Ciência e Natura
ISSN: 0100-8307
cienciaenaturarevista@gmail.com
Universidade Federal de Santa Maria
Brasil

Neubert Savóis, Josias; Freitas, Daiane

Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais

Ciência e Natura, vol. 37, núm. 3, 2015, pp. 47-57
Universidade Federal de Santa Maria
Santa Maria, Brasil

Disponível em: http://www.redalyc.org/articulo.oa?id=467547643005

Ciência e Natura, Santa Maria, v. 37 Ed. Especial PROFMAT, 2015, p. 47 – 57
Revista do Centro de Ciências Naturais e Exatas - UFSM
ISSN impressa: 0100-8307 ISSN on-line: 2179-460X

CIÊNCIA e NATURA 35 anos

Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais

thod for solving Diophantine equations with coefficients in the set of rational numbers

Josias Neubert Savóis[*1] e Daiane Freitas[2]

[1,2] Universidade Federal do Rio Grande, RS, Brasil

Resumo

Desenvolver um conhecimento sólido sobre as equações diofantinas lineares em duas variáveis possibilita a resolução de muitos problemas do cotidiano e, também, o real entendimento de alguns conceitos matemáticos ensinados na escola, mas que parecem sem utilidade e sem aplicação prática. Além disso, as relações que estas equações estabelecem com outros conteúdos que já estão inseridos na educação básica justificam o seu ensino e a tornam uma importante ferramenta de contextualização e interdisciplinaridade. Neste trabalho também mostraremos, a importância do ensino dos números racionais e neste contexto fazer uma análise sobre um novo conceito de máximo divisor comum, chamado máximo divisor comum generalizado, com isto poderemos usar os racionais como conjunto numérico dos coeficientes das equações diofantinas, expandindo a abrangência de problemas solucionados por estas equações. A criação de vários problemas práticos de aplicação da teoria estudada serve para nos convencermos da importância deste trabalho e para incentivar a sua aplicação e a criação de novos problemas levando em consideração a realidade de cada escola e de seus alunos.

***Palavras-chave**: Equações diofantinas. Números racionais. Problemas práticos. Conteúdos relacionados*

Abstract

Develop a solid understanding of linear Diophantine equations in two variables facilitates the resolution of many problems of daily life and also the real understanding of some mathematical concepts taught in school but they seem useless and without practical application. Moreover, the relationships that these equations are established with other content that are already inserted into the basic education justify their education and become an important tool for contextualizing and interdisciplinarity. This work also aims to show the importance of teaching of rational numbers and in this context do analysis on a new concept of greatest common divisor,called generalized maximum common divisor, and thus we can use the numberpad as rational coefficients of Diophantine equations, expanding the breadth of problems solved by these equations. The creation of various practical problems of implementation of the theory studied serves to convince us of the importance of this work and to encourage their implementation and creating new problems taking into account the reality of each school and its students.

***Keywords**: Diophantine Equations. Rational numbers. Practical problems. Related contents.*

Recebido: 26/06/2014 Aceito: 08/10/2014

*josiasneubert@hotmail.com

1 Introdução

Equação diofantina linear em duas variáveis é um tipo de equação que, além de apresentar conceitos especiais na sua resolução, como por exemplo a visão de solução geral da equação que é determinada através da inserção de um parâmetro (conceito este usado no estudo das equações paramétricas, em geometria analítica), ajudam a resolver vários problemas curiosos e interessantes e também desenvolver o raciocínio dos alunos através da união da resolução de cálculos com a interpretação de problemas. Para que seja possível ensinar estas equações, outros conceitos devem ser abordados como pré-requisitos, como por exemplo a divisão euclidiana, o algoritmo de Euclides e o máximo divisor comum (*mdc*) entre dois ou mais números inteiros.

Mesmo que as equações diofantinas não estejam definidas como conteúdo da educação básica, é possível improvisar e inserir este conteúdo no contexto escolar, de preferência relacionando-o com outros conteúdos já trabalhados normalmente, os conteúdos de matemática têm uma flexibilidade que permite adaptar o ensino de acordo com a necessidade e realidade de cada turma, escola ou região.

Fato curioso sobre as equações diofantinas lineares em duas variáveis, as quais podem ser escritas da forma $ax + by = c$, é o de que os coeficientes desta equação devem pertencer ao conjunto dos números inteiros ($\mathbb{Z}$), ou seja , $a, b, c \in \mathbb{Z}$. É muito difícil olhar para estas equações e em algum momento não pensar "será que se os coeficientes pertencessem a outro conjunto numérico teríamos condições de encontrar sua solução geral?"ou mesmo é difícil analisar um problema aplicado resolvido através das equações diofantinas e não passar na mente o devaneio de tentar criar um problema envolvendo dinheiro e decimais de igual resolução através dos mesmos conceitos e do mesmo formato de equação.

Por isso, desenvolvemos uma relação interessante e inovadora entre números racionais e equações diofantinas, possibilitando a resolução de uma infinidade de problemas didáticos e do cotidiano. Esta relação é possível através da generalização de conceitos até então adotados somente no conjunto dos números inteiros aos números racionais ($\mathbb{Q}$), e reais comensuráveis, tais como o conceito de máximo divisor comum que nos racionais chamaremos de máximo divisor comum generalizado (*mdcg*) e os coeficientes de uma equação do tipo diofantina que poderão pertencer ao conjunto dos números racionais ($\mathbb{Q}$).

2 Divisibilidade e Máximo Divisor Comum (MDC)

Ao longo deste trabalho, mostraremos algumas definições, proposições e teoremas que são necessárias para a compreensão do mesmo. Porém, algumas proposições e teoremas que julgamos de fácil compreensão não serão demonstradas, mas podem ser encontradas em (Hefez, 2011), (Martinez, 2011) e (Neto, 2012).

