PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

PMO v.10, n.3, 2022
ISSN: 2319-023X
https://doi.org/10.21711/2319023x2022/pmo1025

Equações diofantinas lineares e não lineares: uma abordagem por meio de questões de Olimpíadas de Matemática

Érick C. A. do Nascimento [1] Thiago Yukio Tanaka [2] Barbara Costa da Silva[3]

Resumo

Neste trabalho, apresentaremos métodos e técnicas de solução para equações diofantinas lineares e não lineares por meio de questões de Olimpíadas de Matemática. No tratamento das equações lineares, exploraremos a teoria de divisibilidade nos números inteiros, o conceito de máximo divisor comum (MDC) e, então, apresentaremos um resultado, provando, assim, a existência de soluções. No caso não linear, exploraremos técnicas para determinados casos, uma vez que, para equações diofantinas não lineares, não há um método geral de solução. Apresentaremos quatro casos de resolução baseados em aritmética dos inteiros, fatorações, desigualdades e parametrizações. Esperamos que este trabalho sirva como fonte de estudo e pesquisa aos discentes e docentes interessados em Olimpíadas de Matemática.

Palavras-chave: Equações Diofantinas; Olimpíadas de Matemática; Número de Frobenius.

Abstract

In this work, we will present methods and solution techniques for Linear and Nonlinear Diophantine Equations through Mathematical Olympiad questions. In the treatment of linear equations, we will explore the theory of divisibility in whole numbers, the concept of greatest common divisor (GCD) and, then, we will present a result, thus proving the existence of solutions. In the nonlinear case, we will explore techniques for certain cases, since, for nonlinear Diophantine Equations, there is no general solution method. We will present four cases solving based on integer arithmetic, factorizations, inequalities and parameterizations. We hope that this work will serve as a source of study and research for students and teachers interested in Mathematics Olympiads.

Keywords: Diophantine Equations; Mathematics Olympiads; Frobenius Number.

1. Introdução

Em diversos problemas matemáticos, estamos interessados em encontrar soluções inteiras para alguma equação, como o problema *Frobenius*, as *Equações de Pell* ou o problema das famosas

[1]Discente do Departamento de Matemática da UFRPE
[2]Docente do Departamento de Matemática da UFRPE
[3]Docente do Departamento de Matemática da UFRPE

Ternas Pitagóricas de números naturais. Equações que permitem que suas variáveis admitam apenas números inteiros como solução são chamadas de *Equações Diofantinas*.

Esse nome é devido ao matemático, Diofante de Alexandria, o primeiro a investigar sobre como encontrar soluções inteiras (ou racionais) positivas, em problemas que possuem mais variáveis que equações. Os problemas estudados por ele, em geral, eram os indeterminados (que admitem infinitas soluções). Sua obra mais famosa, "Aritmética", é composta por 13 livros, dos quais acreditava-se que apenas 6 haviam sobrevivido ao tempo. No entanto, recentemente, alguns historiadores julgam ter encontrado outros quatro livros de sua obra, traduzidos em árabe [13]. Nessa obra, Diofante propõe a resolução de dezenas de problemas, de diversas naturezas, como equações polinomiais de primeiro, segundo e terceiro graus, e resolução de problemas envolvendo medidas de lado racionais para triângulos retângulos. Inclusive, em seu segundo livro, o problema mais famoso é o de número 8, pois, segundo [14], foi na margem de uma cópia que pertencia a Fermat que ele escreveu, ao lado do problema 8, uma observação que ficou mundialmente conhecida como o "Último Teorema de Fermat".

Figura 1: Diofante de Alexandria. Fonte: [3].

Sabemos pouco da vida de Diofante, sendo incertos o período em que viveu e sua idade. Em [14], há relatos de que ele, supostamente, teria vivido após 150 d.C. e antes de 364 d.C.. Além disso, sobre a sua idade: "De acordo com a memória de um resolvedor de problemas, o único detalhe sobre a vida de Diofante que restou foi um enigma, que dizem ter sido gravado na lápide de seu túmulo." (SINGH, 2014).

O texto que supostamente carrega esse enigma é dado por:

> Deus lhe concedeu a graça de ser um menino pela sexta parte de sua vida. Depois, por um doze avos, ele cobriu seu rosto com a barba. A luz do casamento iluminou-o após a sétima parte e cinco anos depois do casamento Ele concedeu-lhe um filho. Ah! criança tardia e má, depois de viver metade da vida de seu pai, o destino frio a levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos, Diofante terminou sua vida.

Sendo x o valor de sua idade, o problema pode ser representado pela equação

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

o que concluímos que Diofante teria vivido 84 anos.

As Olimpíadas Matemáticas costumam chamar a atenção de muitas escolas e universidades, pois além de incentivarem o estudo da Matemática nas diversas idades, são capazes de revelar e dar holofotes a diversos talentos. No Brasil, Olimpíadas de Matemática ganharam força em 1979, com a criação da Olimpíada Brasileira de Matemática (OBM), que, com o passar dos anos, passou por diversas mudanças, como a divisão por séries e a implementação do nível universitário, até que em 2017, a OBM integrou-se à Olimpíada Brasileira de Matemática das Escolas Públicas (Obmep).

Desde de 1979, o Brasil tem sido representado por uma equipe olímpica na Olimpíada Internacional de Matemática (*International Mathematical Olympiad, IMO*), com um total de 41 participações, obtendo 11 medalhas de ouro, 50 de prata, 81 de bronze e 33 menções honrosas. Destaca-se, dentre os premiados, o medalhista de ouro, Arthur Ávila, primeiro brasileiro a obter uma medalha *Fields*.

As Olimpíadas Matemáticas abordam diversos temas, como Álgebra, Teoria dos Números, Combinatória e Geometria, promovendo assim o estudo de teorias e técnicas para a resolução dos problemas propostos. Neste trabalho, daremos foco a um tema que relaciona Álgebra e Teoria dos Números: equações diofantinas. Mais especificamente, destacaremos métodos de resolução de questões olímpicas relacionadas como o tema.

Há diversos trabalhos que trazem resultados envolvendo equações diofantinas com fins educacionais. Por exemplo, [3] elabora uma sequência didática que serve como material de apoio para o estudo das equações diofantinas lineares e aborda o caso das não lineares por meio do método da descida infinita de Fermat. Já [4] trata de equações diofantinas lineares de n variáveis, suas soluções e suas aplicações na resolução de problemas relacionados a números inteiros. Em [12], são propostas atividades que envolvem equações diofantinas próprias para serem aplicadas em uma sala de aula no Ensino Médio. Semelhante ao nosso trabalho, na revista do Professor de Matemática Online (PMO), há dois artigos que abordam temas olímpicos. Em [5], a autora desenvolve a solução para diversos problemas olímpicos de Matemática, nos temas de Aritmética dos Inteiros e Teoria dos Números. Já em [6], os autores abordam sobre dois importantes resultados da Geometria que são os Teoremas de Ceva e o de Menelaus, assim como suas diversas aplicações.

Este trabalho traz uma abordagem inovadora para a discussão do tema das Equações Diofantinas, por meio da análise e resolução de questões olímpicas nacionais e internacionais. Reunimos uma série de resultados significativos, tanto para o caso linear, quanto para o caso não linear, e destacamos a aplicação dessas ferramentas na solução dos problemas propostos.

Este trabalho foi dividido de maneira quase independente, deixando o(a) leitor(a) livre para ler na ordem que preferir, pois cada seção aborda um método específico de resolução de equações que independe dos demais. Apesar disso, sugerimos que o(a) leitor(a), que não tem muita familiaridade com a aritmética, comece pela Seção 2, pois nela realizamos uma abordagem teórica dos principais conceitos e resultados utilizados no decorrer do trabalho. Na Seção 3, descrevemos os principais resultados envolvidos na busca de soluções das equações diofantinas lineares presentes em diversos problemas olímpicos. Na Seção 4, tratamos dos casos que são mais recorrentes em Olimpíadas de Matemática envolvendo equações diofantinas não lineares, especificamente, abordamos quatro métodos de soluções envolvendo técnicas de fatoração, desigualdades, parametrizações e aritmética modular. Por fim, na Seção 5, fazemos a conclusão do trabalho.

