UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

UMA ABORDAGEM PARA A DIFUSÃO DAS EQUAÇÕES DIOFANTINAS LINEARES E QUADRÁTICAS

FELIPE ARANTE MATOS

MANAUS
2019

UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

FELIPE ARANTE MATOS

UMA ABORDAGEM PARA A DIFUSÃO DAS EQUAÇÕES DIOFANTINAS LINEARES E QUADRÁTICAS

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Nilomar Vieira de Oliveira

MANAUS
2019

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Matos, Felipe Arante
M433u Uma Abordagem Para a Difusão das Equações Diofantinas Lineares e Quadráticas / Felipe Arante Matos. 2019
114 f.: il.; 31 cm.

Orientador: Nilomar Vieira de Oliveira
Tese (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Amazonas.

1. Teoria dos Números. 2. Equações Diofantinas Lineares. 3. Frações Contínuas. 4. Ternas Pitagóricas. 5. Equação de Pell. I. Oliveira, Nilomar Vieira de II. Universidade Federal do Amazonas III. Título

FELIPE ARANTE MATOS

UMA ABORDAGEM PARA A DIFUSÃO DAS EQUAÇÕES DIOFANTINAS LINEARES E QUADRÁTICAS

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em 22 de abril de 2019.

BANCA EXAMINADORA

Prof. Dr. Nilomar Vieira de Oliveira
Presidente

Prof. Dr. Roberto Antonio Cordeiro Prata
Membro Interno

Prof. Dr. Alcides de Castro Amorim Neto
Membro Externo

AGRADECIMENTOS

Primeiramente a DEUS, por me conceder a oportunidade de realizar um sonho e estar comigo nos momentos mais difíceis desta caminhada operando as suas maravilhas.

Aos meus pais, dona MARIA DA CONCEIÇÃO ARANTE MATOS e seu FRANCISCO PEREIRA MATOS, por me darem tanto amor, me ensinar o caminho da verdade, desde cedo me mostrarem a importância dos estudos e se esforçarem para me dar o melhor, para que eu pudesse hoje estar concluindo mais essa etapa de conhecimento na minha vida.

À minha esposa, DULCINEIA NOGUEIRA OLERIANO que esteve ao meu lado me dando força nos momentos mais difíceis no qual pensei que não ia mais conseguir. Provérbios 3: 15 Mais preciosa é do que as joias, e nada do que possas desejar é comparável a ela.

À minha gestora, NELISSANDRA DE SOUZA GURGEL que nesses anos com o seu grande coração tem perdoado as minhas falhas, que DEUS lhe abençoe cada dia mais e realize os seus sonhos.

Ao meu amigo DUARTE RAMOS RABELO que por diversas vezes me deu suporte na conquista desse sonho.

Ao meu orientador Prof. Dr. NILOMAR VIEIRA DE OLIVEIRA, por acreditar em mim, mesmo sem me conhecer, pela liberdade e ajuda referente ao tema, pela preocupação e atenção em relação ao desenvolvimento do trabalho.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, pelos 02 (dois) anos de bolsa de estudos.

Aos meus amigos guerreiros que conseguiram chegar a reta final, que me ajudaram diretamente e indiretamente: ANDERSON BRAZ DE SANTANA, ANSELMO LUÍS CORREA DA SILVA, ARTUR SILVA LOPES (TALUDINHO), CARLOS ADALTO SEIXAS PANTOJA, CHAYSE PINHEIRO TEIXEIRA, DANIEL SOMBRA DA SILVA FILHO (GUGU), EVERTON DE ARAÚJO MORAES (URSÃO), GUTEMBERG LEÃO BRASIL, HERMÍNIO EDSON MAIA SANTANA (PERSONAL), LUCAS DA COSTA ARAÚJO, LUZELY COELHO RIBEIRO (VOVÔ), MANOELA FRANCO DA SILVA, MARCELO LUIZ LOPES ROCHA, MARIA VALDEIDA DO VALE CUNHA, MARIO ANDRÉ NUNES RODRIGUES (CAM-

BOTINHA), NILTON MIGUEL DA SILVA (ÁGUIA CANSADA), ROSILEI CARDOSO MOREIRA (MATRIARCA), VALCINEIDE DOS SANTOS MALTA (PATRICINHA).

RESUMO

O presente trabalho tem como objetivo geral proporcionar um material de apoio aos discentes e docentes de todos os níveis do ensino da matemática sobre as equações diofantinas lineares e quadráticas. Essas informações são apresentadas de forma clara, de modo que todos que necessitem deste conhecimento, possam entender com facilidade o que está sendo exposto em vez de apenas memorizar o que está escrito. Desta forma temos como objetivo específico reforçar o entendimento da teoria abordada, através da resolução dos problemas retirados de: olimpíadas matemáticas, revista de treinamento olímpicos e vestibulares. Assim, os docentes/discentes que necessitem do conhecimento exposto fiquem com a mente mais esclarecida abrindo um leque para o entendimento de outros temas da teoria dos números que possuem como base o que foi apresentado. No desenvolvimento deste trabalho, cujos capítulos principais são: Conceitos básicos da Teoria dos Números, Equações Diofantinas Lineares e Quadráticas, destacamos a beleza das demonstrações com todos os argumentos necessários/suficiente com a preocupação de que não ficasse nada nas entrelinhas. Por fim, esperamos que este material seja de grande ajuda para todo publico que necessite de uma linguagem mais acessível dos tópicos abordados.

Palavras-chave: Teoria dos Números, Equações Diofantinas Lineares, Frações Contínuas, Ternas Pitagóricas, Equação de Pell.

ABSTRACT

This present work has as general objective to provide a material support to students and teachers of all levels of teaching Mathematics about linear and quadratic Diophantine equations. these informations are exposed in a clearly way so that all public who needs this knoledge can understand easily what is exposed instead of just memorizy what is written. In this way, we have as specific objective reinforce the understanding about the theory presented through the resolution of the problems taken from: Olympic math, Olympic training magazine, entrance exams. Therefore students and students will understand easily another themes about the theory of numbers that are based on what was presented. In the development of this work, whose chapters are: basic concepts of number theory, linear and quadratic Diophantine equations, we highlight the beauty of the demonstration with all demonstrations in other to understand everything. Finally, we hope this material will be useful and help people who needs a more acessible language about the topics covered.

Keywords: Number Theory, Linear Diophantine Equations, Continuous Fractions, Pythagorean Thirds, Pell Equation.

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{Q}$	Conjunto dos números racionais.
$\mathbb{I}$	Conjunto dos números irracionais.
$\mathbb{R}$	Conjunto dos números reais.
P	Conjunto dos números reais positivos.
$\|x\|$	Valor absoluto de x.
$=$	Igual.
$\neq$	Diferente.
$>$	Maior.
$<$	Menor.
$\geq$	Maior ou igual.
$\leq$	Menor ou igual.
■	Indica o fim de uma demonstração.

Sumário

Introdução

Neste trabalho apresentaremos uma revisão bibliográfico-literária no qual tem como tema principal as equações diofantinas, onde as classificamos em equações diofantinas de primeira ordem (lineares) e equações diofantinas de segunda ordem (quadráticas) tendo como objetivo geral a transcrição do tema de forma clara e sucinta, de tal modo que todo público que necessite deste conhecimento, consiga entender com facilidade o que está sendo exposto em vez de apenas memorizar o que está sendo escrito. Desta forma temos como objetivo específico que através da resolução dos problemas retirados de: olimpíadas matemáticas, revista de treinamento olímpico, exame nacional do ensino médio e vestibulares reforcem o entendimento da teoria abordada e os docentes/discentes que necessitam do conhecimento exposto fiquem com a mente mais esclarecida abrindo um leque para o entendimento de outros temas da teoria dos números que possuem como base o que foi apresentado.

Subdividimos este trabalho da seguinte maneira: introdução, conceitos básicos da teoria dos números, equações diofantinas lineares, equações diofantinas quadráticas e conclusão.

No primeiro capítulo, no qual é o texto base, onde denominamos de "conceitos básicos da teoria dos números" adicionamos os seguintes tópicos: números inteiros, divisibilidade, MDC, MMC, números primos e congruência. Onde demonstramos alguns teoremas famosos como (algoritmo da divisão de Euclides, teorema das divisões sucessivas de Euclides, Lema de Gauss, relação de Bezout) e outras mais.

No segundo capítulo falamos sobre as equações diofantinas lineares, no qual foi distribuída nos seguintes tópicos: equações diofantinas com duas variáveis, equações diofantinas com três variáveis e equações diofantinas com n variáveis. Onde em todos os tópicos demonstramos como achar a solução particular e a solução geral das devidas equações.

No terceiro capítulo falamos sobre algumas equações diofantinas quadráticas que são elas distribuídas nos seguintes tópicos: frações contínuas, ternas pitagóricas e equação de Pell. Onde demonstramos enumeras proposições, no qual podemos destacar uma proposição muito importante no cálculo conhecida como (lema de Dirichelet).

Nos capítulos um, dois e três inserimos alguns exemplos de aplicação, que também é um dos objetivos deste trabalho.

Capítulo 1

Conceitos Básicos da Teoria dos Números

Neste capítulo estudaremos os tópicos que nos darão subsídios para o desenvolvimento e compreensão do tema central deste trabalho que é as equações diofantinas. Ao escrevê-lo, visamos não apenas explaná-lo como referencial teórico do tema abordado, e sim, como uma via de intercâmbio de vários temas da teoria dos números. De tal forma, que nas demonstrações dos resultados apresentados, não deixamos de lado o rigor matemático exigido, porém procuramos explicitar os argumentos o máximo possível, com o objetivo que todo público que precise dos conhecimentos abordados nos tópicos não fique com nenhuma dúvida ou bloqueio de entendimento.

1.1 Números inteiros

Selecionamos este tópico para compor o texto base, pois temos como central deste trabalho que o seu conjunto solução esteja contido no conjunto dos números inteiros, que representamos pelo símbolo $\mathbb{Z}$.

Consideraremos as seguintes propriedades abaixo como axiomas dos números inteiros, ou seja, assumiremos tais propriedades como noções primitivas, as quais não precisamos demonstrá-las.

1) A adição e a multiplicação são *bem definidas*:

   Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

2) A adição e a multiplicação são *comutativas*:

   Para todos $a, b \in \mathbb{Z}, a + b = b + a$ e $a \cdot b = b \cdot a$.

3) A adição e a multiplicação são *associativas*:

   Para todos $a, b, c \in \mathbb{Z}, (a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

4) A adição e a multiplicação possuem *elementos neutros*:

   Para todo $a \in \mathbb{Z}, a + 0 = a$ e $a \cdot 1 = a$.

5) A adição possui *elementos simétricos*:

   Para todo $a \in \mathbb{Z}$, existe $b(= -a)$ tal que $a + b = 0$.

6) A multiplicação é *distributiva* com relação à adição:

   Para todos $a, b, c \in \mathbb{Z}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$.

7) *Fechamento* de $\mathbb{N}$: O conjunto $\mathbb{N}$ é fechado para a adição e para a multiplicação, ou seja, para todos $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $ab \in \mathbb{N}$.

8) *Tricotomia*: Dados $a, b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

   $i)$ $a = b$;

   $ii)$ $b - a \in \mathbb{N}$;

   $iii)$ $-(b - a) = a - b \in \mathbb{N}$.

9) *Princípio da Boa Ordenação*: Se *S* é um subconjunto não-vazio de $\mathbb{Z}$ e limitado inferiormente, então *S* possui um menor elemento.

10) *Princípio da Indução Finita*: Seja B um conjunto dos inteiros positivos. Se B possui as duas seguintes propriedades:

    $i)$ $1 \in B$;

    $ii)$ $k + 1 \in B$ sempre que $1, 2, \ldots, k \in B$.

    então B contém todos os inteiros positivos.

1.2 Divisibilidade

Neste tópico mostraremos que a divisão de um número inteiro por outro número inteiro nem sempre é possível, expressamos essa possibilidade através da relação de divisibilidade. Porém quando não existe uma relação de divisibilidade entre dois inteiros, veremos que ainda assim, será possível efetuar uma "divisão com resto pequeno", chamada de **Divisão Euclidiana**. O fato de sempre ser possível efetuar tal divisão é responsável por inúmeras propriedades dos inteiros que exploraremos neste trabalho.

Definição 1.1. *Dados dois números inteiros a e b, diremos que a divide b, denotaremos como $a \mid b$, quando existir um $k \in \mathbb{Z}$ tal que $b = k \cdot a$. Nesse caso, poderemos dizer também que a é um **divisor** ou um **fator** de b ou ainda que b é um **múltiplo** de a ou que b é **divisível** por a.*

Observe que a notação $a \mid b$ não representa nenhuma operação em $\mathbb{Z}$, tão pouco uma fração. Trata-se de uma sentença que diz ser verdade que existe k inteiro tal que $b = k \cdot a$. A negação dessa sentença representaremos por $a \nmid b$, significando que não existe nenhum número inteiro k tal que $b = k \cdot a$.

Exemplo 1.1. *É fácil verificar pela definição que:*

a) $2 \mid 6$, *pois* $6 = 3 \cdot 2$*;*

b) $-3 \mid 9$, *pois* $9 = 3 \cdot (-3)$*;*

c) $7 \mid 56$, *pois* $56 = 8 \cdot 7$.

Proposição 1.1. *Sejam* $a, b, c \in \mathbb{Z}$*. Tem-se que*

$i)$ $1|a$, $a|a$ *e* $a|0$.

$ii)$ $0|a \iff a = 0$.

$iii)$ a *divide* b *se, e somente se,* $|a|$ *divide* $|b|$.

$iv)$ *se* $a|b$ *e* $b|c$, *então* $a|c$.

Demonstração:

$i)$ Tal demonstração decorre direto da aplicação da definição, pois sabemos que:

- a pode ser escrito como $a = a \cdot 1$, por definição temos que $1|a$
- a também pode ser escrito como $a = 1 \cdot a$, pois o produto é comutativo, logo $a|a$ por definição.
- por último, 0 (zero) pode ser escrito como $0 = 0 \cdot a$, logo $a|0$ por definição.

$ii)$ Toda vez que temos um, se somente se, temos que supor que uma das sentenças é verdadeira, com isso iremos supor que $0|a$; logo existe um $k \in \mathbb{Z}$, tal que $a = k \cdot 0$. Com isso concluímos que $a = 0$. Para a recíproca basta observar que $0 \mid 0$, pelo que foi provado no caso anterior $a \mid a$

$iii)$ $a \mid b \Leftrightarrow b = k \cdot a, k \in \mathbb{Z} \Rightarrow |b| = |k \cdot a| \Rightarrow |b| = |k| \cdot |a| \Rightarrow |a| \mid |b|$.

$iv)$ Segue da definição de divisibilidade que

Se $a|b$, $b = k_1 \cdot a$ onde $k_1 \in \mathbb{Z}$.

Se $b|c$, $c = k_2 \cdot b$ onde $k_2 \in \mathbb{Z}$.

Substituindo o valor de b em c, temos:

$c = k_2 \cdot b \Longrightarrow c = k_2 \cdot k_1 \cdot a$, como $k_2 \cdot k_1 = k \in \mathbb{Z}$, de onde segue que $c = k \cdot a$, logo $a|c$.

■

Proposição 1.2. *Se* $a, b, c, d \in \mathbb{Z}$*, então:*

$$a \mid b \quad \textit{e} \quad c \mid d \qquad \Longrightarrow \qquad a \cdot c \mid b \cdot d$$

Demonstração:

Se $a|b$, por definição temos $b = k_1 \cdot a$ onde $k_1 \in \mathbb{Z}$.

Se $c|d$, por definição temos $d = k_2 \cdot c$, onde $k_2 \in \mathbb{Z}$.

$$\begin{cases} b = k_1 \cdot a \\ d = k_2 \cdot c \end{cases} \Longrightarrow \text{ fazendo o produto membro a membro temos:}$$

$b \cdot d = k_1 \cdot k_2 \cdot a \cdot c$, como $k_1 \cdot k_2 = k \in \mathbb{Z}$, $b \cdot d = k \cdot a \cdot c$, e portanto,

$$a \cdot c \mid b \cdot d$$

■

Exemplo 1.2. $3 \mid 9 \quad \textit{e} \quad 4 \mid 8$*, pela proposição acima* $3 \cdot 4 \mid 9 \cdot 8$*, que é verdade pois* $12 \mid 72$.

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

$$a|b \Longleftrightarrow a|c.$$

Demonstração:

($\Longrightarrow$)

Suponhamos que $a|b+c$, por definição temos que; $b+c = k_1 \cdot a$, onde $k_1 \in \mathbb{Z}$. (I)

Agora se $a|b$, por definição temos que $b = k_2 \cdot a$, onde $k_2 \in \mathbb{Z}$. (II)

Substituindo (II) em (I), temos:

$b + c = k_1 \cdot a \Rightarrow (k_2 \cdot a) + c = k_1 \cdot a \Rightarrow c = k_1 \cdot a - k_2 \cdot a \Rightarrow c = (k_1 - k_2) \cdot a$, como $(k_1 - k_2)$ é igual a um inteiro k, substituindo temos $c = k \cdot a$, logo por definição $a|c$.

($\Longleftarrow$)

Reciprocamente, como no caso anterior, suponhamos que $a|b + c$, por definição temos que: $b+c = k_1 \cdot a$ onde $k_1 \in \mathbb{Z}$. (III)

Agora se $a|c$, por definição temos que $c = k_2 \cdot a$ onde $k_2 \in \mathbb{Z}$. (IV)

Substituindo (IV) em (III), temos:

$b + c = k_1 \cdot a \Rightarrow b + k_2 \cdot a = k_1 \cdot a \Rightarrow b = k_1 \cdot a - k_2 \cdot a \Rightarrow b = (k_1 - k_2) \cdot a$, como $(k_1 - k_2)$ é igual a um inteiro k, temos que $b = k \cdot a$, logo por definição temos que $a|b$.

A diferença, faremos com um pouco menos de explicação por se tratar de uma repetição do que foi feito anteriormente.

($\Longrightarrow$)

Suponhamos que $a|b-c \Rightarrow b-c = k_1 \cdot a$, onde $k_1 \in \mathbb{Z}$, (V)

Agora se $a|b \Rightarrow b = k_2 \cdot a$, (VI)

Substituindo (VI) em (V), temos:

$b-c = k_1 \cdot a \Rightarrow (k_2 \cdot a) - c = k_1 \cdot a \Rightarrow -c = k_1 \cdot a - k_2 \cdot a \Rightarrow c = -k_1 \cdot a + k_2 \cdot a \Rightarrow c = (-k_2 + k_1) \cdot a$, como $(-k_2 + k_1) = k \in \mathbb{Z}$, temos que $c = k \cdot a$, logo $a|c$.

($\Longleftarrow$)

Reciprocamente, suponhamos que $a|b-c \Rightarrow b-c = k_1 \cdot a$, onde $k_1 \in \mathbb{Z}$. (VII)

Agora se $a|c \Rightarrow c = k_2 \cdot a$, onde $k_2 \in \mathbb{Z}$. (VIII)

Substituindo (VIII) em (VII), temos:

$b-c = k_1 \cdot a \Rightarrow b - (k_2 \cdot a) = k_1 \cdot a \Rightarrow b = k_1 \cdot a + k_2 \cdot a \Rightarrow b = (k_1 + k_2) \cdot a$, como $(k_1 + k_2) = k \in \mathbb{Z}$, temos que $b = k \cdot a$, por definição $a|b$.

■

Exemplo 1.3.

a) $3|6 \pm 9 \Longrightarrow 3|6 \Longleftrightarrow 3|9$*;*

b) $5|10 \pm 30 \Longrightarrow 5|10 \Longleftrightarrow 5|30$.

Proposição 1.4. *Dados a, b, c inteiros não nulos, temos que:*

$$a|b \Rightarrow a|b \cdot c$$

Demonstração:

Se $a|b$, por definição temos que $b = k_1 \cdot a$, com $k_1 \in \mathbb{Z}$. (I)

Multiplicando ambos os membros da equação (I) por c, temos:

$b = k_1 \cdot a \Rightarrow b \cdot c = k_1 \cdot a \cdot c \Rightarrow b \cdot c = k_1 \cdot c \cdot a$, como $k_1 \cdot c$ é igual a um inteiro k, temos: $b \cdot c = k \cdot a$, logo $a|b \cdot c$.

O que demonstramos nessa proposição é que se $a|b$, a divide qualquer múltiplo de $b \in \mathbb{Z}$.

■

Exemplo 1.4.

a) $6|12$ *e* $6|12 \cdot 3 = 36$*;*

b) $4|16$ *e* $4|16 \cdot 5 = 80$.

Proposição 1.5. *Dados a, b, c inteiros não nulos, temos que:*

$$a|b \Rightarrow a \cdot c|b \cdot c$$

Demonstração:

Se $a|b$ por definição temos que $b = k_1 \cdot a$, com $k_1 \in \mathbb{Z}$. (I)

Multiplicando ambos os membros da equação (I) por c, temos:

$$b = k_1 \cdot a \Rightarrow b \cdot c = k_1 \cdot a \cdot c \Rightarrow a \cdot c | b \cdot c$$

■

Exemplo 1.5.

a) $6|12 \Longrightarrow 6 \cdot 3|12 \cdot 3$ *ou* $18|36$*;*

b) $7|14 \Longrightarrow 7 \cdot 4|14 \cdot 4$ *ou* $28|56$.

Proposição 1.6. *Se* $a, b, c \in \mathbb{Z}$ *tais que* $a|b$ *e* $a|c$*, então para todo* $x, y \in \mathbb{Z}$

$$a|(xb + yc).$$

Demonstração:

Se $a|b$, temos por definição que $b = k_1 \cdot a$, onde $k_1 \in \mathbb{Z}$. (I)

Se $a|c$ temos por definição que $c = k_2 \cdot a$, onde $k_2 \in \mathbb{Z}$. (II)

Chamaremos os múltiplos de b, somado com os múltiplos de c, de $(xb + yc)$. (III)

Substituindo os valores de (I) e (II) em (III), temos:

$xb + yc = x\ (k_1 \cdot a) + y\ (k_2 \cdot a) = x \cdot k_1 \cdot a + y \cdot k_2 \cdot a = [x \cdot k_1 + y \cdot k_2] \cdot a$, como $[x \cdot k_1 + y \cdot k_2]$, é igual a um inteiro k, obtemos o seguinte:

$$xb + yc = k \cdot a, \text{ logo } a|(xb + yc).$$

■

Exemplo 1.6.

a) $2|4$ *e* $2|6 \Longrightarrow 2|4 \cdot 3 + 6 \cdot 7 = 54$*;*

b) $4|8$ *e* $4|16 \Longrightarrow 4|8 \cdot 6 + 16 \cdot 6 = 144$.

Proposição 1.7. *Dados* $a, b \in \mathbb{Z}$*, onde* $b \neq 0$*, temos que*

$$a|b \Rightarrow |a| \leq |b|.$$

Demonstração:

Usaremos a hipótese de que $a|b$ para provar que $|a| \leq |b|$.

De fato, se $a|b$, por definição temos que $b = k_1 \cdot a$, onde $k_1 \in \mathbb{Z}$. Tomando módulos em b, temos: $|b| = |k_1| \cdot |a|$, como $b \neq 0$, por consequência, temos que $k_1 \neq 0$, logo $|k_1| \geq 1$ e, consequentemente, pela desigualdade triangular, $|a| \leq |k_1| \cdot |a| = |b|$, logo $|a| \leq |b|$.

■

Proposição 1.8. *Sejam $a, b \in \mathbb{Z}$, se $a|b$ e $b|a$, então $|a| = |b|$*

Demonstração:

Temos duas possibilidades:

i) Para $a = 0$: suponhamos que $a = 0$. Como $a \mid b$, ou seja $0 \mid b$, pela Proposição 1.1, item (ii), devemos ter $b = 0$, logo $|a| = 0 = |b|$.

ii) Para $a \neq 0$: Suponhamos que $a \neq 0$. Como $a \mid b$, implica que $b \neq 0$. Assim, pela proposição 1.7, se $a \mid b$ temos que $|a| \leq |b|$ e se $b \mid a$ temos que $|b| \leq |a|$, o que implica $|a| = |b|$. ■

Proposição 1.9. *Dados $a, b \in \mathbb{Z}$, se $a|b$ e $a \neq 0$, então $\frac{b}{a} \mid b$*

Demonstração:

Se $a|b$, por definição temos que $b = k_1 \cdot a$, onde $k_1 \in \mathbb{Z}$ e por consequência $\frac{b}{a} \in \mathbb{Z}$. Como $\frac{b}{a} \cdot a = b$, logo $\frac{b}{a}|b$.

■

Exemplo 1.7.

a) $2|6 \implies \frac{6}{2}|6$ *ou* $3|6$*;*

b) $3|81 \implies \frac{81}{3}|81$ *ou* $27|81$.

Proposição 1.10. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b$ divide $a^n - b^n$*

$$(a - b) \mid (a^n - b^n)$$

Demonstração:

Iremos provar por indução sobre n.

$i)$ Caso base: Para $n = 1$

$a^1 - b^1 = a - b$, logo para $n = 1$, a afirmação é verdadeira pois $(a - b) \mid (a^1 - b^1)$

$ii)$ Hipótese de indução: Suponhamos, agora que $(a - b) \mid (a^n - b^n)$, $\forall\, n \in \mathbb{N}$.

$iii)$ Tese: Queremos demonstrar que $(a-b) \mid (a^{n+1}-b^{n+1})$. Temos:

$$\begin{aligned} a^{n+1}-b^{n+1} &= a^n \cdot a - b^n \cdot b + \ (-b \cdot a^n + b \cdot a^n) \\ &= a^n \cdot a - b \cdot a^n - b^n \cdot b + b \cdot a^n \\ &= a^n \ (a-b) + b \cdot (a^n - b^n) \end{aligned}$$

Como $a-b|a-b$ pelo caso base e, por hipótese de indução $a-b|a^n-b^n$, decorre da igualdade acima e da Proposição 1.6 que $(a-b) \mid (a^{n+1}-b^{n+1})$ estabelecendo assim o resultado para todo n natural.

■

OBS.: Adicionamos $(-b \cdot a^n + b \cdot a^n) = 0$, para facilitar o manejo das operações algébricas na demonstração.

Exemplo 1.8. *Para quais valores de* $a \in \mathbb{N}$, $(a-2) \mid (a^3+4)$.

Solução: Para tal solução utilizaremos o artifício $0 = -2^3+2^3$, aplicando no caso acima temos:

$$a-2 \mid a^3 + (-2^3+2^3) + 4 = (a^3-2^3) + (2^3+4) \qquad \text{(I)}$$

Pela proposição 1.3 se $a-2 \mid$ I, então:

$$a-2 \mid a^3-2^3 \iff a-2 \mid 2^3+4=12$$

Pela proposição 1.10 $a-2 \mid a^3-2^3$, portanto para que (I) seja verdade, depende apenas de $a-2 \mid 12$.

Com isso, temos que os divisores de 12 são:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6 \text{ e } \pm 12$$

Como queremos apenas valores de $a \in \mathbb{N}$, nos restringimos a: $-1, 1, 2, 3, 4, 6$ e 12.

Resolvendo cada um dos casos:

i) $a-2=-1 \Rightarrow a=1$

ii) $a-2=1 \Rightarrow a=3$

iii) $a-2=2 \Rightarrow a=4$

iv) $a-2=3 \Rightarrow a=5$

v) $a-2=4 \Rightarrow a=6$

vi) $a-2=6 \Rightarrow a=8$

vii) $a - 2 = 12 \Rightarrow a = 14$

Proposição 1.11. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b$ divide $a^{2n} - b^{2n}$.*

$$a + b | a^{2n} - b^{2n}$$

Demonstração:

Iremos provar essa proposição por indução sobre n.

$i)$ Caso base: para $n = 1$

$a^{2(1)} - b^{2(1)} = a^2 - b^2 = (a + b) \cdot (a - b)$, logo a afirmação é verdadeira pois $a + b | (a + b) \cdot (a - b)$

$ii)$ Hipótese de indução: Suponhamos, agora que $a + b | a^{2n} - b^{2n}$, $\forall\ n \in \mathbb{N}$.

$iii)$ Tese: Queremos demonstrar que $a + b | a^{2(n+1)} - b^{2(n+1)}$, com isso temos:

$$\begin{aligned} a^{2(n+1)} - b^{2(n+1)} &= a^{2n+2} - b^{2n+2} \\ &= a^2 \cdot a^{2n} - b^2 \cdot b^{2n} \\ &= a^2 \cdot a^{2n} - b^2 \cdot b^{2n} + (b^2 \cdot a^{2n} - b^2 \cdot a^{2n}) \\ &= a^2 \cdot a^{2n} - b^2 \cdot a^{2n} + b^2 \cdot a^{2n} - b^2 \cdot b^{2n} \\ &= (a^2 - b^2) \cdot a^{2n} + (a^{2n} - b^{2n}) \cdot b^2 \end{aligned}$$

Como $a + b | a^2 - b^2$ pelo caso base e por hipótese de indução $a + b | a^{2n} - b^{2n}$, decorre da igualdade acima e da proposição 1.6 que $a + b | a^{2(n+1)} - b^{2(n+1)}$ estabelecendo assim o resultado para todo n natural.

■

OBS.: Adicionamos $(b^2 \cdot a^{2n} - b^2 \cdot a^{2n}) = 0$, para facilitar o manejo das operação algébricas na demonstração.

Exemplo 1.9 (ENQ-PROFMAT 2018.2)**.** *Para quais valores $a \in \mathbb{N} \cup \{0\}$ tem-se que $a + 2 \mid a^4 + 2$?*

Solução: Para tal solução utilizaremos o artifício $0 = -2^4 + 2^4$, aplicando no caso acima temos:

$$a + 2 \mid a^4 + (-2^4 + 2^4) + 2 = (a^4 - 2^4) + (2^4 + 2) \qquad \textbf{(I)}$$

Pela proposição 1.3 se $a + 2 \mid$ I, então:

$$a + 2 \mid a^4 - 2^4 \Leftrightarrow a + 2 \mid 2^4 + 2 = 18$$

Pela proposição 1.11 $a+2 \mid a^4-2^4$, portanto para que (I) seja verdade, depende apenas de $a+2 \mid 18$.

Com isso, temos que os divisores de 18 são:

$$\pm 1, \pm 2, \pm 3, \pm 6, \pm 9 \text{ e } \pm 18$$

Como queremos apenas valores de $a \in \mathbb{N} \cup \{0\}$, nos restringimos a: $2, 3, 6, 9, 18$.

Resolvendo cada um dos casos:

i) $a+2=2 \Rightarrow a=0$

ii) $a+2=3 \Rightarrow a=1$

iii) $a+2=6 \Rightarrow a=4$

iv) $a+2=9 \Rightarrow a=7$

v) $a+2=18 \Rightarrow a=16$

Proposição 1.12. *Dados $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a+b$ divide $a^{2n+1}+b^{2n+1}$.*

Demonstração: Iremos provar essa proposição por indução sobre n.

$i)$ Caso base: para $n=0$

$a^{2(0)+1}+b^{2(0)+1}=a^1+b^1$, logo para $n=0$, a afirmação é verdadeira pois $a+b|a^1+b^1$

$ii)$ Hipótese de indução: Suponhamos, agora que $a+b|a^{2n+1}+b^{2n+1}, \forall\, n \in \mathbb{N}$.

$iii)$ Tese: Queremos demonstrar que $a+b|a^{2(n+1)+1}+b^{2(n+1)+1}$, com isso temos:

$$\begin{aligned} a^{2(n+1)+1}+b^{2(n+1)+1} &= a^{2n+2+1}+b^{2n+2+1} \\ &= a^{2+2n+1}+b^{2+2n+1} \\ &= a^2 \cdot a^{2n+1}+b^2 \cdot b^{2n+1} \\ &= a^2 \cdot a^{2n+1}+b^2 \cdot b^{2n+1}+(b^2 \cdot a^{2n+1}-b^2 \cdot a^{2n+1}) \\ &= a^2 \cdot a^{2n+1}-b^2 \cdot a^{2n+1}+b^2 \cdot b^{2n+1}+b^2 \cdot a^{2n+1} \\ &= (a^2-b^2) \cdot a^{2n+1}+(a^{2n+1}+b^{2n+1}) \cdot b^2 \end{aligned}$$

Como $a+b|a^2-b^2=(a+b) \cdot (a-b)$ e por hipótese de indução $a+b|a^{2n+1}+b^{2n+1}$, decorre da igualdade acima e da proposição 1.6 que

$$a+b|a^{2(n+1)+1}+b^{2(n+1)+1},$$

estabelecendo assim o resultado $\forall\, n \in \mathbb{N}$.

■

OBS.: Adicionamos $(b^2 \cdot a^{2n+1} - b^2 \cdot a^{2n+1}) = 0$, para facilitar o manejo das operações algébricas na demostração.

OBS.: Provamos o caso base para $n = 0$, pois o conjunto é formado por $\mathbb{N} \cup \{0\}$, caso não fosse, poderíamos fazer para $n = 1$, que ficaria:

$$\begin{aligned} a^3 + b^3 &= a^3 + b^3 + (a^2 \cdot b - a^2 \cdot b) \\ &= a^3 + a^2 \cdot b + b^3 - a^2 \cdot b \\ &= a^2 \cdot (a + b) + b \cdot (b^2 - a^2) \\ &= a^2 \cdot (a + b) - b \cdot (a^2 - b^2) \\ &= (a + b) \cdot a^2 + (a + b) \cdot (a - b) \cdot (-b) \\ &= (a + b) \cdot (a^2 + (a - b) \cdot (-b)) \\ &= (a + b) \cdot (a^2 - ab + b^2). \end{aligned}$$

Logo $a + b \mid a^3 + b^3 = (a + b) \cdot (a^2 - a \cdot b + b^2)$

Exemplo 1.10. *Para quais valores de* $a \in \mathbb{N}$, $a + 2 \mid a^4 + 2a^3 + a^2 + 1$.

