

UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

DISSERTAÇÃO DE MESTRADO

Congruência e Equações Diofantinas Lineares:

Uma Proposta para o Ensino Básico.

Paulo Sergio de Almeida Santos



Instituto de Matemática

Maceió, Abril de 2013



PROFMAT

**UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE
NACIONAL**

PAULO SERGIO DE ALMEIDA SANTOS

**CONGRUÊNCIA E EQUAÇÕES DIOFANTINAS:
UMA PROPOSTA PARA O ENSINO BÁSICO**

Maceió

2013

UNIVERSIDADE FEDERAL DE ALAGOAS

INSTITUTO DE MATEMÁTICA

**Congruência e Equações Diofantinas: Uma Proposta para
o Ensino Básico**

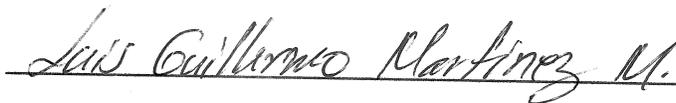
Paulo Sergio de Almeida Santos

Dissertação apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional, coordenado pela Sociedade Brasileira de Matemática e ofertado pelo Instituto de Matemática da Universidade Federal de Alagoas como requisito parcial para obtenção do grau de mestre em matemática.

Banca Examinadora:



Prof. Dr. André Luiz Flores (Orientador - UFAL)



Prof. Dr. Luiz Guillermo Martinez Maza (UFAL)



Prof. Dr. Givaldo Oliveira dos Santos (UFAL)

Catálogo na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária Responsável: Helena Cristina Pimentel do Vale

S237c Santos, Paulo Sergio de Almeida.
Congruência e equações diofantinas : um proposta para o ensino básico /
Paulo Sergio de Almeida Santos. – 2013.
111 f.

Orientador: André Luiz Flores.
Dissertação (mestrado profissional em Matemática em Rede Nacional) –
Universidade Federal de Alagoas. Instituto de Matemática. Maceió, 2013.

Bibliografia: f. 110-111.

1. Matemática – Estudo e ensino. 2. Sequência didática. 3. Equações
diofantinas. 4. Algoritmo de Euclides. I. Título.

CDU: 510.5

Aos meus pais, Maria Luiza e Severino.

AGRADECIMENTOS

A Deus, o que seria de mim sem a fé que eu tenho nele.

Aos meus pais, Maria Luiza e Severino, ao meu irmão, Paulo Roberto, e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

Ao professor André Flores pela paciência na orientação e incentivo que tornaram possível a conclusão desta dissertação.

A todos os professores do curso, que foram tão importantes na minha vida acadêmica e no desenvolvimento desta dissertação.

Aos amigos e colegas, pelo incentivo e pelo apoio constantes.

1. Unidade é aquilo segundo o qual cada uma das coisas existentes é dita um.

2. E número é a quantidade composta de unidade.

RESUMO

O objetivo principal deste trabalho foi o desenvolvimento de sequências didáticas que pudessem auxiliar professores e alunos no processo de ensino-aprendizagem de conceitos de alguns tópicos de Aritmética no Ensino Básico. Serão abordados a congruência módulo n e equações diofantinas lineares com duas incógnitas; também, apresentar a divisão euclidiana de uma forma mais amadurecida, deste mesmo modo também apresentar o algoritmo de Euclides para a obtenção do máximo divisor comum de dois números inteiros ou naturais. Assim também, fazer uma breve análise de como é mostrada a divisão dos naturais e a obtenção do máximo divisor comum nos livros didáticos. Ao longo do trabalho, são expostas as justificativas do porquê está sendo proposto o ensino de congruência módulo n e das equações diofantinas lineares no Ensino Básico, observando de um lado, o amadurecimento do conceito de divisão euclidiana dotar o estudante da capacidade de resolver problemas de caráter cíclicos encontrados em olimpíadas de matemática, e de outro lado, fazer uma natural transição entre a Aritmética e a Álgebra. Assim, nos últimos capítulos são apresentadas sequências didáticas, que representam o produto final deste trabalho dissertativo.

Palavras-chaves: Sequência Didática. Congruência módulo n . Equações diofantinas lineares. Ensino. Divisão euclidiana. Algoritmo de Euclides.

ABSTRACT

The principal objective of this work was the development of didactic sequences that could help teacher and students in the teaching-learning process of concepts, some topics of Arithmetic in Basic Education. Will be see congruence modulo n and diophantine equations linear with two unknowns; also, to show the Euclidean division of a manner more mature, of equal manner to present the Euclidean algorithm to obtain the MDC of two integer numbers or natural numbers. So also make a short analysis is displayer how the division of natural numbers and obtaining MDC in textbooks. Throughout this work are exposed justification of why is being proposed the teaching of congruence modulo n and linear diophantine equations in Basic Education, observing onside, the students of the ability to solve problems of cyclical character found in Math Olympics and otherwise, to make a natural transition between Arithmetic and Algebra. So, in the last chapters are presented didactic sequences, that representing the final product of this dissertation work.

Keywords: Didactic sequences. Congruence modulo n . Diophantine linear equations. Teaching. Euclidian division. Euclid algorithm.

SUMÁRIO

1	INTRODUÇÃO	10
2	DIVISIBILIDADE, DIVISÃO EUCLIDIANA E MDC	15
2.1	Um pouco de história sobre Euclides e da divisão euclidiana	15
2.2	Propriedades da divisibilidade	17
2.3	Divisão Euclidiana.	22
2.4	A divisão dos números naturais vista no Ensino Fundamental	24
2.5	Amadurecendo o conceito de divisão	27
2.6	MDC: Usando o Algoritmo de Euclides pra determinar o mdc.	30
3	ENSINANDO CONGRUÊNCIA MÓDULO N	37
3.1	Introduzindo congruência no Ensino Básico	37
3.2	Um pouco sobre os Números Inteiros \mathbb{Z}	38
3.3	Aritmética dos restos	41
3.4	Aplicações de congruência vista no Ensino Básico	47
3.4.1	Significado do resto	47
3.4.2	A congruência como apoio à compreensão de outros conceitos no Ensino Básico	51
3.5	Paridade	55
3.6	Classe residual módulo 3	57
4	ENSINANDO EQUAÇÕES DIOFANTINAS LINEARES	60
4.1	Em que momento se pode ensinar as equações diofantinas	60
4.2	Um pouco da história de Diofanto e dos problemas diofantinos	61

SUMÁRIO

4.3	Equações Diofantinas Lineares	66
5	SEQUÊNCIA DIDÁTICA PARA A CONGRUÊNCIA MÓDULO N	78
6	SEQUÊNCIA DIDÁTICA PARA AS EQUAÇÕES DIOFANTINAS	93
7	CONCLUSÃO	109
	REFERÊNCIAS	111

1 INTRODUÇÃO

Os PCNs trazem, em relação à área de Matemática, uma pretensão clara no sentido de não conferir um caráter meramente instrumental ou técnico-cientificista, alheio às ciências humanas e descolado das vivências diárias. A hierarquização e a verticalidade dos assuntos a serem tratados e o estrito e linear atendimento à lógica interna da área é apontado como desestimulante ao processo real de aprendizagem, trazendo frustrações às expectativas de aprendizagem dos alunos.

Os PCNs entendem que a escola não pode subestimar os conhecimentos prévios e empíricos do aluno. Outro aspecto que deve ser considerado é o contexto social da escola e do seu entorno, considerando os anseios e objetivos dos alunos e buscando estratégias para estimulá-lo ao estudo da área.

O saber matemático não é construído de modo simples; segundo os PCNs. “O conhecimento matemático é fruto de um processo de que fazem parte a imaginação, os contra-exemplos, as conjecturas, as críticas, os erros e os acertos.” (BRASIL, 1997, p.24). Mas como aponta o conhecimento matemático é em sua natureza exposto de forma descontextualizada, sem limitação do tempo em que foi construído. Pois é preocupação do matemático apresentar resultados gerais.

No processo de criação matemático é em si conflituoso: concreto *versus* abstrato, particular *versus* geral, formal *versus* informal. Tais conflitos também estão presentes no processo de ensino-aprendizagem desta disciplina

Nesse sentido é fundamental que o ensino de Matemática desempenhe seu papel no desenvolvimento da formação de capacidades intelectuais, na criação e agilidade do raciocínio dedutivo e sua aplicação na resolução de problemas. Sob este ponto de vista, os PCNs, diz que:

é fundamental não subestimar a capacidade dos alunos, reconhecendo que resolvem problemas, mesmo que razoavelmente complexos, lançando mão

de seus conhecimentos sobre o assunto e buscando estabelecer relações entre o já conhecido e o novo. (BRASIL , 1997, p.29)

Para isso é fundamental que o professor compreenda um problema matemático em seus diversos aspectos, concebendo-o como uma situação que exige a realização de uma sequência de ações ou operações com o objetivo de chegar a um resultado. Desta forma, o professor deve ter a consciência de que a solução desse problema não está disponível no início, mas é possível construí-la.

Da mesma forma de como a resolução de problemas é importante para o ensino de Matemática, o conhecimento histórico também pode ser usado para a obtenção dos conteúdos matemáticos. Assim os PCNs lança a seguinte orientação de como deve ser a formação do professor de matemática: “O conhecimento da história dos conceitos matemáticos precisa fazer parte da formação dos professores”(BRASIL, 1997, p.30). Pois desta forma, permitir que os alunos conheçam a Matemática como ciência mutável e dinâmica, aberta a novos conhecimentos.

Da mesma forma segundo os PCNs:

A História da Matemática, mediante um processo de transposição didática e juntamente com outros recursos didáticos e metodológicos, pode oferecer uma importante contribuição ao processo de ensino e aprendizagem em Matemática. (BRASIL, 1997, p.34)

O termo Transposição Didática esta usualmente presente neste trabalho dissertativo. Neste aspecto Polidoro afirma que:

A Transposição Didática é um “instrumento” pelo qual analisamos o movimento do saber sábio (aquele que os cientistas descobrem) para o saber a ensinar livros didáticos) e, por este, ao saber ensinado (aquele que realmente acontece em sala de aula).(POLIDORO , 2010, p.153)

Este termo foi inicialmente introduzido em 1975 pelo sociólogo Michel Verret e rediscutido por Yves Chevallard em 1985 em seu livro *La Transposition Didatique* onde mostra as transposições que um saber sofre quando passa do campo científico para a escola e alerta para a importância da compreensão deste processo por aqueles que lidam com o ensino das disciplinas científicas. Chevallard conceitua "Transposição Didática" como o trabalho de fabricar um objeto de ensino, ou seja, fazer um objeto de saber produzido pelo "sábio" (o cientista) ser objeto do saber escolar. Nessa mesma perspectiva:

O termo Transposição Didática implica a diferenciação entre saber acadêmico e saber escolar, que são de natureza e funções distintas, nem sempre evidentes nas análises sobre a dimensão cognitiva do processo de ensino e aprendizagem. Ao definir como Transposição Didática o processo de transformação de objetos de conhecimento em objetos de ensino e aprendizagem. (POLIDORO, 2010, p.154)

O tema central deste trabalho é uma proposta de Transposição Didática do ensino de congruência e equações diofantinas lineares para o Ensino Básico, expandindo o conceito de divisibilidade e tratando o conhecimento da divisão euclidiana, o algoritmo de Euclides e as equações diofantinas lineares de forma construtiva e intuitiva.

Nesse aspecto, ao longo do trabalho busca-se justificar a importância da presença dos tópicos acima mencionados no ensino de Matemática, deixando claro que tais tópicos fiquem como assuntos complementares para o currículo de Matemática e postos em momentos adequados. Lins lança uma crítica muito forte sobre o ensino de Aritmética, tal crítica é uma justificativa pertinente a este trabalho acadêmico, essa crítica é de fato o problema abordado neste trabalho dissertativo.

O desenvolvimento habitual do ensino-aprendizagem da Aritmética nas salas de aula deixa de lado muitos pontos importantes. (LINS , 1997, p.34)

Para deixar mais claro sobre quais são estes pontos importantes, é feita uma breve análise no capítulo primeiro de alguns livros do Ensino Fundamental, daí poder levantar esses pontos. Também tratamos da Aritmética modular e equações diofantinas lineares como pontos importantes a serem vistos no Ensino Básico

Assim que encontramos o tema deste trabalho e o problema abordado (o ensino de Aritmética no Ensino Básico deixam de lado muitos pontos importantes), era necessário estabelecer a metodologia usada para o desenvolvimento. O primeiro foi uma pesquisa bibliográfica sobre os tópicos aritméticos abordados (Divisão Euclidiana, Algoritmo de Euclides, congruência módulo n e equações diofantinas lineares). Uma segunda etapa do trabalho foi uma análise de textos didáticos que abordam assuntos como: divisão nos naturais, máximo divisor comum. Desta forma compreender quais pontos iniciais são necessários para o aprofundamento em sala de aula. Em seguida uma pesquisa em trabalhos acadêmicos que aborda a mesma temática: o ensino da Aritmética dos restos e congruência. O que percebemos que propostas de ensino sobre as equações diofantinas eram vastas. E por fim a elaboração de sequências didáticas, visando esse ser o produto final do trabalho dissertativo.

No primeiro capítulo são abordados, visando o entendimento mais aprimorado, os conteúdos de: divisibilidade, divisão euclidiana e do algoritmo de Euclides. Pois estes são pré-requisitos para as congruências módulo n e das equações diofantinas lineares.

No segundo capítulo é abordado as congruências módulo n e justificativas para sua implantação no Ensino Básico, como desenvolver um significado mais elaborado para o resto em uma divisão euclidiana.

No terceiro capítulo, ainda abordando os conteúdos matemáticos envolvidos nesta dissertação, apresentamos as equações diofantinas lineares, alguns aspectos históricos e principalmente uma discussão de quando se poderia ser ensinada as equações diofantinas lineares no Ensino Básico como também justificativas da importância de ser feita uma transposição didática.

Nos capítulos quatro e cinco são apresentadas duas sequências didáticas, uma para o ensino da Aritmética modular e outra para as equações diofantinas lineares, respectivamente. Esses últimos capítulos são o produto final deste trabalho dissertativo, que visa uma orientação para o professor que deseje ensinar algum desses tópicos de Aritmética.

Na parte do trabalho onde tratamos sobre as equações diofantinas, mostramos que essas traçam uma ponte entre a Aritmética e a Álgebra. Também é apresentada aplicações de congruência na Trigonometria e nos Números Complexos, mostrando assim que a congruência pode ser um bom recurso de apoio para o desenvolvimento de conteúdos tradicionalmente vistos no Ensino Básico, satisfazendo assim um objetivo presente nos PCNs: “estabelecer conexões entre temas matemáticos de diferentes campos.” (BRASIL , 1997, p.37).

Apresentamos no capítulo segundo algumas situações-problema, em sua maioria da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), especificamente para desenvolver um significado mais elaborado do resto de uma divisão euclidiana, já que os PCNs trazem a seguinte orientação.

resolver situações-problema envolvendo números naturais, inteiros, racionais e a partir delas ampliar e construir novos significados da adição, subtração, multiplicação, divisão, potenciação e radiciação (BRASIL , 1998, p.64)

Ainda sobre a abordagem das equações diofantinas, que na sequência didática proposta no capítulo quinto, será inserido esse conteúdo de forma natural com o jogo chamado

"escova diofantina", apresentado em Capilheira [5]; como preparação para sua generalização, propomos diversas situações-problema.

2 DIVISIBILIDADE, DIVISÃO EUCLIDIANA E MDC

Nesse capítulo serão abordados os assuntos: divisibilidade, divisão euclidiana e o algoritmo de Euclides, visando o entendimento mais aprimorado desses conteúdos. Também serão vistas uma breve análise de textos didáticos mostrando como se dá o ensino da divisão dos números naturais, assim como uma explanação sobre o significado do resto e do quociente de uma divisão. A abordagem será sobre os números naturais \mathbb{N} . Sem muita formalidade, é dito que os números naturais formam o primeiro conjunto numérico descoberto pela humanidade, tendo esses números a característica prática de servir para a contagem de objetos.

2.1 Um pouco de história sobre Euclides e da divisão euclidiana

Importante obra de cunho matemático foi os "*Elementos de Euclides*", como diz Howard Eves: "Nenhum trabalho, exceto a Bíblia, foi tão largamente usado ou estudado e, provavelmente, nenhum exerceu influência maior no pensamento científico."(EVES , 2004, p.167).

A obra reuniu toda a Matemática conhecida pelos gregos, egípcios, babilônicos, até Euclides. Apesar de sua importância, pouco se sabe sobre Euclides. Quanto ao seu livro, cuja abordagem perpassa da Geometria à Aritmética, é dividida em 13 livros. A Aritmética está nos livros VII, VIII e IX que "tratam da teoria elementar dos números. O livros VII começa com o processo, hoje conhecido como *algoritmo euclidiano*,"(EVES , 2004, p.173)

O livro *Elementos de Euclides* traz, na tradução de Ireneu Bicudo [10], na primeira proposição do livro VII o método euclidiano para determinar quando dois números são primos entre si:

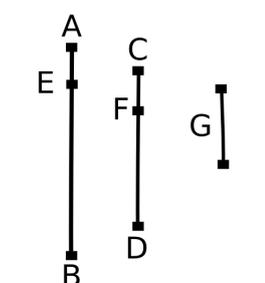
Sendo expostos dois números desiguais, e sendo sempre subtraído de novo o menor do maior, caso o que restou nunca meça exatamente o antes dele mesmo, até que reste uma unidade, os números serão primos entre si. (EUCLIDES, 2009, p.270)

Vale ressaltar que número era tratado como uma *multiplicidade da unidade*; neste sentido, para Euclides os números naturais começava a partir do dois, e sua definição para o número *um* era: “Unidade é aquilo segundo o qual cada uma das coisas existentes é dita uma.” (EUCLIDES, 2009, p.169)

A proposição 2 do livro VII apresenta um método para determinar o máximo divisor comum: “*Sendo dados dois números não primos entre si, achar a maior medida comum dele*” (EUCLIDES, 2009, p.171). Observe que naquela época, a perspectiva geométrica de Matemática era dominante, e números eram tratados quase que exclusivamente como medidas de segmentos, e sob este ponto de vista, o *mdc* de dois números é tratado como a maior medida comum de dois números/segmentos.

A seguir colocamos a prova euclidiana da proposição 2 do livro VII. Usando a figura abaixo como base para demonstração.

Quadro 1: Método euclidiano para o MDC



Fonte: EUCLIDES

Tomando dois números dados não primos entre si AB, CD, inicialmente é necessário achar a maior medida comum dos AB, CD.

Se, tomando o fato que o CD mede o AB (ou seja AB é um múltiplo de CD), é evidente que CD mede também a si mesmo, portanto o CD é uma medida comum de CD e AB. Logo CD também é a medida maior; pois, nenhum maior do que o CD medirá o CD.

Se, tomando o fato que o número CD não mede o AB. Daí dos números AB, CD, usa o processo de sempre subtrair o menor do maior e de novo o menor do maior terá restado

algum número, o qual medirá o número que foi antes dele mesmo, pois, como AB e CD não são primos entre si, como foi suposto, não terá uma unidade restante. Desde modo o lado restante será o lado comum entre os números, pois tomando a figura acima e o lado AE como o lado de número comum, o lado CD, medindo o lado BE, então resta um menor do que ele mesmo, ou seja, o EA. Da mesma forma, o lado EA, medindo o lado DF, então resta um menor do que ele mesmo, ou seja, o lado FC, e o CF meça o AE. Como, o lado CF mede o lado AE, e o AE mede DF, portanto o CF medirá o lado DF; e mede também a si mesmo; portanto medirá o CD todo. E o CD mede o BE; portanto, o CF mede também o BE; e mede também o EA; portanto, medirá também o BA todo; e mede também o CD; portanto, o CF mede os AB, CD. Portanto, o CF é uma medida comum dos AB, CD.

Terminando o procedimento para encontrar uma medida comum a AB e CD, Euclides afirma que: “Digo, então, que também é a maior”, e faz a seguinte prova dessa afirmação:

Pois, se o CF não é a maior medida comum dos AB, CD, algum número medirá os números AB, CD, sendo maior do que CF. Meça, e seja o G. E como o G mede o CD, e o CD mede o BE, portanto o G mede o BE; e mede também o BA todo; portanto medirá também o AE restante. Mas o AE mede o DF; portanto, o G medirá também o DF; e mede também o DC todo; portanto, também medirá o CF restante, o maior, o menor; o que é impossível; portanto, nenhum número medirá os números AB, CD, sendo maior do que CF; portanto, o CF é a maior medida comum dos AB, CD. (EUCLIDES , 2009, p.172)

2.2 Propriedades da divisibilidade

Uma proposta para possível aplicação no Ensino Básico é o uso da notação de divisibilidade. Ao se ensinar os critérios de divisibilidade, esta é apenas expressada de modo verbal ou escrita por extenso. A abordagem e notações apresentadas a seguir é de uso comum em um curso de Aritmética, no nível superior, que pode ser vista em Hefez [12], Domingues [9] e Santos [28], mas como poderemos observar, poderia ser apresentada ao aluno do ensino fundamental.

Definição 2.1 (divide). *Um número a **divide** b , ambos números naturais, denotado por $a \mid b$, se existe um número $c \in \mathbb{N}$ tal que $b = a \cdot c$. Também é dito a é um **divisor** de b ou que b é um **múltiplo** de a .*

Desse modo também se define "a não divide b" denotado por $a \nmid b$, com $a, b \in \mathbb{N}$, quando não existe um tal natural c de forma que $b = a \cdot c$.

Note que pela definição, se $a \mid b$, então $a \leq b$. O número 1 divide qualquer número natural, ou seja, $1 \mid n$, para qualquer $n \in \mathbb{N}$, pois tomando a partir da definição $c = n$, temos $n = 1 \cdot n$, do mesmo modo temos que $n \mid n$. Observe que a definição pode ser estendida naturalmente aos números inteiros \mathbb{Z} .

Exemplo 2.1. $2 \mid 0; 4 \mid 0; 1 \mid 8; 2 \mid 8; 1 \mid 3; 3 \mid 3; 4 \nmid 5; 7 \nmid 9$

Ainda pensando nessa notação como uma possibilidade para o Ensino Básico, observe que está mais relacionada com a operação multiplicação do que com a divisão em si, ou seja, a definição, incluindo a notação, poderia ser introduzida logo após o ensino da operação multiplicação e como um ponto introdutório para a divisão dos naturais.

Assim melhor se define ou inicialmente se definiria o quociente da divisão dos números naturais b por a ao número natural c , quando $a \mid b$, ficando expresso como $c = \frac{b}{a}$.

Exemplo 2.2. $0 = \frac{0}{2}, 0 = \frac{0}{4}, 8 = \frac{8}{1}, 4 = \frac{8}{2}, 3 = \frac{3}{1}, 1 = \frac{3}{3}$

A proposição abaixo 2.1, vista em Santos [28] mostra que a relação de divisibilidade é transitiva.

Proposição 2.1. *Sejam a e b números naturais não nulos e seja c um outro natural, se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Sabendo que $a \mid b$ e $b \mid c$, então existem $f \in \mathbb{N}$ e $g \in \mathbb{N}$, tais que satisfazem as igualdades $b = f \cdot a$ e $c = g \cdot b$, substituindo a primeira igualdade na segunda igualdade, temos; $c = g \cdot f \cdot a$ e então como $f \cdot g = h$, $h \in \mathbb{N}$ chega a tese $a \mid c$. ■

Exemplo 2.3. *Como $4 \mid 12$ e como $12 \mid 36$, então $4 \mid 36$*

As proposições abaixo 2.2 e 2.3 são vistas em Hefez [12] e Domingues [9].

Proposição 2.2. *Tomando a, b naturais não nulos e seja também $c \in \mathbb{N}$. Vale então que:*

(i) $1 \mid c$.

(ii) $a \mid a$.

(iii) $a \mid 0$.

Demonstração: As provas para (i), (ii) e (iii) decorre das seguintes igualdades; $c = 1 \cdot c$, $a = a \cdot 1$ e $0 = a \cdot 0$, respectivamente. ■

Proposição 2.3. *Sejam a, b, c e $d \in \mathbb{N}$, com $a \neq 0$. Então:*

(i) $a \mid b$ e $c \mid d \implies a \cdot c \mid b \cdot d$ (quando $c \neq 0$).

(ii) $a \mid b \iff a \mid c$ (quando $a \mid (b+c)$).

(iii) $a \mid b \iff a \mid c$ (quando $a \mid (b-c)$ e $b \geq c$).

Demonstração: Demonstrando cada parte:

(i) Como $a \mid b$, então existe $f \in \mathbb{N}$, tal que $b = f \cdot a$, do mesmo modo temos a igualdade $d = g \cdot c$, com $g \in \mathbb{N}$. Multiplicando igualdade por igualdade temos $b \cdot d = f \cdot a \cdot g \cdot c$, ou seja, $b \cdot d = (a \cdot c)(f \cdot g)$, portanto $a \cdot c \mid b \cdot d$

(ii) Será feita apenas a ida da proposição, pois a volta é análoga.