2. Um pouco sobre Aritmética dos Inteiros

Exibiremos e demonstraremos alguns conceitos e resultados que serão importantes ao decorrer deste artigo: divisibilidade, máximo divisor comum e congruência modular. A aplicação destes resultados é destacada a partir de soluções de problemas do banco de questões da Obmep.

Definição 1 (Divisibilidade)**.** Dados dois números inteiros a e b com $a \neq 0$, diz-se que a divide b, e denota-se $a \mid b$, quando existe um inteiro c tal que $ac = b$. Nesse caso, também podemos dizer que b é um múltiplo de a. Se a não divide b, então não existe c inteiro tal que $ac = b$. Quando isso acontece, denotamos por $a \nmid b$.

Proposição 1. *Sejam a, b e c números inteiros. Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Como $a \mid b$ existe $q_1 \in \mathbb{Z}$ tal que $b = aq_1$, do mesmo modo, como $b \mid c$ existe $q_2 \in \mathbb{Z}$ tal que $c = bq_2$. Assim, temos que $c = (aq_1)q_2$, concluindo que $a \mid c$.

□

Teorema 1 (Divisão Euclidiana)**.** *Sejam a e b números inteiros, com $0 \neq b$. Existem dois únicos inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$.*

Demonstração. Temos dois casos a considerar: quando $b > 0$ e $b < 0$. É fácil perceber que a deve estar entre dois múltiplos consecutivos de b.

Para $b < 0$, tome $q \in \mathbb{Z}$ tal que

$$qb \leq a < (q-1)b \quad \Rightarrow \quad qb \leq a < qb - b \quad \Rightarrow \quad 0 \leq a - qb < -b.$$

Então, considerando $r = a - qb$, garantimos a existência de q e r satisfazendo as condições do teorema.

Para provar a unicidade, tome q' e r' tais que $a = bq' + r'$, com $0 \leq r' < |b|$. Daí, utilizando as duas expressões para a, temos que $(bq + r) - (bq' + r') = 0$ o que implica que $r - r' = b(q' - q)$. Isso nos diz que $b \mid r - r'$, mas como $r < |b|$ e $r' < |b|$ temos que $|r - r'| < |b|$. Logo, a única possibilidade é termos $r - r' = 0$, logo $r' = r$ e $b(q' - q) = 0$, e como $b \neq 0$ concluímos que $q' = q$, provando assim a unicidade.

Para $b > 0$, basta considerar $qb \leq a < (q+1)b$ e seguir de forma análoga.

□

Observação 1. Nas condições do teorema acima, q e r são respectivamente o quociente e o resto da divisão de a por b.

A proposição que provaremos a seguir vai nos ajudar a concluir o resultado do Exemplo 1.

Proposição 2. *Sejam a, b e c inteiros tais que $a \mid b$ e $a \mid c$, então $a \mid bx + cy$, para quaisquer $x, y \in \mathbb{Z}$.*

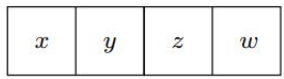
Demonstração. Como $a \mid b$ e $a \mid c$, temos que $b = aq_1$ e $c = aq_2$. Dessa forma, para quaisquer $x, y \in \mathbb{Z}$, temos que

$$bx + cy = (aq_1)x + (aq_2)y = a(q_1x + q_2y),$$

como $q_1x + q_2x \in \mathbb{Z}$, então $a \mid bx + cy$. □

A seguir, é explorado um problema do banco de questões da Obmep 2013 cuja solução que envolve uma equação Diofantina e aplica os resultados apresentados.

Exemplo 1 (Banco de questões OBMEP, 2013, Nível 3, Problema 21, [9])**.** Os números x, y, z e w na figura são números inteiros todos diferentes entre si, maiores do que 1, e foram colocados nas casas abaixo de modo que cada número (a partir do y) é divisor do número na casa da esquerda.



Descubra todas as soluções possíveis para x, y, z e w, sabendo que a soma deles é 329.

Solução. Pelas relações apresentadas no enunciado, vemos que

$$1 < w < z < y < x < 329.$$

Além disso, como $w \mid z$ e $z \mid y$, pela Proposição 1 temos que $w \mid y$, e como $y \mid x$ também concluímos que $w \mid x$, ou seja, w é divisor de todos os números das casas. Dessa forma, pela Proposição 2, w é divisor da soma dos números das casas, isto é, é divisor de 329. Agora, note que 329 pode ser fatorado como a multiplicação de dois primos da seguinte forma: $329 = 7 \cdot 47$, daí concluímos que $w = 7$ ou $w = 47$. Vamos olhar os dois casos.

Caso w = 47. Nesse caso, temos que $x + y + z = 2 \cdot 3 \cdot 47$. Aplicando o mesmo argumento utilizado para w, teremos $z \mid x$ e $z \mid y$, daí z divide $2 \cdot 3 \cdot 47 = 2 \cdot 47 + 2 \cdot 47 + 2 \cdot 47$. Como $z < y < x$, temos que z deve ser menor do que $2 \cdot 47$. Mas z não pode ser igual a $w = 47$ e também não pode ser menor, logo não existe solução quando $w = 47$.

Caso w = 7. Aqui, temos $x + y + z = 322$. Daí, com os mesmos argumentos, sabemos que z divide $322 = 2 \cdot 7 \cdot 23$. Como $w \mid z$ temos que as únicas possibilidades para w são $7 \cdot 2$ e $7 \cdot 23$, mas , como $z < y < x$, para satisfazer a soma devemos ter $z < 7 \cdot 23$, concluindo que $z = 7 \cdot 2$. Substituindo o valor encontrado para z e sabendo que $y \mid x$, vemos que y divide $x + y = 308$, que pode ser fatorado tal como $308 = 2 \cdot 2 \cdot 7 \cdot 11$. Como $14 = z < y$, os valores possíveis para y são $2 \cdot 2 \cdot 7$ e $2 \cdot 7 \cdot 11$. Já que queremos que $x + y = 308$ com $y < x$, temos que $y = 2 \cdot 2 \cdot 7$. E finalmente concluímos que $x = 329 - 7 - 14 - 28 = 280$. Portanto, $w = 7, z = 7 \cdot 2, y = 7 \cdot 2 \cdot 2$ e $x = 7 \cdot 4 \cdot 10$. ■

Definição 2 (Máximo Divisor Comum)**.** Sejam a e b dois inteiros não simultaneamente nulos, diz-se que o inteiro positivo d é o máximo divisor comum de a e b, e denotamos por $d = mdc(a, b)$, se d satisfaz as seguintes condições:

(i) d é um divisor comum de a e b, ou seja, $d \mid a$ e $d \mid b$;

(ii) d é divisível por todo divisor comum de a e b, isto é, se c é divisor comum de a e b, então $c \mid d$.

Teorema 2. *Seja d o máximo divisor comum de a e b. Então existem m e n inteiros, tais que $d = ma + nb$.*

Demonstração. Considere o conjunto

$$A = \{xa + yb; x, y \in \mathbb{Z}\}$$

de todas as combinações lineares de a e b. Claramente, A é não vazio e contém números positivos, negativos e o zero. Dessa forma, podemos escolher m e n tais que $c = ma + nb$ seja o menor inteiro positivo que pertence ao conjunto A.

Note que $c \mid a$ e $c \mid b$. De fato, suponha que $c \nmid a$, pela divisão euclidiana, existem q e r tais que $a = qc + r$, com $0 \leq r < c$. Note que se $0 < r < c$ teríamos

$$r = a - qc \quad \Rightarrow \quad r = a - q(ma + nb) \quad \Rightarrow \quad r = (1 - qm)a - qnb,$$

o que nos diz que r é uma combinação linear de a e b e então pertence a A. O que é uma contradição, pois $0 < r < c$ e tomamos c como o menor número positivo em A. Logo $r = 0$ e, consequentemente, $c \mid a$. De forma análoga, $c \mid b$. Como $d = mdc(a, b)$, vale então que $c \mid d$.

Além disso, existem q_1 e q_2 tais que $a = q_1 d$ e $b = q_2 d$, e então

$$c = ma + nb \quad \Rightarrow \quad c = mq_1 d + nq_2 d \quad \Rightarrow \quad c = d(mq_1 + nq_2),$$

ou seja, $d \mid c$.

Portanto, como $c \mid d$ e $d \mid c$, e sendo ambos positivos, concluímos que $d = c = ma + nb$.