Solução: Para tal solução utilizaremos o artifício:

$$0 = (-2^4 + 2^4), 0 = (+2^3 - 2^3), 0 = (+2^3 - 2^3), 0 = (-2^2 + 2^2)$$

Aplicando no caso acima temos:

$$a + 2 \mid a^4 + (-2^4 + 2^4) + a^3 + (+2^3 - 2^3) + a^3 + (+2^3 - 2^3) + a^2 + (-2^2 + 2^2) + 1$$

Reorganizando para utilizar as propriedades, temos:

$$\begin{gathered} a + 2 \mid (a^4 - 2^4) + 2^4 + (a^3 + 2^3) - 2^3 + (a^3 + 2^3) - 2^3 + (a^2 - 2^2) + 2^2 + 1 \Rightarrow \\ a + 2 \mid (a^4 - 2^4) + (a^3 + 2^3) + (a^3 + 2^3) + (a^2 - 2^2) + 2^4 - 2^3 - 2^3 + 2^2 + 1 \end{gathered}$$

Pela proposição 1.11, $a + 2 \mid (a^4 - 2^4)$ e $a + 2 \mid (a^2 - 2^2)$.
Pela proposição 1.12, $a + 2 \mid (a^3 + 2^3)$.
Pela proposição 1.3, se $a + 2 \mid$ (I), então

$$\begin{gathered} a + 2 \mid [(a^4 - 2^4) + (a^3 + 2^3) + (a^3 + 2^3) + (a^2 - 2^2)] \iff \\ a + 2 \mid (2^4 - 2^3 - 2^3 + 2^2 + 1) = 5 \end{gathered}$$

Com isso temos que os divisores de 5 são: ± 1 e ± 5, como queremos apenas valores de $a \in \mathbb{N}$, nos restringimos apenas ao divisor 5.

Resolvendo, temos:
i) $a + 2 = 5 \Rightarrow a = 3$.

Teorema 1.1 (Algoritmo da divisão de Euclides)**.** *Dado dois inteiros a e b, $b > 0$, existem um único par de inteiros q e r tais que:*

$$a = q \cdot b + r \text{ com } 0 \leq r < b \ (r = 0 \iff b \,|\, a),$$

onde q é chamado de quociente e r de resto da divisão de a por b.

Demonstração: Suponhamos que $b > 0$, (para facilitar a nossa demonstração) e seja q o maior inteiro tal que $b \cdot q \leq a$. Então temos

$$b \cdot q \leq a < b(q + 1)$$

Tal fato deve-se a Eudoxo, ele aparece no livro III dos "Elementos" de Euclides, escrito por volta do ano 300 A.C. Enunciamos o chamado de teorema de Eudoxius: dados a e b inteiros com $b \neq 0$ então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b. Subtraindo bq da desigualdade acima obtemos:

$$bq - bq \leq a - bq < bq + b - bq \Rightarrow 0 \leq a - bq < b,$$

obtemos assim $0 \leq r < b$, tomando $r = a - b \cdot q$.

Fizemos a demonstração para o caso $b > 0$. Se $b < 0$, então $-b > 0$, onde existem q, $r \in \mathbb{Z}$ tais que $a = (-b) \cdot q + r$, com $0 \leq r < -b$. Daí, $a = b \cdot (-q) + r$ com $0 \leq r < -b = |b|$.

Iremos agora demonstrar a sua unicidade

Suponhamos que na divisão de a por b exista um outro quociente e um outro resto ou seja:

$$\begin{cases} a = b \cdot q + r & \text{(I)} \\ a = b \cdot q_1 + r_1 & \text{(II)} \end{cases}$$

Como $a = a$, podemos igualar (I) e (II), $b \cdot q + r = b \cdot q_1 + r_1$, isso implica $b \cdot q - b \cdot q_1 = r_1 - r \Rightarrow b \cdot (q - q_1) = r_1 - r$ o que implica que $b | r_1 - r$, mas como $r_1 < b$ e $r < b$, temos que $|r_1 - r| < b$, portanto a única forma de $b | r_1 - r$ é se $r_1 - r = 0$ isso implica $r_1 = r$. Com isso temos que $b \cdot (q - q_1) = 0$, como o produto de dois números só é zero se ao menos um deles for igual a zero, por hipótese $b > 0$, resulta que $q - q_1 = 0 \Rightarrow q = q_1$.

■

O algoritmo da divisão de Euclides poderia ser enunciado da seguinte forma:

Dados dois inteiros a e b, com $b \neq 0$, existe um único par de inteiros q e r tais que $a = qb + r$, com $0 \leq r < |b|$.

1.3 Máximo Divisor Comum

Escolhemos este tópico por ser de fundamental importância, indispensável na construção do texto base das equações diofantinas, uma vez que esta é a aplicação direta do m.d.c., que mostraremos a seguir através de um teorema conhecido como divisões sucessivas de Euclides.

Dados dois números inteiros a e b, distintos ou não, um inteiro d será dito divisor comum se $d|a$ e $d|b$.

Exemplo 1.11. *Quais os divisores comuns de* 12 *e* 18*?*

Divisores de 12*:*

$$-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$$

Divisores de 18*:*

$$-18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18$$

Divisores comuns de 12 *e* 18*:*

$$-6, -3, -2, -1, 1, 2, 3, 6$$

Dentre os divisores comuns, é lógico se pensar, qual é o maior divisor comum de 12 e 18. Com essa ideia passamos à definição formal de máximo divisor comum.

Definição 1.2. *Um inteiro* $d \geq 0$ *é o máximo divisor comum de* a *e* b*, ou seja,* $d = mdc\,(a, b)$*, se possuir as seguintes propriedades:*

i) d *é um divisor comum de* a *e* b

ii) Se c *é um divisor comum de* a *e* b*, então* $c|d$

Exemplo 1.12.

a) $mdc\,(6, 0) = 6$*, pois todo divisor de* 6 *é também um divisor de zero, ou seja:*

Divisores de 6*:*

$$-6, -3, -2, -1, 1, 2, 3, 6$$

Divisores de 0*:*

Pela Proposição 1.1, item i*). Todo* $a \in \mathbb{Z}$ *divide zero.*

Divisores comum de 0 *e* 6*:*

$$-6, -3, -2, -1, 1, 2, 3, 6$$

Máximo Divisor Comum de 6 *e* $0 = mdc\,(6, 0) = 6$

b) $mdc\,(8, 10) = 2$*, pois:*

Divisores de 8*:*

$$-8, -4, -2, -1, 1, 2, 4, 8$$

Divisores de 10*:*

$$-10, -5, -2, -1, 1, 2, 5, 10$$

Divisores comum de 8 *e* 10*:*

$$-2, -1, 1, \text{ e } 2$$

Máximo Divisor Comum de 8 *e* $10 = mdc\,(8, 10) = 2$

O método utilizado no exemplo anterior, para determinar o $mdc\,(a, b)$ só é eficiente quando a e b forem números pequenos. Para números como $a = 1126$ e $b = 522$, por exemplo, ele já é trabalhoso por envolver o cálculo de todos os divisores de 1126 e 522. Um método mais eficiente, é conhecido por algoritmo de Euclides, que consiste na aplicação sucessiva da proposição que demonstraremos a seguir.

Proposição 1.13. *Se* a *e* b *são inteiros e* r *é o resto da divisão Euclidiana de* a *por* b*, então:*

$$mdc\,(a, b) = mdc\,(b, r)$$

Demonstração: Da divisão Euclidiana de a por b, temos que $a = qb + r$, e pela Proposição 1.6, podemos concluir que todo divisor comum de b e r é também um divisor de a. Esta mesma relação pode ser escrita na forma $r = a - qb$, e pela Proposição 1.6, nos diz que todo divisor de a e b é um divisor de r. Logo o conjunto dos divisores comuns de a e b é igual $mdc\,(a, b) = mdc\,(b, r)$.

■

Teorema 1.2 (Relação de Bezout)**.** *Seja d o máximo divisor comum de a e b, então existem inteiros n_0 e m_0 tais que $d = n_o \cdot a + m_0 \cdot b$*

Demonstração: Seja B o conjunto de todas as combinações lineares $na + mb$, onde n e m são inteiros. Este conjunto contém, claramente números negativos, positivos e também o zero. Vamos escolher n_0 e m_0 tais que $c = n_0a + m_0b$, conjunto das combinações lineares.

Vamos inicialmente provar, por absurdo, que $c|a$ e $c|b$. Seja

$$c = n_0a + m_0b \qquad \text{(I)}$$

Dividiremos esta demonstração em três etapas.

$i)$ Suponhamos que $c \nmid a$.

Como $c \nmid a$, pelo Teorema 1.1, existem inteiros q e r tais que $a = q \cdot c + r$, com $0 < r < c$. Portanto:

$$r = a - q \cdot c \qquad \text{(II)}$$

Substituindo a equação (I), na equação (II), temos:

$$\begin{aligned} r = a - q \cdot c \Rightarrow r &= a - q\,(n_0a + m_0b) \\ \Rightarrow r &= a - q \cdot n_0a - q \cdot m_0 \cdot b \\ \Rightarrow r &= a\,(1 - q \cdot n_0) + b\,(-qm_0) \end{aligned}$$

isso mostra que $r \in B$, pois $(1 - q \cdot n_0)$ e $(-q \cdot m_0)$ são inteiros, ou seja, r pode ser escrito como combinação linear de a e b, que é um absurdo pois $0 < r < c$ e c é o menor elemento positivo de B, por tanto não pode existir um menor elemento, menor do que o menor elemento, logo a hipótese de que $c \nmid a$ é falsa, com isso concluímos que $c|a$.

$ii)$ Suponhamos que $c \nmid b$

Como $c \nmid b$, pelo teorema 1.1, existem inteiros q e r tais que $b = q \cdot c + r$, com $0 < r < c$. Portanto:

$$r = b - q \cdot c \qquad \text{(III)}$$

Substituindo a equação (I) , na equação (III), temos:

$$\begin{aligned} r = b - q \cdot c \Rightarrow r &= b - q \cdot (n_0 a + m_0 b) \\ \Rightarrow r &= b - q \cdot n_0 \cdot a - q \cdot m_0 \cdot b \\ \Rightarrow r &= b\,(1 - q \cdot m_0) + a\,(-q \cdot n_0) \end{aligned}$$

como $(1 - q \cdot m_0)$ e $(-q \cdot n_0)$ são inteiros, isso mostra que $m \in B$, ou seja, r pode ser escrito como combinação linear de a e b, que é um absurdo pois $0 < r < c$ e c é menor elemento positivo de B, portanto não pode existir um menor elemento , menor do que o menor elemento, logo a hipótese de que $c \nmid b$ é falsa, com isso concluímos que $c|b$.

$iii)$ Agora demonstraremos que $c = d$.

Como d é um divisor comum de a e b, existem inteiros k_1 e k_2, tais que $a = k_1 \cdot d$ e $b = k_2 \cdot d$. Como $c = n_0 \cdot a + m_0 \cdot b$, substituindo o valor de a e b em c, temos:

$$\begin{aligned} c = n_0 \cdot a + m_0 \cdot b \Rightarrow c &= n_0 \cdot (k_1 \cdot d) + m_0 \cdot (k_2 \cdot d) \\ \Rightarrow c &= (n_0 \cdot k_1 + m_0 \cdot k_2) \cdot d \end{aligned}$$

como $(n_0 \cdot k_1 + m_0 \cdot k_2) = k \in \mathbb{Z}$, temos que $c = k \cdot d$, o que implica que $d|c$.

Pela proposição 1.7, com $d \mid c \Rightarrow d \leq c$ (ambos positivos), e como $d < c$, não é possível pois d é o maior divisor comum de a e b, e como já provamos que c também é um divisor comum de a e b, por tal motivo d não pode ser menor do que c. Logo, só nos resta que $d = c$.

■

OBS.: Na demonstração deste teorema, mostramos não apenas que o m.d.c de a e b pode ser escrito como uma combinação linear destes números, mas que este é o menor valor positivo dentre todas as combinações lineares. Tal teorema é reconhecido como relação de Bézout.

Teorema 1.3. *O máximo divisor d de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum.*

Demonstração: Sejam c, um divisor comum de a e b, ou seja, $c|a$ e $c|b$, e pela Proposição 1.6, $c|ma+nb$, e pelo Teorema 1.2, sabemos que $d = m_0 \cdot a + n_0 \cdot b$, logo $c|d$. Como não pode existir dois números tendo cada um a propriedade de ser divisível por todo divisor comum. Portanto pela Proposição 1.8, que no caso de números positivos $c = d$.

■

Lema 1.1. *Para a, b e $n \in \mathbb{Z}$. Se existe $mdc\,(a, b + na)$, então, $mdc\,(a, b)$ existe e:*

$$mdc\,(a, b) = mdc\,(a, b + na)$$

Demonstração: Chamaremos de d o $mdc\,(a, b)$ e f o $mdc\,(a, b + na)$.

($\Longrightarrow$) Sejam $d = mdc\,(a, b)$ e $f = mdc\,(a, b + ax)$. Pelo Teorema 1.2 existem inteiros n_0 e m_0 tais que $d = n_0 \cdot a + m_0 \cdot b$ e como esta expressão pode ser escrita como

$$d = n_0 \cdot a + m_0 \cdot b + (anm_0 - anm_0) = a\,(n_0 - n \cdot m_0) + (b + an) \cdot m_0,$$

Já que f é o máximo divisor comum de a e de $b + n \cdot a$, pela Proposição 1.4, se $f|a$ então $f|a \cdot (n_0 - n \cdot m_0)$ e se $f|(b+an) \Rightarrow f|(b+an) \cdot m_0$ e pela Proposição 1.6, se $f|a\ (n_0 - n \cdot m_0)$ e $f|(b + an) \cdot m_0$, $f|a\ (n_0 - n \cdot m_0) + (b + an) \cdot m_0 = d$, ou seja , $f|d$.

($\Longleftarrow$) Tendo mostrado que $f|d$, mostraremos agora que $d|f$. Como $d = mdc\,(a, b)$, temos pela Proposição 1.6, que $d|a$ e $d|b \Rightarrow d|b + ax$ e pelo Teorema 1.3, sabemos que todo divisor comum de a e $b + ax$ é um divisor de f. Tendo, assim, provado que $d|f$. Concluímos, pela Proposição 1.8, que $d = f$, ou seja; $mdc\,(a, b) = mdc\ (a, b + n \cdot a)$, uma vez que ambos são positivos.

■

OBS.: Tal Lema também pode ser escrito como $mdc\,(a, b) = mdc\,(a, b - n \cdot a)$, a demonstração se faz da mesma maneira.

Proposição 1.14. *Para todo inteiro positivo, $mdc\,(ta, tb) = t \cdot mdc\,(a, b)$*

Demonstração: Pelo Teorema 1.2, $mdc\,(ta, tb)$ é o menor valor positivo do conjunto das combinações lineares $m\ (ta) + m\ (tb)$; onde m e n são inteiros, que é igual a t vezes o menor valor positivo de $ma + nb = t \cdot mdc\,(a, b)$.

■

Exemplo 1.13.

a) $mdc\,(6, 4) = 2 \cdot mdc\,(3, 2) = 2 \cdot 1 = 2$

b) $mdc\,(24, 8) = 4 \cdot mdc\,(7, 2) = 4 \cdot 1 = 4$

c) $mdc\,(20, 30, 50) = 10 \cdot mdc\,(2, 3, 5) = 10 \cdot 1 = 10$

Proposição 1.15. *Se $c > 0$ e a e b são divisíveis por c, então:*

$$mdc\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} mdc\,(a, b)$$

Demonstração: Como a e b são divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros. Basta, então, substituir na proposição 1.14, onde $t = \frac{1}{c}$, ou seja:

$mdc\,(t \cdot a, t \cdot b) = t \cdot mdc\,(a, b)$ e, substituindo t por $\frac{1}{c}$, temos:

$$mdc\,(\frac{1}{c} \cdot a, \frac{1}{c} \cdot b) = mdc\,(\frac{a}{c}; \frac{b}{c}) = \frac{1}{c} \cdot mdc\,(a, b)$$

■

Corolário 1.1. *Se* $mdc\,(a, b) = d$ *temos que* $mdc\,(\frac{a}{d}, \frac{b}{d}) = 1$.

Demonstração: No que acabamos de demonstrar na proposição anterior, c é um divisor comum, se substituirmos c por d, ou seja:

$$mdc\,(\frac{a}{c}, \frac{b}{c}) = \tfrac{1}{c} \cdot mdc\,(a, b)$$

substituindo c por $d = mdc\,(a, b)$ temos que:

$$mdc\,(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d} \cdot mdc\,(a, b),$$

como $d = mdc\,(a, b)$, obtemos o seguinte:

$$mdc\,(\frac{a}{d}, \frac{b}{d}) = \frac{1}{mdc\,(a, b)} \cdot mdc\,(a, b) \Rightarrow mdc\,(\frac{a}{d}, \frac{b}{d}) = 1$$

Com isso podemos definir quando dois números sarão primos entre si.

■

Definição 1.3. *Dois números* a *e* b *sarão dito primos entre si, ou coprimos, se* $mdc\,(a, b) = 1$*, ou seja , se o único divisor comum positivo de ambos é* 1.

Proposição 1.16. *Dois números inteiros* a *e* b *são primos entre si se, e somente se, existem números inteiros* m *e* n *tais que* $ma + nb = 1$.

Demonstração: ($\Rightarrow$) Suponhamos a e b primos entre si, logo temos que $mdc\,(a, b) = 1$. Pelo teorema 1.2, temos que $mdc\,(a, b)$ é o menor valor positivo do conjunto das combinações lineares de a e b, ou seja $ma + nb = mdc\,(a, b)$ como $mdc\,(a, b) = 1$, temos o que queríamos demonstrar $ma + nb = 1$.

($\Leftarrow$) Reciprocamente, suponhamos que exista inteiros m e n tais que $ma + nb = 1$. Se $d = mdc\,(a, b)$, temos que $d|a$, $d|b$ e pela proposição 1.4 que $d \mid ma$ e $d \mid nb$, de tal forma que pela proposição 1.6 temos $d|(ma + nb)$, ou seja $d|1$. Por definição $d \geq 0$, o que nos resta que d só pode ser 1.

■

Teorema 1.4. *Sejam a, b e c números inteiros. Se $a|b \cdot c$ e $mdc\,(a, b) = 1$, então $a|c$.*

Demonstração: Se $a|b \cdot c$, então $b \cdot c = k \cdot a$, onde $k \in \mathbb{Z}$. (I)

Se $mdc\,(a, b) = 1$, pela proposição 1.16, existem inteiros m, n, tais que $ma + nb = 1$ (II)

Multiplicamos por c ambos os lados da equação (II), temos que: $ma \cdot c + nb \cdot c = c$.

Organizaremos da seguinte maneira para dar mais clareza na demonstração:

$$c = ma \cdot c + nb \cdot c \tag{III}$$

Substituindo o valor de bc, da equação (I), na equação (III), temos:

$$c = ma \cdot c + nb \cdot c \Rightarrow c = mac + n \cdot ka \Rightarrow c = (mc + nk) \cdot a$$

onde $(mc + nk) = k_1 \in \mathbb{Z}$, logo $c = k_1 \cdot a$ e por definição temos que $a|c$.

■

OBS.: Tal teorema é reconhecido como Lema de Gauss.

Corolário 1.2. *Dados $a, b, c \in \mathbb{Z}$, com b e c não ambos nulos, temos que:*

$$b|a \;\; \textit{e} \;\; c|a \Longleftrightarrow \frac{bc}{mdc\,(b, c)}\Big|a$$

Demonstração: Chamaremos de d o $mdc\,(b, c)$, ou seja, $d = mdc\,(b, c)$.

Como $b|a$, por definição temos que $a = k_1 \cdot b$, onde $k_1 \in \mathbb{Z}$. (I)

Como $c|a$, por definição temos que $a = k_2 \cdot c$, onde $k_2 \in \mathbb{Z}$. (II)

Pela propriedade reflexiva, $a = a$. Com isso, igualando (I) e (II), temos:

$$k_1 \cdot b = k_2 \cdot c$$

Dividindo ambos os membros da equação por $d = mdc\,(b, c)$, temos:

$$k_1 \cdot \frac{b}{d} = k_2 \cdot \frac{c}{d}$$

Pelo Corolário 1.1, temos que $mdc\,(\frac{b}{d}, \frac{c}{d}) = 1$, ou seja são primos entre si.

Pelo teorema 1.4, conhecido como lema de Gauss, temos que se

$$\frac{b}{d}|k_2 \cdot \frac{c}{d} \text{ e } mdc\,(\frac{b}{d}, \frac{c}{d}) = 1, \text{ logo } \frac{b}{d}|k_2.$$

Pela Proposição 1.5 resulta

$$\frac{b}{d} \mid k_2 \;\; \Longrightarrow \;\; \frac{b}{d} \cdot c \mid k_2 \cdot c,$$

onde $k_2 \cdot c = a$ pela equação (II).

Por tanto,

$$\frac{bc}{d}\Big|a, \text{ ou seja, } \frac{bc}{mdc\,(b, c)}|a.$$

■

Corolário 1.3. *Sejam a_1, a_2, ..., a_n inteiros não nulos dados e d seu m.d.c:*

a) $d = 1$ *se, e só se, existirem inteiros* $U_1, U_2, ..., U_n$ *tais que* $a_1U_1 + a_2U_2 + ... + a_nU_n = 1$

b) $mdc\,(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}) = 1$

Demonstração:

a) É uma aplicação direta do Teorema 1.2, (relação de Bézout), que nos garante que o m.d.c pode ser escrito como combinação linear.

$a_1U_1 + a_2U_2 + ... + a_nU_n = mdc\,(a_1, a_2, \ldots, a_n) \implies a_1U_1 + a_2U_2 + ... + a_nU_n = 1$

Reciprocamente, sejam $U_1, U_2, ..., U_n$ inteiros como no enunciado. Como $d|a_1, a_2, ..., a_n$, segue da proposição 1.4, $d \mid a_1 \cdot U_1, d \mid a_2 \cdot U_2, \ldots, d \mid a_n \cdot U_n$. Da Proposição 1.6, segue que $d|(a_1U_1 + a_2U_2 + ... + a_nU_n)$, ou seja $d|1$, que pela definição de m.d.c, temos que $d = 1$.

b) Sendo $d = a_1U_1 + a_2U_2 + ...a_nU_n$, dividimos ambos os lados da igualdade por d, temos: $(\frac{a_1}{d})\,U_1 + (\frac{a_2}{d})\,U_2 + ... + (\frac{a_n}{d})\,U_n = 1$, e o resultado segue imediatamente do item a).

■

Proposição 1.17. *Para a, b e c inteiros não nulos, temos que:*

a) Se $mdc\,(a, c) = 1$*, então* $mdc\,(a, bc) = mdc\,(a, b)$

b) Se $c|b$ *e* $mdc\,(a, b) = 1$*, então* $mdc\,(a, c) = 1$

c) Se $mdc\,(b, c) = 1$*, então* $mdc\,(a, bc) = mdc\,(a, b) \cdot mdc\,(a, c)$*. Em particular, se b e c são primos entre si e dividem a, então bc divide a.*

Demonstração:

a) Sejam $d = mdc\,(a, b)$ e $f = mdc\,(a, bc)$.

Demonstraremos que $d|f$

Se $d = mdc\,(a, b)$, então $d|b$, e pela proposição 1.4, $d|b \cdot c$, assim temos que $d|a$ e $d|b \cdot c$. Se d é um divisor comum de a e bc, então pelo Teorema 1.3, $d|mdc\,(a, bc)$, ou seja $d|f$.

Demonstraremos que $f|d$

Como $mdc\,(a, c) = 1$, segue da proposição 1.16, que existem inteiros m e n tais que: $am + cn = 1$, multiplicando ambos os membros da equação por b, temos:

$$am \cdot b + cn \cdot b = b \Rightarrow a\,(mb) + n\,(bc) = b,$$

como $f = mdc\,(a, bc)$, temos que $f|a$ e $f|b \cdot c$ e pela proposição 1.4, $f \mid a \cdot (mb)$ e $f \mid n \cdot (bc)$ e, pela proposição 1.6, $f|a\ (mb) + n\ (bc)$, ou seja, $f|b$. Como $f|a$ e $f|b$, f é um divisor comum de a e b e pelo teorema 1.3 $f|mdc\,(a, b)$, ou seja, $f|d$. Com isso concluímos pela proposição 1.8 que $f = d$, em outras palavras que $mdc\,(a, bc) = mdc\,(a, b)$.

b) Se $c|b \Rightarrow b = k \cdot c$, onde $k \in \mathbb{Z}$. Como $mdc\,(a, b) = 1$, pela q proposição 1.16, existem inteiros m e n tais que $am + bn = 1$, substituindo o valor de b, na equação temos:

$$am + k \cdot cn = 1 \Rightarrow a\ (m) + c\ (kn) = 1$$

que pela proposição 1.16 nos garante que $mdc\,(a, c) = 1$

c) Seja $d = mdc\,(a, b) \Rightarrow \mathrm{d} \mid a$ e $d \mid b \Rightarrow a = k \cdot d$ e $b = q \cdot d$, onde $(k, q) \in \mathbb{Z}$ e pelo corolário 1.1, temos que $mdc\,(k, q) = 1$. Com isso temos:

$$mdc\,(a, bc) \Rightarrow mdc\,(a, bc) = mdc\,(k \cdot d, q \cdot d \cdot c),$$

pela proposição 1.14, nos garante que $mdc\,(k \cdot d, q \cdot d \cdot c) = d \cdot mdc\,(k, q \cdot c)$, como $mdc\,(k, q) = 1$, pelo item a), temos que:

$$d \cdot mdc\,(k, q \cdot c) = d \cdot mdc\,(k, c).$$

Juntando todas as igualdades temos:

$$mdc\,(a, bc) = mdc\,(k \cdot d, q \cdot d \cdot c) = d \cdot mdc\,(k, q \cdot c) = d \cdot mdc\,(k, c),$$

ou seja:

$$mdc\,(a, bc) = d \cdot mdc\,(k, c) \qquad \text{(I)}$$

Como $d|b$ e $mdc\,(b, c) = 1$, pelo item b) temos que $mdc\,(d, c) = 1$, com isso temos:

$$mdc\,(a, c) = mdc\,(k \cdot d, c) = mdc\,(k, c)$$

ou seja:

$$mdc\,(a, c) = mdc\,(k, c) \qquad \text{(II)}$$

Substituindo a equação (II), na equação (I), temos:

$$\begin{aligned} mdc\,(a, bc) &= d \cdot mdc\,(k, c) \\ &= d \cdot mdc\,(a, c) \\ &= mdc\,(a, b) \cdot mdc\,(a, c) \end{aligned}$$

A segunda afirmação é uma aplicação direta do que acabamos de demonstrar.

O que queremos demonstrar é: se $mdc\,(b, c) = 1$ e $b \mid a$ e $c \mid a$, então $bc \mid a$.

Utilizando a primeira afirmação do item c) para provar o caso particular, temos:

$$mdc\,(a, bc) = mdc\,(a, c) \cdot mdc\,(a, b) \qquad \text{(III)}$$

Como $b|a \Rightarrow a = k_1 \cdot b$, onde $k_1 \in \mathbb{Z}$, com isso temos:

$$mdc\,(a, b) = mdc\,(k_1 \cdot b, b) = b$$

Como $c|a \Rightarrow a = k_2 \cdot c$, onde $k_2 \in \mathbb{Z}$, com isso temos:

$$mdc\,(a, c) = mdc\,(k_2 \cdot c, c) = c$$

Utilizando os resultados obtidos e substituindo na equação (III), temos:

$$\begin{aligned} mdc\,(a, bc) &= mdc\,(a, c) \cdot mdc\,(a, b) \\ &= c \cdot b = b \cdot c \end{aligned}$$

Com isso temos que $mdc\,(a, bc)$ é igual a bc, ou seja, $bc \mid a$.

■

Proposição 1.18. *Dados números $a_1, ..., a_n$, não todos nulos, existe o seu m.d.c e $mdc\,(a_1, ..., a_n) = mdc\,(a_1, ..., mdc\,(a_{n-1}, a_n))$*

Demonstração:

Provaremos por indução sobre n, para $n \geq 2$

$i)$ Caso base para $n = 2$

$mdc\,(a_1, a_2) = mdc\,(a_1, mdc\,(a_1, a_2))$

ii) Hipótese de indução: Suponha que $mdc\,(a_1, ..., a_n) = mdc\,(a_1, ..., mdc\,(a_{n-1}, a_n))$, $\forall\ (a_1, ..., a_n) \in \mathbb{N}$.

iii) Tese: Queremos demonstrar que $mdc\,(a_1, ..., a_n, a_{n+1}) = mdc\,(a_1, ..., mdc\,(a_n, a_{n+1})$.

Seja $d = mdc\,(a_1, ..., mdc\,(a_n, a_{n+1}))$, com isso temos que $d|a_1, ...,\ d|mdc\,(a_n, a_{n+1})$, com isso obtemos que $d|a_1, d|a_2, ..., d|a_n$ e $d|a_{n+1}$.

Por outro lado, seja c um divisor de $a_1, ..., a_n, a_{n+1}$, temos então que c é um divisor comum de $a_1, ..., a_{n-1}$ e $mdc\,(a_n, a_n + 1)$ e por tanto $c|d$.

■

No início do tópico, não calculamos o máximo divisor comum de 1126 e 522, pois daria muito trabalho. Mas, agora calcularemos o $mdc\,(1126, 522)$ utilizando a ideia usada na demonstração do teorema 1.5, para nos auxiliar na compreensão do mesmo. Tal teorema é conhecido como divisões sucessivas de Euclides, o mesmo é a base na resolução das equações diofantinas lineares.

Exemplo 1.14. *Como estamos interessados no cálculo de máximo divisor comum de* $1126, 522$*. Utilizaremos o algoritmo da divisão (Teorema 1) para dividir* 1126 *por* 522*, em seguida dividiremos* 522 *pelo resto* 82*. Depois* 82 *pelo resto* 30 *e assim sucessivamente, até obtemos resto zero.*

$\begin{array}{r|l} a & \mathrm{b} \\ \hline n & q \end{array} \Longrightarrow$ Pela Proposição 1.13, temos que $mdc\,(a, b) = mdc\,(b, r)$ com isso temos:

- $\begin{array}{r|l} 1126 & 522 \\ \hline 82 & 2 \end{array} \Longrightarrow$ pelo Proposição 1.13, temos que $mdc\,(1126, 522) = mdc\,(522, 82)$
- $\begin{array}{r|l} 522 & 82 \\ \hline 30 & 6 \end{array} \Longrightarrow$ pela Proposição 1.13, temos que $mdc\,(522, 82) = mdc\,(82, 30)$
- $\begin{array}{r|l} 82 & 30 \\ \hline 22 & 2 \end{array} \Longrightarrow$ pela Proposição 1.13, temos que $mdc\,(82, 30) = mdc\,(30, 22)$
- $\begin{array}{r|l} 30 & 22 \\ \hline 8 & 1 \end{array} \Longrightarrow$ pela Proposição 1.13, temos que $mdc\,(30, 22) = mdc\,(22, 8)$
- $\begin{array}{r|l} 22 & 8 \\ \hline 6 & 2 \end{array} \Longrightarrow$ pela Proposição 1.13, temos que $mdc\,(22, 8) = mdc\,(8, 6)$
- $\begin{array}{r|l} 8 & 6 \\ \hline 2 & 1 \end{array} \Longrightarrow$ pela Proposição 1.13, temos que $mdc\,(8, 6) = mdc\,(6, 2)$
- $\begin{array}{r|l} 6 & 2 \\ \hline 0 & 3 \end{array} \Longrightarrow$ pela Proposição 1.13, temos que $mdc\,(6, 2) = mdc\,(2, 0)$

Da última igualdade temos que $mdc\,(2,0) = 2$, por tal motivo que o algoritmo de Euclides mostra que $mdc\,(a,b)$ é o ultimo resto não nulo. Devido as aplicações sucessivas da proposição 1.13, temos:

$mdc\,(2,0) = mdc\,(6,2) = mdc\,(8,6) = mdc\,(22,8) = mdc\,(30,22) = mdc\,(82,30) = mdc\,(522,82) = mdc\,(1126,522) = 2$

É desta forma que procede o algoritmo de Euclides, dito isto, estamos prontos para a demonstração do teorema.

■

OBS.: Na demonstração do teorema a seguir, utilizaremos $a = r_0$ e $b = r_1$ para que a sequência dos números fiquem mais compreensível.

Teorema 1.5. *(Teorema das divisões sucessivas de Euclides) Sejam $r_0 = a$ e $r_1 = b$ inteiro não-negativos com $a \geq b$ e $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter.*

$$r_j = q_{j+1}\, r_{j+1} + r_{j+2}, 0 \leq r_{j+2} < r_{j+1}$$

Para $j = 0, 1, 2, ..., n-1$ e $r_{n+1} = 0$ então $mdc\,(a,b) = r_n$, o último resto não nulo.

Demonstração:

Temos duas possibilidades:

i) Se $b|a$

Se $b|a \Rightarrow a = q \cdot b + 0$, onde $q \in \mathbb{Z}$ e pela proposição 1.13, temos que $mdc\,(a,b) = mdc\,(b,0) =$

ii) Se $b \nmid a$

Pelo que foi mostrado no exemplo anterior fica fácil acompanhar a demonstração deste algoritmo. Vamos inicialmente, aplicar o Teorema 1.1 (Algoritmo da Divisão), para dividirmos a por b, ou seja, r_0 por r_1, obtendo $r_0 = q_1 \cdot r_1 + r_2$, em seguida dividimos r_1 por r_2, obtendo $r_1 = q_2 \cdot r_2 + r_3$, em seguida r_2 por r_3, obtendo $r_2 = q_3 \cdot r_3 + r_4$ e assim sucessivamente, até a obtenção do resto $r_{n+1} = 0$. Como, a cada passo o resto é sempre menor do que o anterior, e estamos lidando com números inteiros, como no exemplo 1.11, após um número finito de aplicações do Teorema 1.1 (Algoritmo da Divisão), teremos o resto nulo.