Tomando a hipótese que $a \mid (b+c)$, logo existe um $f \in \mathbb{N}$, tal que

$$b+c = f \cdot a . \tag{2.1}$$

Do mesmo modo $a \mid b$, logo existe um $g \in \mathbb{N}$, tal que

$$b = g \cdot a . \quad (2.2)$$

Substituindo (2.2) em (2.1), temos que

$$g \cdot a + c = f \cdot a \Rightarrow c = f \cdot a - g \cdot a$$

como $c \in \mathbb{N}$, logo $f \cdot a > g \cdot a$, ou seja $f - g > 0$ e portanto $c = (f - g)a \Rightarrow a \mid c$.

(iii) A demonstração é idêntica ao item anterior, provando sua volta.

Tomando $a \mid c$, então $\exists f \in \mathbb{N}$ tal que

$$c = f \cdot a . \quad (2.3)$$

Da mesma forma, como $a \mid (b - c)$, $\exists g \in \mathbb{N}$ que satisfaz

$$b - c = g \cdot a . \quad (2.4)$$

Substituindo o c em (2.4) conforme está em (2.3), leva a

$$b - f \cdot a = g \cdot a \Rightarrow b = g \cdot a + f \cdot a \Rightarrow b = (g + f) \cdot a$$

o que conclui $a \mid b$.

■

Exemplo 2.4. Tomando $a = 12$, $b = 48$, $b + c_1 = 72$ e $b - c_2 = 12$, tem que $12 \mid 48$ e também $12 \mid 72$, portanto pelo item (ii) da proposição 2.3 leva a $12 \mid c_1$ que é $c_1 = 72 - 48 = 24$. Do mesmo modo usando o item (iii) da mesma proposição tem que $12 \mid c_2$, como $c_2 = 48 - 12 = 36$.

A proposição abaixo é vista em Hefez [12].

Proposição 2.4. Sejam a, b, c, f e g todos números naturais com $a \neq 0$ e satisfazendo $a \mid b$ e $a \mid c$, então:

(i) $a \mid (f \cdot b + g \cdot c)$.

(ii) $a \mid (f \cdot b - g \cdot c)$ (quando $f \cdot b \geq g \cdot c$).

Demonstração: A demonstração para o item **(ii)** é análoga ao item **(i)**, feito a seguir:

(i) Como $a \mid b$ e $a \mid c$, então existem x e $y \in \mathbb{N}$, tais que

$$b = x \cdot a \Rightarrow f \cdot b = f \cdot x \cdot a$$

e

$$c = y \cdot a \Rightarrow g \cdot c = g \cdot y \cdot a.$$

Somando as duas equações.

$$f \cdot b + g \cdot c = f \cdot x \cdot a + g \cdot y \cdot a$$

$$f \cdot b + g \cdot c = a \cdot (f \cdot x + g \cdot y).$$

Como $(f \cdot x + g \cdot y) \in \mathbb{N}$, conclui-se que

$$a \mid (f \cdot b + g \cdot c).$$

■

A divisibilidade é ainda uma relação de ordem, ou seja, goza de três propriedades, a *transitiva* vista na proposição 2.1 a *reflexiva* vista na proposição 2.2 e por fim a propriedade vista em Domingues [9] é chamada de *antissimétrica* que será provada na proposição seguinte.

Proposição 2.5. *Sejam $a \in \mathbb{N}$ e $b \in \mathbb{N}$, tais que $a \mid b$ e $b \mid a$, então $a = b$.*

Demonstração: Das hipóteses $a \mid b$ e $b \mid a$, existem f e $g \in \mathbb{N}$, tais que $b = f \cdot a$ e $a = g \cdot b$, o que leva a $b = f \cdot g \cdot b$, podendo ter duas possibilidades para b , se $b = 0$, logo $a = 0$, ou seja, $a = b$, por outro lado, se $b \neq 0$, então $f \cdot g = 1$ e como f e g são naturais logo $f = g = 1$ e portanto $b = 1 \cdot a$, como queria ser demonstrado, provando assim que a divisibilidade é uma relação de ordem.

■

2.3 Divisão Euclidiana.

Nesta seção serão expostos a divisão euclidiana, alguns exemplos e breves aplicações, em Hefez [12] tem o seguinte teorema da divisão euclidiana.

Teorema 2.1 (Divisão Euclidiana). *Dados dois números a e b , com $a < b$ ambos naturais ($a, b \in \mathbb{N}$), existem outros dois únicos números também naturais $q \in \mathbb{N}$ e $r \in \mathbb{N}$, q chamado de quociente e r chamado de resto, tais que vale a seguinte igualdade.*

$$b = aq + r$$

com $r < a$.

Demonstração: Tomando o conjunto R , definido até um valor de n tal que $b - n \cdot a \in \mathbb{N}$

$$R = \{b, b - a, b - 2a, \dots, b - n \cdot a\}.$$

Pelo Princípio da Boa Ordem ¹ o conjunto R terá um menor elemento $r = b - q \cdot a$, note que r será o resto e q o quociente da divisão b por a . Para demonstrar o teorema, basta verificar que $r < a$.

Para $a \mid b$, o menor valor de R será $r = 0$, ou seja $r < a$, já está provado.

Para $a \nmid b$, nesse caso $r \neq 0$ e daí basta provar que $r < a$. Provando por contradição.

Tomando $r > a$, nesse caso existe um número natural c , com $c < r$, com a seguinte condição $r = c + a$, como $r = c + a = b - q \cdot a$, portanto $c = b - (q + 1) \cdot a$, ou seja:

$$c = b - (q + 1) \cdot a \in R, \text{ com } c < r$$

o que é uma contradição pois r é o menor elemento de R .

Para provar a unicidade. Basta tomar dois elementos de R e considera-los os distintos restos da divisão euclidiana de b por a , a diferença entre o maior e o menor é de fato um múltiplo de a , pois $r = b - a \cdot q$ e $r' = b - a \cdot q'$, com $r' < r < a$, $r - r' = -a \cdot q + a \cdot q'$, e portanto $r - r' = a(q' - q)$, ou seja, $r - r' \geq a$, o que acarretaria $r \geq r' + a \geq a$, absurdo, portanto $r = r'$

¹O Princípio da Boa Ordem (PBO) diz que todo conjunto $C \subset \mathbb{N}$ com $C \neq \emptyset$ existe $c \in C$, tal que $c \leq x$, $\forall x \in C$.

Exemplo 2.5. *Encontre o quociente e o resto da divisão de 34 por 7.*

Resolução: Subtraindo 34 por múltiplos de 7:

$$r_1 = 34 - 1 \cdot 7 = 27$$

$$r_2 = 34 - 2 \cdot 7 = 20$$

$$r_3 = 34 - 3 \cdot 7 = 13$$

$$r_4 = 34 - 4 \cdot 7 = 6.$$

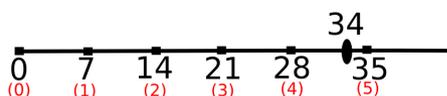
Portanto $q = 4$ e $r = 6$, escrevendo assim $34 = 7 \cdot 4 + 6$.

Escrevendo a igualdade acima no algoritmo prático da divisão,

$$\begin{array}{r} 34 \quad | \quad 7 \\ -28 \quad 4 \\ \hline 6 \end{array}$$

De um modo prático e visual, pode-se dispor uma reta com pontos que representam os múltiplos do divisor a e então inserir o dividendo b entre os pontos aq e $a(q+1)$, onde q é o quociente, e por fim efetuar a diferença $b - aq$, seu respectivo resto. Por exemplo na divisão de $b = 34$ por $a = 7$, o 34 está entre os múltiplos 28 e 35 de 7:

Quadro 2: Representação da divisão em uma reta.



Fonte: AUTOR 2013

$7 \cdot 4 < 34 < 7 \cdot (4+1)$, portanto $q = 4$ e $r = 34 - 28 = 6$.

Exemplo 2.6. *Quantos múltiplos de 5 que existem entre 1 até 156?*

Resolução: Pelo algoritmo da divisão temos que

$$156 = 5 \cdot 31 + 1$$

e portanto, o maior múltiplo que é menor que 156 é $5 \cdot 31 = 155$ e que os múltiplos de 5 de 1 até 156 são

$$1 \cdot 5, 2 \cdot 5, 3 \cdot 5, \dots, 31 \cdot 5$$

e então são em 31 os múltiplos.

■

Exemplo 2.7. *Para qualquer número natural $n \in \mathbb{N}$, na divisão por 2, existem apenas dois possíveis restos:*

- (i) *o resto será 0 quando $2 \mid n$, assim dizermos que n é par e escrito $n = 2 \cdot k$ com $k \in \mathbb{N}$.*
- (ii) *o resto será 1 quando $2 \nmid n$, assim dizermos que n é ímpar e escrito assim $n = 2 \cdot k + 1$ com $k \in \mathbb{N}$.*

O exemplo acima, apesar de sua simplicidade, é rico em conceito, pois dados todos os números naturais, foi esse conjunto repartido em duas categorias, os que deixam resto 1 e os que deixam resto 0. Não só com o número dois se faz isso, mas para qualquer natural n maior do que 1 pode-se repartir os números naturais em n categorias, o que será melhor visto no próximo capítulo.

2.4 A divisão dos números naturais vista no Ensino Fundamental

Nesta seção comentaremos, de modo geral, de como se dá o ensino da divisão dos números naturais no Ensino Básico, no geral este assunto é dado nos primeiros anos do Ensino Fundamental, mas aqui só nos preocuparemos com o que é geralmente visto no 3º ciclo do Ensino Fundamental, que compreende o 6º e 7º ano.

Foi analisado alguns livros didáticos bastante utilizados, especificamente os livros do 6º ano do Ensino Fundamental: "*Matemática*" de Imenes e Lellis [14] e "*Matemática e Realidade*", de Gerson Iezzi [13].

Em Imenes [14], o texto começa mostrando e explicando o algoritmo prático da divisão. São apresentadas algumas questões com enunciado direto, simplesmente efetuar a divisão, e outras apresentam um enunciado mais elaborado, como:

Um comboio com 23 vagões transporta 805 toneladas de minério. A carga foi distribuída igualmente entre os vagões. Quanto carrega cada um?(IMENES , 2009, p.55)

A solução dessa questão é apenas a divisão de 805 por 23, cuja resposta é o quociente. Com esses enunciados e outros o livro propõe uma primeira ideia sobre a divisão: “com a divisão, reparto uma quantidade em partes iguais” (IMENES , 2009, p.55). Logo depois apresenta um outro exemplo:

Os alunos de um colégio vão fazer uma excursão. São 168 pessoas entre alunos e professores. Quantos micro-ônibus de 22 lugares eles deverão alugar?(IMENES , 2009, p.57)

Nesse caso efetua-se a divisão:

$$\begin{array}{r} 168 \quad | \quad 22 \\ 14 \quad 7 \end{array}$$

A solução 7 ônibus com 22 passageiros mais um ônibus com 14 pessoas, ou seja, 8 ônibus. E a partir do exemplo dado conclui-se que a divisão “serviu para descobrir quantos grupos de 22 pessoas são formados com 168 pessoas”, (IMENES, 2009, p.57), ou seja divisão como uma ideia de agrupamento.

Por fim, Imenes apresenta seu último exemplo sobre a divisão, que é o seguinte:

Como chovia, vovó pediu aos 5 netinhos que assistissem à televisão. Ela repartiu bombons entre eles e recomendou que ficassem comportados. Cada neto recebeu 13 bombons e sobraram 3 na caixa. Quantos bombons havia na caixa?(IMENES , 2009, p.62)

Aqui nesse exemplo é exposto como solução o dividendo de uma divisão no qual 5 é o divisor, 3 é o resto e 13 é o quociente. Por fim mostra o dividendo como o resultado da soma do produto do quociente pelo divisor com o resto. Entretanto pouco se explora tal relação nas questões propostas.

Em Iezzi [13] o conteúdo divisão é exposto em duas seções: uma para as divisões exatas, resto igual a 0 e outra seção com divisões com resto diferente de zero. Dentre os exemplos expostos, um deles define a divisão como “repartir em quantidades iguais”.

Em outro exemplo, “Temos 60 livros e queremos colocá-los em pilhas de 12 cada um. Quantas serão formadas?” Iezzi [13] define que “A divisão também é usada para descobrir a quantidade de grupos”.

Na seção destinada a divisão com resto Iezzi lança o seguinte exemplo:

O professor de Educação Física vai organizar um torneio de vôlei com alunos das 5.^{as} séries. Cada equipe de vôlei tem 6 alunos. Quantas equipes, no máximo, podem ser formadas com 32 meninos da 5.^a séries. (IEZZI , 2000, p.43)

Na solução desse problema é feita a divisão:

$$\begin{array}{r} 32 \quad | \quad 6 \\ \underline{\quad} \\ 2 \quad 5 \end{array}$$

mostrando cada elemento da divisão e expondo a expressão $5 \times 6 + 2 = 32$. Por fim lança a condição de resto menor do que o divisor.

Nesta seção de Iezzi [13] os enunciados dos problemas tendem em sua grande maioria a associar o resto de modo direto, com a ideia de sobra, como por exemplo:

Em 11720 dias há quantos meses? Quantos dias *sobram*?(IEZZI , 2000, p.44)

Apenas uma única questão apresenta um raciocínio mais elaborado, que foi a seguinte:

Contando a partir de um domingo, em que dia da semana cai o milésimo dia?(IEZZI , 2000, p.43)

Resolução:

Precisamos descobrir quantas semanas completas há em 1000 dias e quantos dias sobram.

$$\begin{array}{r} 1000 \quad | \quad 7 \\ \underline{\quad} \\ 30 \quad 142 \\ 20 \\ 6 \end{array}$$

Em 1000 dias há 142 semanas completas e sobram 6 dias. Contando a partir de um domingo, o sexto dia será uma sexta-feira. (IEZZI , 2000, p.16, MANUAL DO PROFESSOR)



No geral encontramos nos textos didáticos apenas a exposição do algoritmo que dispõe a divisão da seguinte forma:

$$\begin{array}{r|l} \text{Dividendo} & \text{Divisor} \\ \hline \text{resto} & \text{quociente} \end{array}$$

Muitos textos apresentam a expressão

$$\text{Dividendo} = \text{Divisor} \cdot \text{quociente} + \text{resto}$$

como uma propriedade ou característica e não necessariamente uma forma mais adequada de expor uma divisão dos naturais; geralmente, pouco é usada tal propriedade.

O fato mais marcante dessas análises é que as questões nos livros didáticos abordam quase que exclusivamente as ideias associadas ao quociente de uma divisão, não explorando algumas aplicações que envolva o resto.

Em Imenes [14] pouco se vê a presença explícita do resto em questões com um enunciado mais elaborado, o mesmo ocorrendo em Iezzi [13], com excessões de questões que se pede apenas para dividir dois números, como por exemplo:

6. a) Copie e complete a tabela em seu caderno:

Dividendo	Divisor	Quociente	Resto
205	15	????	????
875	15	????	????
1015	15	????	????
68010	15	????	????

(IMENES , 2009, p.55)

Exceto questões do tipo acima, em Imenes não se encontram outras com enunciados mais práticos de cunho cotidiano, com ideias de sobra ou elementos que ficaram de fora em uma divisão para que se interprete algum significado mais elaborado para o resto de uma divisão.

2.5 Amadurecendo o conceito de divisão

Dividir um número natural a por outro número b , também natural, é escrevê-lo como $a = bq + r$, onde q e r são naturais e $r < b$. Não existe nessa definição impedimentos para que os alunos de 6º ano não o saibam (e já é visto no Ensino Fundamental, mas não como uma definição e sim uma propriedade). Não existe empecilho que possa interferir o ensino da divisão sob este outro ponto de vista, ou seja, usando uma definição mais conhecida dos livros de Aritmética.

Nessa perspectiva, como dividir a por b é encontrar dois números, q e r , chamados de quociente e resto, respectivamente, não há justificativa plausível para as poucas aplicações do resto no Ensino Fundamental, pois apenas focando o quociente como o único resultado esperado em livros didáticos é de fato uma grande limitação do potencial das aplicações da divisão dos números naturais.

Quanto à prática do ensino Lopes nos diz que:

O professor não deve confundir o ensino do algoritmo da divisão com a construção das ideias e dos significados dessa operação. É recomendável que o algoritmo da divisão seja sistematizado apenas quando o professor tiver certeza de que os alunos compreenderam o sentido da divisão e conseguem associar as ideias envolvidas na divisão a situações-problema. (LOPES, 2009, p.43)

Neste sentido é necessário garantir que o aluno seja capaz de entender o sentido da divisão euclidiana, para então ser apresentado o algoritmo da divisão para os alunos.

Quanto às ideias associadas às questões que envolvem a divisão Lopes expõe duas delas: a ideia de partição e a ideia de quotização. Como define Lopes [18]:

- **Ideia de partição.** Nos problemas de partição, é conhecido o número total de elementos de um conjunto que tem de ser distribuído em partes iguais. O problema consiste em determinar o tamanho de cada parte. (LOPES, 2009, p.44)

Sobre esta ideia, como exemplo:

Exemplo 2.8. *Deseja-se repartir 30 bolinhas de gude em 6 sacos. Quantas bolinhas ficaram em cada saco?*

- **Ideia de quotização.** Nos problemas de quotização, o número de elementos deve ser dividido em partes de tamanho determinado; o que se pretende saber é quantas serão as partes (LOPES, 2009, p.44)

Como exemplo dessa ideia:

Exemplo 2.9. *Deseja-se repartir 30 bolinhas de gude em sacos, no qual cada saco fique com 10 bolinhas. Quantos sacos vão ser usados?*

Estas são segundo Lopes ideias associadas à divisão, entretanto são ideias associadas apenas ao quociente de uma divisão e não ao resto dessa divisão. E ainda assim “muitos livros didáticos tratam desses dois tipos de problemas sem a devida atenção para sua diferença ” ([18], 2009, p.44).

Mas quais as ideias associadas as questões que envolvem a divisão, mas que exigem o resto para sua solução? Em Lopes temos a ideia de resto como sobra de uma divisão não exata, ou seja, quando o quociente não é um divisor do dividendo. Seja alguns exemplos vistos no livro de Lopes:

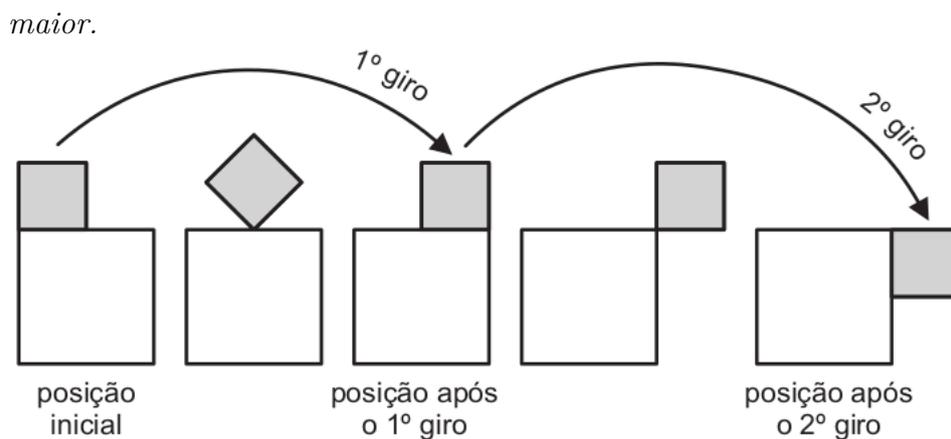
Dona Benta distribuiu igualmente 38 brigadeiros entre 12 alunos. Quantos brigadeiros recebeu cada um? Sobraram brigadeiros? (LOPES, 2009, p.46)

Note que a resposta da segunda questão é obtida através do resto da divisão de 38 por 12, e nesse caso ao resto está associada uma ideia mais comum, que é de sobra da parte que não se pode dividir por ser menor que o divisor.

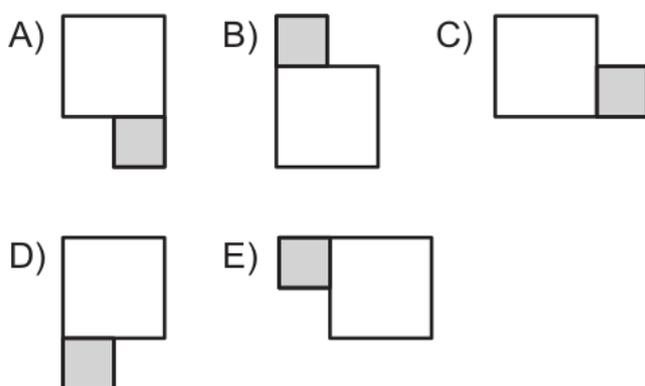
Nas questões da OBMEP, é muito comum a presença de questões que envolvem situações cíclicas, ou seja que se repetem em um dado momento, questões essas que são naturalmente resolvidas a partir de uma divisão entre dois naturais; porém, frequentemente a solução está associada ao resto, e não ao quociente, daí a necessidade de interpretar tal resto.

Apresentamos a seguir um exemplo de uma tal questão, aplicada na OBMEP no ano de 2012 na primeira fase do Nível I (6º ano do Ensino Fundamental):

Exemplo 2.10. *[OBMEP (2012), 1ª Fase, Nível 1] Um quadrado de lado 1 cm roda em torno de um quadrado de lado 2 cm, como na figura, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado*



Qual das figuras a seguir representa a posição dos dois quadrados após o 2012º giro?



Resolução: Basta verificar que após oito giros sucessivos o quadrado menor retorna à sua posição inicial. Como $2012 = 8 \cdot 251 + 4$, após o 2012º giro o quadrado menor terá dado 251 voltas completas no quadrado maior e mais quatro giros, parando na posição que corresponde à alternativa A.

■

Nota-se, do exemplo acima, que o resto de uma divisão tem mais conceitos associadas de que apenas a ideia de sobra. Apesar de não explorada no Ensino Fundamental, mesmo assim os alunos se deparam com questões mais elaboradas e raciocínios não vistos por eles, em sala de aula, presentes na OBMEP.

2.6 MDC: Usando o Algoritmo de Euclides pra determinar o mdc.

Em Hefez encontramos a seguinte definição de máximo divisor comum.

Definição 2.2 (MDC). d será chamado de mdc de a e b se gozar das seguintes propriedades:

- (i) $d | a$ e $d | b$, ou seja, d é um divisor comum.
- (ii) $\forall c \in \mathbb{N}$, com $c | a$ e $c | b$, então $c | d$, ou seja, d é divisível por todo divisor comum de a e b .

Com essa definição podemos facilmente chegar a algumas propriedades. O *máximo divisor comum* de dois números é único, pois, se d e d' são ambos dois máximos divisores comuns de um par de números, a e b por exemplo, então $d \geq d'$, pois d é o maior divisor comum de a e b e d' é um outro divisor comum, de modo análogo se mostra que $d' \geq d$, neste caso mostra que $d = d'$. Uma propriedade imediata é que não importa a ordem do par de números a e b , ou seja, $\text{mdc}(a, b) = \text{mdc}(b, a)$. Abaixo enunciamos e provamos algumas propriedades básicas, vista em Hefez [12] na forma de proposição:

Proposição 2.6. *Sejam a e $b \in \mathbb{N}$, então:*

- (i) $\text{mdc}(0, a) = a$.
- (ii) $\text{mdc}(1, a) = 1$.
- (iii) $\text{mdc}(a, a) = a$.
- (iv) Se $a | b$, então $\text{mdc}(a, b) = a$.

Demonstração: Cada uma das propriedades:

- (i) Primeiramente, vale lembrar que qualquer número é um divisor de 0 , pois $c | 0$, é o mesmo que $0 = f \cdot c$, para algum $f \in \mathbb{N}$, neste caso, tomando $f = 0$, logo para todo $c \in \mathbb{N}$, satisfaz a condição, portanto o conjunto dos divisores de 0 é o próprio conjunto dos números naturais não-nulo. Por outro lado, o maior dos divisores de a é o próprio a , $a | a$, pois $a = 1 \cdot a$, neste caso se conclui que $\text{mdc}(0, a) = a$.
- (ii) O único divisor do número 1 é o próprio 1 , pois dado $c \in \mathbb{N}$ e $c | 1$, ou seja $1 = f \cdot c$, com $f \in \mathbb{N}$, tal igualdade só é possível nos naturais quando $c = 1$ e $f = 1$. Por outro lado, 1 também é um divisor de a , pois $a = a \cdot 1$, o que mostra que $\text{mdc}(1, a) = 1$.

(iii) Como foi dito no item (i) acima, o maior divisor de a é o próprio a , e portanto, $\text{mdc}(a, a) = a$.