□

Lema 1 (Lema de Euclides)**.** *Sejam a, b e n inteiros não nulos, com $a \leq na < b$, então existe $mdc(a, b)$ e $mdc(a, b) = mdc(a, b\text{-}na)$.*

Demonstração. Seja $d = mdc(a, b - na)$, como $d \mid a$, $d \mid b - na$ e $b = b - na + na$, a Proposição 2 garante-nos que $d \mid b$. Logo, d é divisor comum de a e b. Tome c, outro divisor comum de a e b, ou seja, $c \mid a$ e $c \mid b$, mas isso implica que $c \mid b - na$, assim $c \mid d$, pois $d = mdc(a, b - na)$. Note que acabamos de provar que $d = mdc(a, b)$. Portanto, $mdc(a, b)$ existe e é igual ao $mdc(a, b - na)$.

□

Exemplo 2 (OBM, 2011, 2ª Fase, Nível 2, Problema 3, [8])**.** Quantos são os pares ordenados (a, b), com a e b inteiros positivos, tais que

$$a + b + mdc(a, b) = 33?$$

Solução: Considere $d = mdc(a, b)$, daí podemos reescrever a equação da seguinte forma:

$$\frac{a}{d} + \frac{b}{d} + 1 = \frac{33}{d}.$$

Como $d \mid a$ e $d \mid b$, temos que o lado esquerdo da equação acima é uma soma de números inteiros, logo, o lado direito deve ser um número inteiro, o que nos diz que d divide 33. Além disso, pelo Lema 1, vale que

$$mdc\left(\frac{a}{d}, \frac{b}{d}\right) = mdc\left(\frac{a}{d}, \frac{33}{d} - 1\right) = mdc\left(\frac{b}{d}, \frac{33}{d} - 1\right) = 1.$$

Portanto, se fixarmos d, basta encontrarmos pares de inteiros positivos (x, y) com $mdc\left(x, \frac{33}{d} - 1\right) = 1$ com $x + y = \frac{33}{d} - 1$, pois daí também vamos obter $mdc\left(y, \frac{33}{d} - 1\right) = 1$ e que $(a, b) = (dx, dy)$ também é solução. Agora, como $d \mid 33$, vemos que d só pode admitir um dos quatro valores: $1, 3, 11$ e 33. Vejamos os casos:

Caso 1. Para $d = 1$ temos que $x + y = 32$, daí podemos ter 16 soluções, pois basta escolher x ímpar.

Caso 2. Para $d = 3$ temos que $x + y = 10$, teremos 4 possibilidades, pois x deve ser um número menor do que 10 que não pode ser par e nem múltiplo de 5.

Caso 3. Para $d = 11$ temos que $x + y = 2$, logo vamos ter apenas uma solução para x.

Caso 4. Para $d = 33$, não teremos solução, pois nesse caso $x + y = 0$, mas x e y são inteiros positivos.

Assim, concluímos que existem 21 pares de soluções. ■

Exemplo 3 (OBM, 2012, 1ª Fase, Nível 3, Problema 5, [8])**.** Em 2012, foi realizada a edição 34 da OBM, e $mdc(2012, 34) = 2$. Supondo que a OBM sempre será realizada todo ano, qual é o maior valor possível para o MDC do ano e da edição da OBM realizado no ano?

Solução: Se estivermos na edição de número x da OBM, estaremos no ano $1978 + x$. Dessa forma, estamos procurando o valor máximo para $mdc(x, 1978 + x)$. Note que, pelo Lema 1, $mdc(x, 1978 + x) = mdc(x, 1978 + x - x) = mdc(x, 1978)$, portanto o maior valor possível para esse MDC é 1978, que é obtido quando tomamos $x = 1978$. ■

Definição 3. Sejam $a, b, p \in \mathbb{Z}$. Dizemos que a é congruente a b módulo p se $p \mid (a - b)$, ou seja, se a e b deixam o mesmo resto na divisão por p. Nesse caso, denotamos tal congruência por

$$a \equiv b \mod p.$$

Enunciaremos, agora, algumas propriedades de congruência, porém não as provaremos devido à grande quantidade de itens; elas podem ser encontradas em [7].

Proposição 3. *Sejam a, b, c, d, m e n números inteiros, com $m, n > 1$, então:*

1. *Se $a \equiv b \mod n$ e $b \equiv c \mod n$, então $a \equiv c \mod n$;*
2. *Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então $a \cdot c \equiv b \cdot d \mod n$ e $a + c \equiv b + d \mod n$;*
3. *Se $a \equiv b \mod n$, então $a^k \equiv b^k \mod n$, para todo $k \in \mathbb{N}$;*
4. *Se $a \equiv b \mod n$ e $m \mid n$, então $a \equiv b \mod m$;*
5. *Se $a \equiv b \mod n$, então $mdc(a, n) = mdc(b, n)$;*
6. *Se $a + c \equiv b + c \mod n$, então $a \equiv b \mod n$;*
7. *Se $a \equiv b \mod m \cdot n$, então $a \equiv b \mod m$ e $a \equiv b \mod n$;*
8. *Se $a \equiv b \mod m$ e $a \equiv b \mod n$, com $mdc(m, n) = 1$, então $a \equiv b \mod m \cdot n$.*

As propriedades de congruência modular são fortes ferramentas para a resolução de questões olímpicas relacionadas, principalmente, para encontrar restos de uma divisão. Mais adiante, vamos utilizar essas ideias como um método de resolução de equações diofantinas não lineares.

Exemplo 4 (Caderno de Exercícios, Portal da Obmep, Aritmética Modular, Exercício 17, [11])**.** Qual o resto de $36^{36} + 41^{41}$ na divisão por 77?

Solução: Perceba que os números do problema obedecem à seguinte relação: $36 + 41 = 77$. Dessa forma,

$$\begin{aligned} -36 &\equiv 41 \mod 77 \\ (-36)^{41} &\equiv 41^{41} \mod 77 \\ 36^{36} + (-36)^{41} &\equiv 36^{36} + 41^{41} \mod 77 \\ 36^{36}\left(1 - 36^5\right) &\equiv 36^{36} + 41^{41} \mod 77. \end{aligned}$$

Então, basta encontrarmos o resto da divisão de $1 - 36^5$ por 77. Como $36 = 7 \cdot 5 + 1$, temos que $36 \equiv 1 \mod 7$, daí $36^5 \equiv 1 \mod 7$. Além disso, é fácil ver que $36 \equiv 3 \mod 11$ e como $3^5 = 243 = 11 \cdot 22 + 1$, podemos concluir que $36^5 \equiv 3^5 \equiv 1 \mod 11$. Uma vez que $mdc(7, 11) = 1$ e ambos dividem $36^5 - 1$, conclui-se que 77 divide $36^5 - 1$. Portanto, $36^{36} + 41^{41}$ deixa resto 0 na divisão por 77. ■

3. Equações Diofantinas Lineares

Agora com as ferramentas em mãos, iremos nos concentrar em resolver problemas de equações diofantinas lineares que são equações do tipo $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, onde os a_i, com $i = 1, \ldots, n$ são inteiros não simultaneamente nulos e b um inteiro conhecido. Já os símbolos $x_1, \ldots, x_n$ representam as incógnitas da equação, e estamos interessados em encontrar apenas soluções inteiras para a equação. Por conveniência, enunciaremos apenas os resultados para o caso em duas variáveis, mas que podem ser facilmente generalizados para o caso de n variáveis, ver [3].

Teorema 3. *A equação Diofantina $ax + by = c$, com $a \neq 0$ ou $b \neq 0$, terá solução inteira se, e somente se, $d = mdc(a, b)$ divide c.*

Demonstração. Seja (x_0, y_0) uma solução particular e $d = mdc(a, b)$, então temos $a = dk_1$, $b = dk_2$ e $ax_0 + by_0 = c$, o que implica que $dk_1x_0 + dk_2y_0 = c$, ou seja, $d(k_1x_0 + k_2y_0) = c$, portanto $d \mid c$. Reciprocamente, suponha que $d = mdc(a, b)$ e $d \mid c$. Como $d \mid c$, temos $c = dt$. Como $d = mdc(a, b)$ pelo Teorema 2 existem $m, n \in \mathbb{Z}$ tais que $am + bn = d$, multiplicando a igualdade por t, obtemos $amt + bnt = dt = c$. Portanto (mt, nt) é uma solução para a equação em questão.