Colocando o que foi mostrado até agora em uma sequência de equações temos o seguinte.

$r_0 = q_1 r_1 + r_2 \qquad 0 < r_2 < r_1$

$r_1 = q_2 r_2 + r_3 \qquad 0 < r_3 < r_2$

$r_2 = q_3 r_3 + r_4 \qquad 0 < r_4 < r_3$

.

.

.

$r_{n\cdot 2} = q_{n-1}r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$

$r_{n-1} = q_n r_n + 0$

Da ultima igualdade e pela proposição 1.13, temos que $mdc\,(r_{n-1}, r_n) = mdc\,(r_n, 0) = r_n$, aplicando sucessivamente a proposição 1.13, temos a seguinte sequência.

$r_n = mdc\,(r_n, 0) = mdc\,(r_{n-1}, r_n) = mdc\,(r_{n-2}, r_{n-1}) = ... = mdc\,(r_1, r_2) = mdc\,(r_0, r_1) = mdc\,(a, b)$.

Portanto o máximo divisor comum de a e b é o último resto não nulo da sequência de divisões descrita.

Tal teorema pode ser sintetizado e realizado na pratica da seguinte maneira: inicialmente, efetuamos a divisão de a por b e colocamos os números envolvidos no seguinte diagrama:

	q_1	quociente
a	b	dividendo e divisor
r_1		resto

$\Longrightarrow \quad a = q_1 \cdot b + n_1$

A seguir, continuamos efetuando a divisão $b = q_2 \cdot r_1 + r_2$ e colocamos os números no diagrama:

	q_1	q_2	quociente
a	b	r_1	dividendo ou divisor
r_1	r_2		restos

$\Longrightarrow \quad b = q_2 \cdot r_1 + r_2$

Prosseguindo em quanto for possível, teremos:

	q_1	q_2	$\cdots$	q_{n-1}	q_n	
a	b	r_1	$\cdots$	r_{n-2}	r_{n-1}	$r_n = MDC\ (a, b)$
r_1	r_2	r_3	$\cdots$	r_n	0	

■

Exemplo 1.15. *Calcularemos o m.d.c de* 372 *e* 162.

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6	0	

Com isso temos que $mdc\,(372, 162) = 6$ *mas, as contribuições do algoritmo de Euclides descrito dessa forma não param por aí. Sabemos, pela (Relação de Bézout), Teorema 1.2 que o m.d.c pode ser escrito como combinação linear. Tal método nos ajudará a fazer isso. Mostraremos como proceder.*

	2	3	2	(1)	2
372	162	48	(18)	(12)	6
48	18	12	(6)	0	

Não podemos esquecer que no algoritmo de Euclides, o m.d.c é o último resto não nulo. Com isso temos:

$$6 = 18 - 1 \cdot 12$$

	2	3	(2)	1	2
372	162	(48)	(18)	12	6
48	18	(12)	6	0	

$$12 = 48 - 2 \cdot 18$$

	2	(3)	2	1	2
372	(162)	(48)	(18)	12	6
48	(18)	12	6	0	

$$18 = 162 - 3 \cdot 48$$

	(2)	3	2	1	2
(372)	(162)	48	18	12	6
(48)	18	12	6	0	

$$48 = 372 - 2 \cdot 162$$

Organizando todos os valores dos restos, temos:

$$
\begin{aligned}
6 &= 18 - 1 \cdot 12 \qquad (I)\\
12 &= 48 - 2 \cdot 18 \qquad (II)\\
18 &= 162 - 3 \cdot 48 \qquad (III)\\
48 &= 372 - 2 \cdot 162 \qquad (IV)
\end{aligned}
$$

Substituindo (II) em (I), temos:

$$
\begin{aligned}
6 &= 18 - 1 \cdot 12\\
6 &= 18 - 1 \cdot (48 - 2 \cdot 18)\\
6 &= 18 - 1 \cdot 48 + 2 \cdot 18\\
6 &= -1 \cdot 48 + 3 \cdot 18 \quad (V)
\end{aligned}
$$

Substituindo (III) em (V), temos:

$$
\begin{aligned}
6 &= -1 \cdot 48 + 3 \cdot 18\\
6 &= -1 \cdot 48 + 3 \cdot (162 - 3 \cdot 48)\\
6 &= -1 \cdot 48 + 3 \cdot 162 - 9 \cdot 48\\
6 &= 3 \cdot 162 - 10 \cdot 48 \qquad (VI)
\end{aligned}
$$

Substituindo (IV) em (VI), temos:

$$
\begin{aligned}
6 &= 3 \cdot 162 - 10\ (372 - 2 \cdot 162)\\
6 &= 3 \cdot 162 - 10 \cdot 372 + 20 \cdot 162\\
6 &= -10 \cdot 372 + 23 \cdot 162\ \ (VII)
\end{aligned}
$$

Escrevendo $mdc\,(372, 162) = 6$*, como combinação linear, fica:*

$$6 = 372 \cdot (-1) + 162 \cdot (23)$$

Utilizaremos tal método na resolução das equações Diofantinas lineares, no próximo capítulo.

Agora, veremos algumas proposições relacionadas ao m.d.c que nos auxiliarão na resolução das equações diofantinas quadráticas.

Corolário 1.4. *Sejam* a *e* b *inteiros não nulos e* k, m *e* n *números naturais.*

a) Se o $mdc\,(a,b)=1$*, então* $mdc\,(a^m,b^n)=1$.

b) Se $mdc\,(a,b)=1$ *e* $a\cdot b=k^n$*, então existem* $u,v\in\mathbb{Z}$ *tais que* $a=u^n$ *e* $b=v^n$.

Demonstração:

a) A demonstração do item $a)$, consiste numa aplicação direta da proposição 1.17, item $a)$. Se $mdc\,(a,c)=1$, então $mdc\,(a,bc)=mdc\,(a,b)$, onde b^{n-1} fará o papel de b e b fará o papel de c, com isso temos:

$mdc\,(a,b^n)=mdc\,(a,b^{n-1}\cdot b)$, como $mdc\,(a,b)=1$, pela proposição 1.17, temos que $mdc\,(a,b^{n-1}\cdot b)=mdc\,(a,b^{n-1})$, aplicando a proposição 1.17 sucessivamente ou segue por indução sobre n que:

$$mdc\,(a,b^n)=mdc\,(a,b)=1 \qquad \text{(I)}$$

Agora, utilizaremos o resultado acima para provar que $mdc\,(a^m,b^n)=1$.

Assim, $mdc\,(a^m,b^n)=mdc\,(a^{m-1}\cdot a,b^n)$, pela equação (I) o $mdc\,(a,b^n)=1$ e pela proposição 1.17 temos que $mdc\,(a^{m-1}\cdot a,b^n)=mdc\,(a^{m-1},b^n)$. Aplicando a proposição 1.17 sucessivamente ou segue por indução sobre m que:

$$mdc\,(a^m,b^n)=mdc\,(a,b^n)=1,$$

ou seja, se $mdc\,(a,b)=1$, isto implica que $mdc\,(a^m,b^n)=1$.

b) Sejam $u=mdc\,(a,k)$ e $v=mdc\,(b,k)$. Como $mdc\,(a,b)=1$ e $mdc\,(k^n,k)=k$, onde $k^n=a\cdot b$, substituindo temos:

$$k=mdc\,(k^n,k)=mdc\,(a\cdot b,k)$$

como $mdc\,(a,b)=1$, aplicando a proposição 1.17, item $c)$, temos:

$$mdc\,(a\cdot b,k)=mdc\,(a,k)\cdot mdc\,(b,k).$$

Como $u=mdc\,(q,k)$ e $v=mdc\,(b,k)$, substituindo temos:

$$mdc\,(a,k)\cdot mdc\,(b,k)=u\cdot v,$$

juntando todas as igualdades:

$$k=mdc\,(k^n,k)=mdc\,(a\cdot b,k)=mdc\,(a,k)\cdot mdc\,(b,k)=u\cdot v,$$

ou seja, $k = u \cdot v$. Com isso, temos que:

$$a \cdot b = k^n = u^n \cdot v^n$$

Agora, nosso objetivo é provar que $a = u^n$ e $b = v^n$, com isso temos:

i) Se $u \mid a$ e $mdc\,(a, b) = 1$, pela proposição 1.17, item b), temos que $mdc\,(u, b) = 1$. E pelo item anterior, se $mdc\,(u, b) = 1$, isso implica que $mdc\,(u^n, b) = 1$.

ii) Se $v \mid b$ e $mdc\,(a, b) = 1$, pela proposição 1.17, item b), temos que $mdc\,(v, a) = 1$ e pelo item anterior, se $mdc\,(v, a) = 1$, isso implica que $mdc\,(v^n, a) = 1$.

Por fim, como $a \cdot b = u^n \cdot v^n$, temos:

iii) $u^n \mid a \cdot b$, como $mdc\,(u^n, b) = 1$, pelo teorema 1.4, temos que $u^n \mid a$ e isto implica que $u^n \leq a$.

iv) $v^n \mid a \cdot b$, como $mdc\,(v^n, a) = 1$, pelo teorema 1.4, temos que $v^n \mid b$ e isto implica que $v^n \leq b$.

Mas, como $a \cdot b = u^n \cdot v^n$, e $u^n \leq a$, $v^n \leq b$, a única possibilidade é que sejam $a = u^n$ e $b = v^n$.

■

Corolário 1.5. *Todo quadrado perfeito:*

a) deixa resto 0 *ou* 1 *quando dividido por* 3.

b) deixa resto 0 *ou* 1 *quando dividido por* 4.

c) deixa resto 0, 1 *ou* 4 *quando dividido por* 8.

d) é da forma $5k$ *ou* $5k \pm 1$.

Demonstração:

a) Pelo algoritmo da divisão, o resto da divisão de n por 3 é $0, 1$ ou 2, de modo que n pode ser escrito como $n = 3q, n = 3q + 1$ ou $n = 3q + 2$, para algum $q \in \mathbb{Z}$. Com isso, temos:

$$\bullet \text{ Se } \; n = 3q \;\; \Rightarrow n^2 = (3q)^2 = 3 \,.\, 3q^2$$

$$\bullet \text{ Se } \quad n = 3q + 1 \Rightarrow n^2 = (3q+1)^2$$
$$= (3q)^2 + 2 \cdot 3q \cdot 1 + 1^2$$
$$= 3(3q^2 + 2q) + 1$$

$$\bullet \text{ Se } n = 3q + 2 \Rightarrow n^2 = (3q+2)^2$$
$$= (3q)^2 + 2 \cdot 3q \cdot 2 + 2^2$$
$$= 3 \cdot 3q^2 + 4 \cdot 3q + 4$$
$$= 3 \cdot 3q^2 + 4 \cdot 3q + 3 + 1$$
$$= 3(3q^2 + 4q + 1) + 1$$

No primeiro caso acima, n^2 deixa resto 0 quando dividido por 3 e nos outros dois casos, n^2 deixa resto 1 quando dividido por 2.

b) Novamente pelo algoritmo da divisão, o resto da divisão de n por 4 é $0, 1, 2$ ou 3, de modo que n pode ser escrito como $n = 4q$, $n = 4q + 1$, $n = 4q + 2$ ou $n = 4q + 3$, para algum q pertencente aos inteiros.

$$\bullet \text{ Se } n = 4q \Rightarrow n^2 = \ (4q)^2 = \ 4 \cdot 4q^2$$

$$\bullet \text{ Se } n = 4q + 1 \Rightarrow n^2 = (4q+1)^2$$
$$= (4q)^2 + 2 \cdot 4q \cdot 1 + 1^2$$
$$= 4 \cdot (4q^2 + 2q) + 1$$

$$\bullet \text{ Se } n = 4q + 2 \Rightarrow n^2 = (4q+2)^2$$
$$= (4q)^2 + 2 \cdot 4q \cdot 2 + 2^2$$
$$= 4 \cdot 4q^2 + 4 \cdot 4q + 4$$
$$= 4(4q^2 + 4q + 1)$$

$$\bullet \text{ Se } n = 4q + 3 \Rightarrow n^2 = (4q+3)^2$$
$$= (4q)^2 + 2 \cdot 4q \cdot 3 + 3^2$$
$$= 4 \cdot 4q^2 + 6 \cdot 4q + 9$$
$$= 4 \cdot 4q^2 + 4 \cdot 6q + 4 \cdot 2 + 1$$
$$= 4(4q^2 + 6q + 2) + 1$$

No primeiro e no terceiro caso, n^2 deixa resto 0 quando dividido por 4, e no segundo e quarto caso, deixa resto 1 quando dividido por 4.

c) Uma vez mais poderíamos utilizar o algoritmo da divisão, escrevendo $n = 8q + r$, para algum $q \in \mathbb{Z}$ e algum r pertencente ao conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$, demonstrando uma prova análoga ao do item $a)$. No entanto, pelo item $b)$, temos que:

• Se $n = 2q$, então $n^2 = 4q^2$. Há, agora, duas possibilidades:

1) Se q^2 for par, então $q^2 = 2k$ para algum $k \in \mathbb{N}$. Então teríamos que $n^2 = 4 \cdot 2k \Rightarrow n^2 = 8k$.

2) Se q^2 é ímpar, então $q^2 = 2k+1$ para algum $k \in \mathbb{N}$. Então, teríamos $n^2 = 4 \cdot (2k+1) \Rightarrow n^2 = 8k + 4$.

$$\bullet \text{ Se } n = 2q + 1 \Rightarrow n^2 = (2q+1)^2 \Rightarrow n^2$$
$$= (2q)^2 + 2 \cdot (2q) \cdot 1 + 1^2$$
$$= 4q^2 + 4q + 1$$
$$= 4q(q+1) + 1$$

de sorte que o produto de dois números inteiros consecutivos $q \cdot (q+1)$ é par, temos que $q \cdot (q+1) = 2k$, para algum $k \in \mathbb{N}$, com isso temos que $n^2 = 4q(q+1) + 1 = 4 \cdot 2k + 1$, ou seja, $n^2 = 8k + 1$.

Por fim, os casos acima garantem que o resto da divisão de n^2 por 8 só podem ser iguais a $0, 1$ ou 4.

d) Pelo algoritmo da divisão, o resto da divisão de n por 5 é $0, 1, 2, 3$ ou 4, de modo que n pode ser escrito como $n = 5q$, $n = 5q + 1$, $n = 5q + 2$, $n = 5q + 3$ ou $n = 5q + 4$, para algum $q \in \mathbb{Z}$. Com isso, temos:

$$\bullet \text{ Se } n = 5q \Rightarrow n^2 = (5q)^2 \Rightarrow n^2 = 5(5q^2)$$

- Se $n = 5q + 1 \Rightarrow n^2 = (5q + 1)^2$
$$= (5q)^2 + 2 \cdot 5q \cdot 1 + 1^2$$
$$= 5(5q^2 + 2q) + 1$$

- Se $n = 5q + 2 \Rightarrow n^2 = (5q + 2)^2$
$$= (5q)^2 + 2 \cdot 5q \cdot 2 + 2^2$$
$$= 5(5q^2) + 5 \cdot 4q + 4$$
$$= 5(5q^2) + 5 \cdot 4q + 4 + (1 - 1)$$
$$= 5(5q^2 + \cdot 4q + 1) - 1$$

- Se $n = 5q + 3 \Rightarrow n^2 = (5q + 3)^2$
$$= (5q)^2 + 2 \cdot 5q \cdot 3 + 3^2$$
$$= 5(5q^2) + 5 \cdot (6q) + 9$$
$$= 5(5q^2) + 5 \cdot 6q + 9 + (1 - 1)$$
$$= 5(5q^2 + \cdot 6q + 2) - 1$$

- Se $n = 5q + 4 \Rightarrow n^2 = (5q + 4)^2$
$$= (5q)^2 + 2 \cdot 5q \cdot 4 + 4^2$$
$$= 5(5q^2) + 5 \cdot (8q) + 16$$
$$= 5(5q^2 + 8q + 3) + 1$$

Com isso, podemos concluir que todo quadrado é da forma $5k$ ou $5k \pm 1$.

■

1.4 Mínimo Múltiplo Comum

Dizemos que um número inteiro é um múltiplo comum, de dois números inteiros dados, se ele é simultaneamente múltiplo de ambos os números.

Exemplo 1.16. *Quais são os múltiplos de* 2 *e* 3*?*

Múltiplos de 2*:*
$..., -6, -4, -2, 0, 2, 4, 6, ...$*, ou seja, números da forma* $2n$*, onde* $N \in \mathbb{Z}$*.*

Múltiplos de 3*:*
$..., -12, -9, -6, -3, 0, 3, 6, 9, 12, ...$*, ou seja, números da forma* $3n$*, onde* $N \in \mathbb{Z}$*.*

Múltiplos comuns de 2 *e* 3*:*
$..., -12, -6, 0, 6, 12, ...$*, ou seja, números da forma* $6n$*, onde* $N \in \mathbb{Z}$

Dentre os múltiplos comuns, é lógico se pensar, qual é o menor múltiplo comum de 3 e 6. Com isso definiremos o conceito de Mínimo Múltiplo Comum (MMC).

Definição 1.4. $\Rightarrow$ *Dados inteiros não nulos* $a_1, a_2, ..., a_n$*, o Mínimo Múltiplo Comum, de* $a_1, a_2, ..., a_n$*, denotado por* $mmc\,(a_1, a_2, ..., a_n)$*, é menor dentre todos os múltiplos positivos comuns de* $a_1, a_2, ..., a_n$*.*

Exemplo 1.17.

a) $mmc\,(4, 12) = 12$*, pois* 12 *é o menor múltiplo positivo de* 4 *e* 12*, ou seja:*

Múltiplo de 4*:*

$$..., -12, -8, -4, 0, 4, 8, 12, ...$$

Múltiplo de 12*:*

$$..., -24, -12, 0, 12, 24, ...$$

Múltiplos Comuns de 4 *e* 12*:*

$$..., -24, -12, 0, 12, 24, ...$$

Mínimo Múltiplo Comum, pela definição é o menor múltiplo positivo, ou seja, $m.m.c = 12$*.*

b) $mmc\,(4, 5) = 20$*, pois:*

Múltiplo de 4*:*

$$..., -20, -16, -12, -8, -4, 0, 4, 8, 12, 16, 20, ...$$

Múltiplo de 5*:*

$$..., -20, -15, -10, -5, 0, 5, 10, 15, 20, ...$$

Múltiplos Comuns de 4 *e* 5*:*

$$..., -20, 0, 20, ...$$

Mínimo Múltiplo Comum, pela definição é o menor múltiplo positivo, ou seja, $mmc\,(4, 5) = 20$.

Proposição 1.19. *Sejam* $a_1, a_2, ..., a_n \in \mathbb{Z}$ *e* $m = mmc\,(a_1, a_2, ..., a_n)$. *Para todo inteiro* n*, temos que* n *é um múltiplo comum de* $a_1, a_2, ..., a_n$ *se , e só se,* $m|n$.

Demonstração: ($\Longrightarrow$) Seja n um múltiplo comum de $a_1, a_2, ..., a_n$, ou seja, $a_1, a_2, ..., a_n|n$, queremos provar que $m|n$.

Como ainda não podemos afirmar tal caso, pelo Teorema 1.1, podemos escrever que $n = m \cdot q + r$, com $0 \leq r < m$, podemos reescrever tal equação como $r = n - m \cdot q$, como m é o Mínimo Múltiplo Comum de $a_1, a_2, ..., a_n$, temos que: $a_1|m$, pela Proposição 1.4, $a_1|m \cdot q$, como $a_1|n$, pela Proposição 1.6, $a_1|(n - m \cdot q)$, ou seja, $a_1|r$. Analogamente temos que $a_2, ..., a_n|r$, o que demonstra que r também é um múltiplo comum mas, como $0 \leq r < m$, a única possibilidade que nos resta é ter $r = 0$, com isso temos:

$$n = m \cdot q + r \Rightarrow n = m \cdot q + 0 \Rightarrow n = m \cdot q \Rightarrow m|n.$$

■

Lema 1.2. *Sejam* $a_1, a_2, ..., a_n$ *inteiros não nulos. Se* $k \in \mathbb{N}$*, então* $mmc\,(ka_1, ka_2, ..., ka_n) = k \cdot mmc\,(a_1, a_2, ..., a_n)$.

Demonstração: Seja $m = mmc\,(ka_1, ka_2, ..., ka_n)$ e $n = mmc\,(a_1, a_2, ..., a_n)$, se multiplicarmos n por k, $kn = mmc\,(ka_1, ka_2, ..., ka_n)$, teremos que kn é um múltiplo de $ka_1, ka_2, ..., ka_n$, com isso temos que $kn \geq m$, pois m é o Mínimo Múltiplo Comum de $ka_1, ka_2, ..., ka_n$, ou seja, qualquer múltiplo positivo desses elementos é maior ou igual a m. Por outro lado, como m é um múltiplo comum de $ka_1, ka_2, ..., ka_n$, segue que $\dfrac{m}{k}$ é um múltiplo de $a_1, a_2, ..., a_n$, ou seja, $\dfrac{m}{k} \geq n$, ou ainda, que $m \geq k \cdot n$. Logo, pela Proposição 1.8, $m = k \cdot n$.

■

Lema 1.3. *Se* $mdc\,(a,b)=1$*, então o* $mmc\,(a,b)=|a\cdot b|$

Demonstração: Seja m um múltiplo positivo comum de a e b, temos que $a|m$ e $b|m$. Pelo Corolário 1.2, se $a|m$ e $b|m$ isso implica que $\dfrac{a\cdot b}{mdc\,(a,b)}|m$, mas como $mdc\,(a,b)=1$. temos que $\dfrac{a\cdot b}{1}|m$, ou seja $a\cdot b|m$. Por tanto, pela Proposição 1.7, temos que se, $a\cdot b|m$ isso implica que $|a\cdot b|\leq m$, de forma que $|a\cdot b|$ é o menor múltiplo positivo comum de a e b, ou seja, $mmc\,(a,b)=|a\cdot b|$

■

Teorema 1.6. *Se* a *e* b *são inteiros não nulos, então:*

$$mmc\,(a,b)\cdot mdc\,(a,b)=|a\cdot b|$$

Demonstração: Seja $m=mmc\,(a,b)$ e $d=mdc\,(a,b)$, como $d=mdc\,(a,b)$, temos que :

- $d|a\Rightarrow a=k_1\cdot d\Rightarrow \dfrac{a}{d}=k_1$, $k_1\in\mathbb{Z}$
- $d|b\Rightarrow b=k_2\cdot d\Rightarrow \dfrac{b}{d}=k_2$, $k_2\in\mathbb{Z}$

Pelo Corolário 1.1, temos que $mdc\,(\dfrac{a}{d},\dfrac{b}{d})=1$, ou seja, $mdc\,(k_1,k_2)=1$, e pelo lema 1.3, se $mdc\,(k_1,k_2)=1$ isso implica que $mdc\,(k_1,k_2)=|k_1\cdot k_2|$ com isso construímos todas as ferramentas necessárias para finalizar a demonstração, substituindo os valores temos: $mmc\,(a,b)=mmc\,(k_1\cdot d,k_2\cdot d)$, pelo Lema1.2, temos que

$$mmc\,(k_1\cdot d,k_2\cdot d)=d\cdot mmc\,(k_1,k_2),$$

como $mmc\,(k_1,k_2)=|k_1\cdot k_2|$, segue que,

$$mmc\,(a,b)=mmc\,(k_1\cdot d,k_2\cdot d)=d\cdot mmc\,(k_1,k_2)=d\cdot|k_1\cdot k_2|,$$

substituindo os dados em $mmc\,(a,b)\cdot mdc\,(a,b)=d\cdot|k_1\cdot k_2|\cdot mdc\,(a,b)=d\cdot|k_1\cdot k_2|\cdot d=|d\cdot k_1|\cdot|d\cdot k_2|=|a|\cdot|b|=|a\cdot b|$

■

Proposição 1.20. *Sejam* $a_1,...,a_n$ *números inteiros não nulos. Então existe o número* $m=mmc\,(a_1,a_2,...,a_n)$ *e* $mmc\,(a_1,a_2,...,a_n)=mmc\,(a_1,...,mmc\,(a_{n-1},an))$.

Demonstração: Basta provar que, se existe $mmc\,(a_1,...,mmc\,(a_{n-1},a_n))$ vale a igualdade acima. Utilizaremos o mesmo raciocínio utilizando na demonstração da existência do m.d.c, ou seja, provaremos por indução.

Seja $m=mmc\,(a_1,a_2,...,mmc\,(a_{n-1},a_n))$, com isso concluímos que $a_1,a_2,...,a_{n-2}|m$ e $mmc\,(a_{n-1},a_n)|m$. Já que $a_{n-1}|mmc\,(a_{n-1},a_n)$ e $a_n|mmc\,(a_{n-1},a_n)$, chegamos a conclusão de que m é um múltiplo comum de $a_1,...,a_n$.

Por outro lado, suponhamos que n seja um múltiplo comum de $a_1,...,a_n$, com isso temos que $a_1,a_2,...,a_n|n$ e $mmc\,(a_{n-1},a_n)|n$; daí segue que n é um múltiplo de

$$m = mmc\,(a_1, ..., mmc\,(a_{n-1}, a_n)).$$

■

1.5 Números Primos

Neste tópico faremos uma breve síntese sobre o estudo dos números primos, um dos conceitos mais importante da matemática. Esses números desempenham papel fundamental e a eles estão associados muitos problemas famosos cujas as soluções têm resistido aos esforços de várias gerações de matemáticos.

Definição 1.5. *Um inteiro $p > 1$ é primo de seus únicos divisores positivos forem 1 e p. Um inteiro $a > 1$ que não é primo é dito composto.*

Proposição 1.21. *Dados dois números primos p e q e um número a qualquer, decorre da definição os seguintes fatos:*

a) Se $p|q$, então $p = q$

b) Se $p \nmid a$, então $mdc\,(p, a) = 1$

Demonstração:

a) De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Como p é primo, por definição temos que $p > 1$, logo só nos resta que $p = q$.

b) De fato, se $mdc(a, p) = d$, temos que $d|a$ e $d|p$. Como $d|p$, temos que $d = 1$ ou $d|p$, pelo caso a), temos que $p = 1$, pois $p \nmid a$, portanto $d = 1$.

■

Lema 1.4. *Todo inteiro $n > 1$ pode ser expresso como o produto de um número finito de primos, não necessariamente distintos.*

Demonstração: Faremos a prova por indução sobre n.

i) Caso base:

Se $n = 2$, não a nada a fazer pois, 2 é primo.

ii) Hipótese de indução:

Suponhamos que agora que todo inteiro n tal que $2 \leq n < m$ pode ser escrito como o produto de um número finito de primos:

$iii)$ Tese:

Queremos demostrar que m também pode ser escrito como produto finito de primos:

Se m for primo, não há nada a fazer. caso m seja composto, existem inteiros a e b tais que $m = a \cdot b$, com $1 < a < m$ e $1 < b < m$, como produto de números finitos de primos, ou seja:

$a = p_1 \cdot p_2 ... p_k$ e $b = q_1 \cdot q_2 ... q_l$, com $k, l \geq 1$. Logo, $m = a \cdot b = (p_1 \cdot p_2 ... p_k) \cdot (q_1 \cdot q_2 ... q_l)$ que também é um produto de números finitos de primos.

■

Como corolário do lema anterior, temos o seguinte critério de pesquisa de divisores primos de um número composto, devido ao matemático grego Eratóstenes de Cirene.

Corolário 1.6. *(Crivo de Eratóstenes)*
Se um inteiro $n > 1$ for composto, então n possui um divisor primo p, tal que $p \leq \sqrt{n}$.

Demonstração: Seja $n = a \cdot b$, sem perca de generalidade definimos $1 < a = b$. Sendo p um divisor primo de a, temos:

Se $p|a$, pela Proposição 1.7, temos que $p \leq a$ e pela, Proposição 1.4, se $p|a$ então $p|a \cdot b$, ou seja, $p|n$.

Com isso obtemos o seguinte:

Se $p \leq a$, então $p^2 \leq a^2$

Se $a \leq b$, multiplicando ambos os membros da desigualdade por a, temos: $a^2 \leq a \cdot b$, ou seja, $a^2 \leq n$.

Por transitividade, temos:

se $p^2 \leq a^2$ e $a^2 \leq n \implies p^2 \leq n \implies p \leq \sqrt{n}$.

■

Proposição 1.22 (Lema de Euclides)**.** *Sejam $a, b, p \in \mathbb{Z}$, com p primo, se $p|a \cdot b$, então $p|a$ ou $p|b$.*

Demonstração:

Se $p \nmid a$ e $p|a \cdot b$, pelo Teorema 1.4 (Lema de Gauss), temos que $p|b$.

Se $p \nmid b$ e $p|a \cdot b$, pelo Teorema 1.4 (lema de Gauss), temos que $p|a$.

■

Exemplo 1.18. *Use o corolário acima para provar que 641 é primo.*
Prova: *Inicialmente, note que $25 < \sqrt{641} < 26$. Por tanto, se 641 for composto, segue do Corolário 1.4, que 641 deve possuir um divisor primo $p < 25$, de modo que*

$$p \in (2, 3, 5, 7, 11, 13, 17, 19, 23).$$

No entanto, é imediato verificar que, dentre as divisões de 641 *pelos primos acima, nenhuma é exata. Logo, 641 é primo.*

Teorema 1.7 (Demonstração Euclides)**.** *O conjunto dos números primos é infinito.*

Demonstração: Por indução sobre n, provaremos que, se $\mathbb{N}$ contiver n primos distintos, então $\mathbb{N}$ conterá $n+1$ primos distintos.

Suponhamos que $p_1, ..., p_n$ são primos distintos, e seja $m = p_1 \cdots p_n + 1$, ou seja, m é o sucessor do produto de todos os primos. Pelo Lema 1.5, existe um primo p tal que $p|m$. Se $p = p_i$ para algum $1 < i < n$, então $p|p_1 \cdots p_n$. De $m = p_1 \cdots p_n + 1$ segue que $m - (p_1 \cdots p_n) = 1$, como $p|m$ e $p|p_1 \cdots p_n$, pela Proposição 1.6, temos que $p|[m - (p_1 \cdots p_n)]$, ou seja, $p|1$, o que é um absurdo. Logo, p é um primo diferente de todos os p_i's, de maneira que temos pelo menos $n+1$ primos distintos em $\mathbb{N}$.

■

Lema 1.5. *Se* $a_1, ..., a_n \in \mathbb{N}$ *e* p *é um primo tal que* $p|a_1 \cdot a_2 \cdots a_n$*, então existe* $1 \leq i \leq n$*, tal que* $p|a_i$*. Em particular, se* $a_1, ..., a_n$ *forem todos primos, então existe* $1 \leq i \leq n$ *tal que* $p = a_i$*.*

Demonstração:

$i)$ Caso base: Para $n = 2$

$p|a_1 \cdot a_2$, pela Proposição 1.22, $p|a_1$ ou $p|a_2$.

$ii)$ Hipótese de indução: Suponhamos que $p|a_1 \cdots a_n$, $\forall_n \in \mathbb{N}$.

$iii)$ Tese: Queremos demonstrar que $p|a_1 \cdots a_{n+1}$

Pela Hipótese de indução temos que $p|a_1 \cdots a_n$ e pela Proposição 1.4, se $p|a_1 \cdots a_n$ então $p|a_1 \cdots a_{n+1}$ e pela Proposição 1.22, se $p|a_1 \cdots a_{n+1}$ então $p|a_1$ ou $p|a_2$ ou $p|a_{n+1}$. Em especial se todos forem primos ,pela Proposição 1.21, item a), se $p|a_i$ então $p = a_i$.

■

Teorema 1.8 (Teorema fundamental da Aritmética)**.** *Todo inteiro maior do que* 1 *pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração: Se n é primo não há nada a ser demonstrado. Suponhamos pois, n composto. Seja p_1 $(p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário existiria $p, 1 < p < p_1$ com $p|n$, contradizendo a escolha de p_1. Logo, $n = p_1 \cdot n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 \cdot p_2 \cdot n_2$.

Repetindo este procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, ..., n_r$. Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, ..., p_k$ não são, necessariamente distintos, n terá, em geral, a forma: $n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} ... p_k^{\alpha k}$.

Para mostrarmos a unicidade usaremos indução sobre n. [segundo caso de indução]

$i)$ Caso base:

Para $n = 2$ a afirmação é verdadeira.

$ii)$ Hipótese de indução:

Suponhamos que ele é valida para todos os inteiros maiores do que 1 e menores do que n.

$iii)$ Tese:

Queremos demonstrar que ela também é valida para n.

Se n é primo, não há nada á provar. Vamos supor, então que n seja composto e que tenha duas fatorações, isto é:

$$n = p_1 \cdot p_2 \cdots p_b = q_1 \cdot q_2 \cdots q_r$$

Vamos provar que $b = r$ e que cada p_i é igual a algum q_j. Como o p_1 divide o produto $q_1, q_2, ..., q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 | q_1$. Como são ambos primos, pela Proposição 1.21, item a), temos que $p_1 = q_1$. Logo $\dfrac{n}{p_1} = p_2 \cdots p_b = q_2 \cdots q_r$. Como $1 < \dfrac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $b = r$ e , a menor da ordem $p_1, p_2, ..., p_b$ e $q_1, q_2, ..., q_b$ são iguais.

■

1.6 Congruência Módulo m

Neste tópico estudaremos a relação de Congruência, que consiste nos estudos dos restos. Dois números a e b são ditos Congruentes entre si, se possuírem o mesmo resto. Grande parte dos resultados sobre Congruência foi introduzidos por Gauss $(1777 - 1855)$ em um trabalho publicado em 1801 (Disquisitiones Arithmeticae) quando tinha 24 anos. Várias ideias de grande importância, que serviram de base para o desenvolvimento da teoria dos números, até mesmo a notação, lá introduzida, são as mesmas que utilizamos nos dias de hoje.