(iv) Da hipótese tem que $a \mid a$ e $a \mid b$, desse modo tomando um divisor comum c , ou seja, $c \mid a$ e $c \mid b$, temos então que $a \geq c$, logo $\text{mdc}(a, b) = a$.

■

A proposição abaixo 2.7 justificará o Algoritmo de Euclides, que em Hefez [12] é chamada de *Lema de Euclides*.

Proposição 2.7. *Dados $a, b, n \in \mathbb{N}$ com $a < na < b$. Vale a seguinte igualdade:*

$$\text{mdc}(a, b) = \text{mdc}(a, b - na).$$

Demonstração: Tomando $\text{mdc}(a, b - na) = d$, então $d \mid b - na$, por sua vez também $d \mid a$ (hipótese), deste modo $d \mid (b - na) + na$, logo $d \mid b$, assim d é um divisor comum de a e b , basta ver se d é máximo dos divisores comuns. Tomando $c \in \mathbb{N}$ um divisor comum de a e b , nesse caso $c \mid a$ e $c \mid b$, nesse caso $c \mid b - na$, e então $c \mid d$, logo $d \geq c$, portanto $\text{mdc}(a, b) = d$.

■

O corolário abaixo, uma consequência da proposição vista acima, esta presente em Santos [28], sendo que enunciada para os números inteiros.

Corolário 2.1. *Sejam $a, b \in \mathbb{N}$ a divisão euclidiana de b por a , $b = aq + r$, com $r < a$. Vale a igualdade:*

$$\text{mdc}(b, a) = \text{mdc}(a, r).$$

A demonstração desse corolário é idêntica com a proposição 2.7, observando que $r = b - aq$, portanto sua demonstração será omitida. Veja um exemplo que ilustra melhor o resultado acima.

Exemplo 2.11. *Qual é máximo divisor comum de 2252 e 1044?*

Resolução: Utilizando a divisão euclidiana, pois como foi visto anteriormente $mdc(2252, 1044)$ é igual ao $mdc(1044, r)$ em que r é o resto da divisão de 2252 por 1044, e repetindo sucessivamente a divisão euclidiana.

$$\begin{aligned} 2252 &= 1044 \cdot 2 + 164 \\ 1044 &= 164 \cdot 6 + 60 \\ 164 &= 60 \cdot 2 + 44 \\ 60 &= 44 \cdot 1 + 16 \\ 44 &= 16 \cdot 2 + 12 \\ 16 &= 12 \cdot 1 + 4 \\ 12 &= 4 \cdot 3 + 0. \end{aligned}$$

Ou seja, do teorema anterior temos: $mdc(2252, 1044)$ é igual ao $mdc(1044, 164)$, e também $mdc(1044, 164)$ é igual ao $mdc(164, 60)$ e continuando $mdc(164, 60)$ é igual ao $mdc(60, 44)$, continuando $mdc(44, 16)$ é igual ao $mdc(16, 12)$ e por fim $mdc(16, 12)$ é igual ao $mdc(12, 4) = 4$, ou seja $mdc(2252, 1044) = 4$.

■

Como uma aplicação da proposição 2.1 da divisão euclidiana a forma de determinar o mdc de dois números naturais.

Como o máximo divisor comum já é assunto no Ensino Fundamental, muitas vezes presentes no 6º ano ou 8ºano, é viável expor o Algoritmo de Euclides como apoio a uma forma alternativa para sua determinação, esta forma mais próxima da vista em textos de Aritmética.

Em Imenes [14] e [15] assim como em Ribeiro [26] e [27] não é abordado o máximo divisor comum; esses livros trazem essencialmente a mesma abordagem: nos livros de 6º ano são abordados os conceitos de múltiplos e divisores; Imenes [14], no livro do 6º ano, define o máximo divisor comum e no livro [15], do 8º ano, ensina o método de decomposição em números primos. Da mesma forma o livro de Ribeiro [26] do 6º ano, capítulo 7, traz

uma abordagem sobre múltiplos e divisores, enquanto no livro [27], do 8º ano, capítulo 1, que trata dos números primos, aborda sobre o mínimo múltiplo comum. Em ambos os autores, Imenes e Ribeiro, não abordam sobre o máximo divisor comum.

No Ensino Fundamental, o cálculo do mdc , quando visto, é efetuado usando a decomposição de números primos; quanto a definição de máximo divisor comum, basicamente utilizam a definição por conjuntos, e o cálculo para determinar o mdc é baseada na decomposição em números primos; tal exposição não explora diretamente a divisão dos números naturais, um conceito mais simples.

No livro de 5ª série de Gelson Iezzi [13] no capítulo sobre máximo divisor comum, são apresentados os dois métodos para determinar o mdc : o que o autor chama de “Regra das divisões sucessivas” para o cálculo, que é o algoritmo de Euclides, e o método chamado de “Regra da decomposição simultânea para achar o mdc ”. Veja um exemplo de como é encontrado o mdc de dois números com esse método.

Exemplo 2.12. Usando o algoritmo da decomposição em fatores primos, determine $mdc(100, 120)$.

Resolução: Fazendo as decomposições dos números 100 e 120 respectivamente:

$$\begin{array}{r|l}
 100 & 2 \\
 50 & 2 \\
 25 & 5 \\
 5 & 5 \\
 1 & \\
 \hline
 \end{array}
 \qquad
 \begin{array}{r|l}
 120 & 2 \\
 60 & 2 \\
 30 & 2 \\
 15 & 3 \\
 5 & 5 \\
 1 & \\
 \hline
 \end{array}$$

Como $100 = 2^2 \cdot 5^2$ e $120 = 2^3 \cdot 3 \cdot 5$, o $mdc(100, 120)$ será o produto dos fatores primos comuns com o menor dos expoentes de cada fator primo comum, ou seja, $mdc(100, 120) = 2^2 \cdot 5 = 20$.

■

Como um exemplo para mostrar a vantagem de um método em relação a outro método, veja a solução do exemplo (2.12), que pede o $mdc(100, 120)$, usando o algoritmo de Euclides:

$$120 = 100 \cdot 1 + 20$$

$$100 = 20 \cdot 5 + 0.$$

Portanto o $\text{mdc}(120, 100) = 20$, observe que apenas bastou uma conta, para obter o resultado desejado, sem muitos custos computacionais chega ao mdc usando divisão euclidiana. Imagine agora a situação: usando o método da decomposição por números primos, encontrar o mdc de dois números grandes; isso resultará em um custo computacional muito alto, traduzindo-se em muitas contas para os alunos realizarem, inclusive a dificuldade de saber se um número é ou não primo, um problema reconhecidamente de alta complexidade computacional. Desse modo o algoritmo de Euclides leva vantagem.

Exemplo 2.13. *Usando o algoritmo de Euclides, determine $\text{mdc}(186, 81)$.*

Resolução: Fazendo as divisões sucessivas:

$$186 = 81 \cdot 2 + 24$$

$$81 = 24 \cdot 3 + 9$$

$$24 = 9 \cdot 2 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 + 0$$

Nesse caso o último resto diferente de zero é 3, portanto $\text{mdc}(186, 81) = 3$

■

No exemplo abaixo é preciso determinar o mdc de três números, que pode ser calculado da igualdade $\text{mdc}(a, b, c) = \text{mdc}(\text{mdc}(a, b), c)$.

Exemplo 2.14. *Uma questão vista em Iezzi:*

Tenho 84 balas de coco, 144 balas de chocolate e 60 balas de leite. Quero formar pacotes de balas, sem misturar sabores. Todos os pacotes devem ter a mesma quantidade de balas e essa quantidade deve ser a maior possível. Quantas balas devo colocar em cada pacote? Quantos pacotes devo formar? (IEZZI, 2000, p.126)

Resolução: Para determinar o número de balas que deve-se colocar em cada pacote, basta perceber que um divisor comum dos números **84**, **144** e **60** garante que todos os pacotes tenham a mesma quantidade de balas, nesse caso para essa quantidade ser máxima, basta tomar o $mdc(84, 144, 60)$, então, o $mdc(84, 144)$;

$$144 = 84 \cdot 1 + 60$$

$$84 = 60 \cdot 1 + 24$$

$$60 = 24 \cdot 2 + 12$$

$$24 = 12 \cdot 2 + 0$$

logo $mdc(84, 144) = 12$, agora calcula-se o $mdc(12, 60) = 12$, pois $12 \mid 60$, portanto podemos tomar que $mdc(84, 144, 60) = 12$. Deve-se tomar **12** balas em cada pacote. Serão formados 12 pacotes com balas de chocolate, 7 pacotes de balas de coco e 5 pacotes de balas de leite.



3 *ENSINANDO*

CONGRUÊNCIA MÓDULO N

Neste capítulo será proposto uma possível transposição didática sobre congruência módulo n para o Ensino Básico, nesse caso justificada pela sua necessidade ao desenvolver um significado mais elaborado para o resto em uma divisão euclidiana.

Continuando o capítulo, será feito um estudo sobre a Aritmética dos restos e possíveis aplicações no Ensino Fundamental e Médio: inicialmente, serão mostrados alguns exemplos que envolvem a divisão euclidiana, levando à percepção de que existem alguns significados distintos para o resto que apenas o de “sobra”. Por fim uma breve explanação sobre paridade.

3.1 Introduzindo congruência no Ensino Básico

Geralmente grande parte das escolas públicas participam de olimpíadas matemáticas, especialmente a OBMEP. Por exemplo, em 2012 a OBMEP teve na inscrição para 1ª fase¹ 46.728 escolas participando com um total de 19.140.824 alunos, sendo 99,42% do total de municípios brasileiros. A quantidade de alunos que vão para a segunda fase fica bem abaixo da quantidade inicial; em 2012 foram 823.871, correspondendo a um percentual de 4,3%, ou seja, uma aprovação muito baixa. Dessa forma, evidencia-se a falta de preparo dos alunos, também deve-se observar que isso se deve a falta de preparação dos docentes.

Sem uma preparação diferenciada, os alunos geralmente não tem um desempenho satisfatório em olimpíadas matemáticas. A maioria das questões olímpicas envolvem um raciocínio mais elaborado e que exige um trabalho prévio de treinamento. Pensando nessa problemática a própria equipe da OBMEP, elabora materiais de apoio, como o banco de questões, e promove treinamentos.

¹Dados extraídos do site http://www.obmep.org.br/obmep_em_numeros.html, acessado em 21 de dezembro de 2012.

O amadurecimento mais efetivo da Aritmética vista no Ensino Básico e a capacidade de resolver questões da OBMEP semelhante à mostrada no capítulo anterior são objetivos para a introdução dos conceitos de congruência módulo n no Ensino Fundamental e Médio.

3.2 Um pouco sobre os Números Inteiros \mathbb{Z} .

No Ensino Fundamental, usualmente no 7º ano é introduzido o conjunto dos números inteiros. Apesar de não fazer parte do escopo deste trabalho uma proposta de ensino dos números inteiros, no entanto faz-se necessária algumas considerações, pois será usada a congruência nos inteiros.

Os números inteiros, em uma ideia mais informal, pode ser entendido como extensão dos números naturais. Sabendo que a operação de subtração dos números naturais $a - b$, não tem significado quando $a < b$, nesse caso, os novos números permitem tais subtrações, assim como são interpretados intuitivamente como uma dívida ou uma perda, por exemplo, $15 - 20 = -5$, pode ser entendida como, tendo um valor de R\$ 15,00, porém uma dívida de R\$ 20,00, após pagar com o que se tem fica ainda uma dívida de R\$ 5,00. Os números inteiros são divididos em positivos, maiores que zero, $+1 = 1$, $+2 = 2$, $+3 = 3$, $+4 = 4$, $+5 = 5$, $+6 = 6...$ e negativos, quando são menores que zero, resultado de subtrações $a - b$ com b maior que a , são eles -1 , -2 , -3 , -4 , -5 , $-6...$ também inclui aos números inteiros o número zero.

Os números inteiros são representados por \mathbb{Z} .

$$\mathbb{Z} = \{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \dots\}.$$

As definições e propriedades da divisibilidade são análogas as presentes para os naturais. Quanto ao algoritmo da divisão de Euclides, seu enunciado segundo Domingues [9] é um pouco distinto;

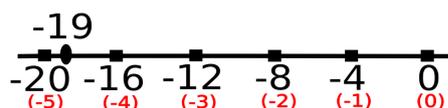
Teorema 3.1 (Divisão Euclidiana em \mathbb{Z}). *Para quaisquer $a, b \in \mathbb{Z}$, $b > 0$, existe um único par de inteiros q e r , de maneira que $a = bq + r$, onde $0 \leq r < b$.*

A demonstração deste teorema é análoga à feita para os números naturais.

Exemplo 3.1. *O quociente e o resto da divisão de -19 por 4 é $q = -5$ e $r = 1$, pois $-19 = 4 \cdot (-5) + 1$.*

Ilustrando a divisão em uma reta numerada, como foi visto no capítulo anterior:

Quadro 3: Representação da divisão em uma reta.



Fonte: AUTOR 2013

com $1 = -19 - 4 \cdot (-5)$.

Já a definição para o máximo divisor comum segundo Domingues [9] é dado por:

Definição 3.1 (MDC em \mathbb{Z}). *Sejam a e b números inteiros quaisquer. O máximo divisor comum de a e b é definido por:*

$$\text{mdc}(a, b) = \text{mdc}(|a|, |b|),$$

Onde $|a|$ denota o valor absoluto de a .

Nesse caso, o *mdc* de dois inteiros é uma extensão natural do *mdc* de dois naturais.

Uma proposição importante para essa teoria, e fundamental para o que tratará o próximo capítulo, de equações diofantinas é a chamada identidade de Bachet-Bézout vista em Oliveira [21].

Proposição 3.1. *Sejam a e $b \in \mathbb{Z}$ com $d = \text{mdc}(a, b)$. Então existem dois outros inteiros x_0 e y_0 de maneira que vale a igualdade*

$$d = a \cdot x_0 + b \cdot y_0.$$

Demonstração: Para $a = 0$ e $b \neq 0$, temos $\text{mdc}(a, b) = b$ e nesse caso para qualquer $x_0 \in \mathbb{Z}$ e $y_0 = 1$, temos a igualdade $b = a \cdot x_0 + b \cdot 1$. Do mesmo modo, se $a \neq 0$ e $b = 0$, $\text{mdc}(a, b) = a$, para quaisquer inteiros y_0 e $x_0 = 1$, vale que $a = a \cdot 1 + b \cdot y_0$.

Para a e b diferentes de zero, tomando o conjunto

$$S = \{a \cdot x + b \cdot y \mid x, y \in \mathbb{Z}\}.$$

Como visto, esse conjunto contém o zero, assim como números negativos e positivos, considerando o conjunto S_+^* , constituído apenas pelos elementos positivos de S , pelo Princípio da Boa Ordem, existe um menor elemento de S_+^* , nesse caso será denotado por δ que será igual a $a \cdot x_0 + b \cdot y_0$, para certos inteiros x_0 e y_0 .

Será provado então que $\delta \mid a$ e de modo análogo $\delta \mid b$. Por absurdo, afirmando que $\delta \nmid a$, assim pela divisão euclidiana de a por δ existe r que vale a desigualdade $0 < r < \delta$ e além disso $r = a - \delta \cdot q$. Portanto,

$$\begin{aligned} r = a - \delta \cdot q &= a - (a \cdot x_0 + b \cdot y_0) \cdot q \\ r &= a(1 - q \cdot x_0) + b(-qy_0) \end{aligned}$$

o que é uma contradição, pois $r \notin S_+^*$, já que δ é o menor elemento de S_+^* e portanto $\delta \mid a$, do mesmo modo se prova que $\delta \mid b$.

Já provado que δ é um divisor comum de a e b , basta provar que δ é máximo.

Tomando $d = \text{mdc}(a, b)$, $a = d \cdot a_0$ e $b = d \cdot b_0$, então

$$\delta = a(d \cdot a_0) + b(d \cdot b_0).$$

Ou seja, $\delta = d(a \cdot x_0 + b \cdot y_0)$, portanto, $d \mid \delta$, daí $\delta \geq d$, mas d é o máximo divisor comum, logo $\delta = d$ o que prova a proposição. ■

Os valores de x_0 e y_0 encontrados na proposição 3.1 não são únicos.

Exemplo 3.2. Usando o processo das divisões sucessivas encontre dois números, x_0 e y_0 para que $\text{mdc}(12, 45) = 12 \cdot x_0 + 45 \cdot y_0$.

Resolução: Determinando o $mdc(12, 45)$:

$$45 = 12 \cdot 3 + 9 \quad (3.1)$$

$$12 = 9 \cdot 1 + 3 \quad (3.2)$$

$$9 = 3 \cdot 3 + 0.$$

Portanto $mdc(12, 45) = 3$. Da equação (3.2), tem $3 = 12 - 9 \cdot 1$; substituindo 9 por $45 - 12 \cdot 3$ vista na equação (3.1):

$$3 = 12 - (45 - 12 \cdot 3) \cdot 1$$

$$3 = 12 - 45 + 12 \cdot 3$$

$$3 = 12 \cdot 4 - 45$$

$$3 = 12 \cdot 4 + 45 \cdot (-1).$$

Neste caso $x_0 = 4$ e $y_0 = -1$.

■

3.3 Aritmética dos restos

Um dos tópicos que faz parte da proposta dessa dissertação é a inserção da Aritmética dos restos como uma proposta de ensino para os alunos do Ensino Fundamental com o objetivo de promover um amadurecimento da divisão euclidiana como também de enriquecer os conceitos que têm o próprio resto de uma divisão euclidiana nos naturais ou inteiros.

Quando dois números, ou um conjunto maior de números, têm a característica de ter o mesmo resto em uma divisão por algum número inteiro dado, é possível estabelecer certas similaridades. Por exemplo 13 e 28, deixam resto 3 quando divididos por 5. Se a ambos somarmos ou subtrairmos um mesmo número, os novos restos da divisão por 5 continuarão os mesmos, vejamos, $13 + 7 = 20$ e $28 + 7 = 35$; 20 e 35 deixam resto 0 na divisão por 5, observe que 7 deixa resto 2 na divisão por 5, neste caso o resto 3, das divisões de 13 e 28 por 5, somado com o resto 2, resulta em 5, que na divisão por 5 dá resto 0. Estas relações serão melhor definidas e demonstradas a seguir.

De acordo com Hefez [12].

Definição 3.2 (congruência módulo n). Dado $n \in \mathbb{N}$, $n \neq 0$, dois números inteiros a e b são **congruentes módulo n** quando o resto da divisão euclidiana de a por n é igual ao resto da divisão euclidiana de b por n e denota por

$$a \equiv b \pmod{n}.$$

Desta mesma forma, pode-se definir números incôngruos módulo n (com notação $\not\equiv$), quando dois números a e b não têm os mesmos restos na divisão por n .

Exemplo 3.3. $73 \equiv 52 \pmod{3}$, pois $73 = 3 \cdot 24 + 1$ e $52 = 3 \cdot 17 + 1$, ambos têm resto 1 na divisão por 3.

Do mesmo modo $-43 \equiv -88 \pmod{5}$, pois $-43 = 5 \cdot (-9) + 2$ e $-88 = 5 \cdot (-18) + 2$, ambos têm resto 2 na divisão por 5.

Exemplo 3.4. $13 \not\equiv 16 \pmod{7}$, pois $13 = 1 \cdot 7 + 6$ e $16 = 2 \cdot 7 + 2$, ambos restos diferentes na divisão por 7.

Repare que no exemplo acima $73 - 52 = 3 \cdot 24 + 1 - 3 \cdot 17 - 1 = 21$ e $3 \mid 21$, esta relação não é coincidência. Veja a proposição seguinte vista em Hefez [12].

Proposição 3.2. Dados $a, b \in \mathbb{Z}$ tem-se $a \equiv b \pmod{n}$ se, e somente se, $n \mid b - a$.

Demonstração: Pela definição, existe $r \in \mathbb{Z}$, com $0 \leq r < n$, tal que $b = n \cdot q_1 + r$ e $a = n \cdot q_2 + r$, portanto $b - a = n \cdot q_1 + r - (n \cdot q_2 + r)$, ou seja, $b - a = n \cdot q_1 - n \cdot q_2 = n(q_1 - q_2)$, logo, $n \mid b - a$.

Para a volta da proposição, tomando a e $b \in \mathbb{Z}$, como $n \mid b - a$. Também fazendo as divisões de a e b por n , tem respectivamente $a = n \cdot q_1 + r_1$ com $0 \leq r_1 < n$ e $b = n \cdot q_2 + r_2$, $r_2 < n$. Temos:

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

e portanto $-n < r_1 - r_2 < n$, pois r_1 e r_2 são ambos menores que n . Por outro lado $n \mid b - a$, implicando em $n \mid r_1 - r_2$. Como $-n < r_1 - r_2 < n$, temos $r_1 - r_2 = 0$ e por fim $r_1 = r_2$; logo $a \equiv b \pmod{n}$.

■

Exemplo 3.5. $7 \equiv 2 \pmod{5}$, pois $5 \mid 7 - 2$ e $6 \not\equiv 3 \pmod{4}$, porque $4 \nmid 6 - 3$.

A congruência módulo n é uma relação de equivalência, ou seja, se comporta, em certo sentido, como uma igualdade. Veja a proposição abaixo presente em Domingues [9].

Proposição 3.3. *Seja $n \in \mathbb{Z}$, $n > 1$. Para todos $a, b, c \in \mathbb{Z}$, vale*

(i) $a \equiv a \pmod{n}$.

(ii) $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$.

(iii) $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$.

Demonstração: Demonstrando cada parte:

(i) Da proposição 3.2, $a \equiv a \pmod{n} \iff n \mid a - a$ e de fato, $n \mid 0$.

(ii) Se $a \equiv b \pmod{n}$, então $n \mid b - a$, ou seja, existe $f \in \mathbb{Z}$, tal que $b - a = f \cdot n$, então $a - b = (-f) \cdot n$, ou seja, $b \equiv a \pmod{n}$.

(iii) De $a \equiv b \pmod{n}$, da proposição 3.2, $n \mid b - a$, assim como em $b \equiv c \pmod{n}$ $n \mid c - b$, então $n \mid (b - a) + (c - b)$, ou seja, $n \mid c - a$ e portanto $a \equiv c \pmod{n}$.

■

Como na proposição anterior, no que segue serão tomadas sempre como hipótese que $n > 1$. A proposição abaixo mostra que a soma, subtração e multiplicação dos inteiros preserva uma congruência como mostra a proposição vista Hefez [12].

Proposição 3.4. *Sejam a, b, c e $n \in \mathbb{Z}$, com $n > 1$. Se $a \equiv b \pmod{n}$, então:*

(i) $a \pm c \equiv b \pm c \pmod{n}$.

(ii) $a \cdot c \equiv b \cdot c \pmod{n}$.

Demonstração:

(i) A partir da hipótese:

$$a \equiv b \pmod{n} \implies n \mid b - a.$$

Somando e subtraindo por c o segundo membro da relação de divisibilidade:

$$n \mid (b \pm c) - (a \pm c) \implies a \pm c \equiv b \pm c \pmod{n}$$

(ii) Para provar que a multiplicação se preserva. Por hipótese e pela proposição (3.2) $b - a = f \cdot n$, $f \in \mathbb{Z}$, multiplicando a igualdade por $c \in \mathbb{Z}$, $bc - ac = fc \cdot n$ e portanto $a \cdot c \equiv b \cdot c \pmod{n}$.

■

Exemplo 3.6. $10 \equiv 17 \pmod{7}$, pois 10 e 17 deixam restos 3 na divisão por 7, $10 + 8 \equiv 17 + 8 \pmod{7}$, $18 \equiv 25 \pmod{7}$ pois 18 e 25 deixam restos 4 na divisão por 7. Também $10 \cdot 3 \equiv 17 \cdot 3 \pmod{7}$, $30 \equiv 51 \pmod{7}$ pois 30 e 51 deixam restos 2 na divisão por 7.

A proposição abaixo também é vista em Domingues [9].

Proposição 3.5. *Sejam a, b, c, d e $n \in \mathbb{Z}$, com $n > 1$. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:*

(i) $a \pm c \equiv b \pm d \pmod{n}$.

(ii) $a \cdot c \equiv b \cdot d \pmod{n}$.

Demonstração: Provando cada parte:

(i) Das hipóteses:

$$n \mid b-a \text{ e } n \mid d-c \implies n \mid (b \pm d) - (a \pm c).$$

Daí,

$$a \pm c \equiv b \pm d \pmod{n}.$$

(ii) Das hipóteses e da proposição (3.4) decorre que $a \cdot c \equiv b \cdot c \pmod{n}$ e $c \cdot b \equiv d \cdot b \pmod{n}$. Pela transitividade: $a \cdot c \equiv b \cdot d \pmod{n}$.