Definição 2.1. *Dados a,$b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a, ou que b é um divisor de a, ou ainda que a é múltiplo de b, e escrevemos $b|a$, se existir $q \in \mathbb{Z}$ tal que $a = bq$. Caso b não divida a, escrevemos $b \nmid a$.*

Proposição 2.1. *Sejam $a, b, c \in \mathbb{Z}^*$ e x, y inteiros quaisquer. Tem- se que:*
(a) Se $b|a$, então $|b| \leq |a|$.
(b) Se $b|a$ e $a|b$, então $a = \pm b$.
(c) Se $c|b$ e $b|a$, então $c|a$.
(d) Se $c|a$ e $c|b$, então $c|(ax + by)$.
(e) Se $c|b$, então $c|ab$(um caso particular do item anterior).
(f) Se $b|a$, então $bc|ac$.

Teorema 2.1 (Divisão Euclidiana)**.** *Para quaisquer $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$, tais que $a = bq + r$, onde $0 \leq r < |b|$.*

Definição 2.2. *O Máximo Divisor Comum de dois inteiros a e b (com a ou b diferente de zero), denotado por $mdc(a, b)$ ou simplesmente por (a, b), é o maior inteiro que divide a e b, ou seja, é o maior inteiro que pertence ao conjunto dos divisores de a e b.*

Definição 2.3. *O Mínimo Múltiplo Comum de dois inteiros a e b (com a ou b diferente de zero), denotado por $mmc(a, b)$ ou simplesmente por $[a, b]$, é o menor inteiro que é múltiplo a e b, ou seja, é o menor inteiro que pertence ao conjunto dos múltiplos de a e b.*

Lema 2.1. *Sejam a e b dois inteiros positivos e $a = bq + r$, com $0 \leq r < b$ e $q \in \mathbb{Z}$. Então $mdc(a, b) = mdc(b, r)$.*

Assim, pelo lema anterior, dados a, b inteiros positivos com $a \geqslant b$, o problema de encontrar o $mdc(a, b)$, reduz-se a encontrar o $mdc(b, r)$, onde r é tal que $a = bq + r$, com $0 \leqslant r < b$. De posse desse resultado, podemos mostrar o algoritmo de Euclides. Este algoritmo apresenta duas funções muito importantes: primeiro, o algoritmo de Euclides fornece o $mdc(a, b)$ de maneira rápida e sistemática; segundo, através deste algoritmo

é possível escrever o $mdc(a,b)$ como combinação linear de a e b, fato este que será indispensável para a resolução das equações diofantinas lineares com duas variáveis, que serão abordadas mais adiante.

Vamos ao método chamado de algoritmo de Euclides. Sejam a e b inteiros positivos, com $a \geq b$. Naturalmente, repetindo o algoritmo da divisão euclidiana,temos:

$$\begin{aligned} a &= bq_1 + r_1, \text{ com } 0 \leq r_1 < b \\ b &= r_1q_2 + r_2, \text{ com } 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, \text{ com } 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \text{ com } 0 \leq r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + r_{n+1}, \text{ com } r_{n+1} = 0. \end{aligned}$$

Como o resto diminui a cada passo, o processo não pode continuar indefinidamente, e alguma das divisões deve ser exata. Suponhamos então que r_{n+1} seja o primeiro resto nulo. Utilizando o resultado do lema anterior, temos que:

$$\begin{aligned} mdc(a,b) &= mdc(b,r_1) = mdc(r_1,r_2) \\ &= mdc(r_2,r_3) = \cdots = mdc(r_{n-1},r_n) \end{aligned}$$

Finalmente, como $r_n \mid r_{n-1}$ é fácil ver que $mdc(r_{n-1},r_n) = r_n$, logo, $mdc(a,b) = r_n$.

Podemos usar o algoritmo de Euclides de maneira mais simplificada e eficiente através do dispositivo prático abaixo, que torna os cálculos mais mecânicos e mais práticos de serem realizados. Este dispositivo prático que sintetiza o algoritmo de Euclides, além de calcular o $mdc(a,b)$, serve para escrever o mesmo como combinação linear dos coeficientes a e b de uma equação diofantina linear com duas variáveis, fato este que será abordado mais adiante.

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = mdc(a,b)$
r_1	r_2	r_3	r_4	...	r_n		

Observação: Com o algoritmo de Euclides encontramos o MDC entre dois números inteiros não nulos, o qual também nos permite obter o MMC através da relação:

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

3 Ensino dos Números Racionais

O conjunto dos números racionais $\mathbb{Q}$ é um dos conjuntos numéricos mais trabalhados nas séries finais do ensino fundamental. Junto com o conjunto dos números inteiros $\mathbb{Z}$ é o conjunto de números que serve de base e é de uso indispensável na maioria dos conteúdos e problemas abordados durante o ensino fundamental. Embora no ensino médio seja dado ênfase ao conjunto dos números reais $\mathbb{R}$, a maioria dos problemas resolvidos em sala de aula, em provas, em concursos e no Enem (Exame Nacional do Ensino Médio) usam os conhecimentos sobre números decimais finitos ou infinitos e periódicos, que podem ser escritos na forma de fração $\frac{p}{q}$, com p,$q \in \mathbb{Z}$ e $q \neq 0$, ou seja, o conjunto dos números racionais.

E não é só no contexto escolar que o conhecimento sobre os números racionais é importante. No cotidiano de qualquer pessoa aparecem situações envolvendo uma fração ou um decimal finito. Basta perceber que todas as pessoas precisam utilizar dinheiro para viver em qualquer sociedade atualmente, e para isto deve-se ter a noção de décimos e centésimos. Além disso, fazer um bolo ou comer uma pizza com os amigos necessita de um conhecimento básico sobre frações.

Cabe apenas uma ressalva sobre a abordagem dos racionais no ensino fundamental, em dois pontos interessantes. Primeiro, o professor deve prestar atenção no uso das multiplicações e divisões de frações (ou decimais) como sendo operações que, também, representam quantidades e que às vezes são esquecidas por causa de formulações que "facilitam"a memorização e a resolução de problemas por parte dos alunos. Exemplo desta memorização pode ser dado pela regra da divisão de frações "na divisão de fração, copia-se a primeira fração e multiplica-se pelo inverso da segunda fração", que é trabalhada por muitos professores somente como um método, uma receita, desvinculando assim o sentido de "repartir"que uma divisão tem. Desse modo, as multiplicações e divisões de frações se tornam abstrações desprendidas de sentido, sem utilização em situações reais encontrados no cotidiano, como por exemplo, calcular a quantidade de cada ingrediente que será necessário para fazer um bolo que rende 6 porções, sabendo que a quantidade de cada ingrediente da receita original rende 15 porções.

