UFRRJ
Instituto de Ciências Exatas
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Dissertação

Equações Diofantinas Lineares: uma proposta para as séries finais do ensino fundamental

André Fellipe Franco Pereira de Oliveira

2018

Universidade Federal Rural do Rio de Janeiro
Instituto de Ciências Exatas
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Equações Diofantinas Lineares: uma proposta para as séries finais do ensino fundamental

André Fellipe Franco Pereira de Oliveira

Sob a orientação do professor
Cláudio Cesar Saccomori Júnior

Dissertação submetida como requisito parcial para obtenção do grau de Mestre, no curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Área de Concentração em Matemática.

Seropédica - RJ
Abril 2018

Universidade Federal Rural do Rio de Janeiro
Biblioteca Central / Seção de Processamento Técnico

Ficha catalográfica elaborada
com os dados fornecidos pelo(a) autor(a)

O48e

Oliveira, André Fellipe Franco Pereira de, 1988-
Equações Diofantinas Lineares: uma proposta para as séries finais do ensino fundamental / André Fellipe Franco Pereira de Oliveira. - 2018.
86 f.: il.

Orientador: Cláudio Cesar Saccomori Jr.
Dissertação(Mestrado). -- Universidade Federal Rural do Rio de Janeiro, Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional, 2018.

1. Equações Diofantinas Lineares. 2. Máximo Divisor Comum. 3. Algoritmo de Euclides. 4. Aritmética Modular. I. Saccomori Jr, Cláudio Cesar, 1977-, orient. II Universidade Federal Rural do Rio de Janeiro. Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional III. Título.

Universidade Federal Rural do Rio de Janeiro
Instituto de Ciências Exatas
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

André Fellipe Franco Pereira de Oliveira

Dissertação submetida como requisito parcial para obtenção do grau de Mestre, no curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Área de Concentração em Matemática.

DISSERTAÇÃO APROVADA EM 25/04/2018.

Cláudio Cesar Saccomori Júnior Dr. UFRRJ
Orientador

André Luiz Martins Pereira. Dr. UFRRJ

Cleber Haubrichs dos Santos Dr. IFRJ

Para minha esposa,
Kamila.

Agradecimentos

Primeiramente, agradeço à Deus por me proteger e guiar o meu caminho durante esta jornada.

À minha esposa, Kamila Costa, por ter me apoiado em todos os momentos e ficar ao meu lado nas horas que eu mais precisava durante o período de elaboração deste trabalho. Agradeço todo carinho, atenção e tempo doados para que realizasse minha pesquisa. Sem esse conjunto de atitudes nada disso seria possível, pois tais ações foram os componentes essenciais para a consumação deste trabalho.

Aos meus pais, Ivo e Olivia, a minha irmã, Rafaella, a minha avó, Regina e a todos os meus familiares que sempre estiveram ao meu lado me concedendo apoio e carinho para que eu obtivesse êxito em todos os projetos em minha vida.

Ao meu orientador, prof. Dr. Cláudio Cesar Saccomori Júnior, por acreditar em meu potencial e, também, pelo convívio, pelo incentivo, pela compreensão e paciência na orientação que tornaram possível a execução desta dissertação. Quero manifestar o meu reconhecimento e admiração pela sua competência profissional.

Aos professores, André Luiz Martins Pereira e Cleber Haubrichs dos Santos, por participarem de minha banca examinadora.

Aos docentes que me conduziram durante a Pós-Gradução, pelas trocas de conhecimento e experiências que foram tão importantes na minha vida acadêmica e pessoal.

Agradeço à CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pela concessão da bolsa durante todo o período de realização deste mestrado.

Aos meus amigos do curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Osni Novaes, Gilmar dos Santos, Anderson Nishimura, Felipe Quirino, Hamilcar Pereira, Rafael Racca, Rodrigo Macedo, Tiago Loyo e Valdinei da Silva que permaneceram nesta Pós-Graduação e, também aos amigos, Angela Carla, Guilherme Nascimento, José Carlos, Marcelo Lima e Ramiro Marins, que tomaram outros caminhos, mas se fizeram presentes na minha vida pessoal e acadêmica em inúmeras ocasiões de estudo e lazer. Torço pelo sucesso de todos.

Agradeço a todos que, mesmo não estando citados aqui, tanto colaboraram para a conclusão desta etapa em minha vida.

Resumo

OLIVEIRA, A. F. F. P. **Equações Diofantinas Lineares: uma proposta para as séries finais do ensino fundamental.** Seropédica, 2018. Dissertação de Mestrado (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT). Instituto de Ciências Exatas, Universidade Federal Rural do Rio de Janeiro.

O presente trabalho tem como objetivo principal apresentar uma proposta de sequência didática sobre Equações Diofantinas Lineares para aplicação nas séries finais do ensino fundamental da educação básica. Almeja-se, também, que, após a aplicação de algumas aulas sobre o tema, os alunos adquiram a capacidade de identificar situações-problemas que possam ser modelados e, em seguida, resolvidos por meio dessas equações. Para isso, serão abordados tópicos essenciais para a compreensão dos conteúdos envolvidos na elaboração da sequência didática, tais como: números inteiros, divisibilidade, divisão euclidiana, máximo divisor comum, algoritmo de Euclides e aritmética modular. Desta forma, tal trabalho se justifica uma vez que, em processos seletivos de concursos militares, Colégio Naval, Colégio Militar e EPCAr, e em provas da Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP, aparecem questões que podem ser solucionadas com esta ferramenta e, também, pelo tema ser possível de assimilação pelos alunos das séries finais do ensino fundamental, pois os mesmos precisam ter apenas conhecimentos básicos de matemática. Além disso, pretende-se levar o aluno a perceber que a matemática é importante para que ele compreenda e saiba solucionar situações-problema vivenciadas em seu cotidiano.

PALAVRAS-CHAVE: Equações Diofantinas Lineares. Máximo Divisor Comum. Algoritmo de Euclides. Aritmética Modular.

Abstract

OLIVEIRA, A. F. F. P.. **Linear Diophantine Equations: a proposal for the final years of middle school.** Seropédica, 2018. Master's Dissertation (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT). Instituto de Ciências Exatas, Universidade Federal Rural do Rio de Janeiro.

The aim of this dissertation is to present a proposal of a didactic sequence for Linear Diophantine Equations to be applied at the final years of middle school. It is also expected that after some classes about the subject the students will be able to identify real word problems that can be modeled and solved through Linear Diophantine Equations. In order to achieve this objective essential topics for the understanding of the contents involved in the elaboration of the didactic sequence, such as: integers, divisibility, Euclidean division, greatest common divisor, Euclid's algorithm and modular arithmetic will be reviewed. Thus, this work is justified since in some selective processes of military competitions, Naval College, Military College and EPCAr, and also in the tests of the Brazilian Mathematics Olympiad of Public Schools - OBMEP, have some questions that can be solved with this tool, and due the fact it is a possible topic for assimilation by the students at the final years of middle schools since they only need basic knowledge of mathematics. In addition, it is intended to lead the student to realize that mathematics is important so that he understands and knows how to solve problem situations experienced in his daily life.

KEYWORDS: Linear Diophantine Equations. Greatest Common Divisor. Euclid's Algorithm. Modular Arithmetic

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Dentre as orientações educacionais contidas nos Parâmetros Curriculares Nacionais (PCN's), destacamos aquelas que fomentam a exploração do ensino de matemática em situações do dia a dia como ferramenta de desenvolvimento das competências e habilidades do aluno. Uma delas, segundo [4, p.40] é:

> A resolução de problemas, na perspectiva indicada pelos educadores matemáticos, possibilita aos alunos mobilizar conhecimentos e desenvolver a capacidade para gerenciar as informações que estão a seu alcance. Assim, os alunos terão oportunidade de ampliar seus conhecimentos acerca de conceitos e procedimentos matemáticos bem como de ampliar a visão que têm dos problemas, da Matemática, do mundo em geral e desenvolver sua autoconfiança.

Sendo assim, situações do cotidiano, por exemplo, "Deseja-se sacar uma quantia de R\$100,00 em um caixa eletrônico o qual possui dois tipos de notas disponíveis: R\$10,00 e R\$20,00. Quantas notas de cada tipo você poderá receber?", possibilitam ao aluno, em geral, elaborar um raciocínio próprio de solução e, além disso, comparar sua solução com as diferentes soluções dos outros alunos, engrandecendo suas habilidades cognitivas e o processo ensino-aprendizagem.

Pela álgebra, podemos modelar a situação apresentada acima pela equação $10x + 20y = 100$, onde x representa a quantidade de notas de R\$10,00 e y, a de notas de R\$20,00. Tal situação nos leva a alguns questionamentos: Será que é possível resolver uma equação deste tipo? Se houver solução, está é única ou existem várias? As repostas sobre esses questionamentos se dão no estudo sobre este tipo de equações, as quais são denominadas de Equações Diofantinas Lineares em homenagem a Diofanto de Alexandria (aprox. 300d.C.), grande matemático e filósofo grego, considerado por muitos estudiosos como o "pai da Álgebra", devido a notação que ele utilizava ser considerada o primeiro passo da álgebra simbólica [8].

Através de pesquisa feita na Base Nacional Comum Curricular [3] e observações em livros didáticos aprovados no Programa Nacional do Livro Didático (PNLD) [5], notou-se que o tema "Equações Diofantinas Lineares" não é abordado em nenhum dos segmentos da educação básica. Em particular, tal tema não é desenvolvido no ensino fundamental como uma aplicação do máximo divisor comum de dois números inteiros. Portanto, o presente trabalho tem como questão norteadora: como introduzir o tema "Equações Diofantinas Lineares com duas incógnitas" nas séries finais do ensino fundamental?

Passaremos agora a descrever sucintamente nosso trabalho. No Capítulo 1 apresentamos resultados prévios que serão essenciais para uma melhor compreensão do leitor nos capítulos posteriores, tais como: divisibilidade, divisão euclidiana, máximo divisor comum e aritmética modular.

No Capítulo 2 apresentamos as teorias das equações diofantinas lineares de duas incógnitas e dois métodos de resolução de tais equações: método algébrico e método aritmético modular.

No Capítulo 3 apresentamos as orientações da metodologia de pesquisa utilizada - Engenharia Didática - e descrevemos, comentamos e analisamos os dados da pesquisa obtidos a partir da experimentação da sequência didática em turmas do 9° ano do ensino fundamental.

CAPÍTULO 1

NOÇÕES PRELIMINARES

O presente capítulo tem como objetivo expor alguns resultados importantes de Aritmética para que o leitor tenha condições de absorver o conteúdo abordado nos demais capítulos. Note que apresentaremos aqui somente os resultados necessários para a compreensão do objetivo principal deste estudo: as Equações Diofantinas Lineares. Sendo assim, o texto não é auto-contido. Tais conceitos são baseados em Hefez [9], Lacerda [10] e Domingues [7].

1.1 Divisibilidade

Sejam a e b dois números inteiros. Diz-se que a *divide* b, escrevendo $a \mid b$, se existir um número inteiro c tal que $b = a \cdot c$. Nesse caso, diz-se também que a é *divisor* de b, que b é *divisível* por a ou ainda que b é *múltiplo* de a. Por exemplo, $4 \mid 24$ e $5 \mid 45$, pois $24 = 4 \cdot 6$ e $45 = 5 \cdot 9$.

Agora, quando não existe nenhum número inteiro c tal que $b = a \cdot c$, diz-se que a *não divide* b. Utilizaremos, nesse caso, $a \nmid b$. Por exemplo, $3 \nmid 20$, pois não existe nenhum número inteiro c tal que $20 = 3 \cdot c$.

Proposição 1.1 *Dados os números inteiros a, b e c, temos que*

1. $1 \mid a$, $a \mid a$ *e* $a \mid 0$.
2. $0 \mid a$ *se, e somente se,* $a = 0$.
3. $a \mid b$ *se, e somente se,* $|a| \mid |b|$.
4. *se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

Demonstração: *1.* Decorre imediatamente das igualdades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = a \cdot 0$.
2. Suponha que $0 \mid a$. Portanto, existe c inteiro tal que $a = 0 \cdot c$. Como $c \cdot 0 = 0$, para

todo inteiro c, então $a = 0$. Para a recíproca basta notar que $0 \mid 0$, o que foi provado no item anterior.

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

$$a \mid b \Longrightarrow b = a \cdot c \Longrightarrow |b| = |a| \cdot |c| \Longrightarrow |a| \mid |b|,$$

como queríamos demonstrar.

4. Suponha que $a \mid b$ e $b \mid c$. Portanto, existem f e g inteiros tais que $b = f \cdot a$ e $c = g \cdot b$. Substituindo o valor de b da primeira equação na segunda, obtemos

$$c = g \cdot b = g(f \cdot a) = (g \cdot f)a,$$

o que nos mostra que $a \mid c$. ■

Por exemplo, como $3 \mid 21$ e $21 \mid 189$, então $3 \mid 189$.

Suponha que $a \mid b$ e que $a \neq 0$. Seja c um número inteiro tal que $b = a \cdot c$. O número c, univocamente determinado, é chamado de *quociente* de b por a e denotado por $c = \dfrac{b}{a}$. Note que $\dfrac{b}{a}$ só está definido quando $a \neq 0$ e $a \mid b$.

Proposição 1.2 *Dados os números inteiros a, b, c e d, temos que se $a \mid b$ e $c \mid d$, então $ac \mid bd$.*

Demonstração: Com efeito, se $a \mid b$ e $c \mid d$, então existem f e g inteiros tais que $b = f \cdot a$ e $d = g \cdot c$. Sendo assim, temos que $bd = (f \cdot a)(g \cdot c) = (f \cdot g)(a \cdot c)$. Logo, $ac \mid bd$, como queríamos provar. ■

Por exemplo, como $4 \mid 24$ e $3 \mid 21$, então $12 = 3 \cdot 4 \mid 24 \cdot 21 = 504$. Em particular, se $a \mid b$, então $ac \mid bc$, para todo c inteiro.

Proposição 1.3 *Sejam números inteiros a, b e c, tais que $a \mid (b \pm c)$. Então $a \mid b$ se, e somente se, $a \mid c$.*

Demonstração: Para tal, suponha que $a \mid (b + c)$. Portanto, existe f inteiro tal que $b + c = af$. Se $a \mid b$, então existe g inteiro tal que $b = ag$. Desta forma, $b + c = ag + c = af$, donde segue-se que $c = (f - g)a$. Logo, $a \mid c$. Reciprocamente, se $a \mid c$, então existe h inteiro tal que $c = ah$. Desta forma, $b + c = b + ah = af$, donde segue-se que $b = (f - h)a$. Logo, $a \mid b$. De forma análoga ocorre para $a \mid (b - c)$. ■

Proposição 1.4 *Sejam os números inteiros a, b e c, tais que $a \mid b$ e $a \mid c$. Então, para todos os números inteiros x e y, temos que $a \mid (xb + yc)$.*

Demonstração: Suponha que $a \mid b$ e $a \mid c$. Portanto, existem f e g inteiros tais que $b = af$ e $c = ag$. Sendo assim,

$$xb + yc = x(af) + y(ag) = (xf + yg)a,$$

o que prova o resultado. ∎

Por exemplo, como $3 \mid 21$ e $3 \mid 189$, então $3 \mid (21 \cdot 4 + 189 \cdot 5)$.

1.2 Divisão Euclidiana

Teorema 1.5 *Dados dois inteiros a e b, com $b \neq 0$, então existem dois únicos inteiros q e r tais que*

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

Demonstração: Seja o conjunto $S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.
Existência: Pela propriedade Arquimediana, existe n inteiro tal que $n(-b) > -a$. Portanto, $a - nb > 0$, o que nos mostra que S é não vazio. Note que o conjunto S é limitado inferiormente por 0. Sendo assim, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos que $r = a - bq$. Vamos demonstrar que $r < |b|$. Suponha, por absurdo, que $r \geq |b|$. Desta forma, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$. Portanto, $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$. Logo, $a = bq + r$, com $0 \leq r < |b|$, o que prova a existência de q e r.
Unicidade: Tomemos $r_1, r_2 \in S$, com $r_1 \neq r_2$. Sem perda de generalidade, considere $r_2 > r_1$. Note que a diferença $r_2 - r_1$ é um múltiplo de b e, assim, essa diferença é no mínimo igual a $|b|$. Portanto, se $r_1 = a - bq_1$ e $r_2 = a - bq_2$, com $r_1 < r_2 < |b|$, então tem-se que $r_2 - r_1 \geq |b|$, implica que $r_2 \geq r_1 + |b| \geq |b|$. Mas isso contradiz o fato de $r_2 < |b|$. Logo, $r_1 = r_2$. Desta forma, segue-se que $a - bq_1 = a - bq_2$, o que implica que $q_1 = q_2$. ∎

Os números inteiros q e r, referenciados no teorema acima, são chamados de *quociente* e *resto*, respectivamente, da divisão de a por b. Por exemplo, o quociente e o resto da divisão de 23 por 4 são $q = 5$ e $r = 3$ e o quociente e o resto da divisão de -23 por 4 são $q = -6$ e $r = 1$.

1.3 Máximo Divisor Comum

Diz-se que um número inteiro d é um *divisor comum* de a e b inteiros, se d divide a e b ao mesmo tempo. Por exemplo, os números $\pm 1, \pm 2, \pm 4$ e ± 8 são os divisores comuns de 16 e 40.

Diz-se que um número inteiro $d \geq 0$ é um *máximo divisor comum (mdc)* de a e b, se satisfaz as condições:

1. $d \mid a$ e $d \mid b$;

2. se $c \mid a$ e $c \mid b$, então $c \leq d$.

Note que o mdc entre dois inteiros a e b sempre existe, pois o conjunto de divisores positivos de a e b é não-vazio, uma vez que 1 divide tanto a quanto b e limitado superiormente, pois $mdc(a,b) \leq min\{|a|,|b|\}$ e é único, pois, caso contrário, existiriam os inteiros d e f tais que $mdc(a,b) = d$ e $mdc(a,b) = f$. Pela definição, como $f \mid a$, $f \mid b$ e $mdc(a,b) = d$, então $f \leq d$. Da mesma forma, como $d \mid a$, $d \mid b$ e $mdc(a,b) = f$, então $d \leq f$. Logo, $d = f$. Por exemplo, o $mdc(16,40)$ é 8.

Lema 1.6 *Sejam a e b inteiros, com $b \neq 0$, e r o resto da divisão euclidiana de a por b. Então, $mdc(a,b) = mdc(b,r)$.*

Demonstração: Para tal, como r é o resto da divisão euclidiana de a por b, então tem-se que $a = bq + r$ e, consequentemente, $r = a - bq$. Seja c um número inteiro tal que $c \mid a$ e $c \mid b$. Sendo assim, pela proposição 1.4, tem-se que $c \mid r$. Portanto, c é um divisor comum de b e r. Reciprocamente, como $a = bq + r$, segue-se que todo divisor comum de b e r também é divisor de a. Portanto, o conjunto dos divisores comuns de a e de b é igual ao conjunto dos divisores comuns de b e de r. Logo, $mdc(a,b) = mdc(b,r)$. ■

Teorema 1.7 (Algoritmo de Euclides) *Sejam a e b inteiros, com $a \geq b > 0$. Se o algoritmo da divisão euclidiana for aplicado sucessivamente, segue, do Lema 1.6, que o último resto não nulo r_n, satisfaz $mdc(a,b) = r_n$, com $n \in \mathbb{N}$.*

Demonstração: Usando sucessivamente o algoritmo da divisão, obtem-se a sequência de igualdades,

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

$$r_2 = r_3q_4 + r_4, \quad 0 \leq r_4 < r_3$$

$$\cdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1}, \quad r_{n+1} = 0.$$

Ilustrando essas divisões sucessivas, tem-se a seguinte tabela:

	q_1	q_2	q_3	q_4	...		q_n	q_{n+1}
a	b	r_1	r_2	r_3	...	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4		...	r_n	r_{n+1}	

.

Sendo assim, como $r_1, r_2, r_3, ..., r_{n-1}, r_n$ são inteiros positivos tais que $b > r_1 > r_2 > r_3 > ... > r_{n-1} > r_n$ e existem apenas $b - 1$ inteiros positivos menores que b, então necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, ou seja, $r_n \mid r_{n-1}$. Logo, como $r_n \mid r_{n-1}$, então temos que $mdc(r_{n-1}, r_n) = r_n$, o que implica que $mdc(a, b) = r_n$. ■

Exemplo 1.3.8 Determinemos o *mdc* de 400 e 255. Para tal, pelo Algoritmo de Euclides, temos

	1	1	1	3	7
400	255	145	110	35	5
145	110	35	5	0	

.

Logo, $mdc(400, 255) = 5$. □

Teorema 1.9 (Teorema de Bèzout) *Dados os inteiros a e b, não ambos nulos, tem-se que o $mdc(a, b) = d$ pode ser escrito como uma combinação linear inteira dos mesmos, ou seja, existem m_0 e n_0 inteiros tais que $d = m_0a + n_0b$.*

Demonstração: Considere o conjunto $C_{a,b} = \{am + bn; m, n \in \mathbb{Z}\}$. Este conjunto de inteiros inclui valores positivos e negativos e, além disso, tomando $m = 0$ e $n = 0$, vemos que $C_{a,b}$ também contém o zero.

Pelo Princípio da Boa Ordenação, podemos escolher m_0 e n_0 tais que $c = am_0 + bn_0$ seja o menor número inteiro positivo contido no conjunto $C_{a,b}$. Agora, mostraremos que $c \mid a$ e $c \mid b$. Provaremos que $c \mid a$ e o outro segue analogamente. Para tal, vamos supor, por absurdo, que $c \nmid a$. Sendo assim, como $c \nmid a$, existem inteiros q e r tais que $a = cq + r$ com $0 < r < c$. Portanto,

$$r = a - cq = a - (am_0 + bn_0)q = a(1 - qm_0) + b(-qn_0)$$

está no conjunto $C_{a,b}$, o que contradiz a hipótese de c ser o menor elemento positivo contido em $C_{a,b}$. Logo, $c \mid a$.

Agora, só resta provar que $c = d$. De fato, como $mdc(a, b) = d$, podemos escrever $a = da_1$, $b = db_1$ e

$$c = am_0 + bn_0 = da_1m_0 + db_1n_0 = d(a_1m_0 + b_1n_0).$$

Sendo assim, $d \mid c$. Portanto, como c e d são positivos e $d \mid c$ então $d \leq c$. Note que $d < c$ é impossível pois $d = mdc(a,b)$. Logo, $d = c = am_0 + bn_0$ como queríamos demonstrar. ∎

Para se determinar os inteiros m e n tais que $mdc(a,b) = am + bn$, existe um dispositivo prático, chamado algoritmo estendido de Euclides, que facilita o cálculo. Tal algoritmo que será apresentado é baseado em Coutinho [6]. Calculando o máximo divisor comum entre a e b, utilizando as divisões sucessivas, obtemos

$$a = bq_1 + r_1 \text{ e } r_1 = ax_1 + by_1$$

$$b = r_1q_2 + r_2 \text{ e } r_2 = ax_2 + by_2$$

$$r_1 = r_2q_3 + r_3 \text{ e } r_3 = ax_3 + by_3$$

$$r_2 = r_3q_4 + r_4 \text{ e } r_4 = ax_4 + by_4$$

$$\ldots \quad \text{e} \quad \ldots$$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \text{ e } r_{n-1} = ax_{n-1} + by_{n-1}$$

$$r_{n-2} = r_{n-1}q_n \text{ e } r_n = 0,$$

onde $x_1, ..., x_{n-1}$ e $y_1, ..., y_{n-1}$ são inteiros a determinar. Ilustrando essas divisões sucessivas, tem-se a seguinte tabela:

$$\begin{array}{cccc}
restos & quocientes & x & y \\
a & * & x_{-1} & y_{-1} \\
b & * & x_0 & y_0 \\
r_1 & q_1 & x_1 & y_1 \\
r_2 & q_2 & x_2 & y_2 \\
\ldots & \ldots & \ldots & \ldots \\
r_{n-2} & q_{n-2} & x_{n-2} & y_{n-2} \\
r_{n-1} & q_{n-1} & x_{n-1} & y_{n-1}
\end{array}.$$

Suponha que a tabela esteja preenchida até $(i-1)$-ésima linha. Começamos a preencher a i-ésima linha dividindo r_{i-2} por r_{i-1} para determinar q_i, de forma que $r_{i-2} = r_{i-1}q_i + r_i$ e $0 \leq r_i < r_{i-1}$. Portanto,

$$r_i = r_{i-2} - r_{i-1}q_i$$

. Como, $r_{i-2} = ax_{i-2} + by_{i-2}$ e $r_{i-1} = ax_{i-1} + by_{i-1}$, obtemos

$$r_i = (ax_{i-2} + by_{i-2}) - (ax_{i-1} + by_{i-1})q_i = a(x_{i-2} - q_ix_{i-1}) + b(y_{i-2} - q_iy_{i-1}).$$

Logo, $x_i = x_{i-2} - q_ix_{i-1}$ e $y_i = y_{i-2} - q_iy_{i-1}$. Note que, para calcular x_i e y_i, usamos apenas os valores das linhas $i-1$ e $i-2$, além do quociente q_i. Temos assim um processo recursivo. Para dar início ao processo recursivo iremos determinar os valores de x e y das duas primeiras linhas da tabela. Sendo assim, temos que $a = ax_{-1} + by_{-1}$ e $b = ax_0 + by_0$, o que nos sugere escolher $x_{-1} = 1$, $y_{-1} = 0$, $x_0 = 0$ e $y_0 = 1$ e assim podemos dar início à recursão. Tendo utilizado o algoritmo de Euclides e determinado que o mdc corresponde ao resto r_{n-1}, obtemos $mdc(a, b) = ax_{n-1} + by_{n-1}$, ou seja, $m = x_{n-1}$ e $n = y_{n-1}$.

