UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

DISSERTAÇÃO DE MESTRADO

Construção do pensamento matemático no ensino médio.

Edvan Horácio dos Santos

Instituto de Matemática

Maceió, Junho de 2016

PROFMAT

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
EDVAN HORÁCIO DOS SANTOS

CONSTRUÇÃO DO PENSAMENTO MATEMÁTICO NO ENSINO MÉDIO

MACEIÓ
2016

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Bibliotecária Responsável: Janaina Xisto de Barros Lima

S237c Santos, Edvan Horácio dos.
Construção do pensamento matemático no ensino médio / Edvan Horácio dos Santos. – 2016.
55 f. : il.

Orientador: José Carlos Almeida de Lima.
Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Alagoas. Instituto de Matemática. Programa de Pós Graduação de Mestrado Profissional em Matemática em Rede Nacional. Maceió, 2016.

Bibliografia: f. [54]-55.

1. Matemática – Estudo ensino. 2. Divisão Euclidiana. 3. Congruência. 4. Domínio de integridade. I. Título.

CDU: 511.12

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
EDVAN HORÁCIO DOS SANTOS

CONSTRUÇÃO DO PENSAMENTO MATEMÁTICO NO ENSINO MÉDIO

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Instituto de Matemática da Universidade Federal de Alagoas como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. José Carlos Almeida de Lima.

MACEIÓ, JUNHO DE
2016

Folha de Aprovação

EDVAN HORÁCIO DOS SANTOS

CONSTRUÇÃO DO PENSAMENTO MATEMÁTICO NO ENSINO MÉDIO

Dissertação submetida ao corpo docente do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Instituto de Matemática da Universidade Federal de Alagoas e aprovada em 21 de junho de 2016.

Banca Examinadora:

Prof. Dr José Carlos Almeida de Lima - UFAL (Presidente)

Prof. Dr. Márcio Henrique Batista da Silva - UFAL

Prof. Dr Carlos Argolo Alves - IFAL

AGRADECIMENTOS

Gostaria de agradecer a todos do Instituto de Matemática da UFAL e principalmente aqueles que fazem parte do PROFMAT. Em especial agradeço ao Prof. Dr. *José Carlos Almeida de Lima*, pois sempre foi extremamente paciente comigo, fazendo as sugestões, correções e ponderações, além de me deixar bastante à vontade na escolha do tema.

Também agradeço aos meus colegas de turma e colegas de trabalho pela compreensão que tiveram em relação a mim. Em especial agradeço à professora de Língua Inglesa do IFAL/MD Niedja Balbino do Egito.

Não podia deixar de agradecer a todos os meus alunos pelas contribuições feitas com perguntas sobre várias coisas relacionadas com a matemática e que me desafia a pensar num modo simples e correto de tratar sobre o conhecimento matemático construído culturalmente ao logo do tempo.

Agradeço a todos da minha família pela compreensão que sempre tiveram em relação às escolhas que fiz.

Finalmente, agradeço à Deus porque é sempre generoso comigo, e sem a Sua intervenção diária eu não poderia concluir esse projeto, porque sou cheio de imperfeições e sem Ele sou um sopro sem vida numa lógica racional criada por padrões humanos antagonicamentes complementares.

RESUMO

Esta dissertação tratará sobre Divisão Euclidiana, alguns itens relacionados à Congruência e Domínio de Integridade. Cada capítulo contém a atividade aplicada em sala com alunos do Ensino Médio bem como um resumo básico dos objetos matemáticos que um curso de graduação cobre e algumas sugestões de outros pontos relacionados que o professor poderá se aprofundar. Além disso, o anexo contém a atividade do capítulo 1 que foi trabalhada em sala, por ter sido mais longa enquanto os exemplos usados dos capítulos 2 e 3 foram menos extensos e, por isso, estão no próprio capítulo. É claro que uma formalização completa não cabe nesse momento e o professor poderá escolher aqueles dentre os quais pretende se aprofundar. No capítulo 1, trataremos sobre a Divisão Euclidiana. Também iremos discutir e dar uma resposta do porquê, quando estamos fazendo a divisão colocamos o zero no quociente e no exercício ER4 da primeira lista de exercícios, isso fica claro quando discutimos sobre unicidade. Já no capítulo 2, os exercícios contidos na atividade mostrarão que é um pequeno esforço para abordar Congruências. Finalmente no capitulo 3, discutimos sobre Domínios de Integridade. Chamamos atenção para outros pontos tais como a comutatividade, uma vez que as matrizes foi um dos exemplos usados e a comutatividade em geral não vale neste anel. Nosso objetivo é mostrar que mesmo no Ensino Médio podemos discutir sobre tais objetos que normalmente temos contato no curso de graduação em Matemática. É claro que procuramos exemplos simples que permitissem isso.

Palavras-chave: Divisão Euclidiana. Congruência. Domínio de Integridade.

ABSTRACT

This dissertation is about Euclidean Division, some items related to Congruence and Domain of Integrity. Each chapter contains the applied activity done at the classroom with high school students, as well as a basic summary of the mathematical objects that a graduation course may cover and some suggestions of other related points that the teacher may deepen. Besides that, there is an attachment that contains the activity of Chapter 1 which was crafted in the classroom, because it was a bit longer, while the examples used in Chapters 2 and 3 were less extensive and, because of that, are inside the chapter itself. Of course, a complete formalization is not suitable for this moment and the teacher can choose those of which s/he intends to go deeper. In Chapter 1, we will talk about the Euclidean Division and we will also discuss and give an answer as to why, when we are doing the division, we put the zero in the quotient and in the exercise called ER4, that is on the first list of exercises, this becomes clear when we will discuss the concept of uniquiness. Then in chapter 2, the exercises inside the activity will show a small effort to address Congruencies. Finally in chapter 3, we discuss Integrity domains. We draw attention to other points such as comutativity, since the matrix used is one of the examples and, in general, there is no commutativity in this ring of matrix. Our goal is to show that even in High School we can discuss such objects which usually we just have contact in undergraduate degree in mathematics. Of course we worked with simple examples that allow that to happen.

Key words: Euclidean Division. Congruence. Domain of Integrity.

Sumário

1. INTRODUÇÃO

Nos Parâmetros Curriculares Nacionais do Ensino Médio(PCNEM) é previsto que a Matemática além de seu caráter formativo instrumental, deve ser vista como ciência, com suas próprias especificidades.

> Contudo, a Matemática no Ensino Médio não possui apenas o caráter formativo ou instrumental, mas também deve ser vista como ciência, com suas características estruturais específicas(PARÂMETROS CURRICULARES NACIONAIS DO ENSINO MÉDIO,1997,p. 40).

Dentro desta perspectiva, descrevemos situações simples que permitirão ao aluno de Ensino Médio compreender sobre: o significado da existência e unicidade do quociente e resto na Divisão Euclidiana, a ideia na definição de Congruência e finalmente Domínio de Integridade.

O ponto de partida foram dúvidas e perguntas que os alunos costumam fazer para nós professores de matemática e que muitas vezes não discutimos nem damos ênfase por julgar que estão relacionados com conteúdos cujo escopo está fora da alçada para um aluno de Ensino Médio. Com base nas perguntas e dúvidas, foram produzidas listas de exercícios sobre cada um dos temas citados anteriormente. Em seguida foram trabalhadas em algumas turmas do Ensino Médio no Instituto Federal de Alagoas, Campus Marechal Deodoro (IFAL/MD) no ano letivo de 2014. Após trabalhar as listas de exercícios, foi feito um resumo sintetizando as informações obtidas na aplicação das atividades. Esses resumos estão nesta dissertação logo após as listas de exercícios.

No capítulo 1 trataremos da Divisao Euclidiana. Para isso, desenvolveremos a teoria básica necessária para demonstrar esse resultado.

Serão feitas duas demonstrações desse resultado e como consequência de uma delas iremos dar uma interpretação do porquê colocamos zero no quociente ao dividirmos a por b, com $a < b$.

A atividade aplicada para discutir sobre o tema desse capítulo está no anexo. No ER4(Exemplo Resolvido 4) dessa atividade, discutimos de forma bastante clara e simples sobre as várias possibilidades de escrever 23 na forma $6q + r$, onde q e r são inteiros, mas ao acrescentarmos a condição $0 \leqslant r < 6$ só há uma forma de escrever o 23. Isso

permite compreender a unicidade de q e r na Divisão Euclidiana de 23 por 6. Além disso, o quociente e resto na Divisão Euclidiana de 2 por 6 são 0 e 2 respectivamente. Esse exemplo permite compreender um fato que costumamos fazer desde as séries iniciais, que é colocar zero no quociente.

Já o capítulo 2 contempla a parte sobre a ideia usada para definir Congruência. Nesse capítulo, além da demonstração das propriedades básicas sobre Congruência, apresento a atividade aplicada em sala que usa a teoria da congruência de forma implícita (questões 3, 4 e 5). Essa atividade contém 5 questões que usam as funções horárias dos móveis que executam movimentos com velociadade constante, das quais as 2 primeiras usam a função horária de móveis que executam um movimento uniforme e as 3 últimas usam a função horária que determina a posição angular dos móveis com velocidade angular constante. A discussão dessas questões permite perceber que não há tanta diferença entre elas, porém, na resolução das três últimas usam-se múltiplos covenientes de 180 e 360 graus. As questões 3 e 4 evidenciam o uso do conceito de Congruência de forma implícita e nos mostra que o esforço é mínimo para formalização desse conceito no Ensino Médio.

Finalmente, no capítulo 3 discutiremos sobre conceito de Domínio de Integridade. Nele apresentaremos a definição de Domínio de Integridade, bem como as propriedades básicas que decorrem da definição. Além disso, registramos a atividade aplicada em sala para discutir esse tema.

Tanto a atividade do capítulo 1 quanto a do capitulo 2 foram aplicadas com alunos do primeiro ano do Ensino Médio porque, no IFAL/Marechal Deodoro oferecemos aulas de reforço (na forma de monitorias e estudos dirigidos) e cursos de nivelamento aos alunos da primeira série. Já a atividade do capítulo 2 foi aplicada com alunos do segundo ano porque os questionamentos realizados por alunos desta série, nos levaram a produzir uma discussão sobre Domínio de Integridade.

Também, nos capítulos 1 e 3, dispomos um material que discute sobre outros pontos que têm relação com o tema abordado, levando o professor a explorar e aguçar a curiosidade dos seus alunos, assim como sua própria curiosidade. Em particular, procurei construir exemplos simples que permitissem discutir de forma significativa e sucinta sobre cada um.

Dessa forma, espero que essa dissertação possa contribuir mostrando que mesmo no Ensino Médio é possivel discutir temas que normalmente são abordados em cursos de graduação, mas que interferem de forma decisiva sobre a matemática que é tratada no Ensino Médio.

2. DIVISÃO EUCLIDIANA

2.1. Introdução

Dados dois números inteiros a e b, com $b \neq 0$, podemos pensar na divisão do número a pelo número b. A Divisão Euclidiana nos garante a existência e unicidade de dois números inteiros q e r tais que $a = bq + r$, com $0 \leqslant r < |b|$. Sob esse olhar, desenvolveremos, neste capítulo, a teoria básica necessária para formalizar a Divisão Euclidiana.

Daremos duas demonstrações desse fato. Salientamos que uma das demonstrações será feita para o conjunto dos números naturais e em seguida estenderemos para o conjunto dos números inteiros. Como consequência dessa demonstração teremos uma justificativa bastante interessante do porquê colocamos zero no quociente, quando dividimos a por b, com $a < b$.

A seguir trataremos de alguns fatos básicos necessário ao bom desenvolvimento da teoria aqui mencionada.

2.2. Alguns resultados preliminares

Definição 2.2.1. *Um subconjunto X do conjunto dos números inteiros será dito limitado inferiormente, se existir um inteiro y tal que $y \leqslant x$ para todo $x \in X$.*

Exemplo 2.2.1. *O conjunto dos números naturais, denotado por $\mathbb{N} = \{0, 1, 2, 3...\}$ é limitado inferiormente?*

Claramente temos que $\mathbb{N} \subset \mathbb{Z}$, porque todo número natutal também é inteiro. Além disso, $-1 \in \mathbb{Z}$ e, $-1 < x$, $\forall x \in \mathbb{N}$. Portanto, $\mathbb{N}$ é limitado inferiormente.

Observe também que $0 \in \mathbb{N}$ e $0 \leqslant x$, $\forall x \in \mathbb{N}$. Logo, poderíamos ter concluído que $\mathbb{N}$ é limitado inferiormente usando um elemento do próprio conjunto.

Definição 2.2.2. *Um subconjunto X do conjunto dos números inteiros será dito limitado superiormente, se existir um inteiro y tal que $x \leqslant y$ para todo $x \in X$.*

Exemplo 2.2.2. *Dado um inteiro "a", o conjunto formado por todos os divisores inteiros de "a"é limitado superiormente, pois se x divide a, então $x \leqslant |a|$.*

De fato, se $a = 0$ é trivial pois $x = 0$. Assim, nossa discussão a seguir, será feita para o caso em que $a \neq 0$. Nesse caso, necessariamente temos $|a| \geqslant 1$. Se $x \mid a$, então existe um inteiro y tal que $xy = a$. Como $a \neq 0$, temos que tanto x quanto y são também diferentes de zero. Em particular, $y \neq 0$, donde $|y| \geqslant 1$. Logo, $|a| = |x|\,|y| \geqslant |x| \geqslant x$, provando a afirmação.

Doravante, dado um número inteiro a denotaremos por D_a ao conjunto constituído por todos os números inteiros que são divisores do número inteiro a, ou seja, $D_a = \{x \in \mathbb{Z}; x \mid a\}$.

Exemplo 2.2.3. *O conjunto dos números naturais, denotado por $\mathbb{N}$, é um exemplo de subconjunto dos números inteiros que não é limitado superiormente.*

De fato, suponhamos exista $y \in \mathbb{Z}$ tal que $x \leqslant y$, $\forall x \in \mathbb{N}$. Nesse caso, $y \in \mathbb{N}$ e consequentemente $y + 1$ também é um número natural. Assim, $y + 1 < y$ e isso constitui um absurdo. Portanto, o conjunto $\mathbb{N}$ não é limitado superiormente.

Definição 2.2.3. *Um subconjunto X do conjunto dos números inteiros será dito limitado quando for limitado superiormente e limitado inferiormente.*

Exemplo 2.2.4. *Todo subconjunto finito do conjunto dos números inteiros é limitado, e portanto, se ele for ilimitado então é infinito.*

Definição 2.2.4. *Um subconjunto X do conjunto dos números inteiros tem um menor elemento (ou elemento minimo), se existir $b \in X$ tal que para todo $x \in X$ se tenha $x \geqslant b$. Denotaremos o menor elemento de um subconjunto X, quando existir, por $minX$.*

Exemplo 2.2.5. *Todo subconjunto não vazio do conjunto dos números naturais, possui elemento mínimo. No entanto, nem todo subconjunto dos números inteiros possui elemento mínimo.*

É fácil observar que o próprio $\mathbb{Z}$ não tem elemento mínimo. A primeira parte do que afirmamos é conhecida com Princípio da Boa Ordenação e será explorado com mais detalhes posteriormente.

Definição 2.2.5. *Um subconjunto X de números inteiros tem um maior elemento(ou elemento máximo), se existir $b \in X$ tal que para todo $x \in X$ se tenha $x \leqslant b$. Denotaremos o máximo de um subconjunto X, quando existir, por $máxX$.*

Exemplo 2.2.6. *Se A e $B \subset \mathbb{Z}$ são subconjuntos limitados então $A \cap B$ também é limitado.*

De fato, se A e B são limitados existem a e b inteiros tais que $-a \leqslant x \leqslant a,\ \forall x \in A$ e $-b \leqslant y \leqslant b, \forall y \in B$. Seja M=máx $\{|a|, |b|\}$. Dessa forma, quaisquer que sejam $x \in A \cap B$ tem-se que $-a \leqslant x \leqslant a,$ e $-b \leqslant x \leqslant b$, donde concluímos que $-M \leqslant x \leqslant M$, ou seja, $A \cap B$ é limitado.

