade EF07MA01 (Números): resolver e elaborar situações-problema envolvendo as noções de divisor e de múltiplo de um número natural, inclusive máximo divisor comum ou mínimo múltiplo comum, sem aplicar algoritmos.

Objeto do conhecimento: Múltiplos e divisores de um número natural.

(2) Habilidade EF07MA03 (Números): ler, comparar e ordenar números inteiros em diferentes contextos, associando-os a pontos da reta numérica.

Objeto do conhecimento: Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações.

(3) Habilidade EF07MA04 (Números): resolver e elaborar situações-problema acerca das operações com números inteiros.

Objeto do conhecimento: Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações.

(4) Habilidade EF07MA13 (Álgebra): compreender a ideia de variável, para expressar relação entre duas grandezas.

Objeto do conhecimento: Linguagem algébrica: variável e incógnita.

(5) Habilidade EF07MA14 (Álgebra): classificar sequências em recursivas e não recursivas.

Objeto do conhecimento: Linguagem algébrica: variável e incógnita.

(6) Habilidade EF07MA15 (Álgebra): utilizar a simbologia algébrica para identificar regularidades encontradas em sequências numéricas e representá-las.

Objeto do conhecimento: Linguagem algébrica: variável e incógnita.

(7) Habilidade EF07MA16 (Álgebra): reconhecer a equivalência ou não equivalência entre duas expressões algébricas que descrevem a regularidade de uma mesma sequência numérica.

Objeto do conhecimento: Equivalência de expressões algébricas: identificação da regularidade de uma sequência numérica.

No 7º ano do Ensino Fundamental, os números inteiros são abordados a partir da ideia de múltiplos e divisores, sendo, posteriormente, associados à reta numérica, remetendo à ideia de ordenação. Inclusive, introduzindo conceitos relacionados à linguagem algébrica, para classificar sequências numéricas e identificar regularidades nestas.

$\Longrightarrow$ 8º ano do Ensino Fundamental

(1) Habilidade EF08MA06 (Álgebra): resolver e elaborar situações-problema relacionadas ao cálculo do valor numérico de expressões algébricas, utilizando as propriedades das operações.

Objeto do conhecimento: Valor numérico de expressões algébricas.

(2) Habilidade EF08MA07 (Álgebra): associar equações lineares com duas incógnitas a uma reta no plano cartesiano.

Objeto do conhecimento: Associação de uma equação linear de 1º grau a uma reta no plano cartesiano.

(3) Habilidade EF08MA10 (Álgebra): identificar a regularidade de uma sequência numérica ou figural não recursiva, construindo um algoritmo capaz de indicar os números ou as figuras seguintes.

Objeto do conhecimento: Sequências recursivas e não recursivas.

(4) Habilidade EF08MA11 (Álgebra): identificar a regularidade de uma sequência numérica recursiva, construindo um algoritmo capaz de indicar os números seguintes.

Objeto do conhecimento: Sequências recursivas e não recursivas.

No 8º ano do Ensino Fundamental, os números inteiros são abordados a partir da ideia de classificar sequências numéricas e identificar regularidades nestas e, posteriormente, trabalha-se com o conceito de equações lineares de 1º grau, sua problematização e suas soluções em $\mathbb{Z}$ ou, particularmente, em $\mathbb{N}$.

$\Longrightarrow$ 9º ano do Ensino Fundamental

(1) Habilidade EF09MA09 (Álgebra): compreender os processos de fatoração de expressões algébricas, tendo, como base, as relações com os produtos notáveis.

Objeto do conhecimento: Expressões algébricas: fatoração e produtos notáveis; resolução de equações polinomiais do $2^{\underline{o}}$ grau por meio de fatorações.

(2) Habilidade EF09MA13 (Geometria): demonstrar relações métricas do triângulo retângulo, entre elas o teorema de Pitágoras, através de estratégias diversas, como a semelhança de triângulos.

Objeto do conhecimento: Relações métricas no triângulo retângulo; Teorema de Pitágoras: verificações experimentais e demonstração.

(3) Habilidade EF09MA14 (Geometria): resolver e elaborar situações-problema aplicando o Teorema de Pitágoras.

Objeto do conhecimento: Relações métricas no triângulo retângulo; Teorema de Pitágoras: verificações experimentais e demonstração.

