UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO AILTON ALCANTARA

TÓPICOS DE ARITMÉTICA: UMA PROPOSTA PARA A EDUCAÇÃO BÁSICA

JUAZEIRO DO NORTE
2014

FRANCISCO AILTON ALCANTARA

TÓPICOS DE ARITMÉTICA: UMA PROPOSTA PARA A EDUCAÇÃO BÁSICA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requesito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Flávio França Cruz

JUAZEIRO DO NORTE
2014

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

A319t Alcântara, Francisco Ailton
Tópicos de aritmética : uma proposta para a educação básica / Francisco Ailton Alcântara. – 2014.
100 f. : il., enc.; 31 cm

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Juazeiro do Norte, 2014.
Área de Concentração: Ensino de Matemática.
Orientação: Prof. Dr. Flávio França Cruz.

1. Aritmética. 2. Números primos. 3. Números inteiros. I. Título.

CDD 372.72

FRANCISCO AÍLTON ALCÂNTARA

TÓPICOS DE ARITMÉTICA: UMA PROPOSTA PARA A EDUCAÇÃO BÁSICA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: 20 / 05 / 2014.

BANCA EXAMINADORA

Prof. Dr. Flávio França Cruz (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Plácido Francisco de Assis Andrade
Universidade Federal do Ceará (UFC)

Prof. Dr. Ricardo Rodrigues de Carvalho
Universidade Regional do Cariri (URCA)

AGRADECIMENTOS

A Deus que me permitiu perseverar durante dois anos de curso e concluir mais essa tarefa.

Aos meus pais José Jocildo de Alcantara e Maria de Lourdes da Silva Alcantara que, na medida de suas possibilidades, lutaram para dar a melhor educação possível aos seus filhos.

Ao Professor Flávio França Cruz pela paciência e tempo disponibilizado à orientação que tanto contribuiu para confecção desse trabalho.

À minha namorada Eliete de Castro pela paciência e companheirismo nos momentos de angústia, aflição e estresse oriundos desses dois anos de mestrado.

Aos meus alunos que, por força da lei, não posso citar seus nomes nesse trabalho e que, apesar do cansaço, foram muito prestativos ao assistir as aulas de Aritmética durante o contra turno de estudos.

A todos os meus colegas e professores do PROFMAT que no decorrer desses dois anos me ajudaram a obter êxito no aprendizado das disciplinas, bem como em todas as avaliações aplicadas.

RESUMO

Este trabalho apresenta Tópicos de Aritmética, relacionados com o estudo da divisão, para aplicação em sala de aula no Ensino Médio, cujo o propósito é buscar o aprofundamento dos conhecimentos de aritmética que os alunos adquirem no Ensino Fundamental. Iniciamos com a abordagem das principais propriedades dos divisores, o algoritmo da divisão e o lema dos restos. Em seguida, estudamos os números primos com especial atenção ao Teorema Fundamental da Aritmética, de importância capital na obtenção de muitos resultados importantes nesse texto. Mais adiante, são apresentadas as definições de máximo divisor comum e mínimo múltiplo comum bem como as caracterizações, propriedades e a interpretação geométrica. Como proposta de continuidade aos estudos sobre divisão no Ensino Médio, apresentamos um estudo elementar sobre as congruências módulo m e sua aplicação na demonstração dos critérios de divisibilidade. Por fim, expomos um relatório de aplicação dos tópicos desse trabalho em sala de aula.

Palavras-chave: Aritmética. Ensino. Divisão.

ABSTRACT

This paper presents arithmetic topics related to the study of the division, for use in the high school classroom, whose purpose is to seek further knowledge of arithmetic that the students learn in elementary school. We begin with the approach of the main properties of divisors, the division algorithm and the motto of the remains. Then we study the prime numbers with special attention to the fundamental theorem of arithmetic, of paramount importance in achieving many important results in this text. Further down, the definitions of greatest common divisor and least common multiple and the characterizations, properties and geometric interpretation. As a proposal for continuing the studies of division in high school, we present an elementary study about the congruence module m and its application in demonstrating of the criteria for divisibility. Finally, we expose an implementation report of the topics of this paper in the classroom.

Keywords: Arithmetic. Education. Division.

SUMÁRIO

1 INTRODUÇÃO

O ensino da Aritmética, em especial o ensino das operações elementares e suas propriedades, iniciado no Ensino Fundamental é essencial para o entendimento dos assuntos de Matemática ensinados em séries posteriores. Dentre as operações aritméticas básicas, a mais difícil para a compreensão dos alunos é sem dúvida a divisão, pois o seu ensino exige o domínio das demais operações elementares bem como domínio de ideias associadas à própria divisão. Com o intuito de ajudar a sanar esse obstáculo, foi preparado esse trabalho, que consiste em um manual de Aritmética Básica com especial atenção ao estudo da divisão e suas propriedades que pode ser utilizado pelo professor para enriquecer sua prática pedagógica em sala de aula.

No atual sistema, o ensino da Aritmética é iniciado e exaurido ainda no 3º ciclo do Ensino Fundamental. Nessa etapa do ensino, a Aritmética é ensinada apenas visando as técnicas operacionais. Esse sistema de ensino é justificado pela necessidade de melhorar as habilidades de cálculos dos alunos nesse ciclo. Porém, habilidades de cálculo e técnicas operacionais sem o conhecimento teórico e conceitual é apenas condicionamento e não aprendizagem. Nessa proposta de ensino a prioridade é o conhecimento conceitual ou seja o rigor das definições, as demonstrações formais e aplicações que exigem argúcia dos estudantes.

O público alvo desse trabalho de conclusão de curso são os professores das escolas de Ensino Fundamental e Médio que querem se aperfeiçoar ou melhorar sua prática pedagógica em sala de aula, bem como turmas de alunos do Ensino Médio do ensino convencional, ou grupos de alunos mais talentosos que desejam aprofundar seus conhecimentos de Aritmética.

Este trabalho apresenta de forma rigorosa a definição e propriedades do divisor de um números inteiro trabalhando suas aplicações. O algoritmo da divisão é demonstrado e aplicado em situações-problema que não sejam apenas a divisão com resto de números naturais. Apresentamos ainda a noção de números primos e suas propriedades, dando ênfase especial ao Teorema Fundamental da Aritmética que justifica como encontrar os divisores de números inteiros bem como a quantidade desses divisores. Abordamos as definições e propriedades do máximo divisor comum e o mínimo múltiplo comum que normalmente nas escolas de Ensino Fundamental é ensinado apenas pelo método da fatoração conjunta para efetuar operações com frações, nesse trabalho será dado prioridade a caracterização, interpretação e propriedades. Como uma possível continuação ou extensão do estudo da divisão e suas propriedades na Educação Básica sugerimos o estudo do resto das divisões utilizando as propriedades das congruências. Por fim, faremos um relatório de avaliação de aplicação de uma sequência de atividades de Aritmética Básica a um grupo de alunos do Ensino Médio.

O material didático desse trabalho é dividido em três partes tradicionalmente ensinadas na Educação Básica (Divisão de Números Inteiros, Números Primos, Múltiplos e Divisores) mais uma proposta de aprofundamento (Introdução ao Estudo das Congruências). No decorrer desse trabalho, procuramos introduzir exemplos e situações-problema que aguçam a curiosidade, bem como uma grande quantidade de questões das principais olimpíadas de matemática do país, nas quais problemas sobre Aritmética aparecem constantemente.

Propomos a aplicação dos tópicos abordados desse trabalho em sala de aula a partir do 1º ano do Ensino Médio, já que nessa etapa do ensino, o aluno tem conhecimento das principais propriedades dos conjuntos dos números naturais e inteiros, requisitos para a compreensão dos estudos de Aritmética. Entretanto, a seleção dos tópicos e quando iniciar seu ensino em sala de aula são de prioridade do professor regente. É de responsabilidade do professor adaptar os conteúdos a realidade de seus alunos, levando em conta que existem turmas de capacidades cognitivas homogêneas e heterogêneas, o tempo que o professor deseja dedicar para trabalhar cada tópico e a relevância social que o aprofundamento dos estudos de Aritmética tem para os alunos.

2 FUNDAMENTAÇÃO DA PROPOSTA

Neste trabalho buscamos seguir as orientações que os Parâmetros Curriculares nacionais (PCNs)(1) fazem a respeito do que se espera da postura do Professor de Matemática em sala de aula, bem como nas recomendações dos PCNs ao ensino da Aritmética na Educação Básica.

Em todas as regiões brasileiras, os alunos do Ensino Fundamental e Médio tem atingido baixos índices de proficiência em Matemática nos vários tipos de avaliações de larga escala aplicados em âmbito estadual e nacional. Esse baixo rendimento de nossos alunos é oriundo, em parte, de uma educação deficiente em nossas escolas. Nessas avaliações, os problemas sobre Aritmética e suas propriedades tem presença constante.

Com relação ao comprometimento do ensino da Aritmética na Educação Básica, segundo os Parâmetros Curriculares Nacionais, essas deficiência é causada, em parte, pelo uso habitual de metodologias inadequadas pelo professor em sala de aula: pouco conhecimento do que ensina, uso do livro didático de forma inadequada, mau uso da linguagem matemática e o abandono do ensino de Aritmética ainda no 4º ciclo do Ensino Fundamental.

É preocupante, segundo os PCNs (2), a formação e a qualificação dos professores da Educação básica. Praticamente todos os conteúdos de Aritmética ensinados aos alunos da Educação Básica são ministrados aos alunos do 1º, 2º e 3º ciclos do Ensino Fundamental. Geralmente os professores desses ciclos são professores polivalentes, encarregados de lecionar todas as disciplinas aos alunos. Entretanto esses professores tem uma formação incipiente na maioria dessas disciplinas que leciona inclusive a matemática. E quando o professor, a muito custo consegue uma melhor qualificação (especialização, mestrado e doutorado), o professor busca melhores oportunidades em outras etapas do ensino (ensino médio e superior). Essas restrições para com a qualificação do professor, condições inadequadas para desenvolver seu trabalho e falta de políticas públicas eficazes para suprir tais problemas desmotivam o professor ao exercer suas atividades.

> "Parte dos problemas referentes ao ensino de Matemática estão relacionados ao processo de formação do magistério, tanto em relação à formação inicial como à formação continuada. Decorrentes dos problemas da formação de professores, as práticas na sala de aula tomam por base os livros didáticos, que, infelizmente, são muitas vezes de qualidade insatisfatória. A implantação de propostas inovadoras, por sua vez, esbarra na falta de uma formação profissional qualificada, na existência de concepções pedagógicas inadequadas e, ainda, nas restrições ligadas às condições de trabalho." (BRASIL, 1997, p.22)

Um fato que dificulta o aprendizado da Aritmética é a grande carga de conhecimen-

tos matemáticos sequenciados que o aluno tem que adquirir em um espaço curto de tempo, forçando os professores a abandonarem os procedimentos aritméticos de forma brusca ainda no 4º ciclo do Ensino Fundamental para dar lugar aos procedimentos algébricos e geométricos.

> "É importante salientar que no quarto ciclo não se pode configurar o abandono da Aritmética, como muitas vezes ocorre. Os problemas sobre Aritmética praticamente não são postos como desafios aos alunos deste ciclo; em geral, as situações trabalhadas pelos professores privilegiam a aplicação de conceitos algébricos." (BRASIL,1998, p. 83)

Para dar conta da cobrança da sociedade por alunos cada vez mais qualificados em matemática, o sistema de ensino atual adota a postura de relacionar a teoria com a resolução de uma grande quantidade de situações-problema, priorizando as longas listas de exercícios, memorização de fórmulas e procedimentos de cálculos e não sua aplicação. Essa postura é refletida nas estrutura dos livros adotados na educação básica. Tópicos importantes de Aritmética nos textos dos livros didáticos tais com o estudo da divisão, números primos entre outros, são vistos em apenas um, no máximo dois, capítulos dos livros do 3º ciclo do Ensino Fundamental, comprometendo a consolidação do conhecimento nesse ciclo. O estudo da Aritmética não encontra nos livros de séries posteriores material para aprofundamento do conhecimento e para agravar a situação, esses livros são utilizados como referência para a confecção do plano anual de curso das escolas. Essa prática dificulta a aprendizagem de novas competências pelos alunos como a capacidade de análise e raciocínio na resolução de problemas, bem como fere, segunda a LDB(3) direitos garantidos aos alunos tais como o de consolidar e aprofundar conteúdos estudados e, ainda no Ensino Fundamental, desenvolver a capacidade de aprender tendo pleno domínio da escrita e do cálculo.

> "O que também se observa em termos escolares é que muitas vezes os conteúdos matemáticos são tratados isoladamente e são apresentados e exauridos num único momento. Quando acontece de serem retomados (geralmente num mesmo nível de aprofundamento, apoiando-se nos mesmos recursos), é apenas com a perspectiva de utilizá-los como ferramentas para a aprendizagem de novas noções."(BRASIL, 1998, p.22)

Algumas "políticas públicas" aplicadas na Educação Básica são prejudiciais ao ensino da Matemática. As escolas são orientadas a ter como principal referência à sua prática pedagógica, as diretrizes do ENEM (Exame Nacional do Ensino Médio). Tais diretrizes afirmam que as questões envolvidas na avaliação devem ser contextualizadas. No entanto há uma distorção no que se refere a ideia de contexto, onde uma interpretação equivocada afirma que se deve trabalhar a Matemática apenas com situações que fazem parte do dia-a-dia do aluno em detrimento ao rigor e abstração da própria Matemática. As situações do cotidiano são importantes pois dão significado ao conteúdo estudado, entretanto também são importantes, a dedução, a abstração e o

pensamento analítico em que muitas vezes se tratam de questões internas da própria matemática.