Exemplo 2.2.7. *Dado um inteiro a, consideremos o conjunto $D_a = \{x \in \mathbb{Z}; x \mid a\}$. Afirmamos que ele tem um elemento máximo e um elemento mínimo.*

Isso decorre do seguinte resultado: Se x divide "a"então $|x| \leqslant |a|$, donde $-a \leqslant x \leqslant a$. Além disso, $a, -a \in D_a$, e, portanto, $-a$ e a são repectivamente o elemento máximo e o elemento mínimo do conjunto D_a.

Exemplo 2.2.8. *Sejam a e b números inteiros não nulos. Mostremos a existência de máximo divisor comum dos números a e b.*

Para isso, consideremos $D_a = \{x \in \mathbb{Z}; x \mid a\}$ e $D_b = \{y \in \mathbb{Z}; y \mid b\}$. Denotaremos, ainda, por $D_a \cap D_b$ o conjunto formado pelos divisores comuns de a e b. Afirmamos que $D_a \cap D_b \neq \phi$. De fato, $1 \in D_a \cap D_b$, o que implica a afirmação. Além disso, $D_a \cap D_b$ é limitado por ser a intersecção de conjuntos limitados e, portanto, finito. Assim, $D_a \cap D_b$ possui um elemento máximo e um elemento mínimo por ser um subconjunto finito de números inteiros.

Proposição 2.1. *Se um subconjunto X de números inteiros tem um menor elemento então ele é único e o mesmo vale para o maior elemento.*

Demonstração:

Sejam x e y menores elementos de um subconjunto X. Sendo x um menor elemento do subconjunto X, temos, por definição que $x \leqslant y$. De forma análoga, usando o fato de y ser um menor elemento do subconjunto X concluímos que $y \leqslant x$. Dessa forma, usando a antissimetria obtemos que $x = y$ e com isso concluímos a unicidade do elemento mínimo.

■

Um resultado básico sobre os números inteiros é o Princípio da Boa Ordenação (PBO), que usaremos como um axioma e provaremos uma versão equivalente dele.

Axioma 2.1. ***Princípio da Boa Ordenação.*** *Todo subconjunto X não vazio de números inteiros limitado superiormente possui elemento máximo.*

Proposição 2.2. *Todo subconjunto X não vazio de números inteiros limitado inferiormente possui elemento mínimo.*

Demonstração:

Seja X um subconjunto não vazio de números inteiros limitado inferiormente pelo número inteiro a, ou seja, $x \geqslant a$, $\forall x \in X$. Consideremos o conjunto $Y = -X = \{y = -x; x \in X\}$ Como $a \leqslant x$, para todo $x \in X$, temos que $-x \leqslant -a$ para todo $x \in X$. Portanto, segue que $y \leqslant -a$, $\forall\, y \in Y$, ou seja, Y é limitado superiormente pelo número inteiro $-a$.

Donde conclui-se, pelo axioma anterior, que o subconjunto Y possui um elemento máximo, $y_0 = -x_0$, com $x_0 \in X$. Dessa forma, $y \leqslant y_0$, donde $-y_0 \leqslant -y$. Assim $-y_0 \leqslant x$, $\forall x \in X$, e desse modo, temos que $-y_0 = x_0$ é o elemento mínimo de X. ■

Vejamos uma aplicação bastante interessante da proposição anterior.

Exemplo 2.2.9. *Não existe número natural x tal que $0 < x < 1$.*

De fato, suponhamos por absurdo que existe um número natural x tal que $0 < x < 1$. Assim, o conjunto A=$\{x \in \mathbb{Z}; 0 < x < 1\}$ é não vazio. Como o conjunto A é limitado inferiormente pelo número 0, segue pela proposição anterior, que existe $m = \text{minA}$. Nesse caso, $m \in A$, donde $0 < m < 1$ e por conseguinte temos que $0.m < m.m < 1.m$. Assim, $0 < m^2 < m < 1$ e, portanto, $m^2 \in A$. Isso constitui um absurdo pois $m = \text{minA}$. Dessa forma, não pode existir x natural tal que $0 < x < 1$.

Proposição 2.3. ***Segundo Princípio da Indução.*** *Seja $X \subset \mathbb{N}$, $0 \in X$, com a seguinte propriedade: dado um natural n, se X contém todos os naturais m tais que $m < n$, então $n \in X$. Nestas condições, $X = \mathbb{N}$.*

Demonstração:

Seja $Y = \mathbb{N} - X$. Afirmamos que o subconjunto $Y = \varnothing$. De fato, se Y não for vazio, pela proposição 1.2, existe um elemento mínimo, digamos y_0. Note que $y_0 \in Y$ e como $0 \in X$, tem-se $y_0 \geqslant 1$. Por outro lado, $\forall x \in \mathbb{N}$ tal que $x < y_0$ tem-se $x \in X$. Mas, pela hipótese sobre X, concluímos que $y_0 \in X$, uma contradição. Portanto, $Y = \varnothing$, donde segue que $X = \mathbb{N}$. ■

Observe que a condição $x < y_0$ é satisfeita pelo menos para o número zero, de sorte que não estamos tratando de um caso de vacuidade.

2.3. Divisão Euclidiana em $\mathbb{Z}$

De posse dos resultados obtidos na seção anterior, no teorema 1.3.1 será feita a primeira demostração da Divisão Euclidiana. Inicialmente mostraremos alguns resultados que culminarão com a demonstração do teorema citado.

Lema 2.1. *Sejam a e b dois números inteiros, com $b > 0$. Então existe um número inteiro d tal que $db \leqslant a$.*

Demonstração:

Suponhamos por absurdo que $a < db$ para todo número inteiro d. Consideremos o conjunto $A = \{db; d \in \mathbb{Z}\}$. Assim, o conjunto A é não vazio e limitado inferiormente por a. Dessa forma, pela proposição 1.2, o subconjunto A possui menor elemento, ou seja, existe $d_0 \in \mathbb{Z}$ com $d_0 b = \min$ A. Assim, $d_0 b > a$. Por outro lado, temos que $(d_0 - 1)b \notin A$. De fato, se $(d_0 - 1)b \in A$, então $d_0 b < (d_0 - 1)b$. Consequentemente, como $b > 0$, temos que $d_0 < (d_0 - 1)$, um absurdo, pois $d_0 > (d_0 - 1)$.

Portanto,$(d_0 - 1)b \notin A$, e assim temos que $(d_0 - 1)b \leqslant a$. Mas isso é um absurdo, porque estamos supondo que $a < db$ para todo número inteiro d. ■

Lema 2.2. *Sejam a e b dois números inteiros, com $b > 0$. Então existem únicos números inteiros q e r tais que $a = bq + r$ e $0 \leqslant r < b$.*

Demonstração:

Dados os inteiros a e b, com $b > 0$, consideremos o conjunto $B = \{db \leqslant a; d \in \mathbb{Z}\}$. Temos, pelo lema anterior, que $B \neq \varnothing$. Por outro lado, B é limitado superiormente pelo número inteiro a. Dessa forma, pelo axioma 1.1, existe elemento máximo $M_0 b$. Por outro lado, $(M_0 + 1)b > a$. De fato, se $(M_0 + 1)b \leqslant a$ teríamos que $(M_0 + 1)b \in B$. Daí $(M_0 + 1)b < M_0 b$. Logo, $M_0 + 1 < M_0$, uma contradição, pois $M_0 + 1 > M_0$. Portanto, temos que $M_0 b \leqslant a < (M_0 + 1)b$, ou de forma equivalente, existe M_0 inteiro tal que $0 \leqslant a - M_0 b < b$.

Sejam $q = M_0$ e $r = a - M_0 b$. Isso dá conta da existência. Observe que a unicidade decorre da unicidade do elemento máximo de B. ■

Corolário 2.3.1. *Sejam a e b dois números inteiros, com $b < 0$. Existem únicos números inteiros q e r tais que $a = bq + r$ e $0 \leqslant r < -b$.*

Demonstração:

A prova é imediata, pois $b < 0$ equivale dizer que $-b > 0$. Pelo lema anterior, existem únicos inteiro Q e R tais que $a = -bQ + R$ e $0 \leqslant R < -b$.

Denotando $q = -Q$ e $r = R$, temos que existem únicos inteiros q e r tais que $a = bq + r$ e $0 \leqslant r < -b$. ■

Teorema 2.3.1. ***Divisão Euclidiana em*** $\mathbb{Z}$

Sejam a e b dois números inteiros, com $b \neq 0$. Existem únicos números inteiros q e r tais que $a = bq + r$ e $0 \leqslant r < |b|$.

Demonstração:

Analisando os casos conforme $b > 0$ ou $b < 0$, a demonstração é uma consequência imediata dos resultados anteriores, conforme a seguir. Se $b > 0$, basta usar o Lema 1.2, e se $b < 0$, basta usar o corolário. ■

2.4. Outra demonstração da Divisão Euclidiana em $\mathbb{Z}$

Agora iremos apresentar uma segunda demonstração da Divisão Euclidiana em $\mathbb{Z}$. Essa demonstração será feita no teorema 1.4.1 Antes, será demonstrado um lema que será usado para estendermos a todos os inteiros.

Lema 2.3. ***Divisão Euclidiana em*** $\mathbb{N}$

Sejam a e b dois números naturais, com $b > 0$. Então, existem únicos números naturais q e r tais que $a = bq + r$, com $0 \leqslant r < b$.

Demonstração:

Se $a < b$, basta escolher $q = 0$ e $r = a$. Assim, vamos nos deter ao caso em que $a \geqslant b$, cuja prova da existência de q e r faremos por indução sobre o número natural a, em sua segunda forma.

Assim sendo, considerando $a \geqslant b$, temos que $0 \leqslant a - b < a$. Portanto, pela hipotese de indução, existem números naturais Q e R tais que $a - b = Qb + R$ e $0 \leqslant R < b$. Lodo, existem números naturais $q = Q + 1$ e $r = R$ tais que $a = bq + r$, com $0 \leqslant r < b$, mostrando, dessa forma, a existência.

Provaremos agora a unicidade. Suponhamos que existam pares de números naturais (Q, R) e (q, r) tais que $a = bq + r$, com $0 \leqslant r < b$ e $a = bQ + R$, com $0 \leqslant R < b$. Suponhamos por absurdo $R \neq r$ e sem perda de generalidades seja $R > r$.

Logo, $0 < R - r = (Q - q)b$ e usando o fato que $R - r < b$ obtemos $0 < R - r = (Q - q)b < b$. Como $b > 0$, segue que $0 < Q - q < 1$. Uma contradição, pois $Q - q$ é um número inteiro e vimos que não existe número inteiro entre 0 e 1. Dessa forma, temos necessariamente que $R = r$, e como consequência, $Q = q$. ■

✠ **Observação 2.1.**

No início da demonstração do lema anterior, verificamos que no caso de a<b a divisão euclidiana é trivialmente satisfeita tomando $q = 0$ e $r = a$. Observe que neste caso, temos claramente um boa justificativa para nossos alunos no que diz respeito em colocar zero no quociente quando o dividendo for menor que o divisor.

Esse fato me chamou à atenção, pois ao longo de minha vida profissional vários alunos me questionaram sobre a questão do zero no quociente. De fato, não tinha percebido que

a explicação se dava pelo fato da unicidade da divisão euclidiana. Sempre que me deparo com tal pergunta faço questão de frisar o porquê e vejo que meus alunos ficam satisfeitos com meus argumentos.

A título de aproximar o aluno com essa realidade mostraremos com dois exemplos que é possível fazer um paralelo entre os conceitos de divisão nas séries iniciais com a divisão euclidiana apresentada neste trabalho.

Achar o quociente e o resto quando:

(a) Dividimos 631 por 6.

(b) Dividimos 32 por 6.

Vamos à solução de cada um deles.

(a) Começamos dividindo 6 por 6, cujo quociente é 1 e o resto é 0. Esse número 1 é o primeiro algarismo do quociente.

631	6
0	1

Em seguida, baixamos o 3 ao lado do resto anterior formando 03. Conforme vimos, pelo lema anterior, o número 03 quando dividido por 6 tem quociente 0 (segundo algarismo do quociente) e resto o próprio 03.

631	6
03	10
03	

Agora, baixamos o 1 ao lado do resto, formando 031, que dividido por 6 tem quociente 5 e resto 1. Esse número 5 é o terceiro algarismo do quociente.

631	6
03	105
031	
001	

Como não há mais algarismo a ser baixado, então o processso se encerra obtendo quociente 105 e resto 1.

Portanto, o quociente da divisão de 631 por 6 é 105 e o resto 1.

(b) Faremos de modo análogo ao que fizemos no item (a).

Começamos dividindo 3 por 6. Conforme vimos no lema anterior, o quociente é 0 é o resto é 3.

$$\begin{array}{r|l} 32 & 6 \\ \cline{2-2} 3 & 0 \end{array}$$

Em seguida, baixamos o 2 ao lado do resto 3, formando o 32. Ao dividir 32 por 6 obtemos quociente 5 e resto 2.

$$\begin{array}{r|l} 32 & 6 \\ \cline{2-2} 32 & 05 \\ 2 & \end{array}$$

Portanto, o quociente da divisão de 32 por 6 é 05 e o resto é 2.

Note que no item (b) o número 05 pode ser escrito simplesmente como sendo 5, uma vez que esse zero à sua esquerda pode ser omitido. Nesse caso, o primeiro passo da divisão poderia ser suprimido. É isso que aprendemos a fazer nas séries iniciais: "Como o 3 é menor do que 6 então passamos ao próximo número, formando o 32."Já no item (a) o quociente é 105 e esse 0 não pode ser omitido, uma vez que os números 15 e 105 não representam o mesmo valor.

Nos dois casos, o zero no quociente apareceu porque estamos fazendo a divisão euclidiana, e para atender às condições sobre existência e unicidade em relação ao quociente e resto, temos necessariamente que o quociente é 0 e o resto o próprio dividendo. Assim, conseguimos uma explicação via divisão euclidiana, do porquê colocamos zero no quociente quando fazendo a divisão em que o dividendo é menor do que o divisor.

Teorema 2.4.1. ***Divisão Euclidiana em*** $\mathbb{Z}$ *Sejam a e b dois números inteiros, com $b \neq 0$. Existem únicos números inteiros q e r tais que $a = bq + r$ e $0 \leqslant r < |b|$.*

Demonstração:

Se a e b são naturais é verdade pelo lema anterior. Sejam a e b inteiros tal que $b \neq 0$. Mas $b \neq 0$ equivale dizer que o módulo de b é não nulo e portanto positivo. Vamos fazer em dois casos, conforme $a > 0$ ou $a < 0$, analisando alguns subcasos.

(i) Seja $a > 0$, pelo lema anterior temos $a = Q|b| + R$. Se b>0 tome $q = Q$ e $r = R$; Se $b < 0$ tome $q = -Q$ e $r = R$.

(ii) Se $a < 0$ então $-a > 0$, e desse modo, existem números nturais Q e R tais que $-a = Q|b| + R$ e $0 \leqslant R < |b|$. Se $R = 0$ então $a = -Q|b| + 0$, donde escolha $q = -Q$ e $r = 0$ quando $b > 0$, e de forma análoga, $q = Q$ e $r = 0$ quando $b < 0$. Seja agora $0 < R < |b|$. Logo, $0 < R - |b| < |b|$ e $a = -Q|b| - R$. Neste caso, tome $r = |b| - R$ e $q = -Q - 1$.