Um exemplo simples do fato de dar sentido às operações com frações, conforme (Ribeiro, 2009), que consideramos uma abordagem obrigatória, é a representação geométrica de uma multiplicação de frações. Veja o exemplo dado na Figura 1..

Do mesmo modo que a multiplicação de fração, a divisão de frações também pode ser representada geometricamente, usando o sentido de repartir que a divisão tem para facilitar o entendimento por parte dos alunos. Vamos mostrar um exemplo de divisão de frações

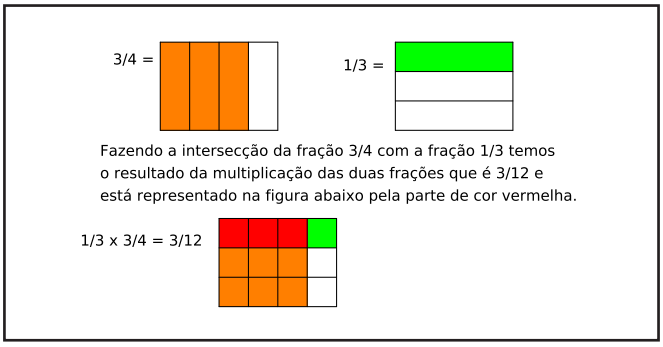

Figura 1 - Multiplicação de Frações

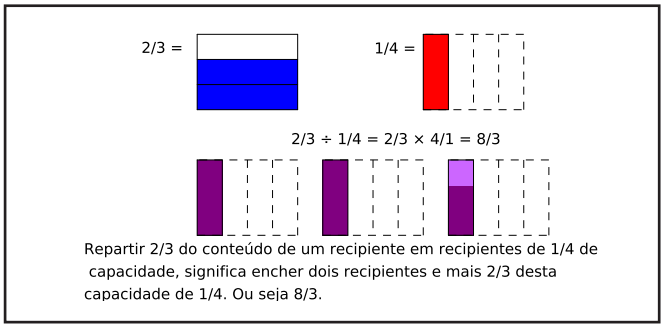

Figura 2 - Divisão de Frações

representando-a geometricamente e passo a passo. Queremos efetuar o cálculo da expressão $\frac{2}{3} \div \frac{1}{4}$ de modo geométrico, ou seja, queremos repartir um produto que ocupa $\frac{2}{3}$ de um determinado recipiente em "potes"que têm $\frac{1}{4}$ da capacidade deste recipiente. Então, para descobrir a quantidade de potes que iremos usar, procedemos de modo semelhante ao caso da multiplicação, conforme Figura 2..

O outro ponto que deve ser abordado com muita atenção é a relação fração-decimal-porcentagem, que exige por parte do aluno um domínio sobre as equivalências entre frações e também multiplicação, divisão e simplificação de frações. Alertar os alunos e fazê-los compreender o fato de que

$$\frac{6}{15} = \frac{2}{5} = 0{,}4 = \frac{4}{10} = \frac{40}{100} = 40\%$$

é de fundamental importância para o desenvolvimento de vários cálculos em várias situações e vários conteúdos de matemática, como por exemplo na resolução de regras de três, cálculo de juros, equações, funções, geometria e trigonometria.

A partir do momento em que os alunos apresentarem um domínio significativo das operações e resoluções de problemas no campo das frações, o ensino da matemática irá atingir outro patamar, podendo ser desenvolvida uma gama maior de conteúdos e de aplicações, facilitando de certo modo o trabalho do professor de matemática do ensino médio e deixando-o a vontade para mostrar aos alunos que quanto mais se aprende e se desenvolve na matemática, mais prazerosa e apaixonante ela fica.

4 Conceito de MDC generalizado

A seguir serão expostas algumas definições que nos permitem generalizar o conceito de máximo divisor comum (e também mínimo múltiplo comum se for do interesse do leitor) para o conjunto dos números racionais e para os números reais comensuráveis. Vale ressaltar que o conceito de máximo divisor comum generalizado (*mdcg*) foi retirado do artigo (Ripoll et al., 2006), publicado em 2006 na revista Matemática Universitária e escrito pelos professores Alveri Sant'anna, Cydara Ripoll e Jaime Ripoll, conceituados professores da Universidade Federal do Rio Grande do Sul (UFRGS).

Definição 4.1. *Dizemos que dois segmentos da reta são comensuráveis quando ambos podem ser obtidos através de um número inteiro de emendas não sobrepostas de um mesmo segmento de reta.*

Definição 4.2. *Dois números reais r e s são comensuráveis se existem inteiros não nulos m, n tais que $mr = ns$.*

Exemplos:
1. Dois racionais são sempre comensuráveis.
2. Dois irracionais podem ser comensuráveis:
por exemplo, $\sqrt{2}$ e $2\sqrt{2}$.
3. Dois reais quaisquer nem sempre são comensuráveis:
basta tomar um racional e um irracional, mas também a maioria de pares de irracionais, como, por exemplo, $\sqrt{2}$ e $\sqrt{3}$.

Definição 4.3. *Dizemos que um número real r é um múltiplo inteiro de um número real s, ou que s é um divisor inteiro de r, se existe um inteiro a tal que $r = as$.*

Devemos observar que a definição acima esclarece o significado de *múltiplo inteiro* e *divisor inteiro* de números reais, que ao longo do texto podem confundir o leitor, pois nos referimos ao múltiplo inteiro comum como sendo um número real que é múltiplo um número inteiro de vezes de outro número real e ao divisor inteiro comum, ao número real que divide outro número real uma quantidade inteira de vezes.