□

Observação 2. Note que, sempre que o $mdc(a, b)$ divide c podemos simplificar a equação $ax+by = c$ por uma do tipo $a'x + b'y = c'$ onde $a' = a/mdc(a, b)$, $b' = b/mdc(a, b)$ e $c' = c/mdc(a, b)$. Dessa forma a' e b' são primos entre si, o que significa que $mdc(a', b') = 1$. Portanto, sempre que uma equação diofantina admite soluções inteiras, podemos obter uma equação equivalente cujos coeficientes são primos entre si, daí segue o resultado:

Proposição 4. *Seja (x_0, y_0) uma solução particular da equação $ax + by = c$, onde $mdc(a, b) = 1$. Então todas as soluções inteiras (x, y) da equação são da seguinte forma: $x = x_0 - bt$, $y = y_0 + at$ e $t \in \mathbb{Z}$.*

Demonstração: Seja (x_0, y_0) uma solução particular conhecida, então $ax_0+by_0 = c$. Se (x, y) é outra solução qualquer, temos $ax + by = c$. Assim, $ax_0 + by_0 = ax + by$, ou seja, $a(x_0 - x) = b(y - y_0)$, o que implica que $a \mid b(y - y_0)$, mas como $mdc(a, b) = 1$ temos, $a \mid y - y_0$, assim $at = y - y_0$. Substituindo, temos $a(x_0 - x) = bat$, obtendo $bt = x_0 - x$. Portanto, $x = x_0 - bt, \quad y = y_0 + at, \quad t \in \mathbb{Z}$. Note que x e y, como definidos acima, são soluções, pois

$$ax + by = a(x_0 - bt) + b(y_0 + at) = ax_0 + by_0 = c.$$

□

Exemplo 5 (Obmep, 2008, 1ª Fase, Nível 2, Problema 13, [9])**.** Os 535 alunos e os professores de uma escola fizeram um passeio de ônibus. Os ônibus, com capacidade para 46 passageiros cada, ficaram lotados. Em cada ônibus havia um ou dois professores. Em quantos ônibus havia dois professores?

Solução: Sendo x o número de ônibus com 1 professor e y o número de ônibus com 2 professores. Note que nos ônibus com 1 professor há 45 alunos e nos ônibus com 2 professores há 44 alunos, pois todos os 46 lugares dos ônibus estão lotados. Assim, obtemos a equação $45x + 44y = 535$, onde queremos encontrar uma solução (x, y) de números naturais. Como $mdc(45, 44) = 1$ e $1 \mid 535$ a equação possui solução, e notando que $45 \cdot 1 + 44 \cdot (-1) = 1$ isso implica que $45 \cdot 535 + 44 \cdot (-535) = 535$. Logo, uma solução particular para a equação é $x_0 = 535$ e $y_0 = -535$. Pela Proposição 4, temos que a solução geral é

$$x = 535 - 44t \quad \text{e} \quad y = -535 + 45t, \ t \in \mathbb{Z}.$$

Como queremos que a solução (x, y) seja um par de números naturais, devemos ter $535 - 44t > 0$ e $-535 + 45t > 0$. Resolvendo essas desigualdades, encontramos o único inteiro $t = 12$ e, consequentemente, a única solução natural é o par $x = 7$ e $y = 5$. Portanto, havia 5 ônibus com 2 professores.

■

Note que uma equação diofantina linear de duas variáveis da forma $ax + by = c$ também pode ser vista como a reta $y = \dfrac{c - ax}{b}$ e, desde que $mdc(a, b)$ divida c, as soluções que estamos procurando para essa equação que modela o problema em tela são os pontos dessa reta cujas coordenadas são, ambas, números inteiros. Durante a solução do Exemplo 5, trabalhamos com a equação $45x + 44y = 535$, e sua reta correspondente é representada a seguir:

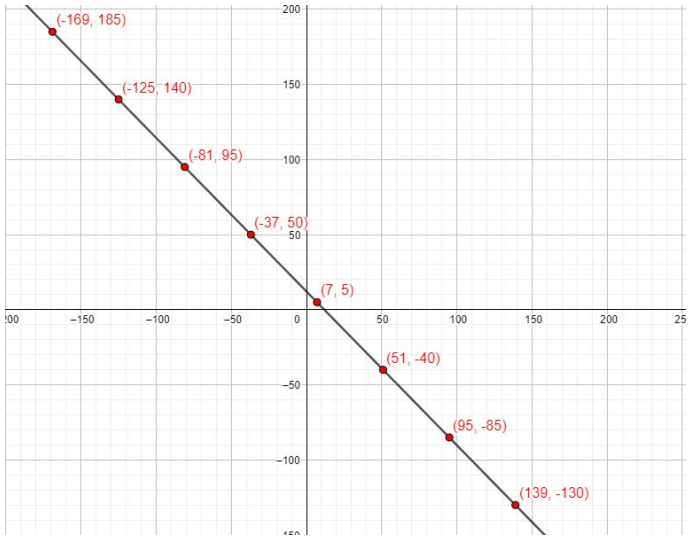


Figura 2: Reta - Exemplo 6. Fonte: Autores.

Os pontos destacados na reta são algumas das infinitas soluções para a equação $45x + 44y = 535$, cujas coordenadas são ambas inteiras. Note que a única solução em inteiros positivos é de fato $x = 7$ e $y = 5$. ■

O exemplo a seguir, apesar de não pertencer a nenhuma olimpíada, é importante pois determina quais dos inteiros positivos podem ser expressos como uma combinação linear positiva de dois inteiros positivos a e b com $mdc(a, b) = 1$. Tal resultado pode ser útil para resolver problemas como o do Exemplo 5.

Exemplo 6 (O Número de Frobenius)**.** Dados a e b inteiros positivos tais que $mdc(a, b) = 1$. Determine o maior inteiro positivo $g = g(a, b)$ tal que todo $d > g$ pode ser expresso como uma combinação linear positiva de a e b, isto é, existem $x, y \in \mathbb{Z}^+$ tais que $ax + by = d$.

Solução: Este é o famoso problema do Número de Frobenius em duas variáveis, e, nesse caso, temos que $g(a, b) = ab - a - b$. De fato, como $mdc(a, b) = 1$ podemos representar qualquer número inteiro positivo p como $p = xa + yb; x, y \in \mathbb{Z}$. Além disso, pela Proposição 4, existem diversas maneiras de representar p desde que $x = x_0 - bt$ e $y = y_0 + at$ onde (x_0, y_0) é uma solução particular e $t \in \mathbb{Z}$. Contudo, note que essa representação torna-se única, quando estamos procurando por $0 \leq x < b$, e nesse caso, p é representável se $y \geq 0$, e o contrário, se $y < 0$. Então, o maior número que não pode ser expresso é quando $x = b - 1$ e $y = -1$, portanto,

$$g(a, b) = (b - 1)a + (-1)b = ab - a - b.$$

■

Este resultado estende-se para n variáveis, e o caso mais geral pode ser encontrado em [1].

4. Traçando Estratégias para Equações Diofantinas Não Lineares

Diferente de problemas de equações diofantinas lineares, os casos não lineares não possuem um método de solução, sendo necessário uma análise específica para cada caso. A grande maioria das

questões de Olimpíadas de Matemática sobre equações diofantinas acaba trazendo em si equações não lineares. Ainda assim, veremos, nesta seção, que mesmo não tendo um formato unificado de solução, há estratégias que podem ser empregadas, dependendo do tipo de solução que envolve o problema (por exemplo: provar que há infinitas soluções ou que não há solução). Apresentaremos quatro técnicas (fatorações, desigualdades, parametrizações e aritmética modular) para o caso não linear.

4.1. Método das Fatorações

A busca por soluções naturais ou inteiras para equações diofantinas, muitas vezes, recai em manipulações algébricas de equações ou sistemas de equações, de modo que essas possam ser simplificadas até que possamos obter conclusões parciais ou mesmo finais. Quando procuramos por soluções que podem ser solúveis por meio de radicais (ou seja, que podem ser resolvidas por meio de operações algébricas ou raízes), as fatorações por meio dos produtos notáveis consistem em fortes ferramentas para essas simplificações, de maneira a deixar explícito informações como divisibilidade ou termos em comum que podem ser simplificados. Nosso primeiro problema recai no uso de um produto notável comum em competições, mas menos usualmente conhecido e utilizado.