No $9^{\underline{o}}$ ano do Ensino Fundamental, os números inteiros são abordados a partir dos processos de fatoração de expressões algébricas e, posteriormente, trabalha-se, no campo da Geometria, com as relações métricas no triângulo retângulo, usando, por exemplo, a semelhança de triângulos, para resolver problemas que tratam do Teorema de Pitágoras e suas implicações.

7.2 A IMPORTÂNCIA DA PRÁTICA PEDAGÓGICA

Conforme previsto pela Base Nacional Comum Curricular (BNCC), o Currículo Paulista de Matemática contém todas as habilidades a serem desenvolvidas ao longo do Ensino Fundamental divididas em Números, Álgebra, Geometria, Grandezas e Medidas, Probabilidade e Estatística. Ao que compete nosso estudo, tratamos somente das habilidades referentes a Números, Álgebra e Geometria. O foco principal é o estudo relacionado aos números inteiros não negativos, quanto à abordagem algébrica e algumas representações geométricas convenientes.

É de extrema importância que todas as habilidades mencionadas na seção anterior sejam desenvolvidas durante o processo de aprendizagem dos alunos, para que a introdução aos quadrados perfeitos e suas propriedades se dê de forma natural e coerente com a série e a idade dos alunos. Por exemplo, numa sala de $6^{\underline{o}}$ ano, é possível trabalhar álgebra e abstração, ao mesmo tempo em que se trabalha com a percepção visual sobre os números inteiros não negativos e, principalmente, a parte da geometria que trata da visualização de elementos e suas propriedades importantes.

Quando o docente inicia seu trabalho no Ensino Fundamental II, é importante que seja introduzido, abordado e desenvolvido um conjunto de ideias fundamentais. A primeira delas é a Equivalência. Nesta, surge a necessidade de utilizar alguns conceitos e definições relacionados a equações e áreas (como a do quadrado, que nos é relevante). A segunda delas é a Ordem, presente nos conjuntos numéricos, na construção de algoritmos e em outros procedimentos, como sequências e organização. Nesse caso, tem-se ainda a inclusão do raciocínio analógico, isto é, utilizar os mesmos mecanismos para resolver problemas de diferentes naturezas. A terceira delas é a Interdependência, que pode ser associada à ideia de funções com ou sem uso de fórmulas, como, por exemplo, em sentenças matemáticas do tipo "se p, então q". A quarta delas é a Representação, que diz respeito à percepção e representação do espaço, de formas geométricas existentes ou imaginadas; podendo, inclusive, ser associada aos números, às operações e à interdependência.

O objetivo do docente ao ensinar Números é desenvolver o pensamento numérico, o que envolve desenvolver conhecimentos sobre os números e suas relações, bem como a compreensão das operações e seus resultados, reconhecendo o significado ao operar com um número para obter outros. Essa parte da Matemática é iniciada a partir da ideia de contagem e, posteriormente, a introdução do Sistema de Numeração Decimal. É imprescindível levar o aluno a reconhecer as diversas funções sociais do número e, por isso, a importância do letramento matemático para o desenvolvimento de habilidades de leitura, da escrita e da ordenação. Exatamente por esse motivo, é também objetivo de ensinar Números valorizar o raciocínio intuitivo, e este deve ser desenvolvido desde a Educação Infantil até os Anos Finais, de forma a ter consolidado o cálculo numérico capaz de estabelecer a ordem de grandeza dos números, bem como desenvolver o raciocínio estruturado aditivo e o cálculo mental, tornando possível o desenvolvimento do raciocínio e processos, como a investigação e a capacidade de produzir argumentos convincentes. É importante que se recorra à história da Matemática, ao tratar desse assunto, pois proporciona-se uma abordagem significativa para o processo ensino/aprendizagem.

No que diz respeito ao ensino da Álgebra, destaca-se que ele deve estar pautado no desenvolvimento da capacidade de abstração e generalização, auxiliando na resolução de problemas. Com isso, ocorre a ampliação da capacidade de abstração e, como consequência, há grandes chances de ocorrerem "saltos" cognitivos no raciocínio matemático. Esse tipo de abordagem contribui para o processo de formação do pensamento algébrico, principalmente quanto aos processos mentais como analisar, estabelecer relações e comparações entre grandezas e quantidades, argumentar e explicar relações proporcionais e compreender relações multiplicativas. A isso tudo dá-se o nome de *raciocínio proporcional*, considerado uma das bases do pensamento algébrico. E quando o tema é retomado no Ensino Fundamental II, é de grande importância que os estudantes sejam capazes de compreender os diferentes significados das variáveis numéricas em uma expressão: estabelecer uma generalização de uma propriedade; investigar a regularidade de uma sequência numérica; indicar um valor desconhecido em uma sentença algébrica; estabelecer a variação entre duas grandezas. Para tanto, é necessário que os estudantes estabeleçam conexões entre incógnita e equação e variável e função.