Exemplo 1.3.10 Determine o mdc de 665 e 504 e, em seguida, escreva o mdc como uma combinação linear dos mesmos.
Para tal, pelo Algoritmo de Euclides, temos

	1	3	7	1	2
665	504	161	21	14	7
161	21	14	7	0	

Portanto, $mdc(665, 504) = 7$. Sendo assim, pelo Teorema de Bézout, temos que existem m e n inteiros tais que $665m + 504n = 7$. Pelo algoritmo estendido de Euclides, temos

$$\begin{array}{cccc}
restos & quocientes & x & y \\
655 & * & 1 & 0 \\
504 & * & 0 & 1 \\
161 & 1 & 1 - 1 \cdot 0 = 1 & 0 - 1 \cdot 1 = -1 \\
21 & 3 & 0 - 3 \cdot 1 = -3 & 1 - 3 \cdot (-1) = 4 \\
14 & 7 & 1 - 7 \cdot (-3) = 22 & -1 - 7 \cdot 4 = -29 \\
7 & 1 & -3 - 1 \cdot 22 = -25 & 4 - 1 \cdot (-29) = 33
\end{array}.$$

Logo, $m = -25$ e $n = 33$ e, consequentemente, $665(-25) + 504(33) = 7$. □

Corolário 1.11 *Quaisquer que sejam os inteiros a e b, não ambos nulos, e k natural, tem-se que $mdc(ka, kb) = k \cdot mdc(a, b)$.*

Demonstração: Sejam a e b inteiros, não ambos nulos, k natural e $mdc(a, b) = d$. Sendo assim, como $d \mid a$ e $d \mid b$, então $dk \mid ak$ e $dk \mid bk$. Portanto, $dk \mid mdc(ak, bk)$. Agora, vamos demonstrar que dk é divisível por todo divisor comum de ak e bk. De fato, seja α inteiro tal que $\alpha \mid ak$ e $\alpha \mid bk$. Tome inteiros x, y tais que $ax + by = d$. Portanto, $kax + kby = kd$. Como $\alpha \mid ak$ e $\alpha \mid bk$, então $\alpha \mid kd$. Logo, $mdc(ak, bk) = dk$ e, consequentemente, $mdc(ak, bk) = dk = k \cdot mdc(a, b)$, como queríamos demonstrar. ■

Dois números inteiros a e b serão ditos *primos entre si*, ou *coprimos*, se $mdc(a, b) = 1$.

Proposição 1.12 *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração: Suponha que a e b sejam números inteiros primos entre si. Portanto, $mdc(a,b) = 1$. Pelo Teorema de Bézout, temos que existem m e n inteiros tais que $ma+nb = mdc(a,b)$. Logo, $ma+nb = 1$. Reciprocamente, suponha que existam números inteiros m e n tais que $ma+nb = 1$. Seja $mdc(a,b) = d$. Pela proposição 1.4, temos que $d \mid (ma+nb)$ e, consequentemente, $d \mid 1$. Portanto, $d = 1$. Logo, a e b são primos entre si. ■

Corolário 1.13 *Dados os inteiros a e b ambos não nulos e $d = mdc(a,b)$, tem-se que* $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração: De fato, se $d = mdc(a,b)$, pelo Teorema de Bézout, existem m e n inteiros tais que $ma+nb = d$. Dividindo-se ambos os membros da igualdade anterior por d, obtemos que

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

Portanto, pela proposição 1.12, temos que os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si. Logo, $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. ■

Teorema 1.14 (Lema de Gauss) *Sejam a, b e c números inteiros. Se $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.*

Demonstração: Se $a \mid bc$, então existe f inteiro tal que $bc = af$. Como $mdc(a,b) = 1$, pela proposição 1.12, então existem m e n inteiros tais que

$$ma + nb = 1.$$

Sendo assim, multiplicando por c ambos os lados da igualdade acima, obtemos

$$cma + cnb = c.$$

Agora, substituindo bc por af, temos que

$$c = cma + naf = a(cm + nf),$$

o que mostra que $a \mid c$, como queríamos provar. ■

Corolário 1.15 *Dados os inteiros a, b e c, com b e c ambos não nulos e $mdc(b,c) = d$, temos que $b \mid a$ e $c \mid a$ se, e somente se, $\frac{bc}{d} \mid a$.*

Demonstração: Com efeito, suponha que $b \mid a$ e $c \mid a$. Então temos que $a = mb = nc$ para alguns m e n inteiros. Desta forma, temos que

$$m\frac{b}{d} = n\frac{c}{d}.$$

Pelo corolário 1.13, temos que $mdc\left(\frac{b}{d}, \frac{c}{d}\right) = 1$. Sendo assim, tem-se que $\frac{b}{d} \mid n$, o que implica que $\frac{b}{d}c \mid nc$. Logo, $\frac{bc}{d} \mid a$. Reciprocamente, como $mdc(b, c) = d$, então $\frac{b}{d} = B \in \mathbb{Z}$. Portanto, se $\frac{bc}{d} \mid a$, então $B \cdot c \mid a$ e, consequentemente, $c \mid a$. De maneira análoga, como $mdc(b, c) = d$, então $\frac{c}{d} = C \in \mathbb{Z}$. Portanto, se $\frac{bc}{d} \mid a$, então $b \cdot C \mid a$ e, consequentemente, $b \mid a$. Logo, se $\frac{bc}{d} \mid a$, então temos que $b \mid a$ e $c \mid a$, como queríamos demonstrar. ■

1.4 Aritmética Modular

Dois números inteiros a e b se dizem *congruentes* módulo d, sendo d um número natural, quando os restos de sua divisão euclidiana por d são iguais. Para indicar a congruência módulo d dos inteiros a e b, utiliza-se a seguinte notação:

$$a \equiv b \ mod \ d.$$

Por exemplo, $34 \equiv 19 \ mod \ 3$, pois os restos da divisão de 34 e 19 por 3 são iguais a 1.

Agora, quando os restos da divisão euclidiana de a e b por d forem diferentes, diremos que a e b são *incongruentes* módulo d. Utilizaremos, nesse caso, $a \not\equiv b \ mod \ d$. Por exemplo, $34 \not\equiv 19 \ mod \ 4$, pois os restos da divisão de 34 e 19 por 4 são iguais a 2 e 3, respectivamente.

Proposição 1.16 *Sejam a, b e d números inteiros, com $d > 1$. A condição necessária e suficiente para que os números a e b sejam congruentes módulo d é que sua diferença seja múltipla de d, ou seja, $d \mid b - a$.*

Demonstração: Sejam $a = dq_1 + r_1$ e $b = dq_2 + r_2$, com $0 \leq r_1 < d$ e $0 \leq r_2 < d$, as divisões euclidianas de a e b por d, respectivamente. Desta forma, temos que

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

Portanto, $a \equiv b \ mod \ d$ se, e somente se, $r_2 = r_1$, ou seja, $r_2 - r_1 = 0$, o que é equivalente a dizer que $d \mid b - a$, já que $|r_2 - r_1| < d$. ■

Proposição 1.17 *Seja d um número natural. Dados $a, b, c \in \mathbb{Z}$, temos que*

1. *$a \equiv a$ mod d,*

2. *se $a \equiv b$ mod d, então $b \equiv a$ mod d,*

3. *se $a \equiv b$ mod d e $b \equiv c$ mod d, então $a \equiv c$ mod d.*

Demonstração: *1.* Note que $d \mid (a - a) = 0$. Portanto, $a \equiv a$ *mod* d.
2. Se $a \equiv b$ *mod* d, então $d \mid (b - a)$ e, consequentemente, $d \mid (a - b)$, o que implica que $b \equiv a$ *mod* d.
3. Suponha que $a \equiv b$ *mod* d e $b \equiv c$ *mod* d. Sendo assim, $d \mid (b - a)$ e $d \mid (c - b)$. Portanto, pela proposição 1.4, $d \mid [(c - b) + (b - a)] = c - a$. Logo, $a \equiv c$ *mod* d. ■

Proposição 1.18 *Sejam a, b, c, d e f números inteiros, com $d > 1$.*

1. *se $a \equiv b$ mod d e $c \equiv f$ mod d, então $a + c \equiv b + f$ mod d,*

2. *se $a \equiv b$ mod d e $c \equiv f$ mod d, então $ac \equiv bf$ mod d.*

Demonstração: Suponha que $a \equiv b$ *mod* d e $c \equiv f$ *mod* d. Portanto, temos que $d \mid b - a$ e $d \mid f - c$.
1. Pela proposição 1.4, temos que $d \mid [(b - a) + (f - c)]$. Portanto, $d \mid [(b + f) - (a + c)]$. Logo, $a + c \equiv b + f$ *mod* d.
2. Note que $bf - ac = f(b - a) + a(f - c)$. Como $d \mid b - a$ e $d \mid f - c$, então $d \mid [bf - ac]$. Logo, $ac \equiv bf$ *mod* d. ■

Corolário 1.19 *Dados os números inteiros a e b e o número natural n, se $a \equiv b$ mod d, então tem-se que $a^n \equiv b^n$ mod d, ou seja, podemos elevar os dois membros de uma congruência ao mesmo expoente.*

Demonstração: Sejam n congruências $a \equiv b$ *mod* d, ou seja,

$$\begin{cases} a \equiv b \; mod \; d, \\ a \equiv b \; mod \; d, \\ \cdots \\ \cdots \\ a \equiv b \; mod \; d. \end{cases}$$

Pela proposição 1.18, temos que

$$\underbrace{a \times a \times \cdots \times a}_{n} \equiv \underbrace{b \times b \times \cdots \times b}_{n} \; mod \; d \implies a^n \equiv b^n \; mod \; d,$$

como queríamos provar. ■

Proposição 1.20 *Sejam a, b, c e d números inteiros, com $d > 1$. Tem-se que $a + c \equiv b + c \ mod \ d$ se, e somente se, $a \equiv b \ mod \ d$.*

Demonstração: Suponha que $a+c \equiv b+c \ mod \ d$. Sendo assim, então $d \mid [(b+c)-(a+c)]$, o que implica que $d \mid b-a$. Portanto, $a \equiv b \ mod \ d$. Reciprocamente, se $a \equiv b \ mod \ d$, como $c \equiv c \ mod \ d$, pela proposição 1.18, tem-se que $a + c \equiv b + c \ mod \ d$. ■

Proposição 1.21 *Sejam a, b, c, d e f números inteiros, com $d > 1$ e $f = mdc(c, d)$. Tem-se que $ac \equiv bc \ mod \ d$ se, e somente se, $a \equiv b \ mod \ \dfrac{d}{f}$.*

Demonstração: Pelo corolário 1.13, temos que $mdc\left(\dfrac{c}{f}, \dfrac{d}{f}\right) = 1$. Portanto,

$$ac \equiv bc \ mod \ d \iff d \mid (b-a)c \iff \frac{d}{f} \mid (b-a)\frac{c}{f} \iff \frac{d}{f} \mid (b-a) \iff a \equiv b \ mod \ \frac{d}{f},$$

como queríamos provar. ■

Proposição 1.22 *Sejam a e b números inteiros e $d, n, d_1, d_2, ..., d_k$ inteiros maiores do que 1. Temos que*

1. *se $a \equiv b \ mod \ d$ e $n \mid d$, então $a \equiv b \ mod \ n$;*

2. *se $a \equiv b \ mod \ d$, então $mdc(a, d) = mdc(b, d)$;*

3. *$a \equiv b \ mod \ d_i$, para todo $i = 1, 2, ..., k$ se, e somente se, $a \equiv b \ mod \ mmc[d_1, d_2, ..., d_k]$.*

Demonstração: *1.* Se $a \equiv b \ mod \ d$, então $d \mid (b-a)$. Como $n \mid d$, segue-se que $n \mid (b-a)$. Logo, $a \equiv b \ mod \ n$.
2. Se $a \equiv b \ mod \ d$, então $d \mid (b-a)$. Sendo assim, $b-a = dk$, o que implica que $b = a+dk$, com $k \in \mathbb{Z}$. Portanto, pelo lema 1.6, temos que $mdc(a, d) = mdc(a + dk, d) = mdc(b, d)$.
3. Se $a \equiv b \ mod \ d_i$, para todo $i = 1, 2, ..., k$, então $d_i \mid (b-a)$, para todo i. Sendo $b - a$ um múltiplo de cada d_i, segue-se que $mmc[d_1, d_2, ..., d_k] \mid (b-a)$. Logo, $a \equiv b \ mod \ mmc[d_1, d_2, ..., d_k]$. A recíproca decorre do item *1*. ■

Proposição 1.23 (Inverso multiplicativo módulo d) *Se o $mdc(a, d) = 1$, então a é invertível módulo d, ou seja, existe o inverso a^{-1} tal que $a \cdot a^{-1} \equiv 1 \ mod \ d$, em que $0 < a < d$ e $0 < a^{-1} < d$.*

Demonstração: Sejam a e d números inteiros positivos tais que $mdc(a, d) = 1$. Sendo assim, pelo Teorema de Bézout, existem m e n inteiros tais que $am+dn = 1$. Desta forma, $am = 1 - dn$ e, consequentemente, $am = 1 + d(-n)$. Portanto, temos que $am \equiv 1 \ mod \ d$. Logo, m é o inverso multiplicativo de a módulo d, que indica-se $m \equiv a^{-1}$. ■

CAPÍTULO 2

EQUAÇÕES DIOFANTINAS LINEARES

Neste capítulo, que será dividido em duas seções, apresentaremos os conceitos que envolvem as equações diofantinas lineares de duas incógnitas e utilizaremos as noções de mdc e congruências, abordadas no capítulo anterior, para resolver tais equações através de dois métodos: algébrico e aritmético modular. Tais conceitos são baseados em Hefez [9], Domingues [7] e Oliveira [11].

2.1 Equação Diofantina Linear

Uma equação polinomial da forma $a_1x_1 + a_2x_2 + ... + a_nx_n = c$, onde os coeficientes $a_1, a_2, ..., a_n \in \mathbb{Z}$, recebe o nome de *equação diofantina linear* em homenagem a Diofanto de Alexandria, devido a sua utilização de métodos algébricos em busca das possíveis soluções.

Neste trabalho estudaremos as equações diofantinas lineares de duas incógnitas x e y:

$$ax + by = c,$$

onde $a, b, c \in \mathbb{Z}$ e suponhamos a e b não simultaneamente nulos. Desta forma, se um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ satisfaz a equação $ax_0 + by_0 = c$, então diz-se que (x_0, y_0) é uma *solução inteira* da equação diofantina. A seguir apresentaremos em quais condições a equação $ax + by = c$ admite soluções inteiras.

Proposição 2.1 *Sejam a, b e c inteiros e seja $d = mdc(a, b)$. A equação $ax + by = c$ admite solução em números inteiros se, e somente se, $d \mid c$.*

Demonstração: Suponha que existam x e y inteiros tais que $ax + by = c$. Como $d \mid a$ e $d \mid b$, pela proposição 1.4, temos que $d \mid (ax + by)$. Logo, $d \mid c$. Reciprocamente, suponha que $d \mid c$. Então, existe $k \in \mathbb{Z}$ tal que $c = kd$. Pelo Teorema de Bézout, existem $x, y \in \mathbb{Z}$

tais que $ax + by = d$. Daí, multiplicando-se ambos os lados desta última igualdade por k, obtém-se

$$a(xk) + b(yk) = dk \Longrightarrow ax_0 + by_0 = c,$$

onde $x_0 = xk$ e $y_0 = yk$. Logo, (x_0, y_0) é solução da equação $ax + by = c$. ■

Sendo assim, se a equação diofantina $ax+by = c$ admitir solução, mostraremos, na proposição a seguir, como determinar as soluções x e y a partir de uma solução particular x_0, y_0.

Proposição 2.2 *Seja (x_0, y_0) uma solução particular da equação $ax + by = c$, onde $mdc(a, b) = 1$. Então, as soluções inteiras x, y da equação são*

$$x = x_0 + tb \quad e \quad y = y_0 - ta, \ com\ t \in \mathbb{Z}.$$

Demonstração: Seja x, y uma solução de $ax + by = c$. Portanto, como (x_0, y_0) é uma solução particular da equação $ax + by = c$, temos que $ax + by = ax_0 + by_0 = c$. Sendo assim, temos que $a(x - x_0) = b(y_0 - y)$. Como $mdc(a, b) = 1$, segue-se que $b \mid (x - x_0)$ e $a \mid (y_0 - y)$. Portanto,

$$\frac{(x - x_0)}{b} = \frac{(y_0 - y)}{a} = t, \ t \in \mathbb{Z}.$$

Daí, tem-se que $x = x_0 + tb$ e $y = y_0 - ta$, $t \in \mathbb{Z}$, o que mostra que as soluções são do tipo exibido. Por outro lado, (x, y), como no enunciado, é solução, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + by_0 = c,$$

como queríamos provar. ■

2.2 Métodos para resolução de Equações Diofantinas

Nesta seção iremos apresentar dois métodos, algébrico e aritmético modular, para determinar a solução particular (x_0, y_0) de uma equação do tipo $ax + by = c$, quando $mdc(a, b) = 1$.

2.2.1 Método algébrico utilizando o algoritmo de Euclides

Primeiro determina-se o $mdc(a, b)$ através do algoritmo de Euclides. Em seguida, usando o dispositivo prático (algoritmo estendido de Euclides), determina-se $m, n \in \mathbb{Z}$ tais que

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

Multiplicando ambos os membros da igualdade acima por c, obtemos

$$cma + cnb = c.$$

Logo, $x_0 = cm$ e $y_0 = cn$ é uma solução particular da equação $ax + by = c$ e todas as outras soluções inteiras são dadas por

$$x = x_0 + tb \text{ e } y = y_0 - ta, \text{ com } t \in \mathbb{Z}.$$

Exemplo 2.2.3 Resolvamos a equação $16x + 9y = 201$.
Como $mdc(16, 9) = 1$ e $1 \mid 201$, então a equação possui solução. Sendo assim, vamos determinar uma solução particular (x_0, y_0). Para tal, pelo Algoritmo de Euclides, temos que

$$\begin{array}{c|c|c|c|c}
 & 1 & 1 & 3 & 2 \\
\hline
16 & 9 & 7 & 2 & 1 \\
\hline
7 & 2 & 1 & 0 &
\end{array}.$$

Pelo dispositivo prático, temos

$$\begin{array}{cccc}
restos & quocientes & x & y \\
16 & * & 1 & 0 \\
9 & * & 0 & 1 \\
7 & 1 & 1 & -1 \\
2 & 1 & -1 & 2 \\
1 & 3 & 4 & -7
\end{array}.$$

Logo, temos que $m = 4$ e $n = -7$. Daí, $16 \cdot (4) + 9 \cdot (-7) = 1$ e, consequentemente, $16 \cdot (804) + 9 \cdot (-1407) = 201$. Desta forma, temos que $x_0 = 804$ e $y_0 = -1407$ é solução particular da equação e, consequentemente, as soluções são

$$x = 804 + 9t \text{ e } y = -1407 - 16t, \ t \in \mathbb{Z},$$

como queríamos determinar. □

No próximo exemplo, veremos como estender ao caso em que $mdc(a, b) \neq 1$.

Exemplo 2.2.4 Resolvamos a equação $400x + 255y = 1205$.
Como $mdc(400, 255) = 5$ e $5 \mid 1205$, então a equação possui solução. Dividindo ambos os membros da equação por $mdc(400, 255) = 5$, obtemos a equação equivalente $80x + 51y =$

241. Sendo assim, vamos determinar uma solução particular (x_0, y_0) desta última equação. Para tal, pelo Algoritmo de Euclides, temos que

	1	1	1	3	7
80	51	29	22	7	1
29	22	7	1	0	

Pelo dispositivo prático, temos

restos	*quocientes*	x	y
80	$*$	1	0
51	$*$	0	1
29	1	1	-1
22	1	-1	2
7	1	2	-3
1	3	-7	11

Logo, temos que $m = -7$ e $n = 11$. Daí, $80 \cdot (-7) + 51 \cdot (11) = 1$ e, consequentemente, $80 \cdot (-1687) + 51 \cdot (2651) = 241$. Desta forma, temos que $x_0 = -1687$ e $y_0 = 2651$ é solução particular da equação e, consequentemente, as soluções são

$$x = -1687 + 51t \text{ e } y = 2651 - 80t, \ t \in \mathbb{Z},$$

como queríamos determinar. $\square$

2.2.2 Método Aritmético Modular

Seja $ax + by = c$ uma equação diofantina, com $mdc(a, b) = 1$. Supondo $a < b$ e $a < c$, pela divisão euclidiana, temos $b = a \cdot q + r$ e $c = a \cdot p + z$. Sendo assim, pela aritmética modular, temos

$$\begin{cases} ax \equiv 0 \ mod \ a \\ by \equiv ry \ mod \ a \\ c \equiv z \ mod \ a \end{cases}$$

e, consequentemente,

$$ax + by \equiv ry \equiv z \ mod \ a.$$

Note que $1 = mdc(a, b) = mdc(a, r)$. Portanto, pela proposição 1.23, considerando $k = r^{-1}$, temos:

$$ry \equiv z \ mod \ a \Leftrightarrow (kr)y \equiv kz \ mod \ a \Leftrightarrow y \equiv kz \ mod \ a.$$

Logo, $y_0 = kz$ e $x_0 = \dfrac{c - b(kz)}{a}$ é uma solução particular da equação $ax + by = c$ e todas as outras soluções inteiras são dadas por

$$x = x_0 + tb \text{ e } y = y_0 - ta, \text{ com } t \in \mathbb{Z}.$$

Exemplo 2.2.5 Resolvamos a equação $16x + 9y = 201$.
Como $mdc(16, 9) = 1$ e $1 \mid 201$, então a equação possui solução. Sendo assim, vamos determinar uma solução particular (x_0, y_0). Para tal, pela aritmética modular, temos que

$$\begin{cases} 16x \equiv 7x \ mod \ 9 \\ 9y \equiv 0 \ mod \ 9 \\ 201 \equiv 3 \ mod \ 9 \end{cases}$$

e, consequentemente,

$$16x + 9y \equiv 7x \equiv 3 \ mod \ 9.$$

Portanto,

$$7x \equiv 3 \ mod \ 9 \Leftrightarrow 28x \equiv 12 \ mod \ 9 \Leftrightarrow x \equiv 3 \ mod \ 9.$$

Desta forma, temos que $x_0 = 3$ e $y_0 = \dfrac{201 - 16 \cdot 3}{9} = 17$ é solução particular da equação e, consequentemente, as soluções são

$$x = 3 + 9t \text{ e } y = 17 - 16t, \ t \in \mathbb{Z},$$

como queríamos determinar. □

No próximo exemplo, veremos como estender ao caso em que $mdc(a, b) \neq 1$.