Proposição 4.1. *Sejam r e s dois números reais não nulos. As seguintes afirmações são equivalentes:*

a) r e s são comensuráveis;
b) o quociente $\frac{r}{s}$ *é um número racional;*
c) existe um real t que é múltiplo inteiro comum de r e de s;
d) existe um real u que é divisor inteiro comum de r e de s.

Demonstração:
$(a) \Rightarrow (b)$ Se r e s são comensuráveis então existem $m, n \in \mathbb{Z}^*$ tais que $mr = ns$. Consequentemente, $\frac{r}{s} = \frac{n}{m} \in \mathbb{Q}$.
$(b) \Rightarrow (c)$ Suponhamos que $\frac{r}{s} \in \mathbb{Q}$, digamos, $\frac{r}{s} = \frac{n}{m}$. Então, multiplicando a igualdade acima por sm obtemos que $t = mr = ns$ é um múltiplo inteiro comum de r e de s, com $t \in \mathbb{R}$.
$(c) \Rightarrow (d)$ Seja $t \in \mathbb{R}$ um múltiplo inteiro comum de r e de s, digamos, $t = mr = ns$, com $m, n \in \mathbb{Z}^*$. Então, o número $u = \frac{r}{n} = \frac{s}{m}$ é um divisor inteiro comum de r e de s.
$(d) \Rightarrow (a)$ Seja u um divisor comum de r e de s, digamos $r = un$ e $s = um$, com $m, n \in \mathbb{Z}^*$. Então, temos que $mr = ns$ concluindo a demonstração.

□

Definição 4.4. *Sejam r e s dois números reais comensuráveis não nulos. Dizemos que u é o máximo divisor comum generalizado (mdcg) entre r e s, e escrevemos* $u = mdcg(r, s)$*, se*
a) u é um divisor inteiro comum de r e s.
b) se u' *é divisor inteiro comum de r e de s então* $u' \leq u$.

De posse das definições acima, podemos enunciar o teorema que nos fornece uma fórmula para o *mdcg* entre dois reais comensuráveis quaisquer.

Teorema 4.1. *Sejam r e s dois reais comensuráveis não nulos. Então*

$$mdcg(r, s) = \frac{r}{u} = \frac{s}{v},$$

onde $\frac{u}{v}$ *é a forma irredutível do racional* $\frac{r}{s}$.

Demonstração:
Consideraremos aqui apenas o caso r e s positivos. Observamos inicialmente que se a,b,c,d são inteiros tais que $ar = bs$ e $cr = ds$ então

$$\frac{b}{a} = \frac{d}{c},$$

e este número nada mais é do que o número $\frac{r}{s}$. Assim, os menores naturais a,b que satisfazem $ar = bs$ são claramente obtidos quando tomamos o numerador e o denominador da fração irredutível que representa o racional $\frac{r}{s}$. Daí, pela definição de *mdcg*, se $\frac{u}{v}$ é tal fração irredutível, então

$$mdcg(r, s) = \frac{r}{u} = \frac{s}{v},$$

o que completa a prova do teorema.

□

No caso de r e s serem números racionais, a fórmula dada no teorema acima pode ser reescrita em termos das representações destes racionais em frações irredutíveis:

Teorema 4.2. *Sejam r,s racionais não nulos e sejam a,b,c,d inteiros tais que* $\frac{a}{b}$ *e* $\frac{c}{d}$ *são as representações para r e s, respectivamente, na forma de fração irredutível. Então* $mdcg(r, s) = \frac{mdc(a,c)}{mmc(b,d)}$.

Demonstração:
Novamente aqui provamos apenas para o caso r e s positivos.
Como $mdc(a,b) = 1 = mdc(c,d)$, temos

$$\frac{r}{s} = \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc} = \frac{a'd'}{b'c'},$$

onde

$$a' = \frac{a}{mdc(a,c)},\ b' = \frac{b}{mdc(b,d)},\ c' = \frac{c}{mdc(a,c)},$$
$$d' = \frac{d}{mdc(b,d)}.$$

É claro, que a fração $\frac{a'd'}{b'c'}$ é irredutível, e portanto, pelo Teorema 4.1 , temos

$$mdcg(r, s) = \frac{r}{a'd'} = \frac{a}{b}.\frac{mdc(a,c)}{a}.\frac{mdc(b,d)}{d}$$

$$= mdc(a,c).\frac{mdc(b,d)}{bd} = \frac{mdc(a,c)}{\frac{bd}{mdc(b,d)}}$$

mas como

$$\frac{bd}{mdc(b,d)} = mmc(b,d)$$

então substituindo esta expressão temos que

$$mdcg(r, s) = \frac{mdc(a,c)}{mmc(b,d)},$$

o que completa a prova.

□

Este conceito de *mdc* generalizado será utilizado mais adiante para possibilitar a resolução de equações do tipo diofantinas com coeficientes racionais e deste modo estender o emprego dos métodos de resolução destas equações para problemas que até o momento são solucionados através de outros artifícios matemáticos. Mas, vale lembrar que a Definição 4.4 só tem sentido quando adotada como referência única e exclusivamente a Definição 4.3. Se pensarmos na divisibilidade em um anel (conjunto munido de duas operações que satisfazem algumas propriedades pré-determinadas), conforme proposto por Ripoll et al. (2006), em que dado um anel A, com a,$b \in A$, então podemos dizer que a é múltiplo de b ou que b é divisor de a se $a = bt$ para algum $t \in A$, teríamos neste caso o diferencial de que um múltiplo a não significa um número inteiro de vezes o número b, como abordamos até o momento.

5 Equações diofantinas lineares em duas variáveis

São chamadas equações diofantinas todas as equações polinomiais (não importando o número de incógnitas) com coeficientes inteiros, sempre que for tomado como conjunto solução das variáveis da equação o conjunto dos números inteiros. Visto a importância, facilidade de resolução e quantidade de problemas que se enquadram neste formato, tomaremos como foco do nosso estudo a compreensão e resolução das equações diofantinas lineares com duas variáveis.