> "... não se deve perder de vista os caracteres especulativo, estético não imediatamente pragmático do conhecimento matemático sem os quais se perde parte de sua natureza. Duas forças indissociáveis estão sempre a impulsionar o trabalho em Matemática. De um lado, o permanente apelo das aplicações às mais variadas atividades humanas, das mais simples na vida cotidiana, às mais complexas elaborações de outras ciências. De outro lado, a especulação pura, a busca de respostas a questões geradas no próprio edifício da Matemática. A indissociabilidade desses dois aspectos fica evidenciada pelos inúmeros exemplos de belas construções abstratas originadas em problemas aplicados e, por outro lado, de surpreendentes aplicações encontradas para as mais puras especulações." (BRASIL, 1998, p.24)

Entre muitas propostas que devem ser aplicadas para reverter essses problemas sobre o ensino de Aritmética na educação, um deles segundo os Parâmetros Curriculares Nacionáis do Ensino Médio (PCNEM)(4), consiste em uma nova apresentação do conteúdo. O aprofundamento sobre o ensino da Aritmética, bem como o ensino diferenciado da divisão, suas propriedades e características no Ensino Médio, ainda é amparado pelo Artigo 26 da LDB (3), que afirma que o conteúdo a ser ensinado na educação básica pode ser complementado por uma parte diversificada de acordo com as necessidades dos alunos de cada escola.

Portanto, o material contido nesse texto tem aplicações que vão desde a aplicação em sala de aula se, por exemplo, o Projeto Político Pedagógico de uma escola contempla o aprofundamento dos estudos de Aritmética vistos no Ensino Fundamental, mesmo que de forma extracurricular; pode ser utilizado como material de apoio na preparação de alunos para Olimpíadas de Matemática e ainda pode ser utilizado texto para cursos de formação continuada para professores que lecionam mas que não são graduados em Matemática. Espera-se que dessa forma, o material contido neste trabalho ajude a diminuir um pouco, o impacto negativo que os problemas enunciados acima causam na educação dos alunos.

> "Também por isso, o currículo a ser elaborado deve corresponder a uma boa seleção, deve contemplar aspectos dos conteúdos e práticas que precisam ser enfatizados. Outros aspectos merecem menor ênfase e devem mesmo ser abandonados por parte dos organizadores de currículos e professores. Essa organização terá de cuidar dos conteúdos mínimos da Base Nacional Comum, assim como fazer algumas indicações sobre possíveis temas que podem compor a parte do currículo flexível, a ser organizado em cada unidade escolar, podendo ser de aprofundamento ou direcionarse para as necessidades e interesses da escola e da comunidade em que ela está inserida."(BRASIL, 1999, p. 43)

A escolha dos conteúdos de Matemática ensinados nas escolas assim como as técnicas e metodologias de ensino devem ser revistos continuamente, adaptando-se

o mais rápido possível às necessidades dos alunos, consequentemente, às necessidades da sociedade.

3 DIVISÃO

No dia-a-dia, as pessoas dividem, repartem, comparam e agrupam objetos constantemente. Esse contexto é o ponto de partida do estudo das divisões. Entretanto quando se fala de divisão, a maior parte das pessoas lembra apenas da operação em si e de suas partes (dividendo, divisor, quociente e resto) bem como a busca pelo quociente e descartando o resto, a princípio sem valor. Entretanto o estudo das divisões no conjunto dos números inteiros tem relação com vários conceitos que serão abordados no decorrer desse trabalho.

Ao iniciar o estudo da divisão, o professor deve tratar o assunto como uma extensão do campo multiplicativo que o aluno aprende em anos anteriores. Esse vínculo com a multiplicação pode ser visto na definição que segue.

Definição 3.1. Seja a e b números inteiros. Dizemos que a divide b (denotamos por $a \mid b$), se existir um número inteiro c tal que $b = ac$.

Exemplo 3.1. $2 \mid 6$; $4 \mid 8$; $2 \mid 0$; $5 \mid 5$; $1 \mid 9$.

Como se vê, se a divide b deve existir um número inteiro c que quando multiplicado por a obtemos b. Pela relação da divisão com a multiplicação temos que as definições abaixo são equivalentes:

a) a divide b;

b) a é fator de b;

c) b é múltiplo de a.

Se o número a não dividir b escrevemos essa informação por $a \nmid b$.

Exemplo 3.2. $5 \nmid 4$; $3 \nmid 2$; $8 \nmid 9$; $7 \nmid 5$; $3 \nmid 4$.

Os símbolos $\mid$ e $\nmid$ não representam operações, os mesmos apenas indicam se um número é, ou não, divisível por outro.

3.1 Propriedades da Divisão

A divisão possui as seguintes propriedades:

a) Se a, b e c são inteiros tais que $a \mid b$ e $b \mid c$, então $a \mid c$;

b) Se a, b, c, m e n são inteiros tais que $c \mid a$ e $c \mid b$, então $c \mid (ma + nb)$. Ou seja, c divide qualquer combinação linear de a e b;

c) Qualquer inteiro (inclusive o número zero) divide a si mesmo, ou seja, $n \mid n$;

d) Se o número d divide n, então ad, divide an, ou seja, $d \mid n$implica que $ad \mid an$;

e) A recíproca da propriedade anterior é válida se $a \neq 0$;

f) O número 1 divide qualquer inteiro, ou seja, $1 \mid n$, para todo $n \in \mathbb{Z}$;

g) Qualquer número inteiro divide o zero, ou seja, $n \mid 0$ para todo $n \in \mathbb{Z}$;

h) Se $d \mid n$ e $n \neq 0$, então $|d| \leqslant |n|$ para todo $n, d \in \mathbb{Z}$;

i) Se $d \mid n$ e $n \mid d$, então $|d| = |n|$;

j) Se $d \mid n$ e $d \neq 0$, então $\frac{n}{d} \mid n$.

Abaixo seguem as demonstrações das referidas propriedades.

a) Pela definição de divisor, se $a \mid b$ e $b \mid c$, então existem inteiros p e q tais que $b = pa$ e $c = qb$. Substituindo b na segunda equação obtemos $c = qb = qpa$. Portanto $a \mid c$.

b) Se $c \mid a$ e $c \mid b$ então $a = pc$ e $b = qc$. Multiplicando a primeira equação por m e a segunda equação por n obtemos $ma = mpc$ e $nb = nqc$. Agora somando as equações membro a membro $ma + nb = (mp + nq)c$, ou seja $c \mid (ma + nb)$.

c) De fato, como $n = 1 \cdot n$, segue da definição de divisor segue que $n \mid n$.

d) De fato, como $d \mid n$, então pela definição de divisor obtemos $n = cd$, onde c é inteiro. Logo $an = cad$, ou seja, $ad \mid an$.

e) Se $ad \mid an$ então, pela definição de divisor, $an = adc$ onde c é um números inteiro. Utilizando a lei do cancelamento na equação anterior obtemos $n = dc$ $(a \neq 0)$. Portanto $d \mid n$.

f) Seja n um número inteiro. Como $n = 1 \cdot n$ temos que $1 \mid n$ provando o resultado.

g) Com efeito, $0 = n \cdot 0$ para qualquer $n \in \mathbb{Z}$. Portanto, pela definição de divisor segue que $n \mid 0$.

h) Se $d \mid n$, então por definição $n = dc$ onde c é inteiro. Por outro lado $n = dc$ implica que $|n| = |dc| = |d||c| \geqslant |d|$ pois $|c| \geqslant 1$ e $n \neq 0$ provando o resultado.

i) Se $d \mid n$ e $n \mid d$, então por definição $n = dc$ e $d = nk$, onde c e k são inteiros. Substituindo o valor de d na primeira equação obtemos $n = nkc$, ou seja, $kc = 1$. Logo $c = k = 1$ ou $c = k = (-1)$ o que implica $d = n$ ou $d = -n$. Portanto $|d| = |n|$.

j) Se $d \mid n$, então $n = kd$ sendo k um número inteiro. Logo $\frac{n}{d}$ é um inteiro. Como $\frac{n}{d} \cdot d = n$ segue pela definição de divisor que $\frac{n}{d} \mid n$.

Como se vê, a notação utilizada nesse texto é a mesma usada em cursos de Aritmética em Nível Superior como as mostradas em Santos (5) e em Hefez (6), porém como as propriedades utilizadas nas argumentações são oriundas das operações fundamentais, não há restrições para o uso no Ensino Médio, se assim desejar o professor. O professor pode apresentar algumas dessas propriedades para seus alunos como exercícios de aplicação da definição de divisor.

Logo abaixo segue alguns exemplos de aplicações da definição e propriedades dos divisores.

Exemplo 3.3. (FILHO, 1981, p.80) Mostrar que, se $a \mid b$, então $(-a) \mid b$; $a \mid (-b)$; $(-a) \mid (-b)$.

Solução: Se $a \mid b$, então existe $q \in \mathbb{Z}$ tal que $b = aq$.

a) $b = aq \Rightarrow b = (-1)(-1)aq = (-1)a(-1)q = (-a)(-q)$. Como $q \in \mathbb{Z}$, segue que $(-q)$ também pertence a $\mathbb{Z}$. Portanto exite um inteiro tal que $b = (-a)(-q) \Rightarrow (-a) \mid b$.

b) $b = aq \Rightarrow (-1)b = (-1)aq \Rightarrow (-b) = a(-q)$. Conforme o item "a", segue que $a \mid (-b)$.

c) $b = aq \Rightarrow (-1)b = (-1)aq \Rightarrow (-b) = (-a)b$. Conforme o item "a", segue que $(-a) \mid (-b)$.

Exemplo 3.4. (FILHO, 1981, p.81) Mostrar que se $a \mid (2x - 3y)$ e $a \mid (4x - 5y)$, então $a \mid y$.

Solução: Pela definição de divisor, se $a \mid (2x - 3y)$ então existe $q \in \mathbb{Z}$ tal que $aq = (2x - 3y)$. Logo

$$aq = (2x - 3y) \Leftrightarrow 2aq = 2(2x - 3y) \Leftrightarrow 4x - 6y = 2aq. \tag{3.1}$$

Da mesma forma, se $a \mid (4x - 5y)$, então então existe $p \in \mathbb{Z}$ tal que

$$ap = (4x - 5y). \tag{3.2}$$

Subtraindo (3.1) de (3.2) obtemos

$$(4x - 5y) - (4x - 6y) = ap - 2aq \Rightarrow 4x - 5y - 4x + 6y = a(p - 2q) \Rightarrow y = a(p - 2q).$$

Como p e $2q$ são inteiros, segue que $(p-2q)$ é inteiro. Portanto existe um inteiro $k = p-2k$ tal que $y = ak$, ou seja, $a \mid y$.

Os casos mais desafiadores de divisões são quando as divisões não são exatas, ou seja, quando a divisão deixa resto não nulo. Para tal fim, será visto um teorema central no estudo dos números inteiros: O Algoritmo da Divisão.

3.2 O Algoritmo da Divisão

De acordo com os PCNs(1), as escolas de Ensino Fundamental devem iniciar o ensino da divisão no 2º ciclo do Ensino Fundamental, aprofundando o seu estudo no 3º ciclo do Ensino Fundamental. Mas essa prática é feita apenas utilizando o método da chave nas divisões que é uma consequência do algoritmo da divisão. O ensino da divisão no atual sistema de ensino é focado apenas em problemas cuja resolução é o quociente da divisão não sendo abordadas as propriedades da divisão. Como consequência, muitos alunos terminam o Ensino Fundamental sem ter domínio sobre a operação de divisão. Outros fazem a divisão de modo automático, como uma receita infalível, sem entender o processo.

Mesmo por "anos" utilizando divisões, poucos alunos conseguem enunciar o algoritmo da divisão, apesar de o utilizar em qualquer divisão. O Algoritmo da Divisão tem muitas aplicações no ensino de Matemática, de simples divisões com números naturais até em assuntos mais complexos como divisão de polinômios.

O próprio Euclides enunciou esse teorema sem demonstrá-lo em virtude das limitações matemáticas da época. Não é recomendado a demonstração do algoritmo da divisão para alunos do Ensino Fundamental. Entretanto, no ensino médio, os alunos já podem ter contato com tal demonstração, desde que conheçam alguns resultados que serão ferramentas indispensáveis na demonstração de muitos teoremas e propriedades nesse texto: O Princípio da Indução Finita, O princípio da Boa Ordenação e o Princípio da Indução Matemática. As demonstrações desses resultados serão omitidas pois não se adequam aos objetivos desse texto[1] .

Axioma 3.1. (Princípio da Indução Finita) Seja I um subconjunto de $\mathbb{N}$. Que satisfaz as seguintes condições:

a) $1 \in I$;

b) Para todo k, se $k \in I$, então $(k + 1) \in I$.

Nessas condições, $I = \mathbb{N}$.

Axioma 3.2. (Princípio da Boa Ordenação) Todo subconjunto não vazio $X \subset \mathbb{N}$ possui um menor elemento.

Teorema 3.1. (Princípio da Indução Matemática - Primeira Forma) Seja $P(n)$ uma propriedade descrita em termos de números inteiros positivos $n \geqslant 1$. Suponhamos que as afirmações abaixo estejam satisfeitas:

a) $P(1)$, é verdadeira;

[1] Leitores interessados no tema podem pesquisar em Lima(7),Krerley(8), Filho(9)e Hefez(10)

b) Para todo $k \geqslant 1$, se $P(k)$ é verdadeira, então, $P(k+1)$ também é verdadeira.

Nesse caso então $P(n)$ é válida para todo $n \geqslant r$.

Teorema 3.2. (Princípio da Indução Matemática - Segunda Forma) Seja $P(n)$ uma propriedade descrita em termos de números inteiros positivos $n \geqslant r$. Suponhamos que as afirmações abaixo estejam satisfeitas:

a) $P(r)$, é verdadeira;

b) Para todo $k \geqslant r$, se $P(k)$ é verdadeira, então, $P(k+1)$ também é verdadeira.

Nesse caso então $P(n)$ é válida para todo $n \geqslant r$.

Usaremos esses resultados para demonstrar propriedades importantes como o Teorema Fundamental da Aritmética, mas podemos utilizar o Princípio da Indução para mostrar resultados elementares sobre divisão. Por exemplo:

Exemplo 3.5. Prove que $\frac{(n+1)}{n} < n$ para todo $n \in \mathbb{N}$ e $n \geqslant 2$.

Solução: Usaremos o princípio da indução em n.

a) Para $n = 2$, segue que $\frac{(2+1)}{2} = \frac{3}{2} < 2$. Verdadeiro.

b) Supondo que a propriedade seja válida para o número natural k ($k > 2$). Logo

$$\begin{aligned} \frac{k+1}{k} < k \quad &\Leftrightarrow \quad \frac{k\cdot(k+1)}{k} < k^2 \Leftrightarrow (k+1) < k^2 \Leftrightarrow (k+1)+1 < k^2+1 \\ &\Leftrightarrow \quad \frac{k+2}{k+1} < \frac{k^2+1}{k+1} \text{ (pois } k > 2) \Rightarrow \frac{k+2}{k+1} < \frac{k^2+2.k+1}{k+1} \\ &\Leftrightarrow \quad \frac{k+2}{k+1} < \frac{(k+1)^2}{k+1} \Leftrightarrow \frac{k+2}{k+1} < k+1. \end{aligned}$$

Portanto $\frac{(n+1)}{n} < n$ para todo n natural maior que ou igual a 2.