Por fim, a Geometria é um campo importante da Matemática, servindo instrumento para outras áreas do conhecimento. Através dela, é possível haver a compreensão do mundo em que se vive, além de se desenvolver a capacidade de descrever, representar, localizar-se; estudar sua posição e deslocamentos; identificar formas e relações entre elementos de figuras planas e espaciais, desenvolvendo, assim, o pensamento geométrico. Durante o processo de desenvolvimento de habilidades, deve-se compreender a percepção espacial, principalmente a memória visual, a percepção de figuras planas e a discriminação visual. Por esse motivo, no Ensino Fundamental II, a Geometria deve ser vista como consolidação e ampliação das aprendizagens, de forma que os estudantes sejam capazes de identificar elementos em cada figura. Tudo isso contribui para a formação do raciocínio hipotético-dedutivo.

Com a consolidação de todos esses pré-requisitos, a abordagem que se dá aos números inteiros não negativos, de que trata o presente trabalho, torna-se um processo de aproximação entre os estudantes do Ensino Fundamental II, principalmente nas escolas da Rede Pública de Ensino, bem como se podem alcançar melhores resultados quando ocorre de maneira eficiente a abordagem dos pré-requisitos mencionados nesse capítulo.

7.3 PROPOSTA DIDÁTICA AO DOCENTE

Nesta seção, apresentaremos uma proposta didática que servirá de apoio ao docente que, em dado momento de sua prática de ensino, assim que julgar necessário, se dispuser a abordar todo o conteúdo desta dissertação. Para isso, traremos uma experiência vivenciada em sala de aula, numa turma de 8º ano do Ensino Fundamental, pelo próprio autor. A proposta se baseia em tópicos de Geometria, principalmente no que diz respeito à demonstração do Teorema de Pitágoras e suas implicações.

7.3.1 *Abordando o Teoremas de Pitágoras*

Uma das demonstrações para o Teorema de Pitágoras, usa simplesmente a reorganização de figuras poligonais [10, p.6].

$\Longrightarrow$ **Elaboração do plano de aula**

Objetivo geral da aula: levar o aluno a perceber que a Geometria é o campo matemático que mais permite a compreensão de algumas propriedades algébricas, como o Teorema de Pitágoras.

Objetivo específico da aula: levar o aluno a perceber que a área ocupada por um conjunto de polígonos não se altera conforme a disposição deles.

Tempo necessário: 4 (quatro) aulas.

Material necessário: 16 folhas de sulfite impressas, contendo um quadrado de lado medindo 17 cm, centralizado; 16 folhas de sulfite impressas, contendo quatro triângulos retângulos, ambos de catetos medindo 5 cm e 12 cm, cada; 8 tesouras sem ponta; 8 kits de lápis de cor; 8 tubos de cola branca ou em bastão.

$\Longrightarrow$ **Execução do plano de aula**

As duas primeiras aulas, por conveniência, devem ser ministradas no mesmo dia. Para essas aulas, faça o seguinte:

(1) Apresente os conceitos referentes à geometria necessários para a compreensão do tema a ser desenvolvido;

(2) Apresente alguns exemplos de que o Teorema de Pitágoras é uma relação válida para números naturais;

(3) Apresente uma demonstração algébrica do Teorema de Pitágoras, usando uma das duas versões apresentadas nesta dissertação;

(4) Proponha aos alunos que realizem tentativas para descobrirem outros três ternos pitagóricos, além dos já apresentados em sala.