Uma equação diofantina linear em duas variáveis é uma expressão da forma $ax + by = c$, na qual a, b, c são inteiros, com a e b não simultaneamente nulos e cujas soluções estão restritas ao conjunto dos números inteiros. Uma solução dessa equação é então um par de inteiros (x_0, y_0) tal que $ax_0 + by_0 = c$.

Vale ressaltar que, apesar deste tipo de equações que visa soluções inteiras receberem o nome de diofantinas devido a Diofanto de Alexandria, o primeiro matemático a encontrar uma solução geral de uma equação diofantina linear foi o hindu Brahmagupta (598 – 670), cuja resolução foi embasada no algoritmo de Euclides, conforme (Eves, 2011).

Teorema 5.1 (Teorema de Bézout)**.** *Se $d = mdc(a, b)$, então existem $x, y \in \mathbb{Z}$, de modo que $ax + by = d$.*

Teorema 5.2. *Sejam $a, b, c \in \mathbb{Z}$, com a e b não simultaneamente nulos. A equação $ax + by = c$ admite solução inteira em x e y se, e somente se, $mdc(a, b) \mid c$. Nesse caso, se $d = mdc(a, b)$ e $x = x_0, y = y_0$ é uma solução inteira qualquer da equação, então as fórmulas $x = x_0 + \frac{b}{d}t$ e $y = y_0 - \frac{a}{d}t$, para todo $t \in \mathbb{Z}$, fornecem todas as soluções inteiras possíveis.*

Demonstração: Se a equação admite solução inteira, pela Proposição 2.1, $mdc(a, b)|ax + by$, logo $mdc(a, b) \mid c$. Reciprocamente, suponhamos que $mdc(a, b) \mid c$, digamos $c = kmdc(a, b)$ com $k \in \mathbb{Z}$. Pelo teorema 5.1 existem inteiros x_0 e y_0, tais que $ax_0 + by_0 = mdc(a, b)$. Multiplicando essa igualdade por k obtemos que $x = kx_0$ e $y = ky_0$ são soluções da equação dada.

Para o que falta, suponha que $mdc(a, b)|c$ e seja $x = x_0$, $y = y_0$ uma solução inteira qualquer da equação. Se $x = x_1$ e $y = y_1$ for outra solução inteira da mesma, então $a(x_1 - x_0) = b(y_0 - y_1)$. Dividindo essa igualdade por $d = mdc(a, b)$, temos:

$$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1). \tag{1}$$

Assim, $\frac{b}{d}|\frac{a}{d}(x_1 - x_0)$ e, como $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, temos que $\frac{b}{d}|(x_1 - x_0)$. Logo $\exists\, t \in \mathbb{Z}$ tal que $x_1 - x_0 = \frac{b}{d}t$, o u seja, $x_1 = x_0 + \frac{b}{d}t$. Substituindo $(x_1 - x_0)$ por $\frac{b}{d}t$ na equação (1), obtemos de modo análogo $y_1 = y_0 - \frac{a}{d}t$, com $t \in \mathbb{Z}$. Reciprocamente, é imediato verificar que tais fórmulas fornecem, de fato, para todo $t \in \mathbb{Z}$, soluções inteiras para a equação.

□

Uma observação importante deve ser feita no teorema acima: como $d|c$, temos que $c = dq$, com $q \in \mathbb{Z}$ e $q = \frac{c}{d}$. Escrevendo $d = ar + bs$, com $r, s \in \mathbb{Z}$, e multiplicando a equação por $q = \frac{c}{d}$ obtém-se a equação $c = ar\frac{c}{d} + bs\frac{c}{d}$, e a partir daí conclui-se que $x_0 = r\frac{c}{d}$ e $y_0 = s\frac{c}{d}$ e que as soluções gerais da equação diofantina $ax + by = c$ podem ser escritas da seguinte forma:
$x = \frac{rc + bt}{d}$ e $y = \frac{sc - at}{d}$, para qualquer $t \in \mathbb{Z}$.

Exemplo de resolução de uma equação diofantina.

Exemplo 5.1. *Vamos resolver a equação $5x + 12y = 81$ com solução pertencente a $\mathbb{Z}$.*

Resolução
Vamos começar usando o algoritmo de Euclides.

	2	2	2
12	5	2	1
2	1		

Pelo Teorema 5.2, como o $mdc(5,12) = 1$ então a equação tem solução. Usando o algoritmo acima e fazendo as substituições necessárias, encontramos a solução particular procurada. Segue que

$$1 = 5 - 2.2 \;\; e \;\; 2 = 12 - 5.2$$

o que implica

$$\begin{aligned} 1 &= 5.1 - 2(12.1 - 2.5) \\ 1 &= 5.5 + 12.(-2) \end{aligned}$$

Multiplicando a equação acima por 81, seque que

$$81 = 5.(405) + 12.(-162).$$

Deste modo temos que a solução geral da equação $5x + 12y = 81$ no conjunto dos inteiros é:

$$X = 405 + 12t \text{ e } Y = -162 - 5t \text{ , com } t \in \mathbb{Z}.$$

6 Aplicações

6.1 Problemas práticos envolvendo equações diofantinas em duas variáveis

As equações diofantinas lineares com duas variáveis são de fundamental importância para solucionar problemas que, geralmente, são apresentados no ensino fundamental e resolvidos por tentativa ou resolvidos através de um sistema de equações. A quantidade de problemas práticos do cotidiano ou didáticos na escola que podem ser resolvidos através deste modelo de equação torna ainda mais significativo o aprendizado deste conteúdo e a sua abordagem no contexto escolar independente da série que o mesmo seja trabalhado, mas sempre vinculando-o com outros conteúdos que são normalmente ensinados, como por exemplo as equações do 7º ano, as funções polinomiais do 1º grau da 8ª série e do 1º ano do ensino médio ou até mesmo a geometria analítica que é abordada normalmente nas séries finais do ensino médio.

Exemplo 6.1. - *Em um pedágio, cada carro paga R$ 7,00 e cada motocicleta paga R$ 4,00. Sabendo que foi arrecadado em um certo período de tempo R$ 142,00, calcule o maior número de carros e o maior número de motos possíveis que tenham passado neste pedágio.*

Resolução

Vamos modelar o problema através de uma equação diofantina $7C + 4M = 142$, onde C é o número de carros e M é o número de motos.