Teorema 3.3. (Algoritmo da divisão) Sejam a e b dois números naturais. Existem dois únicos números naturais q e r tais que $b = aq + r$ com $0 \leqslant r < a$.

Demonstração. Se $b < a$, então: $b = a \cdot 0 + b$ com $q = 0$ e $r = b$ valendo o resultado. Se $b = a$, então $b = a \cdot 1 + 0$ com $q = 1$ e $r = 0$ valendo o resultado. Supondo que $b > a$, considere o conjunto S de inteiros não negativos, definidos por

$$S = \{b - a, b - 2a, \ldots, b - na, \ldots\}. \tag{3.3}$$

O conjunto S não é vazio pois $b - a > 0$. Pelo principio da boa ordenação o conjunto (3.3) tem um menor elemento. Chamaremos esse elemento de r, ou seja, r é da forma $r = b - qa$. Provemos que $r < a$. Se $a \mid b$, então $r = 0$ e nada mais temos que provar. Mas se $a \nmid b$, então $r \neq a$. Agora provemos que não pode ocorrer $r > a$. De fato,

se isso ocorrer, então deve existir um número natural $c < r$ tal que $r = c + a$. Como $r = c + a = b - qa$ temos $c = b - (q+1) \cdot a \in S$, com $c < r$. Isso é uma contradição pelo fato de r, por hipótese, ser o menor elemento de S. Portanto $b = aq + r$ com $r < a$, provando a existência de q e r.

Para provar a unicidade, suponha que existe outro par q_1 e r_1 tal que $b = aq_1 + r_1$ com $r_1 < a$, ou seja,

$$(aq + r) - (aq_1 + r_1) = 0 \Rightarrow a \cdot (q - q_1) = r_1 - r.$$

Logo $a \mid (r_1 - r)$. Mas, como $r_1 < a$ e $r < a$, segue que $|r_1 - r| < a$ e, como $a \mid (r_1 - r)$ devemos ter $r_1 - r = 0$ o que implica $r_1 = r$. Portanto $q_1 \cdot a = qa \Rightarrow q_1 = q$, pois temos que $a \neq 0$. □

A demosntração acima pode ser adaptada para os números a ou b negativos com o resto da divisão pertencente ao conjunto $r = \{0, 1, 2, \ldots, |a| - 1\}$.

Há uma diferença sutil entre o ensino do algoritmo da divisão e o ensino das ideias e significados dessa operação. Dividir é subtrair do dividendo parcelas iguais ao divisor, até que o que a "sobra" seja menor que o divisor. O quociente será o número de subtrações efetuadas, enquanto o resto será o que sobrar no final. Apenas quando o professor tiver ciência que seus alunos entenderam o significado da divisão e conseguem aplicá-la em situações-problema, ele poderá apresentar o Algoritmo da Divisão aos seus alunos.

O algoritmo da divisão tem inúmeras aplicações que vão desde problemas elementares até propriedades importantes como a Propriedade Arquimediana. Também em diversas situações podemos provar propriedades válidas para qualquer inteiro considerando um número finito de casos. Apresentaremos agora algumas dessas aplicações:

Exemplo 3.6. Quantos são os múltiplos de 5 entre 1 e 276?

Solução: Pelo algoritmo da divisão obtemos $276 = 5 \cdot 55 + 1$. Logo o maior múltiplo de 5 menor que 276 é $5 \cdot 55$ onde 55 é o quociente da divisão de 276 por 5. Portanto são 55 múltiplos de 5.

Exemplo 3.7. Mostre que se a é um número inteiro, então a^2 é da forma $4k$ ou $4k + 1$.

Solução: Para a par, pelo algoritmo da divisão, segue que $a = 2q$ para algum $q \in \mathbb{Z}$, logo

$$a^2 = (2q)^2 = 4q^2 = 4k.$$

Para a ímpar, pelo algoritmo da divisão, segue que $a = 2q + 1$ para algum $q \in \mathbb{Z}$. Logo

$$a^2 = (2q + 1)^2 = 4 \cdot q^2 + 4q + 1 = 4(q^2 + q) + 1 = 4k + 1.$$

Portanto, a^2 é da forma $4k$ ou $4k + 1$.

Exemplo 3.8. (FILHO, 1981, p.78) Mostre que o quadrado de qualquer número ímpar é da forma $8k + 1$.

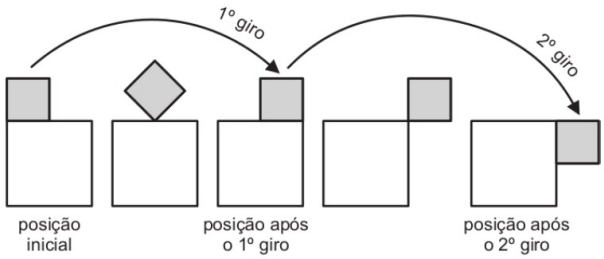
Solução: Pelo algoritmo da divisão qualquer número inteiro n pode ser escrito nas formas $4q$, $4q + 1$, $4q + 2$ e $4q + 3$.

Se n é ímpar, então $n = 4q + 1$ ou $4q + 3$. Logo,

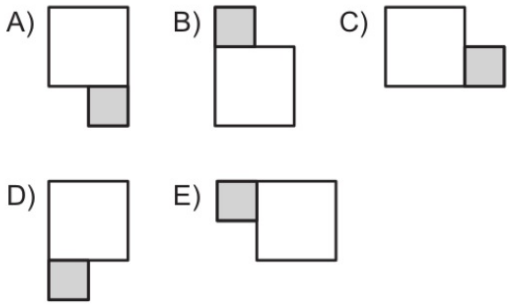
$$\begin{aligned} n^2 &= (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8k + 1. \\ n^2 &= (4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1 = 8k + 1. \end{aligned}$$

Portanto, o quadrado de qualquer número ímpar é da forma $8k + 1$.

Exemplo 3.9. (OBMEP 2012)Um quadrado de lado 1 cm roda em torno de um quadrado de lado 2 cm, como na figura, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado maior.



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



Solução: Nesse tipo de problema trabalhamos com a ideia de agrupamento e interpretação do resto da divisão. Basta verificar que após oito giros sucessivos o quadrado menor retorna à sua posição inicial. Como $2012 = 8 \cdot 251 + 4$, após o 2012º giro o quadrado cinza terá dado 251 voltas completas no quadrado maior e mais quatro giros, parando na posição que corresponde à alternativa A.

Exemplo 3.10. (OEM - RJ/1993) Qual a 1993ª letra da sequência ABCDEDCBABC-DEDCBABCDEDCB...?

Solução: Observe que a sequência ABCDEDCB se repetem num grupo de oito. Dividindo 1993 por 8, obtemos 1 como resto: $1993 = 8 \cdot 249 + 1$. Logo a 1993ª letra será a 1ª após 249 grupos iguais a ABCDEDCB, ou seja, a resposta é A.

Exemplo 3.11. (Propriedade Arquimediana) Dados dois números naturais a e b com $1 < a \leqslant b$, mostre que existe um número natural n tal que: $na \leqslant b < (n+1)a$.

Solução: Pelo algoritmo da divisão, temos que existem $q, r \in \mathbb{N}$ com $r < a$, únicos tais que $b = aq + r$. Agora, basta tomar $n = q$, ou seja, $na \leqslant an + r < (n+1)a$ com $0 \leqslant r < a$.

Exemplo 3.12. (FILHO, 1981, p.81) Mostrar que $\frac{n(n+1)(2n+1)}{6}$ é um inteiro, qualquer que seja o número inteiro positivo n.

Solução: Devemos mostrar que $6 \mid (n(n+1)(2n+1))$. Para isso, é suficiente mostrar que 2 e 3 também dividem essa expressão.
Qualquer que seja $n(n+1)$, ele é sempre múltiplo de 2, pois, pelo algoritmo da divisão, $n = 2k$ ou $n = 2k + 1$.

a) Se $n = 2k$, então $2 \mid n$. Logo $2 \mid n(n+1)$;

b) Se $n = 2k + 1$, então $n + 1 = 2k + 1 + 1 = 2k + 2 = 2(k + 1)$, ou seja, $2 \mid (n + 1)$. Logo $2 \mid n(n + 1)$.

Portanto, para qualquer que seja n inteiro e positivo segue que, $2 \mid n(n+1) \Rightarrow 2 \mid (n(n+1)(2n+1))$.

Pelo algoritmo da divisão, qualquer n inteiro pode ser escrito da forma $n = 3k, n = 3k + 1, n = 3k + 2$, ou seja, temos três possibilidades para n:

a) Se $n = 3k$, então $3 \mid n$. Logo $3 \mid (n(n+1)(2n+1))$;

b) Se $n = 3k + 1$, então $2n + 1 = 2(3k + 1) + 1 = 6k + 2 + 1 = 6k + 3 = 3(2k + 1)$, ou seja, $3 \mid (2n + 1)$. Logo $3 \mid (n(n+1)(2n+1))$;

c) Se $n = 3k + 2$, então $n + 1 = 3k + 2 + 1 = 3k + 3 = 3(k + 1)$, ou seja, $3 \mid (n + 1)$. Logo $3 \mid (n(n+1)(2n+1))$.

Portanto, $6 \mid (n(n+1)(2n+1))$ para qualquer inteiro positivo n.

Nessa etapa da construção do conhecimento do aluno, cabe ao professor explicar que o método utilizado no exemplo anterior é chamado de "Estudo de Caso". O professor deve afirmar com veemência aos seus alunos que o método aplicado é de fato uma é uma técnica de demonstração aplicável em muitas situações envolvendo números inteiros. Como exercício o professor pode preparar alguns problemas para que os alunos tentem identificar em quais deles o estudo de caso pode ser aplicado.

Lembrando ao professor que esses são exemplos para desafiar generalizações do algoritmo da divisão. contudo o professor deve ponderar bem sobre a maturidade da sua turma antes de aplicar esse nível de exemplos. É importante que o professor também use situações do cotidiano, ou seja, situações onde a aluno se depara alguma vez em sua vida. Uma boa estratégia de ensino é aplicar situações onde o próprio aluno crie o seu próprio algoritmo e só depois apresentar o algoritmo da divisão com todo seu rigor.

3.3 Resto da Soma e do Produto

As vezes precisamos determinar restos de divisões cujos dividendos são muito elevados, que são difíceis de se trabalhar. Um resultado importante obtido com o algoritmo da divisão que não é ensinado no Ensino Fundamental é o Lema dos Restos, que substitui esses dividendos por números menores, mais fáceis de manipular. A demonstração desse lema exige o conhecimento do algoritmo da divisão sendo completamente acessível a alunos do Ensino Médio.

Lema 3.1. (Lema dos Restos) A soma e o produto de quaisquer dois números inteiros deixa o mesmo resto que a soma e o produto dos seus restos, na divisão por um inteiro positivo b.

Demonstração. Provemos para a soma:
Sejam a_1 e $a_2 \in \mathbb{Z}$. Dividindo ambos os números por b obtemos

$$a_1 = bq_1 + r_1 \text{ e } a_2 = bq_2 + r_2, \text{ com } 0 \leqslant r_1, r_2 < b.$$

Logo,

$$\begin{aligned} a_1 + a_2 &= (bq_1 + r_1) + (bq_2 + r_2) \\ &= bq_1 + bq_2 + (r_1 + r_2) \\ &= b(q_1 + q_2) + (r_1 + r_2) \\ &= bq + (r_1 + r_2), \end{aligned} \tag{3.4}$$

onde $q = q_1 + q_2$. Agora dividimos $r_1 + r_2$ por b para se obter:

$$r_1 + r_2 = bp + r,\ p \in \mathbb{Z},\ 0 \leq r < b. \tag{3.5}$$

Das igualdades (3.4) e (3.5) obtemos

$$a_1 + a_2 = bq + bp + r = b.(p + q) + r,\ 0 \leq r < b. \tag{3.6}$$

Portanto,de (3.5) e (3.6) tem-se que os restos de $a_1 + a_2$ e $r_1 + r_2$ por b são iguais. Agora provemos para o produto:
Sejam a_1 e $a_2 \in \mathbb{Z}$. Dividindo ambos os números por b obtemos

$$a_1 = bq_1 + r_1 \text{ e } a_2 = bq_2 + r_2, \text{ com } 0 \leqslant r_1, r_2 < b$$

Logo,

$$\begin{aligned} a_1a_2 &= (bq_1 + r_1)(bq_2 + r_2) \\ &= b^2q_1q_2 + bq_1r_2 + bq_2r_1 + r_1r_2 \\ &= b(bq_1q_2 + q_1r_2 + q_2r_1) + r_1r_2 \\ &= bq + r_1r_2 \end{aligned} \tag{3.7}$$

onde $q = bq_1q_2 + q_1r_2 + q_2r_1$. Agora dividimos r_1r_2 por b para se obter

$$r_1r_2 = bp + r,\ p \in \mathbb{Z},\ 0 \leq r < b. \tag{3.8}$$

Das igualdades (3.7) e (3.8) obtemos

$$a_1a_2 = bq + bp + r = b(p + q) + r,\ 0 \leq r < b. \tag{3.9}$$

Portanto, de (3.8) e (3.9) tem-se que os restos de a_1a_2 e r_1r_2 por b são iguais. □

Exemplo 3.13. (FOMIN,D.2012, p.28) Encontre o resto da divisão de:

a) $1989 \cdot 1990 \cdot 1991 + 1992^3$ por 7;

b) 9^{100} por 8.

Solução:

a) Dividindo 1989, 1990, 1991 e 1992 por 7 temos como resultados 1, 2, 3 e 1. Portanto, pelo lema dos restos, o resto da divisão de $1989 \cdot 1990 \cdot 1991 + 1992^3$ por 7 é o resto da divisão de $1 \cdot 2 \cdot 3 + 1 = 7$ por 7, ou seja, a resposta é 0.

b) Dividindo 9 por 8 o resto é 1. Portanto, pelo lema dos restos, o resto da divisão 9^{100} por 8 é o resto da divisão de $1^{100} = 1$ por 8, ou seja, a resposta é 1.