■

Exemplo 3.7. $12 \equiv 37 \pmod{5}$, pois 12 e 37 deixam restos 2 na divisão por 5. $23 \equiv 48 \pmod{5}$, pois 23 e 48 deixam restos 3 na divisão por 5, logo $12 + 23 \equiv 37 + 48 \pmod{5}$, $35 \equiv 85 \pmod{5}$ pois 35 e 85 deixam restos 0 na divisão por 5. Também $12 \cdot 23 \equiv 37 \cdot 48 \pmod{5}$, $276 \equiv 1776 \pmod{5}$ pois 276 e 1776 deixam restos 1 na divisão por 5.

O corolário abaixo é também visto em Domingues [9].

Corolário 3.1. Dados $a, b, e \in \mathbb{Z}$, com $e \geq 1$. Se $a \equiv b \pmod{n}$, então $a^e \equiv b^e \pmod{n}$.

Demonstração: Se $a \equiv b \pmod{n}$, pela proposição anterior, $a \cdot a \equiv b \cdot b \pmod{n}$, e aplicando a mesma proposição e vezes, $a^e \equiv b^e \pmod{n}$.

■

Exemplo 3.8. $2 \equiv 5 \pmod{3}$, então por exemplo para $e = 4$, $2^4 \equiv 5^4 \pmod{3}$, $16 \equiv 625 \pmod{3}$, pois 16 e 625 deixam resto 1 na divisão por 3.

Exemplo 3.9. Mostre que $10^{200} - 1$ é divisível por 11.

Resolução: Como $10 \equiv -1 \pmod{11}$, então $10^{200} \equiv (-1)^{200} \pmod{11}$, $10^{200} \equiv 1 \pmod{11}$ e portanto $10^{200} - 1 \equiv 0 \pmod{11}$, ou seja

$$11 \mid (10^{200} - 1).$$

■

A proposição seguinte é encontrada também em Domingues [9].

Proposição 3.6. *Dados $a, b, c \in \mathbb{Z}$. Se $c \cdot a \equiv c \cdot b \pmod{n}$ e $\text{mdc}(n, c) = d \neq 0$, então*

$$a \equiv b \pmod{\frac{n}{d}}$$

.

Demonstração: Pela hipótese e pela proposição 3.2 vale $n \mid c \cdot (b - a)$, ou seja, $c \cdot (b - a) = kn$, com $k \in \mathbb{Z}$, portanto:

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

Desse modo $\text{mdc}\left(\frac{c}{d}, \frac{n}{d}\right) = 1$ e portanto $a \equiv b \pmod{\frac{n}{d}}$.

■

Exemplo 3.10. *Como $32 \equiv 18 \pmod{14}$, ou seja $2 \cdot 16 \equiv 2 \cdot 9 \pmod{14}$ e $\text{mdc}(2, 14) = 2$ vale a congruência $16 \equiv 9 \pmod{7}$.*

Os dois exemplos abaixo ilustram consequências da proposição 3.6.

Exemplo 3.11. *Se $c \cdot a \equiv c \cdot b \pmod{n}$ e $\text{mdc}(c, n) = 1$, então $a \equiv b \pmod{c}$. Por exemplo, $10 \equiv 30 \pmod{4}$, como $\text{mdc}(4, 5) = 1$, então $2 \equiv 6 \pmod{4}$.*

Exemplo 3.12. *Se $c \cdot a \equiv c \cdot b \pmod{p}$ com p primo e $p \nmid c$, então $a \equiv b \pmod{p}$. Por exemplo, $20 \equiv 35 \pmod{3}$, como $3 \nmid 5$, logo $4 \equiv 7 \pmod{3}$.*

Segue abaixo mais uma proposição que mostra algumas outras propriedades de congruência vista igualmente em Hefez [12].

Proposição 3.7. *Sejam $a, b \in \mathbb{Z}$ e m, n números inteiros positivos diferente de 1:*

(i) $a \equiv b \pmod{m}$ e $n \mid m \implies a \equiv b \pmod{n}$.

(ii) $a \equiv b \pmod{m} \implies \text{mdc}(a, m) = \text{mdc}(b, m)$.

Demonstração: Provando cada parte da proposição e sem perder a generalidade, toma-se $b \geq a$:

(i) Pela hipótese e a proposição (3.2), vale que $m \mid b - a$ e $n \mid m$; por transitividade, $n \mid b - a$, portanto $a \equiv b \pmod{n}$.

(ii) Pela definição a e b têm os mesmos restos da divisão euclidiana, ou seja, $a = m \cdot q_a + r$ e $b = m \cdot q_b + r$, com $0 \leq r < n$, como visto no capítulo anterior. Visto que $\text{mdc}(a, b) = \text{mdc}(a, a \cdot q + r) = \text{mdc}(a, r)$, para $b = a \cdot q + r$, temos $\text{mdc}(a, m) = \text{mdc}(m, m \cdot q_a + r) = \text{mdc}(m, r) = \text{mdc}(m, b \cdot q_b + r) = \text{mdc}(m, b)$.

■

Exemplo 3.13. *Mostre que $2^{20} - 1$ é divisível por 41.*

Resolução: Como $1024 \equiv 40 \pmod{41}$, pois $1024 = 41 \cdot 24 + 40$, logo $2^{10} \equiv -1 \pmod{41}$, elevando cada membro da congruência por 2, $2^{20} \equiv 1 \pmod{41}$, ou seja, $41 \mid 2^{20} - 1$.

■

3.4 Aplicações de congruência vista no Ensino Básico

3.4.1 Significado do resto

A motivação dessa seção é perceber que o resto de uma divisão euclidiana tem significados distintos além do de sobra, geralmente vista em livros didáticos do Ensino Fundamental.

Antes da exposição de enunciados de problemas, é importante saber o que significa eventos cíclicos: um conjunto de eventos ou sequência de valores é cíclica, quando a partir de um momento (esse momento chamado de *período*), o conjunto de eventos ou a sequência de valores se repetem na mesma ordem vista anteriormente.

É muito comum encontrar questões da OBMEP que envolvem situações cíclicas, cuja solução é encontrar um resto da divisão euclidiana do número ordinal que corresponde a posição desejada pelo período encontrado na situação cíclica analisada.

Exemplo 3.14. [OBMEP (2012),

1ª Fase, Nível 2] Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas. Em cada embaralhamento, a primeira carta passa a ser a segunda, a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira. Qual será a primeira carta após 2012 embaralhamentos?



Resolução: Primeiramente listando as posições das cartas e fazendo os embaralhamentos sucessivos de acordo com a regra definida pelo enunciado:

- posição inicial: A2345
- depois do 1º embaralhamento: 3A524
- depois do 2º embaralhamento: 534A2
- depois do 3º embaralhamento: 4523A
- depois do 4º embaralhamento: 24A53
- depois do 5º embaralhamento: A2345, que é a primeira posição

Assim, de 5 em 5 embaralhamentos retornamos à primeira posição, e nesse caso efetua a divisão euclidiana de 2012 por 5, ou seja, $2012 = 5 \cdot 402 + 2$. A posição das cartas depois do 2012º embaralhamento é idêntica que à posição depois do 2º embaralhamento, portanto a primeira carta é a de número 5.



Observe a partir do exemplo acima que o resto da divisão do n -ésimo embaralhamento por 5, representa uma categoria específica, ou seja, se o resto for 1, então as cartas estarão dispostas como na posição inicial, se o resto for 2, as cartas estarão dispostas na posição da mesma forma vista depois do 1 embaralhamento e assim por diante. Este exemplo bem representa uma situação cíclica.

O exemplo seguinte, muito simples e de fácil entendimento, é sem dúvida uma boa situação-problema para introduzir congruência no Ensino Básico.

Exemplo 3.15. *Uma empresa de coleta de lixo dividiu um município em 150 áreas para realizar a coleta de lixo nas casas.*

Abaixo segue um cronograma para a coleta:

<i>Domingo</i>	<i>Segunda</i>	<i>Terça</i>	<i>Quarta</i>	<i>Quinta</i>	<i>Sexta</i>	<i>Sábado</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>	<i>12</i>	<i>13</i>	<i>14</i>
<i>15</i>	<i>16</i>	<i>17</i>	<i>18</i>	<i>19</i>	<i>20</i>	<i>21</i>
<i>22</i>	<i>23</i>	<i>24</i>	<i>...</i>	<i>...</i>	<i>...</i>	<i>...</i>

Pergunta-se:

- 1. Em que dia da semana a área 45 deve esperar o caminhão de lixo? E a área 60 e a área 100?*
- 2. Quantas áreas diferentes essa empresa de coleta de lixo visita na terça-feira? E no sábado?*
- 3. É possível estabelecer uma relação entre a distribuição das áreas e cada dia da semana? Qual?*

Resolução: Respondendo cada item:

1. Observe que as áreas se dividem entre os dias da semana de forma muito homogênea; percebe-se que no domingo são as áreas 1, 8, 15, 22, e assim por diante, ou seja, números da forma $7 \cdot k + 1$. De modo semelhante temos para as áreas da segunda em diante.

Efetuando a divisão euclidiana de 45 por 7 temos, $45 = 7 \cdot 6 + 3$, do mesmo modo, dividindo 60 por 7, $60 = 7 \cdot 8 + 4$, assim como $100 = 7 \cdot 14 + 2$. Por fim a área 45 o caminhão de lixo passará na terça-feira, a área 60 o caminhão de lixo passará na quarta-feira e na área 100, o caminhão de lixo passará na segunda-feira.

2. Como são 150 áreas, temos nesse caso que as 150 áreas se dividem em 7 dias da semana, $150 = 7 \cdot 21 + 3$, olhando , ou melhor, imaginando a tabela acima completa, terá 21 linhas preenchidas e mais uma linha até a terça-feira, veja como fica a linha final da tabela:

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
148	149	150				

Assim na terça-feira a empresa coleta lixo em 22 áreas e no sábado 21 áreas diferentes.

3. Sim é possível estabelecer uma relação entre a distribuição das áreas e os dias da semana. A relação é o resto da divisão do número correspondente a área pelo número 7, dias totais da semana, valendo a seguinte relação:

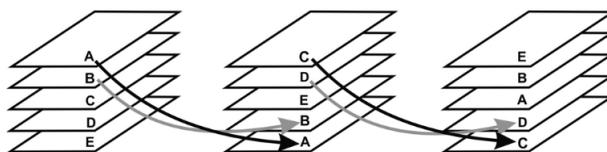
dia	resto
Domingo	1
Segunda	2
Terça	3
Quarta	4
Quinta	5
Sexta	6
Sábado	0

Cada resto corresponde a um dia da semana.



No exemplo visto acima está associado um conjunto específico de números em dias e esta associação é feita a partir do resto da divisão.

Exemplo 3.16. *[OBMEP (2012), Banco de Questões] Estefânia tem cinco cartas marcadas com as letras A, B, C, D e E, empilhadas nessa ordem de cima para baixo. Ela embaralha as cartas pegando as duas de cima e colocando-as, com a ordem trocada, embaixo da pilha. A figura mostra o que acontece nas duas primeiras vezes em que ela embaralha as cartas.*



Se Estefânia embaralhar as cartas 74 vezes, qual carta estará no topo da pilha?

- A) A B) B C) C D) D E) E

Resolução: Empilhamento conforme o enunciando até chegar na posição inicial:

posição inicial	1º	2º	3º	4º	5º	6º
A	C	E	A	C	E	A
B	D	B	D	B	D	B
C	E	A	C	E	A	C
D	B	D	B	D	B	D
E	A	C	E	A	C	E

Como no sexto empilhamento as cartas voltam à posição inicial, o que quer dizer que a cada seis empilhamentos, volta-se a posição inicial, ou seja, no 6º, 12º, 18º, 24º e assim por diante, se tem cartas iguais à posição inicial. Fazendo a divisão euclidiana de 74 por 6, $74 = 6 \cdot 12 + 2$, como o resto da divisão é 2, então a carta que estará no topo da pilha na posição septuagésima quarta é igual a pilha de cartas na segunda posição, como resposta a carta E.

■

Esses três exemplos deixam claro que o resto de uma divisão não apenas tem o significado de sobra como é usualmente encontrado nos livros didáticos.

Com um correto significado para o resto de uma divisão euclidiana, poder organizar os elementos de um conjunto dado em categorias bem definidas e assim dado um evento cíclico, pode-se "prever" o que acontecerá em uma ordem futura.

3.4.2 A congruência como apoio à compreensão de outros conceitos no Ensino Básico

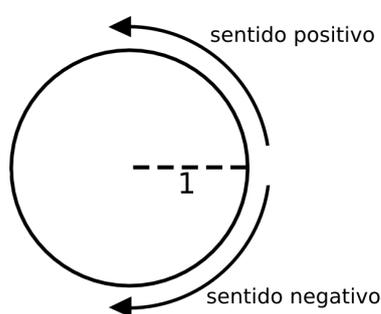
Nesta seção serão mostrados dois momentos do Ensino Médio em que pode ser usada a congruência. O primeiro é quanto aos arcos côngruos e o segundo exemplo é sobre potências do número complexo $i = \sqrt{-1}$.

Na exposição dos conceitos básicos da trigonometria, um elemento importante é a *circunferência unitária* ou *circunferência trigonométrica*, como diz Dante:

Denomina-se *circunferência unitária* (ou *circunferência trigonométrica*) a circunferência orientada cujo raio é 1 unidade de comprimento e na qual o sentido positivo é anti-horário. (DANTE, 2004, p.27)

Ilustrando a definição acima:

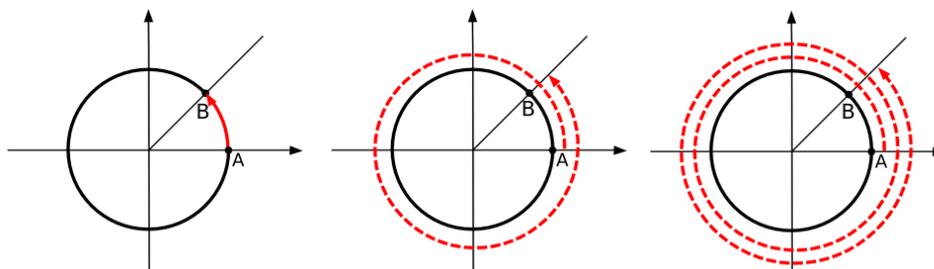
Quadro 4: Circunferência trigonométrica.



Fonte: AUTOR 2013

Observando agora a figura abaixo, veja que, tomando um ângulo $\alpha = med(A\hat{O}B)$, dando uma volta ou n voltas completas sobre o círculo não se altera a posição final do ângulo, neste caso, são chamados de ângulos côngruos.

Quadro 5: Arcos côngruos.



Fonte: AUTOR 2013

Portanto dado um ângulo qualquer α (com a notação de graus), os ângulos da forma $\alpha + 360^\circ \cdot k$, com $k \in \mathbb{Z}$ são os chamados ângulos congruentes a α , e suas representações na circunferência acima coincidem.

Observe que a notação de congruência \equiv pode ser abertamente utilizada pelo professor no momento em que definir arcos côngruos, por exemplo, o arco de 490° é côngruo

Quando se estuda os complexos \mathbb{C} , o cálculo das potências naturais da chamada unidade imaginária $i = \sqrt{-1}$ é um momento possível para aplicação dos conceitos de congruência.

Considerando as operações usuais dos números complexos, vamos resolver a seguinte questão:

Exemplo 3.18. *Efetue as operações indicadas:*

$$a) i^0, i^1, i^2, i^3, i^4, i^5, i^6, i^7, i^8$$

Resolução: Resolvendo diretamente, sem muitos detalhes:

$$\begin{aligned} i^0 &= 1 \\ i^1 &= i \\ i^2 &= -1 \\ i^3 &= i^2 i = (-1)i = -i \\ i^4 &= (i^2)^2 = (-1)^2 = 1 \\ i^5 &= i^4 i = (1)i = i \\ i^6 &= i^4 i^2 = (1)(-1) = -1 \\ i^7 &= i^4 i^3 = (1)(-i) = -i \\ i^8 &= i^4 i^4 = (1)(1) = 1. \end{aligned}$$

■

Continuando as potências de i , percebemos que trata-se de um problema cíclico, onde as potências se repetem a cada ciclo de 4, conforme quadro:

$$\begin{aligned} i^{4n} &= (i^4)^n = (1)^n = 1 \\ i^{4n+1} &= (i^4)^n i = (1)^n i = i \\ i^{4n+2} &= (i^4)^n (i^2) = (1)^n (-1) = -1 \\ i^{4n+3} &= (i^4)^n (i^3) = (1)^n (-i) = -i. \end{aligned}$$

Desse modo pode-se usar as seguintes congruências sobre o expoente das potências de i e então determinar quais valores do conjunto $\{1, i, -1, -i\}$ vale a potência, assim:

expoente de $i \equiv 0 \pmod{4} \implies$ potência de $i = 1$,
 expoente de $i \equiv 1 \pmod{4} \implies$ potência de $i = i$,
 expoente de $i \equiv 2 \pmod{4} \implies$ potência de $i = -1$,
 expoente de $i \equiv 3 \pmod{4} \implies$ potência de $i = -i$.

Exemplo 3.19. Calcule o valor de:

(a) i^{56} (b) i^{203} (c) $4i^{70} - i^{15}$

Resolução:

(a) Como $56 \equiv 0 \pmod{4}$, então $i^{56} = i^0 = 1$.

(b) Da mesma forma $203 \equiv 3 \pmod{4}$ e então $i^{203} = i^3 = -i$.

(c) De um lado $70 \equiv 2 \pmod{4}$ e $15 \equiv 3 \pmod{4}$, por outro lado $4i^{70} - i^{15}$ é o mesmo que $4i^2 - i^3$ que por sua vez vale $4(-1) - (-i) = -4 + i$.

■

3.5 Paridade

Nesta seção será visto um caso bem simples de como lidar com os restos de uma divisão por algum número inteiro.

Aqui trataremos sobre a paridade de um número inteiro, isto é, o fato deste número ser chamado de par ou de ímpar: um número é chamado de par quando na divisão euclidiana por dois deixa resto 0 e é chamado de ímpar quando o resto da divisão desse número por 2 é igual a 1, ou seja, na divisão por 2 há apenas duas possibilidades de resto: 0 ou 1.

Vale analisar algumas considerações sobre a soma de números pares e ímpares:

1. A soma de dois números a e b pares é par, pois fazendo a divisão euclidiana por 2, tem-se $a = 2 \cdot k_1$; do mesmo modo $b = 2 \cdot k_2$, a soma $a + b = 2 \cdot (k_1 + k_2)$ e portanto um número par.

2. A soma de dois números ímpares é par, pois tomando um número natural ímpar a , sua divisão euclidiana por 2 é $a = 2 \cdot k_1 + 1$, assim como b ímpar, sua divisão por 2 é $b = 2 \cdot k_2 + 1$, nesse caso a soma de $a + b$ é $a + b = 2 \cdot (k_1 + k_2) + 2$ e portanto $a + b = 2 \cdot (k_1 + k_2) + 0$, ou seja, a soma é par.
3. A soma de um número par com um ímpar é ímpar, do mesmo modo do que foi feito no casos anteriores.

Também vale analisar algumas considerações sobre o produto de números pares e ímpares:

1. O produto de dois números pares é par, pois tomando um número inteiro a , par, fazendo a divisão euclidiana por 2 fica $a = 2 \cdot k_1 + 0$, do mesmo modo $b \in \mathbb{Z}$ sua divisão por 2 é $b = 2 \cdot k_2 + 0$, o produto é $a \cdot b = 4 \cdot k_1 \cdot k_2 = 2(2 \cdot k_1 k_2) + 0$ e portanto um número par.
2. O produto de dois números ímpares é ímpar, pois tomando um número $a \in \mathbb{Z}$, sua divisão euclidiana por 2 é $a = 2 \cdot k_1 + 1$, assim como $b \in \mathbb{Z}$ sua divisão por 2 é $b = 2 \cdot k_2 + 1$, nesse caso o produto de a por b é $a \cdot b = 2 \cdot k_1(2 \cdot k_2 + 1) + 1 \cdot (2 \cdot k_2 + 1)$ e portanto $a \cdot b = 2(2k_1k_2 + k_1 + k_2) + 1$, ou seja o produto é ímpar.
3. O produto de um número par com um ímpar é par, do mesmo modo, tomando a e b , um par e outro ímpar, respectivamente suas divisões por 2 são; $a = 2 \cdot k_1 + 0$ e $b = 2 \cdot k_2 + 1$, seu produto $a \cdot b = (2k_1)(2k_2 + 1) = 4k_1k_2 + 2k_1$ e portanto $a \cdot b = 2 \cdot (2k_1k_2 + k_1) + 0$, ou seja, o produto é par.

Tomando como $\bar{0}$ para representar os números pares e $\bar{1}$ os números ímpares, ou seja:

$$\begin{aligned}\bar{0} &= \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots, 2 \cdot k + 0, \dots\} \\ \bar{1} &= \{\dots, -5, -3, -1, 1, 3, 5, \dots, 2 \cdot k + 1, \dots\}.\end{aligned}$$

As considerações feitas acima podem ser expressas nas seguintes tabelas que resumem a paridade dos números, podendo estas tabelas serem chamadas de tabuadas de operações:

$$\begin{array}{c|cc} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} \end{array} \qquad \begin{array}{c|cc} \times & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \bar{1} \end{array}$$

Com esta tabuada é possível determinar a paridade de qualquer operação de soma, produto ou potência de números que não precise efetuar a conta, por exemplo:

Exemplo 3.20. *Determine a paridade do seguinte número:*

$$(123275 + 346231)^{234} + (3451 + 4532)^{542}.$$

Resolução: Como exposto, não é preciso operar para saber se é par ou ímpar, basta usar o que foi dito anteriormente, assim substituindo 123275 por $\bar{1}$, 346231 por $\bar{1}$, 3451 por $\bar{1}$ e 4532 por $\bar{0}$, a expressão fica:

$$(\bar{1} + \bar{1})^{234} + (\bar{1} + \bar{0})^{542}.$$

E assim, observando os resultados da tabuada :

$$\bar{0}^{234} + \bar{1}^{542}.$$

Quanto as potências, uma potência de par sempre será par, e uma potência de ímpar sempre será ímpar, portanto:

$$\bar{0} + \bar{1}.$$

Logo $\bar{0} + \bar{1} = \bar{1}$, então o número é ímpar.

■

3.6 Classe residual módulo 3.

O conceito de paridade visto na seção anterior pode ser generalizado para quaisquer valor, veja o exemplo abaixo para o número 3:

Exemplo 3.21. *Quaisquer números inteiros n podem ser escritos usando a divisão euclidiana por 3 das seguintes maneiras $n = 3 \cdot k + 0$, $n = 3 \cdot k + 1$ ou $n = 3 \cdot k + 2$, com k sendo um inteiro, desse modo será possível dispor números inteiros da seguinte forma:*

<i>resto 0</i>	<i>resto 1</i>	<i>resto 2</i>
\vdots	\vdots	\vdots
-6	-5	-4
-3	-2	-1
0	1	2
3	4	5
6	7	8
9	10	11
\vdots	\vdots	\vdots

Observe que se continuar essa tabela de modo que se dispusessem todos os inteiros estaria partindo os números inteiros em três categorias, classes ou conjuntos, classes essas que são classificadas pelo seu resto da divisão por 3. E por nomenclatura serão chamadas as seguintes categorias de *classes residuais*, e por notação terá:

$$\bar{0} = \{\dots, -6, -3, 0, 3, 6, 9, 12, \dots, 3 \cdot k + 0, \dots\}$$

$$\bar{1} = \{\dots, -5, -2, 1, 4, 7, 10, 13, \dots, 3 \cdot k + 1, \dots\}$$

$$\bar{2} = \{\dots, -4, -1, 2, 5, 8, 11, 14, \dots, 3 \cdot k + 2, \dots\}$$

Da mesma forma vista na paridade, pode ser definida duas operações: a soma e a multiplicação, veja a tabela:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Exemplo 3.22. Qual é o resto da divisão por 3 do seguinte número,

$$(401 + 503)^{209} + (101 - 30)^{45}?$$

Resolução: Calculando as bases das potências: $401 + 503 = 904$ e $101 - 30 = 71$, simplificando a expressão:

$$(904)^{209} + (71)^{45}.$$

Como $904 = 3 \cdot 301 + 1$ e $71 = 3 \cdot 23 + 2$, podemos substituir 904 por $\bar{1}$ e 71 por $\bar{2}$, assim:

$$(\bar{1})^{209} + (\bar{2})^{45}. \tag{3.3}$$

Para solucionar as potências, basta fazer algumas observações:

- Potências de um número com resto 1 na divisão por 3, deixa resto sempre 1, pois:

$$\bar{1}^n = \underbrace{\bar{1} \times \bar{1} \times \cdots \times \bar{1}}_{n \text{ vezes}} = \bar{1}$$

- Quanto as potências de $\bar{2}$ na classe residual módulo 3. Observe as primeiras potências de $\bar{2}$:

$$\begin{aligned}\bar{2}^2 &= \bar{2} \times \bar{2} = \bar{1} \\ \bar{2}^3 &= \bar{1} \times \bar{2} = \bar{2} \\ \bar{2}^4 &= \bar{2} \times \bar{2} = \bar{1} \\ \bar{2}^5 &= \bar{1} \times \bar{2} = \bar{2} \\ \bar{2}^6 &= \bar{2} \times \bar{2} = \bar{1}\end{aligned}$$

Deste modo, quando o expoente da potência for par, então o resultado será $\bar{1}$, se o expoente for ímpar, o resultado será $\bar{2}$.