■

Doravante, caso não seja feita nenhuma menção, quando nos referirmos à divisão estamos querendo dizer que se trata da Divisão Euclidiana.

2.5. Todo número racional tem representação decimal finita ou periódica

Dado um número racional, uma aplicação bastante interessante da divisão é mostrar que sua representação decimal é finita ou é periódica. Na justificativa de tal fato será usado também um princípio que tem várias aplicações. Esse princípio é chamado de Princípio das Gavetas ou Princípio das Casas dos Pombos, que iremos enunciar e justificá-lo.

Proposição 2.4. *Se distribuirmos $n + 1$ pombos em n casas, então pelo menos uma casa terá mais de um pombo pois temos $n + 1$ pombos.*

Demonstração:

De fato, suponhamos que em cada casa tenha no máximo um pombo. Neste caso, teríamos no máximo n pombos, provando, dessa forma, que pelo menos uma casa terá mais de um pombo. ■

Feito isso, iremos mostrar como aplicação da divisão o que nos propusemos, ou seja, mostrar que todo número racional possui representação decimal finita ou periódica.

Seja um número racional $r = \dfrac{a}{b}$, com a e b números inteiros e $b \neq 0$. Observe que se $b < 0$, tomemos a fração equivalente $r = \dfrac{a}{b} = \dfrac{-a}{-b}$. Neste caso, $-b > 0$ e, portanto, sem perda de generalidade podemos considerar apenas um número racional $r = \dfrac{a}{b}$, com $b > 0$.

Conforme vimos, pela divisão, existem únicos inteiros q e r tais que $a = bq + r$, com $0 \leqslant r < b$. Vamos analisar dois casos conforme $r = 0$ ou $r \neq 0$.

(i) Se $r = 0$, a divisão é exata e o número racional é inteiro e, portanto, sua representação decimal é finita.

(ii) Se $r \neq 0$, colocamos zero ao lado resto (e uma vírgula ao lado do quociente somente na primeira vez) e prosseguimos com a divisão, obtendo um novo resto. O procedimento consiste em colocar zero ao lado de cada resto obtido e dividir, obtendo o próximo algarimo do quociente e um novo resto.

Sejam r_i, $i \in \{1, 2, ...\}$, esses restos obtidos, e pela divisão, cada um deles são tais que $0 \leqslant r_i < b$. Se algum dos $r_i = 0$ então o processo se encerra e o quociente terá representação finita.

Consideremos o caso em que todos os $r_i \neq 0$ e assim temos que $0 < r_i < b$. Nesse caso os r_i podem assumir no máximo $b - 1$ valores: $1, 2, ..., b - 1$. Sejam r_1, r_2, ...,r_b os b primeiros restos. Olhando r_1, r_2, ...,r_b com pombos e $1, 2, ..., b - 1$ como casas, temos que pelo menos dois dentre os restos r_i assumem o mesmo valor entre os possíveis $1, 2, ..., b - 1$. Assim, essa repetição dos restos provocará a repetição do quociente gerando uma representação periódica.

Portanto, todo número racional tem representação decimal finita ou periódica.

Esse exercício aparece resolvido em [11] apenas para os racionais positivos mas o autor não explicitou todos os detalhes. Para se aprofundar sobre outros aspectos em relação às condições de um um número racional ter representação finita ou periódica veja em [8] e [12].

✠ **Observação 2.2.**

Vamos justificar o fato de ir colocando zeros ao lado do resto para continuar dividindo. Vejamos isso com um exemplo. Obter a representação decimal de $\frac{36}{7}$ com 3 casas decimais.

Como queremos 3 casas decimais, então escrevemos convenientemente $\frac{36}{7} = \frac{36000}{7000}$ e dividimos 36000 por 7 obtendo no quociente 5142. Agora, deslocaremos 3 casas decimais para a esquerda obtendo $5,142$. O que fizemos foi dividir 36000 por 7 e em seguida por 1000, que neste último caso corresponde a contar 3 casas decimais da direita para a esquerda e colocar uma vírgula.

Se já soubéssemos quantas casas decimais seriam usadas, bastava obter a fração equivalente à primeira com uma quantidade de zeros igual à quantidade de casas decimais e em seguida, fazer a divisão do numerador pelo denominador (sem os zeros). Posteriormente deslocamos a vírgula tantas casas decimais para a esquerda quantos forem os zeros. Caso queira obter o quociente em que apareça pelo menos o periodo, então deveremos obter a fração com 8 zeros, uma vez que os possíveis valores do restos são de 0 à 6. No caso geral, dado um número racional $r = \frac{a}{b}$, com $b > 0$, para obter sua representação decimal em que apareça pelo menos o período explícito, basta escrever a fração equivalente com

$b+1$ zeros, porque garante que pelo menos dois restos assumam o mesmo valor dentre os b possíveis em $\{0, 1, ..., b-1\}$, ocasionando repetição dos restos.

A colocação de zeros ao lado do resto para continuar dividindo é um procedimento auxiliar que permite omitir a fase de preparação para obter uma fração equivalente à primeira com uma quantidade de zeros conveniente.

3. CONGRUÊNCIA

3.1. Introdução

Uma vez admitido o conhecimento da divisão euclidiana, naturalmente abordamos o conceito de congruência. Esse conceito é robusto na solução de alguns problemas numéricos interessantes. Como veremos na atividade aplicada em sala, o esforço que aluno e professor deverá desprender é mínimo no sentido dessa abordagem contextualizada do conceito de congruência.

A quem interessar uma abordagem mais profunda sobre o assunto, recomendo uma leitura de [9] e [13]. Este último autor descreve o assunto de forma lógica e capacita o leitor neste conceito desenvolvendo certas habilidades algébricas que permitem um domínio pleno deste conceito.

A seguir daremos o conceito de congruência e usaremos alguns exemplos com o intuito de explicitar de forma concreta esse conceito.

3.2. Definição e propriedades básicas

Definição 3.2.1. *Seja m um inteiro não nulo. Dois inteiros a e b são ditos congruentes módulo m quando a e b deixam mesmo resto na divisão por m. Neste caso, escrevemos $a \equiv b \, mod \, m$. Quando a e b não deixarem o mesmo resto na divisão por m então eles são ditos não congruentes e representamos por $a \not\equiv b \, mod \, m$.*

Proposição 3.1. *Sejam a, b e m números inteiros, com $m \neq 0$. Temos que: $a \equiv b \, mod \, m$ se e somente se $a \equiv b \, mod(-m)$.*

Demonstração:

De fato, suponhamos que a e b sejam congruentes módulo m. Pela divisão, existem inteiros q, Q e R tais que

$$a = qm + r \text{ e } b = Qm + r, \text{ com } 0 \leqslant r < |m|.$$

Note porém, que as expressões anteriores poderiam ser escritas da seguinte forma,

$$a = (-q)(-m) + r \text{ e } b = (-Q)(-m) + r, \text{ com } 0 \leqslant r < |-m|.$$

Isso mostra que a e b deixam também o resto r quando divididos por $-m$ e portanto, concluímos que a e b são congruentes módulo $-m$.

Reciprocamente, suponhamos que a e b sejam congruentes módulo $-m$. Pela divisão, existem inteiros q, Q e r tais que

$$a = q(-m) + r \text{ e } b = Q(-m) + r, \text{ com } 0 \leqslant r < |-m|.$$

De forna análoga ao que fizemos anteriormente, temos que

$$a = -qm + r \text{ e } b = -Qm + r, \textit{ com } 0 \leqslant r < |m|.$$

Portanto, mostramos que a e b são congruentes módulo m. ■

Proposição 3.2. *Para quaisquer números inteiros a e b temos que $a \equiv b \, mod \, 1$.*

Demonstração:

De fato, temos que $a = 1.a + 0$ e $b = 1.b + 0$. Isso mostra que os números inteiros a e b deixam resto 0 quando dividido por um. Portanto, a e b são congruentes módulo 1. ■

Conforme vimos, $a \equiv b \, mod \, m$ se e somente se $a \equiv b \, mod(-m)$ e para quaisquer números inteiros a e b temos que $a \equiv b \, mod \, 1$. Assim, caso não seja feita nenhuma menção usaremos $m > 1$.

Exemplo 3.2.1. *Temos que $7 \equiv 3 \, mod \, 2$ pois $7 = 2.3 + 1$ e $3 = 2.1 + 1$. De forma análoga, $7 \not\equiv -3 mod \, 4$ pois $7 = 2.4 + 3$ e $-3 = -1.4 + 1$.*

Agora, iremos demonstar dois lemas que serão usados quando for feita a demonstração do teorema básico que reúne algumas propriedades da congruência.

Lema 3.1. *Sejam a, b, c e m números inteiros, com $m \neq 0$. Se $m \mid a$ e $m \mid b$ então:*

(i) O inteiro m divide ab.

(ii) $m \mid (ax + by)$, quaisquer que sejam os inteiros x e y. Em particular, $m \mid (a + b)$.

(iii) $m \mid (b \pm c) \Leftrightarrow m \mid c$

Demonstração:

Sejam a, b e m números inteiros, com $m \neq 0$. Se $m \mid a$ e $m \mid b$, então existem inteiros k e l tais que $a = mk$ e $b = ml$. Assim, temos que:

(i) O inteiro ab se escreve da forma $(mk)(ml)$, donde $ab = mx$, com $x = mkl \in \mathbb{Z}$. Portanto, $m \mid ab$.

(ii) O inteiro $ax + by$ se escreve da forma $(mk)x + (ml)y$, donde $ax + by = m(kx + ly)$ e, portanto, $ax + by = mn$ com $n = kx + yl \in \mathbb{Z}$. Logo, $m \mid (ax + by)$.

(iii) Suponhamos que $m \mid (b + c)$. Nesse caso, existe um número inteiro z tal que $b + c = mz$, e usando a hipótese que b=ml, obtemos $c = mz - ml$. Logo, $c = m(z - l)$ e portanto, $c = ms$, com $s = (z - l) \in \mathbb{Z}$. Isso mostra que $m \mid c$. Reciprocamente, se $m \mid c$, então $c = ms$, para algum número inteiro s. Usando a hipótese que $b = ml$ obtemos, $b + c = ml + ms = m(l + s) = mv$, para algum número inteiro v. Portanto, $m \mid (b + c)$.

O caso $b - c$ é análogo e deixamos como exercício para o leitor.

■.

Lema 3.2. *Sejam a, b e m números inteiros. Temos que* $a \equiv b \, mod \, m$ *se, e somente se,* $m \mid (a - b)$.

Demonstração:

Sabemos que se $a \equiv b \, mod \, m$, existem q, Q e r inteiros tais que

$$a = mq + r \text{ e } b = mQ + r.$$

Dessa forma, $a - b = m(q - Q)$. Donde, concluímos que $m \mid (a - b)$.

Reciprocamente, suponhamos que $m \mid (a - b)$. Pela divisão, existem números inteiros $q,\ Q,\ r$ e R tais que

$$a = mq + r, \text{ com } 0 \leqslant r < m \text{ e } b = mQ + R, \text{ com } 0 \leqslant R < m.$$

Dessa forma, $a - b = m(q - Q) + (r - R)$. Como por hipótese $m \mid (a - b)$ e observando que $m \mid m(q - Q)$, segue que $m \mid (r - R)$ e juntamente com o fato de $0 \leqslant R - r < m$, obtém-se $R = r$. Portanto, $a \equiv b \, mod \, m$. ■

Agora será feita a demonstração do teorema que reúne as propriedades básicas da conguência.

Teorema 3.2.1. *Sejam a, b, c, d, m,e n números inteiros, com* $n \geqslant 1$.
Temos que:

(i) $a \equiv a \, mod \, m \ \forall a \in \mathbb{Z}$.

(ii) Se $a \equiv b \, mod \, m$, *então* $b \equiv a \, mod \, m$.

(iii) Se $a \equiv b \, mod \, m$ *e* $b \equiv c \, mod \, m$, *então* $a \equiv c \, mod \, m$.

(iv) Se $a \equiv b \, mod \, m$ *e* $c \equiv d \, mod \, m$, *então* $a + c \equiv b + d \, mod \, m$ *e* $ac \equiv bd \, mod \, m$.

(v) Se $a \equiv b \, mod \, m$, *então* $a^n \equiv b^n \, mod \, m$.

Demonstração:

(i) Claramente, $m \mid (a - a)$ para todo inteiro "a". Então, pelo lema anterior, temos a afirmação.

(ii) Da mesma forma, pelo lema anterior temos que $m \mid (a - b)$. Portanto, $m \mid -(a - b)$. Daí $m \mid (b - a)$. Usando novamente o lema concluímos que $b \equiv a \, mod \, m$.

(iii) Temos por hipótese que $a \equiv b \, mod \, m$ e $b \equiv c \, mod \, m$. Então, pelo lema anterior temos que $m \mid (a - b)$ e $m \mid (b - c)$. Portanto, $m \mid [(a - b) + (b - c)]$, ou seja, $m \mid (a - c)$. Daí $a \equiv c \, mod \, m$.

(iv) Temos por hipótese que $m \mid (a - b)$ e $m \mid (c - d)$. Logo, $m \mid [(a - b) + (c - d)]$, ou seja, $m \mid [(a + c) - (b + d)]$. Donde implica que $a + c \equiv b + d \, mod \, m$.

Como $ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b)$, segue pelo item (ii) do lema 2.1 que $m \mid (ac - bd)$, ou seja, $ac \equiv bd \, mod \, m$.

(v) Faremos por indução sobre n.

Note que o caso $n = 1$ já é verdadeiro por hipótese. Para compreendermos o passo indutivo, iremos fazer o caso $n = 2$. Pelo item anterior, se $a \equiv b \, mod \, m$ então $a.a \equiv b.b \, mod \, m$, donde $a^2 \equiv b^2 \, mod \, m$.

Suponhamos que $a^n \equiv b^n \, mod \, m$ e provemos que que $a^{n+1} \equiv b^{n+1} \, mod \, m$. De fato, se $a^n \equiv b^n \, mod \, m$ e usando a hipótese que $a \equiv b \, mod \, m$ segue que $a^n.a \equiv b^n.b \, mod \, m$.

Portanto, $a^{n+1} \equiv b^{n+1} \, mod \, m$ como queríamos demonstrar.

Assim está provado, por indução sobre n, que $a^n \equiv b^n \, mod \, m$ vale para todo n natural, com $n \geqslant 1$.

■

✠ **Observação 3.1.**

A três primeiras propriedades mostram que a congruência é uma relação que é reflexiva, simétrica e transitiva. Quando uma relação satisfaz a essas três propriedades então ela é chamada de relação de equivalencia. Portanto, a relação de congruência é uma relação de equivalência.

Já a quarta propriedade diz que a congruência é compatível com a soma e o produto. Para maiores detalhes sobre congruência e relação de equivalência sugerimos [9] e [4].

Veremos a seguir alguns exemplos de aplicação dessas propriedades. Antes será demonstrada uma proposição que também será usada nos exercícios exemplos.

Proposição 3.3. *Dados os números inteiros a e m, temos que:*

(i) Se r é o resto da divisão de a por m, então $a \equiv r \, mod \, m$.

(ii) Reciprocamente, se $a \equiv r \, mod \, m$ e $0 \leqslant r < m$, então r é o resto da divisão de a por m.

Demonstração:

De fato, sejam a e m números inteiros. Se r é o resto da divisão de a por m, então $a = mq + r$ para algum número inteiro q. Logo, $a - r = qm$ e, portanto, $m \mid (a - r)$. Conforme já vimos, $m \mid (a - r)$ é equivalente a dizer que $a \equiv r \, mod \, m$, provando, dessa forma, a primeira parte da proposição.