Quando os alunos conseguirem resolver alguns problemas do mesmo nível que o anterior o professor pode trabalhar generalizações do Lema dos Restos.

Exemplo 3.14. Prove que $n^6 + 1$ não é divisível por 3 para qualquer $n \in \mathbb{Z}$.

Solução: Pelo algoritmo da divisão o resto da divisão de n por 3 pode ser 0,1,2. Vamos considerar três casos:

a) Para resto 0: Pelo lema dos restos, o resto da divisão de $n^6 + 1$ por 3 é igual ao resto de $0^6 + 1 = 1$ por 3, ou seja, é 1. Logo não é divisível por 3;

b) Para resto 1: Pelo lema dos restos, o resto da divisão de $n^6 + 1$ por 3 é igual ao resto de $1^6 + 1 = 2$ por 3, ou seja, é 2. Logo não é divisível por 3;

c) Para resto 2: Pelo lema dos restos, o resto da divisão de $n^6 + 1$ por 3 é igual ao resto de $2^6 + 1 = 65$ por 3, ou seja, é 2. Logo não é divisível por 3.

Portanto $n^6 + 1$ não é divisível por 3 para nenhum $n \in \mathbb{N}$.

4 NÚMEROS PRIMOS

Para dar continuidade ao estudo da divisão e suas propriedades é necessário definir números primos e apresentar algumas de suas propriedades. Os números primos são de importância fundamental no estudo divisão, já que todos os números inteiros, objeto de estudo da Aritmética, podem ser representados como produto de números primos bem como seus múltiplos e divisores. Por isso não é de se estranhar que sejam tema de estudo de muitos matemáticos através de séculos. Muitas propriedades foram descobertas por esses matemáticos, algumas muitos difíceis de serem provadas, mas a demonstração dessas propriedades foge aos objetivos do nosso trabalho.

Na tecnologia, os números primos se destacam pelo seu uso em criptografias. A criptografia é a técnica de se ocultar de terceiros informações que devem ser compartilhadas apenas por um grupo fechado de pessoas. É utilizado em qualquer transação feita pela internet, como por exemplo as compras com cartão de crédito. Nesse tipo de transação é vital que apenas o consumidor e a empresa que vai vender um produto ou prestar um serviço tenham conhecimento dos dados do cartão de crédito utilizado. É nesse momento que a criptografia codifica os dados enviado online de modo que apenas os envolvidos na transação possam recuperá-los. A criptografia RSA, que é a mais difundida em transações online, sendo considerada uma das mais seguras da atualidade, tem nos números primos a essência de seu funcionamento. Essa é uma das muitas importâncias em se estudar os números primos.

O caso é que em nossas escolas a maioria dos alunos não sabe a definição de números primos bem como sua importância para a construção dos números e de seus divisores. O conhecimento da definição de números primos que o aluno adiquire no Ensino Fundamental fica comprometida na medida que os alunos não tem intimidade com os conjuntos númericos, que são essenciais para a precisão das definições e propriedades. A ideia agora é associar a definição de números primos aos conjuntos númericos aprimorando assim o conhecimento dos alunos .

Definição 4.1. Um número inteiro n ($n > 1$) possuindo apenas dois divisores positivos 1 e n é chamado de número primo.

Exemplo 4.1. 2, 3, 5, 7, 11, 13 17, ...

Se um número inteiro n ($n > 1$) possui mais de dois divisores positivos, n é chamado de número composto.

Exemplo 4.2. 4, 6, 8, 10, 12, 14 ...

Durante as aulas de Matemática é comum os alunos perguntarem se os números "um" e "zero" são ou não primos. Basta observar as definições de números primos e

compostos e concluimos facilmente que 0 e 1 não se enquadram em nenhuma delas. Portanto, não são nem primos nem compostos.

4.1 Infinitude dos Números Primos

Quantos números primos existem? A maioria dos livros do Ensino Fundamental não responde essa pergunta. No início do Ensino Médio o aluno já pode ter contato com algumas demonstrações sobre a infinitude dos primos.

Proposição 4.1. Existem infinitos números primos.

Existem várias demonstrações desse teorema, daremos três demonstrações acessíveis ao nível de instrução dos alunos do Ensino Médio, pois assim o professor poderá escolher a que melhor se adapta as suas aulas podendo também desafiar seus alunos a encontrarem outras demonstrações.

Demonstração. (Euclides) Seja I, um conjunto finito qualquer de números primos

$$I = \{p_1, p_2, p_3, ..., p_n\}. \tag{4.1}$$

Basta mostrar que existem números primos que não estão nesse conjunto. De fato, seja P o produto de todos os números primos no conjunto (4.1)

$$P = p_1 \cdot p_2 \cdot p_3 \cdots p_n.$$

Tomando $q = P + 1$, o número q pode ser ou não primo:

a) Se q é primo então há pelo menos um número primo a mais que não está no conjunto (4.1).

b) Se q não é primo, então algum fator primo p divide q. Esse fator p não está no conjunto (4.1), pois caso estivesse, ele dividiria P (pois P é o produto de todos os número na lista); mas como sabemos, p divide $P + 1 = q$. Então, para não deixar resto, p teria que dividir a diferença entre os dois números, que é $(P + 1) - P$ ou seja, 1. Mas não existe número primo que divida 1. Logo, p não pode estar na lista. Isso significa que pelo menos mais um número primo existe além dos que estão na lista.

Portanto para qualquer conjunto finito de números primos, há um número primo que não está na lista, ou seja, existem infinitos números primos. □

Demonstração. (Contradição) A demonstração por contradição utiliza o Teorema Fundamental da Aritmética que será discutido logo mais à frente. Suponha que a sequência de primos abaixo seja finita. Seja I o conjunto de todos os primos

$$I = \{2, 3, 5, 7, ..., p_r\}. \tag{4.2}$$

Façamos $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_r + 1$. Pelo Teorema Fundamental da Aritmética, existe um primo p_i que divida P. Esse número p_i não poderá ser igual a nenhum dos números de (4.2) pois caso fosse ele dividiria $P - (2 \cdot 3 \cdot 5 \cdot 7 \cdots p_r) = 1$ o que é absurdo. Logo p_i é um primo que não pertence ao conjunto I, portanto $2, 3, 5, 7, ..., p_r$ não podem formar o conjunto de todos os primos. □

Demonstração. (Hermite) A demonstração de Hermite utiliza o Teorema Fundamental da Aritmética que será discutido logo mais à frente. Seja $n > 1$ um número natural. Defina a função $x(n) = n!+1$. Ora, $x(n)$ gera um número natural para cada n natural, logo pelo Teorema Fundamental da Aritmética, existe um primo p fator de $x(n)$. Afirmamos que esse primo p não pode dividir um número menor do que ou igual a n, pois neste caso, dividiria $n!$ e daí, dividiria $x(n) - n! = 1$. Portanto, dado qualquer natural $n > 1$, sempre existe um primo $p > n$, ou seja existem infinitos números primos. □

Euclides não provou a infinitude dos números primos por contradição, pois não é afirmado que o conjunto de primos utilizado tinha todos os primos, nem os números primos menores que n, mas sim, qualquer conjunto arbitrário de primos.

As demonstrações dadas sobre a infinitude dos primos são de fácil entendimento e podem ser aplicadas em salas de aulas de Ensino Médio, mas não fornecem informações sobre a estrutura desses números primos. As demonstações de Euclides e Contradição garantem apenas que o próximo primo é no mínimo igual a $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_r + 1$. A demonstração dada por Hermite garante apenas que o número dado pela função $x(n) = n! + 1$ para $n \in \mathbb{N}$ tem pelo menos um fator maior do que n. A escolha de qual das demonstrações o professor deve aplicar em sala de aula depende do conhecimento da turma sobre o Teorema Fundamental da Aritmética. Caso a turma não tenha conhecimento desse teorema, apenas a demonstração de Euclides poderá ser trabalhada.

Há muitas outras demonstrações da infinitude dos primos como a de Gauss, que usa o conceito de congruência (assunto esse que veremos mais adiante nesse trabalho); a demonstração de Euler usando séries; a demonstração de Furstenberg usando topologia, que são demonstrações que o professor interessado em se aprofundar no tema pode pesquisar em textos tais como Ribenboim (11). As três demonstrações apresentadas, apesar das suas limitações com relação a estrutura dos primos são ideais para serem trabalhadas com alunos da educação básica, pela simplicidade e argumentos de fácil entendimento para o nível cognitivo desses alunos.

4.2 Teorema Fundamental da Aritmética

É comum alunos do Ensino Fundamental perguntarem porque os números primos são importantes e devem ser estudados. A importância dos números primos é condensada em um teorema central, não só para o ensino da divisão mas para todo o ensino de

Aritmética. O Teorema Fundamental da Aritmética responde muitas dúvidas sobre a estrutura dos números inteiros como por exemplo: Será que qualquer número pode ser decomposto em fatores primos? A fatoração de um número inteiro em um produto de números primos é única? Essas perguntas não são respondidas no 3º ciclo do Ensino Fundamental quando os alunos tem o primeiro contato com os números primos e a partir daí esse assunto fica esquecido. Todas essas perguntas são respondidas pelo Teorema Fundamental da Aritmética. Além do mais a maioria dos problemas envolvendo múltiplos, divisores e números primos estão relacionados com o Teorema Fundamental da Aritmética.

Teorema 4.1. (Teorema Fundamental da Aritmética) Todo número inteiro maior do que 1 é primo ou pode ser escrito de modo único (a menos da ordem dos fatores) em um produto de números primos.

Demonstração. Para provar a existência usamos a indução sobre n.

a) Se $n = 2$ o resultado é óbvio.

b) Supondo que o resultado é válido para qualquer número inteiro k da forma $2 < k < n$. Se o número n é primo, então o resultado vale. Se n é composto, então existem os números inteiros positivos n_1 e n_2 tais que $n = n_1 \cdot n_2$. Como $1 < n_1 < n$ e $1 < n_2 < n$. Por hipótese de indução, existem primos $p_1, \ldots, p_s$ e $q_1, \ldots, q_r$ de forma que os números n_1 e n_2 podem ser escritos como $n_1 = p_1 \ldots p_s$ e $n_2 = q_1 \ldots q_r$. Logo $n = p_1 \ldots p_s \cdot q_1 \ldots q_r$. Portanto n pode ser escrito como produto de primos.

Para provar a unicidade usamos a indução sobre n.

a) Para $n = 2$ o resultado é obvio;

b) Supondo que a afirmação tenha validade para todos os números inteiros maiores do que 2 e menores que n. Provemos que vale também para n. Se n é primo o resultado vale. Supondo n composto e que tenha duas fatorações ou seja: $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$. Como p_1 divide o produto $q_1 q_2 \cdots q_r$ ele deve dividir pelo menos um dos fatores q_i. Sem perda de generalidade supondo que $p_1 | q_1$ (p_1 divide q_1) . Como um número primo só admite ele próprio além do 1 como divisor positivo, segue que $p_1 = q_1$. Logo $\frac{n}{p_1} = p_2 \cdots p_s = q_2 \ldots q_r$. E como $1 < \frac{n}{p_1} < n$, temos que pela hipótese de indução que as duas fatorações são idênticas. Portanto $p_1 p_2 \cdots p_s$ e $q_1 q_2 \cdots q_r$ são iguais.

□

Respondendo às perguntas anteriores, o Teorema Fundamental da Aritmética garante que qualquer número inteiro maior do que 1 pode ser decomposto em produtos

de números primos e essa decomposição é única, mostrando assim a importância dos números primos como geradores de todos os números inteiros.

Observe que se o número 1 fosse considerado primo, o Teorema Fundamental da Aritmética perderia a sua unicidade na decomposição pois cada número inteiro poderia ou não, apresentar o número 1 em sua decomposição.

Observe que em nenhum momento da demonstração do Teorema Fundamental da Aritmética, foi dito que os números $p_1 \dots p_s \cdot q_1 \dots q_r$ eram distintos. Agrupando os números primos idênticos da decomposição de n, podemos escrevê-lo da forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Esse produto é chamado de decomposição primária de n.

Uma das consequência do Teorema Fundamental da Aritmética é de importância fundamental para o estudo da divisão, pois todos os divisores de um número inteiro podem ser obtidos mediante a sua fatoração em um produto de primos como mostra o resultado abaixo.

Corolário 4.1. Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ a decomposição primária de n. Se m é um divisor de n então a decomposição primária de m será da forma $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ onde $0 \leqslant \beta_i \leqslant \alpha_i$.

Demonstração. Como m é um divisor de n então $n = mc$ para c inteiro. Logo, os fatores primos de m, caso exitam, pois m pode ser 1, são fatores primos de n. Supondo $m \neq 1$, e p^β uma potência de um primo p que aparece na decomposição de m, temos que $p^\beta \mid n$. Como p só admite ele mesmo como divisor além do 1, segue que p^β divide apenas um $p_i^{\alpha_i}$ de n . Portanto, $0 \leqslant \beta \leqslant \alpha_i$. □

O resultado acima fornece o modo para determinar o número de divisores de um número natural n.

Corolário 4.2. Seja o número inteiro positivo $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ onde $p_1, ..., p_s$ são números primos e $\alpha_1, ..., \alpha_s \in \mathbb{N}$. O número de divisores do número natural n denotado por $d(n)$ é

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1).$$

Demonstração. Pelo Corolário 4.1, o expoente de cada um dos p_i da fatoração dos divisores de n variam de 0 até α_i. Utilizando o princípio fundamental da contágem para saber o número de escolhas possíveis para os expoentes de cada p_i, o resultado segue. □

O corolário acima é utilizada na resolução de muitos problemas de olimpíadas de matemática para alunos do Ensino Médio. Segue uma aplicação da proposição acima.