Exemplo 2.2.6 Resolvamos a equação $400x + 255y = 1205$.
Como $mdc(255, 400) = 5$ e $5 \mid 1205$, então a equação possui solução. Dividindo ambos os membros da equação por $mdc(255, 400) = 5$, obtemos a equação equivalente $80x + 51y = 241$. Sendo assim, vamos determinar uma solução particular (x_0, y_0) desta última equação. Para tal, pela aritmética modular, temos que

$$\begin{cases} 80x \equiv 29x \ mod \ 51 \\ 51y \equiv 0 \ mod \ 51 \\ 241 \equiv 37 \ mod \ 51 \end{cases}$$

e, consequentemente,

$$80x + 51y \equiv 29x \equiv 37 \ mod \ 51.$$

Portanto,

$$29x \equiv 37 \ mod\ 51 \Leftrightarrow 203x \equiv 259 \ mod\ 51 \Leftrightarrow -x \equiv 4 \ mod\ 51 \Leftrightarrow x \equiv -4 \ mod\ 51.$$

Desta forma, temos que $x_0 = -4$ e $y_0 = \dfrac{241 - 80 \cdot (-4)}{51} = 11$ é solução particular da equação e, consequentemente, as soluções são

$$x = -4 + 51t \text{ e } y = 11 - 80t,\ t \in \mathbb{Z},$$

como queríamos determinar. $\square$

CAPÍTULO 3

SEQUÊNCIA DIDÁTICA

Na elaboração deste trabalho utilizamos como metodologia de pesquisa a Engenharia Didática. Segundo Artigue [2], em uma pesquisa cuja metodologia é a Engenharia Didática, podemos identificar quatro diferentes fases:

1. as análises prévias;
2. a elaboração e análise a priori de experiências didático-pedagógicas;
3. experimentação da sequência didática;
4. análise a posteriori e validação.

Na primeira fase, análise prévia, elabora-se uma revisão bibliográfica abordando as condições presentes nos diversos níveis da sequência didática. Sendo assim, nesta fase, analisa-se como ocorre o ensino atualmente do tema a ser abordado, apresentando as dificuldades encontradas pelos alunos e seus efeitos. Além disso, analisa-se os aspectos epistemológicos do tema e o ambiente aonde ocorrerá a pesquisa.

Na segunda fase, elaboração e análise a priori, constrói-se o embasamento da pesquisa tendo como referência as análises prévias. Nesta fase são determinadas as variáveis de comando: locais (referente à organização de uma sessão ou aula) ou globais (referente à organização de várias sessões ou aulas). Segundo Artigue, a análise a priori comporta duas partes: uma descritiva e uma preditiva.

Na terceira fase, experimentação, coloca-se em prática a sequência didática elaborada. Sendo assim, a experimentação presume: a apresentação da sequência didática; a descrição dos objetivos, das condições e do contexto da realização da pesquisa; a aplicação da sequência didática; a anotação das observações feitas na experimentação.

Na quarta fase, análise a posteriori e validação, deve-se organizar e analisar os dados obtidos na experimentação da sequência didática. Portanto, nesta fase, ocorre o tratamento dos dados obtidos e a comparação com a análise a priori permitindo, assim, verificar quais são as contribuições do objeto de pesquisa e, consequentemente, sua validação.

3.1 Análises prévias

A primeira fase da Engenharia Didática, denominada análises prévias ou análises preliminares, tem como objetivo apresentar a justificativa para a relevância das Equações Diofantinas Lineares para o ensino fundamental, levando-se em consideração a análise do desempenho do ensino do tema e as colaborações que tal implantação possa fomentar.

Por conseguinte, os PCN's ponderam a necessidade de complementar os estudos na Aritmética envolvendo as operações e suas propriedades nos anos finais do ensino fundamental:

> É importante salientar que no quarto ciclo não se pode configurar o abandono da Aritmética, como muitas vezes ocorre. Os problemas aritméticos praticamente não são postos como desafios aos alunos deste ciclo; em geral, as situações trabalhadas pelos professores privilegiam a aplicação de conceitos algébricos. Pode-se até afirmar que os procedimentos não-algébricos (os que não utilizam equações, sistemas etc.) para resolver problemas são desestimulados nos últimos anos do ensino fundamental, mesmo em situações em que a álgebra não é necessária. [4, p.83]

Na confecção das análises prévias, Artigue [2] sugere que se inclua a distinção de três dimensões:

1. dimensão epistemológica;
2. dimensão didática;
3. dimensão cognitiva.

3.1.1 Dimensão epistemológica

Historicamente, as equações diofantinas lineares exerceram um lugar de destaque nos estudos da matemática dos povos egípcio, grego e, em especial, hindu, segundo Eves [8].

> Os hindus revelaram notável habilidade em análise indeterminada, sendo talvez os primeiros a descobrir métodos gerais neste ramo da matemática. Ao contrário de Diofanto, que procurava uma qualquer das soluções racionais de uma equação indeterminada, os hindus empenhavam-se em encontrar todas as soluções inteiras possíveis. [8, p.256]

De acordo com Eves [8], as equações diofantinas lineares recebem este nome em homenagem ao matemático Diofanto de Alexandria, devido a sua utilização de métodos algébricos em busca das possíveis soluções racionais, apesar de Brahmagupta, matemático hindu que viveu na Índia, nos primeiros anos do século VII, ter sido o primeiro a encontrar todas as soluções inteiras possíveis para a equação diofantina linear $ax + by = c$ onde a, b e c são inteiros.

Portanto, pela própria formulação epistemológica, as Equações Diofantinas Lineares do tipo $ax + by = c$ admitem nenhuma ou infinitas soluções inteiras. Além disso, tal temática proporciona a utilização de múltiplos métodos de solução, a partir da tentativa e erro, pois, no aspecto aritmético, a condição necessária e suficiente para que exista solução inteira para esse tipo de equação é que o máximo divisor comum de a e b deve dividir c e, no aspecto algébrico, a representação algébrica desse tipo de equação permite desenvolver o pensamento algébrico e a concepção de uma linguagem generalizante para todas as soluções.

> Desse modo, o ensino de Álgebra precisa continuar garantindo que os alunos trabalhem com problemas, que lhes permitam dar significado à linguagem e às idéias matemáticas. Ao se proporem situações-problema bastante diversificadas, o aluno poderá reconhecer diferentes funções de Álgebra (ao resolver problemas difíceis do ponto de vista aritmético, ao modelizar, generalizar e demonstrar propriedades e fórmulas, estabelecer relações entre grandezas). [4, p.84]

Através de pesquisa feita na Base Nacional Comum Curricular [3], nota-se que o tema Equações Diofantinas Lineares não pertence ao currículo de matemática da educação básica, porém a exploração de problemas envolvendo esse tema possibilita uma contribuição para a formação matemática do aluno do ciclo básico nos campos da aritmética e álgebra.

3.1.2 Dimensão didática

Como o tema Equações Diofantinas Lineares não pertence ao currículo de matemática da educação básica, quando se propõe a discussão quanto à análise didática do objeto matemático, consideramos a abordagem do tema máximo divisor comum presente nos livros de matemática do ensino fundamental distribuídos para as escolas públicas pelo Ministério da Educação e Cultura por meio do Programa Nacional do Livro Didático [5]. Tal tema foi escolhido, pois, por meio dele, se é possível determinar a possibilidade ou não da existência de solução inteira das equações diofantinas lineares.

Um dos livros apresentado é Andrini [1] onde o máximo divisor comum é apresentado de forma superficial com a resolução de uma situação-problema usando o conjunto de divisores. Além disso, é exposto o cálculo do *mdc* pela decomposição em fatores primos e são propostos poucos exercícios. Tal conceito é apresentado em duas páginas, sendo uma de teoria e uma de exercícios.

Agora, em Souza [12], o conceito de máximo divisor comum é abordado de modo breve através de um problema utilizando o conjunto de divisores. Posteriormente, se demonstra o cálculo do *mdc* pela decomposição em fatores primos e pela decomposição simultânea. Tal conceito é apresentado em quatro páginas, sendo duas páginas de teoria e duas de exercícios.

Ocorre que ao consultar algumas obras de ensino de matemática - Andrini [1] e Souza [12] - percebeu-se que o máximo divisor comum é abordado de forma resumida e curta, sem dar destaque as possíveis aplicações do conceito. Além disso, os livros não apresentam o cálculo do *mdc* através do algoritmo de Euclides ou método das divisões sucessivas.

Faz-se necessário também uma análise didática do tema congruências, pois, por meio dele, é possível determinar uma solução particular x_0, y_0 de uma equação diofantina linear do tipo $ax + by = c$. Analisando os livros citados acima, notamos que o conceito de divisão é introduzido a partir de dois casos distintos: um que traz a ideia de repartir uma quantidade em partes iguais e outro com a ideia de calcular quantas vezes uma quantidade cabe em outra. Os autores caracterizam a divisão exata como aquela em que o resto é zero e a divisão não exata como aquela em que há uma "sobra" na operação de divisão. A relação fundamental da divisão, $dividendo = divisor \cdot quociente + resto$, é mostrada em ambos os livros analisados.

Além disso, os exercícios são diversificados e abordam, quase que de modo específico, as ideias associadas ao quociente de uma divisão. O significado do resto é tratado sem ser dada uma relevância maior, que poderia ter sido explicitada, mostrando, por exemplo, o resto como solução de um problema cíclico.

3.1.3 Dimensão cognitiva

No Teste a Priori, que acontece na primeira aula das sequências didáticas (método algébrico e método aritmético modular), os alunos tiveram que resolver duas situações problema do cotidiano que versavam sobre o tema Equações Diofantinas Lineares. Tal aula tinha como objetivo averiguar como seria o comportamento e os conhecimentos prévios dos alunos durante a resolução dos problemas para constatar as possibilidades didáticas da implementação do tema.

Portanto, através da análise das respostas obtidas no Teste a Priori e de uma conversa informal com os alunos, foi possível notar a relevância de se abordar o tema Equações Diofantinas Lineares, pois, o mesmo, contempla temas que ou não são trabalhados (congruências) ou são poucos trabalhados (máximo divisor comum) sem apresentar uma aplicabilidade na resolução de problemas do cotidiano, deixando de desenvolver os conceitos nas áreas da aritmética e álgebra.

Além disso, tal implementação do tema corrobora com o que diz o PCN em relação ao ensino aprendizagem de matemática no quarto ciclo (8° ano e 9° ano):

> Em geral, a ênfase recai no estudo dos conteúdos algébricos, abordados de forma mecânica, distanciando-se ainda mais das situações-problema do cotidiano. É como se, neste ciclo, o aluno tivesse de esquecer quase tudo o que aprendeu antes, porque esses conhecimentos já não lhe servem mais para resolver as situações que ora lhe são propostas. No entanto, essa situação poderá ser revertida se, para os novos conteúdos a serem estudados, esses alunos conseguirem estabelecer relações com os conhecimentos construídos anteriormente. Nesse sentido é importante considerar que alguns aspectos associados ao desenvolvimento cognitivo dos alunos que estão no quarto ciclo em muito favorecem a aprendizagem.[4, p.80]

Logo, o tema Equações Diofantinas Lineares foi aplicado em duas turmas do 9° ano do ensino fundamental da Escola Estadual Aydano de Almeida, situada na região metropolitana do estado do Rio de Janeiro. Os alunos das mencionadas turmas possuem idade entre 14 e 16 anos e a aplicação ocorreu durante as aulas de matemática, onde o professor André é efetivo da turma neste componente curricular.

3.2 Elaboração e análise a priori de experiências didático-pedagógicas

A segunda fase da Engenharia Didática, denominada análise a priori, tem como objetivo determinar as variáveis de comando: locais e globais, além de escolhas didáticas importantes para a aplicação da pesquisa. Sendo assim, norteado pelas análises prévias, foram definidas as variáveis globais que possibilitaram a elaboração das sequências didáticas. Tais variáveis, que dizem respeito à organização de várias aulas, são as seguintes:

1. o conjunto dos números inteiros e o máximo divisor comum;

2. a utilização de situações problema contextualizadas como recurso didático;

3. introduzir os conceitos teorema de Bèzout, congruências e equações diofantinas lineares;

4. possibilitar aos alunos resolverem as situações problema utilizando seus próprios métodos;

5. aprofundar e revisar conceitos matemáticos do ensino fundamental;

6. conduzir os alunos a notarem a limitação do método da tentativa e erro;

7. auxiliar os alunos na construção e desenvolvimento do conhecimento.

Posto isto, com base nas variáveis globais descritas acima, foram feitas algumas escolhas didáticas: a escola, os indivíduos e os meios que possibilitassem a elaboração e experimentação da sequência didática. Assim, delineamos o número de aulas, as datas e o local a serem realizadas. Além disso, direcionamos a elaboração dos instrumentos de pesquisa a partir das análises preliminares, das variáveis globais e dos dados referentes às escolhas anteriores.

3.2.1 Hipóteses

Como citado anteriormente, a análise a priori comporta uma parte preditiva em que são definidas as variáveis locais que estão associadas com as hipóteses que serão confrontadas com a análise a posteriori para a validação da Engenharia Didática. Além disso, as hipóteses estão relacionadas com a análise feita em relação ao comportamento dos alunos, ressaltando-se a importância de verificar a validação de cada uma dessas hipóteses durante a fase de experimentação da sequência didática com o objetivo de averiguar a necessidade de alterações na elaboração da aula seguinte. Tais variáveis, que dizem respeito à organização de uma aula, são as seguintes:

- os alunos perceberão que o método utilizado (método da tentativa e erro) na resolução dos problemas propostos no teste a priori possui limitações;

- os alunos ficarão mais propensos a apreender outros métodos de resolução de problemas;

- ocorrerá a socialização de resultados em cada situação problema;

- introduzir conceitos e algoritmos na busca da resolução das situações problema que possibilitarão ao aluno notar uma aplicabilidade dos seguintes conceitos: máximo divisor comum e congruências.

3.3 Experimentação da sequência didática

Duas sequências de aulas foram desenvolvidas buscando visar sobre os conceitos preliminares e sobre as equações diofantinas lineares, objeto principal de aprendizagem, e foram aplicadas para duas turmas (uma sequência didática para cada turma) do 9° ano do ensino fundamental do Colégio Estadual Aydano de Almeida, situado na cidade de Nilópolis, no estado do Rio de Janeiro.

Ademais, apresentamos uma proposta cujo objetivo é favorecer o professor de matemática da Educação Básica, auxiliando na diversificação das aulas, mostrando o enlace que existe entre Álgebra e Aritmética.

3.3.1 Sequência didática - método algébrico

A seguir apresentamos a sequência didática do método algébrico que consta de seis aulas e abordam os seguintes conceitos: máximo divisor comum, teorema de Bèzout e equações diofantinas. Tal sequência foi aplicada a uma turma de 20 alunos do 9° ano do ensino fundamental.

AULA 1 - TESTE A PRIORI

Plano de aula

Tema: Teste a priori
Conteúdo: Equações Diofantinas Lineares
Objetivos: Propiciar ao aluno: • Estudar aplicações das equações diofantinas na resolução de situações problemas
Metodologia: Os alunos terão 50 minutos para resolver cada situação problema do teste. Espera-se que eles utilizem o método de tentativa e erro para determinar as soluções.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

PROBLEMA DO SAQUE BANCÁRIO

Uma pessoa resolve sacar uma quantia em espécie. Chegando no caixa eletrônico em uma agência bancária, essa pessoa percebe que só havia duas opções de notas disponíveis: R$ 5,00 e R$ 20,00.
a) se essa pessoa deseja sacar R$ 150,00, qual é o número de opções que ela dispõe para fazer o saque?
b) qual é o número máximo de notas que ela pode receber ao efetuar o saque de R$ 150,00?
c) e o número mínimo de notas?

PROBLEMA DO PARQUE DE DIVERSÃO

André, pai de Ana e Carlos, resolve agradar seus filhos levando-os a um parque de diversão. Chegando ao parque, André dá a cada um dos filhos uma quantia de R$ 100,00. Ana e Carlos ao chegarem no caixa para comprar os bilhetes percebem que havia duas opções: R$ 3,00 e R$ 7,00.
a) qual é o número de opções que Ana e Carlos dispõem para fazer a compra dos bilhetes?
b) qual é o número máximo de bilhetes que cada um pode comprar?
c) e o número mínimo de bilhetes?

AULA 2 - REVISÃO DE MDC

Plano de aula

Tema: Máximo Divisor Comum
Conteúdo: MDC e Algoritmo de Euclides
Objetivos: Propiciar ao aluno: • Compreender o conceito de mdc; • Aplicar o algoritmo de Euclides para resolver problemas que envolvam o conceito de mdc;
Metodologia: Relembraremos o conceito de divisibilidade e o conjunto dos divisores de um número. Após, falaremos do conceito do mdc e do algoritmo de Euclides para determinação do mdc de dois números.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Máximo divisor comum

Considere a situação: a tabela abaixo mostra o número de jogos de videogame encomendados pelas lojas A, B e C a determinada empresa.

Jogos encomendados	
Loja	Número de jogos
A	96
B	108
C	132

O encarregado de preparar as encomendas recebeu orientação de colocar o maior número possível de jogos em cada pacote de modo que todos os pacotes tivessem a mesma quantidade de jogos. Além disso, cada pacote deve ter jogos de apenas um tipo: ou A ou B ou C.

Inicialmente, o encarregado determinou os divisores naturais de cada um dos números da tabela:
D(96) = {1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96}
D(108) = {1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108}
D(132) = {1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66, 132}

Note que os números 1, 2, 3, 4, 6 e 12 são divisores de 96, 108 e 132 ao mesmo tempo. Portanto, eles são **divisores comuns** de 96, 108 e 132. Como foi determinado que cada pacote deveria ter o maior número possível de jogos, então cada pacote deveria conter 12 jogos. O que o encarregado fez foi encontrar o **maior divisor comum** de 96, 108 e 132.

Definição: o maior dos divisores comuns de dois ou mais números chama-se **máximo divisor comum (mdc)**.

Agora vamos apresentar um processo prático de cálculo do máximo divisor comum de dois ou mais números.

- Algoritmo de Euclides (divisões sucessivas)

1. Divide-se o número maior pelo menor. Se a divisão for exata, o mdc será o menor deles;

2. Se a divisão não for exata, divide-se o menor pelo resto e assim sucessivamente, até encontrar uma divisão exata. O último divisor será o mdc.

Exemplos: 1. Determine o mdc de 382 e 120.

	3	5	2	5	$\Longrightarrow$ *Quocientes*
382	120	22	10	2	$\Longrightarrow$ *Divisores*
22	10	2	0		$\Longrightarrow$ *Restos*

.

Logo, mdc (382,120) = 2.

2. Determinar o mdc de 96 e 60.

	1	1	1	2	$\Longrightarrow$ *Quocientes*
96	60	36	24	12	$\Longrightarrow$ *Divisores*
36	24	12	0		$\Longrightarrow$ *Restos*

.

Logo, mdc (96,60) = 12.

EXERCÍCIOS

1. Determine:
a) os divisores de 60;
b) os divisores de 72;
c) os divisores comuns de 60 e 72;

d) o maior desses divisores comuns.

2. Utilizando o algoritmo de Euclides, determine:
a) mdc (8,10)
b) mdc (40,50)
c) mdc (32,48)
d) mdc (21,40)
e) mdc (60,72)
f) mdc (75,125)
g) mdc (7,11)
h) mdc (96,108)
i) mdc (16,56)
j) mdc (28,70)

3. Em uma classe, há 28 meninos e 21 meninas. A professora quer formar grupos só de meninos ou só de meninas, com a mesma quantidade de alunos e usando a maior quantidade possível.
a) quantos alunos terá cada grupo?
b) quantos grupos de meninas podem ser formados? E de meninos?

4. Um marceneiro tem duas tiras de madeira, uma com $120cm$ de comprimento e outra com $180cm$ e quer cortá-las em pedaços iguais para montar uma estante. Sabendo que os pedaços devem ser do maior tamanho possível, qual será o comprimento de cada pedaço?

Desafio - Uma editora tem em seu estoque 750 exemplares de um livro A, 1200 de um livro B e 2500 de um livro C. Deseja-se remetê-los a algumas escolas em pacotes, de modo que cada pacote contenha os três tipos de livros em quantidades iguais e com o maior número possível de exemplares de cada tipo. Nessas condições, remetidos todos os pacotes possíveis, o número de exemplares que restarão no estoque é:
a) 1500
b) 1600
c) 1750
d) 2000
e) 2200

AULA 3 - TEOREMA DE BÈZOUT

Plano de aula

Tema: Teorema de Bèzout
Conteúdo: Teorema de Bèzout e dispositivo prático (algoritmo de Euclides estendido)
Objetivos: Propiciar ao aluno: • Compreender o conceito do Teorema de Bèzout; • Aprender o processo do algoritmo de Euclides estendido; • Relacionar os conceitos de mdc e de Teorema de Bèzout;
Metodologia: Iniciaremos a aula enunciando o Teorema de Bèzout e, em seguida, apresentaremos um dispositivo prático (algoritmo de Euclides estendido) para a determinação dos coeficientes m e n.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

Teorema de Bèzout - Dados os inteiros a e b, não ambos nulos, tem-se que o $mdc(a, b) = d$ sempre pode ser escrito como uma combinação linear inteira dos mesmos, ou seja, existem m e n inteiros tais que $d = ma + nb$.

- Dispositivo prático

1. Determine o mdc de a e b utilizando o algoritmo de Euclides.
2. Construa uma tabela na qual a primeira coluna é composta pelos quocientes, excluindo-se o último e inscritos na ordem inversa, obtidos na determinação do $mdc(a, b)$ pelo algoritmo de Euclides e a segunda coluna é a dos coeficientes m e n que é preenchida da seguinta maneira:

- o coeficiente da primeira linha é 1;
- o coeficiente da segunda linha é o produto do coeficiente da primeira linha pelo quociente da segunda linha;
- da terceira linha em diante, seguimos essa regra: o coeficiente de uma determinada linha é o produto do quociente dessa linha pelo coeficiente da linha anterior, adicionado ao coeficiente acima.
- o penúltimo coeficiente é o $|m|$ e o último coeficiente é o $|n|$.

3. Se o número de quocientes utilizado for ímpar, então teremos m positivo e n negativo. Caso contrário, se o número de quocientes utilizado for par, teremos m negativo e n positivo.

Exemplo: Determine o $mdc(132, 204)$ e, em seguida, escreva o mdc como uma combinação linear dos números 132 e 204.
Usando o algoritmo de Euclides temos:

$$\begin{array}{c|c|c|c|c} & 1 & 1 & 1 & 5 \\ \hline 204 & 132 & 72 & 60 & 12 \\ \hline 72 & 60 & 12 & 0 & \end{array}.$$

Portanto, $mdc(204, 132) = 12$. Pelo teorema de Bèzout, temos que $204m + 132n = 12$.
Pelo dispositivo prático, temos:

$$\begin{array}{c|c} q & m, n \\ \hline & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \end{array}.$$

Logo, como a quantidade de quocientes utilizado é um número ímpar, temos que $m = 2$ e $n = -3$ e, consequentemente, $204 \cdot (2) + 132 \cdot (-3) = 12$.