Exemplo 7 (POTI, 2012, Teoria dos Números, Nível 2, Aula 1, Problema 38, [10])**.** Encontre todos os pares de inteiros (x, y) tais que $1 + 1996x + 1998y = xy$.

Solução: Reorganizando a identidade, obtemos

$$xy - 1996x - 1998y = 1. \tag{1}$$

A expressão no lado esquerdo de (1) sugere o seguinte produto: dados $x, y, a, b \in \mathbb{R}$, é possível mostrar que

$$(x - a)(y - b) = xy - bx - ay + ab.$$

Perceba que para corresponder ao produto, ainda falta o termo ab, que nesse caso será $1996 \cdot 1998$. Somando $1996 \cdot 1998$ em ambos os lados de (1) ficaremos com

$$(x - 1998)(y - 1996) = 1996 \cdot 1998 + 1. \tag{2}$$

Relembremos do produto notável $a^2 - b^2 = (a + b)(a - b)$, e perceba agora que o lado direito de (2), o produto $1996 \cdot 1998$ pode ser reescrito, pois $1996 = (1997 - 1)$ e $1998 = (1997 + 1)$, donde

$$1996 \cdot 1998 + 1 = (1997 - 1)(1997 + 1) + 1 = (1997^2 - 1) + 1 = 1997^2. \tag{3}$$

Combinando (2) e (3), concluímos que

$$(x - 1998)(y - 1996) = 1997^2.$$

Chegando aqui, precisamos descobrir os divisores de 1997. Como $45^2 = 2025$, então testando os divisores primos menores do que 45, descobrimos que o número 1997 não é divisível por nenhum deles, portanto 1997 é um número primo. Assim, os divisores de 1997^2 são ± 1, ± 1997 e $\pm 1997^2$, de modo que

$$1997^2 = (\pm 1)(\pm 1997^2) = (\pm 1997)(\pm 1997) = (\pm 1997^2)(\pm 1).$$

Portanto, as possibilidades são

$$\begin{cases} x-1998=\pm 1, \\ y-1996=\pm 1997^2, \end{cases} \quad \text{ou} \quad \begin{cases} x-1998=\pm 1997, \\ y-1996=\pm 1997, \end{cases} \quad \text{ou} \quad \begin{cases} x-1998=\pm 1997^2, \\ y-1996=\pm 1. \end{cases}$$

Perceba que o sistema é simples de ser solucionado, bastando somar 1998 e 1996 em ambos os lados da equação para x e y respectivamente. Obtemos, assim, as soluções

$$(x,y) \in \{(1998 \pm 1, 1996 \pm 1997^2), (1998 \pm 1997, 1996 \pm 1997), (1998 \pm 1997^2, 1996 \pm 1)\}.$$

■

Exemplo 8 (OBM, 2006, 3ª Fase, Nível 1, Primeiro Dia, Problema 3, [8])**.** Encontre todos os pares ordenados (x,y) de inteiros tais que

$$x^3 - y^3 = 3(x^2 - y^2). \tag{4}$$

Solução. Primeiramente, é fácil notar que, para $x = y$, obtemos uma identidade verdadeira em (4). Isso nos diz que os pares da forma (n,n) com $n \in \mathbb{Z}$ são soluções. Daqui em diante, consideramos $x \neq y$. Dados $a, b \in \mathbb{R}$, é possível mostrar que

$$a^3 - b^3 = (a-b)(a^2+ab+b^2) \quad \text{e} \quad a^2 - b^2 = (a+b)(a-b).$$

Perceba que a equação (4) pode ser reescrita como

$$(x-y)(x^2+xy+y^2) = 3(x+y)(x-y).$$

Como $x \neq y$, podemos simplificar os termos $x-y$ e ficamos com

$$x^2 + xy + y^2 = 3x + 3y,$$

que é equivalente à seguinte equação quadrática na variável x,

$$x^2 + (y-3)x + y^2 - 3y = 0. \tag{5}$$

Para que a equação acima tenha solução real, devemos impor a condição que o descriminante Δ deve ser não negativo. Como

$$\Delta = (y-3)^2 - 4(y^2-3y) = (y-3)^2 - 4y(y-3) = (y-3)[(y-3)-4y] = (y-3)(-3y-3) = -3(y-3)(y+1).$$

Forçando a condição $\Delta \geq 0$, obtemos

$$-3(y-3)(y+1) \geq 0 \quad \Leftrightarrow \quad (y-3)(y+1) \leq 0.$$

Fazendo um estudo do sinal para a função $p(y) = (y-3)(y+1)$, percebemos que ela é não positiva para $-1 \leq y \leq 1$. Uma vez que y é inteiro, então temos as seguintes possibilidades $y \in \{-1, 0, 1, 2, 3\}$. Para cada valor de y assumido, substituiremos esse valor na equação (5) e encontraremos as soluções inteiras para x.

Caso 1. $y = -1$**.** A equação (5) assume o seguinte formato

$$x^2 - 4x + 4 = 0 \quad \Rightarrow \quad (x-2)^2 = 0 \quad \Rightarrow \quad x = 2,$$

portanto, obtemos a solução $(-1, 2)$.

Caso 2. $y = 0$**.** A equação (5) assume o seguinte formato

$$x^2 - 3x = 0 \quad \Rightarrow \quad x(x-3) = 0 \quad \Rightarrow \quad x = 0 \text{ ou } x = 3,$$

e as soluções são $(0, 0)$ e $(3, 0)$.

Caso 3. $y = 1$**.** A equação (5) assume o seguinte formato

$$x^2 + 2x - 2 = 0,$$

que não tem solução inteira, pois o discriminante nesse caso é igual a 12.

Caso 4. $y = 2$**.** A equação (5) assume o seguinte formato

$$x^2 - x - 2 = 0 \quad \Rightarrow \quad (x+1)(x-2) = 0 \quad \Rightarrow \quad x = -1 \text{ ou } x = 2.$$

As soluções desse caso são $(-1, 2)$ e $(2, 2)$.

Caso 5. $y = 3$**.** Finalmente, a equação (5) assume o seguinte formato

$$x^2 = 0 \quad \Rightarrow \quad x = 0,$$

e a última solução é $(0, 3)$. Dessa forma, todas as soluções de (4) são

$$\{(-1, 2), (2, -1), (3, 0), (0, 3)\} \cup \{(n, n)/n \in \mathbb{Z}\}.$$

■

4.2. Método das Desigualdades

Outra possibilidade de manipulação consiste no desenvolvimento de desigualdades, de maneira a encaixar as possibilidade em intervalos. Desse modo, como as soluções são inteiras, a quantidade de possibilidades é limitada, fazendo com que o resultado possa ser obtido por meio do esgotamento dos casos possíveis.

Exemplo 9 (Olimpíada de Matemática Romena, [2])**.** Encontre todos os números inteiros positivos x, y, z tais que

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}. \tag{6}$$

Solução: Como a expressão em (6) é simétrica nas variáveis x, y e z, uma vez que encontramos uma solução (a, b, c) de (6) então qualquer permutação ainda é uma solução. Observe agora que se qualquer uma das variáveis for 1, já não há mais solução, uma vez que $\frac{3}{5} < 1$. Assim, para mapear as soluções, vamos supor

$$2 \leq x \leq y \leq z, \tag{7}$$

de modo que qualquer outra solução é obtida por permutação das soluções que encontraremos. Da desigualdade (7), concluímos que

$$\frac{1}{z} \leq \frac{1}{y} \leq \frac{1}{x}, \tag{8}$$

logo,

$$\frac{3}{5} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \leq \frac{3}{x}, \tag{9}$$

donde, $x \leq 5$. Limitamos assim as possibilidades de x ao intervalo $[2, 5]$. Olharemos, agora, cada caso para esgotar as possibilidades:

Caso 1. $x = 2$**.** Nessa situação a equação (6) torna-se

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{10}. \tag{10}$$

Observando a expressão acima, concluímos que tanto y quanto z devem ser maiores do que 10. Mais ainda, prosseguindo como em (8) e (9) obtemos

$$\frac{1}{10} \leq \frac{2}{y} \quad \Rightarrow \quad y \leq 20.$$

Portanto, $11 \leq y \leq 20$. Multiplicando (10) por $10yz$, e organizando, obtemos

$$yz - 10y - 10z = 0 \quad \Rightarrow \quad yz - 10y - 10z + 100 = 100 \quad \Rightarrow \quad (y-10)(z-10) = 100,$$

e isolando z obtemos

$$z = 10 + \frac{100}{y-10}, \tag{11}$$

de modo que 100 precisa ser divisível por $y - 10$ para que z seja inteiro. As únicas possibilidades são $y \in \{11, 12, 14, 15, 20\}$ e, pondo esses valores em (11), obtemos as soluções inteiras $(2, 11, 110)$, $(2, 12, 60)$, $(2, 14, 35)$, $(2, 15, 30)$ e $(2, 20, 20)$.