Exemplo 4.3. (OBM – 2011) Quantos números inteiros positivos menores que 30 têm exatamente quatro divisores positivos?
A) 6 B) 7 C) 8 D) 9 E) 10

Solução: Pelo princípio fundamental da contágem bem como pelo Corolário 4.2, para um número inteiro positivo ter exatamente 4 divisores positivos, sua fatoração em primos deve ser da forma pq ou p^3, onde p e q são primos distintos. Para encontrar esses números, devemos seguir o método das tentativas a partir dos menores primos. Logo, os números de 1 a 30 que possuem exatamente 4 divisores são

$$6 = 2\cdot 3;\ 10 = 2\cdot 5;\ 14 = 2\cdot 7;\ 22 = 2\cdot 11;\ 26 = 2\cdot 13;\ 15 = 3\cdot 5\ 21 = 3\cdot 7;\ 8 = 2^3;\ 27 = 3^3.$$

Portanto, são 9 números.

Há inúmeras aplicações do Teorema Fundamental da Aritmética, sendo das mais importantes as aplicações em divisibilidade, máximo divisor comum e mínimo múltiplo comum que serão vistas mais adiante.

4.3 Crivo de Eratóstenes

Dada a importância do Teorema Fundamental da Aritmética para determinar os divisores de um inteiro pela sua fatoração única em números primos, agora se faz necessário um método para determinar os números primos.

É estudo da Matemática há muito tempo, a tentativa de encontrar algoritmos eficazes para encontrar números primos com o mínimo de esforço e operações consequentemente exigindo menos tempo em sua execução.

Além da importância para a divisão, a tentativa de encontrar números primos cada vez maiores é de grande importância na tecnologia para criar sistemas de códigos cada vez mais seguros a fim de efetuar transferências de dados entre computadores de forma cada vez mais segura.

Uma das dificuldades em expressar uma fórmula eficaz para obtenção dos números primos é o fato de existir intervalos arbitrariamente grandes de números compostos como mostra o resultado abaixo:

Proposição 4.2. Dado um números inteiro $n \geqslant 2$. A sequência $(n+1)!+2, (n+1)!+3, ..., (n+1)!+n+1$ de números inteiros positivos é formada por n numeros consecutivos compostos.

Demonstração. Pela definição de fatorial, o número $(n+1)!$ possui os fatores de 2 até $n+1$. Dado $k = 2, 3, ..., n+1$, o número $(n+1)!+k$ tem o fator k, pois

$$\begin{aligned}(n+1)!+k &= (2\cdot 3\cdots(k-1)\cdot k\cdot(k+1)\cdots(n+1))+k\\ &= k\cdot(2\cdot 3\cdots(k-1)\cdot(k+1)\cdots(n+1))+k\\ &= k\cdot(2\cdot 3\cdots(k-1)\cdot(k+1)\cdots(n+1)+1).\end{aligned}$$

Portanto $(n+1)!+k$ é divisível por k, ou seja, $(n+1)!+k$ é composto. □

Mas nosso objetivo é determinar um método que seja eficaz para o aluno da Educação Básica encontrar números primos com eficiência para desenvolver seus trabalhos escolares. Essa ferramenta é o Crivo de Eratóstenes. Esse método é utilizado pela maioria dos autores de livros de matemática da 6ª série do Ensino Fundamental, entretanto a justificativa da sua construção não é vista nesses livros e seu ensino é incipiente. A justificativa para a construção do Crivo de Eratóstenes é dada pelo resultado abaixo.

Teorema 4.2. Se n é um número inteiro $n > 1$ que não é divisível por nenhum primo p tal que $p^2 \leq n$, então n é primo.

Demonstração. Suponha, por absurdo, que n não é primo. Então segue do Teorema Fundamental da Aritmética que $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, tal que $\alpha_i \geqslant 2$ para algum i ou $s \geqslant 2$. Seja $q = min\{p_1, p_2, \cdots, p_s\}$. Assim $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \geqslant q^{\alpha_1+\alpha_2+\cdots+\alpha_s} \geqslant q^2$. Logo q é primo, $q^2 \leqslant n$ e q divide n. Contradição.

□

Esse teorema é a base da elaboração do Crivo de Eratóstenes. Também fornece um teste de primalidade, pois para verificar se um número inteiro n é primo, basta verificar que nenhum primo menor que $\sqrt{n}$ divida n.

Para elaborar o crivo, basta seguir os passos abaixo:

a) Escolher o tamanho da tabela, ou seja, a quantidade de números que a mesma deve conter, digamos n números;

b) Eliminamos o número "um" da tabela pois o mesmo tem apenas um divisor inteiro positivo (não é primo);

c) Destacamos todos os números primos de 1 a $\sqrt{n}$;

d) Eliminamos todos os múltiplos dos números primos destacados no passo anterior;

e) Destacamos os números que sobrarem pois esses serão os números primos procurados.

Do ponto de vista computacional o Crivo de Eratóstenes é desvantajoso, pois, para conseguir o próximo número primo, o algoritmo faz uma quantidade cada vez maior de cálculos o que o torna inviável para se determinar números primos de valor muito elevado. Mas do ponto de vista educacional o Crivo de Eratóstenes é ideal para alunos da Educação Básica descobrirem se um número é ou não primo já que os mesmos não vão precisar de números primos de valor muito elevado em suas atividades e sua simplicidade o torna aceitável.

O professor também pode trabalhar o Crivo de Eratóstenes de modo interdisciplinar com o professor de artes elaborando uma tabela bem ornamentada para sua sala de

Tabela 1 – Crivo de Eratóstenes até o número 200:

.	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

Fonte: O Autor

aula ou com o professor de história dada a importância de Eratóstenes como cientista e matemático, foi ele o primeiro homem a dar um valor aceitável, para os limites matemáticos da época, do diâmetro da terra.

4.4 A Fatoração do Fatorial

Como uma extensão do estudo dos números primos no 2º ano do Ensino Médio, o professor de ensino médio pode associar o estudo dos números primos com o estudo da análise combinatória mais especificamente com o estudo dos fatoriais mostrando resultados importantes aos alunos sobre divisão.

O "Teorema de Legendre" pode ser utilizado pelo professor do 2º ano do Ensino Médio junto com a Análise Combinatória para aprofundar o conhecimento dos alunos sobre o Teorema Fundamental da Aritmética. Algumas aplicações são de fácil entendimento para alunos do Ensino Médio. Para enunciar o Teorema de Legendre precisamos de alguns resultados preliminares. Nos resultados abaixo seguimos a apresentação dada em Hefez(6).

Lema 4.1. Seja a e m dois números naturais com $a > 1$. Então, existe um número natural n tal que $a^n > m$.

Não justificaremos o resultado do lema acima pois tal demonstração usa termos que fogem aos estudos desse texto.

Proposição 4.3. [1] Se $a \in \mathbb{N}$ e $b, c \in \mathbb{N}^*$, então o quociente da divisão por c do quociente da divisão de a por b é igual ao quociente da divisão de a por b vezes c, ou seja,

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right].$$

A expressão $\left[\frac{a}{b}\right]$ expressa o quociente da divisão de a por b na divisão euclidiana.

Demonstração. Dados q_1 e q_2 da forma

$$q_1 = \left[\frac{a}{b}\right] \text{ e } q_2 = \left[\frac{\left[\frac{a}{b}\right]}{c}\right].$$

Pelo algoritmo da divisão, $a = bq_1 + r_1$, com $0 \leqslant r_1 \leqslant b - 1$. Do mesmo modo, $q_1 = \left[\frac{a}{b}\right] = cq_2 + r_2$ com $0 \leqslant r_2 \leqslant c - 1$. Portanto

$$a = bq_1 + r_1 = b(cq_2 + r_2) + r_1 = bcq_2 + br_2 + r_1.$$

Como $br_2 + r_1 \leqslant b(c-1) + b - 1 = bc - 1$, segue que q_2 é o quociente da divisão de a por bc ou seja,

$$q_2 = \left[\frac{a}{bc}\right].$$

□

Seja p um número primo e m um número natural. Chamamos de $E_p(m)$ o maior expoente da potência de p que divide m, ou seja o expoente de p que aparece na decomposição do número m em fatores primos.

Teorema 4.3. [2](Legendre) Sejam n um número natural e p um número primo. Então

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

Demonstração. Pelo resultado do Lema 4.1, existe um número natural r tal que $p^i > n$ para todo $i \geqslant r$. Logo $\left[\frac{n}{p^i}\right] = 0$, se $i \geqslant r$. Para demonstrar o teorema usa-se a indução sobre n:

[1] HEFEZ, 2006, p. 104
[2] Ibid., p. 105

a) Se $n = 0$ então, $E_p(0!) = 0$ (Verdadeiro).

b) Supondo que o resultado vale para $m < n$. Os múltiplos de p entre 1 e n são $p, 2p, \ldots, \left[\frac{n}{p}\right]p$. O que acarreta

$$E_p(n!) = \left[\frac{n}{p}\right] + E_p\left(\left[\frac{n}{p}\right]!\right).$$

Pela hipótese de indução

$$E_p\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p^2}\right] + \ldots \tag{4.3}$$

Usando o resultado da Proposição 4.3

$$\frac{\left[\frac{n}{p}\right]}{p} = \left[\frac{n}{p^2}\right]; \quad \frac{\left[\frac{n}{p}\right]}{p^2} = \left[\frac{n}{p^3}\right]; \quad \ldots$$

Substituindo em (4.3) obtemos o resultado desejado

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

□

O Teorema de Legendre permite que o aluno conheça e manipule os divisores de $n!$ sem precisar desenvolver esse fatorial (o que na maioria dos casos é inviável até para calculadoras).

Exemplo 4.4. Determine a decomposição primária de 20!.

Solução: Resolvemos o problema encontrando o valor de $E_p(20!)$ para todos os primos menores que 20, ou seja:

$$\begin{aligned}
E_2(20!) &= \left[\frac{20}{2}\right] + \left[\frac{20}{4}\right] + \left[\frac{20}{8}\right] + \left[\frac{20}{16}\right] = 10 + 5 + 2 + 1 = 18 \\
E_3(20!) &= \left[\frac{20}{3}\right] + \left[\frac{20}{9}\right] = 6 + 2 = 8 \\
E_5(20!) &= \left[\frac{20}{5}\right] = 4 \\
E_7(20!) &= \left[\frac{20}{7}\right] = 2 \\
E_{11}(20!) &= \left[\frac{20}{11}\right] = 1 \\
E_{13}(20!) &= \left[\frac{20}{13}\right] = 1 \\
E_{17}(20!) &= \left[\frac{20}{17}\right] = 1 \\
E_{19}(20!) &= \left[\frac{20}{19}\right] = 1
\end{aligned}$$

Logo:

$$20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11^1 \cdot 13^1 \cdot 17^1 \cdot 19^1$$

Exemplo 4.5. Determine a decomposição primária de 15!. Em seguida determine a quantidade de seus divisores e qual a quantidade de zeros que termina esse número.

Solução: Resolvemos o problema encontrando o valor de $E_p(15!)$ para todos os primos menores que 15, ou seja:

$$\begin{aligned}
E_2(15!) &= \left[\frac{15}{2}\right] + \left[\frac{15}{4}\right] + \left[\frac{15}{8}\right] = 7 + 3 + 1 = 11 \\
E_3(15!) &= \left[\frac{15}{3}\right] + \left[\frac{15}{9}\right] = 5 + 1 = 6 \\
E_5(15!) &= \left[\frac{15}{5}\right] = 3 \\
E_7(15!) &= \left[\frac{15}{7}\right] = 2 \\
E_{11}(15!) &= \left[\frac{15}{11}\right] = 1 \\
E_{13}(15!) &= \left[\frac{15}{13}\right] = 1
\end{aligned}$$

Logo:

$$15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1$$

Portanto o número de divisores de 15! é

$$d(15!) = (11 + 1) \cdot (6 + 1) \cdot (3 + 1) \cdot (2 + 1) \cdot (1 + 1) \cdot (1 + 1) = 4032 \text{ divisores}$$

Já o número de zeros é igual ao número de fatores 5. Como existem 3 fatores 5 o número termina com três zeros.

Exemplo 4.6. (HEFEZ, 2006, p.108) Responda:

a) Ache as maiores potências de 2 e 5 que dividem 10000!;

b) Determine com quantos zeros termina a representação decimal de 10000!;

c) Ache a maior potência de 104 que divide 10000!.

Solução:

a) Para achar as maiores potências de 2 e 5 que dividem 10000! devemos encontrar $E_p(10000!)$ para p igual a 2 ou 5:

$$\begin{aligned}
E_2(10000!) &= \left[\frac{10000}{2}\right] + \left[\frac{10000}{4}\right] + \left[\frac{10000}{8}\right] + \left[\frac{10000}{16}\right] + \left[\frac{10000}{32}\right] + \left[\frac{10000}{64}\right] + \left[\frac{10000}{128}\right] + \\
&+ \left[\frac{10000}{256}\right] + \left[\frac{10000}{512}\right] + \left[\frac{10000}{1024}\right] + \left[\frac{10000}{2048}\right] + \left[\frac{10000}{4096}\right] + \left[\frac{10000}{8192}\right] \\
&= 5000 + 2500 + 1250 + 625 + 312 + 156 + 78 + 39 + 19 + 9 + 4 + 1 \\
&= 9993.
\end{aligned}$$

Portanto 2^{9993} é a maior potência de 2 que divide 10000!.

$$\begin{aligned} E_5(10000!) &= \left[\frac{10000}{5}\right] + \left[\frac{10000}{25}\right] + \left[\frac{10000}{125}\right] + \left[\frac{10000}{625}\right] + \left[\frac{10000}{3225}\right] \\ E_5(10000!) &= 2000 + 400 + 80 + 16 + 3 \\ E_5(100001) &= 2499. \end{aligned}$$

Portanto 5^{2499} é a maior potência de 5 que divide 10000!.

b) Para determinar o número de zeros que termina 10000! basta observar a potência de 5. Pelo item "a" sabemos que 5^{2499}, ou seja, a quantidade de zeros em 10000! é 2499 zeros.

c) Decompondo 104 em fatores primos: $104 = 2^3 \cdot 13$. Agora precisamos encontrar $E_2(10000!)$ e $E_{13}(10000!)$.

Pelo item "a" $E_2(10000!) = 9993$, procurando o resultado para $E_{13}(10000!)$:

$$\begin{aligned} E_{13}(10000!) &= \left[\frac{10000}{13}\right] + \left[\frac{10000}{169}\right] + \left[\frac{10000}{2197}\right] \\ E_{13}(10000!) &= 769 + 59 + 4 \\ E_{13}(10000!) &= 832. \end{aligned}$$

O maior expoente de 13 que divide 10000! é 832 e como $2^{9993} = (2^3)^{3331}$, o maior expoente de 2^3 que divide 10000! é 3331. Logo, existem menos fatores de 13 do que 2^3. Assim a maior potência de 104 que divide 10000! é 104^{832}.