EXERCÍCIO

1. Escreva o mdc dos números inteiros abaixo como uma combinação linear dos mesmos:
a) mdc (8,10)
b) mdc (40,50)
c) mdc (32,48)
d) mdc (21,40)
e) mdc (60,72)
f) mdc (75,125)
g) mdc (7,11)
h) mdc (108,132)
i) mdc (56,80)
j) mdc (70,84)
k) mdc (60,72)
l) mdc (21,28)
m) mdc (120,180)
n) mdc (750,1200)

AULA 4 - DEFINIÇÃO DE EQUAÇÕES DIOFANTINAS E CONDIÇÃO DE EXISTÊNCIA DE SOLUÇÃO

Plano de aula

Tema: Equações Diofantinas Lineares
Conteúdo: Equações Diofantinas Lineares - definição e condição de existência de solução
Objetivos: Propiciar ao aluno: • Compreender o conceito de equação diofantina linear de duas incógnitas; • Compreender em quais condições uma equação diofantina linear de duas incógnitas admite soluções inteiras; • Mostrar uma das aplicações do conceito de mdc;
Metodologia: Iniciaremos a aula demonstrando a definição formal de uma equação diofantina linear de duas incógnitas. Posteriormente, apresentaremos a condição de existência de solução inteira como uma aplicação do conceito de mdc.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Equações diofantinas lineares de duas incógnitas

Definição: uma *equação diofantina linear de duas incógnitas* é uma equação da forma $ax + by = c$, onde x, y são as incógnitas e a, b, c são inteiros dados, sendo $ab \neq 0$. Por exemplo, são equações diofantinas lineares de duas incógnitas: $2x + 6y = 24, 4x + 6y = 13, 14x + 22y = 50$ e $2x + 3y = 101$.

Se dois números inteiros x_0, y_0 satisfazem a equação $ax+by = c$, então denomina-se que x_0, y_0 é uma *solução inteira* da equação diofantina $ax+by = c$. Por exemplo, considere a equação $2x + 6y = 24$. Note que: $2(9) + 6(1) = 24$. Portanto, o par de inteiros, 9 e 1, é solução da equação $2x + 6y = 24$. Agora, considere a equação $4x + 6y = 13$. Note que $4x + 6y$ é um número inteiro par para quaisquer que sejam os valores inteiros de x e y, enquanto 13 é um número inteiro ímpar. Portanto, a equação $4x + 6y = 13$ não tem solução inteira.

- Condição de existência de solução

A equação diofantina linear $ax + by = c$ possui solução x_0, y_0 se, e somente se, d divide c, onde $d = mdc(a, b)$.

Exemplos:

1. A equação $2x + 6y = 24$ possui solução inteira, pois $mdc(6, 2) = 2$ e 2 divide 24.

2. A equação $4x + 6y = 13$ não possui solução inteira, pois $mdc(6, 4) = 2$ e 2 não divide 13.

3. A equação $16x + 9y = 59$ possui solução inteira, pois $mdc(16, 9) = 1$ e 1 divide 59.

EXERCÍCIO

1. Determine quais equações diofantinas lineares de duas incógnitas possuem solução em $\mathbb{Z}$. Em caso afirmativo, determine uma solução.
a) $14x + 22y = 50$
b) $2x + 3y = 101$
c) $13x + 9y = 21$
d) $60x + 48y = 234$
e) $28x + 80y = 44$
f) $5x + 15y = 131$
g) $7x + 11y = 100$
h) $19x + 97y = 1997$
i) $10x + 20y = 203$
j) $13x + 4y = 100$

AULA 5 - SOLUÇÕES GERAIS DE UMA EQUAÇÃO DIOFANTINA

Plano de aula

Tema: Equações Diofantinas Lineares
Conteúdo: Soluções gerais de uma equação diofantina do tipo $ax + by = c$
Objetivos: Propiciar ao aluno: • Resolver eficientemente uma equação diofantina; • Mostrar uma das aplicações do teorema de Bèzout;
Metodologia: Iniciaremos a aula demonstrando como determinar as soluções de uma equação do tipo $ax + by = c$ a partir de uma solução particular x_0, y_0. Posteriormente, mostraremos como determinar a solução particular x_0, y_0 através de uma aplicação do Teorema de Bèzout e do dispositivo prático.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Soluções da equação $ax + by = c$

Seja x_0, y_0 uma solução particular da equação diofantina linear $ax + by = c$, onde $mdc(a, b) = 1$. Então todas as outras soluções desta equação são dadas pelas fórmulas: $x = x_0 + bt$ e $y = y_0 - at$, onde t é um inteiro arbitrário.

Exemplo: Determine a solução geral da equação diofantina $24x + 43y = 117$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 43 e 24. Assim, temos

$$\begin{array}{c|c|c|c|c|c}
 & 1 & 1 & 3 & 1 & 4 \\ \hline
43 & 24 & 19 & 5 & 4 & 1 \\ \hline
19 & 5 & 4 & 1 & 0 &
\end{array}.$$

Portanto, como $mdc(43, 24) = 1$ e 1 divide 117, então a equação $24x + 43y = 117$ possui solução inteira. Desta forma, pelo teorema de Bèzout, temos que $43m + 24n = 1$. Daí, pelo dispositivo prático, temos:

$$\begin{array}{c|c}
q & m, n \\ \hline
 & 1 \\
1 & 1 \\
3 & 4 \\
1 & 5 \\
1 & 9
\end{array}.$$

Logo, como a quantidade de quocientes utilizado foi um número par, temos que $m = -5$ e $n = 9$, o que acarreta em $43(-5)+24(9) = 1$ e, consequentemente, $43(-585)+24(1053) = 117$. Portanto, $x_0 = 1053$ e $y_0 = -585$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 1053 + 43t$ e $y = -585 - 24t$, onde t é um número inteiro arbitrário.

EXERCÍCIO

1. Determine a solução geral de cada uma das equações diofantinas abaixo:

a) $10x + 18y = 60$

b) $5x + 3y = 97$

c) $13x + 9y = 37$

d) $72x + 36y = 288$

e) $28x + 92y = 48$

f) $5x + 15y = 130$

g) $7x + 11y = 10$

h) $19x + 97y = 197$

i) $10x + 20y = 1200$

j) $13x + 4y = 79$

AULA 6 - TESTE A POSTERIORI

Plano de aula

Tema: Teste a posteriori
Conteúdo: Equações Diofantinas Lineares
Objetivos: Propiciar ao aluno: • Estudar aplicações das equações diofantinas na resolução de situações problemas
Metodologia: Os alunos terão 50 minutos para resolver cada situação problema do teste. Espera-se que eles utilizem o método algébrico apresentado no decorrer das aulas para determinar as soluções.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

PROBLEMA DOS REFRIGERANTES

Uma pessoa resolve comprar refrigerantes para o almoço em família de domingo. Chegando ao mercado, essa pessoa percebe que só havia duas opções de refrigerantes disponíveis: Coca-Cola, cujo preço é R$ 5,00, e Guaraná Antarctica R$ 4,00.
a) se essa pessoa deseja gastar R$ 100,00, qual é o número de opções que ela dispõe para fazer a compra dos refrigerantes?
b) qual é o número máximo de refrigerantes que ela pode comprar gastando R$ 100,00?
c) E o número mínimo?

PROBLEMA DO ESTACIONAMENTO

Em um estacionamento no centro de uma cidade tinham estacionados apenas carros e motos. Um garagista notou que existiam 30 rodas.
a) qual é o número de opções de carros e motos que podem existir no estacionamento?
b) qual é o número máximo de carros?
c) e o número mínimo?
d) qual é o número de carros e motos, sabendo que a diferença entre esses dois números é a menor possível?

Experimentação da sequência didática

Durante a experimentação da sequência didática do método algébrico foram aplicadas seis aulas de duração de dois tempos de 50 minutos cada, onde foram recolhidos dados para uma análise a posteriori e, consequentemente, sua validação.

- **1° aula - Teste a Priori**

Nesta aula, as situações problema foram resolvidas de forma individual e os registros foram armazenados para serem comparados aos registros obtidos na última aula (Teste a Posteriori).

Os alunos tiveram dificuldades em encontrar todas as opções desejadas e, sem saber uma forma mais efetiva de resolver os problemas, recorreram ao método da tentativa e erro. Além disso, os alunos foram capazes de notar que no cotidiano podem se deparar com esse tipo de situação.

PROBLEMA DO SAQUE BANCÁRIO

Uma pessoa resolve sacar uma quantia em espécie. Chegando no caixa eletrônico em uma agência bancária, essa pessoa percebe que só havia duas opções de notas disponíveis: R$ 5,00 e R$ 20,00.
a) se essa pessoa deseja sacar R$ 150,00, qual é o número de opções que ela dispõe para fazer o saque?
Solução: Seja x a quantidades de notas de R$5,00 e y a quantidades de notas de R$20,00. Assim, temos $5x + 20y = 150$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 5 e 20. Assim, temos

$$\begin{array}{c|c} & 4 \\ \hline 20 & 5 \\ \hline 0 & \end{array}.$$

Portanto, como $mdc(5, 20) = 5$ e 5 divide 150, então a equação $5x + 20y = 150$ possui solução inteira. Dividindo ambos os membros da equação por $mdc(5, 20) = 5$, obtemos a equação equivalente $x + 4y = 30$. Desta forma, pelo teorema de Bèzout, temos que $4m + n = 1$. Pelo dispositivo prático, temos $m = 0$ e $n = 1$, o que acarreta em $4 \cdot 0 + 1 \cdot 1 = 1$ e, consequentemente, $4 \cdot 0 + 1 \cdot 30 = 30$. Portanto, $x_0 = 30$ e $y_0 = 0$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 30 + 4t$ e $y = 0 - t = -t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de notas de R$5,00 e R$20,00, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $-7 \leq t \leq -1$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 8 opções de saque dispostos na tabela a seguir:

Número de opções	Notas de R$ 20,00	Notas de R$ 5,00
1°	0	30
2°	1	26
3°	2	22
4°	3	18
5°	4	14
6°	5	10
7°	6	6
8°	7	2

b) qual é o número máximo de notas que ela pode receber ao efetuar o saque de R$ 150,00?
Resposta: 30 notas, sendo 0 notas de R$ 20,00 e 30 notas de R$ 5,00.

c) e o número mínimo de notas?
Resposta: 9 notas, sendo 7 notas de R$ 20,00 e 2 notas de R$ 5,00.

PROBLEMA DO PARQUE DE DIVERSÃO

André, pai de Ana e Carlos, resolve agradar seus filhos levando-os a um parque de diversão. Chegando ao parque, André dá a cada um dos filhos uma quantia de R$ 100,00. Ana e Carlos ao chegarem no caixa para comprar os bilhetes percebem que havia duas opções: R$ 3,00 e R$ 7,00.
a) qual é o número de opções que Ana e Carlos dispõem para fazer a compra dos bilhetes?
Solução: Seja x a quantidade de bilhetes de R$3,00 e y a quantidade de bilhetes de R$7,00. Assim, temos $3x + 7y = 100$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 3 e 7. Assim, temos

$$\begin{array}{c|c|c} & 2 & 3 \\ \hline 7 & 3 & 1 \\ \hline 1 & 0 & \end{array}.$$

Portanto, como $mdc(3,7) = 1$ e 1 divide 100, então a equação $3x+7y = 100$ possui solução inteira. Desta forma, pelo teorema de Bèzout, temos que $7m + 3n = 1$. Pelo dispositivo prático, temos

$$\begin{array}{c|c} q & m, n \\ \hline & 1 \\ 2 & 2 \end{array}.$$

Logo, como a quantidade de quocientes utilizado foi um número ímpar, temos que $m = 1$ e

$n = -2$, o que acarreta em $7 \cdot 1 + 3 \cdot (-2) = 1$ e, consequentemente, $7 \cdot 100 + 3 \cdot (-200) = 100$. Portanto, $x_0 = -200$ e $y_0 = 100$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = -200 + 7t$ e $y = 100 - 3t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de bilhetes de R$3,00 e R$7,00, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $29 \leq t \leq 33$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 5 opções de compra de bilhetes dispostos na tabela a seguir:

Número de opções	Bilhetes de R$ 3,00	Bilhetes de R$ 7,00
1°	31	1
2°	24	4
3°	17	7
4°	10	10
5°	3	13

b) qual é o número máximo de bilhetes que cada um pode comprar?
Resposta: 32 bilhetes, sendo 31 bilhetes de R$ 3,00 e 1 bilhete de R$ 7,00.

c) e o número mínimo de bilhetes?
Resposta: 16 bilhetes, sendo 3 bilhetes de R$ 3,00 e 13 bilhetes de R$ 7,00.

Para avaliação dos resultados obtidos no Teste a Priori adotamos um conceito em relação ao número de acertos obtido pelo aluno no item a) de cada um dos problemas propostos, usando o seguinte critério:

1. Problema do Saque Bancário

   - Adotamos conceito A aos alunos que determinaram as 8 opções de saque;
   - Adotamos conceito B aos alunos que determinaram entre 5 e 7 opções de saque;
   - Adotamos conceito C aos alunos que determinaram entre 1 e 4 opções de saque;
   - Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de saque;

2. Problema do Parque de Diversão

   - Adotamos conceito A aos alunos que determinaram as 5 opções de compra de bilhetes;
   - Adotamos conceito B aos alunos que determinaram 3 ou 4 opções de compra de bilhetes;
   - Adotamos conceito C aos alunos que determinaram 1 ou 2 opções de compra de bilhetes;

- Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de compra de bilhetes;

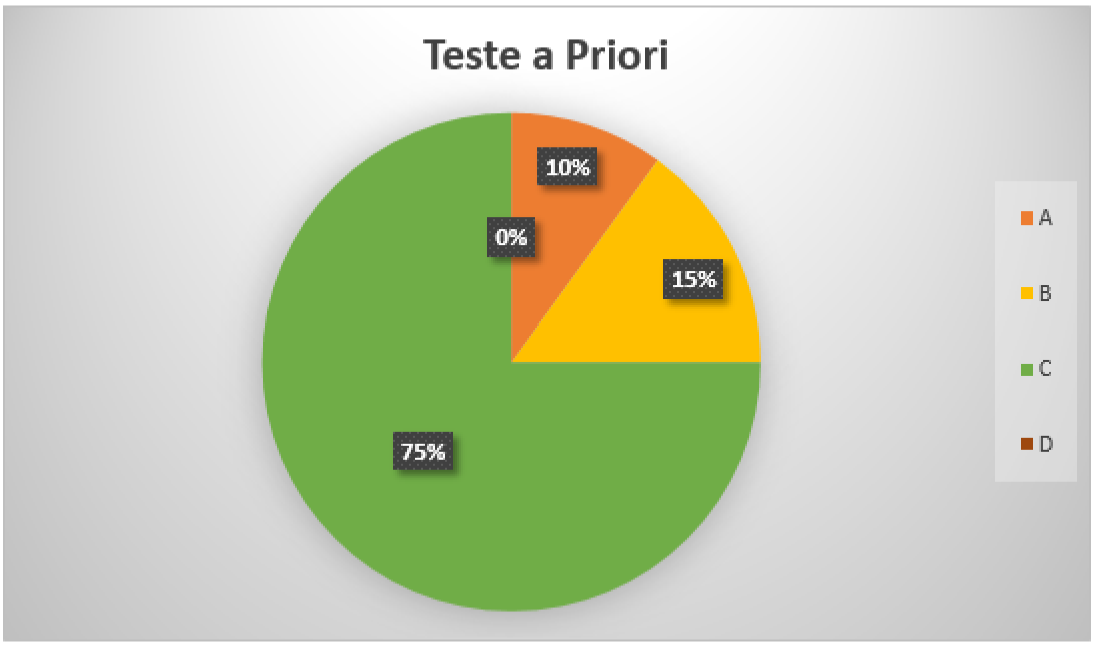
Tal critério esta sintetizado na seguinte tabela:

Conceito	Número de acertos	
	Problema do saque bancário	Problema do parque de diversão
A	8	5
B	5 - 7	3 - 4
C	1 - 4	1 - 2
D	0	0

A seguir, apresentamos a quantidade de alunos que obtiveram os conceitos A, B, C e D nos problemas supracitados.

Conceito	Número de alunos	
	Problema do saque bancário	Problema do parque de diversão
A	2	2
B	3	4
C	15	14
D	0	0
Total	20	20

Como o número de alunos que alcançaram os conceitos A, B, C e D foram basicamente os mesmos para ambos problemas, então para ilustrar os dados obtidos elaboramos o gráfico a seguir baseados nos conceitos que os alunos obtiveram no problema do saque bancário.



- **2° aula - Revisão de MDC**

Na segunda aula efetuou-se uma revisão sobre o conceito de máximo divisor comum e sobre um método para a sua determinação: método das divisões sucessivas, conhecido como algoritmo de Euclides. Além disso, foram propostos alguns exercícios onde os alunos puderam aplicar o algoritmo de Euclides para determinar o mdc e, consequentemente, encontrar a resposta.

Nesta aula, a maior parte dos alunos comentou que desconheciam o algoritmo de Euclides para determinação do mdc de dois números inteiros. Contudo, eles não tiveram dificuldades para entender o algoritmo e, consequentemente, resolveram de forma satisfatória os exercícios.

- **3° aula - Teorema de Bèzout**

Na terceira aula apresentou-se o teorema de Bèzout e um dispositivo prático(algoritmo de Euclides estendido) que permite calcular os inteiros que expressam o mdc dos coeficientes a e b como combinação linear dos mesmos. Além disso, foram propostos alguns exercícios onde os alunos puderam aplicar os conhecimentos adquiridos.

Nesta aula, os alunos relataram que o dispositivo é de fácil uso e se questionavam de que maneira o uso deste dispositivo poderia levar a encontrar alguma solução das situações-problema apresentadas no Teste a Priori.

- **4° aula - Definição de equações diofantinas**

Na quarta aula apresentou-se a definição de uma equação diofantina linear de duas incógnitas. Ademais, mostrou-se em quais condições tais equações admitem soluções inteiras, correlacionando o mdc dos coeficientes com o termo independente e apresentando, assim, uma das possíveis aplicações do conceito de mdc.

Nesta aula, os alunos tiveram dificuldade para compreender a definição das equações diofantinas, porém, segundo a exposição dos exercícios propostos, eles alcançaram uma melhor compreensão.Além disso, com a elucidação da condição de existência de solução das equações diofantinas, ficou claro para os alunos a relevância da aula de revisão de mdc e do algoritmo de Euclides.

- **5° aula - Soluções gerais de uma equação diofantina**

Na quinta aula mostrou-se como determinar as soluções gerais de uma equação diofantina a partir de uma solução particular x_0, y_0. Para tal, foram utilizados o algoritmo de Euclides e o dispositivo prático para explicitação da solução particular x_0, y_0, apresentando, assim, uma das possíveis aplicações do teorema de Bèzout. Além disso, foram propostos alguns exercícios onde os alunos puderam aplicar os conhecimentos adquiridos.

Nesta aula, os alunos narraram que foi bastante útil aprender uma nova maneira de encontrar todas as soluções de uma equação diofantina e, desta forma, poderiam resolver problemas do cotidiano de forma simples e ágil.

- **6° aula - Teste a Posteriori**

Na última aula desta sequência didática, os alunos tiveram contato novamente com a resolução de situações do cotidiano. Nesta aula, as situações-problema foram resolvidas de forma individual e os registros foram armazenados para serem comparados aos registros obtidos na primeira aula (Teste a Priori).

Como já era esperado, a maior parte dos alunos não encontrou maiores dificuldades para determinar de forma satisfatória as soluções dos problemas propostos, pois utilizaram o método algébrico, apresentado no decorrer das aulas da sequência didática, para resolver tais situações-problema. Além disso, notaram que, em consequência das informações apresentadas nos enunciados, apenas algumas soluções inteiras atenderiam as situações-problema.

PROBLEMA DOS REFRIGERANTES

Uma pessoa resolve comprar refrigerantes para o almoço em família de domingo. Chegando ao mercado, essa pessoa percebe que só havia duas opções de refrigerantes disponíveis: marca A, cujo preço é R$4,00, e marca B, cujo preço é R$5,00.
a) se essa pessoa deseja gastar R$ 100,00, qual é o número de opções que ela dispõe para fazer a compra dos refrigerantes?
Solução: Seja x a quantidade de refrigerantes da marca A e y a quantidade de refrigerantes da marca B. Assim, temos $4x + 5y = 100$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 4 e 5. Assim, temos

$$\begin{array}{c|c|c} & 1 & 4 \\ \hline 5 & 4 & 1 \\ \hline 1 & 0 & \end{array}.$$

Portanto, como $mdc(4,5) = 1$ e 1 divide 100, então a equação $4x+5y = 100$ possui solução inteira. Desta forma, pelo teorema de Bèzout, temos que $5m + 4n = 1$. Pelo dispositivo prático, temos

$$\begin{array}{c|c} q & m, n \\ \hline & 1 \\ 1 & 1 \end{array}.$$

Logo, como a quantidade de quocientes utilizado foi um número ímpar, temos que $m = 1$ e $n = -1$, o que acarreta em $5 \cdot 1 + 4 \cdot (-1) = 1$ e, consequentemente, $5 \cdot 100 + 4 \cdot (-100) = 100$.

Portanto, $x_0 = -100$ e $y_0 = 100$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = -100+5t$ e $y = 100-4t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de refrigerantes das marcas A e B, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $20 \leq t \leq 25$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 6 opções de compra de refrigerantes dispostos na tabela a seguir:

Número de opções	marca A	marca B
1°	25	0
2°	20	4
3°	15	8
4°	10	12
5°	5	16
6°	0	20

b) qual é o número máximo de refrigerantes que ela pode comprar gastando R$ 100,00?
Resposta: 25 refrigerantes, sendo 25 refrigerantes da marca A e 0 refrigerantes da marca B.

c) E o número mínimo?
Resposta: 20 refrigerantes, sendo 0 refrigerantes da marca A e 20 refrigerantes da marca B.

PROBLEMA DO ESTACIONAMENTO

Em um estacionamento no centro de uma cidade tinham estacionados apenas carros e motos. Um garagista notou que existiam 30 rodas.
a) qual é o número de opções de carros e motos que podem existir no estacionamento?
Solução: Seja x a quantidade de motos e y a quantidade de carros. Assim, temos $2x + 4y = 30$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 2 e 4. Assim, temos

$$\begin{array}{c|c} & 2 \\ \hline 4 & 2 \\ \hline 0 & \end{array}.$$

Portanto, como $mdc(2, 4) = 2$ e 2 divide 30, então a equação $2x + 4y = 30$ possui solução inteira. Dividindo ambos os membros da equação por $mdc(2, 4) = 2$, obtemos a equação equivalente $x + 2y = 15$. Desta forma, pelo teorema de Bèzout, temos que $2m + n = 1$. Pelo dispositivo prático, temos $m = 0$ e $n = 1$, o que acarreta em $2 \cdot 0 + 1 \cdot 1 = 1$

e, consequentemente, $2 \cdot 0 + 1 \cdot 15 = 15$. Portanto, $x_0 = 15$ e $y_0 = 0$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 15 + 2t$ e $y = 0 - t = -t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de motos e carros, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $-7 \leq t \leq 0$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 8 opções de carros e motos no estacionamento dispostos na tabela a seguir:

Número de opções	Número de carros	Número de motos
1°	0	15
2°	1	13
3°	2	11
4°	3	9
5°	4	7
6°	5	5
7°	6	3
8°	7	1

b) qual é o número máximo de carros?
Resposta: 7 carros.

c) e o número mínimo?
Resposta: 0 carros.

d) qual é o número de carros e motos, sabendo que a diferença entre esses dois números é a menor possível?
Resposta: 5 carros e 5 motos, pois a diferença entre esses dois números é zero.