Uma pessoa não familiarizada com o tópico, pode se perguntar, qual a vantagem de usar uma notação (Congruência Módulo m) que só enxerga o resto da divisão de um número por m?

Existem muitas vantagens, uma delas é o ganho computacional, mas não é o foco desse trabalho. Nosso foco é, por exemplo, calcular mecanicamente e rápido o resto da divisão de

17^{2002} por 13, tarefa que não é fácil cumprir com os métodos dos quais dispomos até o presente momento. A seguir, provaremos algumas propriedades elementares de Congruências Módulo m, que nos ajudarão a resolver problemas como o citado acima e nos auxiliarão no desenvolvimento do restante dessa dissertação.

Definição 1.6. *Sejam a e b em inteiros dados, sendo $m > 1$, dizemos que a é congruente a b, módulo m, e denotamos por $a \equiv b \ (mod\ m)$, se $m|(a-b)$. Se a não for congruente a b módulo m, denotamos por $a \not\equiv b \ (mod\ m)$.*

Exemplo 1.19. *De acordo com a definição acima, podemos escrever:*

a) $3 \equiv 5 \ (mod\ 2)$, *pois* $2|(3-5)$, *ou seja,* 3 *e* 5 *deixa o mesmo resto na divisão por* 2.

b) $-1 \equiv 11 \ (mod\ 12)$, *pois* $12|(-1-11)$, *ou seja,* -1 *e* 11 *deixa o mesmo resto na divisão por* 12.

c) $2 \equiv -1 \ (mod\ 3)$, *pois* $3|(2-(-1))$, *ou seja,* 2 *e* -1 *deixa o mesmo resto na divisão por* 3.

d) $x \equiv -x \ (mod\ 2)$, *pois* $2|(x-(-x))$, *ou seja,* x *e* $-x$ *deixa o mesmo resto na divisão por* 2.

e) $1 \not\equiv 2 \ (mod\ 3)$, *pois* $3 \nmid |(1-2)$, *ou seja,* 1 *e* 2 *não deixam o mesmo resto na divisão por* 3.

f) $20 \not\equiv 15 \ (mod\ 7)$, *pois* $7 \nmid |(20-15)$, *ou seja,* 20 *e* 15 *não deixam o mesmo resto na divisão por* 7.

Com isso podemos levantar os seguintes questionamentos: *O que estamos realmente investigando em um número quando consideramos congruências módulo m?* Para responder essa pergunta, observamos o que ocorre com os números inteiros módulo 4, por exemplo:

$$4k \equiv 0 \ (mod\ 4)$$
$$4k+1 \equiv 1 \ (mod\ 4)$$
$$4k+2 \equiv 2 \ (mod\ 4)$$
$$4k+3 \equiv 3 \ (mod\ 4)$$

Assim, a sequência $..., -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...$, dos números inteiros é igual, a sequência abaixo, módulo 4:

$$..., 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, ...$$

E vemos que todo inteiro é congruente a esses resultados módulo 4, ou seja, que todo inteiro possui resto $0, 1, 2,$ e 3 na divisão por 4, esse resultado continua válido em geral, conforme veremos posteriormente.

Proposição 1.23. *Dados os inteiros a, b, c e m, sendo que $m > 1$, temos:*

a) Reflexiva

$a \equiv a \ (mod \ m)$

b) Simétrica

$a \equiv b \ (mod \ m) \Rightarrow b \equiv a \ (modm)$

c) Transitiva

$a \equiv b \ (mod \ m)$ *e* $b \equiv c \ (mod \ m) \Rightarrow a \equiv c \ (mod \ m)$.

Demonstração:

a) Se $a \equiv a \ (mod \ m)$ então $m|(a - a)$, ou seja, $m|0$ que nos é garantido pela proposição 1.1, item a).

b) Se $a \equiv b \ (mod \ m)$ então $m|(a - b)$, e daí, $m| - (a - b)$, isto é, $m|(b - a)$. Portanto, $b \equiv a \ (mod \ m)$.

c) Se $a \equiv b \ (mod \ m)$ por definição temos que $m|a - b$, isso implica que $a - b = k_1 \cdot m$ (I), onde $k_1 \in \mathbb{Z}$.

Se $b \equiv c \ (mod \ m)$ por definição temos que $m|b - c$ e isso implica que $b - c = k_2 \cdot m$ (II), onde $k_2 \in \mathbb{Z}$.

Somando a equação (I) e a equação (II), temos:

$$\begin{cases} a - b = k_1 \cdot m \\ b - c = k_2 \cdot m \end{cases} \Longrightarrow (a - b) + (b - c) = k_1 \cdot m + k_2 \cdot m$$

Daí segue naturalmente que $a - b + b - c = (k_1 + k_2) \cdot m \Rightarrow a - c = (k_1 + k_2) \cdot m$, e como $(k_1 + k_2) = k \in \mathbb{Z}$, temos que $a - c = k \cdot m$. Logo

$$m|(a - c) \text{ e, portanto, } a \equiv c \ (mod \ m).$$

■

Para verificar se dois números são congruentes módulos m, não é necessário efetuar a divisão Euclidiana de ambos por m para depois comparar seus restos. Basta aplicar a seguinte proposição.

Proposição 1.24. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a = b \ mod \ m$ se, e somente se, $m|a - b$.*

Demonstração: ($\Longrightarrow$) Dado $a, b \in \mathbb{Z}$, pelo algoritmo da divisão de Euclides, Teorema 1.1 ao dividirmos a e b por m, temos:

$a = m \cdot q_1 + r_1$, com $0 \leq r_1 < q_1$. (I)

$b = m \cdot q_2 + r_2$, com $0 \leq r_2 < q_2$. (II)

Ao subtrairmos a equação (I) menos a equação (II), temos:

$$a - b = (m \cdot q_1 + r_1) - (m \cdot q_2 + r_2) \implies a - b = m(q_1 - q_2) + (r_1 - r_2),$$

onde m só vai dividir $a - b$, se somente se, $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$, é equivalente dizer que $m|a - b$, já que $|r_1 - r_2| < m$, o que nos é garantido pelo Teorema 1.1.

($\Longleftarrow$) A recíproca é mais direto. Se $m|(a - b)$ então $a - b = m \cdot q$, isto é, $a \equiv b \; mod \; m$.

■

OBS.: Na definição de congruência, a razão pela qual é excluído o módulo $m = 1$, é porque se usássemos congruência módulo 1, obteríamos $a \equiv b \; (mod \; 1)$, como sinônimo de $1|(a - b)$, que é sempre verdade, ou seja, não faz muito sentido, pois dois inteiros quaisquer seriam indistinguíveis módulo 1.

O que torna útil e poderosa a noção de congruência é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 1.25. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$*

a) Se $a \equiv b \; (mod \; m)$ e $c \equiv d \; (mod \; m)$, então $a + c \equiv b + d \; (mod \; m)$ [compatibilidade com a adição].

b) Se $a \equiv b \; (mod \; m)$ e $c \equiv d \; (mod \; m)$, então $a \cdot c \equiv b \cdot d \; (mod \; m)$ [compatibilidade com o produto].

Demonstração:

a) $a \equiv b \; (mod \; m) \Rightarrow m|(a-b) \Rightarrow a - b = k_1 \cdot m$, onde $k_1 \in \mathbb{Z}$. (I)

$c \equiv d \; (mod \; m) \Rightarrow m|(c-d) \Rightarrow c - d = k_2 \cdot m$, onde $k_2 \in \mathbb{Z}$, (II)

Somando a equação (I) e a equação (II), temos:

$$a - b + c - d = k_1 \cdot m + k_2 \cdot m \Rightarrow (a + c) - (b + d) = (k_1 + k_2) \cdot m,$$

onde $k_1 + k_2 = k \in \mathbb{Z}$.

Com isso $(a + c) - (b + d) = k \cdot m$, logo $m|(a + c) - (b + d)$, portanto, da definição de congruência, temos que $a + c \equiv b + d \; (mod \; m)$.

b) $a \equiv b \ (mod \ m) \Rightarrow m|a-b \Rightarrow a-b = k_1 \cdot m$, onde $k_1 \in \mathbb{Z}$. Tomando $c \in \mathbb{Z}$ e multiplicando ambos os membros da equação, obtemos $ac - bc = k_1 \cdot c \cdot m$ (I)

$c \equiv d \ (mod \ m) \Rightarrow m|c-d \Rightarrow c-d = k_2 \cdot m$, onde $k_2 \in \mathbb{Z}$. Tomando $b \in \mathbb{Z}$ e multiplicando ambos os membros da equação, obtemos $bc - bd = k_2 \cdot b \cdot m$ (II)

Somando as equações (I) e (II), temos:

$$ac + bc - bc - bd = k_1 \cdot c \cdot m + k_2 \cdot b \cdot m \Rightarrow ac - bd = (k_1 \cdot c + k_2 \cdot b) \cdot m,$$

onde $(k_1 \cdot c + k_2 \cdot b) = k \in \mathbb{Z}$, logo, $ac - bd = k \cdot m \Rightarrow m|ac - bd$, portanto, temos que $a \cdot c \equiv b \cdot d \ (mod \ m)$.

■

Corolário 1.7. *Para todos $n \in \mathbb{N}, a, b \in \mathbb{Z}$, se $a \equiv b \ (mod \ m)$, então tem-se que $a^n \equiv b^n \ (mod \ m)$*

Demonstração: Iremos provar esse corolário por indução sobre n.

$i)$ Caso base: Para $n = 1$

$a^1 \equiv b^1 \ (mod \ m) \Longrightarrow m|a-b$, que é verdade por definição.

$ii)$ Hipótese de indução: Suponhamos que $a^n \equiv b^n \ mod \ m$, ou seja, $m|a^n - b^n$, $\forall n \in \mathbb{N}$.

$iii)$ Tese: Queremos demonstrar que se $m|a^{n+1} - b^{n+1}$ isso implica que $a^{n+1} \equiv b^{n+1} \ mod \ m$, com isso temos:

$$\begin{aligned} a^{n+1} - b^{n+1} = a^n \cdot a - b^n \cdot b &= a^n \cdot a - b^n \cdot b + (a \cdot b^n - a \cdot b^n) \\ &= (a^n \cdot a - a \cdot b^n) + (a \cdot b^n - b^n \cdot b) \\ &= a(a^n - b^n) + b^n(a-b) \end{aligned}$$

Como $m|a-b$, pelo caso base e $m|a^n - b^n$, por hipótese de indução, decorre da igualdade acima e da proposição 2.6 que $m|a^{n+1} - b^{n+1}$, ou seja, $a^{n+1} \equiv b^{n+1} \ mod \ m$ estabelecendo o resultado para todo $n \in \mathbb{N}$.

■

OBS.: Adicionamos $(a \cdot b^n - a \cdot b^n) = 0$, para facilitar o manejo das operações algébricas na demonstração.

Proposição 1.26. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. tem-se que:*

$$a + c \equiv b + c \mod m \iff a \equiv b \mod m$$

Demonstração: ($\Longrightarrow$) $a+b \equiv b+c \mod m \Rightarrow m|(a+c)-(b+c) \Rightarrow m|a+c-b-c \Rightarrow m|a-b$, logo $a \equiv b \mod m$.

($\Longleftarrow$) $a \equiv b \; mod \; m \Rightarrow m|a-b \Rightarrow m|(a-b)+(c-c) \Rightarrow m|(a+c)-(b+c)$, logo $a+c \equiv b+c \; mod \; m$.

■

OBS.: A proposição acima nos diz que, para as congruências, vale os cancelamentos com relação a adição. Com relação a multiplicação é necessário mais alguns detalhes, que veremos a seguir.

Proposição 1.27. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos:*

$$ac \equiv bc \; mod \; m \iff a \equiv b \; mod \; \frac{m}{mdc(c,m)}$$

Demonstração: Chamaremos de $d = mdc\,(c,m)$ e pelo corolário 1.1 temos que $mdc\left(\frac{c}{d}, \frac{m}{d}\right) = 1$, com isso temos:

($\Longrightarrow$) $ac \equiv bc \mod m \Rightarrow m|ac-bc \Rightarrow m|(a-b)\cdot c \Rightarrow (a-b)\cdot c = k \cdot m$, onde $k \in \mathbb{Z}$. Dividimos por d ambos os lados da igualdade da seguinte maneira:

$$(a-b)\cdot \frac{c}{d} = k \cdot \frac{m}{d}$$

pelo Teorema 1.4 (Lema de Gauss) se

$$mdc\left(\frac{c}{d}, \frac{m}{d}\right) = 1 \text{ e } \frac{m}{d}|(a-b)\cdot\frac{c}{d} \text{ então } \frac{m}{d}|a-b, \text{ logo } a \equiv b \mod \frac{m}{d}.$$

($\Longleftarrow$) $a \equiv b \mod \frac{m}{d} \Rightarrow \frac{m}{d} \;\Big|\; (a-b) \Rightarrow a-b = k \cdot \frac{m}{d}$, onde $k \in \mathbb{Z}$
multiplicamos ambos os lados da equação por $c \in \mathbb{Z}$. De onde segue que

$$(a-b)\cdot c = k \cdot \frac{m}{d}\cdot c \implies ac-bc = \frac{k}{d}\cdot c \cdot m,$$

onde $\frac{k}{d}\cdot c = q \in \mathbb{Z}$, isso implica que $ac-bc = q\cdot m \Rightarrow m|ac-bc$, logo $ac \equiv bc \; mod \; m$, ou seja,

$$a \equiv b \mod \frac{m}{mdc(c,m)}.$$

■

Proposição 1.28. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $mdc\,(c,m) = 1$. temos que:*

$$ac \equiv bc \mod m \iff a \equiv b \mod m$$

Demonstração: ($\Longrightarrow$) Suponhamos $ac \equiv bc \mod m \Rightarrow m|ac - bc \Rightarrow m|(a-b)\cdot c$, pelo Teorema 1.4 (Lema de Gauss), temos que se $mdc\,(c,m) = 1$ e $m|(a-b)\cdot c \Rightarrow m|a-c$, que por definição de congruência, temos que $a \equiv b\ mod\ m$.

($\Longleftarrow$) Reciprocamente se $a \equiv b \mod m \Rightarrow m|(a-b) \Rightarrow a - b = k_1 \cdot m$, onde $k_1 \in \mathbb{Z}$. Ao multiplicarmos ambos os lados da igualdade por c, temos:

$$c\cdot(a-b) = c\cdot k_1 \cdot m \Longrightarrow ac - bc = c\cdot k_1 \cdot m,$$

onde $k_1 \cdot c = k \in \mathbb{Z}$, com isso obtemos $ac - bc = k\cdot m \Rightarrow m|ac-bc$, e consequentemente $ac \equiv bc \mod m$.

■

Proposição 1.29. *Sejam $a, k, m \in \mathbb{Z}$, com $m > 1$ e $mdc\ (k,m) = 1$. Se $a_1, a_2, ..., a_m$ é um sistema completo de resíduos módulo m, então:*

$$a + ka_1, a + ka_2, ..., a + ka_m$$

Também é um sistema completo de resíduos módulos m.

Demonstração: Para todo $i, j = 0, 1, 2, ..., m-1$, aplicando a Proposição 1.26, temos que $a + kai \equiv a + kaj\ mod\ m \Longleftrightarrow kai \equiv kaj\ mod\ m$ e pela Proposição 1.28, temos que $kai \equiv kaj\ mod\ m \Longleftrightarrow ai \equiv aj\ mod\ m \Longleftrightarrow i = j$.

Isso mostra que $a + ka_1, a + ka_2, ..., a + ka_m$ são, dois a dois, não congruentes módulo m e, por tanto, formam um sistema completo de resíduos módulos m.

■

A seguir demonstraremos, algumas propriedades adicionais das congruências relacionadas com o produto, que nos auxiliarão no decorrer do trabalho.

Proposição 1.30. *Sejam $a, b \in \mathbb{Z}$ e $m, n, m_1, ..., m_r$ inteiros maiores que 1. Temos que:*

a) Se $a \equiv b\ mod\ m$ e $n|m$, então $a \equiv b\ mod\ n$

b) $a \equiv b\ mod\ m_i, \forall i = 1, 2, ..., m \Longleftrightarrow a \equiv b\ mod\ [mmc\,(m_1, m_2, ..., m_r)]$

c) Se $a \equiv b\ mod\ m$, então $mdc\,(a,m) = mdc\,(b,m)$

Demonstração:

a) Se $a \equiv b\ mod\ m \Rightarrow m|a-b \Rightarrow a - b = k_1 \cdot m$, onde $k_1 \in \mathbb{Z}$. (I)

Se $n|m \Rightarrow m = k_2 \cdot n$, onde $k_2 \in \mathbb{Z}$ (II)

Substituindo a equação (II) na equação (I), temos:

$a - b = k_1 \cdot m \Rightarrow a - b = k_1 \cdot k_2 \cdot n$, como $k_1 \cdot k_2 = k \in \mathbb{Z}$, temos que:

$a - b = k \cdot n \Rightarrow n|a-b$, que por definição de congruência, obtemos $a \equiv b\ mod\ n$.

b) ($\Longrightarrow$) Suponhamos que $a \equiv b \ mod \ m_i$, $i = 1, 2, ..., r$, então temos por definição que $m_i|a - b$, ou seja, $m_1, m_2, ..., m_r|a - b$. Sendo $a - b$ um múltiplo de cada mi, ou seja, um múltiplo de $m_1, m_2, ..., m_r$. Com isso podemos concluir que $a - b$ é um múltiplo do $mmc\,(m_1, m_2, ..., m_r)$, ou seja, $mmc\,(m_1, m_2, ..., m_r)|a - b$, logo por definição de congruência temos que $a \equiv b \ mod \ [mmc\,(m_1, m_2, ..., m_r)]$.

($\Longleftarrow$) A recíproca, consiste numa aplicação direta do item (a). Suponhamos que:

$$\begin{aligned} a \equiv b \ mod \ [mmc\,(m_1, m_2, ..., m_r)] &\Rightarrow mmc\,(m_1, m_2, ..., m_r)|(a - b) \\ &\Rightarrow m_1|(a - b), m_2|(a - b), ..., m_r|(a - b), \end{aligned}$$

ou seja, $m_i|(a - b)$, $i = 1, 2, ..., r$, então $a \equiv b \ mod \ m_i$.

c) Se $a \equiv b \ mod \ m$, então $m|a - b \Rightarrow a - b = k \cdot m$, onde $k \in \mathbb{Z}$. Podemos reescrever a equação como $a = b + km$. Logo, pelo lema 1.1, temos que:

$$mdc\,(b, m) = mdc\,(b + km, m) = mdc\,(a, m)$$

■

Exemplo 1.20 (ENQ-PROFMAT 2017.1)**.** *Sejam a, b, m números inteiros, com $m > 1$ e tais que $mdc\,(a, m) = 1$. Prove que $ax \equiv 1 \, mod \, m$ possui solução. Além disso mostre que se $x_1, x_2 \in \mathbb{Z}$ são soluções da congruência, então $x_1 \equiv x_2 \, mod \, m$.*

Solução:

i) Como $mdc\,(a, m) = 1$, pela proposição 1.16 existem inteiros (x, y), tais que $ax+my = 1$, aplicando a linguagem de congruência módulo m, temos:

$$ax \equiv 1 \, mod \, m$$

portanto x é solução.

ii) Se x_1 e x_2 são soluções, temos que:

Se, $ax_1 \equiv 1 \, mod \, m \Rightarrow m \mid ax_1 - 1$ (I)

Se, $ax_2 \equiv 1 \, mod \, m \Rightarrow m \mid ax_2 - 1$ (II)

Se $m \mid ax_1 - 1$ e $m \mid ax_2 - 1$, pela proposição 1.6 $m \mid (ax_1 - 1) - (ax_2 - 1) = ax_1 - 1 - ax_2 + 1 = ax_1 - ax_2 = a(x_1 - x_2)$, ou seja: $m \mid a(x_1 - x_2)$, como $mdc\,(a, m) = 1$, pelo Lema de Gauss, teorema 1.4, temos que $m \mid (x_1 - x_2)$, portanto por definição de congruência $x_1 \equiv x_2 \, mod \, m$.

Exemplo 1.21 (ENQ-PROFMAT 2019.1)**.** *Prove usando congruência que* $11^{n+2} + 12^{2n+1}$ *é divisível por* 133*, para qualquer número natural* n*.*

Solução: Para provar que $133 \mid 11^{n+2} + 12^{2n+1}$, temos que chegar ao resultado: $11^{n+2} + 12^{2n+1} \equiv 0\, mod\, 133$, com isso temos:

$$11^{n+2} + 12^{2n+1} = 11^n \cdot 11^2 + 12^{2n} \cdot 12 = 121 \cdot 11^n + (12^2)^n \cdot 12 = 121 \cdot 11^n + 144^n \cdot 12$$

Aplicando a congruência $mod\, 133$, temos:
$121 \cdot 11^n + 144^n \cdot 12 \equiv 121 \cdot 11^n + 11^n \cdot 12 \equiv (121 + 12) \cdot 11^n \equiv 133 \cdot 11^n \equiv 0\, mod\, 133.$

Exemplo 1.22 (OBMEP - 2011 N_2)**.** *Qual o resto da divisão de* $1 \cdot 2 \cdot 3 \cdots 2011 + 21$ *por* 8*?*

Solução: Podemos reescrever o produto da primeira parcela como

$$8 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 9 \cdots 2011 + 8 \cdot 2 + 5$$

Aplicando a linguagem de congruência temos:

$$(8 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 9 \cdots 2011) + (8 \cdot 2) + 5 \equiv 5 \text{ mod } 8$$

ou seja, o resto é 5.

Capítulo 2

Equações Diofantinas Lineares

Tais equações possuem esse nome em homenagem ao matemático grego *Diofanto de Alexandria*, do qual pouco sabemos a respeito da vida, além de uma tradição referida numa coleção de problemas datando do quinto ou sexto século da era cristã, chamada “Antologia Grega"(descrita abaixo). Segue um de tais problemas:

“Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isto cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz, criança tardia, depois de chegar á metade da vida de seu pai, o destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida.”

Podemos, a partir desse enunciado, representar como uma equação algébrica e descobrirmos sua idade. Com efeito:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4,$$

e calculando o valor x, o qual representa sua idade, obtemos como resultado da equação $x = 84$ anos.

A contribuição mais conhecida de *Diofanto* é ter introduzido uma forma de representar o valor desconhecido em um problema, designando-o como *arithmos*, de onde vem o nome “aritmética”. Outra das contribuições mais significativas deste trabalho diz respeito às notações: são introduzidas algumas abreviaturas para designar quantidades e operações, iniciando o que viria a chamar-se “álgebra sincopada”. (Os historiadores distinguem, em geral, três períodos no desenvolvimento da álgebra: álgebra retórica, em que tudo é explicado por palavras; álgebra sincopada, na qual se usam algumas abreviaturas; e álgebra simbólica).

O pensamento de *Diofanto* sobre os processos de desenvolvimento da matemática, especialmente em relação a resoluções de problemas existentes em sua época, baseado na invenção e no uso de símbolos, certamente para simplificar a escrita e os cálculos matemáticos, fizeram com que as expressões, até então escritas totalmente com palavras, pudessem se apresentar de formas abreviadas. Ao contrário de seus antepassados, que nos procedimentos de resoluções de

problemas utilizavam excessivamente descrições através de palavras sem fazer uso de símbolos para representar incógnitas, Diofanto introduziu no cenário da matemática um novo modo de pensar, tendo por base uma abreviação simbólica das quantidades desconhecidas - as "designações abreviadas" [2]. Por tais fatos, muitos autores designam que *Diofanto* é o pai da álgebra.

2.1 Equações Diofantinas Lineares com Duas Variáveis

A resolução de vários problemas de aritmética recai na resolução, em números inteiros, de equação do tipo:

$$ax + by = c$$

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

Nem sempre essas equações possuem solução nos inteiros, por exemplo, a equação:

$$4x + 6y = 3$$

Não possui nenhuma solução x_0, y_0 em números inteiros pois, caso contrário, teríamos $4x_0 + 6y_0$ *par* e, portanto, nunca igual a 3. Então, é natural perguntarmos em quais condições tal equação possui soluções e, caso as tenha, como determiná-las?

Tais perguntas, serão respondidas, através das duas proposições a seguir.

Proposição 2.1. *Sejam $a, b, c \in \mathbb{Z}$. A equação $ax + by = c$ admite solução em números inteiros se, e somente se, $mdc\,(a, b)|c$.*

Demonstração: ($\Longrightarrow$) Sejam x_0, y_0 soluções inteiras da equação diofantina $ax + by = c$. Assim, $ax_0 + by_0 = c$ e, seja $d = mdc(a, b)$. Como $d \mid a$ e $d \mid b$ pela proposição 1.6 $d \mid ax_0 + by_0$, ou seja, $d \mid c$.

($\Longleftarrow$) Se $d \mid c$ então $c = k \cdot d$, onde $k \in \mathbb{Z}$. Pela relação de Bezout, Teorema 1.2, d pode ser escrito como combinação Linear de a e b, ou seja, $d = ax_0 + by_0$, substituindo em $c = k \cdot d$ temos:

$$c = k \cdot (ax_0 + by_0) \Rightarrow c = a \cdot kx_0 + b \cdot ky_0$$

onde $kx_0 = x \in \mathbb{Z}$ e $ky_0 = y \in \mathbb{Z}$, logo $c = ax + by$ admite soluções em números inteiros.

■

Mostraremos a seguir que as soluções de uma equação Diofantina podem ser determinadas a partir de uma solução particular qualquer x_0, y_0.

Teorema 2.1. *Seja x_0, y_0 uma solução da equação $ax + by = c$, onde $mdc\,(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são da forma:*

$$x = x_0 + b \cdot t, y = y_0 - a \cdot t; \textit{com } t \in \mathbb{Z}$$

Demonstração: Como x_0, y_0 é uma solução particular, substituiremos os valores na equação principal, da seguinte maneira:

$$ax + by = c \quad \text{(I)}$$
$$ax_0 + by_0 = c \quad \text{(II)}$$

Como $c = c$, podemos igualar as equações (I) e (II), com isso temos:

$$ax + by = ax_0 + by_0 \Rightarrow ax - ax_0 = by_0 - by \Rightarrow$$
$$a\,(x - x_0) = b\,(y_0 - y) \quad \text{(III)}$$

Analisando a equação (III), subdividiremos esta parte da demonstração em duas etapas:

i) Por um lado, temos que $b|a\ (x - x_0)$, e como $mdc\ (a, b) = 1$, pelo Lema de Gauss Teorema 1.4, temos que $b|(x - x_0)$ consequentemente $x - x_0 = b \cdot t$, onde $t \in \mathbb{Z}$ substituindo o valor obtido na equação (III), temos:

$$a\ (x - x_0) = b\ (y_0 - y) \Rightarrow a \cdot \cancel{b}\, t = \cancel{b}\ (y_0 - y) \Rightarrow at = y_0 - y \Rightarrow y = y_0 - a \cdot t$$

ii) Agora, analisando a equação (III) de outra maneira, temos que: $a|b\ (y_0 - y)$, e como $mdc\,(a, b) = 1$, pelo Lema de Gauss Teorema 1.4, temos que $a|y_0 - y \Rightarrow y_0 - y = a \cdot t$ substituindo o valor obtido na equação (III), temos:

$$a\ (x - x_0) = b\ (y_0 - y) \Rightarrow \cancel{a}\,(x - x_0) = b \cdot \cancel{a}\, t \Rightarrow x - x_0 = bt \Rightarrow x = x_0 + b \cdot t$$

o que prova que as soluções são do tipo exibido.

Por outro lado, x, y, como no enunciado, é solução, pois:
$ax + by = c$, substituindo os valores de x, y na equação obtemos $a\,(x_0 + b \cdot t) + b\,(y_0 - a \cdot t) = c \Rightarrow ax_0 + \cancel{a \cdot b \cdot t} + by_0 - \cancel{a \cdot b \cdot t} = c \Rightarrow ax_0 + by_0 = c$, o que prova que toda solução das equações Diofantinas possui esse formato. ■

OBS.: Segue-se da proposição demonstrada que a equação Diofantina $ax + by = c$, com $mdc\,(a, b) = 1$, admite infinitas soluções em $\mathbb{Z}$.

Note também que as soluções da equação Diofantinas $ax + by = c$ podem ser escrito como $x = x_0 - b \cdot t, y = y_0 + a \cdot t$, com $t \in \mathbb{Z}$, bastando apenas trocar t por $-t$.

A seguir, descreveremos um método para encontrar uma solução particular de uma equação do tipo $ax + by = c$, quando $mdc\,(a, b) = 1$. Se $|a|, |b|$ e $|c|$ são números pequenos, uma solução pode ser encontrada por inspeção, mas de modo geral, o método que será descrito a seguir permitirá achar uma solução da equação.

Usando o algoritmo estendido, é possível determinar $m, n \in \mathbb{Z}$ tais que:

$$ma + nb = mdc\,(a, b) = 1$$

Multiplicando ambos os membros da igualdade acima por c, obtemos:

$$cma + cnb = c \Rightarrow a \cdot cm + b \cdot cn = c$$

Logo $x_0 = cm$ e $y_0 = cn$ é uma solução particular da equação.

■

Corolário 2.1. *Dado a equação $ax + by = c$, com $a \neq 0$ e $b \neq 0$ admite uma equação equivalente se $mdc\,(a, b) = 1$.*

Demonstração:

Dada a equação, $ax + by = c$, com $d = mdc\,(a, b)$, dividimos toda a equação por d, temos $\frac{a}{d} = a_1, \frac{b}{d} = b_1$ e $\frac{c}{d} = c_1$, pelo Corolário 2.1, temos que $mdc\,(a_1, b_1) = 1$ por tanto a equação equivalente $a_1x + b_1y = c_1$, terá sempre solução.

■

Exemplo 2.1 (ENQ-PROFMAT 2019.1)**.** *Considere os itens abaixo:*

a) Determine o menor número c para o qual a equação

$$5x + 7y = c$$

tenha exatamente 4 soluções em $\mathbb{N} \cup \{0\}$.

b) Determine, explicitamente, as 4 soluções obtidas no item a).

Solução:

a) Dada a equação $5x + 7y = c$ que chamaremos de equação (I). Pela proposição 2.1, como $mdc\,(5, 7) = 1$ e $1 \mid c$, temos que a equação (I) admite infinitas soluções nos inteiros. Pelo teorema 1.2 podemos reescrever o $mdc\,(5, 7) = 1$, como uma combinação linear de 5 e 7. E pelo algoritmo de Euclides estendido, teorema 1.5 nos auxilia a encontrar tais inteiros (x, y), aplicando isso temos:

	1	②
7	⑤	②
2	①	

$$\Longrightarrow \quad a = q_1 \cdot b + n_1$$

Escrevendo o $mdc\,(5, 7)$ como uma combinação linear temos:

$$1 = 5 - 2 \cdot 2 \tag{II}$$

	①	2
⑦	⑤	2
②	1	

$\Longrightarrow \quad a = q_1 \cdot b + n_1$

$$2 = 7 - 1 \cdot 5 \tag{III}$$

Substituindo (III) em (II), temos:

$$1 = 5 - 2 \cdot 2 = 5 - 2(7 - 1 \cdot 5) = 5 - 2 \cdot 7 + 2 \cdot 5 = 3 \cdot 5 + 7(-2)$$
$$1 = 5 \cdot 3 + 7 \cdot (-2) \tag{IV}$$

Para encontrarmos uma solução particular da equação (I), basta multiplicar a combinação (IV), por c, com isso temos:

$$1 \cdot c = 5(3c) + 7(-2c)$$
$$c = 5(3c) + 7(-2c) \Rightarrow x_0 = 3c \text{ e } y_0 = -2c$$

Pelo teorema 2.1, sabemos que a solução da equação (I) é da forma:

$$x = x_0 + b \cdot t \Rightarrow x = 3c + 7t$$
$$y = y_0 - a \cdot t \Rightarrow y = -2c - 5t$$

onde $t \in \mathbb{Z}$.

Como as soluções tem que pertencer a $\mathbb{N} \cup \{0\}$, temos que ter $x \geq 0$ e $y \geq 0$. Logo:

i) $3c + 7t \geq 0 \Rightarrow 7t \geq -3c \Rightarrow t \geq -\frac{3c}{7}$

ii) $-2c - 5t \geq 0 \Rightarrow -5t \geq 2c \Rightarrow t \leq -\frac{2c}{5}$

ou seja, $-\frac{3c}{7} \leq t \leq -\frac{2c}{5}$.

Como queremos 4 soluções $-\frac{2c}{5} - \left(-\frac{3c}{7}\right) \geq 3 \Rightarrow -\frac{2c}{5} + \frac{3c}{7} \geq 3 \Rightarrow \frac{-14c+15c}{35} \geq 3 \Rightarrow c \geq 105$.