Fazendo as substituições devidas em (3.3), tem-se:

$$\bar{1} + \bar{2}.$$

Portanto o resto da divisão por 3 é 0.



4 *ENSINANDO EQUAÇÕES DIOFANTINAS LINEARES*

Inicialmente esse capítulo apresenta uma discussão de quando se poderia ser ensinada as equações diofantinas lineares no Ensino Básico, como também uma justificativa da importância de ser ensinada. Após isto, são mostrados alguns aspectos históricos de Diofanto e de sua importância na Matemática, pois ele é considerado o pai da Aritmética. Também é mostrado como Diofanto resolvia os problemas do livro *Arithmetica*, métodos estes muito práticos e interessantes para serem aplicados no ensino. O capítulo termina com a exposição das equações diofantinas lineares, juntamente com um boa quantidade de exemplos para melhor compreensão.

4.1 **Em que momento se pode ensinar as equações diofantinas**

Tanto no Ensino Fundamental quanto no Ensino Médio é claramente possível introduzir como um tópico para o ensino, as equações diofantinas, pois no Ensino Fundamental após ter visto máximo divisor comum e equações polinomiais do primeiro grau com uma incógnita, os alunos têm requisito para compreender o processo de solução das equações diofantinas. Quanto ao Ensino Médio, um bom momento seria no segundo ano ou em algum momento que esteja sendo trabalhado sistemas de equações lineares.

Como afirma Capilheira :

A resolução de equações diofantinas lineares utiliza basicamente conceitos previstos para o Ensino Fundamental, como o de divisor, máximo divisor comum, divisão euclidiana e equação da reta, o que torna plausível a questão de estudo. Revisitaremos esses conteúdos com mais precisão (de um ponto de vista mais formal), reformulando-os, apresentando mais propriedades e mostrando outras alternativas de abordagem e cálculo, que nos levam a entender e determinar as soluções destas equações. (CAPILHEIRA, 2012, p.15)

Pensando um pouco sobre a inserção das equações diofantinas no Ensino Fundamental, geralmente o ensino de equações polinomiais do primeiro grau, passa pela seguinte sequência: primeiro a solução de equações lineares de apenas uma incógnita, depois para iniciar a solução de sistemas lineares de duas equações com duas incógnitas, passa por uma breve explicação sobre algumas soluções de equações lineares de duas incógnitas, ou seja, a forma $ax + by = c$, com a , b e $c \in \mathbb{R}$. Neste último caso é possível fazer considerações necessárias sobre essas equações, nesse caso, propor o método de solução quando os coeficientes são inteiros, ou seja, introduzir as equações diofantinas lineares.

Não entraremos no mérito da questão sobre a inclusão das Equações Diofantinas Lineares como componente curricular para o Ensino Fundamental nem Ensino Médio, mas expô-lo como um tema acessível ao Ensino Básico e, portanto, podendo ser um complemento para exploração das diversas possibilidades de estratégias de resolução de situações-problema, propiciando assim o desenvolvimento de competências.

Segundo Pommer:

O uso das Equações Diofantinas Lineares no ensino básico possibilita re-explorar situações-problema envolvendo números inteiros. No ensino médio, a concepção vigente é tratar os inteiros simplesmente como subconjuntos dos números reais, o que conduz a simplificações que não consideram aspectos fundamentais dos números inteiros. (POMMER , 2011, p.2)

Também em Pommer, justifica o porquê de ensinar equações diofantinas no Ensino Básico: “Este tema permite articular, a partir da tentativa e erro, outras estratégias de enfoque aritmético” (POMMER , 2011, p.2). Desta forma esta evolui para a escrita algébrica, e portanto “estabelecendo uma natural transição entre a Aritmética e a Álgebra” (POMMER , 2011, p.2).

4.2 Um pouco da história de Diofanto e dos problemas diofantinos

Como esta estrito em Eves [11], Diofanto de Alexandria teve uma enorme importância na construção da Álgebra. Entretanto não se conhece muito sobre sua vida, nem mesmo sobre a época exata em que viveu, mas supõe que é contemporâneo de Herão, em torno do século III da era cristã. Sua carreira floresceu em Alexandria, o que é o único fato certo sobre sua vida.

Quanto a sua contribuição à Matemática, segundo Boyer:

A principal obra de Diofante que é a *Arithmetica*, tratado que era originalmente em treze livros, dos quais só os seis primeiros se preservaram. Deve-se lembrar que na Grécia antiga a palavra Aritmética significava teoria dos números(BOYER , 1974, p.130)

Quanto às características desta obra:“A *Arithmetica* não é uma exposição sistemática sobre as operações algébricas ou as funções algébricas ou a resolução de equações algébricas.” (BOYER , 1974, p.133). O que ela é de fato uma coletânea de 150 problemas, estes todos estudados a partir de exemplos específicos, e mesmo assim, nem se faz um esforço para achar todas as soluções possíveis. Nas soluções das equações do segundo grau, apenas se considerava as soluções positivas. “Não é feita uma distinção clara entre problemas determinados e indeterminados, e mesmo para os últimos, para os quais o número de soluções em geral é infinito, uma só resposta é dada.(BOYER , 1974, p.133)

Diofante desenvolveu diversas abreviações para seus problemas e soluções, sendo assim os rudimentos da Álgebra, abreviações para incógnitas, potências das incógnitas, subtrações e igualdade. Veja:

- σ \longrightarrow Última letra da palavra *arithmos*, a incógnita.
- Δ^Y \longrightarrow primeira letra da palavra *dynamis*, o quadrado da incógnita.
- K^Y \longrightarrow primeira letra da palavra *kybos*, o cubo.
- $\Delta^Y \Delta$ \longrightarrow a quarta potência.
- ΔK^Y \longrightarrow a quinta potência.
- $K^Y K$ \longrightarrow a sexta potência.
- $\overset{O}{M}$ \longrightarrow abreviatura da palavra grega *monades* que significa unidade e representa uma constante.

Veja agora alguns problemas do livro *Arithmetica* que mostra o método diofantino de resolução.

O exemplo abaixo é o problema 27 do Livro I de *Arithmetica* visto em Pitombeira [22].

Exemplo 4.1. *Encontrar dois números cuja soma e produto sejam números dados.*

Resolução: Os números dados para a soma e para o produto são; 20 e 96 respectivamente.

Em Pitombeira [22] mostra a seguinte solução como esta no livro *Arithmetica*: deseja-se encontrar dois números, ou seja, 2 *arithmoi*. Começando a dividir a soma destes dois números, que é 20, por 2, portanto 10. A partir daí considera-se um *arithmos* somado por 10 mais a subtração de *arithmos* por 10, neste caso, $10 - \sigma + 10 - \sigma = 20$, como o produto é 96, então multiplica essas duas quantidades, obtendo 100 subtraída pelo quadrado de um *arithmos*, ou seja, um *dynamis* (Δ^Y), em uma linguagem algébrica, $100 - \Delta^y = 96$, concluindo que *dynamis* vale 4, e portanto um *arithmos* é igual a 2, tendo como resultado 12 e 8, são as respostas desejadas. ■

Buscando maior clareza sobre o método diofantino, a mesma questão será resolvida, mas agora com uma linguagem algébrica conhecida.

Resolução: O enunciado dado reduz ao seguinte sistema:

$$\begin{cases} x + y = 20 \\ xy = 96 \end{cases}$$

Como sua soma é 20, toma $\frac{20}{2} = 10$, atribui uma outra variável k , tais que:

$$\begin{aligned} x &= 10 + k \\ y &= 10 - k. \end{aligned}$$

Multiplicando ambos:

$$\begin{aligned} (10 + k)(10 - k) &= 96 \\ 100 - k^2 &= 96 \\ k^2 &= 100 - 96 \\ k &= 2. \end{aligned}$$

E portanto:

$$\begin{aligned} x &= 12 \\ y &= 8. \end{aligned}$$



Observe que esse problema é semelhante aos problemas vistos quando se é dado sistema de equações que se reduz a equações polinomiais do 2º grau, pois este problema se resume à solução da equação $x^2 - 20x + 96 = 0$, daí usa-se a fórmula:

$$x = \frac{-b \pm \sqrt{\Delta}}{2a}$$

com $\Delta = b^2 - 4ac$, onde a , b e c são os coeficientes da equação $ax^2 + bx + c = 0$, nesse caso o método diofantino para solução desses problemas além de se mostrar uma forma alternativa de solução, propicia uma solução mais Aritmética, o que muitas vezes é bem vista pelos alunos.

Os próximos problemas serão resolvidos apenas usando a linguagem algébrica moderna.

Exemplo 4.2. *Achar dois números tais que sua soma seja 10 e a soma de seus cubos seja 370.*

Resolução: Dado o sistema:

$$\begin{cases} x + y = 10 \\ x^3 + y^3 = 370 \end{cases}$$

Como sua soma é 10, toma $\frac{10}{2} = 5$, atribui uma outra variável k , tais que:

$$\begin{aligned} x &= 5 + k \\ y &= 5 - k. \end{aligned}$$

Substituindo na soma de cubos:

$$\begin{aligned} (5 + k)^3 + (5 - k)^3 &= 370 \\ 125 + 75k + 15k^2 + k^3 + 125 - 75k + 15k^2 - k^3 &= 370 \\ 30k^2 + 250 &= 370 \\ k^2 &= 4 \\ k &= 2. \end{aligned}$$

E portanto:

$$\begin{aligned}x &= 7 \\y &= 3.\end{aligned}$$

■

O último exemplo é muito semelhante ao anterior, porém sendo uma subtração de números, ou seja, $x - y = s$; nesse caso, toma $x = k - \frac{s}{2}$ e $y = k + \frac{s}{2}$.

Exemplo 4.3. *Ache dois números tais que sua diferença e a diferença de seus cubos são iguais a dois números dados.*

Resolução: Tomando estes números como 6 e 936, respectivamente, temos a seguinte sistema em linguagem atual:

$$\begin{cases}x - y = 6 \\x^3 - y^3 = 936\end{cases}$$

Como sua diferença é 6, toma $\frac{6}{2} = 3$, atribui uma outra variável k , tais que:

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

Substituindo na soma de cubos:

$$\begin{aligned}(k + 3)^3 - (k - 3)^3 &= 936 \\k^3 + 9k^2 + 27k + 27 - k^3 + 9k^2 - 27k + 27 &= 936 \\-18k^2 - 54 &= 936 \\k^2 &= 49 \\k &= 7.\end{aligned}$$

E portanto:

$$\begin{aligned}x &= 10 \\y &= 6.\end{aligned}$$



Segue agora uma lista de alguns problemas de Diofanto vista no livro *Arithmetica*:

Problema 6, Livro III: Encontre três números¹ tais que a soma de todos é um quadrado e a soma de dois quaisquer deles também é um quadrado. (Resposta de Diofanto: 80, 320, 41.)

Problema 7, Livro III: Encontre três números em progressão Aritmética, sabendo-se que a soma de dois quaisquer deles é um quadrado. (Resposta de Diofanto: $120\frac{1}{2}$, $840\frac{1}{2}$, $1560\frac{1}{2}$.)

Problema 13, Livro III: Encontre três números tais que o produto de dois quaisquer deles, acrescido do terceiro, é um quadrado.

Problema 15, Livro III: Encontre três números tais que o produto de dois quaisquer deles, acrescido da soma dos mesmos dois, é um quadrado.

Problema 10, Livro IV: Encontre dois números tais que sua soma é igual à soma de seus cubos. (Resposta de Diofanto: $\frac{5}{7}$, $\frac{8}{7}$.)

Problema 21, Livro IV: Encontre três números em progressão geométrica de maneira que a diferença entre dois quaisquer deles é um número quadrado. (Resposta de Diofanto: $\frac{81}{7}$, $\frac{144}{7}$ e $\frac{256}{7}$.) (EVES, 2004, p.208)

4.3 Equações Diofantinas Lineares

Nesta seção será estudada as *equações diofantinas lineares*, de modo específico as que possuem duas incógnitas, ou seja:

$$ax + by = c \quad (4.1)$$

onde a , b são números naturais não simultaneamente iguais a zero. Uma solução para a equação (4.1) é um par ordenado $(x_0, y_0) \in \mathbb{N} \times \mathbb{N}$ de forma que a seguinte igualdade seja verdadeira:

$$ax_0 + by_0 = c.$$

Antes que seja possível mostrar um método para obter alguma solução de uma equação diofantina é preciso analisar determinadas condições para saber quando uma equação admite solução, segundo Domingues [9].

Proposição 4.1. *Uma equação diofantina linear, $ax + by = c$, com $a \neq 0$ ou $b \neq 0$, admite solução se, e somente se, $\text{mdc}(a, b) \mid c$.*

¹Deve-se ter em mente que “número” significa “número racional positivo”

Demonstração: Provando cada parte:

(\implies) Se $(x_0, y_0) \in \mathbb{Z}^2$ é uma solução qualquer, vale a igualdade:

$$ax_0 + by_0 = c.$$

Pela definição de mdc , $mdc(a, b) \mid a$ e $mdc(a, b) \mid b$ usando a proposição 2.4 na página 20 vale a tese, $mdc(a, b) \mid c$.

(\impliedby) Chamando $d = mdc(a, b)$ usando a proposição 3.1 na página 39 garante que $d = ax_0 + by_0$ para algum par $(x_0, y_0) \in \mathbb{Z}^2$, com a hipótese que $d \mid c$ e deste modo $c = d \cdot t$, $t \in \mathbb{Z}$, e portanto:

$$c = d \cdot t = (ax_0 + by_0)t = a(x_0t) + b(y_0t).$$

Ou seja o par (x_0t, y_0t) é uma solução da equação desejada. ■

A proposição acima além de mostrar uma condição para verificar que existe solução, ela também é generosa, pois na demonstração encontramos um método para determinar uma solução. Veja o exemplo:

Exemplo 4.4. *Encontre uma solução, se existir, da equação $12x + 32y = 52$.*

Resolução: Usando a proposição acima 4.1, basta calcular o $mdc(12, 32)$:

$$32 = 12 \cdot 2 + 8 \tag{4.2}$$

$$12 = 8 \cdot 1 + 4 \tag{4.3}$$

$$8 = 4 \cdot 2 + 0.$$

Portanto $mdc(12, 32) = 4$ e $4 \mid 52$, logo existe, uma admite solução para a equação diofantina $12x + 32y = 52$.

Para encontrar uma solução basta usar os cálculos obtidos para a determinação do $mdc(12, 32)$. Da equação (4.3) vale a igualdade $4 = 12 + 8(-1)$ substituindo 8 pela expressão $32 + 12(-2)$ de (4.2), segue:

$$4 = 12 + (32 + 12(-2))(-1)$$

$$4 = 12(3) + 32(-1).$$

E como $52 = 4 \cdot 12$, multiplicando a igualdade acima por 12:

$$4 \cdot 12 = 52 = 12(3 \cdot 12) + 32(-1 \cdot 12)$$

e portanto

$$12(36) + 32(-12) = 52.$$

Logo $(36, -12)$ é uma solução de $12x + 32y = 52$



A proposição abaixo é vista em Domingues [9]

Proposição 4.2. *Se (x_0, y_0) é uma solução qualquer da equação diofantina linear $ax + by = c$, com $a \neq 0$ e $b \neq 0$, então esta equação admite infinitas soluções e o conjunto dessas soluções é:*

$$S = \left\{ \left(x_0 + \frac{b}{\text{mdc}(a,b)}t, y_0 - \frac{a}{\text{mdc}(a,b)}t \right); t \in \mathbb{Z} \right\}.$$

Demonstração: Chamando de $\text{mdc}(a,b) = d$ e indicando por (x^*, y^*) as soluções de $ax + by = c$, vale a igualdade:

$$ax^* + by^* = c = ax_0 + by_0$$

e daí

$$a(x^* - x_0) = b(y_0 - y^*).$$

Como $a = d \cdot f$ e $b = d \cdot g$ com f e $g \in \mathbb{Z}$ onde $\text{mdc}(f, g) = 1$, e então:

$$f(x^* - x_0) = g(y_0 - y^*).$$

Portanto $f \mid (y_0 - y^*)$ e desse modo $y_0 - y^* = ft$, $t \in \mathbb{Z}$, o que leva

$$y^* = y_0 - ft = y_0 - \frac{a}{d}t.$$

E daí

$$f(x^* - x_0) = g(y_0 - y^*) = fgt$$

e obtém-se

$$x^* = x_0 + gt = x_0 + \frac{b}{d}t$$

e por fim

$$\left(x_0 + \frac{b}{\text{mdc}(a,b)}t, y_0 - \frac{a}{\text{mdc}(a,b)}t\right).$$

é a solução da equação dada.

■

O corolário abaixo também está presente em Domingues [9].

Corolário 4.1. *Se a e b são diferentes de zero e $\text{mdc}(a,b) = 1$ e (x_0, y_0) é uma solução particular da **equação diofantina linear** $ax + by = c$, então o conjunto de todas as soluções é dado por:*

$$S = \{(x_0 + bt, y_0 - at); t \in \mathbb{Z}\}.$$

Exemplo 4.5. *Tendo que comprar selos de 5 reais e 7 reais. De quantas maneiras pode-se comprar os selos sabendo que devem ser gastos exatamente 100 reais?*

Resolução: A solução é encontrar os valores dos pares ordenados $(x, y) \in \mathbb{Z}^2$ como $x \geq 0$ e $y \geq 0$ que é solução da equação $5x + 7y = 100$, fazendo as contas:

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1.$$

Assim $\text{mdc}(5,7) = 1$ e $1 \mid 100$, logo a equação tem solução inteira, calculando, substituindo

2 por $7 + 5(-1)$ da expressão $5 + 2(-2) = 1$, tem-se:

$$1 = 5 + (7 + 5(-1))(-2)$$

$$1 = 5 + 7(-2) + 5(2)$$

$$1 = 5(3) + 7(-2).$$

Multiplicando por 100,

$$1 = 5(300) + 7(-200)$$

e portanto a solução é

$$S = \{(300 + 7t, -200 - 5t); t \in \mathbb{Z}\}.$$

Bem essa não é a resposta desejada ainda, basta agora ver quais os valores de t para os quais os x e y sejam ambos positivos, basta resolver as inequações, $-200 - 5t \geq 0$ e $300 + 7t \geq 0$, por fim, $-42 \geq t \geq -40$, seja a tabela com os resultados possíveis:

t	x	y	(x, y)
-40	20	0	(20, 0)
-41	13	5	(13, 5)
-42	6	10	(6, 10)

Portanto as soluções são 20 selos de 5 reais e nenhum selo de 7 reais, 13 selos de 5 reais e 5 selos de 7 reais e a última possível solução 6 selos de 5 reais e 10 selos de 7 reais. ■

Exemplo 4.6. *Responda:*

- (a) *Determine todos os múltiplos positivos de 7 e 13 cuja soma é igual a 90.*
 (b) *Determine todos os múltiplos positivos de 3 e 5 cuja soma é igual a 68.*

Resolução:

- (a) Basta resolver a seguinte equação, $7x + 13y = 90$, e obter os resultados de x e y positivos:

$$\begin{aligned} 13 &= 7 \cdot 1 + 6 \longrightarrow 13 + 7(-1) = 6 \\ 7 &= 6 \cdot 1 + 1 \longrightarrow 7 + 6(-1) = 1. \end{aligned}$$

Fazendo as substituições adequadas:

$$\begin{aligned} 1 &= 7 + (13 + 7(-1))(-1) \\ 1 &= 7 + 13(-1) + 7(1) \\ 1 &= 7(2) + 13(-1). \end{aligned}$$

Multiplicando por 90,

$$7(180) + 13(-90) = 90.$$

Assim uma solução para a equação é $(180, -90)$, mas para obter um par de solução mais adequado ao problema proposto pode ser posto a divisão euclidiana de -90 por 7 , $-90 = 7(-13) + 1$ e substituindo na expressão acima:

$$\begin{aligned} 7(180) + 13(7(-13) + 1) &= 90 \\ 7(180) + 7(-169) + 13(1) &= 90 \\ 7(11) + 13(1) &= 90. \end{aligned}$$

Assim as soluções da equação são postas no conjunto:

$$S = \{(11 + 13t, 1 - 7t); t \in \mathbb{Z}\}.$$

Observe que $x_0 = 11$ e $y_0 = 1$ são os únicos valores positivos para a solução da equação, portanto os múltiplos de 7 e 13 cuja soma é 90 são 77 e 13 respectivamente.

(b) Para solucionar a questão basta resolver a equação $3x + 5y = 68$, ou seja:

$$S = \{(21 + 5t, 1 - 3t); t \in \mathbb{Z}\}.$$

Os valores de $t \in \mathbb{Z}$ tais que os valores de x e y são positivos são os números do intervalo $-4 \leq t \leq 0$, veja a tabela com a soma dos múltiplos de 3 e 5 :

t	x	y	(x, y)	$3x + 5y = 68$
0	21	1	(21, 1)	$63 + 5 = 68$
-1	16	4	(16, 4)	$48 + 20 = 68$
-2	11	7	(11, 7)	$33 + 35 = 68$
-3	6	10	(6, 10)	$18 + 50 = 68$
-4	1	13	(1, 13)	$3 + 65 = 68$

■

Exemplo 4.7. *Um problema visto em Hefez:*

Numa criação de coelhos e galinhas, contaram-se 400 pés. quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível? (HEFEZ, 2011, p.73)

Resolução: Como um coelho tem 4 pés e uma galinha 2 pés basta resolver a equação diofantina

$$2x + 4y = 400. \quad (4.4)$$

com x representando os valores possíveis para as galinhas e y os valores possíveis para os coelhos e então buscar as soluções com valores apenas positivos, como a equação (4.4) é equivalente a equação $x + 2y = 200$, como vale a seguinte igualdade:

$$1(-1) + 2(1) = 1.$$

Multiplicando esta por 200,

$$1(-200) + 2(200) = 200.$$

Fazendo a divisão euclidiana de -200 por 2, ou seja, $-200 = 2 \cdot (-100) + 0$, substituindo pela igualdade acima:

$$\begin{aligned} 1(2 \cdot (-100) + 0) + 2(200) &= 200 \\ 2(-100) + 1(0) + 2(200) &= 200 \\ 1(0) + 2(100) &= 200. \end{aligned}$$

Portanto $x_0 = 0$ e $y_0 = 100$ são soluções para a quantidade de galinhas e coelhos, como solução geral tem-se:

$$S = \begin{cases} x = 0 + 2t \\ y = 100 - t \end{cases} \text{ com } t \in \mathbb{Z}.$$

Para encontrar o valor desejado, ou seja o valor de x e y que sua diferença seja a menor possível e positivo, basta resolver a equação $0 + 2t = 100 - t$ nos racionais \mathbb{Q} e aproximar para o menor inteiro mais próximo, nesse caso $t = \frac{100}{3}$ e portanto tomando $t = 33$, então os valores de $x = 66$ e $y = 67$

■

Exemplo 4.8. *Encontrar todos os números naturais \mathbb{N} menores do que 10.000 tais que:*

- *O resto da divisão de N por 37 é 9;*

- *O resto da divisão de N por 52 é 15.*

Resolução: Aqui está sendo pedido um número que satisfaz na divisão euclidiana:

$$N = 37 \cdot x + 9 \quad (4.5)$$

$$N = 52 \cdot y + 15. \quad (4.6)$$

Igualando (4.5) com (4.6), tem-se a seguinte equação diofantina linear:

$$37x - 52y = 6. \quad (4.7)$$

Como $\text{mdc}(37, -52) = 1$ logo a equação (4.7) tem solução, fazendo as contas necessárias:

$$52 = 37 \cdot 1 + 15 \quad \longrightarrow \quad 52 + 37(-1) = 15$$

$$37 = 15 \cdot 2 + 7 \quad \longrightarrow \quad 37 + 15(-2) = 7$$

$$15 = 7 \cdot 2 + 1 \quad \longrightarrow \quad 15 + 7(-2) = 1.$$

Substituindo o 7 por $37 + 15(-2)$ da igualdade $15 + 7(-2) = 1$:

$$15 + (37 + 15(-2))(-2) = 1$$

$$37(-2) + 15(5) = 1.$$

Substituindo o 15 por $52 + 37(-1)$ da igualdade $37(-2) + 15(5) = 1$:

$$37(-2) + (52 + 37(-1))(5) = 1$$

$$37(-7) + 52(5) = 1.$$

Multiplicando por 6 e fazendo a troca de sinal convenientemente:

$$37(-42) - 52(-30) = 6.$$

Já sabe-se que -42 e -30 são soluções da equação, mas deixando soluções positivas, basta dividir -42 por 52 e -30 por 37, e fazer as substituições:

$$-42 = 52 \cdot (-1) + 10$$

$$-30 = 37 \cdot (-1) + 7.$$

E daí

$$\begin{aligned} 37(52 \cdot (-1) + 10) - 52(37 \cdot (-1) + 7) &= 6 \\ 37(10) - 52(7) &= 6. \end{aligned}$$

Portanto a solução é:

$$S = \begin{cases} x = 10 + 52t \\ y = 7 + 37t \end{cases} \text{ com } t \in \mathbb{Z}.$$

Voltando à pergunta, como $N = 37x + 9$, então $N = 379 + 1924t$, como é pedido no enunciado, basta encontrar os valores de $t \in \mathbb{Z}$ tais que $N < 10000$, que são o $t = 0, 1, 2, 3, 4$ e 5. Por fim mostrando o resultado em uma tabela:

t	N
0	379
1	2302
2	4227
3	6151
4	8075
5	9999

■

Exemplo 4.9. *Uma outra questão proposta por Hefez:*

Subindo uma escada de dois em dois degrau, sobra um degrau. Subindo a mesma escada de três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que o seu número é múltiplo de 7 e está compreendido entre 40 e 100.