Para avaliação dos resultados obtidos no Teste a Posteriori adotamos um conceito em relação ao número de acertos obtido pelo aluno no item a) de cada um dos problemas propostos, usando o seguinte critério:

1. Problema dos Refrigerantes
    - Adotamos conceito A aos alunos que determinaram as 6 opções de compra;
    - Adotamos conceito B aos alunos que determinaram 4 ou 5 opções de compra;
    - Adotamos conceito C aos alunos que determinaram entre 1 e 3 opções de compra;
    - Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de compra;
2. Problema do Estacionamento

- Adotamos conceito A aos alunos que determinaram as 8 opções de carros e motos;

- Adotamos conceito B aos alunos que determinaram entre 5 e 7 opções de carros e motos;

- Adotamos conceito C aos alunos que determinaram entre 1 e 4 opções de carros e motos;

- Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de carros e motos;

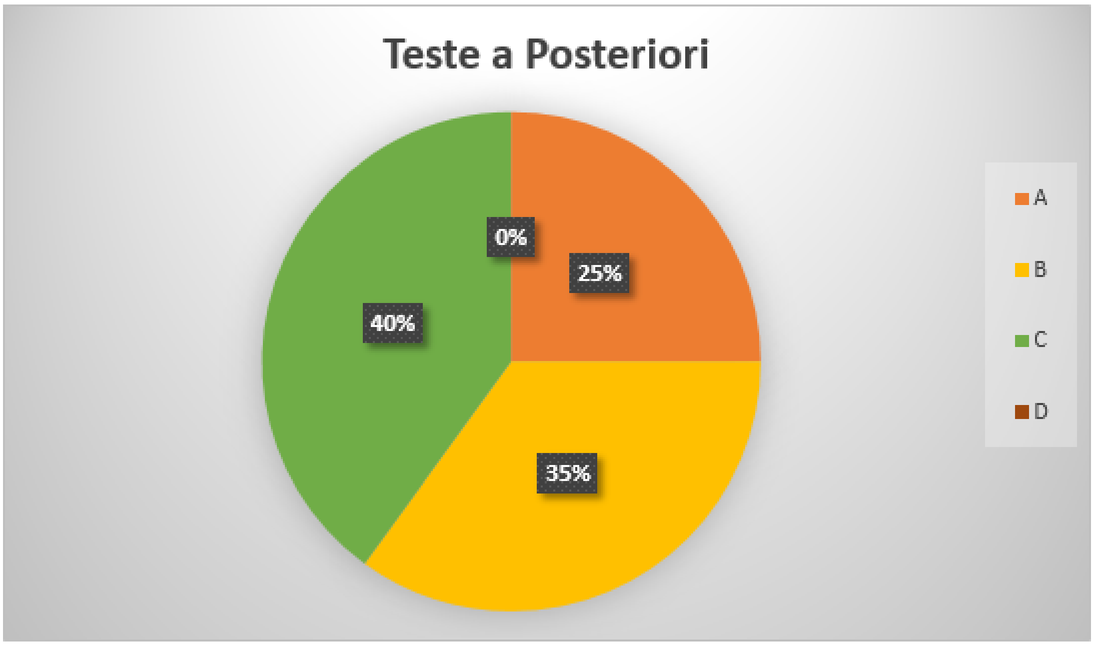
Tal critério esta sintetizado na seguinte tabela:

Conceito	Número de acertos	
	Problema dos refrigerantes	Problema do estacionamento
A	6	8
B	4 - 5	5 - 7
C	1 - 3	1 - 4
D	0	0

A seguir, apresentamos a quantidade de alunos que obtiveram os conceitos A, B, C e D nos problemas supracitados.

Conceito	Número de alunos	
	Problema dos refrigerantes	Problema do estacionamento
A	5	5
B	7	6
C	8	9
D	0	0
Total	20	20

Como o número de alunos que alcançaram os conceitos A, B, C e D foram basicamente os mesmos para ambos problemas, então para ilustrar os dados obtidos elaboramos o gráfico a seguir baseados nos conceitos que os alunos obtiveram no problema dos refrigerantes.



3.3.2 Sequência didática - método aritmético modular

A seguir apresentamos a sequência didática do método aritmético modular que consta de sete aulas e abordam os seguintes conceitos: máximo divisor comum, congruência e equações diofantinas. Tal sequência foi aplicada a uma turma de 30 alunos do 9° ano do ensino fundamental.

Vale observar que as aulas Teste a Priori, Revisão de *mdc*, Definição de Equações Diofantinas e Condição de Existência de Solução e Teste a Posteriori serão as mesmas do método algébrico. Por uma questão de completude, repetimos o texto das aulas nesta seção.

AULA 1 - TESTE A PRIORI

Plano de aula

Tema: Teste a priori
Conteúdo: Equações Diofantinas Lineares
Objetivos: Propiciar ao aluno: • Estudar aplicações das equações diofantinas na resolução de situações problemas
Metodologia: Os alunos terão 50 minutos para resolver cada situação problema do teste. Espera-se que eles utilizem o método de tentativa e erro para determinar as soluções.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

PROBLEMA DO SAQUE BANCÁRIO

Uma pessoa resolve sacar uma quantia em espécie. Chegando no caixa eletrônico em uma agência bancária, essa pessoa percebe que só havia duas opções de notas disponíveis: R$ 5,00 e R$ 20,00.

a) se essa pessoa deseja sacar R$ 150,00, qual é o número de opções que ela dispõe para fazer o saque?

b) qual é o número máximo de notas que ela pode receber ao efetuar o saque de R$ 150,00?

c) e o número mínimo de notas?

PROBLEMA DO PARQUE DE DIVERSÃO

André, pai de Ana e Carlos, resolve agradar seus filhos levando-os a um parque de diversão. Chegando ao parque, André dá a cada um dos filhos uma quantia de R$ 100,00. Ana e Carlos ao chegarem no caixa para comprar os bilhetes percebem que havia duas opções: R$ 3,00 e R$ 7,00.

a) qual é o número de opções que Ana e Carlos dispõem para fazer a compra dos bilhetes?

b) qual é o número máximo de bilhetes que cada um pode comprar?

c) e o número mínimo de bilhetes?

AULA 2 - REVISÃO DE MDC

Plano de aula

Tema: Máximo Divisor Comum
Conteúdo: MDC e Algoritmo de Euclides
Objetivos: Propiciar ao aluno: • Compreender o conceito de mdc; • Aplicar o algoritmo de Euclides para resolver problemas que envolvam o conceito de mdc;
Metodologia: Relembraremos o conceito de divisibilidade e o conjunto dos divisores de um número. Após, falaremos do conceito do mdc e do algoritmo de Euclides para determinação do mdc de dois números.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Máximo divisor comum

Considere a situação: a tabela abaixo mostra o número de jogos de videogame encomendados pelas lojas A, B e C a determinada empresa.

Jogos encomendados	
Loja	Número de jogos
A	96
B	108
C	132

O encarregado de preparar as encomendas recebeu orientação de colocar o maior número possível de jogos em cada pacote de modo que todos os pacotes tivessem a mesma quantidade de jogos. Além disso, cada pacote deve ter jogos de apenas um tipo: ou A ou B ou C.

Inicialmente, o encarregado determinou os divisores naturais de cada um dos números da tabela:
D(96) = $\{1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96\}$
D(108) = $\{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$
D(132) = $\{1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66, 132\}$

Note que os números 1, 2, 3, 4, 6 e 12 são divisores de 96, 108 e 132 ao mesmo tempo. Portanto, eles são **divisores comuns** de 96, 108 e 132.

Como foi determinado que cada pacote deveria ter o maior número possível de jogos, então cada pacote deveria conter 12 jogos. O que o encarregado fez foi encontrar o **maior divisor comum** de 96, 108 e 132.

Definição: o maior dos divisores comuns de dois ou mais números chama-se **máximo divisor comum (mdc)**.

Agora vamos apresentar um processo prático de cálculo do máximo divisor comum de dois ou mais números.

- Algoritmo de Euclides (divisões sucessivas)

1. Divide-se o número maior pelo menor. Se a divisão for exata, o mdc será o menor deles;

2. Se a divisão não for exata, divide-se o menor pelo resto e assim sucessivamente, até encontrar uma divisão exata. O último divisor será o mdc.

Exemplos: 1. Determine o mdc de 382 e 120.

	3	5	2	5	$\Longrightarrow$ *Quocientes*
382	120	22	10	2	$\Longrightarrow$ *Divisores*
22	10	2	0		$\Longrightarrow$ *Restos*

Logo, mdc (382,120) = 2.

2. Determinar o mdc de 96 e 60.

	1	1	1	2	$\Longrightarrow$ *Quocientes*
96	60	36	24	12	$\Longrightarrow$ *Divisores*
36	24	12	0		$\Longrightarrow$ *Restos*

Logo, mdc (96,60) = 12.

EXERCÍCIOS

1. Determine:
a) os divisores de 60;
b) os divisores de 72;
c) os divisores comuns de 60 e 72;
d) o maior desses divisores comuns.

2. Utilizando o algoritmo de Euclides, determine:
a) mdc (8,10)
b) mdc (40,50)
c) mdc (32,48)
d) mdc (21,40)
e) mdc (60,72)
f) mdc (75,125)
g) mdc (7,11)
h) mdc (96,108)
i) mdc (16,56)

j) mdc (28,70)

3. Em uma classe, há 28 meninos e 21 meninas. A professora quer formar grupos só de meninos ou só de meninas, com a mesma quantidade de alunos e usando maior quantidade possível.
a) quantos alunos terá cada grupo?
b) quantos grupos de meninas podem ser formados? E de meninos?

4. Um marceneiro tem duas tiras de madeira, uma com 120cm de comprimento e outra com 180cm e quer cortá-las em pedaços iguais para montar uma estante. Sabendo que os pedaços devem ser do maior tamanho possível, qual será o comprimento de cada pedaço?

Desafio - Uma editora tem em seu estoque 750 exemplares de um livro A, 1200 de um livro B e 2500 de um livro C. Deseja-se remetê-los a algumas escolas em pacotes, de modo que cada pacote contenha os três tipos de livros em quantidades iguais e com o maior número possível de exemplares de cada tipo. Nessas condições, remetidos todos os pacotes possíveis, o número de exemplares que restarão no estoque é:
a) 1500
b) 1600
c) 1750
d) 2000
e) 2200

AULA 3 - ARITMÉTICA MODULAR

Plano de aula

Tema: Aritmética modular
Conteúdo: Congruência módulo m e suas propriedades
Objetivos: Propiciar ao aluno: • Compreender o conceito de congruência módulo m e suas propriedades;
Metodologia: Iniciaremos a aula definindo o conceito de congruência e, em seguida, apresentaremos as principais propriedades.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Congruência

Sejam a e b dois inteiros quaisquer e seja d um natural. Diz-se que a é congruente a b módulo d se os restos das divisões de a e b por d são iguais. Em outros termos, a é congruente a b módulo d se, e somente se, d divide a diferença $a-b$. Notação: $a \equiv b \ mod \ d$. Por exemplo, $48 \equiv 23 \ mod \ 5$, pois os restos da divisão de 48 e 23 por 5 são iguais a 3.

PROPRIEDADES

1°) Todo número é congruente consigo mesmo em relação a qualquer módulo, ou seja, $a \equiv a \ mod \ d$.

2°) Se $a \equiv b \ mod \ d$, então $b \equiv a \ mod \ d$.

3°) Se $a \equiv b \ mod \ d$ e $b \equiv c \ mod \ d$, então $a \equiv c \ mod \ d$.

4°) Podemos somar ou subtrair, membro a membro, duas congruências de mesmo módulo, ou seja, se $a \equiv b \ mod \ d$ e $c \equiv f \ mod \ d$, então $a + c \equiv b + f \ mod \ d$.

5°) Podemos multiplicar, membro a membro, duas congruências de mesmo módulo, ou seja, se $a \equiv b \ mod \ d$ e $c \equiv f \ mod \ d$, então $ac \equiv bf \ mod \ d$.

6°) Podemos somar ou subtrair o mesmo número k aos dois membros de uma congruência, ou seja, se $a \equiv b \ mod \ d$, então $a + k \equiv b + k \ mod \ d$.

7°) Podemos multiplicar os dois membros de uma congruência por um mesmo número k, ou seja, se $a \equiv b \ mod \ d$, então $ak \equiv bk \ mod \ d$.

8°) Podemos elevar os dois membros de uma congruência ao mesmo expoente n inteiro positivo, ou seja, se $a \equiv b \ mod \ d$, então $a^n \equiv b^n \ mod \ d$.

9°) Se o $mdc(a, d) = 1$, então existe o inteiro k tal que $ak \equiv 1 \ mod \ d$, em que $0 < a < d$ e $0 < k < d$. O inteiro k é denominado *inverso multiplicativo* de a módulo d.

EXERCÍCIOS

1. Uma empresa de entrega de correspondências dividiu o município de Nilópolis em 100 setores para realizar a entrega das correspondências nas residências. Para tal, foi feito um cronograma dos setores a serem atendidos nos respectivos dias da semana, de acordo com a tabela abaixo:

DOMINGO	2° FEIRA	3° FEIRA	4° FEIRA	5° FEIRA	6° FEIRA	SÁBADO
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	...

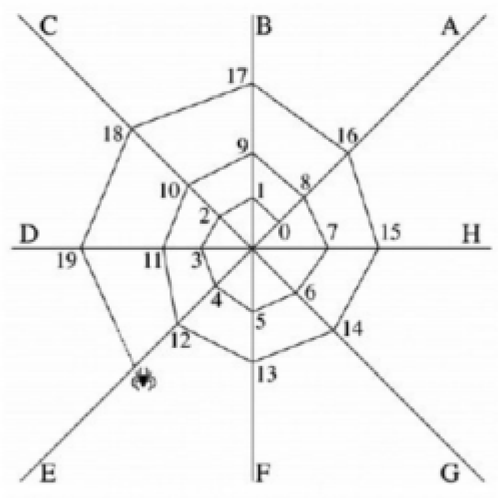
Responda:

a) em qual dia da semana o setor de número 87 deve receber suas correspondências?

b) em qual dia da semana o setor de número 58 deve receber suas correspondências?

c) em qual dia da semana o setor de número 77 deve receber suas correspondências?
d) em qual dia da semana o setor de número 96 deve receber suas correspondências?
e) quantos setores são atendidos pela empresa de entrega de correspondências na 4° feira? E no domingo?
f) é possível estabelecer uma relação entre os dias da semana e a distribuição dos setores? Qual?

2. (OBMEP) A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?



3. Sabendo que o dia 1 de janeiro de 2017 ocorreu num domingo e que o ano de 2017 não é bissexto, ou seja, o mês de fevereiro possui 28 dias, determine em qual dia da semana ocorreu o dia 28 de julho de 2017?

4. Verifique se são verdadeiras ou falsas as seguintes afirmações:
a) $35 \equiv 27 \ mod \ 4$
b) $72 \equiv 32 \ mod \ 5$
c) $83 \equiv 72 \ mod \ 5$
d) $78 \equiv 33 \ mod \ 9$
e) $64 \equiv 36 \ mod \ 3$
f) $97 \equiv 15 \ mod \ 2$

AULA 4 - ARITMÉTICA MODULAR E APLICAÇÕES

Plano de aula

Tema: Aritmética modular
Conteúdo: Congruência módulo m e suas propriedades
Objetivos: Propiciar ao aluno: • Aplicar as propriedades para resolver problemas que envolvam o conceito de congruência;
Metodologia: Iniciaremos a aula dando exemplos da aplicação das propriedades na resolução de problemas. Posteriormente, os alunos terão que resolver exercícios utilizando as propriedades.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Aplicações das propriedades de congruências

Exemplos:
1. Qual o resto da divisão da expressão 123325 - 97465 + 309352 por 7?
Temos que

$$\begin{cases} 123325 \equiv 6 \; mod \; 7 \\ 97465 \equiv 4 \; mod \; 7 \\ 309352 \equiv 1 \; mod \; 7 \end{cases}$$

Portanto, pela propriedade (4), temos

$$123325 - 97465 + 309352 \equiv 6 - 4 + 1 \equiv 3 \; mod \; 7.$$

Logo, a expressão 123325 - 97465 + 309352, ao ser dividida por 7, deixa resto 3.

2. Qual o resto da divisão da expressão $325 \cdot 746 \cdot 952$ por 4?
Temos que

$$\begin{cases} 325 \equiv 1 \; mod \; 4 \\ 746 \equiv 2 \; mod \; 4 \\ 952 \equiv 0 \; mod \; 4 \end{cases}$$

Portanto, pela propriedade (5), temos

$$325 \cdot 746 \cdot 952 \equiv 1 \cdot 2 \cdot 0 \equiv 0 \; mod \; 4.$$

Logo, a expressão $325 \cdot 746 \cdot 952$, ao ser dividida por 4, deixa resto 0.

3. Determine o resto de 3^{25} na divisão por 8?
Temos que

$$\begin{cases} 3 \equiv 3 \ mod\ 8 \\ 3^2 \equiv 1 \ mod\ 8 \end{cases}$$

Portanto, pela propriedade (8), temos

$$3^2 \equiv 1 \ mod\ 8 \Longrightarrow (3^2)^{12} \equiv 1^{12} \ mod\ 8 \Longrightarrow 3^{24} \equiv 1 \ mod\ 8.$$

Sendo assim,

$$3^{25} = 3 \cdot 3^{24} \equiv 3 \cdot 1 \equiv 3 \ mod\ 8.$$

Logo, a expressão 3^{25}, ao ser dividida por 8, deixa resto 3.

4. Determine o inverso multiplicativo de 13 nos seguintes módulos: 5 e 7.
Como $mdc(13, 5) = 1$, pela propriedade (9), existe o inteiro k tal que $13k \equiv 1 \ mod\ 5$. Note que

$$\begin{cases} 13 \times 1 = 13 \equiv 3 \ mod\ 5 \\ 13 \times 2 = 26 \equiv 1 \ mod\ 5. \end{cases}$$

Portanto, o inverso de $13(mod\ 5)$ é 2.
Agora, como $mdc(13, 7) = 1$, pela propriedade (9), existe o inteiro k tal que $13k \equiv 1 \ mod\ 7$. Note que

$$\begin{cases} 13 \times 1 = 13 \equiv 6 \ mod\ 7 \\ 13 \times 2 = 26 \equiv 5 \ mod\ 7 \\ 13 \times 3 = 39 \equiv 4 \ mod\ 7 \\ 13 \times 4 = 52 \equiv 3 \ mod\ 7 \\ 13 \times 5 = 65 \equiv 2 \ mod\ 7 \\ 13 \times 6 = 78 \equiv 1 \ mod\ 7. \end{cases}$$

Portanto, o inverso de $13(mod\ 7)$ é 6.

5. Determine todos os inteiros x que satisfazem $3x \equiv 7 \ mod\ 11$.
Como $3 \times 4 = 12 \equiv 1 \ mod\ 11$, então podemos multiplicar a congruência dada por 4. Sendo assim, temos

$$3x \equiv 7 \ mod\ 11 \Longleftrightarrow 12x \equiv 28 \ mod\ 11 \Longleftrightarrow x \equiv 6 \ mod\ 11.$$

Logo, o inteiro x satisfaz a congruência dada se, e somente se, x deixa resto 6 na divisão por 11, ou seja, $x \in \{..., -27, -16, -5, 6, 17, 28, 39, ...\}$.

EXERCÍCIOS

1. A expressão 51737 + 23678 - 35206, ao ser dividida por 5, deixa que resto?

2. A expressão $51737 \times 23678 + 35207^2$, ao ser dividida por 5, deixa que resto?

3. Encontre o resto de $100 \times 103 \times 104$ na divisão por 7.

4. Encontre o resto de $100^2 \times 102$ na divisão por 9.

5. Encontre o resto de $37^3 \times 2$ na divisão por 3.

6. Encontre o resto de 98×101 na divisão por 11.

7. Achar os restos das divisões de 2^{50} e 41^{65} por 7.

8. Determine o inverso de 11 nos seguintes módulos: 3, 5, 7 e 9.

9. Encontre todos os inteiros x que satisfazem:
a) $2x \equiv 1 \ mod\ 7$
b) $2x \equiv 3 \ mod\ 7$
c) $3x \equiv 9 \ mod\ 13$
d) $5x \equiv 7 \ mod\ 13$

10. (OBM - 98) Qual é o dígito das unidades do número 3^{1998}?
a) 1
b) 3
c) 5
d) 7
e) 9

11. (Colégio Naval) O resto da divisão por 11 do resultado da expressão: $1211^{20} + 9119^{32} \times 343^{26}$, é:
a) 9
b) 1
c) 10
d) 6
e) 7

12. (Colégio Militar - 2011) Dois números inteiros positivos são tais que a divisão do primeiro deles por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa

resto 5. Somando os dois números e dividindo o resultado por 7, o resto será:
a) 1
b) 2
c) 3
d) 4
e) 5

13. (Colégio Naval - 2005) Um número natural N deixa: resto 2 quando dividido por 3; resto 3 quando dividido por 7; e resto 19 quando dividido por 41. Qual é o resto da divisão do número $k = (N+1)(N+4)(N+22)$ por 861?
a) 0
b) 13
c) 19
d) 33
e) 43

AULA 5 - DEFINIÇÃO DE EQUAÇÕES DIOFANTINAS E CONDIÇÃO DE EXISTÊNCIA DE SOLUÇÃO

Plano de aula

Tema: Equações Diofantinas Lineares
Conteúdo: Equações Diofantinas Lineares - definição e condição de existência de solução
Objetivos: Propiciar ao aluno: • Compreender o conceito de equação diofantina linear de duas incógnitas; • Compreender em quais condições uma equação diofantina linear de duas incógnitas admite soluções inteiras; • Mostrar uma das aplicações do conceito de mdc;
Metodologia: Iniciaremos a aula demonstrando a definição formal de uma equação diofantina linear de duas incógnitas. Posteriormente, apresentaremos a condição de existência de solução inteira como uma aplicação do conceito de mdc.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Equações diofantinas lineares de duas incógnitas

Definição: uma equação diofantina linear de duas incógnitas é uma equação da forma $ax + by = c$, onde x, y são as incógnitas e a, b, c são inteiros dados, sendo $ab \neq 0$. Por exemplo, são equações diofantinas lineares de duas incógnitas: $2x + 6y = 24, 4x + 6y = 13, 14x + 22y = 50$ e $2x + 3y = 101$.

Se dois números inteiros x_0, y_0 satisfazem a equação $ax+by = c$, então denomina-se que x_0, y_0 é uma solução inteira da equação diofantina $ax+by = c$. Por exemplo, considere a equação $2x + 6y = 24$. Note que: $2(9) + 6(1) = 24$. Portanto, o par de inteiros, 9 e 1, é solução da equação $2x + 6y = 24$. Agora, considere a equação $4x + 6y = 13$. Note que $4x + 6y$ é um número inteiro par para quaisquer que sejam os valores inteiros de x e y, enquanto 13 é um número inteiro ímpar. Portanto, a equação $4x + 6y = 13$ não tem solução inteira.

- Condição de existência de solução

A equação diofantina linear $ax + by = c$ possui solução x_0, y_0 se, e somente se, d divide c, onde $d = mdc(a, b)$.

Exemplos:

1. A equação $2x + 6y = 24$ possui solução inteira, pois $mdc(6, 2) = 2$ e 2 divide 24.

2. A equação $4x + 6y = 13$ não possui solução inteira, pois $mdc(6, 4) = 2$ e 2 não divide 13.

3. A equação $16x + 9y = 59$ possui solução inteira, pois $mdc(16, 9) = 1$ e 1 divide 59.

EXERCÍCIO

1. Determine quais equações diofantinas lineares de duas incógnitas possuem solução em $\mathbb{Z}$. Em caso afirmativo, determine uma solução.

a) $14x + 22y = 50$
b) $2x + 3y = 101$
c) $13x + 9y = 21$
d) $60x + 48y = 234$
e) $28x + 80y = 44$
f) $5x + 15y = 131$
g) $7x + 11y = 100$
h) $19x + 97y = 1997$
i) $10x + 20y = 203$
j) $13x + 4y = 100$

AULA 6 - SOLUÇÕES GERAIS DE UMA EQUAÇÃO DIOFANTINA

Plano de aula

Tema: Equações Diofantinas Lineares
Conteúdo: Soluções gerais de uma equação diofantina do tipo $ax + by = c$
Objetivos: Propiciar ao aluno: • Resolver eficientemente uma equação diofantina; • Mostrar uma das aplicações das congruências;
Metodologia: Iniciaremos a aula demonstrando como determinar as soluções de uma equação do tipo $ax + by = c$ a partir de uma solução particular x_0, y_0. Posteriormente, mostraremos como determinar a solução particular x_0, y_0 através de uma aplicação das propriedades de congruência.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

- Soluções da equação $ax + by = c$

Seja x_0, y_0 uma solução particular da equação diofantina linear $ax + by = c$, onde $mdc(a, b) = 1$. Então todas as outras soluções desta equação são dadas pelas fórmulas: $x = x_0 + bt$ e $y = y_0 - at$, onde t é um inteiro arbitrário.

Exemplo: Determine a solução geral da equação diofantina $24x + 43y = 117$.

Primeiro, através do algoritmo de Euclides, determina-se o mdc de 43 e 24. Assim, temos

	1	1	3	1	4
43	24	19	5	4	1
19	5	4	1	0	

.