Para as duas próximas aulas, faça o seguinte:

(1) Divida a turma em até 8 (oito) grupos de, no máximo, 5 alunos;

(2) Distribua, para cada grupo, o material necessário: 2 folhas de sulfite contendo o quadrado, 2 folhas de sulfite contendo os triângulos retângulos e 1 unidade de cada um dos outros materiais disponibilizados;

(3) Eleja um aluno para ser coordenar o grupo e os demais executarão as tarefas;

(4) Apresente em slide ou escreva na lousa as seguintes instruções:

Tarefa 1:

- Usando lápis de cor, na cor desejada, pintar dois desses triângulos retângulos de uma mesma cor e, usando uma outra cor, pintar os outros dois (repetir o mesmo processo para os triângulos contidos na outra folha de sulfite);

- Com o auxílio da tesoura, recortar cada um desses triângulos retângulos (repetir o mesmo processo para os triângulos contidos na outra folha de sulfite);

- Com o auxílio da régua, medir cada um dos lados de cada um dos triângulos retângulos e anote-os em seu caderno (repetir o mesmo processo para os triângulos contidos na outra folha de sulfite);

- Usando, como referência, o quadrado de 17 cm de lado, contido na folha de sulfite, dispor cada um desses triângulos, de modo que os catetos de cada triângulo retângulo sobreponha dois dos lados do quadrado de 17 cm e o ângulo reto (de 90°) de cada um desses triângulos deve coincidir com o ângulo reto do quadrado, conforme a figura a seguir.

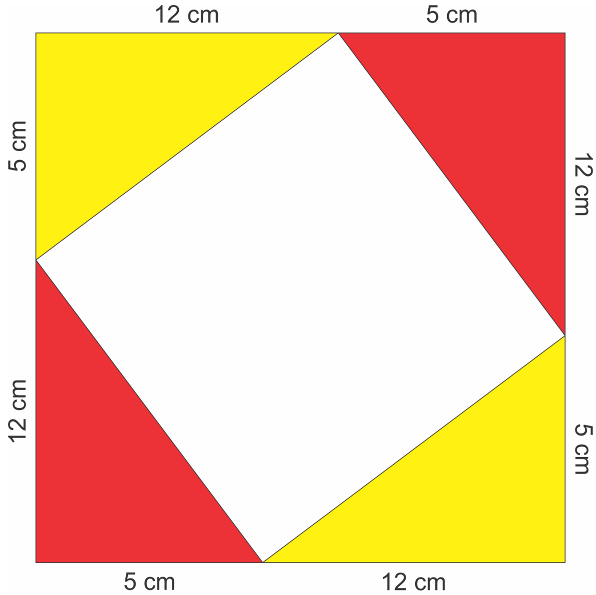

Figura 10. Teorema de Pitágoras (parte 1)

Convém ressaltar que, ao observarmos a disposição dos quatro triângulos retângulos na figura 10, temos um espaço vazio em torno deles. Como todas as medidas dos lados desses triângulos retângulos já foi devidamente mensurada pelos alunos, temos então a formação de um quadrado cujo lado mede 13 cm.

- Usando a cola disponível, aderir os triângulos retângulos à folha de sulfite.

Tarefa 2:

- Usando os outros quatro triângulos retângulos recortados, repetir todos os procedimentos da Tarefa 1, porém sem aderir os triângulos à folha de sulfite;

- Levar o triângulo da base (à esquerda) até o outro triângulo de mesma cor (localizado no topo à direita);

- Levar o triângulo do topo (à esquerda) até a base, sem deslocá-lo horizontalmente nem girá-lo;

- Levar o triângulo da base (à direita) até o triângulo que se encontra na base (à esquerda), sem deslocá-lo verticalmente nem girá-lo.

Observe a figura a seguir.

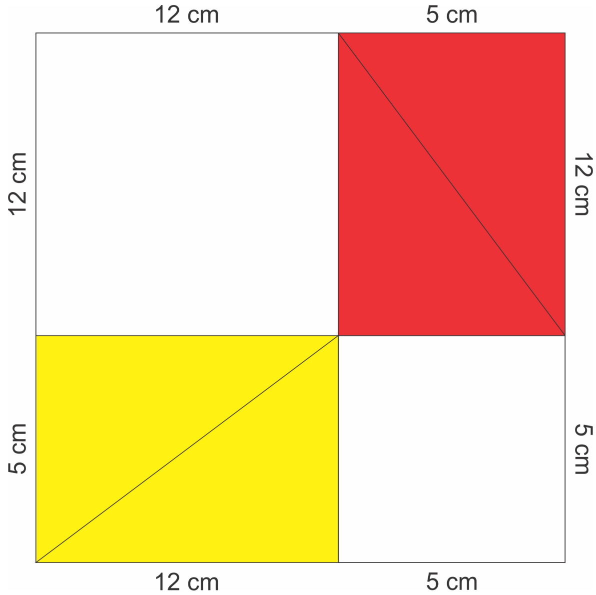

Figura 11. Teorema de Pitágoras (parte 2)

Convém ressaltar que, ao observarmos a disposição dos quatro triângulos retângulos na figura 11, temos um espaço vazio ao redor deles. Como todas as medidas dos lados desses triângulos retângulos já foi devidamente mensurada pelos alunos, temos então a formação de dois quadrados cujos lados medem, respectivamente, 5 cm e 12 cm.