Utilizando o algoritmo de Euclides temos que $1 = 4 - 3.1$ e $3 = 7 - 4.1$, e substituindo a segunda igualdade na primeira temos que $1 = 7.(-1) + 4.(2)$, o que implica $142 = 7.(-142) + 4.(284)$, de onde concluímos que as soluções gerais do problema são $C = -142 + 4t$ e $M = 284 - 7t$, com $t \in \mathbb{Z}$.

Como o número de carros e motos é maior do que zero, podemos definir os limites para a variável t, ou seja,

$$-142 + 4t > 0 \text{ e } 284 - 7t > 0,$$

e portanto, $t \geqslant 36$ e $t \leqslant 40$

Deste modo o valor da variável t fica delimitado assim: $36 \leqslant t \leqslant 40$.

Analisando as sentenças gerais que determinam o número de carros e de motocicletas, podemos perceber que quanto maior o valor de t maior será o número de carros e menor o de motos, e quanto menor o valor de t o número de motos será máximo e o número de carros será mínimo, ou seja, quando $t = 40$ então $C = 18$ e $M = 4$ e quando $t = 36$ então $C = 2$ e $M = 32$. Desta forma concluímos que passou no máximo 18 carros ou no máximo 32 motos neste pedágio.

6.2 Resolução de equações do tipo diofantinas com coeficientes racionais

Exemplo 6.2. *Guardo em um cofre só moedas de R$ 0,25 e R$ 0,10. Quantas moedas são necessárias, no mínimo, tendo ao menos 6 moedas de cada valor, para que eu tenha R$ 25,00?*

Este problema será resolvido utilizando os conhecimentos sobre *mdc* generalizado.

Resolução

Do problema acima extraímos a equação $0{,}25X + 0{,}10Y = 25$. Pelo Teorema 4.2, temos que

$$\begin{aligned} mdcg(0{,}25;0{,}10) &= mdcg\left(\frac{1}{4},\frac{1}{10}\right) = \\ \frac{mdc(1,1)}{mmc(4,10)} &= \frac{1}{20} = 0{,}05 \end{aligned}$$

Assim, utilizando o algoritmo de Euclides para encontrar o *mdcg* como combinação linear dos coeficientes, temos a equação

$$0{,}05 = 0{,}25 + 0{,}10.(-2)$$

que multiplicada por 500 resulta

$$25 = 0{,}25.(500) + 0{,}10.(-1000)$$

Se pensarmos em uma resolução análoga ao Teorema 5.2 para os coeficientes racionais, teremos

$$\begin{aligned} X &= 500 + \frac{0{,}1}{0{,}05}t \\ Y &= -1000 - \frac{0{,}25}{0{,}05}t \end{aligned}$$

Então a "solução geral"da equação com coeficientes racionais é dada por

$$\begin{aligned} X &= 500 + 2t, \text{ com } t \in \mathbb{Z} \\ Y &= -1000 - 5t, \text{ com } t \in \mathbb{Z} \end{aligned}$$

Calcula-se agora os limites do valor de t possíveis de acordo com as exigências do problema.

$$\begin{array}{ll} 500 + 2t \geq 6 & -1000 - 5t \geq 6 \\ t \geq -247 & t \leq -202 \end{array}$$

Analisando o problema percebe-se que o número mínimo de moedas ocorre quando $t = -202$. Dessa maneira,

$$\begin{aligned} X &= 500 + 2.(-202) = 96 \text{ moedas} \\ Y &= -1000 - 5.(-202) = 10 \text{ moedas} \end{aligned}$$

O número mínimo de moedas deve ser 96 moedas de R$ 0,25 e 10 moedas de R$ 0,10.

Exemplo 6.3. *Em um posto de combustível o preço da gasolina é R$ 2,89 o litro e o preço do óleo diesel é R$ 2,39 o litro. Em um dia foram arrecadados R$ 5000,00 com a venda de combustível. Calcule o total de litros de gasolina e óleo diesel vendidos, sabendo que foi vendido mais gasolina do que diesel, mas a diferença foi a mínima possível.*

Resolução

Usando G para representar a quantidade de litros de gasolina e D para a quantidade de litros de óleo diesel vendidos, podemos encontrar uma equação do tipo diofantina mas com coeficientes racionais para solucionar o problema.

$$\begin{aligned} 2{,}89G + 2{,}39D &= 5000 \\ mdcg(2{,}89; 2{,}39) &= mdcg(\frac{289}{100}, \frac{239}{100}) \\ &= \frac{mdc(289, 239)}{mmc(100, 100)} \\ &= \frac{1}{100} = 0{,}01 \end{aligned}$$

Como o $mdcg(2{,}89; 2{,}39) = 0{,}01$ divide 5000, então o problema tem solução e podemos usar o algoritmo de Euclides para encontrar o $mdcg$ dos coeficientes como combinação linear dos coeficientes da equação.

	1	4	1	3	1	1	5
2,89	2,39	0,5	0,39	0,11	0,06	0,05	0,01
0,5	0,39	0,11	0,06	0,05	0,01		

Fazendo as substituições necessárias, encontramos a "solução geral"

$$\begin{aligned} G &= -21500000 + 239t \quad \text{, com } t \in \mathbb{Z} \\ D &= 26000000 - 289t \quad \text{, com } t \in \mathbb{Z} \end{aligned}$$

Usando as restrições do problema, temos:

$$\begin{aligned} -21500000 + 239t &> 26000000 - 289t \\ 528t &> 47500000 \\ t &\geq 89963 \\ G &= -21500000 + 239.89963 = 1157 \\ D &= 26000000 - 289.89963 = 693 \end{aligned}$$

Portanto, foram vendidos 1157 litros de gasolina e 693 litros de óleo diesel.