Portanto, como $mdc(43, 24) = 1$ e 1 divide 117, então a equação $24x + 43y = 117$ possui solução inteira. Sendo assim, vamos determinar uma solução particular x_0, y_0 desta equação. Para tal, pela aritmética modular, temos que

$$\begin{cases} 24x \equiv 0 \ mod \ 24 \\ 43y \equiv 19y \ mod \ 24 \\ 117 \equiv 21 \ mod \ 24 \end{cases}$$

e, consequentemente,

$$24x + 43y \equiv 19y \equiv 21 \ mod \ 24.$$

Portanto,

$$19y \equiv 21 \ mod \ 24 \Longleftrightarrow 95y \equiv 105 \ mod \ 24 \Longleftrightarrow -y \equiv 9 \ mod \ 24 \Longleftrightarrow y \equiv -9 \ mod \ 24.$$

Logo, $y_0 = -9$ e $x_0 = \dfrac{117 - 43(-9)}{24} = 21$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 21 + 43t$ e $y = -9 - 24t$, onde t é um número inteiro arbitrário.

EXERCÍCIO

1. Determine a solução geral de cada uma das equações diofantinas abaixo:
a) $10x + 18y = 60$
b) $5x + 3y = 97$
c) $13x + 9y = 37$
d) $72x + 36y = 288$
e) $28x + 92y = 48$
f) $5x + 15y = 130$
g) $7x + 11y = 10$
h) $19x + 97y = 197$
i) $10x + 20y = 1200$
j) $13x + 4y = 79$

AULA 7 - TESTE A POSTERIORI

Plano de aula

Tema: Teste a posteriori
Conteúdo: Equações Diofantinas Lineares
Objetivos: Propiciar ao aluno: • Estudar aplicações das equações diofantinas na resolução de situações problemas
Metodologia: Os alunos terão 50 minutos para resolver cada situação problema do teste. Espera-se que eles utilizem o método aritmético modular apresentado no decorrer das aulas para determinar as soluções.
Avaliação: cada discente será avaliado através da participação na resolução dos exercícios.
Recursos didáticos: Quadro branco e pincel.
Duração: dois tempos de 50 minutos cada

PROBLEMA DOS REFRIGERANTES

Uma pessoa resolve comprar refrigerantes para o almoço em família de domingo. Chegando ao mercado, essa pessoa percebe que só havia duas opções de refrigerantes disponíveis: Coca-Cola, cujo preço é R$ 5,00, e Guaraná Antarctica R$ 4,00.
a) se essa pessoa deseja gastar R$ 100,00, qual é o número de opções que ela dispõe para

fazer a compra dos refrigerantes?
b) qual é o número máximo de refrigerantes que ela pode comprar gastando R$ 100,00?
c) E o número mínimo?

PROBLEMA DO ESTACIONAMENTO

Em um estacionamento no centro de uma cidade tinham estacionados apenas carros e motos. Um garagista notou que existiam 30 rodas.
a) qual é o número de opções de carros e motos que podem existir no estacionamento?
b) qual é o número máximo de carros?
c) e o número mínimo?
d) qual é o número de carros e motos, sabendo que a diferença entre esses dois números é a menor possível?

Experimentação da sequência didática

Durante a experimentação da sequência didática do método aritmético modular foram aplicadas sete aulas de duração de dois tempos de 50 minutos cada, onde foram recolhidos dados para uma análise a posteriori e, consequentemente, sua validação.

- **1° aula - Teste a Priori**

Nesta aula, as situações problema foram resolvidas de forma individual e os registros foram armazenados para serem comparados aos registros obtidos na última aula (Teste a Posteriori).

Os alunos tiveram dificuldades em encontrar todas as opções desejadas e, sem saber uma forma mais efetiva de resolver os problemas, recorreram ao método da tentativa e erro. Além disso, os alunos foram capazes de notar que no cotidiano podem se deparar com esse tipo de situação.

PROBLEMA DO SAQUE BANCÁRIO

Uma pessoa resolve sacar uma quantia em espécie. Chegando no caixa eletrônico em uma agência bancária, essa pessoa percebe que só havia duas opções de notas disponíveis: R$ 5,00 e R$ 20,00.
a) se essa pessoa deseja sacar R$ 150,00, qual é o número de opções que ela dispõe para fazer o saque?
Solução: Seja x a quantidades de notas de R$5,00 e y a quantidades de notas de R$20,00.

Assim, temos $5x + 20y = 150$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 5 e 20. Assim, temos

$$\begin{array}{c|c} & 4 \\ \hline 20 & 5 \\ \hline 0 & \end{array}.$$

Portanto, como $mdc(5, 20) = 5$ e 5 divide 150, então a equação $5x + 20y = 150$ possui solução inteira. Dividindo amobos os membros da equação por $mdc(5, 20) = 5$, obtemos a equação equivalente $x + 4y = 30$. Sendo assim, vamos determinar uma solução particular x_0, y_0 desta equação. Para tal, pela aritmética modular, temos que

$$\begin{cases} x \equiv x \ mod\ 4 \\ 4y \equiv 0 \ mod\ 4 \\ 30 \equiv 2 \ mod\ 4 \end{cases}$$

e, consequentemente,

$$x + 4y \equiv x \equiv 2 \ mod\ 4.$$

Portanto, $x \equiv 2 \ mod\ 4$. Logo, $x_0 = 2$ e $y_0 = \dfrac{30-2}{4} = 7$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 2 + 4t$ e $y = 7 - t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de notas de R\$5,00 e R\$20,00, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $0 \leq t \leq 7$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 8 opções de saque dispostos na tabela a seguir:

Número de opções	Notas de R$ 20,00	Notas de R$ 5,00
1°	0	30
2°	1	26
3°	2	22
4°	3	18
5°	4	14
6°	5	10
7°	6	6
8°	7	2

b) qual é o número máximo de notas que ela pode receber ao efetuar o saque de R$ 150,00?

Resposta: 30 notas, sendo 0 notas de R$ 20,00 e 30 notas de R$ 5,00.

c) e o número mínimo de notas?

Resposta: 9 notas, sendo 7 notas de R$ 20,00 e 2 notas de R$ 5,00.

PROBLEMA DO PARQUE DE DIVERSÃO

André, pai de Ana e Carlos, resolve agradar seus filhos levando-os a um parque de diversão. Chegando ao parque, André dá a cada um dos filhos uma quantia de R$ 100,00. Ana e Carlos ao chegarem no caixa para comprar os bilhetes percebem que havia duas opções: R$ 3,00 e R$ 7,00.

a) qual é o número de opções que Ana e Carlos dispõem para fazer a compra dos bilhetes?

Solução: Seja x a quantidade de bilhetes de R$3,00 e y a quantidade de bilhetes de R$7,00. Assim, temos $3x + 7y = 100$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 3 e 7. Assim, temos

$$\begin{array}{c|c|c} & 2 & 3 \\ \hline 7 & 3 & 1 \\ \hline 1 & 0 & \end{array}.$$

Portanto, como $mdc(3, 7) = 1$ e 1 divide 100, então a equação $3x+7y = 100$ possui solução inteira. Sendo assim, vamos determinar uma solução particular x_0, y_0 desta equação. Para tal, pela aritmética modular, temos que

$$\begin{cases} 3x \equiv 0 \ mod \ 3 \\ 7y \equiv y \ mod \ 3 \\ 100 \equiv 1 \ mod \ 3 \end{cases}$$

e, consequentemente,

$$3x + 7y \equiv y \equiv 1 \ mod \ 3.$$

Portanto, $y \equiv 1 \ mod \ 3$. Logo, $y_0 = 1$ e $x_0 = \dfrac{100 - 7}{3} = 31$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 31 + 7t$ e $y = 1 - 3t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de bilhetes de R$3,00 e R$7,00, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $-4 \leq t \leq 0$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 5 opções de compra de bilhetes dispostos na tabela a seguir:

Número de opções	Bilhetes de R$ 3,00	Bilhetes de R$ 7,00
1°	31	1
2°	24	4
3°	17	7
4°	10	10
5°	3	13

b) qual é o número máximo de bilhetes que cada um pode comprar?
Resposta: 32 bilhetes, sendo 31 bilhetes de R$ 3,00 e 1 bilhete de R$ 7,00.

c) e o número mínimo de bilhetes?
Resposta: 16 bilhetes, sendo 3 bilhetes de R$ 3,00 e 13 bilhetes de R$ 7,00.

Para avaliação dos resultados obtidos no Teste a Priori adotamos um conceito em relação ao número de acertos obtido pelo aluno no item a) de cada um dos problemas propostos, usando o seguinte critério:

1. Problema do Saque Bancário

   - Adotamos conceito A aos alunos que determinaram as 8 opções de saque;
   - Adotamos conceito B aos alunos que determinaram entre 5 e 7 opções de saque;
   - Adotamos conceito C aos alunos que determinaram entre 1 e 4 opções de saque;
   - Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de saque;

2. Problema do Parque de Diversão

   - Adotamos conceito A aos alunos que determinaram as 5 opções de compra de bilhetes;
   - Adotamos conceito B aos alunos que determinaram 3 ou 4 opções de compra de bilhetes;
   - Adotamos conceito C aos alunos que determinaram 1 ou 2 opções de compra de bilhetes;
   - Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de compra de bilhetes;

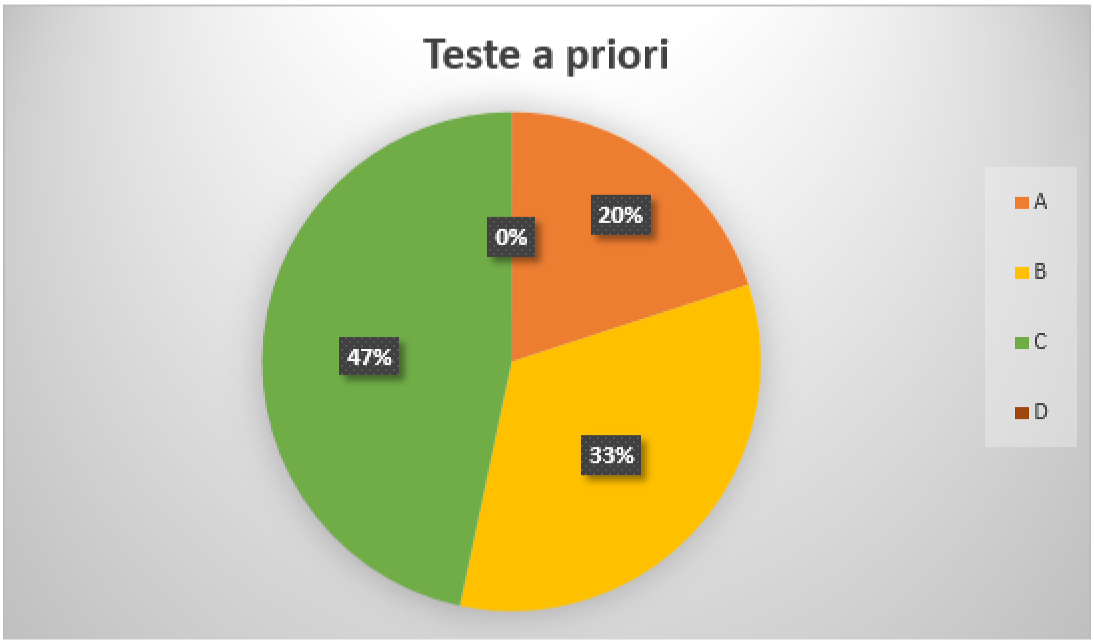
Tal critério esta sintetizado na seguinte tabela:

Conceito	Número de acertos	
	Problema do saque bancário	Problema do parque de diversão
A	8	5
B	5 - 7	3 - 4
C	1 - 4	1 - 2
D	0	0

A seguir, apresentamos a quantidade de alunos que obtiveram os conceitos A, B, C e D nos problemas supracitados.

Conceito	Número de alunos	
	Problema do saque bancário	Problema do parque de diversão
A	6	6
B	10	11
C	14	13
D	0	0
Total	30	30

Como o número de alunos que alcançaram os conceitos A, B, C e D foram basicamente os mesmos para ambos problemas, então para ilustrar os dados obtidos elaboramos o gráfico a seguir baseados nos conceitos que os alunos obtiveram no problema do saque bancário.



- **2° aula - Revisão de MDC**

Na segunda aula efetuou-se uma revisão sobre o conceito de máximo divisor comum e sobre um método para a sua determinação: método das divisões sucessivas, conhecido como algoritmo de Euclides. Além disso, foram propostos alguns exercícios onde os alunos puderam aplicar o algoritmo de Euclides para determinar o mdc e, consequentemente, encontrar a resposta.

Nesta aula, os alunos relataram que tal revisão foi de grande relevância para a continuidade dos estudos, pois eles puderam ter contato com um conceito simples que lhes fora ensinado nos anos iniciais do segundo segmento do ensino fundamental (6° ano) e que tinha sido deixado de lado nos anos posteriores. Além disso, um aluno relatou que estava pensando de que maneira o mdc poderia nos levar a determinar alguma solução das situações-problema apresentadas no Teste a Priori.

- **3° aula - Aritmética modular: congruência**

Na terceira aula apresentou-se a definição de congruência, conceito que eles desconheciam, e algumas propriedades que seriam necessárias para se determinar as soluções gerais de uma equação diofantina linear.

Nesta aula, devido a ser um conceito novo, os alunos contaram ter dificuldades em compreender a ideia cíclica envolvendo os restos, mas, depois da resolução dos exercícios, os alunos conseguiram entender melhor.

- **4° aula - Aritmética modular: aplicações das propriedades de congruência**

Na quarta aula efetuou-se a aplicação de algumas propriedades de congruência através da resolução de alguns exemplos. Posteriormente, foram propostos alguns exercícios onde os alunos puderam aplicar os conhecimentos adquiridos.

Nesta aula, os alunos comentaram que, devido a resolução dos exemplos, puderam compreender o que tinha sido apresentado na aula anterior. Além disso, comentaram não ter maiores dificuldades para resolver os exercícios propostos.

- **5° aula - Definição de equações diofantinas**

Na quinta aula apresentou-se a definição de uma equação diofantina linear de duas incógnitas. Ademais, mostrou-se em quais condições tais equações admitem soluções inteiras, correlacionando o mdc dos coeficientes com o termo independente e apresentando, assim, uma das possíveis aplicações do conceito de mdc.

Nesta aula, os alunos relataram ter uma certa dificuldade de entender a definição de uma equação diofantina linear, mas conforme foi apresentado os exercícios eles conseguiram entender melhor. Além disso, com a elucidação da condição de existência de solução das equações diofantinas, ficou esclarecido para os alunos a importância da aula de revisão de mdc e do algoritmo de Euclides.

- **6° aula - Soluções gerais de uma equação diofantina**

Na sexta aula mostrou-se como determinar as soluções gerais de uma equação diofantina a partir de uma solução particular x_0, y_0. Para tal, foram aplicadas as propriedades de aritmética modular para explicitação da solução particular x_0, y_0, apresentando, assim, uma das possíveis aplicações de congruências. Além disso, foram propostos alguns exercícios onde os alunos puderam aplicar os conhecimentos adquiridos.

Nesta aula, os alunos narraram que, inicialmente, tiveram dificuldades em entender como utilizar as propriedades de congruências para determinar a solução particular x_0, y_0, mas, com a resolução dos exercícios, essas dúvidas foram sanadas. Além disso, comentaram que foi interessante aprender uma nova forma de determinar todas as soluções de uma equação diofantina e, assim, poderiam resolver problemas do cotidiano de forma simples e ágil.

- **7° aula - Teste a Posteriori**

Na última aula desta sequência didática, os alunos tiveram contato novamente com a resolução de situações do cotidiano. Nesta aula, as situações-problema foram resolvidas de forma individual e os registros foram armazenados para serem comparados aos registros obtidos na primeira aula (Teste a Priori).

Como já era esperado, a maior parte dos alunos não encontrou maiores dificuldades para determinar de forma satisfatória as soluções dos problemas propostos, pois utilizaram o método aritmético modular, apresentado no decorrer das aulas da sequência didática, para resolver tais situações-problema. Além disso, notaram que, em consequência das informações apresentadas nos enunciados, apenas algumas soluções inteiras atenderiam as situações-problema.

PROBLEMA DOS REFRIGERANTES

Uma pessoa resolve comprar refrigerantes para o almoço em família de domingo. Chegando ao mercado, essa pessoa percebe que só havia duas opções de refrigerantes disponíveis: marca A, cujo preço é R\$4,00, e marca B, cujo preço é R\$5,00.

a) se essa pessoa deseja gastar R\$ 100,00, qual é o número de opções que ela dispõe para fazer a compra dos refrigerantes?

Solução: Seja x a quantidade de refrigerantes da marca A e y a quantidade de refrigerantes da marca B. Assim, temos $4x + 5y = 100$. Primeiro, através do algoritmo de Euclides, determina-se o mdc de 4 e 5. Assim, temos

$$\begin{array}{c|c|c} & 1 & 4 \\ \hline 5 & 4 & 1 \\ \hline 1 & 0 & \end{array}.$$

Portanto, como $mdc(4,5) = 1$ e 1 divide 100, então a equação $4x+5y = 100$ possui solução inteira. Sendo assim, vamos determinar uma solução particular x_0, y_0 desta equação. Para tal, pela aritmética modular, temos que

$$\begin{cases} 4x \equiv 0 \; mod \; 4 \\ 5y \equiv y \; mod \; 4 \\ 100 \equiv 0 \; mod \; 4 \end{cases}$$

e, consequentemente,

$$4x + 5y \equiv y \equiv 0 \; mod \; 4.$$

Portanto, $y \equiv 0 \; mod \; 4$. Logo, $y_0 = 0$ e $x_0 = \dfrac{100}{4} = 25$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 25+5t$ e $y = 0-4t = -4t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de refrigerantes das marcas A e B, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $-5 \leq t \leq 0$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 6 opções de compra de refrigerantes dispostos na tabela a seguir:

Número de opções	marca A	marca B
1°	25	0
2°	20	4
3°	15	8
4°	10	12
5°	5	16
6°	0	20

b) qual é o número máximo de refrigerantes que ela pode comprar gastando R$ 100,00?
Resposta: 25 refrigerantes, sendo 25 refrigerantes da marca A e 0 refrigerantes da marca B.

c) E o número mínimo?
Resposta: 20 refrigerantes, sendo 0 refrigerantes da marca A e 20 refrigerantes da marca B.

PROBLEMA DO ESTACIONAMENTO

Em um estacionamento no centro de uma cidade tinham estacionados apenas carros e motos. Um garagista notou que existiam 30 rodas.
a) qual é o número de opções de carros e motos que podem existir no estacionamento?
Solução: Seja x a quantidade de motos e y a quantidade de carros. Assim, temos

$2x + 4y = 30$. Primeiro, através do algoritmo de Euclides, determina-se o *mdc* de 2 e 4. Assim, temos

$$\begin{array}{c|c} & 2 \\ \hline 4 & 2 \\ \hline 0 & \end{array}.$$

Portanto, como $mdc(2,4) = 2$ e 2 divide 30, então a equação $2x + 4y = 30$ possui solução inteira. Dividindo ambos os membros da equação por $mdc(2,4) = 2$, obtemos a equação equivalente $x + 2y = 15$. Sendo assim, vamos determinar uma solução particular x_0, y_0 desta equação. Para tal, pela aritmética modular, temos que

$$\begin{cases} x \equiv x \ mod \ 2 \\ 2y \equiv 0 \ mod \ 2 \\ 15 \equiv 1 \ mod \ 2 \end{cases}$$

e, consequentemente,

$$x + 2y \equiv x \equiv 1 \ mod \ 2.$$

Portanto, $x \equiv 1 \ mod \ 2$. Logo, $x_0 = 1$ e $y_0 = \dfrac{15-1}{2} = 7$ é uma solução particular e, por conseguinte, todas as demais soluções são dadas pelas fórmulas: $x = 1 + 2t$ e $y = 7 - t$, onde t é um número inteiro arbitrário. Como x e y representam as quantidades de motos e carros, respectivamente, então tem-se $x \geq 0$ e $y \geq 0$ e, consequentemente, $0 \leq t \leq 7$.

Resposta: Tendo assim a certeza de não haver esquecido nenhuma solução apresentamos as 8 opções de carros e motos no estacionamento dispostos na tabela a seguir:

Número de opções	Número de carros	Número de motos
1°	0	15
2°	1	13
3°	2	11
4°	3	9
5°	4	7
6°	5	5
7°	6	3
8°	7	1

b) qual é o número máximo de carros?
Resposta: 7 carros.

c) e o número mínimo?
Resposta: 0 carros.

d) qual é o número de carros e motos, sabendo que a diferença entre esses dois números é a menor possível?
Resposta: 5 carros e 5 motos, pois a diferença entre esses dois números é zero.

Para avaliação dos resultados obtidos no Teste a Posteriori adotamos um conceito em relação ao número de acertos obtido pelo aluno no item a) de cada um dos problemas propostos, usando o seguinte critério:

1. Problema dos Refrigerantes

   - Adotamos conceito A aos alunos que determinaram as 6 opções de compra;
   - Adotamos conceito B aos alunos que determinaram 4 ou 5 opções de compra;
   - Adotamos conceito C aos alunos que determinaram entre 1 e 3 opções de compra;
   - Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de compra;

2. Problema do Estacionamento

   - Adotamos conceito A aos alunos que determinaram as 8 opções de carros e motos;
   - Adotamos conceito B aos alunos que determinaram entre 5 e 7 opções de carros e motos;
   - Adotamos conceito C aos alunos que determinaram entre 1 e 4 opções de carros e motos;
   - Adotamos conceito D aos alunos que não conseguiram determinar nenhuma das opções de carros e motos;

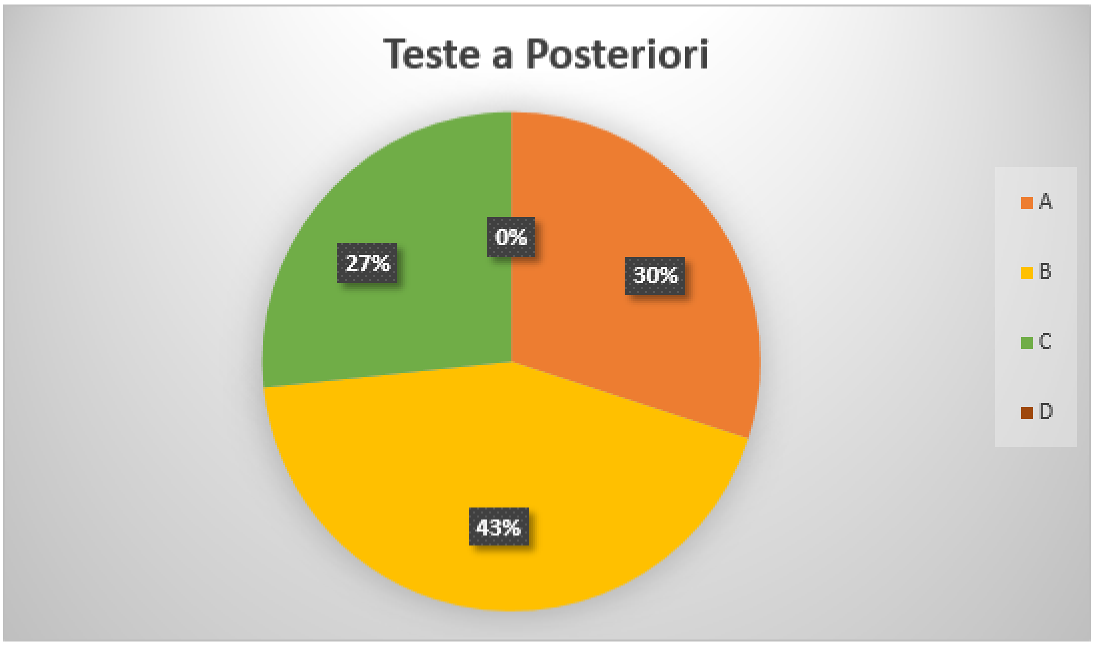
Tal critério esta sintetizado na seguinte tabela:

Conceito	Número de acertos	
	Problema dos refrigerantes	Problema do estacionamento
A	6	8
B	4 - 5	5 - 7
C	1 - 3	1 - 4
D	0	0

A seguir, apresentamos a quantidade de alunos que obtiveram os conceitos A, B, C e D nos problemas supracitados.