Provaremos, agora, a segunda parte da proposição. Consideremos o inteiro r tal que $a \equiv r \, mod \, m$ e $0 \leqslant r < m$. Ora, $a \equiv r \, mod \, m$ equivale a dizer que $m \mid (a - r)$. Logo, $a - r = qm$ para algum número inteiro q e assim, temos que $a = qm + r$. Sejam Q e R, respectivamente, o quociente e o resto da divisão de a por m. Pela unicidade do quociente e o do resto da divisão de a por m, temos que $R = r$ e $Q = q$. Isso prova a afirmação que se $a \equiv r \, mod \, m$ e $0 \leqslant r < m$, então r é o resto da divisão de a por m. ■

Exemplo 3.2.2. *Achar o resto da divisão de 7^{10} por 51.*

Note que $7^2 \equiv -2 \, mod \, 51$. Pela última propriedade do teorema anterior, podemos elevar membro a membro a qualquer expoente natural. Convenientemente elevaremos à quinta potência e obtemos que $7^{10} \equiv -32 \, mod \, 51$. Mas $32 \equiv 19 \, mod \, 51$. Pela terceira propriedade do mesmo teorema segue que $7^{10} \equiv 19 \, mod \, 51$.

Logo, conforme a proposição anterior temos que 7^{10} deixa resto 19 quando dividido por 51.

Exemplo 3.2.3. *Mostrar que 19^{8n} deixa resto 1 quando é dividido por 17, para todo natural n.*

Observe que $19 \equiv 2\, mod\, 17$. De forma análoga ao que fizemos no exemplo anterior elevamos membro a membro à uma potência conveniente, que nesse caso é a quarta potência, obtendo $19^4 \equiv 16\, mod\, 17$. Como $16 \equiv -1\, mod\, 17$ então $19^4 \equiv -1\, mod\, 17$. Elevando membro a membro ao quadrado obtemos $19^8 \equiv 1\, mod\, 17$ e portanto, $19^{8n} \equiv 1\, mod\, 17$.

Pela proposição anterior, temos que 19^{8n} deixa resto 1 quando é dividido por 17.

3.3. Atividade aplicada

A lista de exercícios a seguir foi trabalhada com 40 alunos do primeiro ano do Ensino Médio, no ano letivo de 2014, com o objetivo de mostrar que é possível compreender a definição de congruência no Ensino Médio. As questões 1 e 2 têm como objetivo principal de preparar os alunos para conpreender melhor as três últimas questões, cuja ideia implícita é tratar a definição de congruência.

INSTITUTO FEDERAL DE ALAGOAS: CAMPUS MARECHAL DEODORO
DISCIPLINA: MATEMÁTICA. CURSO: MEIO AMBIENTE
PROFESSOR: EDVAN HORÁCIO DOS SANTOS
ALUNO (A):..... N^0:.....
DATA:..../.... /..... TURMA:.....
O MOVIMENTO CIRCULAR E AS CONGUÊNCIAS

01)Dois móveis A e B estão numa rodovia distantes 360m e partem ao mesmo tempo e no mesmo sentido de B para A. O móvel A percorre 40m em cada segundo e se encontra no marco 360m. Já o B 60m por segundo e se encontra na origem das posições . Assim,as funções horárias deles podem ser representadas por $S_A(t) = 360 + 40t$ e $S_B(t) = 60t$. Determine:

a)Depois de quanto tempo o móvel B alcança A.

b)Qual a posição do encontro.

02)Dois móveis A e B estão numa rodovia distantes 180m e partem ao mesmo tempo e no mesmo sentido de B para A. O móvel A percorre 40m em cada segundo e se encontra no marco 180. Já o B 60m por segundo e se encontra na origem das posições. Assim,as funções horárias deles podem ser representadas por $S_A(t) = 180 + 40t$ e $S_B(t) = 60t$. Determine:

a)Depois de quanto tempo o móvel B alcança A.

b)Qual a posição do encontro.

03)Dois móveis A e B estão num círculo e partem ao mesmo tempo e no mesmo sentido. O móvel A percorre 40^0 em cada segundo e o B 60^0 por segundo. Assim,as funções horárias deles podem ser representadas por $\theta_A(t) = 40t$ e $\theta_B(t) = 60t$. Note que o móvel B está mais rápido do que o móvel A. Determine:

a)Depois de quanto tempo o móvel B alcança o móvel A pela primeira vez.

b)Depois de quanto tempo o móvel B alcança o móvel A pela segunda vez.

c)Depois de quanto tempo o móvel B alcança o móvel A pela terceira vez.

d) Determine uma expressão geral que caracteriza o momento em que o móvel B alcança o móvel A.

04)Dois móveis A e B estão num círculo e partem ao mesmo tempo e em sentidos contrários.O móvel A percorre 40^0 em cada segundo e o B 20^0. Assim, as funções horárias deles podem ser representadas por $\theta_A(t) = 40t$ e $\theta_B(t) = 20t$.

a)Depois de quanto tempo eles se cruzam pela primeira vez.

b)Depois de quanto tempo eles se cruzam pela segunda vez.

c)Depois de quanto tempo eles se cruzam pela terceira vez.

d)Determine uma expressão geral que carcteriza o momento em que eles se cruzam.

05)Dois móveis A e B estão num círculo e partem ao mesmo tempo e em sentidos contrários. O móvel A descreve 4 rpm e B 6 rpm. Assim,as funções horárias deles podem ser representadas por $\theta_A(t) = 24t$ e $\theta_B(t) = 36t$. Determine:

a)Após quanto tempo eles estarão alinhados com o centro sem que estejam na mesma posição .

b)Após quanto tempo eles estarão alinhados com o centro, numa segunda vez, sem que estejam na mesma posição.

c)Após quanto tempo eles estarão alinhados com o centro, numa terceira vez, sem que estejam na mesma posição .

d)Uma expressão geral que caracteriza após quanto tempo eles estarão alinhados com o centro, sem que estejam na mesma posição .

Apresentamos a resolução dessa lista de exercícios no final desse capítulo. Ela foi trabalhada com 40 alunos do primeiro ano do Ensino Médio, no ano letivo de 2014, e o resultado com o total de alunos que acertaram os respectivos itens de cada questão está conforme a tabela a seguir.

Questão	item a	item b	item c	item d
01	40	40	X	X
02	40	40	X	X
03	40	40	40	40
04	40	40	40	40
05	40	8	8	8

Ao analisarmos suas respostas, observamos que que 32 alunos responderam errado os itens b, c e d da última questão. Eles não perceberam que apareciam apenas múltiplos ímpares de 180 graus. Para os 8 alunos que resolveram corretamente a última questão mostrei que podemos obter a expressão t= 6k+3 onde k é um natural, donde t deixa resto 3 quando dividido por 6.

Os alunos resolveram as questões três e quatro mesmo sem saber que estavam resolvendo um problema de congruência. Na questão 03 aparecem múltiplos de 360 graus e na questão 40 aparecem múltiplos de 180 graus. As duas primeiras questões foram colcadas para que eles percebessem a relação com as questões três e quatro, cuja solução são bastante semelhantes.

Em uma das turmas foram feitas sugestões a partir da questão três, cujo objetivo foi comparar os tipos de respostas e dúvidas apresentadas. Surpreendentemente, os resultados não foram substanciamente diferentes nas duas turmas.

Assim, os alunos resolveram os exercícios mesmo sem saber que alguns deles se tratavam de congruência. Em [13] são apresentadas várias outras situações em que a congruência é usada de forma implíca ou explícita.

A seguir, daremos a solução de cada questão, fazendo comentários em algumas delas.

Questão 01.

(a) Basta igualar as expressões das funções horárias dos móveis, conforme a seguir.

$\theta_B(t) = \theta_A(t) \Leftrightarrow 60t = 40t + 360 \Leftrightarrow 20t = 360 \Leftrightarrow t = 18$ s.

(b) De posse do item (a), basta substituir em uma das expressões das funções horárias.

$\theta_B(18) = 60.18 = 1080m$

Questão 02. É análoga à questão 01.

(a) $\theta_B(t) = \theta_A(t) \Leftrightarrow 60t = 40t + 180 \Leftrightarrow 20t = 180 \Leftrightarrow t = 9$ s.

(b) $\theta_B(9) = 60.9 = 540m$.

Questão 03.

(a) A resolução é exatamente a mesma que foi feita na letra (a) da primeira questão.

(b) Basta ver que o móvel B está com 2 voltas na frente do móvel A.

$\theta_B(t) = \theta_A(t) \Leftrightarrow 60t = 40t + 2.360 \Leftrightarrow 20t = 720 \Leftrightarrow t = 36$ s.

(c) É análogo ao item anterior.

$\theta_B(t) = \theta_A(t) \Leftrightarrow 60t = 40t + 3.360 \Leftrightarrow 20t = 1080 \Leftrightarrow t = 54$ s.

(d) Esse item constitui uma generalização dos itens anteriores.

$\theta_B(t) = \theta_A(t) \Leftrightarrow 60t = 40t + k.360 \Leftrightarrow 20t = 360k \Leftrightarrow t = 18k$, $k \in \mathbb{N}$.

Note que o último item pode ser escrito da forma $\theta_B(t) - \theta_A(t) = k.360$, o que equivale a $\theta_B(t) \equiv \theta_A(t) mod\, 360$. Portanto, a ideia de congruência aparece de forma bastante natural durante a resolução desse problema, mostrando que é um esforço mínimo a formalização de tal conceito.

Questão 04.

(a) Basta notar que soma dos ângulos descritos pelos dois móveis corresponde a 360^0.

$\theta_B(t) + \theta_A(t) = 360 \Leftrightarrow 60t = 360 \Leftrightarrow t = 6$ s.

(b) Basta notar que soma dos ângulos descritos pelos dois móveis corresponde a duas voltas, ou seja, 2.360^0.

$\theta_B(t) + \theta_A(t) = 2.360 \Leftrightarrow 60t = 720 \Leftrightarrow t = 12$ s.

(c) Basta notar que soma dos ângulos descritos pelos dois móveis corresponde a três voltas, ou seja, 3.360^0.

$\theta_B(t) + \theta_A(t) = 3.360 \Leftrightarrow 60t = 1080 \Leftrightarrow t = 18$ s.

(d) Constitui uma generalização dos itens anteriores.

$\theta_B(t) + \theta_A(t) = k.360 \Leftrightarrow 60t = 360k \Leftrightarrow t = 6k$, $k \in \mathbb{N}$.

Note que o último item pode ser escrito da forma $\theta_B(t)+\theta_A(t) = k.360$, o que equivale a $\theta_B(t)+\theta_A(t) \equiv 0 mod\, 360$. Da mesma forma que a questão anterior, a ideia de congruência aparece de forma bastante natural durante sua resolução.

Questão 05.

(a) Basta notar que soma dos ângulos descritos pelos dois móveis corresponde a 180^0.

$\theta_B(t) + \theta_A(t) = 180 \Leftrightarrow 60t = 180 \Leftrightarrow t = 3$ s.

(b) De maneira análoga, temos que soma dos ângulos descritos pelos dois móveis corresponde a 3.180^0.

$\theta_B(t) + \theta_A(t) = 3.180 \Leftrightarrow 60t = 540 \Leftrightarrow t = 9$ s.

(c) É semelhante ao item anterior, cuja soma dos ângulos descritos pelos dois móveis corresponde a 5.180^0.

$\theta_B(t) + \theta_A(t) = 5.180 \Leftrightarrow 60t = 900 \Leftrightarrow t = 15$ s.

(d) Constitui uma generalização dos itens anteriores, pois soma dos ângulos descritos pelos dois móveis corresponde a um múltiplo ímpar de 180^0.

$\theta_B(t) + \theta_A(t) = k.180 \Leftrightarrow 60t = 180k \Leftrightarrow t = 3k$, $k \in \mathbb{N}$, tal que k é ímpar. Aqui, também poderíamos modelar com a congrência.

As figuras a mostram as fotos da anotação de um aluno e sua respectiva turma quando essa lista de exercícios foi aplicada.

Primeira figura da atividade sobre congruência

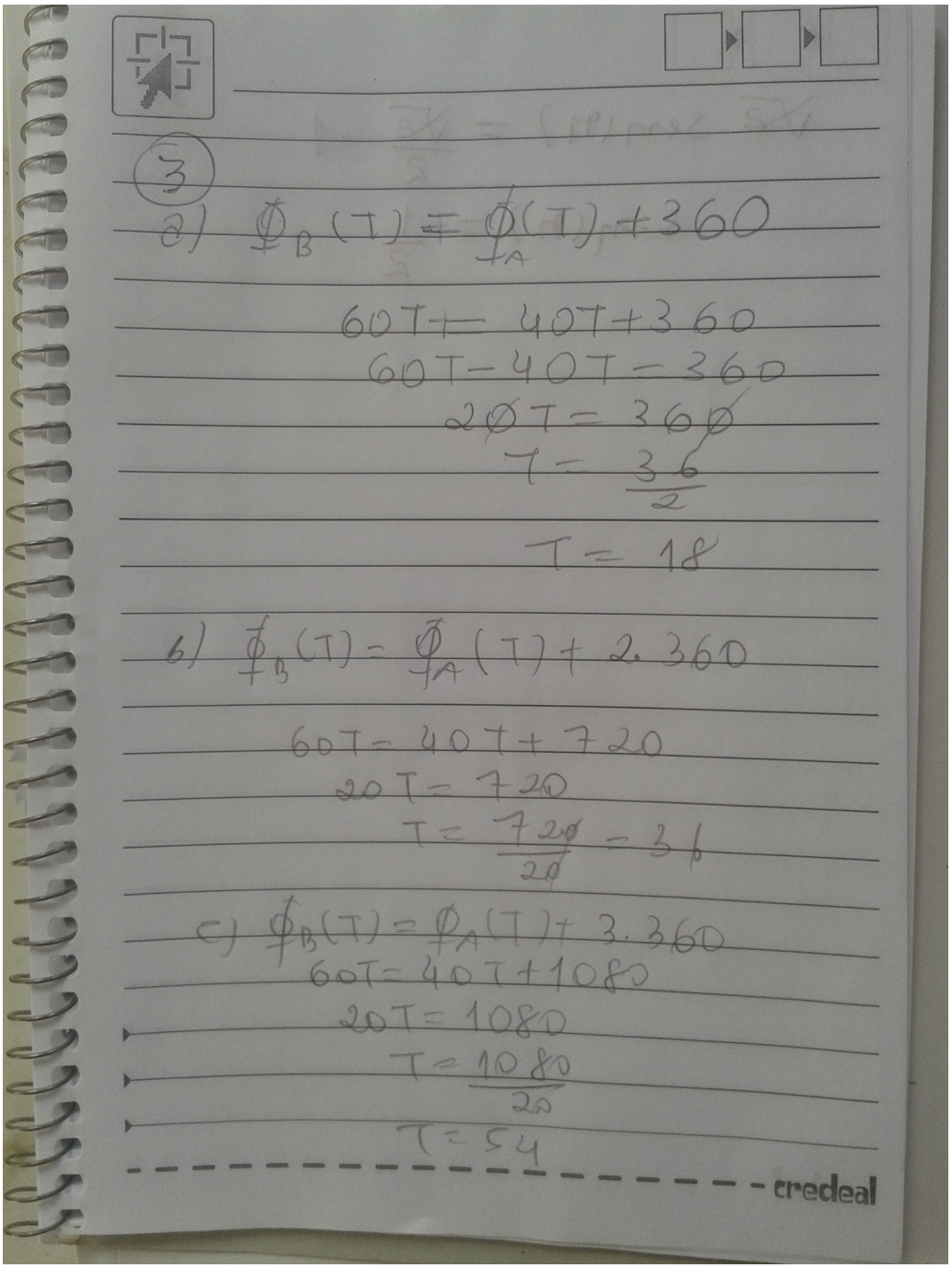

Figura 3.1: Fonte: Autor, 2014.

Segunda figura da atividade sobre congruência

Figura 3.2: Fonte: Autor, 2014.