Para os demais casos, o raciocínio é análogo, considerando y no intervalo pertinente, e considerando as diversas possibilidades inteiras para z.

Caso 2. $x = 3$**.** Obtemos $\frac{1}{y} + \frac{1}{z} = \frac{4}{15}$, o que nos dá

$$\frac{4}{15} \leq \frac{2}{y} \quad \Rightarrow \quad y \leq \frac{15}{2},$$

portanto, $y \in [3, 7]$. Perceba que

$$z = \frac{15y}{4y - 15},$$

e, novamente substituindo os valores de y, encontramos as seguintes soluções de triplas inteiras $(3, 4, 60)$, $(3, 5, 15)$ e $(3, 6, 10)$.

A partir daqui, usaremos as mesmas ideias dos casos 1 e 2, dessa maneira, omitiremos os detalhes.

Caso 3. $x = 4$**.** A equação (6) reduz-se a $\frac{1}{y} + \frac{1}{z} = \frac{7}{20}$, o que nos dá $y \in [4, 5]$, e a única solução é $(4, 4, 10)$.

Caso 4. $x = 5$**.** Por fim, ficamos com $\frac{1}{y} + \frac{1}{z} = \frac{2}{5}$, e $y = z = 5$ é a única solução; portanto obtemos $(5, 5, 5)$.

Considerando $x < y < z$, obtemos como soluções $(x, y, z) \in \{(2, 11, 110), (2, 12, 60), (2, 14, 35), (2, 15, 30), (2, 20, 20), (3, 4, 60), (3, 5, 15), (3, 6, 10), (4, 4, 10), (5, 5, 5)\}$. Cabe observar que, como (6) é simétrica em relação às variáveis x, y, z, então todas as permutações das ternas ordenadas indicadas compõem o conjunto solução de (6). ■

Exemplo 10 (Olimpíada de Matemática da Rússia, 1997, Rodada Final, 10ª Série, Primeiro Dia, Problema 1, [2])**.** Encontre todas as soluções inteiras da equação

$$(x^2 - y^2)^2 = 1 + 16y. \tag{12}$$

Solução. O formato de (12) sugere-nos imediatamente fatorações diversas utilizando produtos notáveis, todas sem grandes conclusões. Por outro lado, olhando sob a perspectiva do método das desigualdades, rapidamente vemos que o lado direito de (12), por ser o quadrado de um número, deve ser positivo ou nulo, assim, olhando para o lado direito de (12), devemos ter $y \geq 0$, obtemos, assim, a primeira desigualdade para y. Mais ainda, temos que $1 + 16y \geq 1$. Podemos então reescrever a seguinte desigualdade envolvendo (12),

$$(x^2 - y^2)^2 \geq 1 \quad \Rightarrow \quad x^2 - y^2 \geq 1 \quad \text{ou} \quad x^2 - y^2 \leq -1,$$

donde

$$x^2 \geq y^2 + 1 \quad \text{ou} \quad x^2 \leq y^2 - 1.$$

Como x e y são inteiros, dizer que $x^2 \geq y^2 + 1$, implica que $|x|$ é pelo menos uma unidade maior do que $|y|$, dessa maneira $|x| > |y| + 1$. Pensando de forma análoga, dizer que $x^2 \leq y^2 - 1$, implica que $|x|$ é pelo menos uma unidade menor do que $|y|$, donde $|x| \leq |y| - 1$. Elevando ao quadrado as duas desigualdades, ficaremos com

$$|x|^2 \geq (|y| + 1)^2 \quad \Rightarrow \quad |x|^2 \geq |y|^2 + 2|y| + 1 \quad \Rightarrow \quad |x|^2 - |y|^2 \geq 2|y| + 1, \tag{13}$$

e

$$|x|^2 \leq (|y| - 1)^2 \quad \Rightarrow \quad |x|^2 \leq |y|^2 - 2|y| + 1 \quad \Rightarrow \quad |y|^2 - |x|^2 \geq 2|y| - 1. \tag{14}$$

Elevando as últimas expressões do lado direito de (13) ou de (14), obtemos a seguinte desigualdade

$$(2y - 1)^2 \leq \left(|x|^2 - |y|^2\right)^2. \tag{15}$$

Combinando (15) com (12), obtemos

$$(2y - 1)^2 \leq 1 + 16y \quad \Rightarrow \quad 4y^2 - 4y + 1 \leq 1 + 16y \quad \Rightarrow \quad 4y^2 - 20y \leq 0 \quad \Rightarrow \quad 0 \leq y \leq 5. \tag{16}$$

Agora basta esgotar os casos.

Caso 1. $y = 0$ A equação (12) assume o seguinte formato

$$x^4 = 1 \quad \Rightarrow \quad x = -1 \text{ ou } x = 1,$$

obtemos portanto as soluções $(-1, 0)$ e $(1, 0)$.

Caso 2. $y = 1$ Nesse caso, teremos

$$(x^2 - 1)^2 = 17,$$

e portanto, x não será inteiro.

Caso 3. $y = 2$ Aqui, a equação (12) fica

$$(x^2 - 4)^2 = 33,$$

e, novamente, não temos soluções inteiras para x.

Caso 4. $y = 3$ Teremos

$$(x^2 - 9)^2 = 49 \quad \Rightarrow \quad x^2 - 9 = \pm 7,$$

portanto

$$x^2 = 2 \quad \text{ou} \quad x^2 = 16,$$

logo, as soluções são $(-4, 3)$ e $(4, 3)$.

Caso 5. $y = 4$ Aqui, a equação (12) fica

$$(x^2 - 16)^2 = 65,$$

e novamente não temos soluções inteiras para x.

Caso 6. $y = 5$ No último caso teremos

$$(x^2 - 25)^2 = 81 \quad \Rightarrow \quad x^2 - 25 = \pm 9,$$

portanto

$$x^2 = 16 \quad \text{ou} \quad x^2 = 34,$$

cujas soluções inteiras são $x = -4$ e $x = 4$. Assim, as soluções são $(-4, 5)$ e $(4, 5)$.

Obtemos as soluções $\{(-1, 0), (1, 0), (-4, 3), (4, 3), (-4, 5), (4, 5)\}$ que podem ser vistas, geometricamente, com a seguinte figura

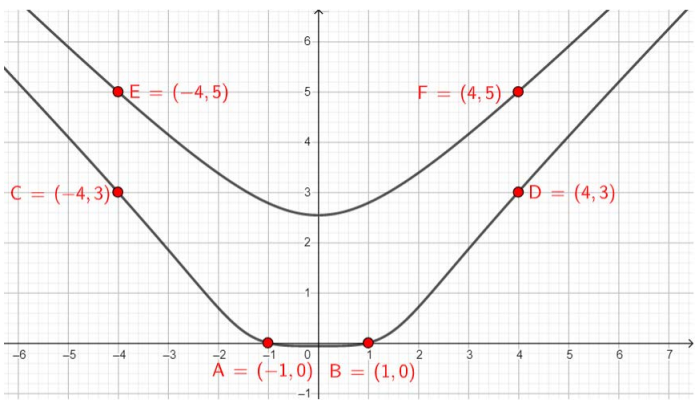


Figura 3: Pontos com coordenadas inteiras da curva implícita $(x^2 - y^2) = 1 + 16y$. Fonte: Autores.