Substituindo o valor de c, no intervalo, temos:

$$\frac{-3 \cdot 105}{7} \leq t \leq \frac{-2 \cdot 105}{5} \Rightarrow -45 \leq t \leq -42.$$

Portanto, temos exatamente as 4 soluções correspondentes $t = -45, -44, -43, -42$.

b) Para encontramos as 4 soluções da equação (I), basta substituir o valor de c e t na equação geral.

i) Para $t = -45$

$$x = 3c + 7t \Rightarrow x = 3 \cdot 105 + 7(-45)$$
$$= 315 - 315 = 0$$

$$y = -2c - 5t \Rightarrow y = -2 \cdot 105 - 5(-45)$$
$$= -210 + 225 = 15$$

ii) Para $t = -44$

$$x = 3c + 7t \Rightarrow x = 3 \cdot 105 + 7(-44)$$
$$= 315 - 308 = 7$$

$$y = -2c - 5t \Rightarrow y = -2 \cdot 105 - 5(-44)$$
$$= -210 + 220 = 10$$

iii) Para $t = -43$

$$x = 3c + 7t \Rightarrow x = 3 \cdot 105 + 7(-43)$$
$$= 315 - 301 = 14$$

$$y = -2c - 5t \Rightarrow y = -2 \cdot 105 - 5(-43)$$
$$= -210 + 215 = 5$$

iv) Para $t = -42$

$$x = 3c + 7t \Rightarrow x = 3 \cdot 105 + 7(-42)$$
$$= 315 - 294 = 21$$

$$y = -2c - 5t \Rightarrow y = -2 \cdot 105 - 5(-42)$$
$$= -210 + 210 = 0$$

Exemplo 2.2. *Resolvamos a equação* $24x + 14y = 18$

Solução: *Como* $mdc\,(24, 14) = 2$ *e* $2|18$*, logo a equação tem solução. Pelo Corolário 2.1, podemos dividir ambos os membros da equação por* $mdc\,(24, 14) = 2$*, obtendo assim,uma equação equivalente* $12x + 7y = 9$*.*

Agora acharemos uma solução particular x_0, y_0 *desta última equação, pelo algoritmo das divisões sucessivas de Euclides, Teorema 1.5 temos:*

•	1	1	2	*quociente*
12	7	5	2	*dividendo e divisor*
5	2	1		*resto*

$$1 = 5 - 2 \cdot 2 \qquad \textit{(I)}$$
$$2 = 7 - 5 \cdot 1 \qquad \textit{(II)}$$
$$5 = 12 - 7 \cdot 1 \qquad \textit{(III)}$$

Substituindo a equação (II) na equação (I), temos:

$$1 = 5 - 2 \cdot 2 \Rightarrow 1 = 5 - 2\,(7 - 5 \cdot 1) \Rightarrow 1 = 5 - 2 \cdot 7 + 5 \cdot 2 \Rightarrow 1 = -2 \cdot 7 + 5 \cdot 3 \qquad \textit{(IV)}$$

Substituindo a equação (III) na equação (IV), temos:

$$1 = -2 \cdot 7 + 3 \cdot 5 \Rightarrow 1 = -2 \cdot 7 + 3\,(12 - 7 \cdot 1) \Rightarrow 1 = -2 \cdot 7 + 3 \cdot 12 - 7 \cdot 3 \Rightarrow 1 = 12 \cdot 3 + 7\,(-5)$$

para encontrar uma solução particular para a equação, basta multiplicarmos a combinação linear $12\,(3) + 7\,(-5) = 1$*, por* 9*, com isso temos:*

$$12\,(3 \cdot 9) + 7\,(-5 \cdot 9) = 1 \cdot 9 \Rightarrow 12\,(27) + 7\,(-45) = 9$$

Logo, $x_0 = 27$ *e* $y_0 = -45$ *é solução particular da equação e, consequentemente,pelo teorema 2.1 as soluções são do tipo:*

$x = x_0 + b \cdot t \Rightarrow x = 27 + 7t$

$y = y_0 + a \cdot t \Rightarrow y = -45 - 12t;\ t \in \mathbb{Z}$

OBS.: Tal método nos auxilia a encontrar uma solução particular, para que possamos encontrar as demais soluções, mas podemos encontrar tais soluções por inspeção, por exemplo, podemos perceber que $(-1, 3) = (x_0, y_0)$ também é uma solução particular da equação, e ao substituirmos na equação paramétrica, poderemos encontrar as mesmas soluções da equação anterior.

$$x = -1 + 7t$$

$$y = 3 - 12t$$

2.2 Equação Diofantinas Lineares com três variáveis

Nesta etapa construirmos a ideia de como encontrar uma solução particular como também a geral de uma equação Diofantina Linear com n variáveis através dos estudos da resolução das equação Diofantina com três variáveis.

2.2.1 Solução Particular

Dada a equação

$$a_1x + a_2y + a_3z = c \tag{I}$$

Onde $a_1, a_2, a_3 \in \mathbb{Z}$ ambos são diferentes de zero. Notemos que, pela Proposição 2.1, uma equação Diofantina Linear possui solução se $d|c$, onde $d = mdc\,(a_1, a_2, a_3)$. Pela Proposição 1.18, vimos que é possível calcular o mdc de uma quantidade finita de números no caso particular que $mdc\,(a_1, a_2, a_3)$ pode ser calculado da seguinte maneira $mdc\,(a_1, a_2) = d_1$ e $mdc\,(d_1, a_3) = d$.

Logo, pelo Teorema 1.2 temos que d_1 pode ser escrito como combinação linear de a_1 e a_2, de maneira que existem $k_1, k_2 \in \mathbb{Z}$, tal que $d_1 = a_1 \cdot k_1 + a_2 \cdot k_2$. Como $d = mdc\,(d_1, a_3)$, pelo Teorema 1.2 temos que d pode ser escrito como combinação linear de d_1 e a_3, de maneira que existam $k, z_0 \in \mathbb{Z}$, tal que $d = d_1 \cdot k + a_3 \cdot z_0$, substituindo o valor d_1 em d, temos

$$d = (a_1 \cdot k_1 + a_2 \cdot k_2) \cdot k + a_3 \cdot z_0 \Rightarrow d = a_1\,(k_1 \cdot k) + a_2\,(k_2 \cdot k) + a_3 \cdot z_0$$

Tomando $k_1 \cdot k = x_0$ e $k_2 \cdot k = y_0$, temos:

$$d = a_1x_0 + a_2y_0 + a_3z_0 \tag{II}$$

Como $d|c \Rightarrow c = q \cdot d$, onde $q \in \mathbb{Z}$. Agora basta multiplicarmos a equação (II) por q, que obteremos:

$$a_1 \cdot (x_0 \cdot q) + a_2 \cdot (y_0 \cdot q) + a_3 \cdot (z_0 \cdot q) = q \cdot d$$

e $c = q \cdot d$, temos:

$$a_1 \cdot (x_0 \cdot q) + a_2 \cdot (y_0 \cdot q) + a_3 \cdot (z_0 \cdot q) = c$$

onde $(x_0 \cdot q, y_0 \cdot q, z_0 \cdot q)$ é uma solução particular da equação (I).

■

Agora utilizaremos o Exemplo 2.2 para nos auxiliar na compreensão da solução geral para uma equação Diofantina Linear com três variáveis.

Exemplo 2.3. *Encontre a solução geral da equação* $5x + 6y + 9z = 15$.
Solução: *Como* $mdc\,(5, 6, 9) = 1$, $1|15$ *logo a equação possui infinitas soluções. Agora reduziremos a equação dada, para uma de duas variáveis. De tal forma, que onde está* $5x + 6y$ *colocaremos* k*, ou seja,*

$$5x + 6y = k \qquad \textit{(III)}$$

de onde segue que

$$k + 9z = 15 \qquad \textit{(IV)}$$

Como $mdc\,(1, 9) = 1$, $1|15$ *logo a equação possui solução, pelo Teorema 1.2, podemos escrever o* $mdc\,(1, 9)$ *como uma combinação linear de* 1 *e* 9*, da seguinte maneira:*

$$1 = 1 \cdot (-8) + 9 \qquad \textit{(V)}$$

Multiplicando ambos os lados da combinação Linear por 15, acharemos uma solução particular de $k + 9z = 15$, com isso temos:

$$1 \cdot 15 = 1\,(-8 \cdot 15) + 9 \cdot 15$$
$$15 = 1 \cdot (-120) + 9\,(15)$$

Pelo Teorema 2.1 temos que as soluções da equação (IV) são da seguinte maneira onde $k_0 = -120$ e $z_0 = 15$, substituindo em

$$k = k_0 + b \cdot t \Rightarrow k = -120 + 9t_1 \qquad \text{(VI)}$$
$$z = z_0 - a \cdot t \Rightarrow z = 15 - t_1 \qquad \text{(VII)}$$

Agora voltaremos para a equação $5x + 6y = k$.

Como $mdc\,(5, 6) = 1$, $1|k$ logo a equação possui infinitas soluções, pelo Teorema 1.2, podemos escrever o $mdc\,(5, 6)$, como combinação linear de 5 e 6, da seguinte maneira:

$$1 = 6 - 1 \cdot 5$$

Multiplicando ambos os lados da equação por k, acharemos uma solução particular, com isso temos:

$$1 \cdot k = 6\,(k) + 5\,(-1 \cdot k) \Rightarrow 5\,(-k) + 6\,(k) = k$$

Pelo Teorema 2.1 as soluções da equação (III) são da seguinte maneira onde $x_0 = -k$ e $y_0 = k$, substituindo em:

$$x = x_0 + b \cdot t \Rightarrow x = -k + 6t_2 \tag{VIII}$$
$$y = y_0 - a \cdot t \Rightarrow y = k - (5) \cdot t_2 \tag{IX}$$

Substituindo o valor de k, equação (VI) na equação (VIII) temos:

$$x = -(-120 + 9t_1) + 6t_2 \Rightarrow x = 120 - 9t_1 + 6t_2$$
$$y = (-120 + 9t_1) - 5t_2 \Rightarrow y = -120 + 9t_1 - 5t_2$$

Logo a solução geral é:

$$S = \begin{cases} x = 120 - 9t_1 + 6t_2 \\ y = -120 + 9t_1 - 5t_2 \\ z = 15 - t_1 \end{cases} \qquad \forall\, t_i \in \mathbb{Z}$$

2.2.2 Solução Geral

Através da ideia constituída na resolução desse exemplo, demonstraremos a solução geral de

$$ax + by + cz = q \tag{I}$$

Demonstração: Seja $d = mdc\,(a, b, c)$, dividimos a equação (I) por d temos:

$$\frac{a}{d}x + \frac{b}{d}y + \frac{c}{d}z = \frac{q}{d}$$

Pelo Corolário 2.1 obteremos uma equação semelhante, fazendo

$$\frac{a}{d} = a_1, \frac{b}{d} = a_2, \frac{c}{d} = a_3 \quad \text{e} \quad \frac{q}{d} = w.$$

De tal forma que

$$a_1x + a_2y + a_3z = w \tag{II}$$

Que pelo Corolário 1.3 item *(b)*, temos que $mdc\,(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}) = 1 = mdc\,(a_1, a_2, a_3)$ o que nos permite dizer que a equação (II) possui infinitas soluções, agora reduziremos a equação (II) para uma equação de duas variáveis, com isso chamaremos:

$$a_1x + a_2y = k \tag{III}$$

desta forma a equação (II) fica reduzida a uma equação com duas variáveis.

$$k + a_3 z = w \tag{IV}$$

Como $mdc\,(1, a_3) = 1$ e $1|w$ logo a equação (IV) possui infinitas soluções nos inteiros, e pelo Teorema 2.1, as suas soluções são do tipo:

$$\begin{aligned} k &= k_0 + a_3 \cdot t \\ z &= z_0 - t \quad \text{onde } t \in \mathbb{Z} \end{aligned} \tag{V}$$

Agora voltamos a analisar a equação (III) $a_1 x + a_2 y = k$, como o $mdc\,(a_1, a_2) = 1$ e $1|k$, logo a equação possui infinitas soluções nos inteiros, e pelo Teorema 2.1 as suas soluções são do tipo:

$$\begin{aligned} x &= x_0 + a_2 \cdot l \\ y &= y_0 - a_1 \cdot l \quad \text{onde } l \in \mathbb{Z} \end{aligned} \tag{VI}.$$

Busquemos uma solução particular da equação (III), ou seja (x_0, y_0). Sabemos que $mdc\,(a_1, a_2) = 1$ e pelo Teorema 1.2, relação de Bezout, sabemos que $mdc\,(a_1, a_2) = 1$ pode ser escrito como combinação linear de a_1 e a_2, com isso temos $(\lambda_0, \beta_0) \in \mathbb{Z}$, tais que

$$1 = a_1\,(\lambda_0) + a_2\,(\beta_0)$$

multiplicando a identidade por k

$$\begin{aligned} k \cdot 1 &= a_1\,(\lambda_0 \cdot k) + a_2\,(\beta_0 \cdot k) \\ k &= a_1\,(\lambda_0 \cdot k) + a_2\,(\beta_0 \cdot k) \end{aligned}$$

Onde $\lambda_0 \cdot k = x_0$, $\beta_0 \cdot k = y_0$ é uma solução particular, substituindo na equação (VI), temos:

$$\begin{aligned} x = x_0 + a_2 \cdot l \Rightarrow x &= \lambda_0 \cdot k + a_2 \cdot l \\ y = y_0 - a_1 \cdot l \Rightarrow y &= \beta_0 \cdot k - a_1 \cdot l \end{aligned} \tag{VII}$$

Substituindo o valor de k da equação (V) na equação (VII) temos:

$$\begin{aligned} x = \lambda_0 \cdot k + a_2 \cdot l \Rightarrow x = \lambda_0\,(k_0 + a_3 \cdot t) + a_2 \cdot l \Rightarrow x = \lambda_0 \cdot k_0 + \lambda_0 \cdot a_3 \cdot t + a_2 \cdot l \\ y = \beta_0 \cdot k - a_1 \cdot l \Rightarrow y = \beta_0\,(k_0 + a_3 \cdot t) - a_1 \cdot l \Rightarrow y = \beta_0 \cdot k_0 + \beta_0 \cdot a_3 \cdot t - a_1 \cdot l \end{aligned}$$

Portanto a solução geral da equação (I) é dado por:

$$S = \begin{cases} x = \lambda_0 \cdot k_0 + a_2 \cdot l + \lambda_0 \cdot a_3 \cdot t \\ y = \beta_0 \cdot k_0 - a_1 \cdot l + \beta_0 \cdot a_3 \cdot t \\ z = z_0 - t \end{cases}$$

■

2.3 Equações Diofantinas com n variáveis

Nesta etapa, mostraremos um método que consiste não só em encontrar uma solução particular de uma equação Diofantina Linear com n variáveis, mas como também todas as suas soluções. Para isso consideremos a equação Diofantina Linear com n variáveis.

$$a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n = c \tag{I}$$

e nosso objetivo é encontrar um conjunto com n-uplas $(x_1, x_2, ..., x_n)$ inteiras em que a condição da equação (I) seja satisfeita. Para isso, utilizaremos a mesma técnica utilizada na equação Diofantina Linear com três variáveis, ou seja, reduzir a equação (I) em uma equação Diofantina Linear com duas variáveis. Esta etapa teve como base [9].

2.3.1 Solução Particular

Dada a equação (I), e seja $d = mdc\,(a_1, a_2, ..., a_n)$, dividimos a equação (I) por d, temos:

$$\frac{a_1}{d} \cdot x_1 + \frac{a_2}{d} \cdot x_2 + ... + \frac{a_n}{d} \cdot x_n = \frac{c}{d}$$

Pelo Corolário 2.1, obteremos uma equação semelhante, fazendo.

$$\frac{a_1}{d} = b_1, \frac{a_2}{d} = b_2, ..., \frac{a_n}{d} = b_n \text{ e } \frac{c}{d} = w$$

$$b_1 \cdot x_1 + b_2 \cdot x_2 + ... + b_n \cdot x_n = w \tag{II}$$

Pelo Corolário 1.3 item *(b)* temos que $mdc\,(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}) = 1 = mdc\,(b_1, b_2, ..., b_n)$, que pelo Teorema 1.2, relação de Bezout, nos garante que o mdc pode ser escrito como uma combinação linear de seus elementos, ou seja,

$$mdc\,(b_1, b_2, ..., b_n) = 1 \Rightarrow 1 = b_1\,(c_1) + b_2\,(c_2) + ... + b_n\,(c_n) \tag{III}$$

onde $c_i \in \mathbb{Z}, \forall_i \in \mathbb{N}$.

Multiplicando a identidade (III) por w, temos:

$$w \cdot 1 = b_1 \ (c_1) + b_2 \ (c_2) + ... + b_n \ (c_n) \cdot w$$
$$w \cdot 1 = b_1 \ (c_1 \cdot w) + b_2 \ (c_2 \cdot w) + ... + b_n \ (c_n \cdot w)$$

e, dessa forma, $c_1 \cdot w, c_2 \cdot w, ..., c_n \cdot w$ são soluções particulares da equação (II).

■

2.3.2 Solução Geral

Para encontrarmos a solução geral de (II), basta reduzirmos a equação, para uma equação com duas variáveis, como temos feito nos casos anteriores, com isso temos:
Demonstração: Dado $b_1 \cdot x_1 + b_2 \cdot x_2 + ... + b_n \cdot x_n = w$, coloquemos $b_1 \cdot x_1 + b_2 \cdot x_2 + ... + b_{n-1} \cdot x_{n-1} = k_1$, teremos então:

$$k_1 + b_n \cdot x_n = w \tag{IV}$$

Como $mdc\,(1, b_n) = 1$ e $1|w$, logo a equação possui infinitas soluções nos inteiros e pelo Teorema 2.1 elas são do tipo:

$$\begin{cases} k_1 = k_1^{'} + b_n \cdot t_1 \\ x_n = x_n^{'} - t_1 \end{cases} \qquad \text{onde } t_1 \in \mathbb{Z}$$

Portanto a solução geral da equação (II) pode ser dada por:

$$\begin{aligned} x_1 &= x_1^{'} + b_2 \cdot t_{n-1} \\ x_2 &= x_2^{'} - b_1 \cdot t_{n-1} \\ x_3 &= x_3^{'} + b_4 \cdot t_{n-2} \\ x_4 &= x_4^{'} - b_3 \cdot t_{n-2} \\ &\vdots \\ x_n &= x_n^{'} - t_1 \end{aligned}$$

Onde o seu conjunto solução pode ser exposto da seguinte forma:

$$s = \{(x_1^{'} + b_2 \cdot t_{n-1}, x_2^{'} - b_1 \cdot t_{n-1}, x_3^{'} + b_4 \cdot t_{n-2}, x_4^{'} - b_3 \cdot t_{n-2}, ..., x_n^{'} - t_1)\}$$

■

Exemplo 2.4 (ENQ-PROFMAT 2017.1)**.** *Resolva a congruência* $13x \equiv 1\, mod\, 2436$
Solução: *Por definição de congruência, temos que* $2436|(13x-1) \Rightarrow 13x-1 = 2436y$*, onde* $y \in \mathbb{Z}$*, podemos reescrever a equação da seguinte maneira:*

$$13x - 2436y = 1$$

Pelo Proposição 1.16, se existe inteiros (x, y)*, tal que:*

$$13x - 2436 = 1 \Rightarrow mdc\,(13, 2436) = 1$$

Pelo Teorema 1.2, podemos reescrever $mdc\,(13, 2436) = 1$*, como uma combinação linear de* 13 *e* 2436*.*

E pelo algorítimo Euclidiano estendido Teorema 1.5 nos auxilia a encontrar tais inteiros (x, y) *aplicando isso temos:*

	187	2	1	(1)	2
2436	13	5	(3)	(2)	1
5	3	2	(1)	0	

Escrevendo o $mdc\,(13, 2436) = 1$*, como combinação linear temos*

$$1 = 3 - 1 \cdot 2 \qquad \textit{(I)}$$

	187	2	(1)	1	2
2436	13	(5)	(3)	2	1
5	3	(2)	1	0	

$$2 = 5 - 1 \cdot 3 \qquad \textit{(II)}$$

	187	(2)	1	1	2
2436	(13)	(5)	3	2	1
5	(3)	2	1	0	

$$3 = 13 - 2 \cdot 5 \qquad \textit{(III)}$$

	(187)	2	1	1	2
(2436)	(13)	5	3	2	1
(5)	3	2	1	0	

$$5 = 2436 - 187 \cdot 13 \qquad \textit{(IV)}$$

Substituindo (II) em (I), temos:

$$1 = 3 - 1 \cdot 2 = 3 - 1\,(5 - 1 \cdot 3) = 3 - 1 \cdot 5 + 1 \cdot 3 = -1 \cdot 5 + 2 \cdot 3$$

$$1 = -1 \cdot 5 + 2 \cdot 3 \qquad \textit{(V)}$$

Substituindo (III) em (V), temos:

$$1 = -1 \cdot 5 + 2 \cdot 3 = -1 \cdot 5 + 2\,(13 - 2 \cdot 5) = -1 \cdot 5 + 2 \cdot 13 - 4 \cdot 5 = 2 \cdot 13 - 5 \cdot 5$$

$$1 = 2 \cdot 13 - 5 \cdot 5 \qquad \textit{(VI)}$$

Substituindo (IV) em (VI), temos:

$$1 = 2 \cdot 13 - 5 \cdot 5 = 2 \cdot 13 - 5\,(2436 - 187 \cdot 13) = 2 \cdot 13 - 5 \cdot 2436 + 935 \cdot 13 =$$

$$1 = 13\,(2 + 935) - 5 \cdot 2436$$

$$1 = 13\,(937) - 2436\,(5)$$

Portanto $13x - 2436y = 1 \Rightarrow x = 937$.

Exemplo 2.5 (ENQ-PROFMAT 2018.2)**.** *Considere a equação Diofantina Linear* $5x + 3y = 2018$

a) Escreva a solução geral em $\mathbb{Z}$.

b) Quantas soluções existem e $\mathbb{N} \cup \{0\}$*?*

Solução:

a) Dada a equação $5x + 3y = 2018$ *(I)*

Pela Proposição 2.1, como $mdc\,(5, 3) = 1$ *e* $1|2018$*. temos que a equação (I) admite infinitas soluções nos inteiros.*

Utilizaremos a linguagem de congruência na solução deste problema.

$5x + 3y = 2018\,(mod\ 3) \Rightarrow 2x \equiv 2\,mod\,3$ *(II)*

ou

$5x+3y = 2018\,(mod\ 5) \Rightarrow 3y \equiv 3\,mod\,5$ *(III)*

Poderíamos escolher, quaisquer equação, escolheremos a equação (I), $2x \equiv 2\, modo\, 3$*, por definição de congruência, temos:*

$3|2x-2 \Rightarrow 3|2\,(x-1)$*, como* $mdc\,(3,2)=1$*, pelo lema de Gauss, Teorema 1.4* $3|(x-1) \Rightarrow x-1=3t, t\in\mathbb{Z}$*. Com isso temos*

$$x-1=3t \Rightarrow x=1+3t \qquad \textit{(IV)}$$

Substituindo o valor obtido na equação (I), temos:

$$\begin{aligned} 5x+3y=2018 \Rightarrow\ & 5\,(1+3t)+3y=2018 \\ & 5+15t+3y=2018 \\ & 3y=2018-5-15t \\ & y=\frac{2013-15t}{3} \\ & y=671-5t \qquad (V) \end{aligned}$$

Portanto a solução geral da equação (I), é dado por

$$\begin{cases} x=1+3t \\ y=671-5t \end{cases} \qquad \textit{onde } t\in\mathbb{Z}$$

b) Como as equações tem que pertencer a $\mathbb{N}\cup\{0\}$*, temos que ter* $x\geq 0$ *e* $y\geq 0$*, logo:*

i) $1+3t\geq 0 \Rightarrow 3t\geq -1 \Rightarrow t\geq -\frac{1}{3} \Rightarrow t\geq -0,3333...$

Como t *é um número inteiro,* $t\geq 0$*.*

ii) $671-5t\geq 0 \Rightarrow -5t\geq -671 \Rightarrow t\leq \frac{671}{5} \Rightarrow t\leq 134,2$

Como t *é um número inteiro,* $t\leq 134$*.*

Com isso temos $0\leq t\leq 134$*.*

Portanto existem 135 *soluções em* $\mathbb{N}\cup\{0\}$*.*

Exemplo 2.6 (OBMEP - 2018 - N_3)**.** *De quantas maneiras podemos trocar uma nota de R$ 20,00 por moedas de 10 e 25 centavos?*

Solução: *Sejam* x *e* y *a quantidade de moedas de R$* $0,25$ *e R$* $0,10$*, usadas para formar a quantia de R$* $20,00$*, temos a seguinte equação:*

$$0,25x+0,10y=20 \qquad \textit{(I)}$$

Multiplicando (I) por 20*, temos:*

$$5x + 2y = 400 \qquad \textit{(II)}$$

Utilizando congruência módulo 5 *na equação (II), temos:* $2y \equiv 0$ *mod* $5 \Rightarrow 5 \mid 2y$. *Como* $mdc\,(5, 2) = 1$, *pelo lema de Gauss, Teorema 1.4,*

$$5 \mid y \Rightarrow y = 5t,\ t \in \mathbb{Z} \qquad \textit{(III)}$$

Substituindo (III), na equação (II), temos:

$$\begin{aligned} 5x + 2(5t) = 400 &\Rightarrow 5x + 10t = 400 \\ &\Rightarrow 5x = 400 - 10t \\ &\Rightarrow x = \frac{400 - 10t}{5} \\ &\Rightarrow x = 80 - 2t \end{aligned}$$

Como queremos saber de quantas maneiras podemos trocar uma nota, o conjunto solução da equação pertence a $\mathbb{N} \cup \{0\}$, *com isso temos:*

i) $x \geq 0 \Rightarrow 80t - 2t \geq 0 \Rightarrow -2t \geq -80 \Rightarrow t \leq \frac{+80}{+2} \Rightarrow t \leq 40$

ii) $y \geq 0 \Rightarrow 5t \geq 0 \Rightarrow t \geq 0$

$\therefore\ 0 \leq t \leq 40$, *totalizando* 41 *maneiras.*

Capítulo 3

Equações Diofantinas Quadráticas

Uma equação diofantina é uma equação polinomial para a qual procuramos soluções inteiras ou racionais. No capítulo anterior apresentamoss as equações diofantinas lineares, como ($a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ onde o objetivo é encontrar as n-uplas $x_1, x_2, \ldots, x_n$ que satisfaçam a equação) neste capítulo veremos outras equações diofantinas conhecidas como equações diofantinas quadráticas, começando pelas frações contínuas, passando pelas ternas pitagóricas e concluindo com a equação de Pell. De forma geral dada uma equação diofantina com qualquer número de variáveis e com coeficientes inteiros, descrever um processo que determine em um número finito de passos se a equação admite solução inteira, é essencialmente conhecido como o décimo problema de Hilbert. Considera-se que este problema foi resolvido por Martin Davis, Yuri Matiyasevich, Hilary Putnam e Julia Robison, não por eles terem descrito um tal processo mas, por eles terem demonstrado que não existe um algoritmo que, dada uma equação diofantina possamos Decidir se a equação admite solução inteira.

Existe muitos problemas famosos em equações diofantinas mas , com certeza o problema mais famoso é aquele que foi durante séculos conhecido como o último Teorema de Fermat, até sua demonstração ser completada por Andrew wiles e seu aluno Richard Taylor, provaram que para $n \geq 3$ qualquer solução inteira de ($x^n + y^n = z^n$) é trivial (no sentido que $x \cdot y \cdot z = 0$).

3.1 Frações Contínuas

Neste seção, faremos um breve estudo sobre a teoria das frações contínuas que consiste em apresentar um número racional, através de uma sequência finita de números inteiros, e também nos permite fazer boas aproximações de números irracionais, através de números racionais. De outra forma, podemos dizer que o conjunto $\mathbb{Q}$ dos números racionais é denso nos reais, isto é, os números reais podem ser, arbitrariamente bem aproximados por números racionais. De modo mais formal, $\forall\ \alpha \in \mathbb{R}, \forall\, \varepsilon > 0; \exists\ \dfrac{p}{q} \in \mathbb{Q}$ com erro de aproximação $|\alpha - \dfrac{p}{q}| < \varepsilon$.

Mostraremos também que para uma aproximação ser considerada boa, ela tem que vir da fração contínua.

O objetivo deste tópico é apresentar de forma clara, um tema que até nos dia de hoje ainda é objeto de pesquisa. O mesmo, servirá como base, para o estudo do tópico, a equação de Pell.

Boa parte desta exposição teve como referência [6].

Definição 3.1. *(Geral, Recursivamente) Seja α um número real e a_0 a sua parte inteira, no que denotaremos por $a_0 = \lfloor \alpha \rfloor \in \mathbb{Z}$. Se α for inteiro, ou seja, $\alpha = a_0$, não temos mais nada a fazer. Caso contrário, definimos um $\alpha_1 = \dfrac{1}{\alpha - a_0} > 1$, com isso temos que $\alpha = a_0 + \dfrac{1}{\alpha_1}$, a partir desse fato, podemos fazer isso sucessivamente. De modo geral, para $n \geq 1$, vamos ter um $\alpha_n > 1$, definimos então $a_n = \lfloor \alpha_n \rfloor \in \mathbb{N}$. Se α_n for inteiro, ou seja, $\alpha_n = a_n$, não temos mais nada a fazer. Caso contrário definimos um $\alpha_{n+1} = \dfrac{1}{\alpha_n - a_n} > 1$, logo $\alpha_n = a_n + \dfrac{1}{\alpha_{n+1}}$.*

Podemos representar as frações contínuas da seguinte maneira:

$$\begin{aligned}
\alpha_n = [a_0; a_1, a_2, ..., a_n, \alpha_{n+1}] &= a_0 + \frac{1}{\alpha_1} \\
&= a_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2}} \\
&= ... = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots \; + \cfrac{1}{a_n + \cfrac{1}{\alpha_{n+1}}}}}}
\end{aligned}$$

OBS.: Denotaremos a_0 como sendo a parte inteira de α_n, observe que o termo a_0 é separado por ponto e vírgula para evidenciar a parte inteira do número representado.

Definição 3.2. *(Frações Contínuas) Seja x um número real, uma expressão finita ou infinita é da forma:*

1^o Caso: finita se $\forall n \in \mathbb{N}$, existir algum n, tal que $\alpha_n = a_n$.

$$x = [a_0; a_1, a_2, ..., a_n]^{def} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots \; + \cfrac{1}{a_n}}}}$$

2^o Caso: infinita se $\alpha_n \notin \mathbb{Z}$.

$$x = [a_0; a_1, a_2, ...]^{def} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$$

Onde os ai são números reais, com $a_1, a_2, ..., \geq 1$, os números ai são chamados de quocientes parciais da fração contínua.

No primeiro caso, x pertence ao conjunto dos números racionais, no qual veremos a seguir que a sua representação por fração contínua é finita e, no segundo caso, x pertence ao conjunto dos números irracionais, onde sua representação por fração contínua é infinita.

Proposição 3.1. *Um número x, tem fração contínua finita, se somente se, ele é racional.*

Demonstração: Suponhamos x, seja um número racional, ou seja, x é da forma $\frac{p}{q}$, com $p \in \mathbb{Z}$, $q \in \mathbb{Z}$, com $(q > 0)$. Pelas divisões sucessivas de Euclides, Teorema 1.5, temos:

$p = a_0 \cdot q + r_1 \qquad 0 \leq r_1 < q$
$q = a_1 \cdot r_1 + r_2 \qquad 0 \leq r_2 < r_1$
$r_1 = a_2 \cdot r_2 + r_3 \qquad 0 \leq r_3 < r_2$
$r_2 = a_3 \cdot r_3 + r_4 \qquad 0 \leq r_4 < r_3$
.
.
.
$r_{n-2} = a_{n-1} \cdot r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$
$r_{n-1} = a_n \cdot r_n$

Tal método foi usado para calcular o $mdc\,(p, q)$ que, no caso, seria r_n. Mas, nesse caso, estamos interessados nos coeficientes $(a_0, a_1, a_2, ..., a_{n-1}, a_n)$, com isso temos:

$$x = \frac{p}{q} = \frac{a_0 \cdot q + r_1}{q} = \frac{a_0 \cdot q}{q} + \frac{r_1}{q} = a_0 + \frac{r_1}{q} = a_0 + \frac{1}{\frac{q}{r_1}} = a_0 + \frac{1}{\frac{a_1 \cdot r_1 + r_2}{r_1}}$$

$$= a_0 + \frac{1}{\frac{a_1 \cdot r_1}{r_1} + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{a_2 \cdot r_2 + r_3}{r_2}}}$$

$$= a_0 + \frac{1}{a_1 + \frac{1}{\frac{a_2 \cdot r_2}{r_2} + \frac{r_3}{r_2}}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_3}{r_2}}} = ... = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}$$

Ou seja, $x = [a_0, a_1, a_2, ..., a_n]$, como o processo do algoritmo da divisão de Euclides é finito, podemos concluir que a fração contínua de um número racional é finita, desta forma, a última expressão é a fração contínua que representa o número racional $x = \frac{p}{q}$.

■

Pela Proposição 3.1, vimos que todo número racional pode ser representado por uma fração contínua finita, do tipo:

$$x = \frac{p}{q} = [a_0; a_1, a_2, ..., a_n]$$

onde $a_0 \in \mathbb{Z}$, $\forall n \geq 0$ e $a_0, a_1, a_2, ..., a_n$ são todos inteiros positivos. Agora consideremos as frações:

$$x = \alpha_0 = \frac{a_0}{1}, \alpha_1 = a_0 + \frac{1}{a_1}, \alpha_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, ...$$

obtidas pelas expansões das frações contínuas $[a_0], [a_0, a_1], [a_0, a_1, a_2], ...$

Estas frações são chamadas de primeiro, segundo, terceira, ..., convergente, respectivamente, da fração contínua $x = [a_0, a_1, a_2, ..., a_n]$. Sendo que, o n-ésimo terma dessa fração é chamado de n-ésimo reduzida e convergente da fração contínua de x e será igual a própria fração contínua.

Até esta etapa ainda não foi apresentado, qual a vantagem de usar as frações contínuas e por enquanto, é apenas um jeito diferente de escrever números reais. A seguir, mostraremos qual a finalidade de usar frações contínuas, ou seja, iremos mostrar porque as frações contínuas acabam nos dando boas aproximações, dado um número real.

Provaremos também porque quando paramos a fração contínua num determinado termo con-

vergente, isso nos dá uma boa aproximação do número em questão. Antes disso, demonstraremos a proposição 3.2 que nos auxiliará nos cálculos de uma fração contínua , sem ter que começar tudo do início novamente. Dessa forma essa proposição nos ajudará a calcular os próximos termos de uma fração contínua, conhecendo um termo anterior. Denotaremos daqui em diante como $\frac{p_n}{q_n}$ a n-ésima convergente da fração contínua de x. Para uma aplicação da proposição anterior resolveremos um exemplo.