4. DOMÍNIO DE INTEGRIDADE

4.1. Motivação para tratar sobre Domínio de Integridade

Nos Parâmetros Curriculares Nacionais do Ensino Médio(PCNEM) é previsto que a Matemática além de seu caráter formativo ou instrumental, deve ser vista como ciência com suas próprias específicidades.

> Contudo, a Matemática no Ensino Médio não possui apenas o caráter formativo ou instrumental, mas também deve ser vista como ciência, com suas características estruturais específicas(PARÂMETROS CURRICULARES NACIONAIS DO ENSINO MÉDIO,1997,p. 40).

Dentro desta perspectiva serão descritas duas situações que ensejaram a possibilidade de discussão sobre um objeto matemático conhecido como Domínio de Integridade.

Fui surpreendido por alguns alunos do segundo ano do Ensino Médio, quando me questionaram sobre qual fundamentação teórica podemos nos desbruçar para garantir a eles a aplicação da "Lei do Corte", ou seja, poder cortar P_2 na equação

$$\frac{P_2V_1}{10} = \frac{P_2V_0}{2},$$

que aparece de forma natural no estudo de Gases na disciplina de Química. Quando tentei responder ao questionamento desses alunos, senti a necessidade de recorrer ao fato do conjunto dos números reais, $\mathbb{R}$, ser um domínio de integridade. Inicialmente chamei atenção dos mesmos para o fato de $P_2 \neq 0$ ser de fundamental importância para que possamos concluir, a partir da equação dada, que $V_1 = 5V_0$. Também enfatizei para o fato de que em caso de ocorrer $P_2 = 0$, a equação é atendida para quaisquer valores de V_1 e V_0. Salientei que nas aulas seguintes traria subsídios necessários que permitissem identificar um domínio de integridade e que daria exemplos de objetos matemáticos conhecidos por

eles, onde a Lei do Cancelamento não vale. Nesse sentido, disse para eles o seguinte: Se $ax = ay$, com $a \neq 0$, não podemos concluir, em geral, que $x = y$. Novamente, em outro momento, fui surpreendido com a mesma pergunta, por alunos de uma outra turma, sobre o cancelamento do número $\sqrt{3}$ ao usar a lei Snell-Descartes em uma aplicação envolvendo a Refração da Luz. Ao aplicarem essa lei em um exercício obtiveram a equação

$$\sqrt{3}.sen(r) = \frac{\sqrt{3}}{2}.1.$$

Durante a resolução desse exercício, que se encontrava em [7], eles observaram que $\sqrt{3}$ era cortado explicitamente e escrevia

$$sen(r) = \frac{1}{2},$$

cuja solução é r como sendo 30 graus. Novamente, me deparei com o mesmo tipo de questionamento sobre a Lei do Cancelamento feito anteriormente por outros alunos. Minha resposta, foi dizer que como $\sqrt{3} \neq 0$, juntamente com o fato de $\mathbb{R}$ ser um domímio de integridade permite que faça o cancelamento. Informei a esses alunos que nas próximas aulas forneceria elementos teóricos que permitissem a eles tirar conclusões sobre quando vale a Lei do Cancelamento.

4.2. Definição, propriedades básicas e exemplos

Nesta seção iremos formalizar o conceito de Domínio de Integridade e em seguida demonstrar as propriedades básicas de um Domínio de Integridade.

Em seguida serão dados alguns exemplos de conjuntos para ilustrar o fato do conjunto ser ou não Domínio de Integriadde.

Definição 4.2.1. *Sejam A um conjunto, $\oplus$ e $\odot$ duas operações em A chamadas de adição e multiplicação respectivamente.*

*A terna $(A, \oplus, \odot)$ será chamada de **ANEL** quando as propriedades abaixo forem verificadas quaisquer que sejam $a, b, c \in A$.*

1. *$(a \oplus b) \oplus c = a \oplus (b \oplus c)$ (a adição é associativa).*
2. *Existe $\alpha \in A$ tal que $a \oplus \alpha = \alpha \oplus a = a$ (existência de elemento neutro para a adição).*
3. *Para todo $x \in A$ existe um $y \in A$ tal que $x \oplus y = y \oplus x = \alpha$ (existência de elemento simétrico para a adição).*

4. $a \oplus b = b \oplus a$ *(a adição é comutativa).*

5. $(a \odot b) \odot c = a \odot (b \odot c)$ *(a multiplicação é associativa).*

6. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ *(distributividade à direita).*

7. $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$ *(distributividade à esquerda).*

8. *Se, além disso, um anel* $(A, \oplus, \odot)$ *satisfaz a seguinte propriedade: Existe um elemento* $\beta \in A$*, com* $\beta \neq \alpha$*, tal que* $a \odot \beta = \beta \odot a = a$*,* $\forall a \in A$*, dizemos que* $(A, \oplus, \odot)$ *é um* ***Anel com elemento unidade*** β*.*

9. *Se* $a \odot b = b \odot a$ $\forall a, b \in A$*, dizemos que* $(A, \oplus, \odot)$ *é um* ***Anel Comutativo****.*

10. *Quando um anel* $(A, \oplus, \odot)$ *satisfaz a seguinte propriedade: Se* $a \odot b = 0$*, com* $a, b \in A$*, implica* $a = 0$ *ou* $b = 0$*, dizemos que* $(A, \oplus, \odot)$ *é um* ***Anel Sem Divisores de zero****.*

    Um anel $(A, \oplus, \odot)$ *comutativo e sem divisores de zero é denominado* ***Domínio de Integridade****.*

11. *Se um anel* $(A, \oplus, \odot)$ *com elemento unidade* β *satisfaz a seguinte propriedade: Para todo* $a \neq \alpha$ *existe* $b \neq \alpha$ *tal que* $a \odot b = \beta$ *dizemos que* $(A, \oplus, \odot)$ *é um* ***Corpo****.*

Proposição 4.1. *Num anel* $(A, \oplus, \odot)$ *temos a unicidade dos seguintes elementos:*

(i) Elemento neutro da adição.

(ii) Elemento simétrico.

(iii) Elemento unidade

Demonstração:

Provemos cada um dos itens conforme a seguir.

(i) Sejam α e α' elementos neutros da adição. Assim, temos que $a \oplus \alpha = \alpha \oplus a = a$, $\forall\ a \in A$ e $a \oplus \alpha' = \alpha' \oplus a = a$, $\forall\ a \in A$. Em particular, temos que $\alpha = \alpha \oplus \alpha' = \alpha' \oplus \alpha = \alpha'$.

(ii) Sejam y e y' elementos simétricos de um elemento $x \in A$. Assim, temos que

$x \oplus y = y \oplus x = \alpha$ e $x \oplus y' = y' \oplus x = \alpha$.

Por outro lado, note que

$y = y \oplus \alpha = y \oplus (x \oplus y') = (y \oplus x) \oplus y' = \alpha \oplus y' = y'$.

Logo, $y = y'$.

(iii) Sejam β e β' elementos neutros da multiplicação. Nestas condições, temos que $a \odot \beta = \beta \odot a = a,\ \forall\ a \in A$ e $a \odot \beta' = \beta' \odot a = a,\ \forall\ a \in A$. Em particular, temos que $\beta = \beta \odot \beta' = \beta' \odot \beta = \beta'$.

■

Doravante, fazendo um paralelo com o conjunto dos números reais, usaremos os símbolos $0, -x$ e 1 para representar o elemento neutro da adição, elemento simétrico de um elemento x qualquer e elemeto unidade, respectivamente.

Enunciaremos a seguir algumas propriedades básicas que decorrem do fato de $(A, \oplus, \odot)$ ser um Domínio de Integridade.

Proposição 4.2. *Num domínio de integridade $(D, \oplus, \odot)$ temos que:*

(i) *Se $x \oplus a = x \oplus b$, então $a = b$.*

(ii) $a \odot 0 = 0,\ \forall a, b \in D$.

(iii) *O elemento neutro da adição não é invertível.*

(iv) $(-1) \odot a = -a,\ \forall a \in D$

(v) *(Lei do Cancelamento ou Lei do Corte) $\forall a, x, y \in D$, com $a \neq 0$, se $a \odot x = a \odot y$ então $x = y$.*

Demonstração:

Observe que

$$\begin{aligned} a &= 0 \oplus a \\ &= ((-x) \oplus x) \oplus a \\ &= (-x) \oplus (x \oplus a) \\ &= (-x) \oplus (x \oplus b) \\ &= ((-x) \oplus x) \oplus b \\ &= 0 \oplus b \\ &= b. \end{aligned}$$

provando, dessa forma, o item (i).

Para demonstrar (ii), basta observar o seguinte:

$$\begin{aligned} 0 \oplus (a \odot 0) &= a \odot 0 \\ &= a \odot (0 \oplus 0) \\ &= (a \odot 0) \oplus (a \odot 0). \end{aligned}$$

Donde, pelo item anterior, concluímos que $a \odot 0 = 0$.

Agora, demonstraremos o item (iii). Suponhamos por absurdo, que o elemento neutro da adição seja invertível, ou seja, existe $b \in D$ tal que $0 \odot b = 1$. Conforme o item (ii), temos que $0 = 1$, e portanto um absurdo. Logo o elemento neutro da adição não é invertível.

Para demonstrar (iv) note que

$$\begin{aligned} a \oplus ((-1) \odot a) &= (1 \odot a) \oplus ((-1) \odot a) \\ &= (1 \oplus (-1)) \odot a \\ &= 0 \odot a \\ &= 0. \end{aligned}$$

Portanto, pela unicidade do elemento simétrico temos que $(-1) \odot a = -a$.

Finalmente, vamos demonstrar o item (v). Note que $a \odot x = a \odot y$ equivale ao resultado $a \odot x \oplus (-a \odot y) = 0$. Assim, temos que $a \odot (x + (-y)) = 0$

Por hipótese, temos que $a \neq 0$ e portanto, $x \oplus (-y) = 0$, donde $x = y$.

■

Exemplo 4.2.1. *Dentre os conjuntos numéricos* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, *e* $\mathbb{R}$ *apenas* $\mathbb{N}$ *não é um domínio de integridade porque nenhum elemento tem simétrico aditivo. No entanto, vale a lei do corte em* $\mathbb{N}$. *Note que omitimos as operações por se tratar das operações usuais.*

Exemplo 4.2.2. *Seja* $\mathbb{C} = \mathbb{R}^2 = \{(x, y); x \in \mathbb{R} \, e \, y \in \mathbb{R}\}$. *Usando as operações usuais de soma e produto do conjunto dos números reais,* $\mathbb{R}$, *iremos definir em* $\mathbb{C}$ *duas operações, e em seguida mostraremos que o conjunto* $\mathbb{C}$, *munido dessas duas operações é um Domínio de Integridade.*

Dados $(a, b) \, e \, (c, d) \in \mathbb{C}$, *definiremos a adição, denotada por* $\oplus$, *entre os elementos* $(a, b) \, e (c, d)$ *ao par ordenado* $(a + c, b + d)$, *isto é,*$(a, b) \oplus (c, d) := (a + c, b + d)$; *Definiremos a multiplicação, denotada por* $\odot$, *entre os elementos* $(a, b) \, e \, (c, d)$ *de* $\mathbb{R}^2$, *ao par ordenado* $(a.c - b.d, a.d + b.c)$, *ou seja,* $(a, b) \odot (c, d) := (a.c - b.d, a.d + b.c)$.

É fácil ver que essa operação $\oplus$ goza das seguintes propriedades: associativa, existe elemento neutro, existe elemento simétrico, comutativa.

De fato, mostraremos cada uma delas nos itens a seguir:

(i) Dados $z = (a, b)$ e, $w = (c, d)$ segue que

$$\begin{aligned} z \oplus w &= (a, b) \oplus (c, d) \\ &= (a + c, b + d) \\ &= (c + a, d + b) \\ &= (c, d) \oplus (a, b) \\ &= w \oplus z \end{aligned}$$

Assim, $\oplus$ é comutativa. Note que substituimos $a+c$ por $c+a$, uma vez que a adição é comutativa no conjunto dos números reais. O mesmo comentário se aplica em $b + d$.

(ii) De fato, sejam $z_1 = (a, b); z_2 = (c, d)$ e $z_3 = (e, f)$. Basta ver que

$$\begin{aligned} (z_1 \oplus z_2) \oplus z_3 &= ((a, b) \oplus (c, d)) \oplus (e, f) \\ &= (a + c, b + d) \oplus (e, f) \\ &= ((a + c) + e, (b + d) + f)) \\ &= (a + (c + e), b + (d + f)) \\ &= (a, b) \oplus (c + e, d + f) \\ &= (a, b) \oplus ((c, d) \oplus (e, f)) \\ &= z_1 \oplus (z_2 \oplus z_3) \end{aligned}$$

E isso prova que $\oplus$ é associativa. Note que substituimos $(a+c)+e$ por $a+(c+e)$, uma vez que a adição é associativa no conjunto dos números reais. O mesmo comentário se aplica em $(b + d) + f$.

(iii) Dado $w = (a, b)$, tome $\alpha = (0, 0)$. Note que $\alpha \in \mathbb{C}$.

Basta ver que

$$\begin{aligned} \alpha \oplus w &= w \oplus \alpha \\ &= (a, b) \oplus (0, 0) \\ &= (a + 0, b + 0) \\ &= (a, b) \\ &= w. \end{aligned}$$

Assim, $\alpha \oplus w = w \oplus \alpha = (a, b) \oplus (0, 0) = (a + 0, b + 0) = (a, b) = w$.

Portanto, como vimos acima, a operação $\oplus$ possui elemento neutro.

(iv) Dados $z = (a, b)$, tome $w = (-a, -b) \in \mathbb{C}$. Desse modo, temos que,

$$\begin{aligned} w \oplus z &= z \oplus w \\ &= (a,b) \oplus (-a,-b) \\ &= (a+(-a), b+(-b)) \\ &= (0,0) \\ &= \alpha. \end{aligned}$$

Logo, $\forall z \in \mathbb{C}\,, \exists w \in \mathbb{C}$ tal que $z + w = \alpha$.

Do mesmo modo, afirmamos que a operação $\odot$ goza das seguintes propriedades: comutativa, associativa, distributiva à direita e à esquerda, e sem divisores de zero.

De forma análoga ao que fizemos anteriormente, vamos provar cada uma das propriedades conforme os itens a seguir:

(i) Dados $z = (a,b)$ e $w = (c,d)$ temos que

$$\begin{aligned} z \odot w &= (a,b) \odot (c,d) \\ &= (a.c - b.d, a.d + b.c) \\ &= (c.a - d.b, c.b + d.a) \\ &= (c,d) \odot (a,b) \\ &= w \odot z \end{aligned}$$

Isso mostra que $\odot$ é comutativa.

(ii) De fato, sejam $z_1 = (a,b); z_2 = (c,d)$ e $z_3 = (e,f)$, basta observar que:

$$\begin{aligned} (z_1 \odot z_2) \odot z_3 &= ((a,b) \odot (c,d)) \odot (e,f) \\ &= (a.c - b.d, a.d + bc) \odot (e,f) \\ &= ((a.c - bd).e - (a.b + bc).f, (a.c - b.d.)f + (a.d + b.c).e) \\ &= (a.c.e - b.d.e - a.d.f - d.c.f, a.c.f - b.d.f + a.d.e + b.c.e) \\ &= (a.c.e - a.d.f - b.d.e - d.c.f, a.d.e + a.c.f + b.c.e - b.d.f) \\ &= (a.(c.e - d.f) - b.(d.e + c.f), a.(d.e + c.f) + b.(c.e - d.f)) \\ &= (a,b) \odot (c.e - d.f, c.f + d.e) \\ &= (a,b) \odot ((c,d) \odot (e,f) \\ &= z_1 \odot (z_2 \odot z_3). \end{aligned}$$

Portanto, a operação $\odot$ é associativa. Observe que substituimos

$$a.c.e - a.d.f - b.d.e - d.c.f \text{ pela expressão } a.(c.e - d.f) - b.(d.e + c.f),$$

uma vez que em $\mathbb{R}$ vale essa propriedade.