O problema acima pode em alguma turma da educação básica "assustar os alunos"devido aos altos valores das soluções G_0, D_0 e também da variável t. Mas vale lembrar que existem infinitas soluções gerais de uma equação diofantina, e pode ser encontrado uma solução geral que tenha os valores de x_0 e y_0 bem menores e com isto os limites da variável t também se tornam menores.

7 Relação entre equações diofantinas e função afim

Ao estudarmos as equações diofantinas lineares em duas variáveis é inevitável a comparação das mesmas com uma função polinomial do 1º grau (ou função afim), pois toda função afim pode ser escrita da forma $ax + by = c$, com $a, b, c, x, y \in \mathbb{R}$.

Contudo, esta comparação deve ser efetuada com muito cuidado, devido aos conjuntos numéricos distintos em que são trabalhados uma equação diofantina e uma função afim. É correto afirmar, por exemplo, que

toda equação diofantina linear com duas variáveis representa uma função afim que tenha a restrição das variáveis x e y pertencerem ao conjunto dos números inteiros ($\mathbb{Z}$) (ou seja, representa um conjunto de pontos que estão alinhados no plano) ou que ao permitirmos que as variáveis x e y de uma equação diofantina pertençam ao conjunto dos números reais ($\mathbb{R}$) obtém-se uma função afim. Porém, não é verdade que toda função afim representa uma equação diofantina, e para mostrar isto basta tomar os coeficientes $a, b \in \mathbb{I}$, onde $\mathbb{I}$ representa o conjunto dos números irracionais.

Para esclarecer melhor estas diferenças citadas acima, vamos analisar um exemplo através da sua resolução e sua representação geométrica no plano cartesiano.

Exemplo 7.1. *Encontre a solução geral da equação diofantina $3x + 2y = 7$, represente esta solução no plano cartesiano e compare com o gráfico da função afim $f : \mathbb{R} \to \mathbb{R}$ que tem a forma cartesiana $3x + 2y = 7$.*

Resolução

A equação $3x + 2y = 7$ pode ser resolvida facilmente usando os conhecimentos adquiridos até o momento.

$$\begin{aligned} 1 &= 3 \cdot (1) + 2 \cdot (-1) \quad \cdot (7) \\ 7 &= 3 \cdot (7) + 2 \cdot (-7) \end{aligned}$$

A solução geral é $x = 7 + 2t$ e $y = -7 - 3t$, com $t \in \mathbb{Z}$. A representação no plano da equação acima é apresentada na Figura 3.

O gráfico apresentado na Figura 4 é o gráfico da função afim $3x + 2y = 7$, com x,$y \in \mathbb{R}$ e serve para que possamos comparar e entender as semelhanças e diferenças entre a função afim $3x + 2y = 7$ e a equação diofantina $3x + 2y = 7$.

Fazendo a análise do gráfico acima, percebemos que a partir do momento em que encontramos um único ponto (x_0, y_0) onde x_0,y_0 são uma solução particular da equação diofantina estudada conseguimos encontrar todos os outros pontos que também são solução da equação, pois como a solução geral é representa por $x = x_0 + \frac{b}{d}t$ e $y = y_0 - \frac{a}{d}t$ com $t \in \mathbb{Z}$ e $d = mdc(a, b)$ como já vimos anteriormente, basta aumentar ou diminuir $\frac{b}{d}$ no valor da abscissa x_0 e respectivamente diminuir ou aumentar $\frac{a}{d}$ no valor da ordenada y_0 e repetir este processo em cada ponto (x_n, y_n) encontrado.

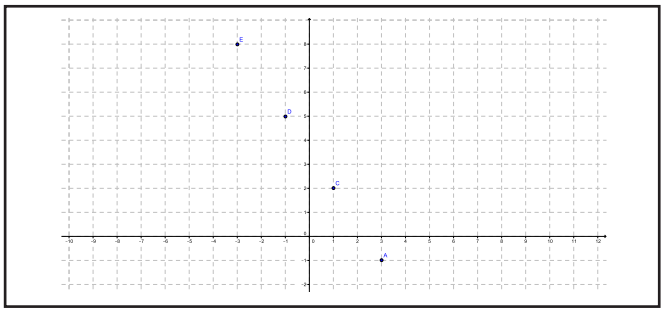

Figura 3 - Solução da equação diofantina $3x + 2y = 7$

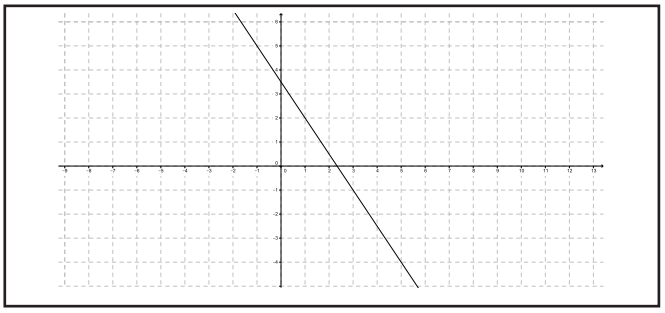

Figura 4 - Gráfico da função afim $3x + 2y = 7$

8 Relação entre equações diofantinas e progressão aritmética (P.A.)

Uma progressão aritmética (P.A.) é uma sequência numérica em que a diferença entre um termo e seu antecessor é sempre a mesma, para qualquer termo da sequência. O termo geral de uma P.A. é encontrado através da fórmula $a_n = a_1 + (n-1).r$, onde a_n é o termo geral, a_1 é o primeiro termo da P.A., $n \in \mathbb{N}^*$ é a posição do termo procurado e r é a razão da P.A. que é definida por $r = a_2 - a_1 = ... = a_n - a_{n-1}$. Para facilitar a associação que pretendemos fazer, vamos escrever o termo geral da P.A. como $a_n = a_1 - r + rn$. E o fato de $n \in \mathbb{N}^*$ é condição necessária em uma P.A. pois n é a ordem do elemento a_n.