■

4.3. Método da Parametrização

Veremos agora que há casos em que a equação diofantinas pode ser representada da seguinte maneira

$$f(x_1, x_2, ..., x_{n-1}, x_n) = 0,$$

e, nessa situação, as soluções podem ser escritas como equações paramétricas da forma

$$x_i = g_i(k_1, k_2, ..., k_{l-1}, k_l),\ i = 1, 2, ..., n-1, n,$$

com $g_i : \mathbb{Z}^n \to \mathbb{Z}$ são funções e $k_j \in \mathbb{Z}$, $j = 1, ..., l$. O tratamento desses casos, em geral, ocorre quando não há uma maneira explícita de encontrar todas as soluções, em particular, o método que explicitaremos garante-nos a existência de infinitas soluções para esses problemas.

Exemplo 11 (Torneio das Cidades, [2])**.** Prove que existem infinitas triplas de inteiros (x, y, z) tais que

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2. \tag{17}$$

Solução: Perceba, inicialmente, que o enunciado não nos pede para explicitar exatamente quais são essas soluções; mais ainda, por serem infinitas, certamente estamos em um caso de parametrização de soluções. Para darmos o primeiro passo, colocaremos alguma das variáveis em função de outra(s), de maneira que consigamos reduzir a quantidade de termos iniciais. Perceba que se $z = -y$, então

$$y^3 + z^3 = 0 \quad \text{e} \quad y^2 + z^2 = 2y^2. \tag{18}$$

Pondo (18) em (17), obtemos

$$x^3 = x^2 + 2y^2. \tag{19}$$

Novamente, para simplificar a expressão (19) acima, podemos considerar $y = kx$, com $k \in \mathbb{Z}$, e obtemos

$$x^3 = x^2 + 2(kx)^2 \quad \Rightarrow \quad x^3 = x^2(1 + 2k^2) \quad \Rightarrow \quad x = 0 \text{ ou } x = 2k^2 + 1. \tag{20}$$

O caso $x = 0$ torna-se trivial e pode ser desconsiderado. Portanto, triplas da forma $(x, y, z) = (g_1(k), g_2(k), g_3(k)) = (2k^2 + 1, 2k^3 + k, -2k^3 - k)$, com $k \in \mathbb{Z}$, satisfazem a equação. ■

Finalizaremos o método da parametrização com o clássico problema das ternas pitagóricas.

Mas antes vamos considerar o seguinte lema:

Lema 2. *Seja (x, y, z) uma Terna Pitagórica primitiva, isto é, $x^2 + y^2 = z^2$ com $x, y, z \in \mathbb{Z}$ primos entre si. Então x e y têm paridades distintas e z é ímpar.*

Demonstração. Primeiramente, note que não podemos ter x e y, ambos pares, já que, por hipótese, eles são primos entre si. Agora, sem perda de generalidade, podemos supor que y é ímpar. Assim, existe k_1 inteiro tal que $y = 2k_1 + 1$, logo

$$y^2 = 4k_1^2 + 4k_1 + 1 \equiv 1 \bmod 4.$$

Note que dado um inteiro par qualquer $p = 2k$, temos que

$$p^2 = 4k^2 \equiv 0 \bmod 4,$$

dessa forma, vemos que todo quadrado perfeito nos inteiros é congruente a 0 ou 1 módulo 4. Logo, x não pode ser ímpar, pois caso o fosse existiria k_2 inteiro tal que $x^2 = 4k_2^2 + 4k_2 + 1$, e, então, $z^2 = x^2 + y^2 \equiv 2 \bmod 4$, o que não pode ocorrer. Portanto x é par e, consequentemente, z é ímpar.

□

Exemplo 12 (Ternas Pitagóricas)**.** Encontre todas as soluções de inteiros positivos (x, y, z) tais que

$$x^2 + y^2 = z^2. \tag{21}$$

Solução. Certamente esse problema tem infinitas soluções. Note que $(3, 4, 5)$ é uma terna solução de (21), pois $3^2+4^2 = 9+16 = 25 = 5^2$. Dessa maneira, também serão soluções as ternas $(3k, 4k, 5k)$ com $k \in \mathbb{Z}$. A questão aqui não é apenas mostrar que (21) tem infinitas soluções, mas sim encontrar todas as soluções, o que torna este problema um pouco mais refinado.

Procedendo como no problema anterior, perceba que se $y = k_1 x$, onde k_1 é um inteiro, então o lado esquerdo de (21) torna-se mais simples, e ficamos com

$$x^2 + k_1^2 x^2 = z^2 \quad \Rightarrow \quad z^2 = x^2(k_1^2 + 1) \quad \Rightarrow \quad z = x\sqrt{k_1^2 + 1}.$$

Apesar de conseguirmos expressar y e z em função de x, o que permitiria uma parametrização da solução bastando tomar $x = k_2$, ainda devemos nos preocupar em explicitar valores de k_1 de maneira que $k_1^2 + 1$ seja um quadrado perfeito. Seguiremos, então, outra estratégia. Pelo Lema 2 podemos tomar y e z ímpares: além disso, $y \leq z$. Perceba que podemos reescrever (21) da seguinte maneira:

$$x^2 = z^2 - y^2 = (z + y)(z - y). \tag{22}$$

Como y e z são ímpares, $z + y$ e $z - y$ são pares. Sendo $mdc(y, z) = 1$, pelo Lema 1, temos que $mdc(y + z, z) = mdc(y + z - z, z) = 1$. Além disso, como $y + z$ é par, vale que $mdc(2z, z + y) = 2$ e novamente pelo Lema 1, notando que $z \geq y$, temos $mdc(2z, z + y) = mdc(2z - (z + y), z + y) = mdc(z - y, z + y) = 2$, e daí $mdc\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$. Por (22) temos que $(z-y)(z+y)$ é um quadrado perfeito, e $\frac{z-y}{2}$ e $\frac{z+y}{2}$ são primos entre si; daí, pelo Teorema Fundamental da Aritmética, concluímos que $\frac{z-y}{2}$ e $\frac{z+y}{2}$ são quadrados perfeitos. Considere $k_1, k_2 \in \mathbb{N}$ tais que

$$\frac{z+y}{2} = k_1^2 \quad \text{e} \quad \frac{z-y}{2} = k_2^2, \quad \text{com} \quad mdc(k_1, k_2) = 1. \tag{23}$$

Comparando (23) com (22) temos que $x = 2k_1k_2$. E, finalmente, isolando z e y em (23) concluímos que todas as soluções de (21) de inteiros positivos são da forma $(x, y, z) = (g_1(k_1, k_2), g_2(k_1, k_2), g_3(k_1, k_2)) = \left(2k_1k_2, k_1^2 - k_2^2, k_1^2 + k_2^2\right)$, em que $k_1 > k_2$ são inteiros positivos. ■

4.4. Utilizando Aritmética Modular

A aritmética modular é uma forte ferramenta quando tratamos de casos específicos, em particular, por permitirem simplificações. É possível, com as relações de congruência modular, verificar a existência de soluções de uma equação, sem precisar de fato resolvê-la. Por exemplo, se estamos trabalhando com quadrados perfeitos, uma boa ideia é usar congruência módulo 3, módulo 4 ou módulo 8, pois todo quadrado perfeito é congruente a 0 ou 1 módulo 3 ou módulo 4, e é congruente a 0, 1 ou 4 módulo 8; nos casos de cubos perfeitos a estratégia é usar congruência módulo 7, pois todo cubo perfeito é congruente a 0, 1 ou 6 módulo 7.

Exemplo 13 (Olímpia Matemática Húngara, [2])**.** Mostre que a equação

$$(x+1)^2 + (x+2)^2 + \ldots + (x+99)^2 = y^z \tag{24}$$

não possui solução com x, y, z inteiros tais que $z > 1$.

Solução. Já sabemos, nesse ponto, que fatorações podem ser ferramentas para obtenção da solução ou simplificação de cálculos. Dados $a, b \in \mathbb{R}$, temos que $(a+b)^2 = a^2 + 2ab + b^2$.