(iii) Sejam $z_1 = (a, b); z_2 = (c, d)$ e $z_3 = (e, f)$, provemos a distributividade à esquerda e a distributividade à direita respectivamente.

Temos que:

(a)

$$\begin{aligned}(z_1 \odot z_2) \oplus z_3 &= (a, b) \odot ((c, d) \oplus (e, f)) \\ &= (a, b) \odot (c + e, d + f) \\ &= (a.(c + e) - b.(d + f), a.(d + f) + b.(c + e)) \\ &= ((a.c - b.d) + (a.e - b.f), (a.d + b.c) + (a.f + b.e)) \\ &= (a.c - b.d, a.d + b.c) \oplus (a.e - b.f, a.f + b.e) \\ &= (z_1 \odot z_3) \oplus (z_2 \odot z_3).\end{aligned}$$

Logo,a operação $\odot$ é distributiva à esquerda.

(b) Usando o fato que $\odot$ é comutativa e o item (a) temos que,

$$\begin{aligned}z_1 \odot (z_2 \oplus z_3) &= (z_2 \oplus z_3) \odot z_1 \\ &= (z_2 \odot z_1) \oplus (z_3 \odot z_1) \\ &= (z_1 \odot z_2) \oplus (z_1 \odot z_3).\end{aligned}$$

Portano, a operação $\odot$ é distributiva à direita.

(iv) Finalmente, resta provar que $\mathbb{C}$ não possui divisores de zero.

Consideremos $z = (a, b)$ e $w = (c, d)$ tais que $z \odot w = (0, 0)$. Basta observar as equivalências a seguir.

$z \odot w = (0, 0) \Leftrightarrow (a, b) \odot (c, d) = (0, 0) \Leftrightarrow (a.c - b.d, a.d + b.c) = (0, 0)$

$\Leftrightarrow a.c - b.d = 0$ e $a.d + b.c = 0$.

Agora, façamos a análise sobre o número real "a"conforme ele seja igual a zero ou diferente de zero, respectivamente.

(i) Se $a = 0$, então $b.d = 0$ e $b.c = 0$. Para continuar a discussão, iremos separar em dois subcasos, conforme b seja igual a zero ou b diferente de zero.

(1) Caso $b = 0$, concluímos que z=(0,0).

(2) Caso $b \neq 0$, usaremos o fato que $\mathbb{R}$ é um Domínio de Integridade para concluirmos que $c = 0$ e $d = 0$, donde w=(0,0). Assim, se $a = 0$, então z=(0,0) ou w=(0,0).

(ii) Se $a \neq 0$, isolamos c na equação $a.c - b.d = 0$, obtendo $c = \dfrac{b.d}{a}$ e em seguida substituiremos na equação $a.d + b.c = 0$, conforme a seguir.

$$\begin{aligned} a.d + b.c &= 0 \\ a.d + b.\frac{b.d}{a} &= 0 \\ \frac{(a^2+b^2).d}{a} &= 0. \end{aligned}$$

Dessa última igualdade obtemos que $(a^2 + b^2).d = 0$. Por outro lado, usando o fato que $a^2+b^2 \neq 0$, juntamente com o fato de $\mathbb{R}$ ser um Domínio de Integridade, obtemos d=0. Observe, no entanto, que d=0 implica $c = \dfrac{b.0}{a} = 0$ e, portanto w=(0,0).

Desse modo, mostramos que se z=(a,b) e w=(c,d)são tais que $z \odot w = (0, 0)$, então z=(0,0) ou w=(0,0).Isso completa a prova das propriedades da operação $\odot$.

Com base nos argumentos anteriores, temos, por definição que $(\mathbb{C}, \oplus, \odot)$ é um Domínio de Integridade.

Exemplo 4.2.3. *Seja $\mathbb{K}$ um corpo, então o conjunto das matrizes de ordem n com coeficientes em $\mathbb{K}$ não é um domínio de integridade.*

De fato, consideremos as matrizes

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \text{ e } B = \begin{pmatrix} -2 & -2 \\ 1 & 1 \end{pmatrix}.$$

Observe que

$$A.B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

mesmo A e B sendo matrizes não nulas.

4.3. Atividade aplicada em sala

Lista de exercícios usados para discutir sobre a comutatividade e a lei do corte

INSTITUTO FEDERAL DE ALAGOAS: CAMPUS MARECHAL DEODORO
DISCIPLINA: MATEMÁTICA. CURSO: MEIO AMBIENTE
PROFESSOR: EDVAN HORÁCIO DOS SANTOS
ALUNO (A):..... N^0:.....
DATA:..../.... /..... TURMA:.....
LEI DO CORTE E COMUTATIVIDADE

Durante o estudo de Gases, em Química, apareceu a equação $\frac{P_2V_1}{10} = \frac{P_2V_0}{2}$. Em seguida o professor cortou P_2 e concluiu que necessariamente $V_1 = 5V_0$.

Alguns de vocês me perguntaram se podia fazer isso e o porquê. A resposta é sim, desde que $P_2 \neq 0$. Se $P_2 = 0$ não podemos concluir que necessariamente $V_1 = 5V_0$ uma vez que obtemos zero nos dois membros, independentemente dos valores de V_1 e V_0.

Tal fato ocorre porque os números reais é um domínio de integridade. Na verdade é mais do que isso. Ele é um corpo mas vamos discutir um pouco sobre o que é um domínio de integridade .

Um domínio de integridade é um conjunto tais que as operações de adição e multiplicação satisfazem às seguintes propriedades:

1. A adição é: comutativa, associativa tem elemento neutro (representado por 0), tem elemento simétrico.

2. A multiplicação é: comutativa, associativa tem elemento neutro.

3. Vale a distributividade: A(B+C)= AB+AC.

4. Vale a lei do corte: Se $A \neq 0$ e AB=AC então necessariamente B = C.

Um conjunto é chamado de **Anel Comutativo com Elemento Unidade** quando são válidas as 3 primeiras.

Houve outro exemplo envolvendo a lei do corte.

Em uma questão envolvendo a Lei de Snell-Descartes apareceu $\sqrt{3}.sen(r) = \frac{\sqrt{3}}{2}.1$.

Como $\sqrt{3} \neq 0$ e todos os "objetos"envolvidos são números reais então vale a lei do corte. Assim obtemos $sen(r) = \frac{1}{2}$ e portanto $r = 30^o$.

Para matrizes algumas regras são quebradas. A comutatividade e a lei do corte são algumas delas.

LEI DO CORTE

01)Considerando as matrizes a seguir,

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, B = \begin{pmatrix} -2 & -2 \\ 1 & 1 \end{pmatrix} \text{ e } C = \begin{pmatrix} -6 & -8 \\ 3 & 4 \end{pmatrix},$$

determine os produtos nos itens (a) e (b). Além disso, usando os resultados de (a) e (b), conclua o que está afirmado em (c).

(a) AB=

(b) AC=

(c) Note que $A \neq 0$ e apesar de AB=AC não é verdade que B=C. Portanto, não vale a lei do corte.

✠ **Observação 4.1.**

Então toda vez que alguém perguntar o seguinte: Se $A \neq 0$ e AB=AC vale necessariamente B=C? A resposta é: Depende de que conjunto estamos usando. Em termos mais precisos, depende do anel. No conjunto das funções reais também não vale a lei do corte, conforme veremos na questão 03. .

COMUTATIVIDADE

02)Sejam as matrizes

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \text{ e } B = \begin{pmatrix} -2 & -2 \\ 1 & 1 \end{pmatrix}$$

determine os produtos nos itens (a) e (b), (c). Além disso, usando os resultados de (a) e (b), conclua o que está afirmado em (c).

(a) AB=

(b) BA=

(c) Note que $AB \neq BA$ e portanto não vale a comutatividade para matrizes.

03)Considere as funções f, g e h definidas conforme a seguir;

$$f(x) = \begin{cases} 0, & \text{se} \quad x \neq 3 \\ 1, & \text{se} \quad x = 3 \end{cases}$$

$$g(x) = \begin{cases} 0, & \text{se} \quad x \neq 5 \\ 1, & \text{se} \quad x = 5 \end{cases}$$

$$h(x) = \begin{cases} 0, & \text{se} \quad x \neq 8 \\ 1, & \text{se} \quad x = 8 \end{cases}$$

Mostre que $f(x)g(x) = f(x)h(x) \equiv 0$ mas não é verdade que $g(x) \equiv h(x)$, uma vez que elas têm imagens diferentes em $x = 5$ e $x = 3$.

Portanto, conclua que não vale a lei do corte para o conjunto das funções reais.

Vários alunos ficaram surpresos com o fato de nas matrizes não serem validas algumas propriedades usuais tais como a comutatividade. No caso dos números reais, devido ao conhecimento adquirido na vivências das séries anteriores, usamos esse fato de forma bastante natural. Usamos a comutatividade para justificar por exemplo que 40% de 30 equivale a 30% de 40. De fato,temos que

$$\begin{aligned} 40\%\, de\, 30 &= \frac{40}{100}.30 \\ &= \frac{40.30}{100} \\ &= \frac{30.40}{100} \\ &= 30\%\, de\, 40 \end{aligned}$$

porque 30.40=40.30. Argumentando da mesma forma temos que, a% de b equivale a b% de a, uma vez que vale a comutatividade de números reais, isto é $a.b = b.a\ \forall a,\ b \in \mathbb{R}$.

Já a lei do corte foi uma novidade para todos. Eles perceberam que dependendo dos objetos envolvidos podemos garantir a validade de tal propriedade ou fazer restrições para que valha. Além disso, se surpreenderam ao verificar que para funções e matrizes não valem em geral. Alguns deles inclusive perguntaram se no caso das matrizes há algum caso que poderia cortar. Tal fato evidencia a possibilidade de num futuro estender essa discussão para corpos uma vez que num corpo, se $ab = ac$ e $a \neq 0$ então $b = c$. No caso das matrizes temos o seguinte: A é invertível e AB=AC então necessariamente que B=C.

A seguir, temos a foto da anotação de um dos alunos quando a atividade foi aplicada.

Figura da atividade sobre domínio de integridade.

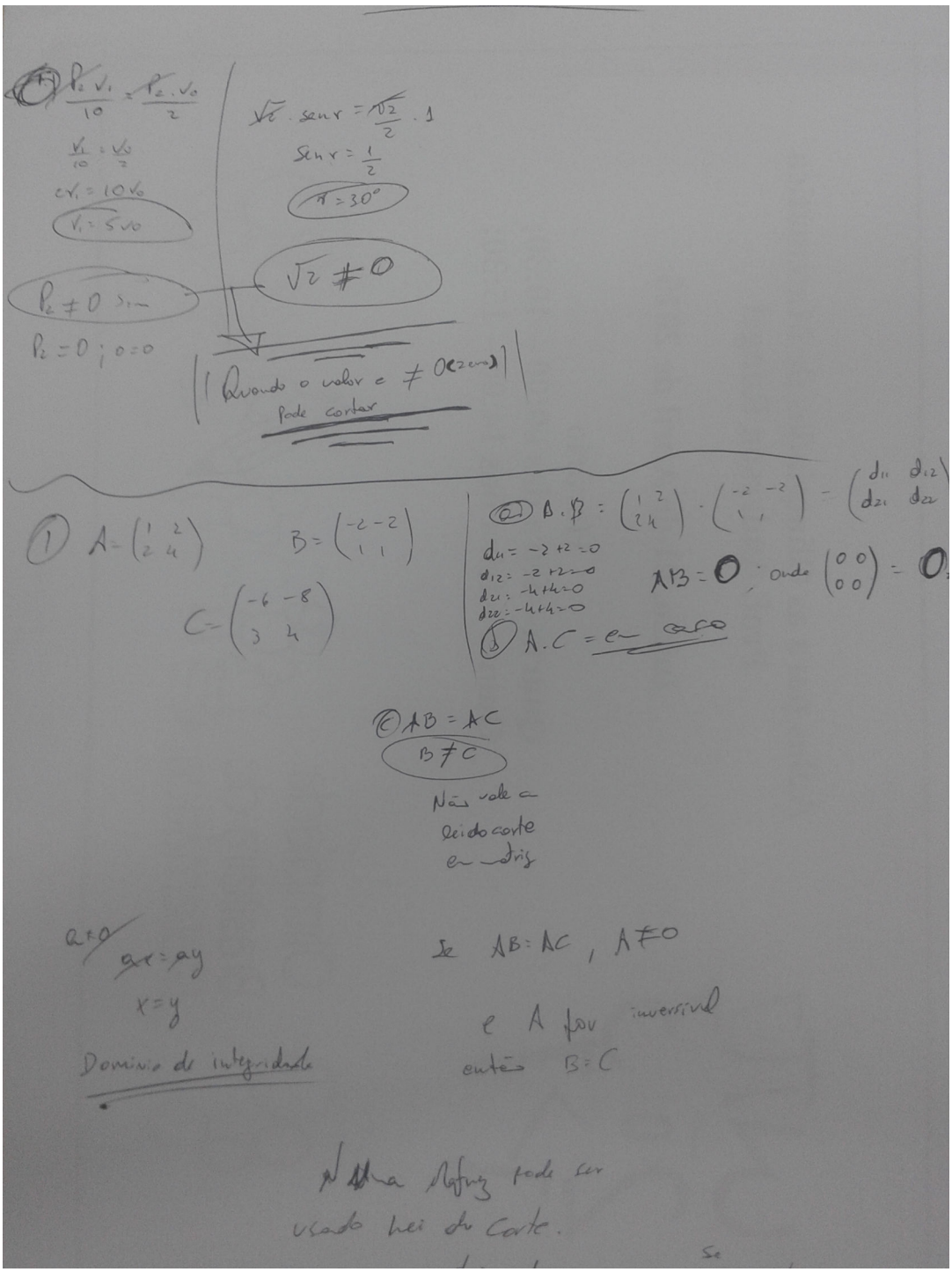

Figura 4.1: Fonte: Autor, 2014.

Note que o aluno escreveu errada uma equação pois em lugar de $\sqrt{2}.sen(r) = \frac{\sqrt{2}}{2}.1$, era na verdade $\sqrt{3}.sen(r) = \frac{\sqrt{3}}{2}.1$, mas todo o restante dos cálculos estão corretos.

4.4. Complemento sobre os exemplos usados em sala

O exercício 3 da lista aplicada em sala é muito interessante pois nos dar uma maneira de construir infinitos exemplos onde a "lei do corte"não é válida. Além disso, dele concluiremos que existem infinitos divisores de zero. Para cada número real "a"considere a função

$$f_a(x) = \begin{cases} 0, & \text{se} \quad x \neq a \\ 1, & \text{se} \quad x = a \end{cases} .$$

Observe que esta família de funções, além de serem divisores de zero também são soluções da equação $x^2 = x$ no conjunto das funções reais. De fato, a primeira afirmação é simples de ser verificada, bastando para isso proceder conforme o exemplo 03 da lista, usando f_a ef_b com $a \neq b$. Vamos à segunda afirmação. Basta ver que:

$$f_a(x).f_a(x) = \begin{cases} 0.0 = 0, & \text{se} \quad x \neq a \\ 1.1 = 1, & \text{se} \quad x = a \end{cases} .$$

ou seja, $f_a(x).f_a(x) = f_a(x)$.