Para representar uma progressão aritmética no plano cartesiano podemos escrever a P.A. como função de x e y onde $a_n = y$ e $n = x$. Mas como n pertence ao conjunto $\mathbb{N}^* = \{1,2,3,4,5,\cdots\}$, podemos perceber que seu gráfico será discreto, ou seja será igual ao gráfico de uma equação diofantina. Então, podemos estabelecer uma relação entre estes assuntos de matemática. Fazendo as substituições de x e y temos:

$$\begin{aligned} a_n &= a_1 - r + rn \\ y &= a_1 - r + rx \end{aligned}$$

e portanto

$$-rx + y = a_1 - r$$

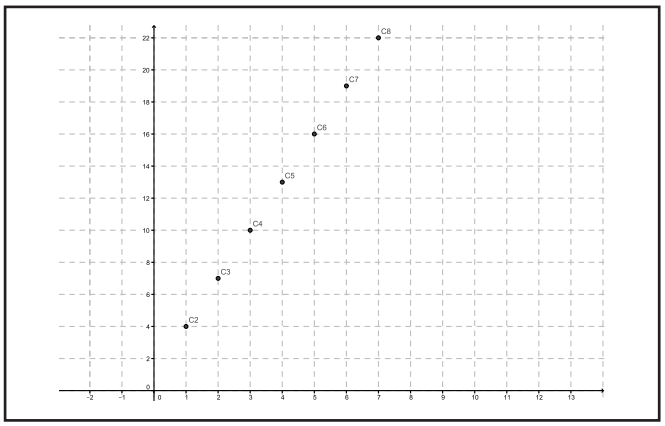

Figura 5- Gráfico da P.A $a_n = 1 + 3n$ e solução da equação $-3x + y = 1$

A equação $-rx + y = a_1 - r$ é uma equação diofantina, onde $a = -r$, $b = 1$ e $c = a_1 - r$. Como $mdc(-r,1) = 1$ e $1|a_1 - r$ então a equação tem solução. E a solução geral será $x = x_0 + t = 1 + t$, pois sempre teremos $x_0 = 1$ e $y = y_0 + rt$, com $t \in \mathbb{N}$, $y_0 = a_1$ e r é a razão da P.A. que da origem a esta equação.

Pelo que foi provado acima, podemos concluir que toda equação diofantina da forma $ax + y = c$ que obedecem as restrições adicionais de só admitir $x \in \mathbb{N}^*$ e $t \in \mathbb{N}$, representam também, automaticamente, uma progressão aritmética (P.A.). Mas é fácil verificar que a recíproca não é verdadeira, ou seja, nem toda P.A. de termo geral $a_n = a_1 + (n-1).r$ gera uma equação diofantina. Basta tomar uma P.A. em que o primeiro termo é um número decimal.

Veja o exemplo abaixo de uma progressão aritmética que pode ser trabalhada como uma equação diofantina, relacionando os dois conteúdos e mostrando graficamente a correspondência entre os dois formatos.

Exemplo 8.1. *Seja a P.A. (4,7,10,13,...). Encontre a equação diofantina correspondente a esta P.A., calcule sua solução geral, e construa o gráfico discreto que representa esta sequência e equação simultaneamente.*

Resolução

Na P.A. acima temos $a_1 = 4$, $r = 3$ e então o terno geral será $a_n = 1 + 3n$. Fazendo as substituições de $a_n = y$ e $n = x$ chegamos na equação desejada:

$$\begin{aligned} y &= 1 + 3x \\ -3x + y &= 1 \end{aligned}$$

A solução geral neste caso pode ser calculada utilizando as informações da P.A. destacados nas fórmulas citadas acima:

$$\begin{aligned} x &= 1 + t \quad , com \;\; t \in \mathbb{N} \\ t &= 4 + 3t \quad , com \;\; t \in \mathbb{N} \end{aligned}$$

O gráfico apresentado na Figura 5 representa a P.A de termo geral $a_n = 1 + 3n$ e a solução da equação diofantina $-3x + y = 1$ foi construído utilizando a 1ª maneira de construção que citamos, utilizando as funções de uma planilha eletrônica no Geogebra.

9 Conclusões

Tivemos a oportunidade de esclarecer e desenvolver o estudo das equações diofantinas lineares em duas variáveis, um tipo de equação que se mostra eficaz na resolução de vários problemas do cotidiano dos estudantes e rica em relação à quantidade, diversidade e proporções destes problemas. Outro fator importante que foi apresentado e comprovado, é o fato de estas equações se relacionarem diretamente com outros conteúdos de outras áreas de conhecimento da matemática que já são abordadas normalmente na educação básica.

A aceitação de um novo conjunto de coeficientes para estas equações se baseia na fundamentação teórica de um novo conceito de *mdc*, o máximo divisor comum generalizado (*mdcg*), que possibilita explorar o conjunto dos números racionais $\mathbb{Q}$ em sua totalidade e com amostras práticas de utilização dos conhecimentos adquiridos sobre este assunto. Nos exemplos de aplicação das equações do tipo diofantinas com coeficientes racionais trabalhamos com situações que realmente podem acontecer no dia a dia, seja na zona urbana ou na zona rural. Devido aos altos valores encontrados em suas resoluções, acreditamos, que alguns destes exemplos poderão causar espanto nos alunos em um primeiro momento, mas que uma de suas funções será cumprida depois do seu entendimento que é mostrar a realidade da matemática.

Referências

EVES, H., 2011. Introdução à história da matemática., 5th Edition. Editora da Unicamp, São Paulo.

HEFEZ, A., 2011. Elementos de Aritmética, 2nd Edition. SBM, Rio de Janeiro.

MARTINEZ, F. B., 2011. Teoria dos números, um passeio com primos e outros números familiares pelo mundo inteiro, 2nd Edition. IMPA, Rio de Janeiro.

NETO, A. C. M., 2012. Tópicos de Matemética Elementar: teoria dos números. Vol. 5. SBM, Rio de Janeiro.

RIBEIRO, J., 2009. Matemática 7o ano;Coleção Projeto Radix. SCIPIONE, São Paulo.

RIPOLL, J., RIPOLL, C., SANT'ANA, A., 2006. O mínimo múltiplo comum e o máximo divisor comum generalizados, 59–74.