Além disso, destacamos as fórmulas fechadas para a soma dos n primeiros números naturais e soma dos quadrados dos n primeiros inteiros positivos.

$$\sum_{i=1}^{n} i = 1 + 2 + \ldots + (n-1) + n = \frac{n(n+1)}{2}, \tag{25}$$

e

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \ldots + (n-1)^2 + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{26}$$

Salientamos que tais fórmulas podem ser rapidamente provadas pelo Princípio de Indução Finita. Este resultado pode ser encontrado em [2] ou [10]. Por meio destes resultados, perceba que

$$\begin{aligned}
y^z &= (x+1)^2 + (x+2)^2 + \ldots + (x+98)^2 + (x+99)^2 \\
&= (x^2 + 2x + 1) + (x^2 + 2\cdot 2x + 2^2) + \ldots + (x^2 + 2\cdot 98x + 98^2) + (x^2 + 2\cdot 99x + 99^2) \\
&= (x^2 + 2x + 1) + (x^2 + 2x\cdot 2 + 2^2) + \ldots + (x^2 + 2x\cdot 98 + 98^2) + (x^2 + 2x\cdot 99 + 99^2) \\
&= 99x^2 + 2x(1 + 2 + \ldots + 98 + 99) + (1 + 2^2 + \ldots + 98^2 + 99^2) \\
&= 99x^2 + 2x(1 + 2 + \ldots + 98 + 99) + (1 + 2^2 + \ldots + 98^2 + 99^2) \\
&= 99x^2 + 2x\frac{99\cdot 100}{2} + \frac{99\cdot 100\cdot 199}{6} = 99x^2 + 99\cdot 100x + 33\cdot 50\cdot 199 \\
&= 33(3x^2 + 300x + 50\cdot 199) = 3\cdot 11(3x^2 + 300x + 50\cdot 199).
\end{aligned}$$

Como x, y, z são inteiros, então y^z é uma potência inteira de y. Como 3 divide y^z, então devemos ter $3|y$, o que implica $3^2|y^2$. Mas note que $z \geq 2$, portanto $3^2|y^z$. Mas isso é falso, pois $3x^2 + 300x + 50\cdot 199$ não é divisível por 3, uma vez que $3|3x^2 + 300x$, mas $3 \nmid 50\cdot 199$. Provamos assim que não existem inteiros x, y, z com $z > 1$ satisfazendo (24). ■

Um resultado comumente utilizado em simplificações em cálculos de congruência modular é o seguinte

Teorema 4 (Pequeno Teorema de Fermat)**.** *Dados $a, p \in \mathbb{Z}$ com p primo, têm-se que $a^p \equiv a \bmod p$. Em particular, se $mdc(a,p) = 1$, então $a^{p-1} \equiv 1 \bmod p$.*

Demonstração. Ver [7].

Em posse desse resultado, considere.

Exemplo 14 (OBM, 2009, 3ª Fase, Nível 2, Problema 3, [8])**.** Prove que não existem inteiros positivos x e y tais que $x^3 + y^3 = 2^{2009}$.

Solução. Pelos comentários no início da questão, como estamos trabalhando com termos elevados ao cubo, optaremos por trabalhar com congruência módulo 7. Sabemos que para todo número inteiro x, temos que x^3 só pode ser congruente a 0, 1 ou 6 módulo 7, e o mesmo ocorre com y^3. Assim, fazendo uma combinação dessas possibilidades, temos que $x^3 + y^3$ deve ser congruente a 0, 1, 2, 5 ou 6 módulo 7. Mas pelo Pequeno Teorema de Fermat, $2^7 \equiv 2 \mod 7$ ou $2^6 \equiv 1 \mod 7$, donde

$$2^{2009} \equiv 2^{6\cdot 334+5} = (2^6)^{334} \cdot 2^5 \equiv (1)^{334} \cdot 2^5 \equiv 32 \equiv 4 \mod 7.$$

Isso prova que não existem x e y inteiros positivos tais que $x^3 + y^3 = 2^{2009}$. ■

5. Conclusão

Neste trabalho, são discutidos alguns resultados e técnicas de soluções envolvendo equações diofantinas lineares e não lineares. Em relação às lineares, fizemos uma revisão de conceitos importantes como divisão euclidiana, máximo divisor comum e congruência modular, a fim de encontrarmos soluções para equações com duas variáveis. Por outro lado, fizemos o tratamento do caso não linear por meio de quatro abordagens bem específicas, divididas por métodos que utilizam fatorações; desigualdades; parametrizações e aritmética modular. Pudemos observar que o método das fatorações é uma ferramenta muito útil nas simplificações das expressões algébricas contidas nos problemas. O método das desigualdades é eficiente, quando conseguimos determinar um intervalo em que a(s) variável(is) estão limitada(s), de maneira que podemos esgotar os casos ao estudar todas as possibilidades. Já o método das parametrizações é utilizado na busca por soluções de equações com infinitas soluções. E, por fim, o método que utiliza aritmética modular está muito presente nas questões que lidam com restos de divisões ou para determinar a existência de solução em alguns problemas, por meio de resultados sobre congruência módulo já conhecidos.

Referências

[1] ALFONSÍN, Jorge L. Ramírez *et al.* The diophantine Frobenius problem. Oxford University Press on Demand, 2005.

[2] ANDREESCU, Titu *et al.* An introduction to Diophantine equations: a problem-based approach. New York: Birkhäuser, 2010.

[3] ANJOS, A. A. Equações Diofantinas: Sequência Didática e o Método da Descida Infinita de Fermat. Mestrado Profissional em Rede Nacional - Centro de Ciências e Tecnologia, Universidade Federal do Ceará, Fortaleza, 2015.

[4] CAMPOS, Giseli Duardo Maciano. Equações diofantinas lineares. 70 f. Dissertação Profmat (Mestrado Profissional em Matemática) - Universidade Federal de Mato Grosso, Cuiabá, 2013.

[5] CHAVES, A. P. A. Álgebra e teoria dos números para olimpíadas. *Professor de Matemática Online (PMO)*, v. 7, nº 1, p. 66-76, 2019.

[6] DOS SANTOS, Jhonata Avelar et al.Explorando os teoremas de Menelaus e Ceva em questoes de olimpıadas de matemática. *Professor de Matemática Online (PMO)*, v. 9, n° 3, 2021.

[7] NETO, Altino da Silva. Convite às Equações Diofantinas: uma abordagem para a educação básica. Dissertação Profmat (Mestrado Profissional em Matemática) — Universidade Federal de Roraima, Boa Vista, 2016. Disponível em ⟨https://sca.profmat-sbm.org.br/sca_v2/get_tcc3.php?cpf=

57831246215&d=20210421133048&h=52cfdaf6160ca690145f62a1c045fad6649ec641⟩. Acesso em 11 Mar. de 2021.

[8] Olimpíada Brasileira de Matemática. Disponível em: ⟨https://www.obm.org.br/⟩. Acesso em 11 Mar. de 2021.

[9] Olimpíada Brasileira de Matemática das Escolas Públicas. Disponível em: ⟨http://www.obmep.org.br⟩. Acesso em 11 Mar. de 2021.

[10] Polos Olímpicos de Treinamento Intensivo. Disponível em: ⟨https://poti.impa.br/⟩. Acesso em 21 Fev. de 2021.

[11] Portal da Obmep - Aritmética dos Restos - Caderno de Exercícios - Aritmética Modular. Disponível em: ⟨https://cdnportaldaobmep.impa.br/portaldaobmep/uploads/material/5oeoy5b8w0gso.pdf⟩. Acesso em 11 Mar. de 2021.

[12] RIBEIRO, Rildo. *Equações diofantinas: uma abordagem para o ensino médio*. Dissertação PROFMAT (Mestrado Profissional em Matemática) — Universidade de Brasília, Brasília, 2014.

[13] SERRÃO, Marcelo Miranda; BRANDEMBERG, João Cláudio. *Utilizando problemas da história antiga da Matemática como estratégia para o ensino de equações no 9º ano da escola básica*. X Seminário Nacional de História da Matemática. Campinas - São Paulo, 2013.

[14] SINGH, Simon. *O último teorema de Fermat: A história do enigma que confundiu as mais brilhantes mentes do mundo durante 358 anos*. Editora Best Seller, 2014.

Érick C. A. do Nascimento
Universidade Federal Rural de Pernambuco
Departamento de Matemática (DM-UFRPE)
Recife/PE
<erick.alves@ufrpe.br>

Thiago Yukio Tanaka
Universidade Federal Rural de Pernambuco
Departamento de Matemática (DM-UFRPE)
Recife/PE
<thiago.tanaka@ufrpe.br>

Barbara Costa da Silva
Universidade Federal Rural de Pernambuco
Departamento de Matemática (DM-UFRPE)
Recife/PE
<barbara.costasilva@ufrpe.br>

Recebido: 10/09/2021
Publicado: 13/07/2022