5 MÁXIMO DIVISOR COMUM E MÍNIMO MÍNIMO MÚLTIPLO COMUM

Serão tratados nesse capítulo as definições, propriedades e caracterizações do Máximo Divisor Comum e do Mínimo Múltiplo Comum. Por definição, a ideia de Máximo Divisor Comum e o Mínimo Múltiplo Comum de dois ou mais números inteiros é escolher entre os múltiplos comuns desses números o menor deles e entre os divisores comuns o maior deles. Veremos agora porque essas ideias merecem tanta atenção apesar de sua "aparente" simplicidade.

5.1 Máximo Divisor Comum

A fatoração de um número inteiro em um produto de primos evidencia os seus divisores. Dois ou mais números inteiros tem pelo menos um divisor positivo comum (o número 1). Se esses números inteiros apresentam fatores primos em comum nas suas fatorações então eles terão outros divisores comuns além do número 1. Dos divisores comuns, um deles merece atenção especial: o Máximo Divisor Comum.

Agora, será desenvolvida a teoria sobre Máximo Divisor Comum e suas aplicações bem como algumas de suas aplicações de modo rigoroso porém, acessível aos alunos e professores da Educação Básica.

Definição 5.1. Dados dois números inteiros a e b, o número inteiro $d \neq 0$ é um divisor comum de a e b se $d \mid a$ e $d \mid b$.

Exemplo 5.1. Os números $\pm 1, \pm 2, \pm 3, \pm 5, \pm 10, \pm 15, \pm 30$ são divisores comuns de 30 e 60.

Definição 5.2. (Máximo Divisor Comum) O máximo divisor comum (*mdc*) de dois inteiros "a" e "b" não ambos nulos ($a \neq 0$ ou $b \neq 0$), que denotaremos por $mdc(a, b)$, é o maior inteiro positivo que divide a e b.

Agora surgem duas perguntas: O Máximo Divisor Comum de dois inteiros sempre existe? Se existir o Máximo Divisor Comum de dois inteiros, ele é único? Para caracterizar o Máximo Divisor Comum, que a partir de agora chamaremos de *mdc*, e também responder às perguntas propostas acima, precisamos de um teorema: a Identidade de Bézout.

Teorema 5.1. (Identidade de Bézout) Se a e b são dois inteiros, então existem inteiros "x_0" e "y_0" tais que $mdc(a, b) = ax_0 + by_0$.

Demonstração. Seja P o conjunto de todos os inteiros da forma $ax + by$ com $x, y \in \mathbb{Z}$, ou seja,

$$P = \{ax + by; \text{ com } x, y \in \mathbb{Z}\}.$$

Tomando $y = 0$ e $x = 0$ podemos ver que P tem o zero. Afirmamos que o conjunto P tem elementos positivos e negativos. De fato, basta tomar o número inteiro $a \neq 0$ escrito das formas $a = a \cdot 1 + b \cdot 0$ e $-a = a \cdot (-1) + b \cdot 0$. Como a e $-a$ são opostos, um deles é positivo e o outro é negativo e pertencem a P. Pelo Princípio da Boa Ordenação existe um menor inteiro positivo em P que chamaremos de d. Pela formação do conjunto P, existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$. Basta mostrar que $d = mdc(a, b)$. Pelo algoritmo da divisão,

$$a = du + r \text{ com } 0 \leqslant r < d \Rightarrow r = a - du = a - (ax_0 + by_0)u = a(1 - ux_0) + b(-uy_0).$$

No caso, r é uma combinação linear de a e b, ou seja, $r \in P$. Como $0 \leqslant r < d$ e $d > 0$ é o menor elemento positivo de P, segue que $r = 0$ e $a = du$, ou seja $d \mid a$. Do mesmo modo se prova que $d \mid b$. Logo d é um divisor comum positivo de a e b, ou seja $d \leqslant mdc(a, b)$. Agora se c é um divisor inteiro positivo de a e b, então pelo item (b) das propriedades do divisor

$$c \mid a \text{ e } c \mid b \Rightarrow c \mid (ax_0 + by_0) \Leftrightarrow c \mid d \Rightarrow c \leqslant d.$$

Se $c = mdc(a, b)$, então $mdc(a, b) \mid d$, ou seja, $mdc(a, b) \leqslant d$ logo, pela desigualdade $d \leqslant mdc(a, b)$, segue que $mdc(a, b) = d$. Portanto d é o maior divisor comum positivo de a e b, ou seja, $mdc(a, b) = d = ax_0 + by_0$ com $x, y \in \mathbb{Z}$. □

A Identidade de Bézout garante a existência do *mdc* de dois números inteiros a e b desde que esses não sejam simultaneamente nulos ($a \neq 0$ ou $b \neq 0$). O Princípio da Boa Ordenação utilizado na demonstração da Identidade de Bézout, garante a unicidade do *mdc*. Porém, apesar do $mdc(a, b)$ ser único, a combinação linear $mdc(a, b) = ax + by$ não é única, ou seja, existem vários valores de x e y que satisfazem a relação. Entretanto a demosntração garante que o $mdc(a, b)$ é o menor inteiro positivo dentre todas as combinações lineares da forma $\{ax + by;$ com $x, y \in \mathbb{Z}\}$. Nesse trabalho, usaremos a identidade de Bézout para justificar propriedades importantes sobre *mdc* e congruências módulo m, além das aplicações nesse trabalho que o professor também pode utilizar na sala de aula.

Exemplo 5.2. Dado o conjunto $a \cdot \mathbb{Z} + b \cdot \mathbb{Z} = \{an + bm; m, n \in \mathbb{Z}\}$, mostre que o menor elemento positivo desse conjunto é o $mdc(a, b)$.

Solução: De fato, se $d = mdc(a, b)$, então por definição $d \mid a$ e $d \mid b$. Pela propriedade (b) dos divisores, temos que d divide qualquer elemento de $a \cdot \mathbb{Z} + b \cdot \mathbb{Z}$. Logo pela propriedade (h) dos divisores, d é menor ou igual a qualquer inteiro positivo de $a.\mathbb{Z} + b.\mathbb{Z}$. Pela identidade de Bézout, existem $x_0, y_0 \in \mathbb{Z}$ tal que $d = ax_0 + by_0$, ou seja $d \in a \cdot \mathbb{Z} + b \cdot \mathbb{Z}$. Portanto d é o menor elemento positivo do conjunto $a \cdot \mathbb{Z} + b \cdot \mathbb{Z}$.

Proposição 5.1. Para a e b inteiros não ambos nulos e c um inteiro positivo, vale a igualdade $mcd(ca, cb) = c \cdot mdc(a, b)$.

Demonstração. Pela identidade de Bézout, segue que

$$mdc(ca, cb) = min\{cax + cby > 0 | x, y \in \mathbb{Z}\} = c \cdot min\{ax + by > 0 | x, y \in \mathbb{Z}\} = c \cdot mdc(a, b).$$

□

Corolário 5.1. Se c é um inteiro positivo e a e b são inteiros divisíveis por c, então $mdc\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot mdc(a, b)$.

Demonstração. Como $c \mid a$ e $c \mid b$, segue que $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros. Portanto, basta substituir na proposição anterior a por $\frac{a}{c}$ e b por $\frac{b}{c}$, para obtermos

$$c \cdot mdc\left(\frac{a}{c}, \frac{b}{c}\right) = mdc\left(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}\right) \Rightarrow c \cdot mdc\left(\frac{a}{c}, \frac{b}{c}\right) = mdc(a, b) \Rightarrow mdc\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot mdc(a, b).$$

□

Corolário 5.2. Se $mdc(a, b) = d$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração. Basta tomar c no corolário anterior como sendo $mdc(a, b) = d$ e o resultado segue. □

A principal propriedade do $mdc(a, b)$ não é ser o maior divisor comum de a e b, mas sim que todo divisor comum de a e b é divisor do $mdc(a, b)$. A justificativa, não tão óbvia é dada pelo próximo resultado.

Proposição 5.2. O número inteiro positivo d é o máximo divisor comum de a e b (não conjuntamente nulos) se, e somente se, possuir as propriedades abaixo:

a) O número d é um divisor comum de a e b;

b) Se um número d' é divisor comum de a e b, então $d' \mid d$.

Demonstração. Supondo que $d = mdc(a, b)$, então $d \mid a$ e $d \mid b$. Logo, pela definição de mdc, a primeira condição é válida. Por outro lado, pela Identidade de Bézout, existem certos inteiros x_0 e y_0 tais que $ax_0 + by_0 = d$, e se $d' \mid a$ e se $d' \mid b$, então pela propriedade (b) dos divisores, $d' \mid (ax_0 + by_0)$, ou seja, $d' \mid d$ e a segunda condição é válida.

Reciprocamente, como $a \neq 0$ ou $b \neq 0$, pela segunda condição $d \neq 0$, e pela primeira e segunda condição, segue que $d > 0$. Ainda pela segunda condição, se d' é um divisor comum de a e b, então d' também é divisor de d, isto é $d' \mid d$. Logo, pela propriedade (h) dos divisores, segue que $d' \leqslant |d| = d$. Portanto d é o $mdc(a, b)$. □

A proposição acima é conhecida como caracterização do mdc e pode perfeitamente ser utilizada como definição para o mdc de dois números inteiros como acontece em muitos textos, caso semelhante ocorre em Hefez(6). Muitas vezes, a aplicação das propriedades da caracterização do mdc mostra-se mais vantajosa do que sua definição original. Veremos isso em algumas situações-problema e em outras propriedades.

5.1.1 *Algoritmo de Euclides*

O algoritmo de Euclides é um método simples e eficiente de encontrar o *mdc* de dois números inteiros e diferentes de zero. Pela sua simplicidade ele é ensinado a crianças do Ensino Fundamental sem muitas dificuldades. Na obra "Os Elementos" de Euclides já tinha uma descrição do seu uso. Entretanto o lema de Euclides, que justifica o funcionamento do algoritmo não é enunciado nesses livros. O Lema de Euclides é uma das ferramentas mais importantes para resolução de muitos problemas envolvendo a definição de *mdc* de dois números.

Lema 5.1. (Lema de Euclides) Se a e b são números inteiros e $b = aq + r$ onde, q e r são inteiros, então $mdc(a, b) = mdc(a, r)$.

Demonstração. Pelo algoritimo da divisão, se $b = aq + r$, então, pela propriedade (b) dos divisores, todo divisor de a e r é um divisor de b. Escrevendo $r = b - aq$, e novamente pela propriedade (b) dos divisores podemos ver que todo divisor de a e b é divisor de r. Como os divisores comuns de a e b são os mesmos divisores comuns de a e r, segue que, $mdc(a, b) = mdc(a, r)$. □

No Lema de Euclides não é condição necessária utilizar o resto da divisão de b por a, podemos também utilizar uma combinação da forma $b - na, n \in \mathbb{N}$ no lugar do resto, ou seja, se o $mdc(a, b - an)$ existe então $mdc(a, b) = mdc(a, b - an)$.

Teorema 5.2. (Algoritmo de Euclides) Sejam a e b números inteiros não negativos com $a \neq 0$. Ao se aplicar o algoritmo da divisão para se obter a sequência

$$b = aq_1 + r_1 \text{ com } 0 < r_1 < a$$

$$a = r_1q_2 + r_2 \text{ com } 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3 \text{ com } 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n \text{ com } 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_n + 0,$$

ou seja, até o número r_n dividir r_{n-1}, segue que o $mdc(a, b)$ é o último resto não nulo da sequência da de divisões.

Demonstração. Aplicando o lema de Euclides nas equações acima obtemos

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{r-1}) = \ldots = mdc(r_1, r_2) = mdc(a, r_1) = mdc(a, b).$$

Portanto o *mdc* dos números a e b é o último resto não nulo das divisões acima. □

A tabela a seguir mostra o procedimento para utilizar o Algoritimo de Euclides na prática:

Tabela 2 – Dispositivo prático para o algoritmo de Euclides

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

Fonte: O Autor

O Algoritmo de Euclides deve ser revisto de maneira mais rigorosa no Ensino Médio pela sua importância teórica e prática em aplicações como o uso em criptografias, equações diofantinas e congruências. Além disso o Algoritmo de Euclides é uma ferramenta poderosa usada em Olimpíadas de Matemática e em demonstração de teoremas importantes não só de Aritmética como também de outras áreas da Matemática.

O lema de Euclides merece especial atenção dos alunos e professores pois o mesmo pode ser muito útil em cálculos de *mdc*, principalmente quando há expressões algébricas envolvidas.

Logo abaixo será listado alguns exemplos da aplicação do algoritmo de Euclides e do lema de Euclides que o professor pode utilizar em sala de aula.

Exemplo 5.3. Um pastor tinha 100 ovelhas das quais 64 eram fêmeas. O pastor decidiu vendê-las na maior quantidade possível de grupos de tal forma que em um grupo tem que ter o maior número possível de fêmeas e machos. Quantos grupos são possíveis e com quantas fêmeas e machos cada um pode ter?

Solução: Calculamos o $mdc(64, 36)$ pois a quantidade de ovelhas machos e fêmeas deve ser o maior dos divisores comuns. Usando o Algoritmo de Euclides:

	1	1	2	2
64	36	28	8	4
28	8	4	0	

Logo $mdc(64, 36) = 4$. Assim são 4 grupos cada um com $64 \div 4 = 16$ fêmeas e $36 \div 4 = 9$ machos.

Exemplo 5.4. Obtenha x e y inteiros de modo que $56x + 72y = mdc(56, 72)$.

Solução: Pela Identidade de Bézout, temos que os valores de x e y que satisfazem a igualdade acima existem. Vamos utilizar o algoritmo de Euclides para encontrá-los: Calculando (72,56) pelo algoritmo de Euclides:

	1	3	2
72	56	16	8
16	8	0	

Agora vamos escrever 8 como combinação linear de 56 e 72. Usando o algoritmo da divisão de trás para frente obtemos $56 = 3 \cdot 16 + 8 \Rightarrow 8 = 56 - 3 \cdot 16 = 56 - 3 \cdot (72 - 56) = 4 \cdot 56 - 3 \cdot 72$. Portanto, uma solução para o problema são os valores $x = 4$ e $y = -3$.