Resolução: Do enunciado, “subindo uma escada de dois em dois degrau, sobra um degrau”, tem-se a expressão:

$$N = 2 \cdot x + 1 \tag{4.8}$$

onde N representa a quantidade de degraus que tem a escada e x a quantidade de passos dados quando sobe a escada de dois em dois degraus.

Do enunciado, “subindo a mesma escada de três em três degraus, sobram dois degraus”, tem-se a expressão:

$$N = 3 \cdot y + 2 \quad (4.9)$$

com y a quantidade de passos dados quando sobe a escada de três em três degraus. Igualando (4.8) com (4.9):

$$2 \cdot x - 3 \cdot y = 1 \quad (4.10)$$

como $2 \cdot 2 - 3 \cdot 1 = 1$, neste caso, a solução é:

$$S = \begin{cases} x = 2 + 3t \\ y = 1 + 2t \end{cases} \text{ com } t \in \mathbb{Z}.$$

Como queremos $40 < N < 100$ e tomando $N = 2 \cdot x + 1$, então $20 \leq x \leq 49$, desses valores de x , quando $x = 38$, temos $N = 77$.

■

Exemplo 4.10. *Uma camiseta custa, R\$ 21,00, mas comprador só tem notas de R\$ 2,00, e o caixa, só de R\$ 5,00. Nessas condições, será possível pagar a importância da compra, e de que modo?*

Resolução: Primeiramente, observe que sempre em uma compra de um produto, vale a seguinte regra:

$$\text{Valor Pago} - \text{Troco} = \text{Valor do Produto},$$

como o enunciado diz, o comprador só pode pagar com um múltiplo de 2, ou seja, $2 \cdot x$, $x \in \mathbb{N}$, enquanto o caixa só poderá retornar um valor múltiplo de 5, ou seja, $5 \cdot y$, $y \in \mathbb{N}$. Logo basta ver se a seguinte equação diofantina linear tem solução:

$$2 \cdot x - 5 \cdot y = 21. \quad (4.11)$$

Como $\text{mdc}(2, 5) = 1$, logo a equação acima possui solução, basta procurar as soluções positivas. Como $2 \cdot 13 - 5 \cdot 1 = 21$, logo, se o comprador pagar R\$ 26,00, então receberá R\$ 5,00 de troco, não apenas essa é uma solução possível, observando a solução apenas naturais: (4.11):

$$S = \begin{cases} x = 13 + 5t \\ y = 1 + 2t \end{cases} \text{ com } t \in \mathbb{N},$$

vale construir uma tabela com as primeiras soluções:

t	0	1	2	3
Valor Pago	26	36	46	56
Troco	5	15	25	35

■

Exemplo 4.11. *Em Pommer [24]:*

Uma loja de conveniência trabalha com diversas marcas de café. Num determinado mês, um comprador desta loja adquiriu 2 tipos de café: tipo A (normal) e tipo B (descafeinado). Sabendo-se que ele gastou exatamente R\$ 58,00, quais são as diversas maneiras que ele pode adquirir os pacotes do tipo A e do tipo B? O preço do pacote da marca A é R\$ 2,00 e do pacote da marca B, R\$ 3,00 (POMMER, 2008, p.61).

Resolução: Encontrando todas as soluções positivas da seguinte equação:

$$2 \cdot A + 3 \cdot B = 58 \quad (4.12)$$

onde A denota quantidade comprada do café tipo A e B denota a quantidade comprada do café tipo B. Como $\text{mdc}(2, 3) = 1$ e $1 \mid 58$, logo a equação (4.12) têm solução. Tomando a igualdade:

$$2 \cdot (-1) + 3 \cdot 1 = 1$$

e multiplicando por 58,

$$2 \cdot (-58) + 3 \cdot 58 = 58. \quad (4.13)$$

Fazendo a divisão euclidiana de -58 por 3, têm $-58 = 3 \cdot (-20) + 2$, substituindo em (4.13):

$$2 \cdot (3 \cdot (-20) + 2) + 3 \cdot 58 = 58$$

$$2 \cdot 2 + 3 \cdot (-40) + 3 \cdot 58 = 58$$

$$2 \cdot 2 + 3 \cdot (18) = 58$$

Assim as soluções para os inteiros são:

$$S = \begin{cases} A = 2 + 3t \\ B = 18 - 2t \end{cases} \text{ com } t \in \mathbb{Z}.$$

Para os valores adequados de t , encontramos os seguintes resultados:

t	0	1	2	3	4	5	6	7	8
A	2	5	8	11	14	17	20	23	26
B	18	16	14	12	10	8	6	4	2



5 *SEQUÊNCIA DIDÁTICA PARA A CONGRUÊNCIA MÓDULO N*

A seguinte sequência didática tem o objetivo de orientar para o ensino de congruência módulo n para os alunos do 7º ano do Ensino Fundamental. Neste momento é esperado que os alunos tenham conhecimento dos números inteiros.

Entretanto alguns conceitos devem ser melhor vistos, conceitos como a divisão euclidiana, assim como o significado desta divisão, ou seja, o significado do quociente e resto.

Devemos lembrar que existe uma distinção entre o conhecimento científico, conhecimento esse que exige um rigor ao ser elaborado e transmitido enquanto saber científico, e esse mesmo conhecimento ao ser transposto ao ensino. Daí define-se o que pode ser dito de uma transposição didática, um conhecimento acadêmico ser posto como conhecimento escolar.

Fica claro que conhecimento acadêmico e conhecimento escolar tem suas características próprias e se distinguem pelas diversidades presente em cada contexto.

Portanto, não se está tratando aqui a Matemática com demonstrações e minúcias que o rigor exige, mas sim definições mais leves com atividades que permitam o amadurecimento de conceitos e técnicas de cálculo.

A sequência é formada de atividades que no geral foram pensadas para ser aplicada em um tempo médio de duas a três horas de aula.

Atividade 5.1. *Divisao euclidiana (1ª Parte).*

Objetivo: Conhecer a História de Euclides e sua importância na Matemática. Também descobrir intuitivamente a divisão euclidiana.

Descrição Geral: Apresentar a história de Euclides, expondo a forma como em sua época era tratado o conceito de número, assim como mostrar a importância histórica de Euclides, devida ao seu livro, Os Elementos.

Após isso propor através de matérias como: palitos, corda com nós devidamente espaçados, desenvolver atividades que promova o conceito da divisão euclidiana.

Uma ideia para esta atividade é que divida-se em grupos os alunos e então em cada grupo de uma quantidade definida de palitos, por exemplo 50 palitos, então o professor pede que agrupe estes palitos em uma outra quantidade definida, por exemplo 7, deseja-se que faça agrupamentos com os palitos com 7 cada, então pergunta quantos grupos foram feitos e quantos palitos sobraram. No exemplo dado a resposta certa encontrada é 7 grupos de sete palitos e apenas um palito ficou por fora, da mesma forma pode pensar nesta atividade com uma corda com nós igualmente espaçados.

Observe que o que esta sendo feito aqui é apenas a divisão euclidiana usando materiais e não números.

Atividade 5.2. *Divisão Euclidiana (2ª Parte).*

Objetivo: Apresentar o enunciado da divisão euclidiana e sua interpretação na reta.

Descrição Geral: Expor o enunciado da divisão euclidiana, fazer diversos exemplos e apresentar sua interpretação na reta, e por fim fazer exercícios para encontrar o resto e o quociente de uma divisão, saber quantos múltiplos de um número tem em um intervalo. Veja algum desses exercícios.

Problemas Propostos para a Atividade

1. Encontre o resto e o quociente na divisão de:

(a) 30 por 4.

(b) -58 por 7.

(c) 60 por 12.

(d) -81 por 15.

2. Em cada item construa uma reta numerada e represente com ela a divisão de:

(a) 54 por 13.

(b) -30 por 4.

(c) 58 por 8.

(d) -46 por 5.

Observação: As duas questões acima, espera-se que os alunos possam fixar a divisão euclidiana e exercitar uma ou mais de uma técnica para fazer a divisão: fazendo subtrações sucessivas, usando a reta numérica ou o algoritmo da chave.

3. Quantos múltiplos de 7 existe entre 1 até 234?

4. Quantos múltiplos de 5 existe entre 113 até 800?

Observação: Através da interpretação da divisão euclidiana é possível perceber o quociente representa quantidade de múltiplos do divisor que existem de 1 até o dividendo da divisão.

Atividade 5.3. *Significado do quociente.*

Objetivo: Conhecer os diversos significados que o quociente pode ter na resolução de problemas.

Descrição Geral: Apresentar uma diversidade de problema que vise buscar os significados do quociente de uma divisão. São alguns exemplos desses problemas:

Problemas Propostos para a Atividade

1. Deseja-se repartir 30 bolinhas de gude em 6 sacos. Quantas bolinhas ficaram em cada saco?

2. Em uma empresa existem 5 sócios, o lucro da empresa é repartido igualmente. Em um mês a empresa teve um lucro de R\$ 8.500,00. Assim quanto cada um dos sócios vai receber?
3. Um construtora esta fazendo uma rodovia que terá no final da obra 180 *km*, o prazo para a construção é de 45 dias, para que se cumpra o prazo quantos quilômetros por dia essa empresa deve fazer?
4. Deseja-se repartir 30 bolinhas de gude em sacos, no qual cada saco fique com 10 bolinhas. Quantos sacos vão ser usados.
5. Um padaria recebeu uma encomenda para fazer 1000 salgados, essa padaria tem a capacidade de fazer 200 saldados por dia, em quantos dias serão feitos todos os salgados?

Observação: Os problemas acima tentam mostrar aplicações simples da divisão euclidiana, especificamente tentar mostrar os significados distintos do resto de uma divisão, *partição* e *quotização*. Fica claro também que estes problemas não são inéditos, pois os alunos de 7º já vivenciaram estes problemas em anos anteriores.

Atividade 5.4. *Significado do resto.*

Objetivo: Conhecer os diversos significados que o resto pode ter na resolução de problemas.

Descrição Geral: Apresentar uma diversidade de problema que envolvam situações cíclicas e pedidos de sobra de uma partição, para assim buscar os significados do resto de uma divisão, principalmente questões da OBMEP.

Problemas Propostos para a Atividade

1. Em 11720 dias há quantos meses? Quantos dias *sobram*?
2. Dona Benta distribuiu igualmente 38 brigadeiros entre 12 alunos. Quantos brigadeiros recebeu cada um? Sobraram brigadeiros?

Observação: Os problemas acima tratam da ideia do resto de uma divisão como apenas sobra do dividendo, abaixo será tratado questões mais elaboradas, estas são necessário uma interpretação sobre o resto uma nova forma de dividir um conjunto de elementos.

3. Contando a partir de um domingo, em que dia da semana cai o milésimo dia?
4. Uma empresa de coleta de lixo dividiu um município em 150 áreas para realizar a coleta de lixo nas casas.

Abaixo segue um cronograma para a coleta:

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	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

Observação: Entenda que a tabela acima ela esta dividindo os números da área de coleta de lixo, com os dias da semana em uma relação com o resto, bastando dividir a número da área por 7 e então toma o resto, resto 1 é domingo, resto 2 em uma segunda, e assim por diante, Pergunta-se:

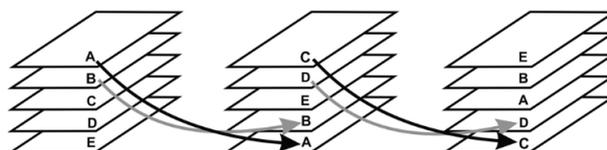
- (a) Em que dia da semana a área 45 deve esperar o caminhão de lixo? E a área 60 e a área 100?
- (b) Quantas áreas diferentes essa empresa de coleta de lixo visita na terça-feira? E no sábado?
- (c) É possível estabelecer uma relação entre a distribuição das áreas e cada dia da semana? Qual?

Observação: As questões abaixo, todas extraídas da OBMEP, são boas questões para a nossa proposta de ensino, pois acredito que estas podem promover um amadurecimento do conceito da divisão.

5. [OBMEP (2012), 1ª Fase, Nível 2] Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas. Em cada embaralhamento, a primeira carta passa a ser a segunda, a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira. Qual será a primeira carta após 2012 embaralhamentos?



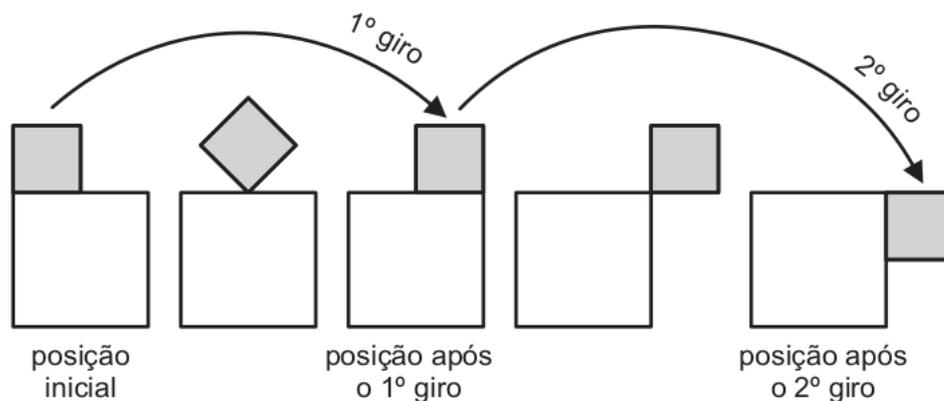
6. [OBMEP (2012), Banco de Questões] Estefânia tem cinco cartas marcadas com as letras A, B, C, D e E, empilhadas nessa ordem de cima para baixo. Ela embaralha as cartas pegando as duas de cima e colocando-as, com a ordem trocada, embaixo da pilha. A figura mostra o que acontece nas duas primeiras vezes em que ela embaralha as cartas.



Se Estefânia embaralhar as cartas 74 vezes, qual carta estará no topo da pilha?

- A) *A* B) *B* C) *C* D) *D* E) *E*

7. [OBMEP (2012), 1ª Fase, Nível 1] Um quadrado de lado 1 cm roda em torno de um quadrado de lado 2 cm, como na figura, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado maior.



Qual das figuras a seguir representa a posição dos dois quadrados após o 2012º giro?

- A) B) C) D) E)

Dificuldades Previstas: Quanto as questões onde se busca a sobra de uma partição é possível não encontrar nem uma dificuldade, entretanto nas que envolve situações

cíclicas, é muito comum nestas questões, onde se deseja saber o comportamento de algo em um posição “muito longe” os alunos acharem que deve fazer os processos definido pelo enunciado do problema até o ponto pedido. Isso é uma prova que os alunos não tem o significado do resto. Portanto deve-se ai ter calma e garantir que o aluno adquira o significado do resto.

Atividade 5.5. *Definição e notação de congruência.*

Objetivo: Conhecer a definir congruência módulo n . Saber usar corretamente a notação de congruência.

Descrição Geral: Expor a definição formal de congruência módulo n , explorar detalhadamente através de diversos exemplos numéricos. Aplicar exercícios que explorem a definição e a notação de congruência.

Problemas Propostos para a Atividade

1. Conhecendo a definição de congruência:

Dado $n \neq 0$ natural, dois outros inteiros a e b são **congruentes módulo n** quando o resto da divisão euclidiana de a por n é igual ao resto da divisão euclidiana de b por n . denota-se $a \equiv b \pmod{n}$.

Faça alguns exemplos de congruência.

Observação: Espera-se que os alunos possam com essa questão fixar a definição de congruência, assim como desenvolver a capacidade de leitura de uma definição matemática, pois para os alunos uma definição cheia de termos genéricos é uma barreira para o entendimento do mesmo. Entretanto ser capaz de entender uma definição matemática é um passo para o gosto e entendimento matemático.

2. Determine se cada item abaixo é verdadeiro ou falso. Em caso negativo, corrija a congruência usando o simbolo de não-côngruo, que é $\not\equiv$.

(a) $20 \equiv 5 \pmod{3}$.

(b) $14 \equiv 6 \pmod{8}$.

- (c) $19 \equiv 13 \pmod{5}$.
 (d) $49 \equiv 19 \pmod{10}$.
 (e) $15 \equiv 2 \pmod{13}$.
 (f) $76 \equiv 7 \pmod{10}$.
 (g) $35 \equiv 0 \pmod{6}$.

Observação: Nessas questões os alunos são instigados a verificar a uma congruência, o que reforça a definição de congruência, assim como a próxima questão que estimula fazer associação com um par de divisões e uma congruência.

3. Em uma coluna existem duas divisões euclidianas e na outra coluna um congruência. Relacione as colunas:

- | | |
|--|--------------------------------|
| • $73 = 3 \cdot 24 + 1$ e $52 = 3 \cdot 17 + 1$. | • $34 \equiv 22 \pmod{4}$. |
| • $-43 = 5 \cdot (-9) + 2$ e $-88 = 5 \cdot (-18) + 2$. | • $14 \not\equiv 4 \pmod{3}$. |
| • $28 = 2 \cdot 14 + 0$ e $3 = 2 \cdot 1 + 1$. | • $73 \equiv 52 \pmod{3}$. |
| • $14 = 3 \cdot 4 + 2$ e $4 = 3 \cdot 1 + 1$. | • $-43 \equiv -88 \pmod{5}$. |
| • $-21 = 4 \cdot (-6) + 3$ e $-25 = 4 \cdot (-7) + 3$. | • $28 \not\equiv 3 \pmod{2}$. |
| • $34 = 4 \cdot 8 + 2$ e $22 = 4 \cdot 5 + 2$. | • $-21 \equiv -25 \pmod{4}$. |

Atividade 5.6. *Propriedades de congruência.*

Objetivo: Conhecer e aplicar adequadamente algumas propriedades de congruência, entre elas, as que define congruência como uma relação de equivalência.

Descrição Geral: Expor a propriedade seguinte:

Dados a e $b \in \mathbb{Z}$ com $a \equiv b \pmod{n}$ se, e só se, $n \mid b - a$.

Sem o rigor de demonstrá-la, mas sim de expor com grande riqueza em exemplos. Da mesma forma apresentar as seguintes propriedades que definem a congruência como uma relação de equivalência:

Seja $n \in \mathbb{Z}$ com $n > 1$. Para todos a, b e $c \in \mathbb{Z}$ vale:

1. $a \equiv a \pmod{n}$. (**reflexiva**)
2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$. (**simétrica**)
3. $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$. (**transitiva**)

Após isso aplicar os seguintes exercícios:

Problemas Propostos para a Atividade

1. Verifique se as congruências são verdadeiras usando o fato que $a \equiv b \pmod{n} \Leftrightarrow n \mid b - a$.

Veja o exemplo:

exemplo: $15 \equiv 3 \pmod{4}$.

Resposta: Como $3 - 15 = -12$ e $4 \mid -12$ logo é verdadeira a congruência.

- (a) $21 \equiv 14 \pmod{7}$
- (b) $13 \equiv 53 \pmod{10}$
- (c) $89 \equiv -1 \pmod{5}$
- (d) $56 \equiv -3 \pmod{4}$
- (e) $27 \equiv 34 \pmod{6}$

Observação: Fica claro que esta questão trata de uma nova forma de verificar uma congruência, agora usando uma proposição vinda a partir da definição.

Da mesma forma a questão abaixo verifica-se a proposição com alguns exemplos, assim fixa melhor o conceito que estamos trabalhando.

2. Complete as frases abaixo conforme o exemplo:

exemplo: 73 e 52 na divisão euclidiana por 3, temos: $73 = 3 \cdot 24 + 1$ e também $52 = 3 \cdot 17 + 1$ então $73 - 52 = 3 \cdot (24 - 17) + 1 - 1 = 21$, como 21 é um múltiplo de 3, ou seja, $3 \mid 21$, logo vale a congruência $52 \equiv 73 \pmod{3}$.

- (a) 65 e 33 na divisão euclidiana por 4, temos: _____ e também _____ então _____, como _____ é um múltiplo de 4, ou seja, _____, logo vale a congruência _____.
- (b) 30 e 16 na divisão euclidiana por 14, temos: _____ e também _____ então _____, como _____ é um múltiplo de 14, ou seja, _____, logo vale a congruência _____.
- (c) 46 e 21 na divisão euclidiana por 5, temos: _____ e também _____ então _____, como _____ é um múltiplo de 5, ou seja, _____, logo vale a congruência _____.

3. Complete as frases abaixo conforme o exemplo e tente entender o que esta sendo feito:

exemplo: Tomando a congruência $24 \equiv 46 \pmod{11}$, como sabemos é verdadeira, pois $11 \mid 46 - 24$, por que $46 - 24 = 22 = 11 \cdot 2$, desta mesma forma $24 - 46 = -22$ que também é múltiplo de 11, logo $46 \equiv 24 \pmod{11}$.

- (a) Tomando a congruência $12 \equiv 21 \pmod{9}$, como sabemos é verdadeira, pois _____, por que _____, desta mesma forma _____ que também é múltiplo de 11, logo _____.
- (b) Tomando a congruência $-4 \equiv 16 \pmod{10}$, como sabemos é verdadeira, pois _____, por que _____, desta mesma forma _____ que também é múltiplo de 11, logo _____.
- (c) Tomando a congruência $-9 \equiv -27 \pmod{6}$, como sabemos é verdadeira, pois _____, por que _____, desta mesma forma _____ que também é múltiplo de 11, logo _____.

Qual propriedade você acabou de usar nos itens acima?

4. Usando a propriedade transitiva, que diz: Para todos a, b e $c \in \mathbb{Z}$, se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$. Conclua as frases.

- (a) se $12 \equiv 27 \pmod{5}$ e $27 \equiv 57 \pmod{5}$, então _____.
- (b) se $78 \equiv 29 \pmod{7}$ e $29 \equiv 50 \pmod{7}$, então _____.
- (c) se $44 \equiv 27 \pmod{12}$ e $27 \equiv 57 \pmod{12}$, então _____.

Atividade 5.7. *Propriedades operacionais das congruências.*

Objetivo: Operar sobre as congruências.

Descrição Geral: Apresentar as propriedades, sem o rigor de demonstrá-las, mas com grande riqueza em exemplos. As propriedades são:

Dados a, b, c e $n \in \mathbb{Z}$, com $n > 1$. Se $a \equiv b \pmod{n}$, então:

1. $a \pm c \equiv b \pm c \pmod{n}$.
2. $a \cdot c \equiv b \cdot c \pmod{n}$.

Dados a, b, c, d e $n \in \mathbb{Z}$, com $n > 1$. Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então:

1. $a \pm c \equiv b \pm d \pmod{n}$.
2. $a \cdot c \equiv b \cdot d \pmod{n}$.

Dados a, b e $e \in \mathbb{Z}$, com $e \geq 1$. Se $a \equiv b \pmod{n}$, então $a^e \equiv b^e \pmod{n}$.

E por fim aplicar exercícios que explorem tais propriedades.

Problemas Propostos para a Atividade

1. Em cada congruência abaixo, some e multiplique cada membro por um número de sua escolha. Verifique que a congruência permaneceu válida.

exemplo: $15 \equiv 3 \pmod{4}$.

Resposta: Tomando o número 6, a congruência $15 + 6 \equiv 3 + 6 \pmod{4}$, resolvendo, $21 \equiv 9 \pmod{4}$ é uma congruência válida, assim como, $15 \cdot 6 \equiv 3 \cdot 6 \pmod{4}$, multiplicando, $90 \equiv 18 \pmod{4}$ também é uma congruência válida.