Exemplo 3.1 (OBMEP - 2018 -N_2, N_3)**.** *Na igualdade abaixo a, b e c são números inteiros positivos. Qual é o valor de c?*

$$\frac{10}{7} = a + \frac{1}{b + \frac{1}{c}}$$

Solução: Como o problema exige apenas um número finito de quocientes parciais, podemos utilizar a proposição 3.1 que consiste no uso das divisões sucessivas de Euclides, Teorema 1.5, com isso temos:

	①	②	③
10	7	3	1
3	1	0	

Portanto, temos que $a = 1$, $b = 2$ e a resposta do problema $c = 3$.

Proposição 3.2. *Dada uma sequência (finita ou infinita) $t_0, t_1, t_2, ... \in \mathbb{R}$ tal que $t_k > 0$, para todo $k = 1$, definimos as sequências (x_m) e (y_m) por $x_0 = t_0, y_0 = 1, x_1 = t_0 \cdot t_1 + 1, y_1 = t_1$ de modo que $x_{m+2} = t_{m+2} \cdot x_{m+1} + x_m$ e $y_{m+2} = t_{m+2} \cdot y_{m+1} + y_m$, para todo $m \geq 0$. Temos então:*

$$[t_0, t_1, t_2, ..., t_n] = t_0 + \cfrac{1}{t_1 + \cfrac{1}{t_2 + \ddots + \cfrac{1}{t_n}}} = \frac{x_n}{y_n}, \forall n \geq 0$$

Além disso, $x_{n+1} \cdot y_n - x_n \cdot y_{n+1} = (-1)^n$, para todo $n \geq 0$.

Demonstração: A prova será por indução em n.

Caso base:

i) Para $n = 0$

$$\frac{x_n}{y_n} = \frac{x_0}{y_0} = \frac{t_0}{1} = t_0 = [t_0]$$

ii) Para $n = 1$

$$\frac{x_n}{y_n} = \frac{x_1}{y_1} = \frac{t_0 \cdot t_1 + 1}{t_1} = \frac{t_0 \cdot t_1}{t_1} + \frac{1}{t_1} = t_0 + \frac{1}{t_1} = [t_0, t_1]$$

iii) Para $n = 2$

$$\begin{aligned}\frac{x_n}{y_n} = \frac{x_2}{y_2} = \frac{t_2 \cdot x_1 + x_0}{t_2 \cdot y_1 + y_0} = \frac{t_2\,(t_0 \cdot t_1 + 1) + t_0}{t_2\,(t_1) + 1} &= \frac{t_2 \cdot t_0 \cdot t_1 + t_2 + t_0}{t_2 \cdot t_1 + 1} \\ &= \frac{t_0(t_2 \cdot t_1 + 1) + t_2}{(t_2 \cdot t_1 + 1)} = t_0 + \frac{t_2}{t_2 \cdot t_1 + 1} \\ &= t_0 + \frac{1}{\frac{t_2 \cdot t_1 + 1}{t_2}} = t_0 + \frac{1}{\frac{t_2 \cdot t_1}{t_2} + \frac{1}{t_2}} \\ &= t_0 + \frac{1}{t_1 + \frac{1}{t_2}} = [t_0, t_1, t_2]\end{aligned}$$

Hipótese de indução:

Suponhamos que a afirmação $x_n = t_n \cdot x_{n-1} + x_{n-2}$ e $y_n = t_n \cdot y_{n-1} + y_{n-2}$, seja válido para todo $n \in \mathbb{N}$.

Tese:

Queremos demonstrar que a expansão é valida para x_{n+1}, y_{n+1}, lembrando que, o $(n+1)$ -ésimo covergente $[t_0, t_1, t_2, ..., t_n, t_{n+1}]$ é obtido substituindo na expressão do n-ésimo convergente $[t_0, t_1, t_2, ..., t_n]$ substituindo o número t_n por $t_n + \frac{1}{t_{n+1}}$, seguindo os passos pretendidos temos:

$$[t_0, t_1, ..., t_n, t_{n+1}] = t_0 + \cfrac{1}{t_1 + \cfrac{1}{t_2 + \cfrac{1}{t_3 + \ddots + \cfrac{1}{(t_n + \frac{1}{t_{n+1}})}}}}$$

O ponto chave na demonstração é olharmos para os elementos entre parentese e considerarmos como um termo só, pois não altera em nada na definição dos $t_0, t_1, t_2, ..., t_{n-1}$ precedentes, ou seja:

$$x_{n-1} = \frac{t_{n-1} \cdot x_{n-2} + x_{n-3}}{t_{n-1} \cdot y_{n-2} + y_{n-3}}$$

Por tanto, como os números $x_{n-2}, x_{n-3}, y_{n-2}, y_{n-3}$ são independentes do quociente t_n, eles

não se alteram com a substituição, sendo assim, aplicamos $t_n + \dfrac{1}{t_n + 1}$.

$$
\begin{aligned}
[t_0; t_1, t_2, ..., t_n, t_{n+1}] = \left[t_0; t_1, t_2, ..., t_n + \frac{1}{t_{n+1}}\right] &= \frac{(t_n + \frac{1}{t_{n+1}}) \cdot x_{n-1} + x_{n-2}}{(t_n + \frac{1}{t_{n+1}}) \cdot y_{n-1} + y_{n-2}} \\
&= \frac{t_n \cdot x_{n-1} + \frac{x_{n-1}}{t_{n+1}} + x_{n-2}}{t_n \cdot y_{n-1} + \frac{y_{n-1}}{t_{n+1}} + y_{n-2}} \\
&= \frac{\frac{t_{n+1} \cdot t_n \cdot x_{n-1} + t_{n+1} \cdot x_{n-2}}{\cancel{t_{n+1}}}}{\frac{t_{n+1} \cdot y_{n-1} + y_{n-1} + t_{n+1} \cdot y_{n-2}}{\cancel{t_{n+1}}}} \\
&= \frac{t_{n+1} \cdot t_n \cdot x_{n-1} + x_{n-1} + t_{n+1} \cdot x_{n-2}}{t_{n+1} \cdot t_n \cdot y_{n-1} + y_{n-1} + t_{n+1} \cdot y_{n-2}} \\
&= \frac{t_{n+1}\,(t_n \cdot x_{n-1} + x_{n-2}) + x_{n-1}}{t_{n+1}\,(t_n \cdot y_{n-1} + y_{n-2}) + y_{n-1}}
\end{aligned}
$$

Pela hipótese de indução, temos que $x_n = t_n \cdot x_{n-1} + x_{n-2}$ e $y_n = t_n \cdot y_{n-1} + y_{n-2}$ substituindo na equação temos:

$$\frac{t_{n+1}\,(t_n \cdot x_{n-1} + x_{n-2}) + x_{n-1}}{t_{n+1}\,(t_n \cdot y_{n-1} + y_{n-2}) + y_{n-1}} = \frac{t_{n+1} \cdot x_n + x_{n-1}}{t_{n+1} \cdot y_n + y_{n-1}} = \frac{x_{n+1}}{y_{n+1}}$$

■

Provamos a primeira afirmação da proposição.

Agora, provaremos a segunda afirmação, $x_{n+1} \cdot y_n - x_n \cdot y_{n+1} = (-1)^n$, por indução sobre n, sabendo que:

$x_0 = t_0, y_0 = 1, x_1 = t_0 \cdot t_1 + 1, y_1 = t_1, x_2 = t_2 \cdot x_1 + x_0$ e $y_2 = t_2 \cdot y_1 + y_0$, com isso temos:

i) Caso base:

Para $n = 1$, verdade pois:

$$
\begin{aligned}
x_{n+1} \cdot y_n - x_n \cdot y_{n+1} &= x_2 \cdot y_1 - x_1 \cdot y_2 \\
&= [t_2 \cdot x_1 + x_0] \cdot t_1 - [t_0 \cdot t_1 + 1] \cdot [t_2 \cdot y_1 + y_0] \\
&= [t_2\,(t_0 \cdot t_1 + 1) + t_0] \cdot t_1 - [t_0 \cdot t_1 + 1] \cdot [t_2 \cdot (t_1) + 1] \\
&= [t_2 \cdot t_0 \cdot t_1 + t_2 + t_0] \cdot t_1 - [t_0 \cdot t_1 \cdot t_2 \cdot t_1 + t_0 \cdot t_1 + t_2 \cdot t_1 + 1] \\
&= \cancel{t_2 \cdot t_0 \cdot t_1 \cdot t_1} + \cancel{t_2 \cdot t_1} + \cancel{t_0 \cdot t_1} - \cancel{t_0 \cdot t_1 \cdot t_2 \cdot t_1} - \cancel{t_0 \cdot t_1} - \cancel{t_2 \cdot t_1} - 1 \\
&= -1
\end{aligned}
$$

ii) Hipótese de indução:

Suponhamos que $x_{n+1} \cdot y_n - x_n \cdot y_{n+1} = (-1)^n$, seja valida $\forall n \in \mathbb{N}$.

iii) Tese:

Queremos demonstrar que a afirmação é valido para $(n+1)$ elementos, ou seja,

$$x_{n+2} \cdot y_{n+1} - x_{n+1} \cdot y_{n+2} = (-1)^{n+1}$$

Sabendo que $x_{n+2} = t_{n+2} \cdot x_{n+1} + x_n$ e

$$y_{n+2} = t_{n+2} \cdot y_{n+1} + y_n$$

com isso temos:

$$\begin{aligned} x_{n+2} \cdot y_{n+1} - x_{n+1} \cdot y_{n+2} &= (t_{n+2} \cdot x_{n+1} + x_n) \cdot y_{n+1} - x_{n+1} \cdot (t_{n+2} \cdot y_{n+1} + y_n) \\ &= \cancel{t_{n+2} \cdot x_{n+1} \cdot y_{n+1}} + x_n \cdot y_{n+1} \cancel{- x_{n+1} \cdot t_{n+2} \cdot y_{n+1}} - x_{n+1} \cdot y_n \\ &= +x_n \cdot y_{n+1} - x_{n+1} \cdot y_n \\ &= -1 \cdot (x_{n+1} \cdot y_n - x_n \cdot y_{n+1}) \end{aligned}$$

Que por hipótese de indução, temos que $x_{n+1} \cdot y_n - x_n \cdot y_{n+1} = (-1)^n$,

logo:

$$-1 \cdot (x_{n+1} \cdot y_n - x_n \cdot y_{n+1}) = -1 \cdot (-1)^n = (-1)^{n+1}$$

■

Só para reforçar, o que citamos anteriormente, tal proposição é útil para calcular o que podemos chamar de frações contínuas trocadas, ou seja, se pararmos no enésimo termo, ela nos permite calcular termos consecutivos da fração contínua.

Por conta da Proposição 3.2, ganharemos alguns corolário quase que de graça, que são eles:

Corolário 3.1. *As sequências* (p_n) *e* (q_n) *satisfazem as recorrências* $p_{n+2} = a_{n+2} \cdot p_{n+1} + p_n$ *e* $q_{n+2} = a_{n+2} \cdot q_{n+1} + q_n$ *para todo* $n \geq 0$*, com* $p_0 = a_0, p_1 = a_0 \cdot a_1 + 1, q_0 = 1$ *e* $q_1 = a_1$.

Demonstração: As sequências (p_n) e (q_n) definidas pelas recorrências acima satisfazem, pela primeira afirmação da Proposição 3.2, a igualdade $\dfrac{p_n}{q_n} = [a_0, a_1, a_2, ..., a_n]$. ■

Corolário 3.2. *Para todo convergente* $\frac{p_n}{q_n}$ *da fração contínua de* x*, tem-se que* $mdc\,(p_n, q_n) = 1$.

Demonstração:

Pela segunda afirmação da Proposição 3.2, temos que:

$$p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = (-1)^{n-1}$$

Seja $d = mdc\,(p_n, q_n)$, isso implica que $d|p_n$ e $d|q_n$ e pela Proposição 1.6, temos que

$$d|p_n \cdot q_{n+1} - p_{n-1} \cdot q_n$$

ou seja, $d| \pm 1$ que pela definição de mdc, temos que $d = 1$, portanto $mdc\,(p_n, q_n) = 1$.

■

Corolário 3.3. *Temos para todo* $n \in \mathbb{N}$*,*

$$x = \frac{\alpha_n \cdot p_{n-1} + p_{n-2}}{\alpha_n \cdot q_{n-1} + q_{n-2}} \quad \textit{e} \quad \alpha_n = \frac{p_{n-2} - q_{n-2} \cdot x}{q_{n-1} \cdot x - p_{n-1}}$$

Demonstração: Dado $x = [a_0; a_1, a_2, ..., a_{n-1}, \alpha_n] = \frac{p_n}{q_n}$, a primeira igualdade é uma consequência direta da primeira afirmação da Proposição 3.2, ou seja:

$$x = \frac{\alpha_n \cdot p_{n-1} + p_{n-2}}{\alpha_n \cdot q_{n-1} + q_{n-2}}$$

Por outro lado, temos que a segunda igualdade $\alpha_n = \frac{p_{n-2} - q_{n-2} \cdot x}{q_{n-1} \cdot x - p_{n-1}}$ é consequência direta da primeira igualdade, ou seja, de $x = \frac{\alpha_n \cdot p_{n-1} + p_{n-2}}{\alpha_n \cdot q_{n-1} + q_{n-2}}$, de fato pois:

$$\begin{aligned} x = \frac{\alpha_n \cdot p_{n-1} + p_{n-2}}{\alpha_n \cdot q_{n-1} + q_{n-2}} &\Rightarrow (\alpha_n \cdot q_{n-1} + q_{n-2}) \cdot x = \alpha_n \cdot p_{n-1} + p_{n-2} \\ &\Rightarrow \alpha_n \cdot q_{n-1} \cdot x + q_{n-2} \cdot x = \alpha_n \cdot p_{n-1} + p_{n-2} \\ &\Rightarrow \alpha_n \cdot q_{n-1} \cdot x - \alpha_n \cdot p_{n-1} = p_{n-2} - q_{n-2} \cdot x \\ &\Rightarrow \alpha_n \cdot (q_{n-1} \cdot x - p_{n-1}) = p_{n-2} - q_{n-2} \cdot x \\ &\Rightarrow \alpha_n = \frac{p_{n-2} - q_{n-2} \cdot x}{q_{n-1} \cdot x - p_{n-1}} \end{aligned}$$

Através do que já foi exposto, podemos calcular o erro da aproximação por fração contínua.

■

Corolário 3.4. *Seja* x *um número irracional e* $\frac{p_n}{q_n}$ *os convergentes da expansão de* x *em frações contínuas, temos:*

$$|x - \frac{p_n}{q_n}| = \frac{1}{q_n\,(\alpha_{n+1} \cdot q_n + q_{n-1})} \qquad \textit{(I)}$$

ou

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1}+\beta_{n+1})\cdot q_n^2},\ \textit{onde}\ \beta_{n+1} = \frac{q_{n-1}}{q_n} = [0; a_n, a_{n-1}, a_{n-2}, ..., a_1] \qquad \textit{(II)}$$

Demonstração: Pela primeira igualdade do Corolário 3.3, temos que $x = \dfrac{\alpha_{n+1} \cdot p_n + p_{n-1}}{\alpha_{n+1} \cdot q_n + q_{n-1}}$ substituindo no primeiro membro da equação (I), obtemos:

$$\begin{aligned}
x - \frac{p_n}{q_n} &= \frac{\alpha_{n+1} \cdot p_n + p_{n-1}}{\alpha_{n+1} \cdot q_n + q_{n-1}} - \frac{p_n}{q_n} \\
&= \frac{(\alpha_{n+1} \cdot p_n + p_{n-1}) \cdot q_n + (\alpha_{n+1} \cdot q_n + q_{n-1}) \cdot (-p_n)}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} \\
&= \frac{\alpha_{n+1} \cdot p_n \cdot q_n + p_{n-1} \cdot q_n + (\alpha_{n+1} \cdot q_n) \cdot (-p_n) + (q_{n-1}) \cdot (-p_n)}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} \\
&= \frac{\cancel{\alpha_{n+1} \cdot p_n \cdot q_n} + p_{n-1} \cdot q_n - \cancel{\alpha_{n+1} \cdot p_n \cdot q_n} - q_{n-1} \cdot p_n}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} \\
&= \frac{p_{n-1} \cdot q_n - q_{n-1} \cdot p_n}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} = \frac{(-1)(p_n \cdot q_{n-1} - p_{n-1} \cdot q_n)}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})}
\end{aligned} \qquad \text{(III)}$$

Pela segunda afirmação da Proposição 3.2, temos que $p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = (-1)^{n-1}$, substituindo na equação (III), temos:

$$= \frac{(-1) \cdot (p_n \cdot q_{n-1} - p_{n-1} \cdot q_n)}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} = \frac{(-1) \cdot (-1)^{n-1}}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} = \frac{(-1)^n}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} \qquad \text{(IV)}$$

Para chegarmos na expressão (II), basta evidenciarmos q_n, ou seja

$$\begin{aligned}
= \frac{(-1)^n}{q_n \cdot (\alpha_{n+1} \cdot q_n + q_{n-1})} &= \frac{(-1)^n}{q_n \cdot [q_n \cdot (\alpha_{n+1} + \frac{q_{n-1}}{q_n})]} \\
&= \frac{(-1)^n}{q_n^2 \cdot (\alpha_{n+1} + \frac{q_{n-1}}{q_n})} \\
&= \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1}) \cdot q_n^2}
\end{aligned}$$

■

3.1.1 Reduzidas e Boas Aproximações

Dando continuidade a demonstrações de corolários, porém com a ênfase de mostrar que as frações contínuas, entre as ferramentas de aproximações, possui o menor erro de aproximação.

Corolário 3.5. *Seja x um número irracional e $\frac{p_n}{q_n}$ os convergentes da expansão de x em frações contínuas, temos que:*

$$|x - \frac{p_n}{q_n}| \leq \frac{1}{q_n^2}$$

Demonstração: Olhando para o primeiro membro da desigualdade, pelo Corolário 3.4, temos que:

$$|x - \frac{p_n}{q_n}| = \frac{1}{q_n\ (\alpha_{n+1}\ \cdot\ q_n\ +\ q_{n-1})} = \frac{1}{\alpha_{n+1}\ \cdot\ q_n^2\ +\ q_{n-1}\ \cdot\ q_n} < \frac{1}{\alpha_{n+1}\ \cdot\ q_n^2}$$

Por definição sabemos que a parte inteira de $\lfloor \alpha_{n+1} \rfloor = a_{n+1}$, que substituído na equação anterior obtemos o seguinte:

$$\frac{1}{\alpha_{n+1}\ \cdot\ q_n^2}\ \leq\ \frac{1}{a_{n+1}\ \cdot\ q_n^2}\ \leq\ \frac{1}{q_n^2}$$

Em particular, $\forall \alpha \in \mathbb{R}$, existem infinitos racionais $\frac{p}{q}$, com $p, q \in \mathbb{Z}$, tais que $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$, tal afirmação é conhecida como Teorema de Dirichlet.

Portanto, o que acabamos de demonstrar foi que o erro da aproximação que vem da fração contínua é sempre menor do que o inverso do quadrado do denominador, em resumo.

$$|x - \frac{p_n}{q_n}| < \frac{1}{\alpha_{n+1} \cdot q_n^2} \leq \frac{1}{a_{n+1} \cdot q_n^2} \leq \frac{1}{q_n^2}$$

■

Por outro lado, podemos observar pelo Corolário 3.4 que se:

i) n é par $\frac{p_n}{q_n} \leq x$

ii) n é ímpar $\frac{p_n}{q_n} \geq x$

Ou seja, x sempre vai pertencer ao intervalo $|x - \frac{p_n}{q_n}| + |x - \frac{p_{n+1}}{q_{n+1}}| = |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = |\frac{p_{n+1}\ \cdot\ q_n\ -\ p_n\ \cdot\ q_{n+1}}{q_n\ \cdot\ q_{n+1}}| = |\frac{(-1)^n}{q_n\ \cdot\ q_{n+1}}| = \frac{1}{q_n\ \cdot\ q_{n+1}}$

Um Corolário disso é a seguinte proposição

Proposição 3.3. $\forall n \in \mathbb{N}$, $|x - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}$ *ou* $|x - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{2q_{n+1}^2}$

Demonstração: Se a proposição fosse falsa, teríamos que
$|x - \frac{p_n}{q_n}| \geq \frac{1}{2q_n^2}$ ou $|x - \frac{p_{n+1}}{q_{n+1}}| \geq \frac{1}{2q_{n+1}^2}$ somando as duas desigualdades temos:

$$\begin{aligned}
&\frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} \leq |x - \frac{p_n}{q_n}| + |x - \frac{p_{n+1}}{q_{n+1}}| = \frac{1}{q_n \cdot q_{n+1}} \\
\Rightarrow\ &\frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} \leq \frac{1}{q_n \cdot q_{n+1}} \quad \Rightarrow \quad \frac{2q_{n+1}^2 + 2q_n^2}{4q_n^2 \cdot q_{n+1}^2} \leq \frac{1}{q_n \cdot q_{n+1}} \\
\Rightarrow\ &\frac{2\,(q_{n+1}^2 + q_n^2)}{4q_n^2 \cdot q_{n+1}^2} \leq \frac{1}{q_n \cdot q_{n+1}} \quad \Rightarrow \quad \frac{q_{n+1}^2 + q_n^2}{2q_n^2 \cdot q_{n+1}^2} \leq \frac{1}{q_n \cdot q_{n+1}}
\end{aligned}$$

Dividindo ambos os membros da desigualdade por $q_n \cdot q_{n+1}$, temos

$$\begin{aligned}
&\frac{q_{n+1}^2 + q_n^2}{2q_n \cdot q_{n+1}} \leq 1 \quad \Rightarrow \quad q_{n+1}^2 + q_n^2 \leq 2q_n \cdot q_{n+1} \\
\Rightarrow\ &q_{n+1}^2 - 2q_n \cdot q_{n+1} + q_n^2 \leq 0 \\
\Rightarrow\ &(q_{n+1} - q_n)^2 \leq 0 \quad \Rightarrow \quad q_{n+1} - q_n \leq 0 \\
\Rightarrow\ &q_{n+1} \leq q_n
\end{aligned}$$

Absurdo pois $q_{n+1} > q_n \forall n \geq 1$. Tal fato, decorre da utilização do corolário abaixo.
Corolário 3.1 de tal modo que $q_{n+1} = a_{n+1} \cdot q_n + q_{n-1} > q_n + q_{n-1} > q_n \ \ \forall n \geq 1$

■

Corolário 3.6. *Seja x um número irracional e $\frac{p_n}{q_n}$ os convergentes da expansão de x em frações contínuas, com isso temos que:*
$|x - \frac{p_n}{q_n}| > \frac{1}{(a_{n+1} + 2) \cdot q_n^2}$ *, onde* $a_{n+1} = \lfloor \alpha_{n+1} \rfloor$ *e* $\alpha_{n+1} < a_{n+1} + 1$

Demonstração: Pelo corolário 3.4, temos que

$$\begin{aligned}
|x - \frac{p_n}{q_n}| &= \frac{1}{q_n\,(\alpha_{n+1} \cdot q_n + q_{n-1})} \\
&= \frac{1}{\alpha_{n+1} \cdot q_n^2 + q_n \cdot q_{n-1}} \\
&> \frac{1}{(\alpha_{n+1} + 1) \cdot q_n^2} \\
&> \frac{1}{(a_{n+1} + 2) \cdot q_n^2}
\end{aligned}$$

■

3.1.2 Boas Aproximações São Reduzidas

O próximo teorema, caracteriza as reduzidas em termo do erro reduzido da aproximação de x por $\frac{p_n}{q_n}$, o que é por definição $|q_n \cdot x - p_n|$. A razão entre $|x - \frac{p_n}{q_n}|$ e o erro máximo da aproximação por falta com denominador q_n, ou seja, $\frac{1}{q_n}$. Em termos matemáticos temos que

$$\frac{|x - \frac{p_n}{q_n}|}{\frac{1}{q_n}} = |q_n \cdot x - p_n|$$

O que podemos também chamar de erro relativo.

Teorema 3.1. *Para todo $p, q \in \mathbb{Z}$, com $0 < q < q_{n+1}$ temos*

$$|q_n \cdot x - p_n| \leq |q \cdot x - p|$$

Além disso, se $0 < q < q_n$ a desigualdade acima é estrita.

Demonstração: Sabemos que pelo Corolário 3.4 que

Se n par $\frac{p_n}{q_n} < x \leq \frac{p_{n+1}}{q_{n+1}}$

Se n impar $\frac{p_{n+1}}{q_{n+1}} \leq x < \frac{p_n}{q_n}$

Suponhamos então sem perda de generalidade n par.

Pelo Corolário 3.2, sabemos que $mdc\,(p_n, q_n) = 1$, então se $\frac{p}{q} = \frac{p_n}{q_n}$ a desigualdade estaria satisfeita pois teríamos, $p = k \cdot p_n$ e $q = k \cdot q_n$, onde $k \in \mathbb{Z}$. Com isso temos:

$$|q_n \cdot x - p_n| \leq |q \cdot x - p| = |k \cdot q_n \cdot x - k \cdot p_n| = k\,|q_n \cdot x - p_n|$$

Sendo assim, podemos supor que $\frac{p}{q} \neq \frac{p_n}{q_n}$ de modo que:

$$|\frac{p}{q} - \frac{p_n}{q_n}| = |\frac{p \cdot q_n - p_n \cdot q}{q \cdot q_n}| \geq \frac{1}{q \cdot q_n} > \frac{1}{q_{n+1} \cdot q_n} = |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}|$$

Já que definimos $q < q_{n+1}$. Sendo assim, podemos dizer que $\frac{p}{q}$ esta fora do intervalo de estremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$, com isso temos duas possibilidades $\frac{p}{q} < \frac{p_n}{q_n}$ ou $\frac{p_{n+1}}{q_{n+1}} < \frac{p}{q}$.

1ª Possibilidade: Se $\frac{p}{q} < \frac{p_n}{q_n}$

$$|x - \frac{p}{q}| \geq |\frac{p_n}{q_n} - \frac{p}{q}| = |\frac{p_n \cdot q - p \cdot q_n}{q_n \cdot q}| \geq \frac{1}{q \cdot q_n}$$

por tanto temos $|x - \frac{p}{q}| \geq \frac{1}{q \cdot q_n}$,

se multiplicarmos tudo por $q > 0$, temos:

$$|x - \frac{p}{q}| \cdot q \geq \frac{1}{q \cdot q_n} \cdot q \Rightarrow |q \cdot x - p| \geq \frac{1}{q_n}$$

mas por outro lado sabemos que

$$|x - \frac{p_n}{q_n}| \leq |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = |\frac{p_{n+1} \cdot q_n - p_n \cdot q_{n+1}}{q_n \cdot q_{n+1}}| = \frac{1}{q_n \cdot q_{n+1}}$$

por tanto temos $|x - \frac{p_n}{q_n}| \leq \frac{1}{q_n \cdot q_{n+1}}$,
se multiplicarmos tudo por $q_n > 0$, temos:

$$|x - \frac{p_n}{q_n}| \cdot q_n \leq \frac{1}{q_n \cdot q_{n+1}} \cdot q_n \Rightarrow |q_n \cdot x - p_n| \leq \frac{1}{q_{n+1}}$$

com isso temos a seguinte situação $|q_n \cdot x - p_n| \leq \frac{1}{q_{n+1}} < \frac{1}{q_n} \leq |q \cdot x - p|$
Portanto, por transitividade

$$|q_n \cdot x - p_n| \leq |q \cdot x - p|$$

2ª Possibilidade: Se $\frac{p_{n+1}}{q_{n+1}} < \frac{p}{q}$.

$$|x - \frac{p}{q}| \geq |\frac{p}{q} - \frac{p_{n+1}}{q_{n+1}}| = |\frac{p \cdot q_{n+1} - p_{n+1} \cdot q}{q \cdot q_{n+1}}| \geq \frac{1}{q \cdot q_{n+1}}$$

por tanto temos: $|x - \frac{p}{q}| \geq \frac{1}{q \cdot q_{n+1}}$
se multiplicarmos tudo por $q > 0$, temos:

$$|x - \frac{p}{q}| \cdot q \geq \frac{1}{q \cdot q_{n+1}} \cdot q \Rightarrow |q \cdot x - p| \geq \frac{1}{q_{n+1}}$$

da primeira possibilidade temos que $\frac{1}{q_{n+1}} \geq |q_n \cdot x - p_n|$, então temos a seguinte situação $|q \cdot x - p| \geq \frac{1}{q_{n+1}} \geq |q_n \cdot x - p_n|$.
Portanto, por transitividade

$$|q \cdot x - p| \geq |q_n \cdot x - p_n|$$

■

O que acabamos de demonstrar no Teorema 3.1 é que as aproximações por frações contínuas além de serem muito boas, todas as aproximações que são muito boas, tem que vim das frações contínuas.

No próximo Teorema iremos demonstrar que qualquer número irracional tem infinitas apro-

ximações racionais, com erro menor que a metade do quadrado do denominador, ou seja, $\frac{1}{2q_n^2}$ e mostrar que qualquer aproximação racional de um número dado que tem essa propriedade tem que vim das frações contínuas.

Teorema 3.2. *Se* $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$ *então* $\frac{p}{q}$ *é uma reduzida da fração contínua de* α*, ou seja,* $\frac{p}{q} = \frac{p_n}{q_n}$.

Demonstração: Como no Teorema anterior, seja $n \in \mathbb{N}$ tal que $q_n < q < q_{n+1}$ sem perda de generalidade suponhamos n par, pelo Corolário 3.4 temos que $\frac{p_n}{q_n} < \alpha \leq \frac{p_{n+1}}{q_{n+1}}$, logo:

$$|\frac{p}{q} - \frac{p_n}{q_n}| = |\frac{p \cdot q_n - p_n \cdot q}{q \cdot q_n}| = \frac{1}{q \cdot q_n}$$

Suponhamos $\frac{p_n}{q_n} \neq \frac{p}{q}$.

$$|\frac{p}{q} - \frac{p_n}{q_n}| \geq \frac{1}{q \cdot q_n} > \frac{1}{q_n \cdot q_{n+1}} = |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}|$$

Ou seja, como no Teorema 3.1, $\frac{p}{q}$ esta fora do intervalo de extremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$. Com isso temos dois casos:

1ª Caso: $\frac{p}{q} < \frac{p_n}{q_n}$, com $q > q_n$.

$$|\alpha - \frac{p}{q}| > |\frac{p_n}{q_n} - \frac{p}{q}| \geq \frac{1}{q \cdot q_n} \geq \frac{1}{q^2} > \frac{1}{2q^2}$$

Absurdo pois, estamos supondo que $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$, logo $\frac{p}{q}$ não pode estar a esquerda de $\frac{p_n}{q_n}$

2ª Caso: $\frac{p}{q} > \frac{p_{n+1}}{q_{n+1}}$, deste temos duas possibilidades:

i) $q \geq \frac{q_{n+1}}{2} \Rightarrow 2q \geq q_{n+1}$

$$|\alpha - \frac{p}{q}| \geq |\frac{p}{q} - \frac{p_{n+1}}{q_{n+1}}| = |\frac{p \cdot q_{n+1} - p_{n+1} \cdot q}{q \cdot q_{n+1}}| \geq \frac{1}{q \cdot q_{n+1}} > \frac{1}{2q^2}$$

Absurdo pois $|\alpha - \frac{p}{q}| > \frac{1}{2q^2}$, que não é o que queremos.

ii) $q < \frac{q_{n+1}}{2} \Rightarrow 2q < q_{n+1}$.

$$|\alpha - \frac{p}{q}| \geq |\frac{p}{q} - \frac{p_{n+1}}{q_{n+1}}| = |\frac{p}{q} - \frac{p_n}{q_n}| - |\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| =$$
$$|\frac{p \cdot q_n - p_n \cdot q}{q \cdot q_n}| - |\frac{p_{n+1} \cdot q_n - p_n \cdot q_{n+1}}{q_{n+1} \cdot q_n}| \geq \frac{1}{q \cdot q_n} - \frac{1}{q_{n+1} \cdot q_n} =$$
$$\frac{q_{n+1} \cdot q_n - q \cdot q_n}{q \cdot q_n \cdot q_{n+1} \cdot q_n} = \frac{q_n \left(q_{n+1} - q\right)}{q_n \cdot q_{n+1} \cdot q \cdot q_n} = \frac{q_{n+1} - q}{q_{n+1} \cdot q \cdot q_n} =$$
$$\frac{q_{n+1} \left(1 - \frac{q}{q_{n+1}}\right)}{q_{n+1} \cdot q \cdot q_n} = \frac{1 - \frac{q}{q_{n+1}}}{q \cdot q_n}$$

Como temos que $q < \frac{q_{n+1}}{2} \Rightarrow q < q_{n+1} \cdot \frac{1}{2} \Rightarrow \frac{q}{q_{n+1}} < \frac{1}{2}$, logo:

$$\frac{1 - \frac{q}{q_{n+1}}}{q \ \cdot \ q_n} \geq \frac{1 - \frac{1}{2}}{q \ \cdot \ q_n} = \frac{\frac{1}{2}}{q \ \cdot \ q_n} = \frac{1}{2 \ \cdot \ q \ \cdot \ q_n} \geq \frac{1}{2q^2}$$

novamente um absurdo.

Esgotando assim todas as possibilidades de $\frac{p}{q} \neq \frac{p_n}{q_n}$, por tanto podemos concluir que $\frac{p}{q} = \frac{p_n}{q_n}$.

■

Ao fim deste tópico concluímos que quando estamos interessados em boas aproximações de um dado número real ou irracional, basta olharmos para as aproximações que vem das frações contínuas pois, todas as aproximações realmente muito boas, estão nas aproximações por frações contínuas.