Os dois proximos exemplos são encontrados em Hefez(6).

Exemplo 5.5. (HEFEZ, 2006, p.58) Mostre que $mdc(n + 1, n^2 + n + 1) = 1$ para $n \in \mathbb{N}$.

Solução: O lema de Euclides é ideal para lidar com *mdc* envolvendo expressões algébricas. Utilizando o Lema de Euclides, obtemos $mdc(n + 1, n^2 + n + 1) = mdc(n + 1, n \cdot (n + 1) + 1) = mdc(n + 1, 1) = 1$.

Exemplo 5.6. (HEFEZ, 2006, p. 55) Determine os valores de a e n de tal forma que $a + 1 \mid a^{2n} + 1$ com $n \in \mathbb{N}$.

Solução: Para resolver essa questão usaremos o lema abaixo. Sua demonstração pode ser feita por indução (o professor pode encorajar seus alunos a tentar demonstrar esse lema).

Lema 5.2. Sejam $a, b, n \in \mathbb{N}$, com $a \geqslant b > 0$ então $a + b \mid a^{2n} - b^{2n}$.

Demonstração. Usaremos a indução sobre n:

a) Se $n = 1$, então $a^{2\cdot 1} - b^{2\cdot 1} = a^2 - b^2 = (a + b) \cdot (a - b)$, ou seja, $a + b$ divide $a^{2\cdot 1} - b^{2\cdot 1}$;

b) Supondo que $a + b \mid a^{2k} - b^{2k}$ para um certo k inteiro positivo. De fato,

$$a^{2(k+1)} - b^{2(k+1)} = a^2 \cdot a^{2k} - b^2 a^{2k} + b^2 a^{2k} - b^2 b^{2k} = (a^2 - b^2)a^{2k} + b^2(a^{2k} - b^{2k})$$

como $a + b \mid a^2 - b^2$ pois $a^2 - b^2 = (a + b).(a - b)$ e, por hipótese, $a + b \mid a^{2k} - b^{2k}$, logo,

$$a + b \mid (a^2 - b^2)a^{2k} + b^2(a^{2k} - b^{2k}) \Rightarrow a + b \mid a^{2(k+1)} - b^{2(k+1)}.$$

Portanto, $a + b \mid a^{2n} - b^{2n}$ para $a, b, n \in \mathbb{N}$.

□

Voltando ao problema do exemplo, veja que $a + 1 \mid a^{2n} + 1$ se, e somente se, $mdc(a + 1, a^{2n} + 1) = a + 1$.

Logo, como $a^{2n} + 1 = (a^{2n} - 1) + 2$ e $a + 1 \mid a^{2n} - 1$ (Veja o lema acima) e utilizando o lema de Euclides obtemos $mdc(a + 1, a^{2n} + 1) = mdc(a + 1, (a^{2n} - 1) + 2) = mdc(a + 1, 2)$.

Portanto $a + 1 \mid a^{2n} + 1$ se e somente se $a + 1 = mdc(a + 1, 2)$ o que acontece se, $a = 0$ ou $a = 1$.

5.1.2 *Máximo Divisor Comum com Teorema Fundamental da Aritmética*

Podemos utilizar a fatoração única dos inteiros para demonstrar um processo de cálculo do *mdc* de dois ou mais números. Nos próximos resultados usaremos a seguinte notação para a fatoração dos números inteiros $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_s^{a_s}$ e $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_s^{b_s}$, onde os expoentes dos fatores primos não comuns as duas fatorações é igual a zero. O resultado a seguir é encontrado em Santos(5).

Proposição 5.3. [1] Se dois inteiros positivos a e b tem como fatorações

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_s^{a_s} \qquad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_s^{b_s}$$

onde $p_1, p_2, \ldots, p_s$ são números primos, então o máximo divisor comum de a e b é:

$$mdc(a,b) = p_1^{c_1} \cdot p_2^{c_2} \cdots p_s^{c_s} \quad \text{onde } c_i = min\{a_i, b_i\} \text{ para } 1 \leqslant i \leqslant s.$$

Demonstração. De fato, para que o produto de fatores primos comuns seja um divisor comum, nenhum dos expoentes c_i de p_i poderá ser maior de que a_i ou b_i. Como queremos o maior divisor positivo basta que c_i seja o menor deles. □

Exemplo 5.7. Calcule o $mdc(120, 75)$.

Solução: Usando o Teorema Fundamental da Aritmética para decompor os dois números, temos:

$$120 = 2^3 \cdot 3^1 \cdot 5^1 \text{ e } 75 = 2^0 \cdot 3^1 \cdot 5^2$$

Logo o $mdc(120, 75) = 3^1 \cdot 5^1 = 15$.

Exemplo 5.8. (XXII OBM-Segunda Fase, N.1) Qual é o maior inteiro positivo n tal que os restos das divisões de 154, 238 e 334 por n são iguais?

Solução: Dois números deixam o mesmo resto quando divididos por n se e só se sua diferença é múltipla de n. Logo, as diferenças $238 - 154 = 84$ e $334 - 238 = 96$ são ambas múltiplas de n. Como n é o maior possível, concluímos que n deve ser o $mdc(84, 96)$. Como $84 = 2^2 \cdot 3 \cdot 7$ e $99 = 2^5 \cdot 3$, segue que o $mdc(84, 96) = 2^2 \cdot 3 = 12$.

Definição 5.3. Se dois números inteiros positivos a e b não tem fatores primos em comum, então o $mdc(a, b) = 1$. Esses números são chamados de primos entre si ou coprimos.

A definição de números primos entre si e o Teorema Fundamental da Aritmética podem ser utilizados para demonstrar propriedades sobre divisões.

Proposição 5.4. Sejam p e q números inteiros positivos coprimos:

[1] SANTOS, 2000, p.10

a) Se algum inteiro é divisível por p e q, então é divisível por pq.

b) Se o número inteiro pk é divisível por q, então k é divisível por q.

Demonstração. Provemos cada um dos itens acima separadamente:

a) Seja n um número inteiro divisível por p. Logo, podemos escrever n como $n = pr$ ($r \in \mathbb{Z}$). Como p e q são coprimos e $q \mid n$, isso acarreta que $q \mid r$. Assim, podemos escrever r da forma $r = qs$ com $s \in \mathbb{Z}$. Substituindo $r = qs$ em $n = pr$ obtemos $n = pqs$ provando a primeira parte.

b) Para provar a segunda parte se pk é divisivel por q, então podemos escrever pk como $pk = qr$ com $r \in \mathbb{Z}$, mas isso acarreta que $k = \frac{qr}{p}$. Como k é um número inteiro, então $p \mid r$ (pois p e q são coprimos). Chamando $\frac{r}{p}$ de s temos que $k = sq$ com $s \in \mathbb{Z}$ provando a segunda parte.

□

5.2 Mínimo Múltiplo Comum

Por definição, múltiplo é um número inteiro cuja divisão por outro número inteiro não deixa resto, ou seja, podemos interpretar o múltiplo de um número como o dividendo de uma divisão de inteiros com resto zero. Verifica-se facilmente que dois ou mais números inteiros tem infinitos múltiplos comuns. Dentre esses infinitos múltiplos comuns, um deles merece destaque: o Mínimo Múltiplo Comum.

O aluno aprende a definição de Mínimo Múltiplo Comum, que a partir de agora chamaremos de *mmc*, e o algoritmo para encontrá-lo no Ensino Fundamental, mas em muitos livros não há menção sobre o Teorema Fundamental da Aritmética que é o fundamento do algoritmo para encontrar o *mmc* e além disso, muitas perguntas ficam não respondidas tais como: O *mmc* de dois ou mais números existe? Se existe *mmc* de dois ou mais números ele é único? Existe alguma relação entre *mdc* e *mmc*? Responderemos essas perguntas no decorrer desse trabalho.

Definição 5.4. Dados dois números inteiros a e b, não nulos, o número inteiro m é um múltiplo comum de a e b se $a \mid m$ e $b \mid m$.

Exemplo 5.9. Os múltiplos comuns de 4 e 6 são $0, \pm 12, \pm 24, \pm 36, \pm 48, \ldots$

Definição 5.5. (Mínimo Múltiplo Comum) O mínimo múltiplo comum (*mmc*) de dois inteiros "a" e "b" não nulos ($a \neq 0$ e $b \neq 0$), que denotaremos por $mmc(a, b)$, é o menor inteiro positivo que é múltiplo de a e b.

Teorema 5.3. Seja a e b dois números inteiros positivos. O $mmc(a, b)$ existe e é único.

Demonstração. Seja $M \subset \mathbb{N}$ o conjunto de todos os múltiplos comuns de a e b. O conjunto M não é vazio pois contêm o produto ab. Assim, pelo princípio da boa ordenação, M tem "um" elemento mínimo, ou seja, o $mmc(a, b)$. □

Do modo semelhante ao *mdc* de dois números inteiros, o que caracteriza o *mmc* de dois números inteiros não é ser o menor múltiplo comum desses números. O que caracteriza o *mmc* de dois números a e b, é o fato que todo múltiplo comum de a e b também é múltiplo do $mmc(a, b)$. Essa afirmação não tão óbvia é dada pela pelo resultado abaixo.

Proposição 5.5. O número inteiro positivo m é o mínimo múltiplo comum de a e b (não nulos) se, e somente se, possuir as propriedades abaixo:

a) O número m é um múltiplo comum de a e b;

b) Se um número m' é múltiplo comum de a e b, então $m \mid m'$.

Demonstração. Supondo que o $m = mmc(a, b)$, então pela definição de *mmc* $a \mid m$ e $b \mid m$. Assim, a primeira condição é satisfeita. Por outro lado, seja m' um múltiplo comum de a e b. Pelo algoritmo da divisão podemos escrever $m' = mq + r$, com $0 \leqslant r < m$. Logo, $r = m' - mq$. Como m' e mq são múltiplos comuns de a e b segue que,

$$m' = ap \text{ e } mq = as \quad \text{ou} \quad m' = bp' \text{ e } mq = as' \quad \text{com} \quad p, s, p', s' \in \mathbb{Z}.$$

Logo, podemos escrever r como $r = a(p - s)$ ou $r = b(p' - s')$, ou seja, r é múltiplo comum de a e b. Mas isso acarreta que $r = 0$, pois caso contrário teríamos um múltiplo comum r de a e b , tal que $0 < r < m$ contrariando a escolha de m. Portanto $m \mid m'$.

Reciprocamente, seja m um inteiro positivo que satisfaz as duas condições acima. Pela segunda condição, se m' é um múltiplo comum de a e b também é múltiplo de m, isto é $m \mid m'$ ou seja $m \leqslant m'$. Portanto $m = mmc(a, b)$. □

A proposição acima é conhecida como caracterização do *mmc* e pode perfeitamente ser utilizada como definição para o *mdc* de dois números inteiros. Para determinar o $mmc(a, b)$ de dois números basta recorrer ao Teorema Fundamental da Aritmética decompondo a e b em fatores primos. O resultado abaixo é encontrado em Santos (5).

Proposição 5.6. [2] Se dois inteiros positivos a e b tem como fatorações

$$a = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_s^{b_s}$$

onde $p_1, p_2, \ldots, p_s$ são números primos, então o mínimo multiplo comum de a e b é

$$mdc(a, b) = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s} \quad \text{onde } c_i = max\{a_i, b_i\} \text{ para } 1 \leqslant i \leqslant s.$$

[2] SANTOS, 2000, p.13

Demonstração. De fato, para que o produto de fatores primos comuns seja um múltiplo comum, nenhum dos expoentes c_i de p_i poderá ser menor de que a_i ou b_i. Como queremos o menor múltiplo positivo basta que c_i seja o maior desses deles. □

Exemplo 5.10. (PUC–SP) Numa linha de produção, certo tipo de manutenção é feita na máquina A a cada 3 dias, na máquina B, a cada 4 dias, e na máquina C, a cada 6 dias. Se no dia 2 de dezembro foi feita a manutenção nas três máquinas, após quantos dias as máquinas receberão manutenção no mesmo dia.

Solução: Para a realização da manutenção das três máquinas no mesmo dia precisamos dos múltiplos comuns de 3,4 e 6. A próxima manutenção se dará na menor quantidade de dias que é múltiplo comum de 3,4 e 6, ou seja, precisamos do $mmc(3,4,6)$:

$$3 = 3^1, 4 = 2^2 \text{ e } 6 = 2^1 \cdot 3^1$$

Logo $mdc(3,4,6) = 2^2 \cdot 3^1 = 12$. A manutenção simultânea deve ser feita a cada 12 dias. Logo, se a última manutenção foi no dia 2 de dezembro a próxima deve ser no dia 14 de dezembro.

O *mmc* e *mdc* estão relacionados por um resultado que torna certos problemas bem mais fáceis de serem manipulados. Representaremos por $max\{a,b\}$ e $min\{a,b\}$ o maior e respectivamente o menor dos números inteiros a e b. Sem perda de generalidade, supondo que $max\{a,b\} = a$, logo $min\{a,b\} = b$, ou seja, $max\{a,b\} + min\{a,b\} = a + b$.

Proposição 5.7. Para todo a e b inteiros positivos vale a relação: $mdc(a,b) \cdot mmc(a,b) = ab$.

Demonstração. Se $a = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ e $b = p_1^{b_1} p_2^{b_2} \cdots p_s^{b_s}$ são as fatorações dos números inteiros a e b então,

$$mdc(a,b) = p_1^{min\{a_1,b_1\}} p_2^{min\{a_2,b_2\}} \cdots p_s^{min\{a_s,b_s\}} \text{ e } mmc(a,b) = p_1^{max\{a_1,b_1\}} p_2^{max\{a_2,b_2\}} \cdots p_i^{max\{a_s,b_s\}}.$$

Multiplicando as expressões acima, obtemos

$$\begin{aligned} mdc(a,b) \cdot mmc(a,b) &= (p_1^{min\{a_1,b_1\}} p_2^{min\{a_2,b_2\}} \cdots p_s^{min\{a_s,b_s\}})(p_1^{max\{a_1,b_1\}} p_2^{max\{a_2,b_2\}} \cdots p_s^{max\{a_s,b_s\}}) \\ &= p_1^{\{a_1+b_1\}} p_2^{\{a_2+b_2\}} \cdots p_s^{\{a_s+b_s\}} \\ &= (p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s})(p_1^{b_1} p_2^{b_2} \cdots p_s^{b_s}) \\ &= ab. \end{aligned}$$

Concluindo a demonstração. □

Segue abaixo alguns exemplos utilizando a relação entre *mmc* e *mdc*:

Exemplo 5.11. (HEFEZ, 2006. p.65) Seja $n \in \mathbb{N}^*$, calcule $mmc(n^2+1, n+1)$.