(5) Solicite aos alunos que, durante 5 (cinco) minutos, discutam entre os membros de seus respectivos grupos sobre as tarefas que acabaram de realizar e o que é possível concluir, através das observações quanto às duas figuras assim formadas;
(6) Ao fim dos cinco minutos, solicite que cada representante exponha para a turma as conclusões a que chegaram durante a discussão.

É importante ressaltar que o objetivo específico dessas duas primeiras aulas é que os alunos tenham percebido que, como os quatro triângulos retângulos são congruentes entre si e que, quando dispostos dentro do quadrado de 17 cm de lado, eles ocupem juntos a mesma área, não importando a disposição deles. Assim, torna-se possível cumprir o objetivo geral: demonstrar geometricamente o Teorema de Pitágoras.

7.3.2 *Descobrindo ternas pitagóricas primitivas*

Esse tema já foi abordado no Capítulo 2 desta dissertação. Convém ressaltar que há dois métodos para encontrarmos ternas pitagóricas primitivas: o primeiro é atribuído a Platão e o segundo, a Pitágoras. Essa proposta encontra-se disponível no Caderno do Aluno, do São Paulo Faz Escola, de 2019, volume único.

$\Longrightarrow$ **Elaboração do plano de aula**

Objetivo geral da aula: levar o aluno a perceber que as ternas pitagóricas primitivas podem ser obtidas por meio de um algoritmo.

Objetivo específico da aula: levar o aluno a perceber que existem infinitas ternas pitagóricas, primitivas ou não.

Tempo necessário: 2 (duas) aulas.

Material necessário: caneta esferográfica azul ou preta; lápis; borracha; apontador.

$\Longrightarrow$ **Execução do plano de aula**

Essas duas aulas, por conveniência, devem ser ministradas no mesmo dia. Para essas aulas, faça o seguinte:

(1) Apresente, como referência, a terna primitiva **3, 4 e 5** e solicite aos alunos que verifiquem que $3^2 + 4^2 = 5^2$;

(2) Solicite aos alunos que multipliquem por um mesmo número natural cada uma dessas medidas e verifiquem se a igualdade permanece (por exemplo: $(3 \cdot 2)^2 + (4 \cdot 2)^2$ é igual a $(5 \cdot 2)^2$?);

(3) Apresente o primeiro método atribuído a Platão sobre como determinar ternas pitagóricas, descrevendo passo a passo, conforme a seguir:

- Escolha um número ímpar;

- Calcule o quadrado desse número ímpar;

- Subtraia 1 unidade ao quadrado obtido e calcule a metade;

- Some 1 unidade ao quadrado obtido e calcule a metade;

- Anote os três números na mesma ordem em que eles foram obtidos e calcule o quadrado de cada um deles;

- Responda: *A soma dos dois primeiros quadrados é igual ao terceiro quadrado?*

(4) Apresente o segundo método atribuído a Platão sobre como determinar ternas pitagóricas, descrevendo passo a passo, conforme a seguir:

- Escolha um número par;

- Divida-o por 4;

- Subtraia 1 unidade do resultado obtido no 2º passo;

- Some 1 unidade ao resultado obtido no 2º passo;

- Anote os três números na mesma ordem em que eles foram obtidos e calcule o quadrado de cada um deles;

- Responda: *A soma dos dois primeiros quadrados é igual ao terceiro quadrado?*

(5) Proponha aos alunos que realizem, durante 20 minutos, tentativas para descobrirem outros quatro ternos pitagóricos, para cada um dos dois métodos atribuídos a Platão, além dos já apresentados em sala.

(6) Ao fim dos 20 minutos, solicite aos alunos que, voluntariamente, escrevam na lousa uma das ternas pitagóricas que conseguiram obter usando os procedimentos fornecidos.

É importante ressaltar que o objetivo específico dessas duas aulas é que os alunos tenham percebido que existem infinitas ternas pitagóricas, primitivas ou não. Assim, torna-se possível cumprir o objetivo geral: perceber que as ternas pitagóricas primitivas podem ser obtidas por meio de um conjunto de instruções, o qual denominamos *algoritmo*.