Note que a equação $x^2 = x$ possui infinitas soluções no conjunto das funções reais como vimos anteriormente. Isso decorre pelo fato do conjunto das funções reais não ser um Domínio de Integridade. Observe que esse fato merece ser destacado, pois como sabemos toda equação polinomial de grau n sobre $\mathbb{C}$ possui exatamente n soluções em $\mathbb{C}$. Como o conjunto das funções reais não é um Domínio de Integridade, vimos anteriormente que essa afirmação do número finito de soluções de uma equação polinomial não é verdadeiro. Para o conjunto das matrizes de ordem 2 também mostraremos a seguir que existem infinitas soluções da equação $x^2 = x$.

De fato, seja

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

com a, b, c e d números reais. Queremos saber para quais valores reais de a, b, c e d se verifica a equação $X^2 = X$, onde X é a matriz

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Nesse caso, basta resolver a igualdade

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

donde

$$\begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

.

Logo, obtemos as seguintes equações:

(i) $a^2 + bc = a$

(ii) $ab + bd = b$

(iii) $ac + cd = c$

(iv) $bc + d^2 = d$

Observe na segunda equação que o número b aparece nos dois membros e só poderemos cortar ele se $b \neq 0$. Portanto, vamos analisar dois casos: $b = 0$ e $b \neq 0$.

- Se $b = 0$, obtemos que $a^2 = a$ e $d^2 = d$, donde $a = 0$ ou $a = 1$ e da mesma forma, $d = 0$ ou $d = 1$. Com esses valores de a e d teremos 4 possíveis opções: $a = 0$ e $d = 0$; $a = 0$ e $d = 1$; $a = 1$ e $d = 0$; $a = 1$ e $d = 1$. Tanto no primeiro quanto no quarto caso o valor de c é zero. No segundo e terceiro caso o número c pode assumir qualquer valor real. Portanto, se $b = 0$ teremos as seguintes matrizes:

  $$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} \text{ e } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

  que são soluções da equação matricial $X^2 = X$.

- Se $b \neq 0$ obtemos que $a + d = 1$ pois vale cortar b na segunda equação.

  Além disso, usando a primeira equação, obtemos os seguintes valores para o número real a: $a = \frac{1\pm\sqrt{1-4bc}}{2}$, com $bc \leqslant \frac{1}{4}$. Assim, obtemos os seguintes valores para os números reais a e d :

  (i) $a = \frac{1+\sqrt{1-4bc}}{2}$ e $d = \frac{1-\sqrt{1-4bc}}{2}$ ou

  (ii) $d = \frac{1+\sqrt{1-4bc}}{2}$ e $a = \frac{1-\sqrt{1-4bc}}{2}$,

com $bc \leqslant \frac{1}{4}$.

Portanto, se $b \neq 0$, também exibimos infinitas matrizes de ordem 2 tal que $X^2 = X$.

Reunindo esses resultados obtidos obtemos infinitas matrizes da forma $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ que são soluções da equação $X^2 = X$..

Desse modo, justificamos a afirmação de que no conjunto das matrizes de ordem 2 há infinitas soluções para a equação $x^2 = x$. Agora, iremos discutir um pouco mais sobre os exemplos usados na lista de exercícios aplicada em sala. A seguir, descreveremos uma forma de construir matrizes quadradas de ordem 2 em que naõ vale a lei do corte.

Para construir exemplos de matrizes quadradas de ordem 2 que não vale a lei do corte, basta obter matrizes de ordem 2 cujo determinante é diferente de zero e além disso

$$AX = 0$$

.

Sob essa ótica, dadas as matrizes

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \text{ e } X = \begin{pmatrix} x & y \\ z & t \end{pmatrix},$$

determinemos reais x, y, z e t tais que

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Essa equação matricial nos fornece $x = -2z$ e, $y = -2t$. Portanto, temos infinitas matrizes da forma

$$\begin{pmatrix} -2z & -2t \\ z & t \end{pmatrix},$$

que são soluções da equação matricial AX=0. Logo, existem matrizes de ordem 2, $X \neq Y$ tais que AX=AY=0 e como consequência não vale a lei do corte.

4.5. Algumas situações que usam o fato de $\mathbb{R}$ ser um Domínio de Integridade

Mostraremos a seguir duas situações que usam o fato de $\mathbb{R}$ ser um Domínio de Integridade. São dois exemplos que aparecem nas turmas a partir do nono ano do Ensino

Fundamental.

1. Quando trabalho com radicais nos deparamos com a seguinte propriedade

$$a \geqslant 0 \,\text{e}\, b \geqslant 0, \text{então } \sqrt{a.b} = \sqrt{a}.\sqrt{b}.$$

Proponho como atividade verificar essa afirmação atribuíndo valores para a e b. Em seguida investigamos, se existe uma propriedade análoga para a soma, ou seja, sendo

$$a \geqslant 0 \,\text{e}\, b \geqslant 0, \text{então } \sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$

Procedendo como anteriormente, eles verificam que em geral não vale. Poucos livros citam esse fato mas em [2] o autor chama atenção que em geral não vale $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ bem como $\sqrt{a-b} = \sqrt{a} - \sqrt{b}$.

Em seguida proponho que pesquisem para quais condições sobre a e b se verifiquem $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ e $\sqrt{a-b} = \sqrt{a} - \sqrt{b}$, com $a \geqslant 0$, $b \geqslant 0$ e no segundo caso acrescento a hipótese de $a \geqslant b$. O interessante é que eles conseguem exibir exemplos que vale $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ substituindo $a = 0$ ou $b = 0$ mas não conseguem mostrar que só vale para esses casos. Uma solução completa requer que se resolva um tipo de equação que eles estudam com o nome de equações irracionais mas pouquíssimos deles se lembram como se resolve. Após vencer essa barreira da equação irracional aparece outra, que é $ab = 0$ e poucos completam os cálculos. Aqui vamos fazer os detalhes desses para a soma e deixar para que o leitor faça o caso da diferença.

Mostremos que $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ se, e somente se, $a = 0$ ou $b = 0$.

De fato, temos que:

$\sqrt{a} + \sqrt{b} = \sqrt{a+b} \Leftrightarrow a + b + 2\sqrt{a.b} = a + b \Leftrightarrow a.b = 0 \Leftrightarrow a = 0 \,ou\, b = 0.$

No caso de $\sqrt{a-b} = \sqrt{a} - \sqrt{b}$ temos o seguinte : Sendo $a \geqslant b \geqslant 0$ então $\sqrt{a-b} = \sqrt{a} - \sqrt{b}$ apenas quando $b = 0$ ou $a = b$. A prova é semelhante.

2. A resolução de equações do segundo grau pode ser feita por uma fatoração do primeiro membro e no segundo membro deixamos apenas o zero. Particularmente, nas equações incompletas isso fica muito claro.

Por exemplo, a equação do segundo grau incompleta $x^2 = 25$, transformamos em $x^2 - 25 = 0$ e por conseguinte $(x-5)(x+5) = 0$. Como $\mathbb{R}$ é um Domínio de Integridade então $x - 5 = 0 \,\text{ou}\, x + 5 = 0$. Assim $x = 5$ ou $x = -5$.

É claro que em alguns casos precisamos usar que $\mathbb{R}$ é um corpo mas nossa ênfase aqui é o fato dele ser um Domínio de Integridade

5. CONCLUSÃO

Esta dissertação teve como objetivo principal mostrar que é possível discutir no ensino médio sobre alguns temas que normalmente são tratados nos cursos de graduação em matemática, mas que refletem sobremaneira na compreensão do modo como a matemática que é trabalhada no ensino médio.

Cada capítulo tratou de um tema. No primeiro, os alunos compreenderam o que significa existência e unicidade da divisão euclidiana. Quando discutimos em sala, sobre a condição em relação ao resto, concluimos que ela é importante para determinar a unicidade do quociente e o do resto. Vimos também, como corolário, o porquê colocamos zero no quociente quando o módulo do dividendo é menor do que módulo do divisor. Esse fato de colocar zero no quociente causou muita dúvida entre os alunos, mas usando as condições euclidianas a explicação se tornou relativamente simples. Já no capítulo 2, os alunos resolveram problemas cuja essência é a definição de congruência. Isso mostra que o estudo das congruências podem ser feito no ensino médio. Finalmente, no capítulo 3 tratamos sobre domínio de integridade. A atividade proposta permitiu aos alunos compreenderem que, dependendo dos objetos envolvidos, algumas propriedades podem não serem válidas. Compreenderam que nas matrizes e nas funções reais não vale a lei do corte. É claro que uma formalização completa desses temas não cabem nesse momento, mas vimos que é possivel discutir com clareza sobre cada um dos temas abordados. Os exemplos usados para discutir os temas de cada capítulo são próprios da educação básica. Nessa dissertação, demos um enfoque chamando atenção para vários aspectos que em geral não são discutidos no ensino médio.

Em cada capítulo, foram produzidas e aplicadas em sala atividades relativas ao tema em questão. Durante a aplicação das atividades foi constatado que os alunos tiveram grau de compreensão satisfatório, mostrando domínio quanto ao que se pretendia em cada uma. Ao mesmo tempo eles puderam comparar a experiência vivenciada nas séries anteriores com o modo que nós abordamos os temas. Assim, foram construídos novos significados para aqueles que eles já dispunham e também puderam perceber que a Matemática tem suas próprias especificidades. Essa experiência contribuiu para ampliar o conhecimento

dos alunos bem como dirimir dúvidas em relação a vários conteúdos.

Essa forma de abordagem está em consonância com os próprios Parâmetros Curriculares Nacionais do Ensino Médio, uma vez que nele é contemplada a possibilidade do estudo da Matemática levando em conta suas características estruturais específicas. Assim, espero que essa dissertação contribua para nortear o trabalho do professor em sala de aula na construção do conhecimento matemático trabalhado no ensino médio.

Portanto, é possivel discutir, mesmo no ensino médio, sobre vários aspectos que em geral são tratados em cursos de graduação em Matemática. É claro que procuramos exemplos do quotidiano dos alunos que permitissem isso de forma significativa. Contudo, cabe ao professor, juntamente com sua turma, decidir o melhor momento e a abordagem que atenda ao objetivo proposto.

6. PERSPECTIVAS FUTURAS

Em breve pretendo ingressar num doutorado para aprimorar cada vez mais minha prática docente e vislumbrar novos horizontes, uma vez que, todo profissional deve está sempre em busca de novidades para poder oferecer novos olhares e novas possibilidades, com o objetivo de melhorar sua prática.

Portanto, fazer um doutorado é um projeto que em breve pretendo concretizar.

REFERÊNCIAS

[1] BRASIL. Ministério da Educação, Parâmetros Curriculares Nacionais: Matemática: Ensino Médio. Brasília: MEC/SEF, 1998.

[2] DANTE, Luiz Roberto.**Matemática.** 1 ed. , 2^a imp. São Paulo: Ática, 2012.326p.(Projeto Teláres. Matemática, v. 4)

[3] FERREIRA, Jamil. **A Construção dos Números.** 1 ed. Rio de Janeiro: SBM, 2010. 133p.(Coleção Textos Universitários, 9)

[4] GONÇALVES, Adilson. **Introdução à Álgebra.**5 ed., 2^a imp. Rio de Janeiro: Associação Instituto de Matemática Pura e Aplicada, 2003. 194p.(Projeto Euclides).

[5] IEZZI, Gelson. **Fundamentos de Matemática Elementar v. 6.** Complexos, polinômios e equações. 6 ed. São Paulo: Atual Editora, 1993. 241p.

[6] IEZZI, Gelson; HAZZAN, Samuel Hazzan. **Fundamentos de Matemática Elementar v. 4.** Matrizes, Determinantes e Sistemas Lineares. 6^a ed. São Paulo: Atual Editora, 1993. 231p.

[7] RAMALHO JÚNIOR, Francisco et al. **Os Fundamentos da Física, v. 2.** Termologia, óptica e ondas. 6 ed. São Paulo: Editora Moderna, 1993. 528 p.

[8] LIMA, Elon Lages. **Meu Professor de Matemática e outras histórias.** 5 ed. Rio de Janeiro: SBM, 2006.206p.(Coleção do Professor de Matemática).

[9] HEFEZ, Abramo. **Álgebra volume 1.** 2 ed. Rio de Janeiro: SBM ,1997. 226p.(Coleção Matemática Universitária).

[10] OLIVEIRA, Krerley Irraciel Martins de e Adán José Corcho Fernandez. **Iniciação à Matemática:** um curso com problemas e soluções. 1 ed. Rio de Janeiro: SBM, 2010. 283p.(Coleção Olimpíada de Matemática, 4).

[11] PAIVA, Manoel. **Matemática volume 1.** 2 ed. São Paulo: Editora Moderna, 2009. 256p.

[12] ROQUE, Tatiana; CARVALHO, João Bosco Pitombeira de.**Tópicos de História da Matemática:** 1 ed. Rio de Janeiro: SBM, 2012. 467(Coleção PROFMAT, 03).

[13] SANTOS, Paulo Sérgio de Almeida. **Congruência e equações diofantinas: uma proposta para o ensino básico .** 2013. 113 f. Dissertação de Mestrado (Mestrado Profissional em Matemática em Rede Nacional)- Instituto de Matemática, Programa de Pós-Graduação de Mestrado Profissional em Matemática em Rede Nacional, Universidade Federal de Alagoas, Maceió, 2013.

7. ANEXO A

Lista de exercícios usada para trabalhar a Divisão Euclidiana com os alunos.

INSTITUTO FEDERAL DE ALAGOAS: CAMPUS MARECHAL DEODORO
DISCIPLINA: MATEMÁTICA. CURSO: MEIO AMBIENTE
PROFESSOR: EDVAN HORÁCIO DOS SANTOS
ALUNO (A):..... N^0:.....
DATA:..../.... /..... TURMA:.....
CURSO DE NIVELAMENTO
DIVISÃO EUCLIDIANA: A EXISTÊNCIA E UNICIDADE DO QUOCIENTE E DO RESTO NA DIVISÃO

O Teorema da Divisão Euclidiana garante o seguinte. Dados dois números inteiros a e b com $b \neq 0$ existem únicos pares de inteiros q e r tais que a=bq+r e $0 \leqslant r < |b|$.

Há uma versão deste teorema para os naturais. Dados dois naturais a e b com $b \neq 0$, existem únicos naturais q e r tais que $a = bq + r\, e\, 0 \leqslant r < b$.

Lembramos que representamos os naturais por $\mathbb{N} = \{0, 1, 2, 3, ...\}$. Já os inteiros é representado por $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$, isto é, os inteiros envolvem os números positivos, negativos e o zero. Já os naturais apenas os positivos e o zero.

É muito comum trabalharmos apenas com os números naturais mas em alguns casos a discussão fica mais proveitosa quando ampliamos para os inteiros. Vamos compreender o significado da existência e unicidade do quociente e do resto na Divisão Euclidiana. Será discutido o seguinte problema em relação à divisão: Sob que condições temos única solução? Poderão existir outras soluções?

Vamos aos exemplos resolvidos (ER).

ER1)Achar o quociente e o resto da divisão de a por b nos seguintes casos.

(a) a=17 e b=2

(b) a=19 e b=5

ER2)Se 5 pássaros pousarem em cada árvore então sobrarão 2 pássaros. Já se 3 pássaros pousarem em cada árvore então sobrarão 10 pássaros. Determine quantos pássaros e quantas árvores são.

1ª solução : Testando valores, representando as árvores como caixas para colocar os pássaros.

Situação A: ⌴ ⌴ ⌴ ⌴

Situação B: ⌴ ⌴ ⌴ ⌴

2ª solução : Exibindo um sistema de equações.

ER3)Se 3 pássaros pousarem em cada árvore então sobrarão 2 pássaros. Mas se 5 pássaros tentarem pousar em cada árvore então 2 árvores ficarão vazias e as demais com 5 pássaros cada uma . Determine quantos pássaros e quantas árvores são .

1ª solução :Testando valores, representando as árvores como caixas para colocar os pássaros.