- (a) $29 \equiv 35 \pmod{2}$.
- (b) $10 \equiv 35 \pmod{5}$.
- (c) $17 \equiv 3 \pmod{7}$.
- (d) $10 \equiv 19 \pmod{9}$.
- (e) $14 \equiv 40 \pmod{13}$.
- (f) $50 \equiv 65 \pmod{15}$.

Observação: Tem nessa questão acima uma forma de “brincar ” com as congruências acima, o objetivo desta questão e que o aluno perceba que a soma e o produto de um número em cada membro da congruência são operações que não alterem a veracidade de uma congruência.

2. Mostre que

- (a) $10^{200} - 1$ é divisível por 11.
- (b) $9^{100} - 1$ é divisível por 10.
- (c) $21^{1000} - 1$ é divisível por 20.
- (d) $2^{20} - 1$ é divisível por 41.

Observação: A questão acima, é de fato, a questão mais instigante, pois agora com as propriedades operacionais das congruências. Veja a seguinte solução do primeiro item:

Resolução:

Sabendo que $10^2 \equiv 1 \pmod{11}$, pois $11 \mid 100 - 1$. Usando a potenciação em cada membro da congruência, elevando a 100 cada membro:

$$10^{200} \equiv 1^{100} \pmod{11},$$

o que mostra claramente que $11 \mid 10^{200} - 1$.

■

3. Ache o resto da divisão

- (a) de 7^{10} por 51.

- (b) de 5^{21} por 127.
- (c) de 2^{100} por 11.
- (d) de 14^{256} por 17.
- (e) de 12^{480} por 5.

Observação: Como a questão anterior, essa também deseja muita atenção e dedicação para que os alunos sejam capazes que realizarem sua solução. Veja a solução do primeiro item:

Resolução:

Para que possamos encontrar o resto da divisão de 7^{10} por 51 é preciso pensar em alguma potência de 7 mais próxima de 51, ou seja, $7^2 = 49$, como 7^2 é congruente a -2 módulo 51, $7^2 \equiv -2 \pmod{51}$, elevando cada membro por 5, temos: $7^{10} \equiv -32 \pmod{51}$, e como $-32 \equiv 19 \pmod{51}$, portanto o resto da divisão desejada é 19.



Atividade 5.8. *Paridade e sistema de restos módulo 3.*

Objetivo: Estudar a paridade de um número. Resolver problemas sobre paridade e do sistema de restos módulo 3.

Descrição Geral: Apresentação sobre a paridade de um número bem como uma análise de resultados sobre a soma e produto de números pares e ímpares. Da mesma forma apresentar o sistema de restos módulo 3 e a tabela de soma e produto. Terminado assim com uma lista de exercícios.

Problemas Propostos para a Atividade

1. Determine a paridade do seguinte número:

$$(123275 + 346231)^{234} + (3451 + 4532)^{542}.$$

2. Usando a tabuada da classes residuais módulo 3, mostre que não existe quadrado que deixa resto 2 pela divisão por 3.

Observação: Essa questão tenta fazer que o aluno manipule a tabela operacional.

3. (OBMEP-2008-Banco, modificado) Na aula sobre divisão a professora pediu que seus alunos colocassem números no lugar das estrelas. Quais são estes números:

$$\begin{array}{r} \star \quad | \quad 3 \\ (\star) \quad 7 \end{array}$$

DICAS:

- Lembre-se que $\star = 3 \times 7 + (\star)$.
- Os possíveis restos de uma divisão por 3 são: 0, 1 e 2.

4. (3^a OBM-Banco) Mostre que n é ímpar, então $n^2 - 1$ é divisível por 8.

DICAS:

- Todo número inteiro n é da forma $2k$, se for par, ou $2k + 1$ se ímpar.
- Quando existem dois números consecutivos, um deles é par.

5. Um sistema de restos módulo 4 é o seguinte conjunto:

$$\bar{0} = \{0, 4, 8, \dots, 4k, \dots\}$$

$$\bar{1} = \{1, 5, 9, \dots, 4k + 1, \dots\}$$

$$\bar{2} = \{2, 6, 10, \dots, 4k + 2, \dots\}$$

$$\bar{3} = \{3, 7, 11, \dots, 4k + 3, \dots\}$$

Complete a tabela da soma e subtração abaixo.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$				
$\bar{3}$				

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$				
$\bar{3}$				

6. (5^a OBM-Banco, modificado) Demostre que o quadrado de um inteiro é da forma $8n$ ou $8n + 1$ ou $8n + 4$.

DICAS:

- Todo número inteiro n é igual à uma das seguintes formas $8k$, $8k + 1$, $8k + 2$, $8k + 3$, $8k + 4$, $8k + 5$, $8k + 6$ ou $8k + 7$ em que $k \in \mathbb{Z}$.
- Comece a questão fazendo um tabela com inteiros e seus respectivos quadrados.
- Use o produto notável $(a + b)^2 = a^2 + 2ab + b^2$ e quando possível simplifique.

6 SEQUÊNCIA DIDÁTICA PARA AS EQUAÇÕES DIOFANTINAS

A seguinte sequência didática trata de ensinar equações diofantinas lineares para ser aplicado no Ensino Médio. Tal sequência didática é uma proposta de ensino adaptada do trabalho dissertativo de Bianca Herreira Capilheira [5], não esquecendo que nesta sequência está também lista de exercícios e propostas minhas.

Quanto a dissertação de Capilheira [5], com o título “EQUAÇÕES DIOFANTINAS LINEARES: UMA PROPOSTA PARA O ENSINO MÉDIO”, foi uma:

pesquisa qualitativa com o apoio da Engenharia Didática, uma vez que esta oportuniza avaliar a produção dos alunos a partir do confronto de análises de produções dos alunos em questão e da proposta do professor.

Escolhemos desenvolver o trabalho no primeiro ano do ensino médio, por entender que os alunos, nesse período, já possuem o amadurecimento matemático, bem como os pré-requisitos necessários para o desenvolvimento da nossa proposta e, também, porque é um dos níveis de ensino em que a mestranda atua. (CAPILHEIRA, 2012, p.15)

Quanto à Engenharia Didática: “tem inspiração no trabalho do engenheiro, cuja produção exige sólido conhecimento científico, básico e essencial, mas também exige enfrentamento de problemas práticos para os quais não existe teoria prévia — momentos em que é preciso construir soluções” (CARNEIRO apud CAPILHEIRA, 2012, p.17). ” e também “a teoria da Engenharia Didática pode ser vista como referencial para o desenvolvimento de produtos para o ensino, gerados na junção do conhecimento prático com o conhecimento teórico.” (CARNEIRO apud CAPILHEIRA, 2012, p.17).

A experiência de ensino criada pela autora de dissertação é a iniciação do assunto usando o jogo “Escova Diofantina” como um recurso didático, neste aspecto, Silva e Kodama apud Capilheira diz que:

os jogos matemáticos podem dar efetivas contribuições ao processo de ensino-aprendizagem da matemática, auxiliando o trabalho do professor, que têm em suas mãos um recurso didático que lhe permite o trabalho com diversos conteúdos, de acordo com a sua necessidade, podendo tornar o seu planejamento mais dinâmico e atrativo, além de contribuir para a aprendizagem dos alunos, que se sentem mais motivados a aprender matemática e podem construir seus conhecimentos de uma forma mais interativa e prazerosa, encontrando nas aulas de matemática a oportunidade de adquirir saberes, desenvolver habilidades de resolução de problemas, de cooperação e trabalho em equipe. (CAPILHEIRA, 2012, p.98)

Atividade 6.1. *O jogo “Escova Diofantina”.*

Objetivo: Introduzir de forma lúdica os conceitos das equações diofantinas com o jogo escova diofantina.

Descrição Geral: Começar as atividades de ensino é o estudo alguns tipos de equações. Apresentar o jogo Escova Diofantina, que têm regras parecidas como jogo escova, veja as regras do jogo, regras escritas tal qual em Capilheira [5]:

REGRAS DO JOGO:

Material necessário

- 1 baralho comum.

Retire do baralho as Figuras (rei, dama e valete) dos quatro naipes e também os coringas. Agora estas com um baralho de 40 cartas composto por quatro sequências de Ás a 10.

Descrição

Embaralhe as cartas e distribua 3 para cada jogador. Abra as próximas 4 cartas e coloque-as no centro da mesa desviradas. O monte restante é posto de lado.

O primeiro a jogar deve procurar uma carta em sua mão que somada a uma das cartas da mesa dê um total de 15. (**ATENÇÃO:** poderão ser utilizados no máximo 2 números diferentes)

O jogador coloca à sua frente as cartas pegadas da mesa, assim como a carta de sua mão que permitiu a soma de 15, com a face voltada para baixo. Caso ele não consiga

pegar nenhuma carta da mesa, deve simplesmente descartar na mesa uma das cartas de sua mão. Se o jogador conseguir pegar todas as cartas restantes na mesa de uma única vez o jogador fez uma *escova diofantina*. Ao colocar na sua frente as cartas pegas, ele deverá colocar uma delas com a face voltada para cima e perpendicular ao monte de cartas voltadas para baixo. Será o sinal de que ele fez uma *escova diofantina*. Para cada *escova diofantina* feita, o mesmo procedimento deverá ser repetido.

Quando os jogadores tiverem utilizado suas 3 cartas, uma nova mão de 3 cartas é distribuída, utilizando o monte que havia sido posto de lado. A partida prossegue da mesma maneira até que o monte de cartas termine. Aí é feita a contabilização dos pontos.

Contabilização dos pontos:

Cada escova diofantina vale 1 ponto.

Os pontos conquistados por cada jogador (ou equipe) são anotados em uma Folha, as cartas são embaralhadas e uma nova mão tem início, ao término da qual os pontos são novamente somados. Vence a partida quem atingir 5 pontos.

Enquanto os alunos jogam, pedir para que eles registrem as jogadas realizadas no jogo com a seguinte tabela:

Quadro 6: Registro das jogadas

1ª carta	Quantidade da 1ª carta	2ª carta	Quantidade da 2ª carta	Soma 15

Fonte: CAPILHEIRA

Nesta tabela espera-se que os alunos façam as combinações com duas cartas de tipos diferentes, com quantidades de carta de mesmo tipo que pode variar de zero até quatro.

Veja alguns exemplos de possíveis combinações que os alunos podem registrar:

Quadro 7: Registro das jogadas

1ª carta	Quantidade da 1ª carta	2ª carta	Quantidade da 2ª carta	Soma 15
5	3	4	0	15
7	1	8	1	15
3	4	1	3	15
4	2	7	1	15
10	1	5	1	15
9	1	3	2	15

Fonte: AUTOR 2013

Atividade 6.2. *Combinação linear.*

Objetivo: Através do registro das jogadas definir e expor algumas combinações lineares vista no jogo.

Descrição Geral: “Após aplicar o jogo “escova diofantina”, separar as apresentações por grupo/cartas da última coluna da tabela de registros do jogo. A partir das apresentações dos alunos dos registros das possibilidades de jogadas, construir a definição de combinação linear, partindo das escritas das jogadas apresentadas e registradas na Folha de registro das jogadas”(CAPILHEIRA, 2012, p.37). Veja Alguns exemplos:

Se tirar 1 carta de número 9 e 2 cartas de número 3, obtemos 15.

$$9 \times 1 + 3 \times 2 = 15$$

Se tirar 1 carta de número 8 e 1 cartas de número 7, obtemos 15.

$$8 \times 1 + 7 \times 1 = 15$$

Assim dizemos que 15 é combinação linear 9 e 3, também é combinação linear de 8 e 7.

Atividade 6.3. *Equação Diofantina Lineares*

Objetivo: “Definir equação diofantina, através da generalização da escrita das equações que modelam o jogo Escova Diofantina”(CAPILHEIRA , 2012, p.36)

Descrição Geral: Fazer a definição geral de uma equação diofantina linear de duas incógnitas, $ax + by = c$, onde a , b e c são números inteiros e x e y são as incógnitas.

Em seguida escrever a equação que modela o jogo com um baralho, por exemplo, se tomar a carta 1, (ás), são estas as seguintes possibilidades, usando x como quantidade das cartas “ás” e “y” como a quantidade das outras cartas, construímos a tabela abaixo, onde as equações em vermelho não têm soluções no jogo e as verdes têm soluções no jogo.

$1x + 2y = 15$	$1x + 3y = 15$	$1x + 4y = 15$	$1x + 5y = 15$	$1x + 6y = 15$
$1x + 7y = 15$	$1x + 8y = 15$	$1x + 9y = 15$	$1x + 10y = 15$	

Desta forma apresentar a seguinte atividade proposta por Capilheiro [5].

Problemas Propostos para a Atividade

1. Observe as possibilidades de soma, conforme o quadro visto em aula. Agora pense nas possibilidades que resultam em soma igual a 15 para uma o jogo escova diofantina com um baralho.

Quadro 8: Tabela das possíveis equações diofantinas vistas no jogo.

$1x+2y=15$	$1x+3y=15$	$1x+4y=15$	$1x+5y=15$	$1x+6y=15$	$1x+7y=15$	$1x+8y=15$	$1x+9y=15$	$1x+10y=15$
$2x+1y=15$	$2x+3y=15$	$2x+4y=15$	$2x+5y=15$	$2x+6y=15$	$2x+7y=15$	$2x+8y=15$	$2x+9y=15$	$2x+10y=15$
$3x+1y=15$	$3x+2y=15$	$3x+4y=15$	$3x+5y=15$	$3x+6y=15$	$3x+7y=15$	$3x+8y=15$	$3x+9y=15$	$3x+10y=15$
$4x+1y=15$	$4x+2y=15$	$4x+3y=15$	$4x+5y=15$	$4x+6y=15$	$4x+7y=15$	$4x+8y=15$	$4x+9y=15$	$4x+10y=15$
$5x+1y=15$	$5x+2y=15$	$5x+3y=15$	$5x+4y=15$	$5x+6y=15$	$5x+7y=15$	$5x+8y=15$	$5x+9y=15$	$5x+10y=15$
$6x+1y=15$	$6x+2y=15$	$6x+3y=15$	$6x+4y=15$	$6x+5y=15$	$6x+7y=15$	$6x+8y=15$	$6x+9y=15$	$6x+10y=15$
$7x+1y=15$	$7x+2y=15$	$7x+3y=15$	$7x+4y=15$	$7x+5y=15$	$7x+6y=15$	$7x+8y=15$	$7x+9y=15$	$7x+10y=15$
$8x+1y=15$	$8x+2y=15$	$8x+3y=15$	$8x+4y=15$	$8x+5y=15$	$8x+6y=15$	$8x+7y=15$	$8x+9y=15$	$8x+10y=15$
$9x+1y=15$	$9x+2y=15$	$9x+3y=15$	$9x+4y=15$	$9x+5y=15$	$9x+6y=15$	$9x+7y=15$	$9x+8y=15$	$9x+10y=15$
$10x+1y=15$	$10x+2y=15$	$10x+3y=15$	$10x+4y=15$	$10x+5y=15$	$10x+6y=15$	$10x+7y=15$	$10x+8y=15$	$10x+9y=15$

Fonte: CAPILHEIRA

Tinte as células das tabelas do seguinte modo:

	Situação já considerada
	Há solução
	Não há solução

Esperamos que os alunos obtenhas as seguintes soluções.

Quadro 9: Tabela das possíveis equações diofantinas vistas no jogo pintada.

$1x+2y=15$	$1x+3y=15$	$1x+4y=15$	$1x+5y=15$	$1x+6y=15$	$1x+7y=15$	$1x+8y=15$	$1x+9y=15$	$1x+10y=15$
$2x+1y=15$	$2x+3y=15$	$2x+4y=15$	$2x+5y=15$	$2x+6y=15$	$2x+7y=15$	$2x+8y=15$	$2x+9y=15$	$2x+10y=15$
$3x+1y=15$	$3x+2y=15$	$3x+4y=15$	$3x+5y=15$	$3x+6y=15$	$3x+7y=15$	$3x+8y=15$	$3x+9y=15$	$3x+10y=15$
$4x+1y=15$	$4x+2y=15$	$4x+3y=15$	$4x+5y=15$	$4x+6y=15$	$4x+7y=15$	$4x+8y=15$	$4x+9y=15$	$4x+10y=15$
$5x+1y=15$	$5x+2y=15$	$5x+3y=15$	$5x+4y=15$	$5x+6y=15$	$5x+7y=15$	$5x+8y=15$	$5x+9y=15$	$5x+10y=15$
$6x+1y=15$	$6x+2y=15$	$6x+3y=15$	$6x+4y=15$	$6x+5y=15$	$6x+7y=15$	$6x+8y=15$	$6x+9y=15$	$6x+10y=15$
$7x+1y=15$	$7x+2y=15$	$7x+3y=15$	$7x+4y=15$	$7x+5y=15$	$7x+6y=15$	$7x+8y=15$	$7x+9y=15$	$7x+10y=15$
$8x+1y=15$	$8x+2y=15$	$8x+3y=15$	$8x+4y=15$	$8x+5y=15$	$8x+6y=15$	$8x+7y=15$	$8x+9y=15$	$8x+10y=15$
$9x+1y=15$	$9x+2y=15$	$9x+3y=15$	$9x+4y=15$	$9x+5y=15$	$9x+6y=15$	$9x+7y=15$	$9x+8y=15$	$9x+10y=15$
$10x+1y=15$	$10x+2y=15$	$10x+3y=15$	$10x+4y=15$	$10x+5y=15$	$10x+6y=15$	$10x+7y=15$	$10x+8y=15$	$10x+9y=15$

	Situação já considerada
	Há solução
	Não há solução

Fonte: CAPILHEIRA

Após esta atividade, será proposta uma atividade semelhante, mas agora com uma quantidade indefinida de baralhos. O que resulta nesta solução.

Quadro 10: Tabela das possíveis equações diofantinas já pintadas vistas no jogo com mais de um baralho .

$1x+2y=15$	$1x+3y=15$	$1x+4y=15$	$1x+5y=15$	$1x+6y=15$	$1x+7y=15$	$1x+8y=15$	$1x+9y=15$	$1x+10y=15$
$2x+1y=15$	$2x+3y=15$	$2x+4y=15$	$2x+5y=15$	$2x+6y=15$	$2x+7y=15$	$2x+8y=15$	$2x+9y=15$	$2x+10y=15$
$3x+1y=15$	$3x+2y=15$	$3x+4y=15$	$3x+5y=15$	$3x+6y=15$	$3x+7y=15$	$3x+8y=15$	$3x+9y=15$	$3x+10y=15$
$4x+1y=15$	$4x+2y=15$	$4x+3y=15$	$4x+5y=15$	$4x+6y=15$	$4x+7y=15$	$4x+8y=15$	$4x+9y=15$	$4x+10y=15$
$5x+1y=15$	$5x+2y=15$	$5x+3y=15$	$5x+4y=15$	$5x+6y=15$	$5x+7y=15$	$5x+8y=15$	$5x+9y=15$	$5x+10y=15$
$6x+1y=15$	$6x+2y=15$	$6x+3y=15$	$6x+4y=15$	$6x+5y=15$	$6x+7y=15$	$6x+8y=15$	$6x+9y=15$	$6x+10y=15$
$7x+1y=15$	$7x+2y=15$	$7x+3y=15$	$7x+4y=15$	$7x+5y=15$	$7x+6y=15$	$7x+8y=15$	$7x+9y=15$	$7x+10y=15$
$8x+1y=15$	$8x+2y=15$	$8x+3y=15$	$8x+4y=15$	$8x+5y=15$	$8x+6y=15$	$8x+7y=15$	$8x+9y=15$	$8x+10y=15$
$9x+1y=15$	$9x+2y=15$	$9x+3y=15$	$9x+4y=15$	$9x+5y=15$	$9x+6y=15$	$9x+7y=15$	$9x+8y=15$	$9x+10y=15$
$10x+1y=15$	$10x+2y=15$	$10x+3y=15$	$10x+4y=15$	$10x+5y=15$	$10x+6y=15$	$10x+7y=15$	$10x+8y=15$	$10x+9y=15$

Fonte: CAPILHEIRA

Atividade 6.4. *Interpretação geométrica da equação na experimentação.*

Objetivo: Representar uma equação diofantina linear, vista no jogo “escova diofantina”.

Descrição Geral: Através do software GeoGebra, mostrar representações geométricas de equações vistas no jogo, tanto as que possui soluções quantos as que não possuem solução.

Evidenciar que buscar a solução da equação $ax + by = c$ equivale a procurar pares ordenados de ambas coordenadas inteiras que sejam pontos da reta. Para a primeira e a terceira equações, que são do jogo e cuja solução já tínhamos observado que seria possível sob as condições do jogo, conseguimos infinitos pares ordenados cujas coordenadas pertencem a \mathbb{Z} , o que de fato indica que a equação diofantina possui solução para casos de infinitos baralhos.(CAPILHEIRA, 2012, P.40)

Veja a seguinte atividade proposta para os alunos e em seguida a análise das soluções.

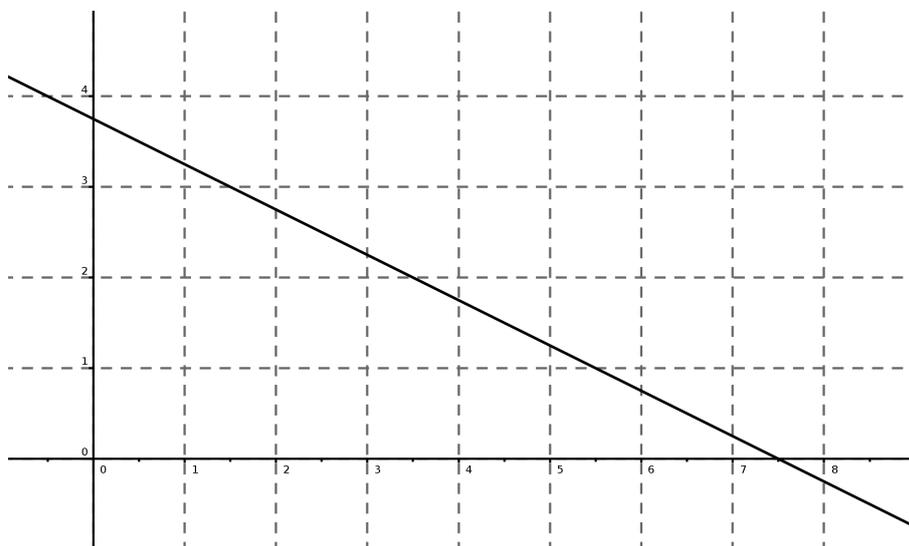
Problemas Propostos para a Atividade

1. Como representarias no plano cartesiano a equação $2x + 4y = 15$?
2. Como representarias no plano cartesiano a equação $x + 3y = 15$?

Resolução:

1. Construindo o gráfico da função $2x + 4y = 15$ através do software GeoGebra:

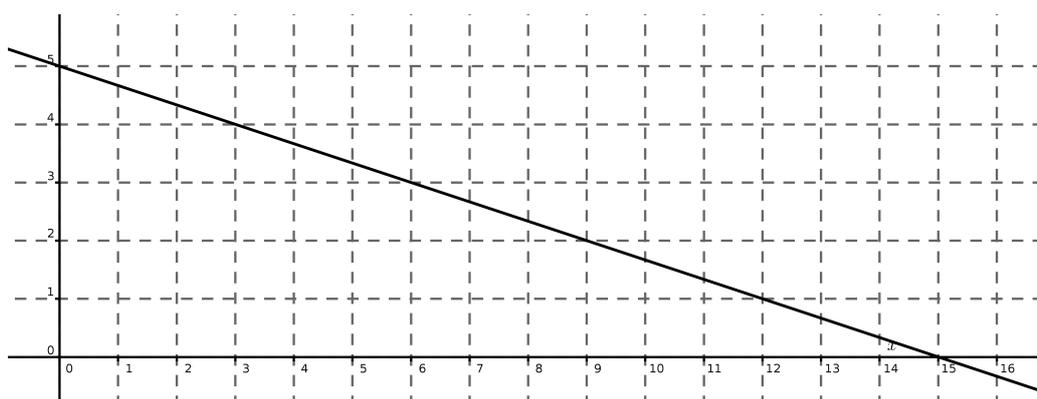
Quadro 11: Gráfico da função $2x + 4y = 15$.



Fonte: AUTOR 2013

Observe que em nenhum momento a reta da equação não toca em nenhum momento da malha do sistema cartesiano, isso quer dizer que não existe solução nos naturais

2. Construindo o gráfico da equação $x + 3y = 15$ através do software GeoGebra:

Quadro 12: Gráfico da função $x + 3y = 15$.

Fonte: AUTOR 2013

Os pontos sobre a malha que são tocados são exatamente soluções inteiras, são eles: $x = 0$ e $y = 5$; $x = 3$ e $y = 4$; $x = 6$ e $y = 3$; $x = 9$ e $y = 2$; $x = 12$ e $y = 1$; $x = 15$ e $y = 0$. Tais soluções tem as seguintes interpretações: em um jogo de “escola diofantina” com uma quantidade ilimitada de baralhos, x representa a quantidade de cartas “ás” e y representa a quantidade de cartas “3” e os pontos da equação onde tocam as malhas são as possíveis quantidade de cartas dos tipos respectivos.