Conceito	Número de alunos	
	Problema dos refrigerantes	Problema do estacionamento
A	9	9
B	13	11
C	8	10
D	0	0
Total	30	30

Como o número de alunos que alcançaram os conceitos A, B, C e D foram basicamente os mesmos para ambos problemas, então para ilustrar os dados obtidos elaboramos o gráfico a seguir baseados nos conceitos que os alunos obtiveram no problema dos refrigerantes.



3.4 Análise a posteriori e validação

A quarta e última fase da Engenharia Didática, denominada análise a posteriori e validação, tem como objetivo examinar os dados adquiridos durante a experimentação das sequências didática para, assim, elaborar a análise a posteriori e, consequentemente, verificar a validação interna do objeto de pesquisa, pois esta se constitui na comparação entre análise a priori e a análise a posteriori.

3.4.1 Análise a posteriori

Confrontando os dados obtidos no Teste a Priori com o Teste a Posteriori temos:

- **Método algébrico**

1. Dois alunos foram capazes de solucionar os problemas propostos no Teste a Priori, enquanto que cinco alunos resolveram as situações-problema do Teste a Posteriori. Sendo assim, deu-se um progresso de 150%.

2. Três alunos foram capazes de acertar mais da metade das soluções possíveis dos problemas propostos no Teste a Priori, enquanto que sete alunos acertaram mais da metade das soluções possíveis das situações-problema do Teste a Posteriori. Desta maneira, ocorreu um crescimento em torno de 133%.

3. Quinze alunos foram capazes de determinar menos da metade das soluções dos problemas propostos no Teste a Priori, enquanto que oito alunos determinaram menos da metade das soluções as situações-problema do Teste a Posteriori. Portanto, verificou-se um decrescimento aproximado de 47%, o que representa uma evolução tendo em vista que este alunos passaram a encontrar um número maior de soluções possíveis após a aplicação da sequência didática.

4. Dos vinte alunos que fizeram o Teste a Priori, cinco conseguiram resolver de forma satisfatória os problemas propostos e, após a experimentação da sequência didática, doze alunos foram capazes de resolver de forma satisfatória as situações-problema do Teste a Posteriori. Isso configura uma evolução de 140% em relação a quantidade inicial de alunos que conseguiram resolver de forma satisfatória o teste inicial.

- **Método aritmético modular**

1. Seis alunos foram capazes de solucionar os problemas propostos no Teste a Priori, enquanto que nove alunos resolveram as situações-problema do Teste a Posteriori. Sendo assim, deu-se um progresso de 50%.

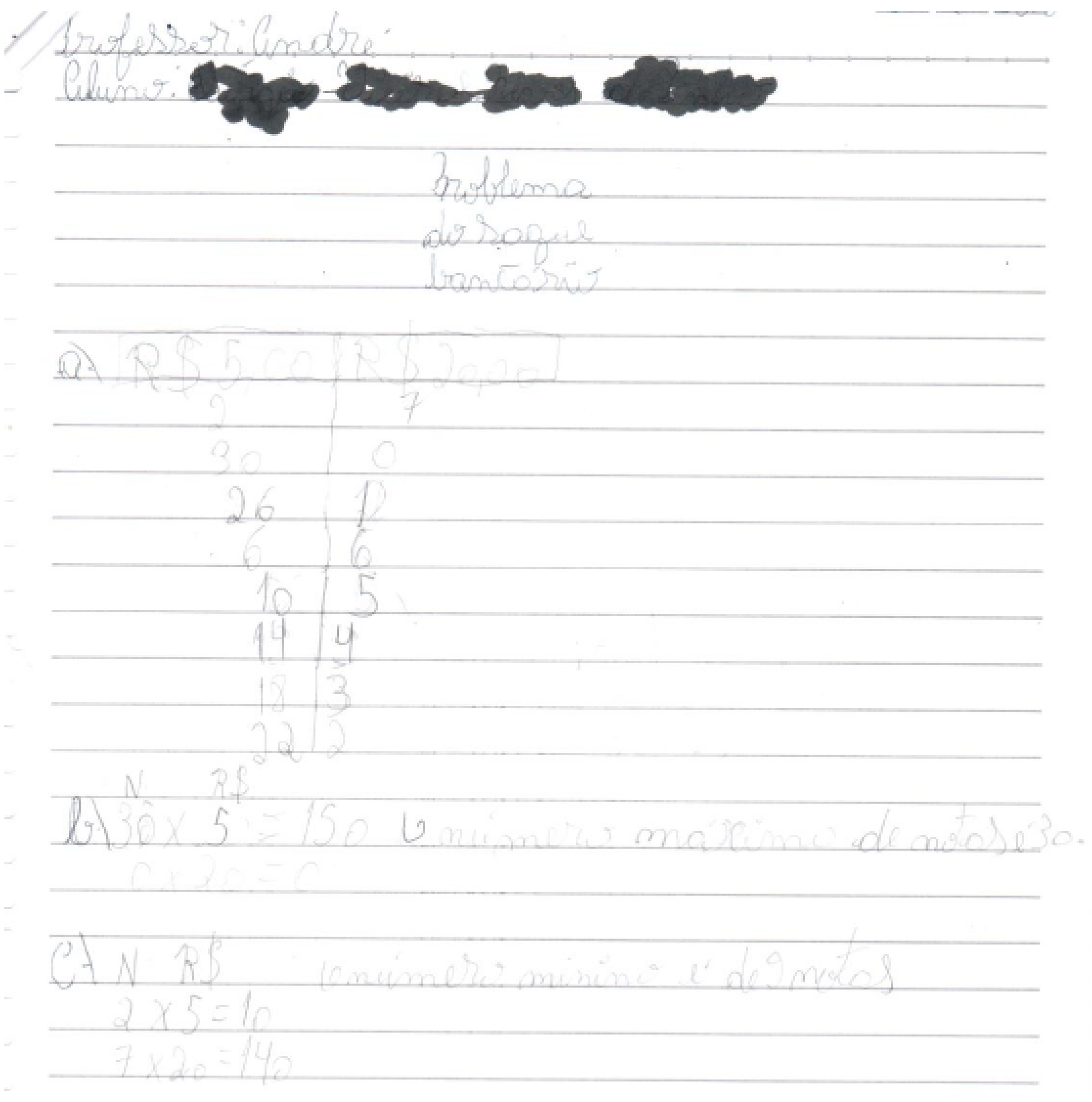
2. Dez alunos foram capazes de acertar mais da metade das soluções possíveis dos problemas propostos no Teste a Priori, enquanto que treze alunos acertaram mais da metade das soluções possíveis das situações-problema do Teste a Posteriori. Desta maneira, ocorreu um crescimento em torno de 30%.

3. Quatorze alunos foram capazes de determinar menos da metade das soluções dos problemas propostos no Teste a Priori, enquanto que oito alunos determinaram menos da metade das soluções as situações-problema do Teste a Posteriori. Portanto, verificou-se um decrescimento aproximado de 43%, o que representa uma evolução tendo em vista que este alunos passaram a encontrar um número maior de soluções possíveis após a aplicação da sequência didática.

4. Dos trinta alunos que fizeram o Teste a Priori, dezesseis conseguiram resolver de forma satisfatória os problemas propostos e, após a experimentação da sequência didática, vinte e dois alunos foram capazes de resolver de forma satisfatória as situações-problema do Teste a Posteriori. Isso simboliza uma evolução de 37,5% em relação a quantidade inicial de alunos que conseguiram resolver de forma satisfatória o teste inicial.

De maneira geral, dos 50 alunos que participaram desta pesquisa tivemos 21 alunos resolvendo de forma satisfatória o Teste a Priori e, posteriormente a aplicação das sequências didática, 34 alunos solucionaram de forma satisfatória o Teste a Posteriori. Isso representa uma evolução aproximadamente de 62% em relação a quantidade inicial de alunos que conseguiram resolver de forma satisfatória o teste inicial.

Ademais, é pertinente a avaliação de alguns registros individuais. As Figuras 3.1 e 3.2 representam o registro do Teste a Priori de um aluno X. Este aluno respondeu corretamente os itens a, b e c dos problemas do saque bancário e do parque de diversões e construiu uma tabela no item a de ambos os problemas para melhor expor os dados. Para chegar a tais respostas o aluno X utilizou o método da tentativa e erro.



Professor: André
Aluno: [redacted]

Problema do saque bancário

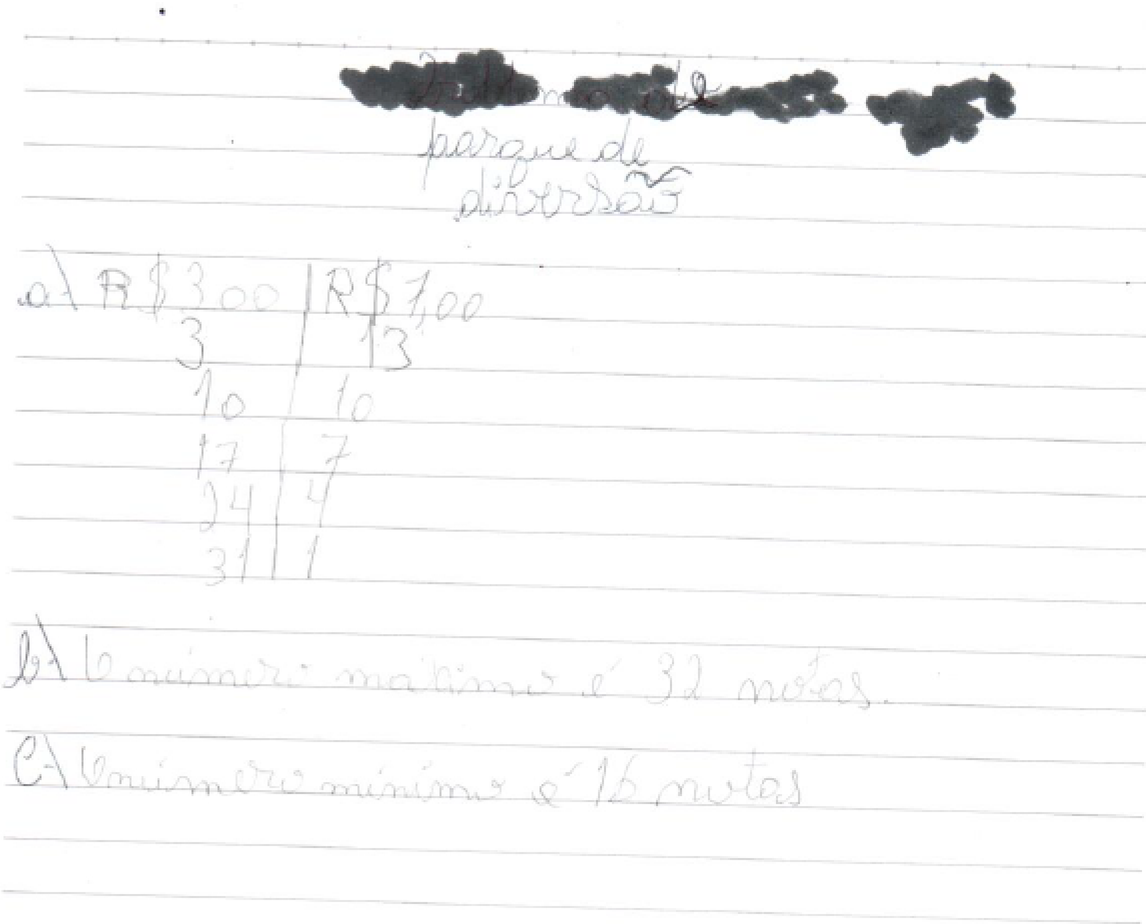
a)

R$ 5,00	R$ 20,00
2	7
30	0
26	1
6	6
10	5
14	4
18	3
22	2

N R$
b) 30 x 5 = 150 o número máximo de notas é 30.
0 x 20 = 0

c) N R$ o número mínimo é de 9 notas
2 x 5 = 10
7 x 20 = 140

Figura 3.1: Registro do aluno X para o problema do saque bancário


[redacted] parque de diversão

a) R$ 3,00 | R$ 1,00

R$ 3,00	R$ 1,00
3	13
10	10
17	7
24	4
31	1

b) O número máximo é 32 notas.

c) O número mínimo é 16 notas

Figura 3.2: Registro do aluno X para o problema do parque de diversões

Agora, apresenta-se um registro (Figuras 3.3 e 3.4) de um aluno Y que conseguiu acertar o primeiro problema proposto do Teste a Posteriori tendo determinado as soluções gerais $x = 100 + 4t$ e $y = -100 - 5t$, para t inteiro, do problema dos refrigerantes através do método algébrico, explicitando os possíveis valores do parâmetro t: $-25 \leq t \leq -20$. Já, no problema do estacionamento, o aluno não conseguiu determinar todas as opções desejadas, pois não simplificou a equação diofantina $4x + 2y = 30$ pelo $mdc(4, 2) = 2$.

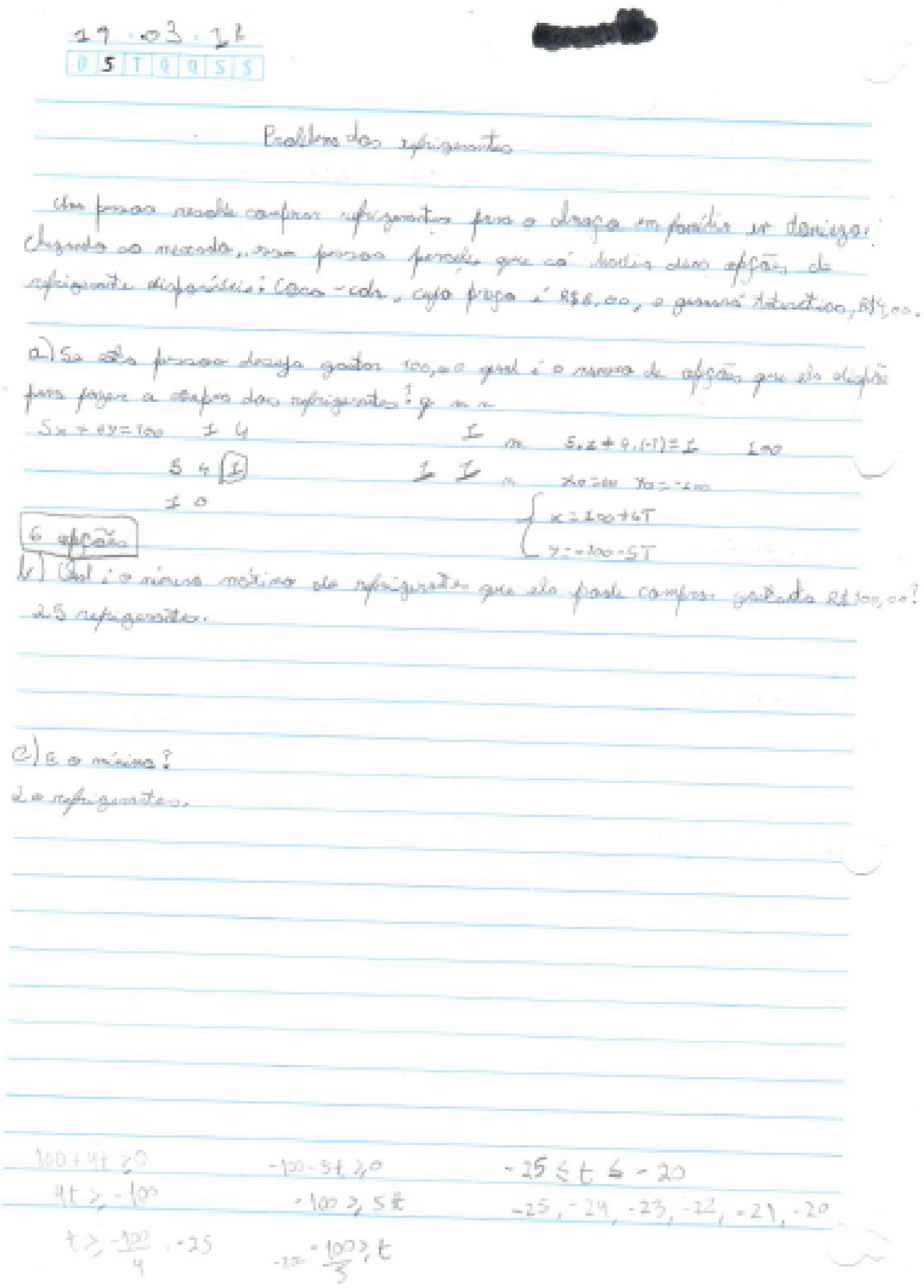
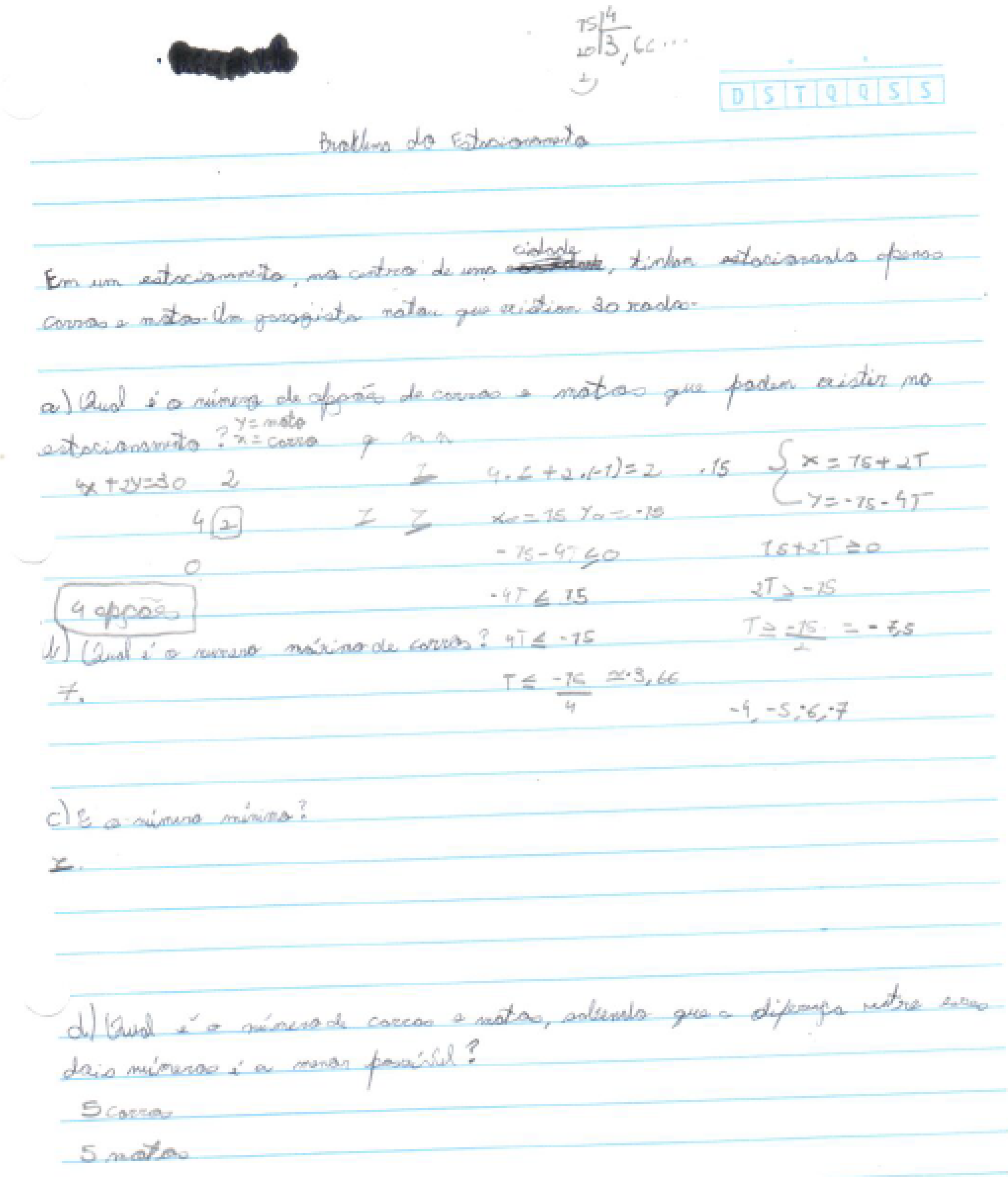


Figura 3.3: Registro do aluno Y aplicando o método algébrico


[redacted]

Problema do Estacionamento

Em um estacionamento, no centro de uma cidade, tinha estacionado apenas carros e motos. Um garagista notou que existiam 30 rodas.

a) Qual é o número de opções de carros e motos que podem existir no estacionamento? y = moto x = carro

4x + 2y = 30

x = 15 + 2T

y = -15 - 4T

4 opções

b) Qual é o número máximo de carros?

7.

c) E o número mínimo?

1.

d) Qual é o número de carros e motos, sabendo que a diferença entre esses dois números é a menor possível?

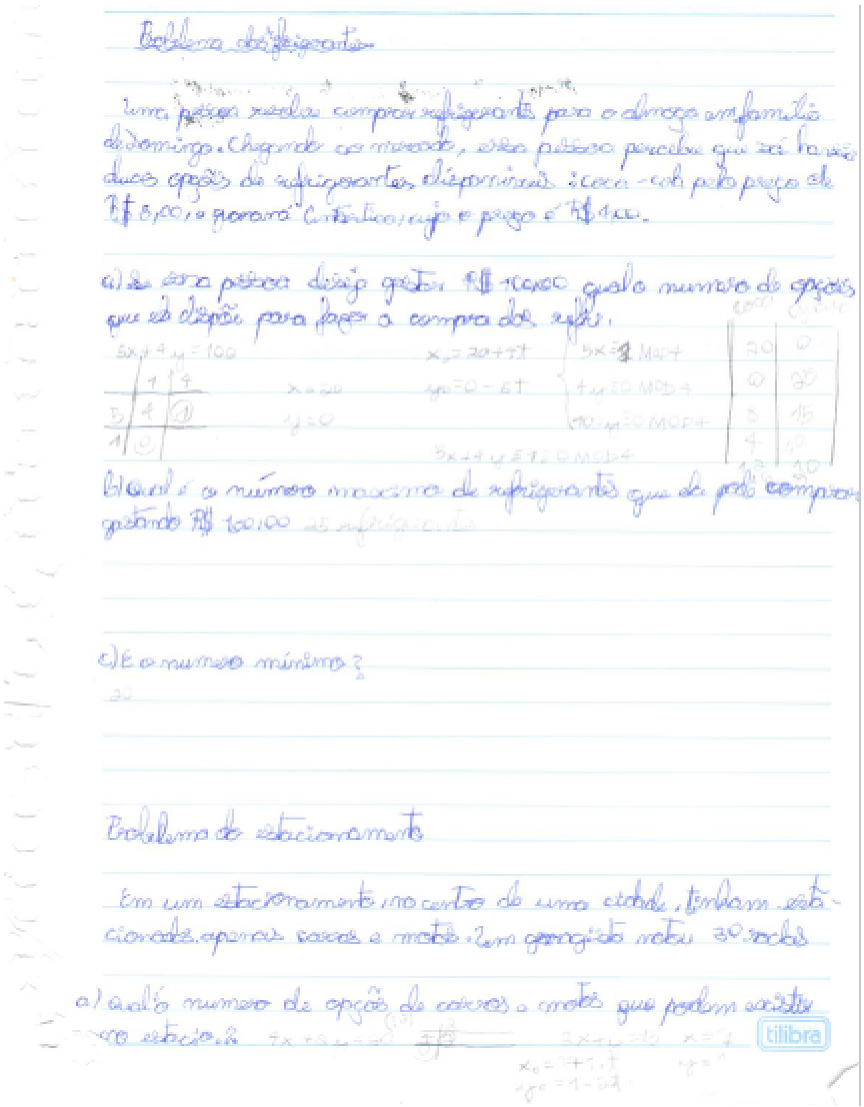
5 carros

5 motos

Figura 3.4: Registro do aluno Y aplicando o método algébrico

Neste outro registro (Figuras 3.5 e 3.6), o aluno Z conseguiu acertar o primeiro problema proposto do Teste a Posteriori tendo determinado as soluções gerais $x = 20 + 4t$ e $y = -5t$, para t inteiro, do problema dos refrigerantes através do método aritmético modular, explicitando os possíveis valores de x e y através de uma tabela.