3.2 Ternas Pitagóricas

O nome Ternas Pitagóricas provêm do fato da equação está relacionada com o teorema de Pitágoras sobre triângulos retângulos. Quando os lados de um tal triângulo forem números naturais, ele será chamado de Triângulo Pitagórico.

Mostraremos a seguir todas as soluções inteiras da equação $x^2 + y^2 = z^2$. As únicas soluções com uma das coordenadas nulas são $(0, b, \pm b)$, $(a, 0, \pm a)$, onde a e $b \in \mathbb{Z}$. Essas soluções são chamadas de soluções Triviais. Por outro lado, como os expoentes a que estão elevadas as incógnitas são todas pares, basta encontrar as soluções em Números Naturais. Após encontradas veremos como utilizar as informações obtidas para resolver outras equações em números inteiros.

Definição 3.3. *Uma Terna de números naturais (x, y, z) chama-se Pitagórica se $x^2 + y^2 = z^2$. Além disso, a Terna (x, y, z) chama-se Primitiva se $mdc\,(x, y, z) = 1$.*

Proposição 3.4. *Se (x, y, z) é uma Terna Pitagórica, com $k \geq 1$, então (xk, yk, zk) também será uma Terna Pitagórica.*

Demonstração: Dada a equação $x^2 + y^2 = z^2$, substituindo os valores xk, yk na equação temos:

$$(xk)^2 + (yk)^2 = x^2k^2 + y^2k^2 = k^2\ (x^2 + y^2)$$

como $x^2 + y^2 = z^2$, substituindo obtemos:

$$(xk)^2 + (yk)^2 = k^2z^2 = (kz)^2$$

■

Proposição 3.5. *Seja (x, y, z) uma Terna Primitiva, então*

$$mdc(x, y) = mdc\,(y, z) = mdc\,(x, z) = 1,$$

ou seja, x, y, z são relativamente primos dois a dois.

Demonstração: Seja $d = mdc\,(x, y) = 1$, suponhamos que exista um p primo, tal que $p|x$ e $p|y$, mas isso implica que $p^2|x^2$ e $p^2|y^2$ com isso podemos concluir, pela Proposição 1.6 que $p^2|x^2 + y^2$, ou seja, $p^2|z^2$ e isso implica que $p|z$. Como $mdc\,(x, y) = d$ e p também é um divisor comum de x e y, concluímos pelo Teorema 1.3 que $p \leq d$, ou seja, $p \leq 1$ que é um absurdo. Por tanto $mdc\,(x, y) = 1$ de modo análogo se demonstra que $mdc\,(y, z) = 1 = mdc\,(x, z)$.

■

Proposição 3.6. *Sejam (x, y, z) uma Terna Pitagórica qualquer , $d = mdc\,(x, y, z)$ e os quocientes $x_1 = \dfrac{x}{d}, y_1 = \dfrac{y}{d}$ e $z_1 = \dfrac{z}{d}$. Então (x_1, y_1, z_1) formam uma Terna Pitagórica Primitiva e vale (dx_1, dy_1, dz_1).*

Demonstração: Pelo Corolário 1.3, sabemos que $mdc\,(x_1, y_1, z_1) = 1$, e como vale $(x, y, z) = (dx_1, dy_1, dz_1)$, temos:

$$(x_1)^2 + (y_1)^2 = (\frac{x}{d})^2 + (\frac{y}{d})^2 = \frac{x^2}{d^2} + \frac{y^2}{d^2} = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = (\frac{z}{d})^2 = z_1^2$$

Por tanto, o que acabamos de demonstrar é que (x_1, y_1, z_1) é uma Terna Pitagórica Primitiva e para encontrarmos uma Terna Pitagórica não Primitiva, basta multiplicar os seus elementos por um número positivo maior do que 1, ou seja, todas as soluções de $x^2 + y^2 = z^2$ resultam de (x_1, y_1, z_1), onde $mdc\,(x_1, y_1, z_1) = 1$.

■

Proposição 3.7. *A soma dos quadrados de dois números inteiros ímpares nunca pode ser um quadrado perfeito.*

Demonstração: Suponhamos $b = 2k + 1$ e $c = 2q + 1$, com $k, q \in \mathbb{Z}$. Dessa forma, temos

$$b^2 + c^2 = (2k+1)^2 + (2q+1)^2 = (4k^2 + 4k + 1) + (4q^2 + 4q + 1) = 4\,(k^2 + k + q^2 + q) + 2$$

onde podemos chamar $(k^2+k+q^2+q) = w \in \mathbb{N}$, logo $4w+2$ é par. Porém, não é um quadrado perfeito pois pelo Corolário 1.5, item b), todo quadrado perfeito quando dividido por 4, deixa resto 0 ou 1, que não é o caso.

■

Proposição 3.8. *Dado três inteiros positivos a, b e c onde $a^2 = b^2 + c^2$, então b ou c é par e o outro é impar, e pelo menos um dentre a, b e c é um múltiplo de 5.*

Demonstração: Pela Proposição 3.7 o número b ou c tem que ser par, senão a não seria um quadrado perfeito, com isso podemos supor sem perda de generalidade que b é par, logo c é ímpar o que conclui a primeira parte da demonstração.

Agora provaremos que a, b ou c é múltiplo de 5.

Suponhamos que b e c não seja múltiplo de 5, como b^2 e c^2 são quadrado perfeitos, pelo Corolário 1.5 item d), a^2 e c^2 são da forma:

$b^2 = 5k \pm 1$ e $c^2 = 5q \pm 1$, logo $a^2 = (5k^2 \pm 1) + (5q \pm 1)$ onde $k, q \in \mathbb{N}$, testando todas as possibilidades temos:

1) $a^2 = (5k+1) + (5q+1) = 5k + 5q + 2 = 5\,(k+q) + 2 = 5w + 2$

2) $a^2 = (5k+1) + (5q-1) = 5k + 5q = 5\,(k+q) = 5w$

3) $a^2 = (5k-1) + (5q+1) = 5k + 5q + 2 = 5\,(k+q) + 2 = 5w + 2$

4) $a^2 = (5k-1) + (5q-1) = 5k + 5q - 2 = 5\,(k+q) - 2 = 5w - 2$

Com isso podemos perceber que $a^2 = b^2 + c^2$ é da forma $5w$ ou $5w \pm 2$. Pelo Corolário 1.5 item d), sabemos que a^2 só pode ser da forma $5w$ ou $5w \pm 1$ e não $5w \pm 2$. O que nos resta que $a^2 = 5w$, por tanto a é múltiplo de 5.

■

Teorema 3.3. *Os termos (x, y, z) de inteiros não nulos tais que $x^2, y^2 = z^2$ são dados por:*

$$\begin{cases} x = 2 \cdot u \cdot v \cdot d \\ y = (u^2 - v^2) \cdot d \\ z = (u^2 + v^2) \cdot d \end{cases} \quad \textit{ou} \quad \begin{cases} x = (u^2 - v^2) \cdot d \\ y = 2 \cdot u \cdot v \cdot d \\ z = (u^2 + v^2) \cdot d \end{cases},$$

onde d, u e v são inteiros não nulos, com u e v de paridade diferentes, ou seja, $mdc\,(u, v) = 1$.

Demonstração: Dada a equação $x^2 + y^2 = z^2$, se escolhermos $x = 0$ ou $y = 0$, teríamos as chamadas soluções triviais $(0, y, \pm y)$ ou $(x, 0, \pm x)$. São soluções $\forall, x, y \in \mathbb{Z}$, com isso sem perda de generalidade, suponhamos x, y, z inteiros positivos.

Se $d = mdc\,(x, y, z)$, pela Proposição 3.6, temos que:

$$x = d \cdot b,\ y = d \cdot c \ \text{ e } \ z = d \cdot a,$$

onde $mdc\,(b, c, a) = 1$ e pela Proposição 3.5 $mdc\,(b, c) = mdc\,(b, a) = mdc\,(c, a) = 1$ e pela Proposição 3.8, sabemos que b e c possuem paridade diferente, suponhamos então sem perda de generalidade c é par e b é ímpar, por tanto a será ímpar, com isso temos o seguinte:

$$b^2 + c^2 = a^2 \quad \Longrightarrow \quad b^2 = a^2 - c^2 \quad \Longrightarrow \quad b^2 = (a + c) \cdot (a - c),$$

como b é ímpar, obtemos que $(a+c), (a-c)$ serão ambos ímpares e $mdc\,(a+c, a-c) = 1$. Com efeito: seja $r = mdc\,(a + c, a - c)$, implicando que $r|a + c$ e $r|a - c$ e, pela mesma Proposição 1.6, temos

$$r|(a + c) + (a - c) = 2a \quad \Longrightarrow \quad r|mdc\,(2a, 2c)$$

e pela Proposição 1.6, $r|(a + c) - (a - c) = 2c$.

Se $r|2a$ e $r|2c$ pela Proposição 1.4, $r|2\,mdc\,(a, c)$, como $mdc\,(a, c) = 1$, temos que $r|2 \cdot 1$ ou seja $r|2$, o que nos leva a $r = 1$ ou $r = 2$, porém $a + c, a - c$ são ambos ímpares, ou seja, eles não são múltiplos de 2. Assim, o que nos resta que é $mdc\,(a + c, a - c) = 1$

Como $b^2 = (a + c) \cdot (a - c)$ e concluímos que $mdc\,(a + c, a - c) = 1$, temos pelo Corolário 1.4 item b), que existem inteiros u e v tais que:

$$a + c = u^2 \ \text{ e } \ a - c = v^2$$

Resolvendo o sistema obtemos:

$a + c = u^2$ (I)

$\underline{a - c = v^2}$ (II)

$2a = u^2 + v^2 \Rightarrow a = \dfrac{u^2 + v^2}{2}$, substituindo o valor de a na equação (I), temos:

$a + c = u^2 \Rightarrow c = u^2 - a \Rightarrow c = u^2 - (\dfrac{u^2 + v^2}{2}) \Rightarrow c = \dfrac{u^2 - v^2}{2}$

Com isso já sabemos o valor de $a = \dfrac{u^2 + v^2}{2}$, $c = \dfrac{u^2 - v^2}{2}$, só nos resta encontrar um valor de b, substituindo o valor de (I) e (II) em: onde $b^2 = (a + c) \cdot (a - c)$, temos: $b^2 = u^2 \cdot v^2 \Rightarrow$

$$b = u \cdot v$$

Onde as soluções podem ser da forma:

$$(x, y, z) = (d \cdot b, d \cdot c, d \cdot a) = (d \cdot u \cdot v, d \cdot \frac{u^2 - v^2}{2}, d \cdot \frac{u^2 + v^2}{2})$$

Podemos multiplicar tudo por 2, que teremos as soluções da seguinte forma:

$$(2 \cdot d \cdot u \cdot v, 2 \cdot d \cdot \frac{u^2 - v^2}{2}, 2 \cdot d \cdot \frac{u^2 + v^2}{2}) = (2duv, d\,(u - v^2), d\,(u^2 + v^2)),$$

ou

$$(d\,(u^2 - v^2), 2duv, d\,(u^2 + v^2))$$

■

Exemplo 3.2. *Ache todas as soluções inteiras não nulas da equação*

$$x^2 + y^2 = 2z^2, \text{ com } x \neq \pm y.$$

Solução: Dada a equação $x^2 + y^2 = 2z^2$, (I)
pela proposição 3.7, devemos ter x e y ambos pares ou ambos ímpares, pois caso contrário, $x^2 + y^2$ seria ímpar.

Tomando como artifício $x = a + b$, $y = a - b$, substituindo na equação (I), temos:

$$\begin{aligned}(a+b)^2 + (a-b)^2 = 2z^2 &\Rightarrow a^2 + 2ab + b^2 + a^2 - 2ab + b^2 = 2z^2 \\ &\Rightarrow a^2 + b^2 + a^2 + b^2 = 2z^2 \\ &\Rightarrow 2a^2 + 2b^2 = 2z^2 \\ &\Rightarrow a^2 + b^2 = z^2, \qquad (II)\end{aligned}$$

onde a solução da equação (II), pela proposição 3.3, são do tipo:

$$\begin{cases} x = 2 \cdot u \cdot v \cdot d \\ y = (u^2 - v^2) \cdot d \\ z = (u^2 + v^2) \cdot d \end{cases} \quad \text{ou} \quad \begin{cases} x = (u^2 - v^2) \cdot d \\ y = 2 \cdot u \cdot v \cdot d \\ z = (u^2 + v^2) \cdot d \end{cases}$$

i) Substituindo em $x = a + b$, temos que:

$$x = 2 \cdot u \cdot v \cdot d + (u^2 - v^2) \cdot d = (2 \cdot u \cdot v + u^2 - v^2) \cdot d$$

ou

$$x = (u^2 - v^2) \cdot d + 2 \cdot u \cdot v \cdot d = (u^2 - v^2 + 2 \cdot u \cdot v) \cdot d$$

ii) Substituindo $y = a - b$, temos que:

$$y = 2 \cdot u \cdot v \cdot d - (u^2 - v^2) \cdot d = (2 \cdot u \cdot v - u^2 + v^2) \cdot d$$

ou

$$y = (u^2 - v^2) \cdot d - 2 \cdot u \cdot v \cdot d = (u^2 - v^2 - 2 \cdot u \cdot v) \cdot d$$

Portanto, as soluções de (I), são dos tipos:

$$[x, y, z] = [(2 \cdot u \cdot v + u^2 - v^2) \cdot d, (2 \cdot u \cdot v - u^2 + v^2) \cdot d, (u^2 + v^2) \cdot d]$$
ou
$$[x, y, z] = [(2 \cdot u \cdot v + u^2 - v^2) \cdot d, (u^2 - v^2 - 2 \cdot u \cdot v) \cdot d, (u^2 + v^2) \cdot d]$$

Exemplo 3.3. *Encontre as soluções em* $\mathbb{N}$ *de* $3^m + 7 = 2^n$.

Solução:

i) Primeiramente podemos olhar para a equação mod 3, com isso temos:

$$3^m + 7 = 2^n \Rightarrow 3^m + 7 \equiv 1 \equiv 2^n \equiv (-1)^n \,(\text{mod } 3)$$

como $1 \equiv (-1)^n \,(\text{mod } 3)$, isso implica que n é par, ou seja, é da forma $n = 2k$.

ii) Como $n = 2k$, isso implica que $3^m + 7 = 2^{2k} = 4k$, aplicando a linguagem de congruência mod 4 na equação, temos:

$$3^m + 7 = 4^k \Rightarrow 3^m + 7 \equiv 0 \equiv (-1)^m - 1 \equiv \text{ mod } 4$$

como $0 \equiv (-1)^m - 1 \,(\text{mod } 4)$, isso implica que m é par, ou seja, é da forma $m = 2l$.

Substituindo na equação, temos:

$$3^m + 7 = 2^n \Rightarrow 3^{2l} + 7 = 2^{2k} \Rightarrow 2^{2k} - 3^{2l} = 7 \Rightarrow (2^k + 3^k)(2^k - 3^k) = 7$$

Como 7 é primo, temos que:

$2^k + 3^l = 7$ (I)

$\underline{2^k - 3^l = 1}$ (II)

$2^k + 2^k = 8 \Rightarrow 2 \cdot 2^k = 8 \Rightarrow 2^k = 4 \Rightarrow k = 2$

Substituindo o valor em (I), temos:

$$2^k + 3^l = 7 \Rightarrow 2^2 + 3^l = 7 \Rightarrow 3^l = 7 - 4 \Rightarrow 3^l = 3 \Rightarrow l = 1$$

Com isso, temos que:

$$m = 2l = 2 \cdot 1 = 2$$
$$n = 2k = 2 \cdot 2 = 4$$

3.3 Equação de Pell

Neste tópico, estudaremos a chamada equação de Pell, isto é, a equação Diofantina.

$$x^2 - Ay^2 = 1 \qquad \text{(I)}$$

Onde A é dado como inteiro arbitrário, nos casos em que $A < 0$ (Elipse), nos casos em que A é um quadrado perfeito maior do que zero (Hipérbole, cuja razão entre o maior e o menor eixo é racional), nesse caso a equação (I) admite apenas as chamadas soluções Triviais, e para $A = 0$ (reta dupla) um número infinito. Por outro lado, o fato de (I) ter um número infinito de soluções para o caso em que A um número positivo livre de quadrados (Hipérbole, cuja a razão entre o eixo maior e o eixo menor é irracional), se revelará um Teorema bastante profundo, no qual, será o nosso objeto de estudo deste tópico.

3.3.1 Soluções Triviais da equação de Pell

Em primeiro lugar, trataremos dos casos especiais da (I).

1º Caso, para $A < -1$:

Como $1 \geq |A|\, y^2$, devemos ter $y = 0$ e $x = \pm 1$.

2º Caso, para $A = -1$:

Substituindo em (1) temos $x^2 + y^2 = 1$, claramente teremos as quatros soluções para $x = 0, y = \pm 1$ ou para $y = 0, x = \pm 1$.

3º Caso, para $A = a^2 > 0$ ou de uma outra forma $A \in \mathbb{N}$ mais $\sqrt{A} \notin \mathbb{N}$.

Substituindo em Equação (I), temos:

$$x^2 - a^2 \cdot y^2 = (x + ay) \cdot (x - ay) = 1$$

O produto de dois inteiros é 1 se ambos forem 1 ou ambos forem -1. Logo, essa equação só é possível se:

$$(x + ay) = (x - ay)$$

Resolvendo a equação temos:

$$(x + ay) = (x - ay) \Rightarrow x + ay - x + ay = 0 \Rightarrow 2ay = 0 \Rightarrow y = 0$$

Substituindo na equação Equação (I) o valor de $y = 0$, temos que $x = \pm 1$, com isso podemos concluir que quando A é um quadrado perfeito, temos apenas as soluções triviais $x = \pm 1$ e $y = 0$.

Portanto, pelo que acabamos de mostrar, certamente a Equação (I) possui as soluções:

$$x = \pm 1 \qquad y = 0$$

Nosso objetivo neste tópico é mostrar que existem muito mais. Por isso, assumiremos de agora em diante que $A \in \mathbb{N}$ não é um quadrado perfeito e portanto $\sqrt{A}$ é um número irracional.

De fato, se $\sqrt{A} = \dfrac{p}{q}$, com $p, q \in \mathbb{Z}$, $q \neq 0$, podemos supor $mdc\,(p, q) = 1$, isso nos leva admitir que $q > 1$ pois $\sqrt{A} \notin \mathbb{N}$, com isso temos que $A = \dfrac{p^2}{q^2}$, como $mdc\,(p, q) = 1$, pelo Corolário 1.4 item a), $mdc\,(p^2, q^2) = 1$, como temos $q > 1 \Rightarrow q^2 > 1$, absurdo pois $A \in \mathbb{N}$, e um número natural não pode ser escrito como a razão de dois inteiros positivos primos entre si com o denominador maior do que 1.

A equação de Pell como já foi falado correspondem a pontos inteiros sobre uma hipérbole. Por exemplo $x^2 - 2y^2 = 1$;

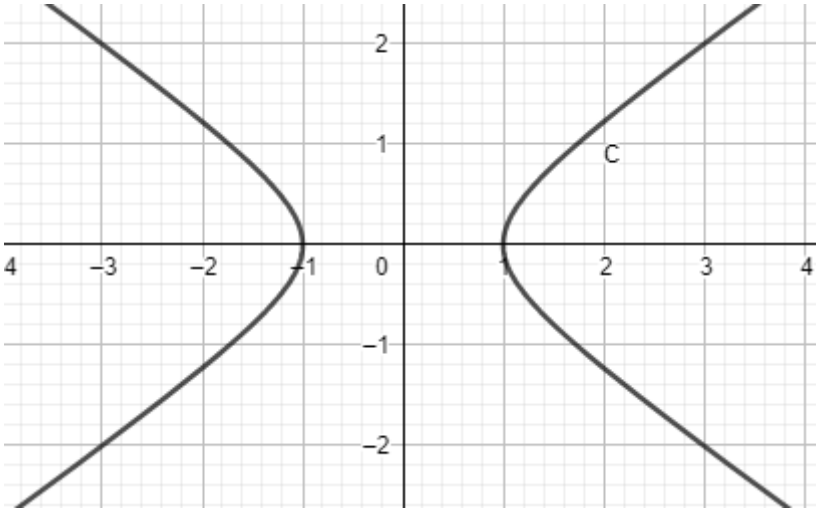

Figura 3.1: Hipérbole.

Na figura acima, a hipérbole é $x^2 - 2y^2 = 1$: o ponto $(3, 2)$ é um exemplo de ponto inteiro pertencente ao conjunto de pontos sobre a Hipérbole pois $3^2 - 2 \cdot 2^2 = 1$ mas o ponto $(7, 5)$ está próximo a hipérbole mais não pertence ao conjunto de soluções pois $7^2 - 2 \cdot 5^2 = -1 \neq 1$.

A seguir definiremos uma função que se chama *norma*, que leva a números da forma $x + y\sqrt{A}$, exatamente em $x^2 - Ay^2$, e tal ferramenta nos auxiliará na demonstração de alguns teoremas e proposições.

Definição 3.4. *Sejam*

$$\mathbb{Z}\,[\sqrt{A}] = \{x + y\sqrt{A}; x, y \in \mathbb{Z}\} \quad \textit{e} \quad \mathbb{Q}\,[\sqrt{A}] = \{x + y\sqrt{A}; x, y \in \mathbb{Q}\} \supset \mathbb{Z}\,[\sqrt{A}].$$

Dado $\boldsymbol{y} = x + y\sqrt{A} \in \mathbb{Q}[\sqrt{A}]$ *com* $x, y \in \mathbb{Q}$*, podemos definir seu conjugado como* $\hat{\boldsymbol{y}} = x - y\sqrt{A}$*, e sua Norma* $N\,(\boldsymbol{y}) = y \cdot \hat{y} = (x + y\sqrt{A}) \cdot (x - y\sqrt{A}) = x^2 - A \cdot y^2$.

Proposição 3.9. *Dado* $x, y, z, w \in \mathbb{Q}$ *e* $x + y\sqrt{A} = z + w\sqrt{A}$*, então* $x = z$ *e* $y = w$.

Demonstração:

$x + y\sqrt{A} = z + w\sqrt{A} \Rightarrow y\sqrt{A} - w\sqrt{A} = z - x \Rightarrow \sqrt{A}\,(y - w) = z - x.$

Se $(y - w) = 0 \Rightarrow y = w$ e $z - x = (y - w)\,\sqrt{A} \Rightarrow z - x = 0 \Rightarrow z = x.$

Se $(y - w) \neq 0 \Rightarrow \sqrt{A}\,(y - w) = z - x \Rightarrow \sqrt{A} = \dfrac{z - x}{y - w}$, absurdo pois $\sqrt{A} \notin \mathbb{Q}$ de outra forma isso é, um absurdo pois, um racional menos um racional, sobre um racional menos um racional é um racional e $\sqrt{A}$ não é racional.

Por tanto o que acabamos de demonstrar é que números desta forma $x + y\sqrt{A}$, possuem uma única representação dessa forma.

Um fato muito importante é que a Norma é uma função multiplicativa.

Proposição 3.10. *Dado a função* $N : \mathbb{Q}\,[\sqrt{A}] \longrightarrow \mathbb{Q}$ *é uma função multiplicativa, e* $x + y\sqrt{A}, u + v\sqrt{A} \in \mathbb{Q}\,[\sqrt{A}] \times \mathbb{Q}[\sqrt{A}]$, *então* $N\,((x + y\sqrt{A}) \cdot (u + v\sqrt{A})) = N\,(x + y\sqrt{A}) \cdot N\,(u + v\sqrt{A})$.

Demonstração:

Sabemos por definição que $N\,(x + y\sqrt{A}) = x^2 - Ay^2$ e $N\,(u + v\sqrt{A}) = u^2 - Av^2$

$(x+y\sqrt{A})\cdot(u+v\sqrt{A}) = (xu+xv\sqrt{A}+uy\sqrt{A}+yvA) = (xu+yvA)+(xv\sqrt{A}+uy\sqrt{A}) = (xu+Ayv)+(xv+yu)\,\sqrt{A}$ (I)

Agora faremos o produto dos seus conjugados

$(x-y\sqrt{A})\cdot(u-v\sqrt{A}) = (xu-xv\sqrt{A}-uy\sqrt{A}+yvA) = (xu+Ayv)+(-uy\sqrt{A}-xv\sqrt{A}) = (xu+Ayv)-(uy\sqrt{A}+xv\sqrt{A}) = (xu+Ayv)-(xv+yu)\,\sqrt{A}$ (II)

Ao multiplicarmos (I) vezes (II) temos:

$$
\begin{aligned}
[(xu + Ayv) + (xv + yu)\,\sqrt{A}] \cdot [(xu + Ayv) - (xv + yu)\,\sqrt{A}] &= \\
(xu + Ayv)^2 - [(xv + yu)\,\sqrt{A}]^2 &= \\
(xu + Ayv)^2 - A\,(xv + yu)^2 &= \\
x^2u^2 + 2xuAyv + A^2y^2v^2 - A\,(x^2v^2 + 2xvyu + y^2u^2) &= \\
x^2u^2 + \cancel{2xuAyv} + A^2y^2v^2 - \cancel{2xuAyv} - Ax^2v^2 - Ay^2u^2 &= \\
x^2u^2 - Ax^2v^2 + A^2y^2v^2 - Ay^2u^2 &= \\
x^2\,(u^2 - Av^2) + A\,(Ay^2v^2 - y^2u^2) &= \\
x^2\,(u^2 - Av^2) + Ay^2\,(Av^2 - u^2) &= \\
x^2\,(u^2 - Av^2) - Ay^2\,(u^2 - Av^2) &= \\
(u^2 - Av^2) \cdot [x^2 - Ay^2] &= \\
(x^2 - Ay^2) \cdot (u^2 - Av^2) &= \\
N\,(x + y\sqrt{A}) \cdot N\,(u + v\sqrt{A})
\end{aligned}
$$

Por tanto o que acabamos de demonstrar é que a Norma do produto é igual ao produto das Normas.

■

É fácil observar (a partir da multiplicatividade da Norma) que se a equação possui alguma solução inicial (x_1, y_1) com $y_1 \neq 0$ então possui infinitas.

Mais geralmente, se $x_1^2 - Ay_1^2 = \pm 1$, temos:

$$N\left((x_1 + \sqrt{A}y_1)^n\right) = (x_1 + y_1\sqrt{A})^n \cdot (x_1 - y_1\sqrt{A})^n = (x_1^2 - Ay_1^2)^n = (\pm 1)^n$$

.

Podemos utilizar o Binômio de Newton para descrever todas as soluções de $x^2 - Ay^2 = 1$, aplicado na solução inicial, conhecida como solução mínima ou fundamental.

$$x_n + \sqrt{A}y_n = (x_1 + y_1\sqrt{A})^n =$$

$$x_1^n + \binom{n}{1} x_1^{n-1} \cdot y_1 \cdot \sqrt{A} + \binom{n}{2} x_1^{n-2} \cdot y_1^2 \cdot A + \binom{n}{3} x_1^{n-3} \cdot y_1^3 \cdot A\sqrt{A} + \binom{n}{4} x_1^{n-4} \cdot y_1^4 \cdot A^2 + ...$$

$$\Rightarrow x_n = x_1^n + \binom{n}{2} x_1^{n-2} \cdot y_1^2 \cdot A + \binom{n}{4} x_1^{n-4} \cdot y_1^4 \cdot A^2 + ... \Rightarrow$$

$$x_n = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} x_1^{n-2i} \cdot y_1^{2i} \cdot A^i$$

$$\sqrt{A} \cdot y_n = \sqrt{A}\left[\binom{n}{1} x_1^{n-1} \cdot y_1 + \binom{n}{3} x_1^{n-3} \cdot y_1^3 \cdot A + ...\right]$$

$$\Rightarrow y_n = \binom{n}{1} x_1^{n-1} \cdot y_1 + \binom{n}{3} x_1^{n-3} \cdot y_1^3 \cdot A + ... \Rightarrow$$

$$y_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} x_1^{n-2i-1} \cdot y_1^{2i+1} \cdot A^i$$

Veremos agora que a equação de Pell sempre terá solução.

Teorema 3.4. *A equação $x^2 - Ay^2 = 1$, com A diferente de um quadrado perfeito, possui solução não trivial em inteiros positivos, isto é, com $x + y\sqrt{A} > 1$.*

Demonstração:

Como A é um número livre de quadrados, ou seja, $\sqrt{A} \notin \mathbb{Q}$. Pelo Corolário 3.5, conhecida como Lema de Dirichlet nos garante que a desigualdade $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$ tem infinitas soluções racionais $p|q$. Note que

$$|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2} \qquad \text{ou} \qquad |\frac{p}{q} - \sqrt{A}| < \frac{1}{q^2} \tag{I}$$

Sendo assim olhamos primeiramente para a $N\ (p + q\sqrt{A}) = p^2 - A \cdot q^2$, então temos que

$$|p^2 - Aq^2| = |(p + q\sqrt{A}) \cdot (p - q\sqrt{A})| = \frac{q^2}{q^2}\ |(p + q\sqrt{A}) \cdot (p - q\sqrt{A})| =$$
$$q^2\ |\frac{(p + q\sqrt{A})}{q} \cdot \frac{(p - q\sqrt{A})}{q}| = q^2\ |(\frac{p}{q} + \sqrt{A}) \cdot (\frac{p}{q} - \sqrt{A})|$$

Pela desigualdade (I), temos:

$$q^2\ |(\frac{p}{q} + \sqrt{A}) \cdot (\frac{p}{q} - \sqrt{A})| < \cancel{q^2} \cdot |\frac{p}{q} + \sqrt{A}| \cdot \frac{1}{\cancel{q^2}} = |\frac{p}{q} + \sqrt{A}| = |\frac{p}{q} - \sqrt{A} + 2\sqrt{A}|$$

que pela desigualdade Triangular

$$|\frac{p}{q} - \sqrt{A} + 2\sqrt{A}| \leq 2\sqrt{A} + |\frac{p}{q} - \sqrt{A}|$$

que pela desigualdade (I), temos

$$2\sqrt{A} + |\frac{p}{q} - \sqrt{A}| < 2\sqrt{A} + \frac{1}{q^2} \leq 2\sqrt{A} + 1$$

Sendo assim, podemos considerar infinitos pares de inteiros positivos (p_n, q_n) com

$$|\sqrt{A} - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$$

onde teremos sempre que $a|N\ (p_n + q_n\sqrt{A})| = |p_n^2 - Aq_n^2| < 2\sqrt{A} + 1$, por tanto teremos um número finito de possibilidades para o valor (inteiro) de $p_n^2 - Aq_n^2$. Consequentemente, existe um inteiro $k \neq 0$ tal que $p_n^2 - Aq_n^2 = k$ para infinitos valores de n. Observa-se que se tivéssemos $k = 0$, teríamos um absurdo pois,

$$p^2 - Aq^2 = 0 \Rightarrow p^2 = Aq^2 \Rightarrow \frac{p^2}{q^2} = A \Rightarrow \left(\frac{p}{q}\right)^2 = A \Rightarrow \frac{p}{q} = \sqrt{A}$$

onde temos que $\sqrt{A} \in \mathbb{Q}$. Logicamente um absurdo.

Da equação $p_n^2 - Aq_n^2 = k$, obtemos duas sequências crescentes de pares de inteiros positivos $(u_r), (v_r), r \in \mathbb{N}$ tais que $u_r^2 - v_r^2 = k$ para todo r.

Como há apenas $|k|^2$ possibilidades para os pares $(u_r\ mod\ k, v_r\ mod\ k)$ existem inteiros $(a, b) \in \{0, 1, 2, 3, ..., |k| - 1\}$ para infinitos valores de r tais que $(u_r \equiv a\ (mode\ k)$ e $v_r \equiv b\ (mod\ k))$. Tomamos $(u_b, v_b) \neq (u_r, v_r)$ de modo que:

$$(u_b, v_b) \neq (u_r, v_r) \Rightarrow u_b + v_b\sqrt{A} \neq u_r + v_r\sqrt{A}$$

De tal forma que $u_b^2 - Av_b^2 = u_r^2 - Av_r^2 = k$, com $u_b \equiv u_r \ (mod\ |k|)$ e $v_b \equiv v_r \ (mod\ |k|)$ (II)

Suponhamos sem perda de generalidade $1 \leq u_r + v_r\sqrt{A} < u_b + v_b\sqrt{A}$ com isso consideremos o número $x + y\sqrt{A} = \dfrac{u_b + v_b\sqrt{A}}{u_r + v_r\sqrt{A}} > 1$, temos que:

$$\begin{aligned} x + y\sqrt{A} &= \frac{u_b + v_b\sqrt{A}}{u_r + v_r\sqrt{A}} \cdot \frac{u_r - v_r\sqrt{A}}{u_r - v_r\sqrt{A}} \\ &= \frac{u_b \cdot u_r - u_b \cdot v_r\sqrt{A} + v_b\sqrt{A} \cdot u_r - v_b \cdot v_r \cdot A}{u_r^2 - A \cdot v_r^2} \\ &= \frac{(u_b \cdot v_r - A \cdot v_b \cdot v_r) + (v_b \cdot u_r - u_b \cdot v_r)\sqrt{A}}{u_r^2 - A \cdot v_r^2} \end{aligned}$$

Como $u_r^2 - A \cdot v_r^2 = k$, temos

$$\begin{aligned} x + y\sqrt{A} &= \frac{(u_b \cdot v_r - A \cdot v_b \cdot v_r) + (v_b \cdot u_r - u_b \cdot v_r)\sqrt{A}}{k} \\ &= \frac{(u_b \cdot v_r - A \cdot v_b \cdot v_r)}{k} + \frac{(v_b \cdot u_r - u_b \cdot v_r)\sqrt{A}}{k} \end{aligned}$$

Olhando para $u_b \cdot v_r - A \cdot v_b \cdot v_r$, por (II), temos

$$u_b \cdot v_r - A \cdot v_b \cdot v_r \equiv u_b^2 - Av_b^2 = k \equiv 0 \ (mod\ |k|)$$

e

$$v_b \cdot u_r - u_b \cdot v_r \equiv a \cdot b - b \cdot a = 0 \equiv 0 \ (mod\ k)$$

Portanto, $x = \dfrac{u_b \cdot v_r - A \cdot v_b \cdot v_r}{k}$ e $y = \dfrac{v_b \cdot u_r - u_b \cdot v_r}{k}$ são números inteiros. Por outro lado, como

$$x + y\sqrt{A} = \frac{u_b + v_b\sqrt{A}}{u_r + v_r\sqrt{A}} \Rightarrow (x + y\sqrt{A}) \cdot (u_r + v_r\sqrt{A}) = u_b + v_b\sqrt{A}$$

onde,

$$N\ (x + y\sqrt{A}) \cdot N\ (u_r + v_r\sqrt{A}) = N\ (u_b + v_b\sqrt{A})$$

Como $N\ (u_r + v_r\sqrt{A}) = u_r^2 - A \cdot v_r^2 = k$ e $N\ (u_b + v_b\sqrt{A}) = u_b^2 - A \cdot v_b^2 = k$
Temos:

$$\begin{aligned} N\ (x + y\sqrt{A}) \cdot N\ (u_r + v_r\sqrt{A}) &= N\ (u_b + v_b\sqrt{A}) \\ &\Rightarrow N\ (x + y\sqrt{A}) \cdot k = k \\ &\Rightarrow N\ (x + y\sqrt{A}) = \frac{k}{k} = 1 \end{aligned}$$

onde,

$$N\ (x + y\sqrt{A}) = x^2 - Ay^2 = 1$$

■

Teorema 3.5. *Se $A > 1$ é um número natural livre de quadrados, então a equação $x^2 - Ay^2 = 1$ admite infinitas soluções em inteiros positivos x e y. Mais precisamente, se $x = x_1$ e $y = y_1$ é a solução em inteiros positivos para o qual a soma $x + y\sqrt{A}$ é a menor possível, então as demais soluções inteiras positivas da equação são dadas pelos naturais (x_n, y_n) que satisfazem a igualdade*

$$x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n \text{ , onde } N \in \mathbb{N}$$

.