8 CONSIDERAÇÕES FINAIS

O presente estudo possibilitou uma investigação a respeito dos números quadrados perfeitos, desde a origem do termo e as primeiras utilizações práticas até os conceitos mais atuais acerca da Aritmética Modular e as propriedades inerentes ao tema. O que possibilitou identificarmos alguns fatos curiosos sobre os quadrados perfeitos:

(1) Um quadrado perfeito de ordem n é a soma de dois números triangulares, o primeiro de ordem n e o segundo de ordem $n-1$;

(2) Existem quadrados perfeitos que podem ser escritos como soma de outros dois quadrados perfeitos (ternos pitagóricos) e é possível calcularmos infinitos ternos pitagóricos;

(3) Um quadrado perfeito ímpar sempre deixa resto 1 na divisão por 8;

(4) É possível obtermos o quadrado de um dado número natural utilizando apenas de seus algarismos;

(5) O mdc entre dois ou mais quadrados perfeitos é sempre um quadrado perfeito;

(6) Através do Pequeno Teorema de Fermat, é possível mostrarmos que existem infinitos quadrados perfeitos que deixam resto 1 na divisão por um primo ímpar, desde que este seja coprimo com a base;

(7) Se uma PA infinita possui um termo que é um quadrado perfeito, então essa PA possui infinitos quadrados perfeitos;

(8) É possível escrevermos qualquer número natural como soma de quatro quadrados perfeitos.

Além disso, essas investigações tornaram possível identificarmos algumas aplicações para os quadrados perfeitos. Especialmente, no que diz respeito à geometria plana – onde tudo começou – e ao ramo da álgebra, principalmente no uso das fórmulas de recorrência (no caso da soma dos n primeiros ímpares e do número triangular de ordem n) e na demonstração de proposições que tornam ainda mais interessante a abordagem didática no estudo dos números inteiros, em especial os números primos.

Com esse estudo, pretendemos incentivar professores de Matemática (especialmente da Rede Pública de Ensino) a aprimorarem seus conhecimentos sobre tópicos em Números, Álgebra e Geometria, de forma a tornarem mais precisas e concisas as aplicações do tema, durante suas aulas no Ensino Fundamental II, sendo de extrema importância a abordagem significativa de cada um dos pré-requisitos para o estudo tratado no presente projeto. Com isso, aumentar a percepção do aluno com relação aos números inteiros, no que diz respeito às suas propriedades, principalmente relacionadas aos números primos e aos quadrados perfeitos.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Currículo Paulista. São Paulo, (2019), disponível em https://efape.educacao.sp.gov.br/curriculopaulista/wp-content/uploads/sites/7/2019/09/curriculo-paulista-26-07.pdf

[2] FILHO, Inocêncio Fernandes Balieiro. As Ternas Pitagóricas e os Números Congruentes: Uma breve História, México, (2015), disponível em: http://xiv.ciaem-redumate.org/index.php/xiv_ciaem/xiv_ciaem/paper/viewFile/159/106

[3] HEFEZ, Abramo, Aritmética, 1 ed., Rio de Janeiro: SBM, (2013).

[4] HEFEZ, Abramo. Indução Matemática. Apostila OBMEP (2009), disponível em http://www.obmep.org.br/docs/apostila4.pdf

[5] MARTINEZ, Fabio Brochero; MOREIRA, Carlos Gustavo; SALDANHA, Nicolau; TENGAN, Eduardo, Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro, 2 ed., Rio de Janeiro, IMPA, (2013).

[6] MORGADO, Augusto César. CARVALHO, Paulo Cezar Pinto. Matemática Discreta. Coleção Prof-mat, 2 ed., 2013.

[7] PÉTIN, P., Tópicos de História da Matemática através de Problemas, disponível em http://www.professores.uff.br/marco/wp-content/uploads/sites/37/2017/08/Pierre-1.pdf

[8] PITOMBEIRA, J. B.; ROQUE, T., Tópicos de História da Matemática, SBM, Coleção PROFMAT, (2012).

[9] SANTOS, José Plínio de Oliveira, Introdução à Teoria dos Números, 3 ed. IMPA, (2011).

[10] WAGNER, Eduardo. Teorema de Pitágoras e Áreas, Rio de Janeiro, (2010), disponível em http://www.obmep.org.br/docs/apostila3.pdf