■

Atividade 6.5. *Divisor, Divisor Comum e Máximo Divisor Comum* .

Objetivo: Revisar o que já foi visto sobre divisor de um número, divisores comuns de dois números e mdc e calcular o mdc de dois ou mais números usando a decomposição por primos. Aprofundar algumas propriedades do mdc .

Descrição Geral: Fazer uma revisão de máximo divisor comum, propondo atividades que usem a a sua definição e seu cálculo usando a decomposição com primos. Apresentar algumas propriedades tais como:

Sejam a e $b \in \mathbb{N}$, então:

1. $mdc(0, a) = a$.

2. $\text{mdc}(1, a) = 1$.
3. $\text{mdc}(a, a) = a$.
4. Se $a \mid b$, então $\text{mdc}(a, b) = a$.

E por fim apresentar exercícios.

Problemas Propostos para a Atividade

1. Considere o número 36.
 - (a) Cite um divisor de 36
 - (b) Cite todos os divisores de 36
2. Como definirias divisor de um número inteiro?
3. Considere os números 16 e 20.
 - (a) Cite todos os divisores de 16
 - (b) Cite todos os divisores de 20
 - (c) Quais os divisores comuns de 16 e 20?
 - (d) Qual o maior dos divisores comuns de 16 e 20?
 - (e) Sabes como se chama o maior dos divisores comuns de 16 e 20? Como?
4. Responda:
 - (a) Quais são os divisores de 18?
 - (b) Os números 18 e 24 possuem quatro divisores comuns. Quais são?
 - (c) Qual é o maior dos divisores comuns?
5. Escreva todos os divisores de:
 - (a) 15.
 - (b) 45.

Qual é então o maior divisor comum de 15 e 45?

Observação: As questões acima são questões que ajudam a lembrar do conceito e até mesmo reconstruir o próprio conceito de máximo divisor comum. As questões abaixo são para trabalhar algumas das propriedades do *mdc*.

6. Calcule o *mdc* sem fazer nenhum cálculo, só usando as propriedades.

- | | |
|---------------------------|---------------------------|
| (a) $mdc(0, 54)$. | (d) $mdc(0, 1.234.734)$. |
| (b) $mdc(1, 2.013)$. | (e) $mdc(1, 4.133)$. |
| (c) $mdc(4.026, 4.026)$. | (f) $mdc(22, 22)$. |

7. Observando a propriedade: se $a \mid b$, então $mdc(a, b) = a$. Complete.

- (a) Como $4 \mid 12$, pois $12 = 4 \cdot 3$ então $mdc(4, 12) = \underline{\hspace{2cm}}$.
- (b) Como $15 \mid 60$, pois $60 = 15 \cdot 4$ então $mdc(15, 60) = \underline{\hspace{2cm}}$.
- (c) Como $12 \mid 36$, pois $\underline{\hspace{2cm}}$ então $mdc(12, 36) = \underline{\hspace{2cm}}$.
- (d) Como $25 \mid 100$, pois $\underline{\hspace{2cm}}$ então $mdc(25, 100) = \underline{\hspace{2cm}}$.

8. Em cada item, encontre o *mdc* usando a decomposição por primos.

- | | |
|-----------------------|------------------------|
| (a) $mdc(14, 12)$. | (d) $mdc(450, 100)$. |
| (b) $mdc(64, 40)$. | (e) $mdc(280, 335)$. |
| (c) $mdc(300, 750)$. | (f) $mdc(1024, 640)$. |

Atividade 6.6. *Solução e o mdc dos coeficientes.*

Objetivo: “Instigar os alunos a pensarem sobre a relação entre o MDC dos coeficientes da equação e o seu resultado.”(CAPILHEIRA, 2012, p.79)

Descrição Geral: Propor a atividade que faça o aluno perceber a relação entre as soluções de uma equação diofantina linear $ax + by = c$ e o *mdc* de seus coeficientes a e b .

Problemas Propostos para a Atividade

- Escreva o MDC entre os números das cartas do jogo de soma 15 abaixo. (coloque o MDC logo abaixo da equação - na célula da tabela)

Quadro 13: As equações diofantinas e o MDC de seus coeficientes.

$1x+2y=15$	$1x+3y=15$	$1x+4y=15$	$1x+5y=15$	$1x+6y=15$	$1x+7y=15$	$1x+8y=15$	$1x+9y=15$	$1x+10y=15$
	$2x+3y=15$	$2x+4y=15$	$2x+5y=15$	$2x+6y=15$	$2x+7y=15$	$2x+8y=15$	$2x+9y=15$	$2x+10y=15$
		$3x+4y=15$	$3x+5y=15$	$3x+6y=15$	$3x+7y=15$	$3x+8y=15$	$3x+9y=15$	$3x+10y=15$
			$4x+5y=15$	$4x+6y=15$	$4x+7y=15$	$4x+8y=15$	$4x+9y=15$	$4x+10y=15$
				$5x+6y=15$	$5x+7y=15$	$5x+8y=15$	$5x+9y=15$	$5x+10y=15$

Fonte: CAPILHEIRA.

Quais são situações em que o MDC é divisor de 15?

2. Dada uma equação $ax + by = c$, de acordo com o observado na tabela e na pergunta acima, quando podes afirmar que é possível resolver a equação em \mathbb{N} ?

Observação: A partir dessa questão definir a condição geral de existência de solução inteiro de uma equação diofantina linear.

Uma **equação diofantina linear**, $ax + by = c$, com $a \neq 0$ ou $b \neq 0$, admite solução se, e somente se, $mdc(a, b) \mid c$.

Atividade 6.7. *Algoritmo de Euclides e aplicações de mdc.*

Objetivo: Conhecer o algoritmo de Euclides e sua praticidade para o cálculo do mdc .

Descrição Geral: Apresentar a propriedade seguinte:

Sejam $a, b \in \mathbb{N}$ a divisão euclidiana de b por a , $b = aq + r$, com $r < a$. Vale a igualdade:

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

Usando exemplos que mostram a pratica deste método para a obtenção do mdc . Por fim apresentar a seguinte lista de exercícios para que os alunos resolvam. Também propor um comparativo entre os dois métodos vistos em sala: o da decomposição por primos e o algoritmo de Euclides. Mostrar problemas que envolva o uso do mdc .

Problemas Propostos para a Atividade

1. Em cada item, encontre o mdc usando o algoritmo de Euclides, também use a decomposição por primos e tente ver qual é o método mais rápido.
 - (a) $mdc(14, 12)$.
 - (b) $mdc(120, 100)$.
 - (c) $mdc(1502, 672)$.
 - (d) $mdc(1234, 896)$.
 - (e) $mdc(1254, 994)$.
 - (f) $mdc(65214, 5434)$.
2. Uma empresa de logística é composta de três áreas: administrativa, operacional e vendedores. A área administrativa é composta de 30 funcionários, a operacional de 48 e a de vendedores com 36 pessoas. Ao final do ano, a empresa realiza uma integração entre as três áreas, de modo que todos os funcionários participem ativamente. As equipes devem conter o mesmo número de funcionários com o maior número possível. Determine quantos funcionários devem participar de cada equipe e o número possível de equipes.
3. Uma indústria Têxtil fabricou 180 m de tecido de algodão, 216 m de tecido "Jeans" e 288 m de poliéster. Esses tecidos devem ser embalados em peças de mesmo tamanho e comprimento. Considerando que deva haver o MAIOR aproveitamento possível dos tecidos, então, serão embaladas:
 - (a) 5 peças de tecido de algodão com 30 m cada uma.
 - (b) 5 peças de tecido de "jeans" com 42 m cada uma.
 - (c) 6 peças de tecido de "jeans" com 36 m cada uma.
 - (d) 6 peças de tecido de poliéster com 42 m cada uma.
 - (e) 7 peças de tecido de poliéster com 36 m cada uma.

As seguintes questões foram extraídas de Iezzi [[13]].

4. Tenho 84 balas de coco, 144 balas de chocolate e 60 balas de leite. Quero formar pacotes de balas, sem misturar sabores. Todos os pacotes devem ter a mesma quantidade de balas e essa quantidade deve ser a maior possível. Quantas balas devo colocar em cada pacote? Quantos pacotes devo formar?
5. Dona Estela vai cortar duas peças de tecido em pedaços iguais. Esse tamanho deve ser o maior possível. Uma das peças tem 90 metros, a outra tem 78 metros. De que tamanho dona Estela deve cortar cada pedaço? Com quantos pedaços ela vai ficar?

6. A livraria em que seu Arnaldo trabalha precisa atender a dois pedidos: um de 126 livros e outro de 270 livros. Os livros desses dois pedidos vão ser empacotados. Todos os pacotes devem ter o mesmo número de livros e o número de pacotes deve ser o menor possível. Determine quantos livros seu Arnaldo deve colocar em cada pacote e quantos pacotes ele deve fazer.
7. Um marceneiro recebeu 40 toras, com 8 metros de comprimento cada uma, e 60 toras, com 6 metros de comprimento cada uma. Ele deve cortar todas as toras em pedaços de mesmo tamanho, sendo esse tamanho o maior possível. Qual o tamanho de cada pedaço? Quantos pedaços serão obtidos?
8. No Colégio 1^o. de Maio matricularam-se:
- 280 alunos de 5^a. série;
 - 224 alunos de 6^a. série;
 - 168 alunos de 7^a. série;
 - 112 alunos de 8^a. série;

O diretor notou que todas as classes do colégio poderiam ter o mesmo número de alunos. O número considerado ideal por ele seria não menos de 20 e não mais de 40 alunos.

- (a) Quantos alunos o diretor colocou em cada classe?
- (b) Quantas classes de cada série foram formadas?

Atividade 6.8. *Um pouco sobre a história de Diofanto e dos problemas diofantinos.*

Objetivo: Apresentar a história de Diofanto e o seu método de solução de alguns problemas.

Descrição Geral: Nessa atividade será feita uma exposição breve da história de Diofanto, bem como da sua importância para o surgimento da Álgebra. E por fim fazer expor o método que Diofanto resolvia problemas do tipo: conhecendo a soma e o produto de dois números encontrar o tais número ou problemas conhecer a soma ou diferença de dois números e a soma dos quadrados ou cubos destes mesmos números, encontrar tais números, resumindo, métodos para solução de sistemas de equações não-lineares. Por fim, apresentar uma lista de exercício no qual é possível usar o método diofantino.

Problemas Propostos para a Atividade

1. Encontrar dois números cuja soma e produto sejam: 20 e 96, respectivamente.
2. Achar dois números tais que sua soma seja 10 e a soma de seus cubos seja 370.
3. Ache dois números tais que sua diferença e a diferença de seus cubos são iguais a 6 e 936, respectivamente.
4. Resolva os seguintes sistemas usando o método diofantino.

(a)

$$\begin{cases} x+y = 10 \\ xy = 24 \end{cases}$$

(b)

$$\begin{cases} x+y = 10 \\ xy = -40 \end{cases}$$

(c)

$$\begin{cases} x+y = 6 \\ x^2-y^2 = 72 \end{cases}$$

(d)

$$\begin{cases} x+y = 14 \\ x^2+y^2 = 106 \end{cases}$$

Atividade 6.9. *Teorema de Bachet-Bêzout.*

Objetivo: Desenvolver a capacidade de usar divisões sucessivas e o retroceder alguns desses resultado das divisões para obter a relação $a \cdot x_0 + b \cdot y_0 = d$, em que $d = mdca, b$ e x_0 e y_0 são inteiros quaisquer.

Descrição Geral: Enunciar o teorema de Bachet-Boout, claro que não faz parte desta proposta didática apresentar a demonstração com todo o rigor exigido pela Matemática, mas sim apresentar expondo exemplos numéricos. Também a possibilidade de usando o algoritmo de Euclides, fazendo substituição e substituição de restos deixados pela divisões euclidianas sucessivas encontrar os valores x_0 e y_0 .

Lembrar que cada escrita feita para calcular o MDC é uma combinação linear. Assim, escrever o MDC como combinação linear dos números envolvidos. Associar a escrita do MDC como combinação linear a uma equação diofantina linear e indicar uma solução. Quando aparecer esta associação, em uma equação obtida no jogo, comparar a solução encontrada anteriormente com a de agora para começar a pensar sobre as outras soluções de uma equação. (CAPILHEIRA, 2012, p.48)

Por fim apresentar o seguinte exercício.

Problemas Propostos para a Atividade

1. Usando o processo de divisões sucessivas encontre dois números, x_0 e y_0 para que o $mdc(a, b) = a \cdot x_0 + b \cdot y_0$ em cada item abaixo.

(a) $mdc(12, 45)$.

(b) $mdc(25, 80)$.

(c) $mdc(124, 64)$.

(d) $mdc(36, 120)$.

Atividade 6.10. *Equações diofantinas lineares.*

Objetivo: Apresentar o método de solução das equações diofantinas lineares.

Descrição Geral: Após a exposição da equação diofantina linear. Por fim fazer um lista de exercício que corroborem com o entendimento da atividade proposta e fixar o método de solução.

Problemas Propostos para a Atividade

1. Verifique se cada equação diofantina linear abaixo existe solução.

(a) $4x + 5y = 17$.

(d) $44x - 32y = 64$.

(b) $6x + 3y = 20$.

(e) $-42x + 24y = 19$.

(c) $7x - 21y = 18$.

(f) $13x + 7y = 14$.

2. Resolva as seguintes equações diofantinas lineares, se tiver solução.

(a) $4x + 5y = 17$.

(d) $44x - 32y = 64$.

(b) $6x + 3y = 20$.

(e) $-42x + 24y = 19$.

(c) $7x - 21y = 18$.

(f) $13x + 7y = 14$.

3. Resolva algumas equações vistas no jogo “escova diofantina”.

4. Tendo que comprar selos de 5 reais e 7 reais. De quantas maneiras pode-se comprar os selos sabendo que devem ser gastos exatamente 100 reais?

5. Responda:

- (a) Determine todos os múltiplos positivos de 7 e 13 cuja soma é igual a 90.
- (b) Determine todos os múltiplos positivos de 3 e 5 cuja soma é igual a 68.
6. Numa criação de coelhos e galinhas, contaram-se 400 pés. quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?
7. Subindo uma escada de dois em dois degrau, sobra um degrau. Subindo a mesma escada de três degraus, sobram dois degraus. Determine quantos degraus possui a escada, sabendo que o seu número é múltiplo de 7 e está compreendido entre 40 e 100.
8. Pedro, fã de música, tem uma quantia de R\$ 96,00 para a compra de CDs ou DVDs. Um CD custa R\$ 8,00 e um DVD R\$ 16,00. Quais são as várias possibilidades de aquisição destes dois bens, gastando-se exatamente R\$ 96,00?
9. Uma camiseta custa, R\$ 21,00 , mas comprador só tem notas de R\$ 2,00, e o caixa, só de R\$ 5,00. Nessas condições, será possível pagar a importância da compra, e de que modo?
10. Multiplicando a data do dia do meu nascimento, por 12, e o número que indica o mês do meu nascimento por 31, fazendo a soma dos dois produtos teve como resultado 612. Qual é a data do meu nascimento
11. Decomponha o número 100 em duas parcelas positivas tais que uma é múltiplo de 7 e a outra de 11.
12. O valor da entrada de um cinema é R\$ 8,00 e da meia entrada R\$ 5,00. Qual é o menor número de pessoas que pode assistir a uma sessão de maneira que a bilheteria seja de R\$500,00?

7 CONCLUSÃO

Este trabalho assumiu como objetivo propor possíveis transposições didáticas de alguns tópicos de Aritmética para o Ensino Básico. Os temas escolhidos foram divisão euclidiana, o algoritmo de Euclides, congruência modular e equações diofantinas lineares. Para tal, repensou-se nos pré-requisitos necessário para o estudo desses tópicos, concluindo pela possibilidade de seu estudo no Ensino Básico.

Propomos uma abordagem mais abrangente sobre a divisão dos números naturais, com relação à forma tradicionalmente apresentada nos livros didáticos, observando a importância de uma melhor compreensão do significado da divisão dos naturais, especificamente o resto e o quociente. Fizemos uma breve análise de textos didáticos para ter uma noção sobre os pontos em que o ensino de Aritmética deixa de lado e então propor a inserção de requisitos necessários para o ensino de congruência modular e as equações diofantinas lineares.

Com este trabalho, podemos observar a necessidade e viabilidade de aprofundamento do significado da operação divisão e seu desenvolvimento natural para congruências. Assim, é possível olhar a expressão $a = b \cdot q + r$ não como uma mera propriedade da divisão, e sim como a própria divisão (inclusive com sua demonstração), assim como introduzir a notação de divisibilidade e conhecer algumas de suas propriedades, inclusive com demonstrações.

O algoritmo de Euclides para determinar o máximo divisor comum de dois números é na maioria das vezes um método muito mais rápido e eficiente do que o método da decomposição em números primos, e quando a divisão euclidiana é bem conceituada e fixada, pode-se apresentar o método de Euclides abertamente e utilizado de forma consciente, não apenas como uma sequência sistematizada de passos.

Uma compreensão do significado do resto de uma divisão euclidiana leva naturalmente à solução de problemas envolvendo eventos cíclicos, podendo "prever" certo comportamento futuro. Constatou-se que esse significado é pouco explorado nos livros didáticos

do Ensino Básico, embora seja muitas vezes cobrado nas Olimpíadas de Matemática, notadamente na OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas). Assim sugeriu-se que sejam expostas situações-problema para os alunos, levando a construção natural de tais significados e conseqüentemente à solução conciente dos problemas apresentados.

Este trabalho aponta ainda para a possibilidade de inserir os conceitos congruência módulo m no Ensino Básico, pois além de aprofundar o significado do resto e manipulá-lo, os alunos ganham uma ferramenta importante em aplicações de outros assuntos; por exemplo, no ensino médio, no momento em que se estuda arcos cômgruos e as potências naturais do número complexo $i = \sqrt{-1}$, promovendo assim uma conexão entre temas matemáticos.

Quanto às equações diofantinas, percebe-se que o método de solução que Diofanto resolvia alguns dos problemas visto em seu livro *Arithmetica*, pode ser usado abertamente na solução de alguns problemas, principalmente nos problemas para encontrar dois números cuja soma e o produto são dados. É importante promover o ensino das equações diofantinas lineares, pois além dos problemas concretos associados que elas permitem resolver, fazem uma ponte entre a Álgebra e a Aritmética, desse modo ajudando na formação de conceitos mais gerais.

Por fim, esta pesquisa constitui um levantamento de propostas de transposições didáticas, que ao longo do trabalho se mostraram promissoras na sua efetivação. Uma proposta para trabalhos futuros, em continuidade a este, é a realização de trabalho de campo através da chamada "Engenharia Didática", conforme colocados nas referências [1] e [5].

REFERÊNCIAS

- [1] ALMOULOU, Saddo Ag; Maria José Ferreira da Silva. *Engenharia didática: evolução e diversidade*. REVEMAT: R. Eletr. Educ. Mat., UFSC/MTM/PPGECT, Florianópolis, SC, Brasi, v. 7, n.2,2012. Disponível em <http://www.periodicos.ufsc.br/index.php/revemat/article/view/1981-1322>. 2012v7n2p22. Data de acesso: 24 de Março de 2013.
- [2] BOYER, Carl Benjamin *História da Matemática*. Tradução: Elza F. Gomide, São Paulo: Editora Edgard Blücher, 1974.
- [3] BRASIL. Secretaria de Educação Fundamental. *Parâmetros curriculares nacionais : matemática* /Secretaria de Educação Fundamental. – Brasília : MEC/SEF, 1997.
- [4] BRASIL. Secretaria de Educação Fundamental. *Parâmetros curriculares nacionais : matemática* /Secretaria de Educação Fundamental. – Brasília : MEC/SEF, 1998.
- [5] CAPILHEIRA, Bianca Herreira. *Equações Diofantinas Lineares: Uma Proposta para o Ensino Médio*. 2012. 149 f. Dissertação (Mestrado em Ensino de Matemática) - Universidade Federal do Rio Grande do Sul. Instituto de Matemática. Programa de Pós-Graduação em Ensino de Matemática. Porto Alegre, RS. 2012
- [6] D'AMBROSIO, Ubiratam *Uma História Concisa da Matemática no Brasil* . Coleção Textos universitários, 2.ed. Petrópolis,RJ: Editora Vozes, 2011.
- [7] DANTE, Luiz Roberto. *Matemática*. volume 2. São Paulo: Ática, 2004
- [8] DANTE, Luiz Roberto. *Matemática*. volume 3. São Paulo: Ática, 2004
- [9] DOMINGUES, Higino H. *Fundamentos de Aritmética*. São Paulo: Atual, 1991.
- [10] EUCLIDES. *Os Elementos*. Tradução e introdução de Ireneu Bicudo. São Paulo, SP: Editora UNESP, 2009
- [11] EVES, Howard. *Introdução à História da Matemática*. Campinas,SP: Editora Unicamp, 2004.
- [12] HEFEZ, Abramo. *Elementos de Aritmética*. 2.ed. Rio de Janeiro: SBM, 2011. Coleção textos Universitários.
- [13] IEZZI, Gelson; et al. *Matemática e Realidade:5ª série*. 4.ed. São Paulo, SP: Atual, 2000
- [14] IMENES, Luiz Márcio; Marcelo Lellis. *Matemática: Imenes & Lellis*. volume 1. São Paulo, SP: Editora Moderna, 2009
- [15] IMENES, Luiz Márcio; Marcelo Lellis. *Matemática: Imenes & Lellis*. volume 3. São Paulo, SP: Editora Moderna, 2009
- [16] LIMA, Elon Lages; et al. *A Matemática do Ensino Médio: Volume 1*. 9.ed. Rio de Janeiro: IMPA, 2006. Coleção do Professor de Matemática.

- [17] LINS, Romulo Campos; Joaquim Gimenez. *Perspectiva em Aritmética e Álgebra Para o Século XXI*. 7.ed. Campinas, SP: Editora Papirus, 1997.
- [18] LOPES, Antônio José; Joaquim Gimenez Rodriguez. *Metodologia para o Ensino da Aritmética: Competência Numérica no Cotidiano*. São Paulo, SP: Editora FTD, 2009
- [19] MARTINEZ, Fábio Brochero; et al. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 2.ed. Rio de Janeiro: IMPA, 2000. Projeto Euclides.
- [20] NETO, Antônio Caminha Muniz. *Tópicos de Matemática Elementar Volume 5: Teoria dos Números*. Rio de Janeiro: SBM, 2012. Coleção do professor de matemática.
- [21] OLIVEIRA, Krerley Irraciel Martins; Fernández, Adán Jose Corcho . *Iniciação à Matemática: um curso com problemas e soluções*. Rio de Janeiro: SBM, 2012. Coleção Olimpíadas de Matemática.
- [22] PITOMBEIRA, João Bosco; Tatiana Roque *Tópicos de História da Matemática*. Rio de Janeiro: SBM, 2012. Coleção PROFMAT.
- [23] POLIDORO, Lurdes de Fátima; Robson Stigar. *A Transposição Didática: a passagem do saber científico para o saber escolar*. Disponível em [http:// ciberteologia. paulinas.org.br/ ciberteologia /index.php/ notas/ a-transposicao- didatica-a-passagem -do-saber-cientifico- para- o- saber- escolar/](http://ciberteologia.paulinas.org.br/ciberteologia/index.php/notas/a-transposicao-didatica-a-passagem-do-saber-cientifico-para-o-saber-escolar/) Acesso em: 31 de Janeiro de 2013.
- [24] POMMER, Wagner Marcelo. *EQUAÇÕES DIOFANTINAS LINEARES: Um Desafio Motivador para Alunos do Ensino Médio*. 2008. 155f. Dissertação de Mestrado Acadêmico em Educação Matemática, PUC/SP.
- [25] POMMER, Wagner Marcelo. *Uma Engenharia Didática Tematizada nas Equações Diofantinas Lineares para Articular Conteúdos e Competências no Ensino Básico*. In: III ENCONTRO REGIONAL EM EDUCAÇÃO MATEMÁTICA: Diálogos de Educação Matemática e Outros Saberes . 3, Mossoró-RN , 2011. Disponível em: <http://stoa.usp.br/wmpommer/files/3810> Acesso em: 28 de Dezembro de 2012.
- [26] RIBEIRO, Jackson da Silva. *Projeto Radix: matemática, 6.º ano*. São Paulo, SP: Editora Scipione, 2009
- [27] RIBEIRO, Jackson da Silva. *Projeto Radix: matemática, 8.º ano*. São Paulo, SP: Editora Scipione, 2009
- [28] SANTOS, J.P.O. *Introdução à Teoria dos Números*. 2.ed. Rio de Janeiro:IMPA, 2000.