Situação A:⌴ ⌴ ⌴ ⌴ ⌴ ⌴

Situação B: ⌴ ⌴ ⌴ ⌴ ⌴ ⌴

2ª solução: Exibindo um sistema de equações.

ER4)Vamos discutir o significado da Divisão Euclidiana de 23 por 6 e o Zero no Quociente quando for analisar o quociente da divisão de 2 por 6.

Para compreendermos o que está sendo pedido, iremos resolver em 2 partes:

1. Significado da Divisão Euclidiana de 23 por 6

   Quanto é o quociente e o resto da divisão de 23 por 6?

   Se no quociente escrevermos 2 então o resto será 11.

   Neste caso, dizemos que o quociente é pouco pois 11 não é menor do que 6. Na verdade, preferimos dizer que este resto 11 a condição de ser menor do que 6.

   Sabemos que o quociente é 3 e o resto é 5, pois $23 = 6.3+5$ e $0 \leqslant 5 < 6$.

   Se no quociente for colocado 2 o resto é 11 e apesar de $23 = 6.2 +11$ não é verdade que $0 \leqslant 11 < 6$.

   Se o quociente for 1 o resto é 17 e apesar de $23 = 6.1+17$ não é verdade que $0 \leqslant 17 < 6$.

   Se o quociente for 0 o resto é 23 e apesar de $23 = 6.0+23$ não é verdade que $0 \leqslant 23 < 6$.

   Note que os "restos"são positivos mas vários deles não são menores do que 6 .

   Se no quociente for colocado 4 o resto é -1 e apesar de $23 = 6.4 +(-1)$ não é verdade que $0 \leqslant -1 < 6$.

Já se o quociente for 5 o resto é -7 e apesar de $23 = 6.5 + (-7)$ não é verdade que $0 \leqslant -7 < 6$.

Nestes dois últimos casos os "restos são negativos". Você acha isso impossível? Pois será mostrada uma situação bem simples.

Nós aqui no Brasil enfrentamos fila pra tudo. Num posto de saúde tinham 23 pessoas e 6 bancos de cimento com nenhum conforto.

Se for acomodando 4 pessoas no primeiro banco, 4 no segundo, etc então o último banco ficará com apenas 3, pois faltará uma pessoa para completar as quatro pessoas. Isso é o caso "Se o quociente for 4 o resto é -1 e apesar de $23 = 6.4 + (-1)$ não é verdade que $0 \leqslant -1 < 6$".

Analogamente de 5 em 5 "Se o quociente for 5 o resto é -7 e apesar de $23 = 6.5 + (-7)$ não vale que $0 \leqslant -7 < 6$". Neste caso um banco ficará vazio e outro ficará com apenas 3 pessoas .

O modo que somos habituados fazer, conforme a divisão, consiste em colocar 3 pessoas em cada banco e sobrarão 3 pessoas.

Fazer a Divisão Euclidiana de 23 por 6 ou dividir 23 por 6 significa determinar números inteiros q e r tais que:

(i) $23=6q+r$

(ii) $0 \leqslant r < 6$.

O que fizemos na discussão anterior foi compreender que só existe um par de inteiros q e r que satisfazem a essas duas condições. Essa conclusão sobre existência e unicidade é garantido por um resutado conhecido como Divisão Euclidiana. Essa é a divisão usual que aprendemos desde as séries iniciais. Se não forem colocadas as condições então não poderemos saber qual quociente e qual resto está sendo pedido. Portanto, podemos ver como um problema em que só queremos que exista uma solução, no entanto, para que isso ocorra deveremos acrescentar condições.

2. Vamos agora ao Zero no Quociente. Conforme vimos anteriormente, há somente um par de números inteiros q e r tai que $2=6q+r$, com $0 \leqslant r < 6$. Nesse caso específico significa que o quociente e o resto são respectivamente, $q=0$ e $r=2$.

   Com isso explicamos o zero no quociente quando dividimos 2 por 6. O quociente é zero e o resto é 2. Do contrário não atenderemos às condições Euclidianas. Você já tinha pensado nisso?

Com base no que vimos, compreendemos o que significa existência e unicidade no tocante à Divisão Euclidiana e como consequência dela compreendemos porque colocamos zero no quociente quando estamos dividindo um número natural a pelo numero natural $b \neq 0$, com a < b.

✠ **Observação 7.1.**

No exercício EP4) fazemos uma interpretação, via Divisão Euclidiana, do porquê nao dividir por zero.

ER5)Na divisão euclidiana, quando b =2 o resto r é tal que $0 \leqslant r < 2$. Assim, os possíveis valores de r são: r = 0 ou r = 1. Quando r = 0 o número a se escreve da forma a= 2q+0 = 2q ; Quando r = 1 então ele se escreve da forma a = 2q+1. Logo, todo número inteiro é da forma 2q ou 2q+1. No primeiro caso ele é dito NÚMERO PAR e no segundo é dito número ÍMPAR. Com base nesses argumentos, faça o que se pede:

(i) O número 0 (zero) é par ou ímpar?

(ii) E o 45 é par ou ímpar? E o - 67?

(iii) Na divisão euclidiana, quando b = 3, quais os possíveis valores para o resto?

(iv) Na divisão euclidiana, quando b = 4, quais os possíveis valores do resto?

Vejamos os exemplos propostos (EP).

EP1)Determine o quociente e o resto da divisão de a por b nos casos:

(a) a=18 e b=4

(a) a= 2 e b=5

(a) a=13 e b= -2

(a) a=8 e b=2014.

EP2)Em um posto de saúde alguns moradores esperam na fila. Como é muito cansativo esperar em pé, então eles tentam se acomodarem em alguns bancos. Se 5 pessoas se sentarem em cada banco então 5 pessoas ainda ficarão em pé mas se sentarem 6 em cada banco ocorre o seguinte. Um dos bancos ficam com 4 pessoas e os demais com 6. Quantos bancos e quantas pessoas estão na fila?

EP3)Se for dividir 6 por 20, qual o quociente e qual o resto? E de modo geral, ao dividir a por b, com a < b então o quociente é zero e o resto obtido é o próprio a.

EP4)As pessoas dizem que não existe divisão por zero, mas podemos dar uma interpretação interessante usando a "Divisão Euclidiana". Quando b=0, analise cada um dos seguintes itens a seguir:

(a) Se $a \neq 0$ o que ocorre?

(b) Se a=0 o que ocorre?

(c) Se a=0 e mudamos a condição $0 \leqslant r < b$ para $0 \leqslant r \leqslant b$ o que ocorre?

EP5)Na divisão euclidiana, quando b=6, quais os possíveis valores do resto?

EP6)Na divisão euclidiana, quando b=7, quais os possíveis valores do resto?

EP7)Quando o ano não é bissexto ele tem 365 dias. Uma semana tem 7 dias. Se um ano que não é bissexto e começar numa terça feira o ano seguinte começará em que dia da semana?

Essa lista de exercícios sobre divisão euclidiana foi aplicada com 20 alunos. Eles relataram que nenhum professor jamais discutiu sobre as condições da divisão euclidiana. Quinze relataram que seus professores diziam estar errada a divisão quando o resto era maior do que o divisior e os demais disseram que, segundo seus professores, a divisão estava incompleta. Além disso, a divisão com resto negativo jamais foi citada.

Os alunos acharam bastante interessante em ver que podemos ter mais de uma forma de dividir e que "a divisão"se refere a um problema cujas hipótese conduz a solução única.

Revelei a eles que, um resultado análogo a esse sobre divisão eu vi pela primeira vez em [5] quando estava no terceiro ano do Ensino Médio e que na minha graduação, quando fazia a disciplina de Álgebra Abstrata, rapidamente fiz a conexão e também foi desvelado o zero no quociente.

Em [4] isso é demonstrado no contexto dos naturais e no contexto dos polinômios. Já em [5] é feito no contexto dos polinômios mas ambos analisam casos imediatos, um dos quais é o zero no quociente.

As figuras a seguir mostram as anotações feita por dois alunos quando esse material foi aplicado.

Primeira figura da atividade sobre divisão

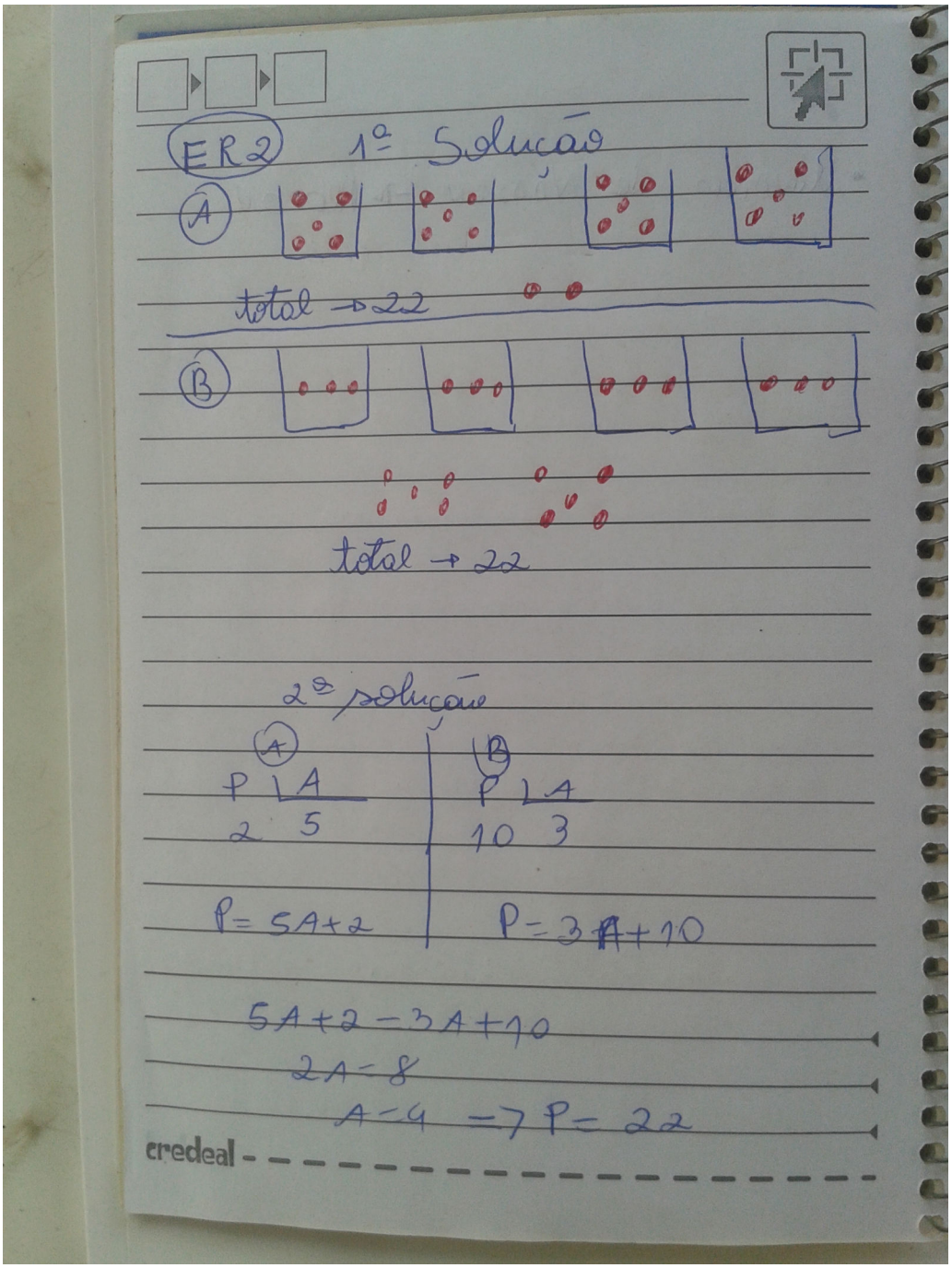

Figura 7.1: Fonte: Autor, 2014.

Segunda figura da atividade sobre divisão

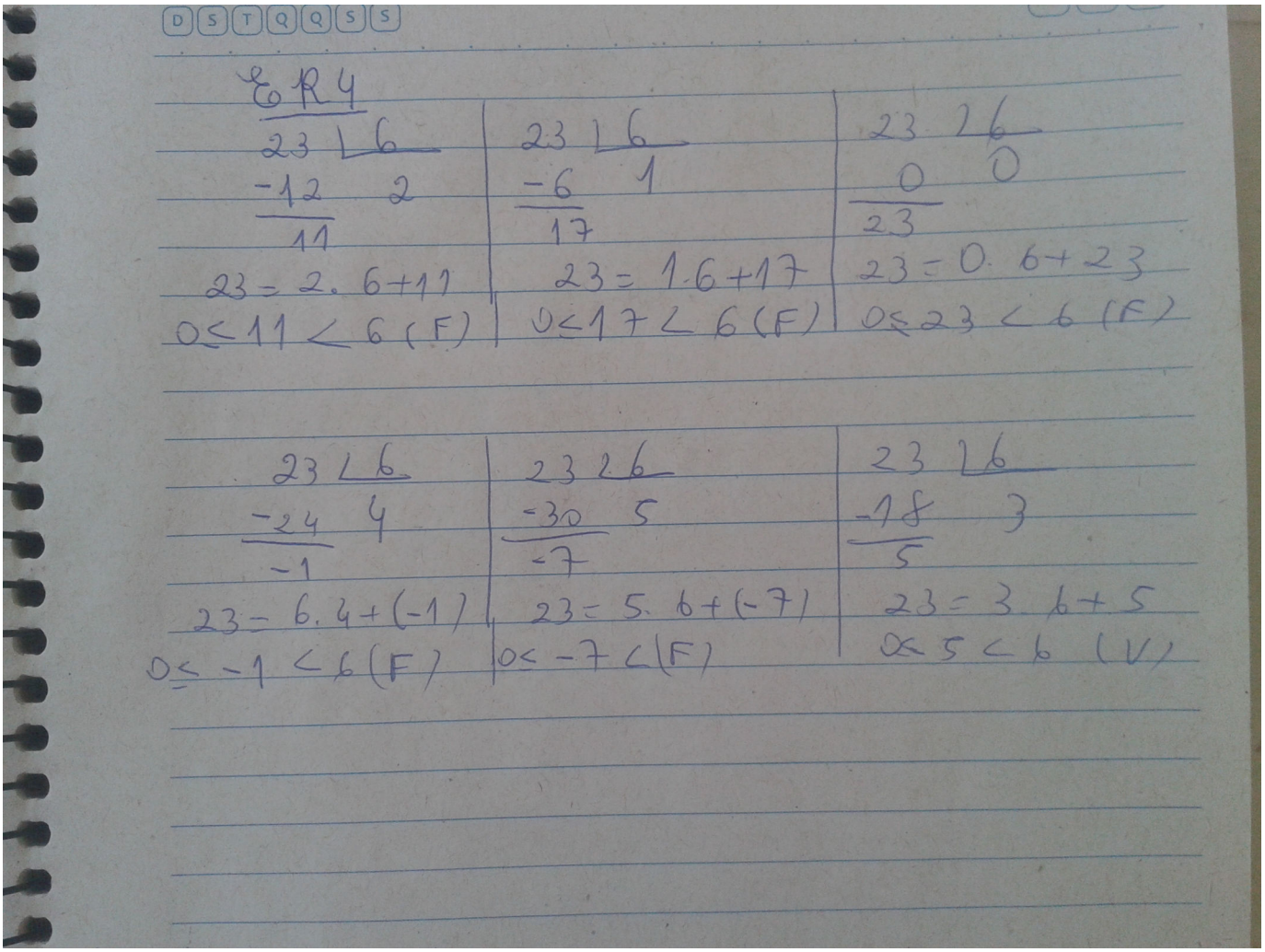

Figura 7.2: Fonte: Autor, 2014.