Já, no problema do estacionamento, o aluno Z conseguiu determinar todas as opções desejadas, pois lembrou-se de simplificar a equação diofantina $4x + 2y = 30$ pelo $mdc(4, 2) = 2$, obtendo a equação equivalente $2x + y = 15$. Sendo assim, determinou as soluções gerais a partir da solução particular $x_0 = 7$ e $y_0 = 1$.


Problema dos refrigerantes

Uma pessoa resolve comprar refrigerantes para o almoço em família de Domingo. Chegando ao mercado, essa pessoa percebe que só haviam duas opções de refrigerantes disponíveis: coca-cola pelo preço de R$ 5,00, e guaraná Antártica, cujo o preço é R$ 4,00.

a) Se essa pessoa deseja gastar R$ 100,00 qual o numero de opções que ela dispõe para fazer a compra dos refris.

b) Qual é o número maximo de refrigerantes que se pode comprar gastando R$ 100,00 25 refrigerantes

c) E o numero mínimo?
20

Problema do estacionamento

Em um estacionamento no centro de uma cidade, tinham estacionados apenas carros e motos. Um garagista notou 30 rodas

a) Qual o numero de opções de carros e motos que podem existir no estacio.?

Figura 3.5: Registro de um aluno Z aplicando o método aritmético modular

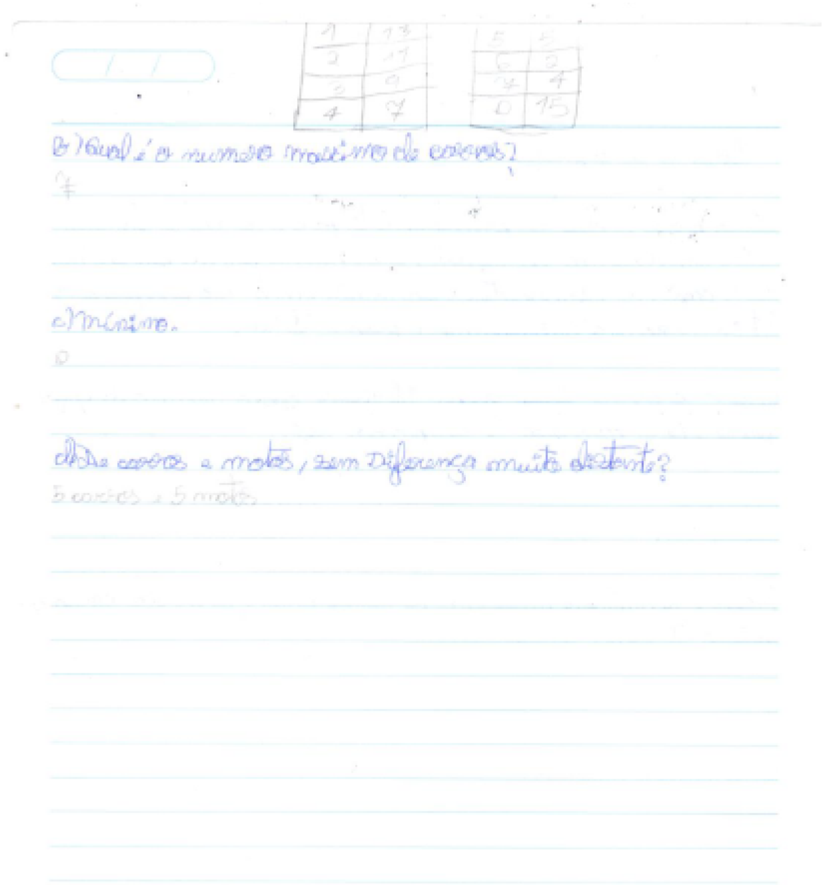


Figura 3.6: Registro de um aluno Z aplicando o método aritmético modular

A Figura 3.7 e as Figuras 3.8 e 3.9 representam o registro do Teste a Priori e o registro do Teste a Posteriori, respectivamente, de um aluno W. Analisando o Teste a Priori deste aluno tem-se que o mesmo determinou 3 opções de saque para o primeiro problema e 2 opções de compra de bilhetes para o segundo problema. Sendo assim, obteve um conceito C no Teste a Priori.

Agora, analisando o Teste a Posteriori deste aluno tem-se que o mesmo foi capaz de determinar as soluções gerais $x = 100+4t$ e $y = -100-5t$, para t inteiro, do problema dos refrigerantes e $x = 30+2t$ e $y = -30-4t$, para t inteiro, do problema do estacionamento. Como não explicitou os possíveis valores do parâmetro t, este aluno obteve um conceito B no Teste a Posteriori. Contudo, devido a experimentação da sequência didática, pode-se observar uma evolução significativa deste aluno na resolução de situações-problema que abranjam as equações diofantinas linerares.

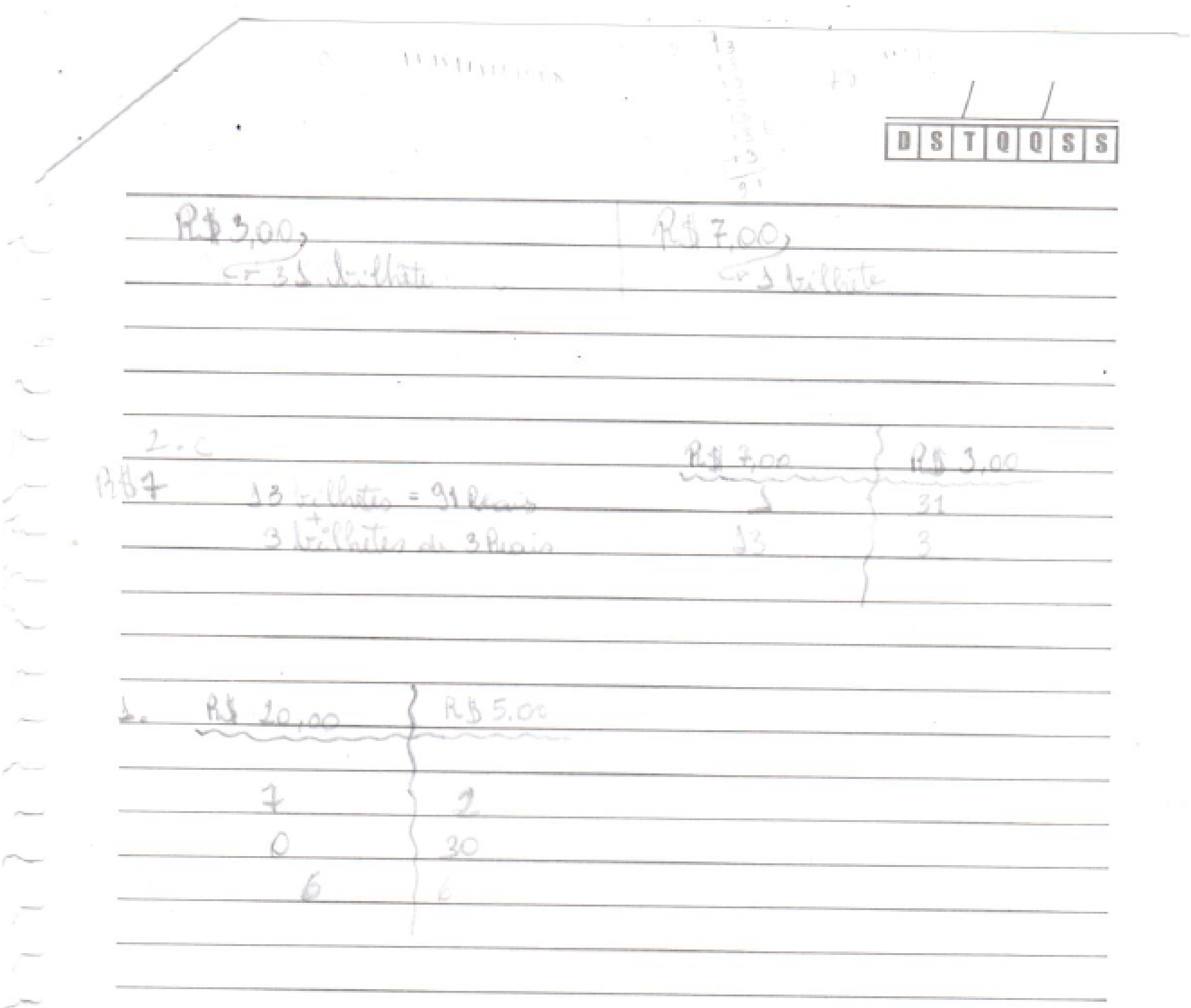


Figura 3.7: Registro do Teste a Priori de um aluno W

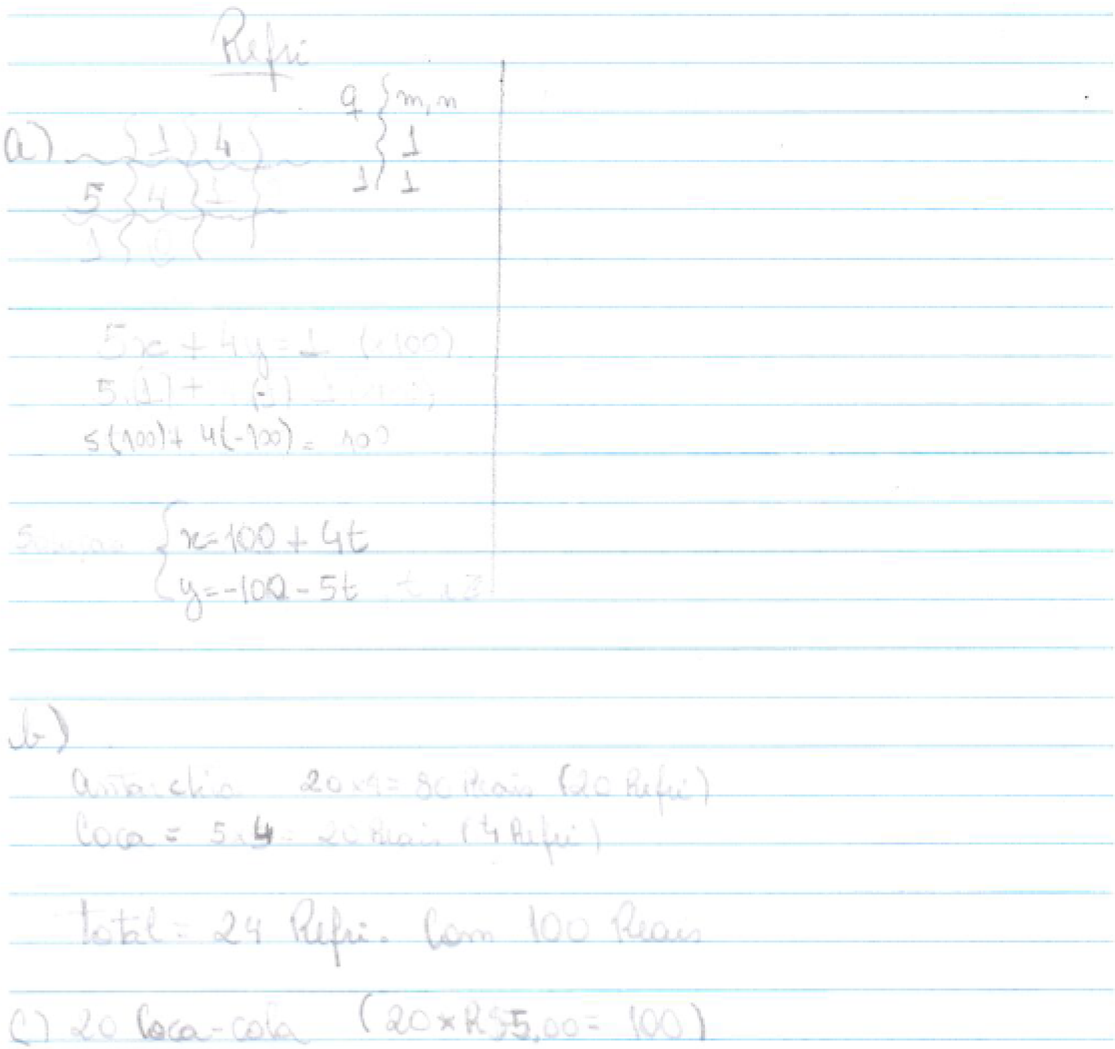


Figura 3.8: Registro do Teste a Posteriori de um aluno W - problema dos refrigerantes

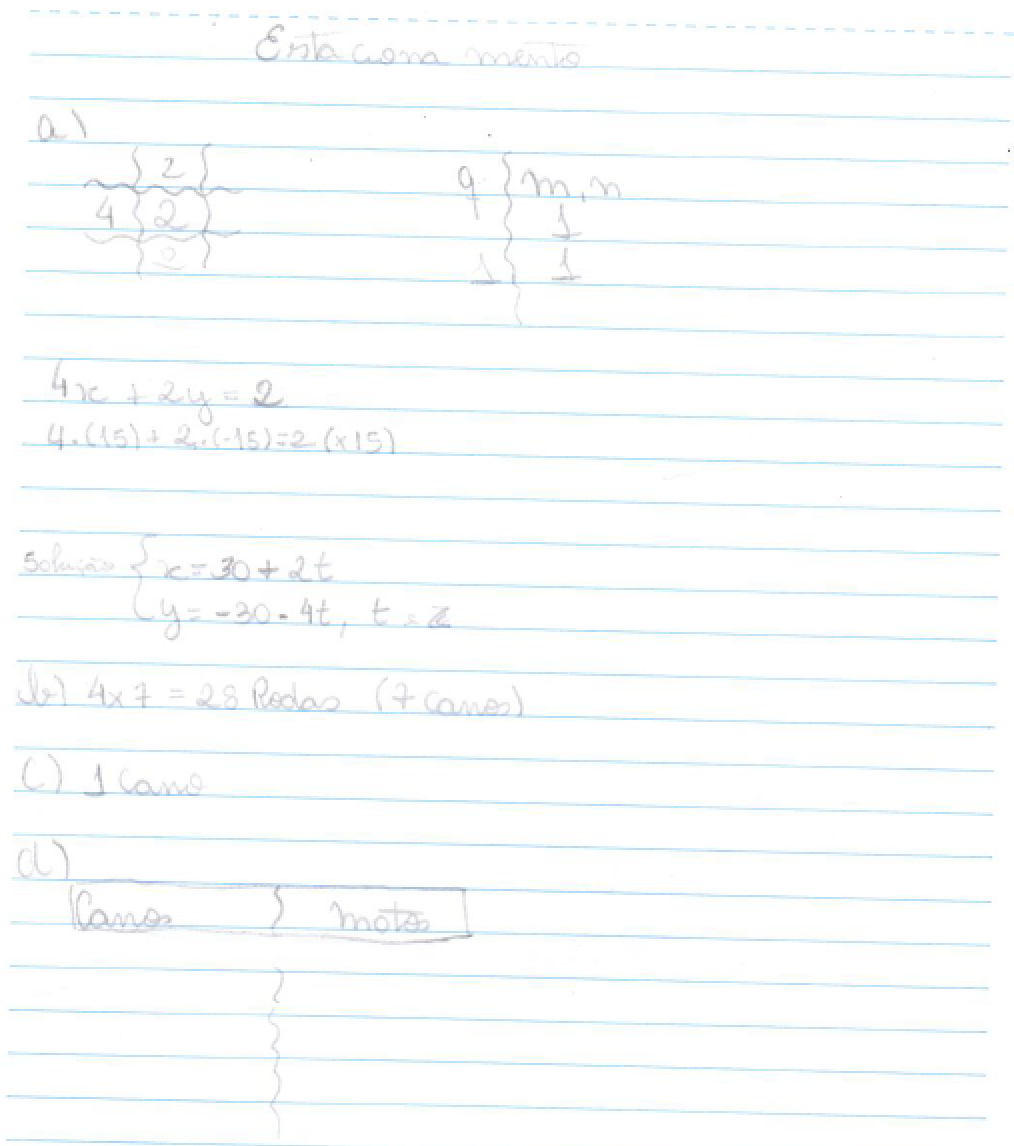

Estacionamento
a)
4x + 2y = 2
4.(15) + 2.(-15) = 2 (x15)
Solução { x = 30 + 2t
y = -30 - 4t, t ∈ Z
b) 4x7 = 28 Rodas (7 carros)
c) 1 carro
d)
Carros | motos

Figura 3.9: Registro do Teste a Posteriori de um aluno W - problema do estacionamento

3.4.2 Validação

A primeira hipótese dizia: "os alunos perceberão que o método utilizado (método da tentativa e erro) na resolução dos problemas propostos no teste a priori possui limitações". Esta hipótese foi confirmada durante a experimentação das sequências didática, principalmente no teste a priori, onde os alunos tiveram dificuldades em determinar todas as soluções possíveis das situações-problema propostas.

Entretanto, não se pode negligenciar o método da tentativa e erro, pois em diversas ocasiões o mesmo torna-se uma ferramenta vantajosa para determinar as soluções de uma equação diofantina linear. Além disso, o método da tentativa e erro proporciona aos alunos uma revisão sobre as operações fundamentais abrangendo os números inteiros.

Agora, a segunda hipótese dizia: "os alunos ficarão mais propensos a apreender outros métodos de resolução de problemas". Tal hipótese foi confirmada durante a experimentação das sequências didática, especialmente após serem apresentados os seguintes resultados: algoritmo de Euclides, teorema de Bèzout (dispositivo prático), congruências e as soluções gerais de uma equação diofantina.

Ainda que alguns alunos persistissem pelo método da tentativa e erro, com o desenvolvimento das atividades propostas nas sequências didática, os alunos descobriram a capacidade facilitadora da linguagem aritmética e da linguagem algébrica na resolução dos problemas propostos.

Já a terceira hipótese dizia: "ocorrerá a socialização de resultados em cada situação problema". Esta hipótese foi amplamente confirmada no decorrer das atividades propostas nas sequências didáticas, pois, ao final de cada atividade, os alunos expunham a forma pela qual determinou as soluções dos exercícios propostos para os colegas de classe.

Isto ofereceu circunstâncias para realizar-se a troca de ideias entre todos os alunos. No decurso das argumentações, alguns alunos conseguiram supor que existia uma relação entre os três dados numéricos expostos nas situações-problema. Além disso, os alunos notaram que nas atividades propostas as soluções versam no conjunto dos números inteiros.

Por fim, a quarta hipótese dizia: "introduzir conceitos e algoritmos na busca da resolução das situações problema que possibilitarão ao aluno notar uma aplicabilidade dos seguintes conceitos: máximo divisor comum e congruências".

Tal hipótese foi confirmada, pois, com a aplicação das atividades, os alunos tiveram contato com o algoritmo de Euclides - método este que eles desconheciam - puderam verificar a existência de soluções e aproveitar os resultados obtidos para aplicar no dispositivo prático do teorema de Bèzout e, assim, expressar o mdc de dois números inteiros como combinação linear dos mesmos. Além disso, foi possível praticar a linguagem aritmética dos alunos ao introduzir o conceito de congruências e a sua aplicação na elucidação das soluções gerais das mencionadas equações.

CONSIDERAÇÕES FINAIS

Tendo como base tudo que foi apresentado durante este trabalho, concluímos que, mesmo se lidando de alunos na faixa de 14 anos, as proposições apresentadas nos métodos de resolução de Equações Diofantinas Lineares se revelaram de simples assimilação, pois envolvem apenas conhecimentos básicos de matemática, tais como: números inteiros, máximo divisor comum, algoritmo de Euclides e congruência.

Sendo assim, constatamos as possibilidades didático-pedagógicas da sequência proposta sobre o tema supracitado, pois as aplicações de situações do cotidiano constituíram um ambiente favorável para o ensino contextualizado das Equações Diofantinas Lineares, propiciando desenvolver as competências essenciais dos alunos nos campos da aritmética e da álgebra.

A junção de uma estrutura teórica adequada e a simples possibilidade de contextualização do tema seguem a atual linha de ensino de matemática na educação básica: estimular a capacidade de compreensão e raciocínio em detrimento da memorização e à sua aplicabilidade ao cotidiano em vez de profundidade.

Portanto, tendo como base os dados conseguidos através da experimentação das sequências didática, a inserção do tema Equação Diofantina Linear nas séries finais do ensino fundamental mostra-se adequado, pois desenvolve o raciocínio lógico, possibilita um processo de ensino-aprendizagem significativo e um maior aperfeiçoamento nos campos da álgebra e aritmética.

Ademais, conseguimos estruturar um material capaz de ser empregue em formação continuada de docentes e que também pode auxiliar o professor da educação básica na diversificação das aulas, com atividades propícias ao público alvo.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANDRINI, Álvaro. **Praticando matemática 6.** 4 ed. São Paulo: Editora do Brasil, 2015.

[2] ARTIGUE, Michele. Engenharia Didática. In: BRUN, Jean. **Didáctica das Matemáticas.** Lisboa: Instituto Piaget, 1996, p.193-217.

[3] BRASIL. **Base Nacional Comum Curricular.** Terceira versão. Brasília: Ministério da Educação e Cultura, 2017.

[4] BRASIL. **Parâmetros Curriculares Nacionais.** Terceiro e Quarto ciclos do ensino fundamental: matemática. Brasília: Ministério da Educação e Cultura, 1997.

[5] BRASIL. **Programa Nacional do Livro Didático 2014: matemática.** Brasília: Ministério da Educação e Cultura, Secretaria de Educação Básica, 2013.

[6] COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA.** 2 ed. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, 2005.

[7] DOMINGUES, Hygino Hugueros. **Fundamentos da Aritmética.** São Paulo: Editora Atual, 1991.

[8] EVES, Howard. **Introdução à História da Matemática.** Campinas - SP: Editora Unicamp, 2004.

[9] HEFEZ, Abramo. **Aritmética.** 1 ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2014.

[10] LACERDA, José Carlos Admo. **Praticando a Aritmética.** 7 ed. Rio de Janeiro: XYZ, 2014.

[11] OLIVEIRA, Marcelo Rufino de. **Coleção Elementos de Matemática, 1.** 3 ed. Fortaleza: Editora VestSeller, 2010.

[12] SOUZA, Joamir Roberto de. **Vontade de saber matemática, 6°ano.** 3 ed. São Paulo: FTD, 2015.

Apêndice A

AUTORIZAÇÃO DA UNIDADE ESCOLAR

Eu, André Fellipe Franco Pereira de Oliveira, responsável principal pelo projeto de dissertação, o qual pertence ao curso de Mestrado Profissional de Matemática em Rede Nacional - PROFMAT da Universidade Federal Rural do Rio de Janeiro - UFRRJ, venho pelo presente, solicitar autorização da Escola Estadual Aydano de Almeida para realização da coleta de dados, no período de fevereiro e março, para o trabalho de pesquisa sob o título **"Equações Diofantinas Lineares: uma proposta para as séries finais do ensino fundamental"**, com o objetivo de apresentar uma proposta de sequência didática sobre o tema supracitado.
Contando com a autorização desta instituição, coloco-me à disposição para qualquer esclarecimento.

Local e data:____________________, __________ de __________________ de 2018.

____
Professor Andre Fellipe Franco Pereira de Oliveira

Apêndice B

AUTORIZAÇÃO DOS RESPONSÁVEIS LEGAIS

Eu, abaixo assinado, responsável legal pelo(a) aluno(a) ______________________________ do 9° ano do ensino fundamental da Escola Estadual Aydano de Almeida, autorizo que o referido aluno participe da pesquisa intitulada por **"Equações Diofantinas Lineares: uma proposta para as séries finais do ensino fundamental"** realizada pelo professor André Fellipe Franco Pereira de Oliveira e declaro que foi devidamente exposto pelo pesquisador os procedimentos envolvidos e os benefícios para os estudantes de tal implementação.

Local e data:________________, ________ de _______________ de 2018.

Assinatura do responsável legal:____________________________________