Demonstração:

Demonstraremos que (x_1, y_1) é a nossa solução miníma, se como antes, definimos $(x_n, y_n) \in \mathbb{N}^2$ pela relação $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$, temos que $(x_n, y_n), n \geq 1$, são todas as soluções inteiras positivas da equação de Pell. De fato, já vimos que (x_n, y_n) são soluções, e se (x', y') é uma outra solução, então como $x_1 + y_1\sqrt{A} > 1$ existe $n \geq 1$ tal que

$$(x_1 + y_1\sqrt{A})^n \leq x' + y'\sqrt{A} < (x_1 + y_1\sqrt{A})^{n+1}$$

Multiplicando por $x_n - y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^{-n} > 0$, obtemos

$$(x_1+y_1\sqrt{A})^n \cdot (x_1+y_1\sqrt{A})^{-n} \leq (x'+y'\sqrt{A}) \cdot (x_n-y_n\sqrt{A}) < (x_1+y_1\sqrt{A})^{n+1} \cdot (x_1+y_1\sqrt{A})^{-n}$$

$$(x_1 + y_1\sqrt{A})^{n-n} \leq (x' + y'\sqrt{A}) \cdot (x_n - y_n\sqrt{A}) < (x_1 + y_1\sqrt{A})^{n+1-n}$$

$$1 \leq (x' + y'\sqrt{A}) \cdot (x_n - y_n\sqrt{A}) < (x_1 + y_1\sqrt{A})^1$$

Como $N\ ((x' + y'\sqrt{A}) \cdot (x_n - y_n\sqrt{A})) = N\ (x' + y'\sqrt{A}) \cdot N\ (x_n - y_n\sqrt{A}) = ((x')^2 - A\ (y')^2) \cdot (x_n^2 - Ay_n^2) = 1 \cdot 1 = 1$, como isso temos que

$$(x' \cdot x_n - y' \cdot y_n \cdot A, y' \cdot x_n - x' \cdot y_n)$$

também é uma solução da equação de Pell, e menor que a solução miníma.

Temos também que

$$x' \cdot x_n - y' \cdot y_n \cdot A \geq 0$$

pois caso contrário $x' \cdot x_n - y' \cdot y_n \cdot A < 0 \Leftrightarrow x' \cdot x_n < y' \cdot y_n \cdot A \Rightarrow \dfrac{x' \cdot x_n}{y' \cdot y_n} < A$, porém $x_n^2 - Ay_n^2 = 1 \Rightarrow x_n^2 = Ay_n^2 + 1$, dividindo tudo por y_n^2, temos

$$\frac{x_n^2}{y_n^2} = \frac{Ay_n^2}{y_n^2} + \frac{1}{y_n^2} \Rightarrow (\frac{x_n}{y_n})^2 = A + (\frac{1}{y_n^2}) > A \Rightarrow \frac{x_n}{y_n} > \sqrt{A} \quad \text{(I)}$$

e analogamente, temos que

$$(x')^2 - A\,(y')^2 = 1 \Rightarrow (x')^2 = A\,(y')^2 + 1$$

dividindo tudo por $(y')^2$, temos

$$\frac{(x')^2}{(y')^2} = \frac{A\,(y')^2}{(y')^2} + \frac{1}{(y')^2} \Rightarrow (\frac{x'}{y'})^2 = A + \frac{1}{(y')^2} > A \Rightarrow \frac{x'}{y'} > \sqrt{A} \quad \text{(II)}$$

Fazendo o produto de (I) vezes (II), temos

$$\frac{x' \cdot x^n}{y' \cdot y^n} > A$$

O que contradiz, $\dfrac{x' \cdot x^n}{y' \cdot y^n} < A$. Da mesma forma, $y' \cdot x_n - x' \cdot y_n \geq 0$ pois caso contrário $y' \cdot x_n - x' \cdot y_n < 0 \Leftrightarrow y' \cdot x_n < x' \cdot y_n \Leftrightarrow \dfrac{x_n}{y_n} < \dfrac{x'}{y'}$,

porém $(\dfrac{x_n}{y_n})^2 = A + \dfrac{1}{y_n^2}$ e $(\dfrac{x'}{y'})^2 = A + \dfrac{1}{y_n^2}$,

de $\dfrac{x_n}{y_n} < \dfrac{x'}{y'} \Rightarrow \dfrac{(x_n)^2}{(y_n)^2} < \dfrac{(x')^2}{(y')^2}$,

logo $A + \dfrac{1}{y_n^2} < A + \dfrac{1}{(y')^2} \Rightarrow \dfrac{1}{y_n^2} < \dfrac{1}{(y')^2} \Rightarrow (y')^2 < y_n^2$

$\Rightarrow y' < y_n$

$\Rightarrow x' < x_n$.

o que contradiz o fato de

$$x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n \leq x' + y'\sqrt{A}$$

.

Resumindo, temos que $(x' \cdot x_n - y' \cdot y_n \cdot A, y' \cdot x_n - x' \cdot y_n) \in \mathbb{N}^2$ é uma solução menor do que a solução miníma, logo $x' \cdot x_n - y' \cdot y_n \cdot A = 1$ e $y' \cdot x_n - x' \cdot y_n = 0$, ou seja, $(x' + y'\sqrt{A}) \cdot (x_1 - y_1\sqrt{A})^{-n} = 1 \Leftrightarrow x' + y'\sqrt{A} = x_n + y_n\sqrt{A}$, onde $x' = x_n$ e $y'' = y_n$, como queríamos demonstrar.

■

Concluímos essa etapa que, as soluções da equação $x^2 - Ay^2 = 1$ com x e y inteiros positivos

podem ser enumeradas por $(x_n, y_n), n \geq 0$ de modo que, para todo n.

$$x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$$

e portanto,

$$x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n \quad \text{(I)}$$
$$x_n - y_n\sqrt{A} = (x_1 - y_1\sqrt{A})^n \quad \text{(II)}$$

Somando (I) e (II) temos

$$2x_n = (x_1 + y_1\sqrt{A})^n + (x_1 - y_1\sqrt{A})^n$$

$$x_n = \frac{(x_1 + y_1\sqrt{A})^n + (x_1 - y_1\sqrt{A})^n}{2}$$

Substituindo o valor de x_n em (I) temos:

$$y_n = \frac{(x_1 + y_1\sqrt{A})^n - (x_1 - y_1\sqrt{A})^n}{2\sqrt{A}}$$

Ou seja,

$$(x_n, y_n) = \left(\frac{(x_1 + y_1\sqrt{A})^n + (x_1 - y_1\sqrt{A})^n}{2}, \frac{(x_1 + y_1\sqrt{A})^n - (x_1 - y_1\sqrt{A})^n}{2\sqrt{A}} \right)$$

OBS.: As sequências $(x_n), (y_n)$ acima satisfazem a recorrência

$$u_{n+2} = 2x_1 \cdot u_{n+1} - u_n, \forall_n \geq 1$$

3.3.2 Solução Inicial da Equação de Pell

Nesta etapa mostraremos um procedimento que consiste em encontrar, explicitamente uma solução para a equação

$$x^2 - Ay^2 = 1$$

Para determinar tal solução, precisaremos recorrer aos conceitos estudados sobre frações contínuas. Isso é meio natural pois $\sqrt{A} \notin \mathbb{Q}$ e se x, y são inteiros positivos tais que $x^2 - Ay^2 = \pm 1$ e pelo Corolário 3.5, temos que se, $\sqrt{A} \notin \mathbb{Q}$, existem infinitos $\frac{p}{q} \in \mathbb{Q}$ tal que $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$, de tal forma que todas as aproximações que vem das frações contínuas satisfazem essa propriedade.

Por outro lado se, $x^2 - Ay^2 = 1$, com x, y inteiros positivos

$$|x - y\sqrt{A}| \cdot |x + y\sqrt{A}| = 1 \Rightarrow |x - y\sqrt{A}| = \frac{1}{|x + y\sqrt{A}|} < \frac{1}{y\sqrt{A}} < \frac{1}{y} \leq 1$$

Com isso temos que

$$|x - y\sqrt{A}| \leq 1 \Rightarrow x - y\sqrt{A} > -1 \Rightarrow x > y\sqrt{A} - 1 \Rightarrow x + y\sqrt{A} > y\sqrt{A} + y\sqrt{A} - 1 \Rightarrow$$
$$x + y\sqrt{A} > 2y\sqrt{A} - 1 > 2y$$

Por transitividade

$$x + y\sqrt{A} > 2y$$

Com isso

$$|x - y\sqrt{A}| = \frac{1}{x + y\sqrt{A}} < \frac{1}{2y} \Rightarrow |x - y\sqrt{A}| < \frac{1}{2y}$$

Dividindo tudo por y

$$\frac{|x - y\sqrt{A}|}{y} < \frac{\frac{1}{2y}}{y} \Rightarrow |\frac{x}{y} - \sqrt{A}| < \frac{1}{2y^2}$$

Logo, pelo Teorema 3.2, $\frac{x}{y}$ é uma reduzida $\frac{p_n}{q_n}$ da fração contínua de $\sqrt{A}$

De antemão o que podemos perceber, é que podemos procurar na fração contínua de $\sqrt{A}$, soluções da equação de Pell.

Agora iremos considerar a fração contínua de $\sqrt{A} + \lfloor\sqrt{A}\rfloor = [a_0; a_1; a_2, ...]$ a qual difere da fração contínua de $\sqrt{A}$ apenas pelo primeiro termo $a_0 = 2\lfloor\sqrt{A}\rfloor$, que na fração contínua de $\sqrt{A}$ é igual a $\lfloor\sqrt{A}\rfloor = \frac{a_0}{2}$. O que iremos mostrar é que a fração contínua de $\sqrt{A} + \lfloor\sqrt{A}\rfloor$ é puramente periódica, ou seja,

$$\sqrt{A} + \lfloor\sqrt{A}\rfloor = [a_0; a_1, a_2, ..., a_{k-1}, a_0; ...]$$

Portanto, ela é periódica a partir do primeiro termo a_0 e quando termina esse período, teremos uma solução para a equação de Pell.

Dito isso, vamos mostrar que existem duas sequências de inteiros positivos b_i e c_i de modo que

$$0 < \frac{\sqrt{A} - c_i}{b_i} < 1 \text{ e } \frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2}, ...] = \alpha_i, \forall i \geq 0$$

Tais que

$$b_0 = 1 \text{ e } c_0 = \lfloor\sqrt{A}\rfloor$$

Note que, para $i = 0$

i) $0 < \dfrac{\sqrt{A} - c_i}{b_i} < 1 \Rightarrow 0 < \dfrac{\sqrt{A} - c_0}{b_0} < 1 \Rightarrow 0 < \sqrt{A} - \lfloor \sqrt{A} \rfloor < 1$

ii) $\alpha_i = \dfrac{\sqrt{A} + c_i}{b_i} \Rightarrow \alpha_0 = \dfrac{\sqrt{A} + c_0}{b_0} \Rightarrow \alpha_0 = \sqrt{A} + \lfloor \sqrt{A} \rfloor$

Em geral, definimos recursivamente

$$c_{i+1} = a_i \cdot b_i - c_i \text{ e } b_{i+1} = \frac{(A - c_{i+1}^2)}{b_i}$$

Por definição de fração contínua, temos que

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i} = \frac{1}{\dfrac{\sqrt{A} + c_i}{b_i} - a_i} = 1 \cdot \frac{b_i}{\sqrt{A} + c_i - a_i b_i} = \frac{b_i}{\sqrt{A} + c_i - a_i b_i} \cdot \frac{(\sqrt{A} + a_i b_i - c_i)}{(\sqrt{A} + a_i b_i - c_i)}$$

Resolvendo separadamente o denominador $(\sqrt{A} + c_i - a_i b_i) \cdot (\sqrt{A} + a_i b_i - c_i)$ temos:

$$A + \sqrt{A} \cdot a_i + b_i - \sqrt{A} \cdot c_i + a_i b_i c_i - c_i^2 - \sqrt{A} \cdot a_i \cdot b_i - a_i^2 \cdot b_i^2 + a_i b_i c_i =$$
$$A + a_i \cdot b_i \cdot c_i - c_i^2 - a_i^2 \cdot b_i^2 + a_i \cdot b_i \cdot c_i = A - (a_i^2 \cdot b_i^2 - 2a_i \cdot b_i + c_i^2) = A - (a_i b_i - c_i)^2$$

Substituindo, temos:

$$\alpha_{i+1} = \frac{b_i \cdot (\sqrt{A} + a_i b_i - c_i)}{A - (a_i b_i - c_i)^2}$$

Dividindo tudo por b_i

$$\alpha_{i+1} = \frac{\dfrac{\cancel{b_i} \cdot (\sqrt{A} + a_i b_i - c_i)}{\cancel{b_i}}}{\dfrac{A - (a_i b_i - c_i)^2}{b_i}} = \frac{\sqrt{A} + a_i b_i - c_i}{\dfrac{A - (a_i b_i - c_i)^2}{b_i}}$$

Substituindo o valor de $c_{i+1} = a_i b_i - c_i$, temos:

$$\alpha_{i+1} = \frac{\sqrt{A} + c_{i+1}}{\dfrac{A - (c_{i+1})^2}{b_i}}$$

Substituindo o valor de $b_{i+1} = \dfrac{A - (c_{i+1})^2}{b_i}$, temos

$$\alpha_{i+1} = \frac{\sqrt{A} + c_{i+1}}{b_{i+1}}$$

Agora mostraremos por indução que b_i e c_i são inteiros com $b_i \neq 0$ e tais que $b_i | A - c_i^2, \forall_i \in \mathbb{N}$.

Demonstração:

i) Caso base: Para $i = 0$, claramente verdade pois

$b_0 = 1 | A - c_0^2 = A - \lfloor A \rfloor^2$

ii) Hipótese de indução: Suponhamos que b_i e c_i são inteiros tais que

$b_i|A - c_i^2, \forall_i \in \mathbb{N}$.

iii) Tese: Queremos demonstrar que

$b_{i+1}|A - c_{i+1}^2$

Como por hipótese de indução b_i e c_i são inteiros,portanto $c_{i+1} = a_i b_i - c_i$ também será, e $A - c_{i+1}^2 \neq 0$ já que A não é um quadrado perfeito. Além disso,

$$A - c_{i+1}^2 = A - (a_i b_i - c_i)^2 = A - [a_i^2 \cdot b_i^2 - 2a_i \cdot b_i \cdot c_i + c_i^2] = A - a_i^2 \cdot b_i^2 + 2a_i \cdot b_i \cdot c_i - c_i^2 = A - c_i^2 + (-a_i^2 \cdot b_i^2 + 2a_i \cdot b_i \cdot c_i) = A - c_i^2 - b_i\ (a_i^2 \cdot b_i - 2a_i \cdot c_i)$$

Como por hipótese de indução $b_i|A - c_i^2$ e $b_i| - b_i\ (a_i^2 \cdot b_i - 2a_i \cdot c_i)$, pela proposição 1.6 $b_i|(A - c_i^2) - b_i\ (a_i^2 \cdot b_i - 2a_i \cdot c_i)$

Portanto, $b_i|A - c_{i+1}^2 \Rightarrow b_{i+1} \in \mathbb{Z}$.

Desta forma, temos

$$\frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2}, ...] = a_i + \frac{\sqrt{A} - c_{i+1}}{b_i} = a_i + \frac{b_{i+1}}{\sqrt{A} + c_{i+1}} = a_i + \frac{1}{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}}}$$

De modo que (I), será valida para todo i.

Vamos provar agora que b_i e c_i são positivos. Para isso, vamos provar por indução que $b_i > 0$ e $0 < c_i < \sqrt{A}$.

i) Caso base: Para $i = 0$, verdade pois

$c_0 = \lfloor \sqrt{A} \rfloor$ e A não é um quadrado perfeito.

ii) Hipótese de indução: Suponhamos b_i e c_i positivos, de tal forma que $b_i > 0$ e $0 < c_i < \sqrt{A}$.

iii) Tese: Queremos demonstrar que $b_{i+1} > 0$ e $0 < c_{i+1} < \sqrt{A}$.

$$a_i < \frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2}, ...] < a_{i+1}$$

Donde obtemos que $a_i b_i < \sqrt{A} + c_i < a_i \cdot b_i + b_i$ (já que $b_i > 0$ por hipótese de indução) e portanto

$$c_{i+1} = a_i b_i - c_i < \sqrt{A} < a_i b_i - c_i + b_i = c_{i+1} + b_i$$

E assim, $c_{i+1} < \sqrt{A}$, o que implica $b_{i+1} = \frac{(A - c_{i+1}^2)}{b_i} > 0$, ou seja, $b_{i+1} > 0$.

Agora, suponhamos que $c_{i+1} \leq 0$.

Neste caso, teríamos $b_i > \sqrt{A} - c_{i+1} \geq \sqrt{A}$, mas como $\sqrt{A} > c_i$ por hipótese de indução, teríamos $b_i > c_i$, donde $c_{i+1} = a_i b_i - c_i \geq b_i - c_i > 0$, o que é um absurdo.

Portanto $c_{i+1} > 0$, completando a indução.

■

Finalmente, temos

$$\frac{\sqrt{A} - c_{i+1}}{b_{i+1}} = \frac{\sqrt{A} - c_{i+1}}{\frac{(A - c_{i+1}^2)}{b_i}} = \frac{b_i}{\sqrt{A} + c_{i+1}} = \frac{b_i}{\sqrt{A} + a_i b_i - c_i} = \frac{1}{a_i + \frac{(\sqrt{A} - c_i)}{b_i}} \in (0, 1),$$

pois $a_i \geq 1$ e $\frac{(\sqrt{A} - c_i)}{b_i} > 0$

Como $0 < c_i < \sqrt{A}$ e $b_i | A - c_i^2$, temos que as sequências (c_i) e (b_i) só assumem um número finito de valores. Além disso, podemos recuperar os valores de b_i e c_i a partir dos b_{i+1} e c_{i+1}, para todo $i \geq 0$.

De fato, $b_i = \frac{(A - c_{i+1}^2)}{b_{i+1}}$. Além disso, como temos $0 < \frac{\sqrt{A} - c_i}{b_i} < 1$,

Podemos escrever

$$a_{i+1} = [a_i + \frac{\sqrt{A} - c_i}{b_i}] = [\frac{\sqrt{A} + c_{i+1}}{b_i}]$$

Finalmente, temos $c_i = a_i b_i - c_{i+1}$.

Portanto, estas sequências, assim como a fração contínua de $\sqrt{A} + \lfloor \sqrt{A} \rfloor = [a_0; a_1, a_2, ...]$, são periódicas puras, digamos de período k. Em particular $bk = 1$ e $ck = a_0$.

Note que como $a_0 = 2\ \lfloor \sqrt{A} \rfloor$, temos que a expansão em fração contínua de $\sqrt{A}$ é $[\frac{a_0}{2}; a_1, a_2, ...]$.

Logo, para $i \geq 1$, denotando por $\frac{p_i}{q_i}$ a i - ésima convergente desta fração contínua, temos.

$$\sqrt{A} = \frac{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}} + p_{i-1}}{\frac{\sqrt{A} + c_{i+1}}{b_{i+1}} + q_{i-1}}$$

e portando

$$Aq_i + c_{i+1}\sqrt{A}\ q_i + \sqrt{A}\ b_{i+1} \cdot q_{i-1} = \sqrt{A}\ p_i + c_{i+1} \cdot p_i + b_{i+1} \cdot p_{i-1}$$

Separando parte racional da parte irracional obtemos as equações

$$Aq_i = c_{i+1} \cdot p_i + b_{i+1} \cdot p_{i-1} \quad \text{e} \quad p_i = c_{i+1} \cdot p_i + b_{i+1} \cdot p_{i-1}$$

isolando c_{i+1} nas equações anteriores e igualando obtemos

$$\frac{Aq_i - b_{i+1} \cdot p_{i-1}}{p_i} = \frac{p_i - b_{i+1} \cdot q_{i-1}}{q_i}$$

$\Leftrightarrow Aq_i^2 - b_{i+1} \cdot p_{i-1} \cdot q_i = p_i^2 - b_{i+1} \cdot q_{i-1} \cdot p_i$
$\Leftrightarrow p_i^2 - Aq_i^2 = b_{i+1}\,(p_i q_{i-1} - p_{i-1} \cdot q_i)$
$\Leftrightarrow p_i^2 - Aq_i^2 = (-1)^{i+1} \cdot b_{i+1}$

Donde obtemos uma solução da equação $x^2 - Ay^2 = (-1)^{i+1} \cdot b_{i+1}$. Se k é o período teremos que $bk = 1$ e portanto a equação $x^2 - Ay^2 = -1$ tem solução se k é impar, enquanto que $x^2 - Ay^2 = 1$ sempre tem solução (tomando $i + 1 = 2k$).

Por outro lado, se x e y são inteiros positivos tais que $x^2 - Ay^2 = \pm 1$, vimos que $\frac{x}{y}$ é uma reduzida $\frac{p_n}{q_n}$ da fração contínua de $\sqrt{A}$, como $p_n^2 - Aq_n^2 = (-1)^{n+1} \cdot b_{n+1}$, segue que $b_{n+1} = 1$, mas, como $0 < \sqrt{A} - c_{n+1} = \dfrac{\sqrt{A} - c_{n+1}}{b_{n+1}} < 1$,

segue que $c_{n+1} = \lfloor \sqrt{A} \rfloor$, donde $[a_{n+1}; a_{n+2}, a_{n+3}, ...] = \dfrac{\sqrt{A} - c_{n+1}}{b_{n+1}} = \sqrt{A} + \lfloor \sqrt{A} \rfloor$,

e portanto $n + 1$ é necessariamente múltiplo de período k.

Exemplo 3.4. *Encontre a solução da equação* $x^2 - 21y^2 = 1$.

Solução:

Vimos anteriormente que $a_{i+1} = \left\lfloor \dfrac{\sqrt{A} + c_{i+1}}{b_{i+1}} \right\rfloor$, $c_{i+1} = a_i \cdot b_i - c_i$ e $b_{i+1} = \dfrac{A - c_{i+1}^2}{b_i}$.

Por definição, temos que:

$$a_0 = 2\lfloor \sqrt{A} \rfloor = 2\lfloor \sqrt{21} \rfloor = 2 \cdot 4 = 8,\ c_0 = \lfloor \sqrt{A} \rfloor = \lfloor \sqrt{21} \rfloor = 4 \ \text{ e } \ b_0 = 1$$

com isso para encontrarmos a solução de:

$$x^2 - 21y^2 = 1$$

basta olharmos para a fração contínua de $\sqrt{A} + \lfloor \sqrt{A} \rfloor$. Para tal, tomamos $i \geq 0$, logo:

i) Para $i = 0$, temos:
$c_1 = a_0 \cdot b_0 - c_0 = 2\lfloor \sqrt{21} \rfloor \cdot 1 - \lfloor \sqrt{21} \rfloor = 2\lfloor \sqrt{21} \rfloor - \lfloor \sqrt{21} \rfloor = \lfloor \sqrt{21} \rfloor = 4$

$$b_1 = \frac{A - c_1^2}{b_0} = \frac{21 - 4^2}{1} = 21 - 16 = 5$$

$$a_1 = \left\lfloor \frac{\sqrt{A} + c_1}{b_1} \right\rfloor = \left\lfloor \frac{\sqrt{21} + 4}{5} \right\rfloor = 1$$

ii) Para $i = 1$, temos:
$c_2 = a_1 \cdot b_1 - c_i = 1 \cdot 5 - 4 = 1$

$$b_2 = \frac{A - c_2^2}{b_1} = \frac{21 - 1^2}{5} = \frac{21 - 1}{5} = \frac{20}{5} = 4$$

$$a_2 = \left\lfloor \frac{\sqrt{A} + c_2}{b_2} \right\rfloor = \left\lfloor \frac{\sqrt{21} + 1}{4} \right\rfloor = 1$$

iii) Para $i = 2$, temos:

$$c_3 = a_2 \cdot b_2 - c_2 = 1 \cdot 4 - 1 = 4 - 1 = 3$$

$$b_3 = \frac{A - c_3^2}{b_2} = \frac{21 - 3^2}{4} = \frac{21 - 9}{4} = \frac{12}{4} = 3$$

$$a_3 = \left\lfloor \frac{\sqrt{A} + c_3}{b_3} \right\rfloor = \left\lfloor \frac{\sqrt{21} + 3}{3} \right\rfloor = 2$$

iv) Para $i = 3$, temos:

$$c_4 = a_3 \cdot b_3 - c_3 = 2 \cdot 3 - 3 = 6 - 3 = 3$$

$$b_4 = \frac{A - c_4^2}{b_3} = \frac{21 - 3^2}{3} = \frac{21 - 9}{3} = \frac{12}{3} = 4$$

$$a_4 = \left\lfloor \frac{\sqrt{A} + c_4}{b_4} \right\rfloor = \left\lfloor \frac{\sqrt{21} + 3}{4} \right\rfloor = 1$$

v) Para $i = 4$, temos:

$$c_5 = a_4 \cdot b_4 - c_4 = 1 \cdot 4 - 3 = 4 - 3 = 1$$

$$b_5 = \frac{A - c_5^2}{b_4} = \frac{21 - 1^2}{4} = \frac{21 - 1}{4} = \frac{20}{4} = 5$$

$$a_5 = \left\lfloor \frac{\sqrt{A} + c_5}{b_5} \right\rfloor = \left\lfloor \frac{\sqrt{21} + 1}{5} \right\rfloor = 1$$

vi) Para $i = 5$, temos:

$$c_6 = a_5 \cdot b_5 - c_5 = 1 \cdot 5 - 1 = 5 - 1 = 4$$

$$b_6 = \frac{A - c_6^2}{b_5} = \frac{21 - 4^2}{5} = \frac{21 - 16}{5} = \frac{5}{5} = 1$$

$$a_6 = \left\lfloor \frac{\sqrt{A} + c_6}{b_6} \right\rfloor = \left\lfloor \frac{\sqrt{21} + 4}{1} \right\rfloor = 8$$

Podemos observar que $a_6 = a_0, b_6 = b_0$ e $c_6 = c_0$, ou seja, a fração contínua é periódica a partir de um certo ponto, portanto pelo que demonstramos anteriormente uma solução da equação de Pell é dada por:

$$\frac{p_5}{q_5} = 4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1}}}}} = \frac{55}{12}$$

E $55 - 21 \cdot 12^2 = 3025 - 3024 = 1$ isso implica que $x_1 = 55$ e $y_1 = 12$, portanto as demais soluções são dadas por $x + y\sqrt{A} = (x_1 + y_1\sqrt{A})^n = (55 + 12\sqrt{21})^n$.

Exemplo 3.5. *Sejam (F_n) e (L_n) as sequências de Fibonacci e Lucas, respectivamente, definidas por:*

$$F_1 = 1, F_2 = 1 \quad e \quad F_{n+1} = F_n + F_{n-1},\ n \geq 2$$
$$L_1 = 1, L_2 = 3 \quad e \quad L_{n+1} = L_n + L_{n-1},\ n \geq 2$$

Mostre que a equação $5x^2 - y^2 = 4$ admite uma solução (x, y) nos inteiros positivos se, e somente se, $(x, y) = (F_{2n-1}, L_{2n-1})$.

Solução:

Podemos perceber que $(x, y) = (1, 1)$ é a única solução com $y \leq 2$. Podemos supor, portanto, que $y \geq 3$. Sendo α e β as duas raízes da equação $x^2 - x - 1 = 0$, é conhecido que:

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{e} \quad \lambda_n = \alpha^n + \beta^n$$

Com isso temos que os pares (F_{2n-1}, L_{2n-1}) satisfazem nossa equação, o que nos vai dar um pouco de trabalho é mostrar que elas são as únicas soluções. Seja:

$$S = \{(F_{2n-1}, L_{2n-1})\}, n \geq 1$$

Por absurdo, suponhamos que exista uma solução $(x, y) \notin S$ e tome aquela que minimiza o valor de x. Como x e y têm a mesma paridade, as frações $\dfrac{3x - y}{2}$ e $\dfrac{3y - 5x}{2}$ são inteiros positivos, pois:

i) $x^2 > -1 \Rightarrow 9x^2 > 5x^2 - 4 \Rightarrow 9x^2 > y^2 \Rightarrow 3x > y$

ii) $y^2 > 5 \Rightarrow 9y^2 > 5y^2 + 20 \Rightarrow 9y^2 > 25x^2 \Rightarrow 3y > 5x$

Afirmamos que $\left(\dfrac{3x - y}{2}, \dfrac{3y - 5x}{2}\right)$ é uma solução da equação que não está em S. De fato,

$$5\left(\frac{3x - y}{2}\right)^2 - \left(\frac{3y - 5x}{2}\right)^2 = \frac{20x^2 - 4y^2}{4} = 4$$

e, se $\left(\dfrac{3x - y}{2}, \dfrac{3y - 5x}{2}\right) \in S$, existiria n para o qual:

$$\begin{array}{ccccc} \dfrac{3x - y}{2} = F_{2n-1} & \text{e} & \dfrac{3y - 5x}{2} = L_{2n-1} \\ \Longleftrightarrow & & \Longleftrightarrow \\ x = F_{2n+1} & \text{e} & y = L_{2n-1} \end{array}$$

o que contraria o fato de que (x, y) não está em S. Por fim, temos que $\dfrac{3x - y}{2} < x$, ou seja, obtemos uma solução cuja primeira coordenada é maior que x. Com isso, podemos concluir que todas as soluções estão em S.

Considerações Finais

Ao longo do desenvolvimento deste trabalho, apresentamos inúmeras proposições, lemas, teoremas, corolários e suas respectivas demonstrações e aplicações das mesmas na resolução de exemplos que reforcem o entendimento dos tópicos abordados da teoria dos números. Esperamos, ter alcançado nossos objetivos que era transcrever tal tema de uma maneira clara e acessível a todo o público que necessite de tal conhecimento (Docentes e Discentes da Educação Básica, Estudante de Graduação, e até mesmo colegas integrantes do PROFMAT), pois ainda possuímos pouca bibliografia existente na área no nosso pais em Língua portuguesa.

Referências Bibliográficas

[1] FOMIN, Dmitri; GENKIN, Sergey; *et al* . *Círculos Matemáticos*. Traduzido por: Valéria de Magalhães Iório. Rio de Janeiro, Impa: 2012.

[2] HEFEZ, Abramo. *Aritmética*. Rio de Janeiro: SBM, 2014. (Coleção PROFMAT; 08)

[3] HEFEZ, Abramo. *Exercícios resolvidos de Aritmética*. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT; 17)

[4] LANDAU, Edmund G. H. *Teoria elementar dos números*. Rio de Janeiro: Ciência Moderna, 2002.

[5] LIMA, Elon Lages. *Análise real*. Vol. 1. 12.ed. Rio de Janeiro: Impa, 2008.

[6] MARTINEZ, Fabio Bochero; et al. *Teoria dos números*: um passeio com primos e outros números familiares pelo mundo inteiro. 4. ed. Rio de Janeiro: IMPA, 2015. (Projeto Euclides)

[7] MUNIZ NETO, Antonio Caminha. *Tópicos de Matemática Elementar*: teoria dos números. 2. ed. Rio de Janeiro: SBM, 2013. (Coleção Professor de Matemática; 28)

[8] SANTOS, José Plínio de Oliveira. *Introdução à teoria dos números*. 3. ed. Rio de Janeiro: IMPA: 2015. (Coleção Matemática Universitária)

[9] SOUZA, Romario Sidrone de. *Equações diofantinas linerares, quadráticas e aplicações*. Dissertação (Mestrado Profissional em Matemática). Universidade Estadual Paulista "Júlio de Mesquita Filho". Rio Claro, 2007