Solução: Utilizando o lema de Euclides, obtemos

$$mdc(n^2+1, n+1) = mdc((n^2-1)+2, n+1) = mdc((n+1)(n-1)+2, n+1) = mdc(2, n+1).$$

Como 2 é número primo, segue que $mdc(2, n+1)$ é o $min\{2, n+1\}$. Logo, $n = 0$ ou $n = 1$, ou seja, o $mdc(n^2+1, n+1) = 1$ ou $mdc(n^2+1, n+1) = 2$. Discutiremos as possibilidades:

a) Se $mdc(n^2+1, n+1) = 1$, então pela relação entre *mmc* e *mdc* segue que,

$$mmc(n^2+1, n+1) \cdot mdc(n^2+1, n+1) = (n^2+1)(n+1) \Rightarrow mmc(n^2+1, n+1) = n^3+n^2+n+1.$$

b) Se $mdc(n^2+1, n+1) = 2$, então pela relação entre *mmc* e *mdc* segue que,

$$mmc(n^2+1, n+1) \cdot mdc(n^2+1, n+1) = (n^2+1)(n+1) \Rightarrow mmc(n^2+1, n+1) = \frac{1}{2} \cdot (n^3+n^2+n+1).$$

Exemplo 5.12. Dados a e b inteiros positivos, mostre que $mdc(a, b) = mmc(a, b)$ é equivalente a $a = b$.

Solução:
Se $mdc(a, b) = mmc(a, b)$, então pela relação entre *mmc* e *mmc* obtemos

$$mmc(a, b) \cdot mdc(a, b) = ab \Rightarrow mmc(a, b)^2 = ab.$$

Seja $m = mmc(a, b)$, ou seja, $m = ca$ e $m = db$ para c e d positivos. Logo

$$m^2 = (ca)^2 = ab \Rightarrow c^2 a = b \text{ ou } m^2 = (db)^2 = ab \Rightarrow d^2 b = a.$$

Somando membro a membro as igualdades acima, segue que

$$ab = d^2 b c^2 a \Rightarrow d^2 \cdot (c^2 a) = a \Rightarrow (cd)^2 = 1 \Rightarrow c = d = 1.$$

Portanto $a = b$.

Reciprocamente, se $a = b$ então $mmc(a, b) = mmc(a, a) = a$ e $mdc(a, b) = mdc(a, a) = a$. Portanto $mdc(a, b) = mmc(a, b)$.

5.3 MDC E MMC Para Vários Inteiros

A definição de *mdc* e *mmc* de dois inteiros se estende para mais de dois inteiros assim como sua caracterização e propriedades.

Um número inteiro positivo d é o *mdc* de $a_1, ..., a_n$ se possuir as propriedades:

a) d é divisor comum de $a_1, a_2, \ldots, a_n$;

a) Se d' é divisor comum de $a_1, a_2, \ldots, a_n$, então $d' \mid d$.

Do mesmo modo, número inteiro positivo m é o mmc de $a_1, ..., a_n$ se possuir as propriedades:

a) m é múltiplo comum de $a_1, a_2, \ldots, a_n$;

a) Se m' é múltiplo comum de $a_1, a_2, \ldots, a_n$, então $m \mid m'$.

Proposição 5.8. Se $a_1, \ldots, a_n$, são números inteiros positivos então:

a) $mdc(a_1, \ldots, a_{n-1}, a_n) = mdc(a_1, \ldots, mdc(a_{n-1}, a_n))$;

b) $mmc(a_1, \ldots, a_{n-1}, a_n) = mmc(a_1, \ldots, mmc(a_{n-1}, a_n))$;

A demonstração dessa proposição foge aos objetivos desse texto, entretanto mostraremos um caso particular para três inteiros positivos.

Proposição 5.9. Se a_1, a_2, a_3 são inteiros positivos então,

a) $mdc(a_1, a_2, a_3) = mdc(a_1, mdc(a_2, a_3))$;

b) $mmc(a_1, a_2, a_3) = mmc(a_1, mmc(a_2, a_3))$.

Demonstração. Demonstraremos cada item separadamente:

a) Seja $mdc(a_1, a_2, a_3) = d$ e $mdc(a_1, mdc(a_2, a_3)) = d'$. Tomando $mdc(a_1, a_2, a_3) = d$ temos que $d \mid a_1$, $d \mid a_2$ e $d \mid a_3$. Pela caracterização do mdc segue que $d \mid a_1$ e $d \mid mdc(a_2, a_3)$, novamente pela caracterização do mdc obtemos $d \mid mdc(a_1, mdc(a_2, a_3))$, ou seja, $d \mid d'$. Por outro lado, tomando $mdc(a_1, mdc(a_2, a_3)) = d'$, segue que $d' \mid a_1$ e $d' \mid mdc(a_2, a_3)$. Pela definição do mdc, segue que $d' \mid a_1$, $d' \mid a_2$ e $d' \mid a_3$, pela caracterização do mdc segue que $d' \mid mdc(a_1, a_2, a_3)$, ou seja $d' \mid d$. Como $d \mid d'$ e $d' \mid d$ com d, d' positivos, segue que $d = d'$, ou seja, $mdc(a_1, mdc(a_2, a_3)) = mdc(a_1, a_2, a_3)$.

b) Seja $mmc(a_1, a_2, a_3) = m$ e $mmc(a_1, mmc(a_2, a_3)) = m'$. Tomando $mmc(a_1, a_2, a_3) = m$ temos que $a_1 \mid m$, $a_2 \mid m$ e $a_3 \mid m$. Pela caracterização do mmc segue que $a_1 \mid m$ e $mmc(a_2, a_3) \mid m$, novamente pela caracterização do mmc obtemos $mmc(a_1, mmc(a_2, a_3)) \mid m$, ou seja, $m' \mid m$. Por outro lado, tomando $mmc(a_1, mmc(a_2, a_3)) = m'$, segue que $a_1 \mid m'$ e $mmc(a_2, a_3) \mid m'$. Como $a_2 \mid mmc(a_2, a_3)$ e $a_3 \mid mmc(a_2, a_3)$, segue que $a_1 \mid m'$, $a_2 \mid m'$ e $a_3 \mid m'$ e pela caracterização do mmc segue que $mmc(a_1, a_2, a_3) \mid m'$, ou seja $m \mid m'$. Como $m \mid m'$ e $m' \mid m$ com m, m' positivos, segue que $m = m'$, ou seja, $mmc(a_1, mmc(a_2, a_3)) = mmc(a_1, a_2, a_3)$.

□

Exemplo 5.13. Determine o mdc e o mmc de 2145,120 e 75.

Solução:

a) Vamos calcular primeiro o $mdc(2145, 120)$:

	17	1	
2145	120	105	15
105	15	0	

Agora calculamos o $mdc(75, 15)$:

	5	
75	15	
0		

Portanto o $mdc(2145, 120, 75) = 15$.

b) Vamos calcular primeiro o $mmc(2145, 120)$: Pela decomposição primária temos $2145 = 3 \cdot 5 \cdot 11 \cdot 13$ e $120 = 2^3 \cdot 3 \cdot 5$, logo $mmc(2145, 120) = 2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13 = 17160$.

Agora calculamos o $mdc(17160, 75)$: Pela decomposição primária temos $17160 = 2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13$ e $75 = 3 \cdot 5^2$, logo $mmc(17160, 75) = 2^3 \cdot 3 \cdot 5^2 \cdot 11 \cdot 13 = 85800$.

Observe que pela proposição anterior obteríamos o mesma resposta fatorando simultaneamente os três números.

5.4 Interpretação Geométrica do MDC E MMC

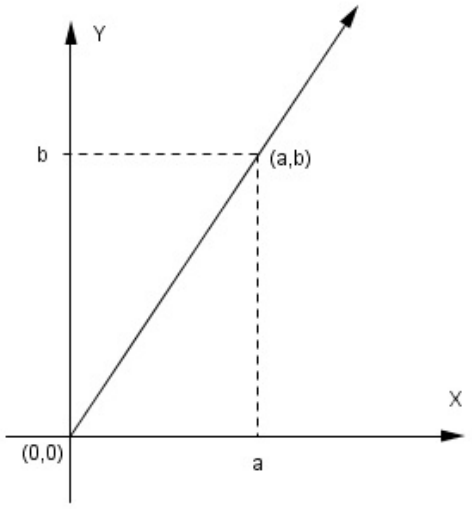
Pode-se utilizar várias interpretações para se consolidar um conhecimento matemático em sala de aula. Apesar do *mdc* e *mmc* serem de cunho essencialmente aritmético, eles podem ser interpretados geometricamente.

No 1º ano do Ensino Médio, os alunos estão consolidando conhecimentos básicos de geometria plana, nesse momento, o professor pode aproveitar para dar uma interpretação geométrica para *mdc* e *mmc*. A demonstração do resultado a seguir é mérito do Professor Marcelo Polezzi (12) em seu belo artigo publicado na Revista do Professor de Matemática. O resultado foi escrito como proposição como uma tentativa de facilitar o entendimento dos alunos do Ensino Médio. A justificativa da proposição é recomendada aos alunos do 3º ano de Ensino Médio já que utiliza conhecimentos oriundos da geometria analítica plana ou a alunos do 1º ano, caso tenham sólido conhecimento sobre funções afins.

Proposição 5.10. Seja a e b números interios positivos e S um retângulo cujas coordenadas dos vértices no plano cartesiano são $(0, 0)$, $(a, 0)$, $(0, b)$, (a, b). Se $d = mdc(a, b)$, então a diagonal de S pode ser dividida em d partes iguais de coordenadas inteiras e o $mmc(a, b)$ é a área de cada região retangular de base a e altura $\frac{b}{d}$ determinadas pelas "d" divisões de sua diagonal.

Demonstração. [3] Tomando um plano cartesiano e um par de coordenadas inteiras (x, y) como mostra a figura abaixo:

Figura 1 – Retângulo de coordenadas $(0,0)$, $(a,0)$, $(0,b)$, (a,b)



Fonte: O Autor

Seja m o coefiente angular da diagonal do retângulo, ou seja, $m = \frac{b}{a}$, logo:

$$y = mx \Rightarrow y = \frac{b}{a} \cdot x \Rightarrow \frac{x}{y} = \frac{a}{b}$$

Portanto, qualquer par de inteiros (p, q) que satisfaz a relação $\frac{p}{q} = \frac{a}{b}$ pertence a diagonal.

Seja $d = mdc(a, b)$. Logo existem u e v primos entre si tal que $a = du$ e $b = dv$. Isso acarreta que:

$$d = \frac{a}{u} = \frac{b}{v} \Rightarrow \frac{a}{b} = \frac{u}{v}.$$

Afirmamos que a diagonal do retângulo do gráfico acima fica dividida em d partes iguais. De fato, se (p, q) pertence a diagonal (com p e q inteiros e positivos), então

$$\frac{p}{q} = \frac{a}{b} = \frac{u}{v} \Rightarrow pv = uq.$$

Mas como $mdc(u, v) = 1$, isso acarreta que $q = rv$ e $p = ru$ com $0 \leq r \leq d$. Portanto a diagonal do retângulo fica dividida em d partes iguais e além disso ela possui $d + 1$ pares de inteiros não negativos (contando com o par $(0, 0)$).

Os $d + 1$ pontos de coordenadas inteiras da diagonal divide o retângulo S em d retângulos cuja base mede a. Chamando a área de cada um desses retângulos de A, obtemos

$$Ad = ab. \tag{5.1}$$

[3] POLEZZI, M. Como Obter o MDC e MMC sem Fazer Contas da RPM nº 51.

Mas

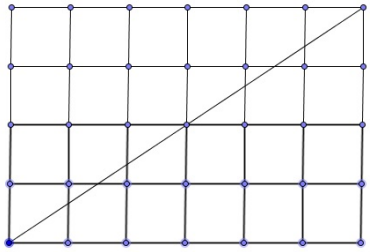
$$mdc(a,b) \cdot mmc(a,b) = ab. \tag{5.2}$$

Comparando (5.1) com (5.2) segue que $Ad = mdc(a,b) \cdot mmc(a,b) \Rightarrow mmc(a,b) = A$. □

Exemplo 5.14. Dê a interpretação geométrica do $mdc(6,4)$ e $mmc(6,4)$.

Solução: Basta fazer um retângulo de dimensões 6 e 4, traçar sua diagonal e verificar quais os pontos da diagonal que tem coordenadas inteiras:

Figura 2 – Retâgulo de dimensões 6x4



Fonte:O Autor

Como se vê existe um ponto de coordenadas inteiras que divide a diagonal em duas partes congruêntes logo o $mdc(6,4) = 2$. O $mmc(6,4)$ é a área de cada uma das partes dividida pela diagonal, logo $mmc(6,4) = 6 \cdot 2 = 12$.

6 O ENSINO DA DIVISÃO NA EDUCAÇÃO BÁSICA

Para suprir as necessidade dos alunos em aprender habilidades de cálculo, nas escolas brasileiras, o ensino de Aritmética é predominante nas séries iniciais. No 1º e 2º ciclo do Ensino Fundamental os alunos estudam as operações aditivas (adição e subtração) e a multiplicação. No início do 3º ciclo do Ensino Fundamental o aluno entra em contato com a divisão.

Entretanto, o ensino da divisão não se consiste apenas em encontrar o quociente e o resto da divisão. Duas dessas situações-problemas ensinadas nas escolas, consistem em repartir em quantidades iguais (quotização) e na quantidade de grupos (partição). Cada uma dessas situações requer formas de raciocínio diferente e cabe aos professores desenvolverem estratégias para ajudar o aluno a interpretar em qual ideia se enquadra cada situação problema. Portanto, o ensino da divisão deve ser desenvolvido priorizando não a técnica de dividir e sim os significados para a mesma.

Para tornar as aulas sobre divisão e suas propriedades mais atrativas para os alunos, o professor pode utilizar jogos de competição entre seus alunos. O professor pode separar os alunos de sua sala em equipes mesclando alunos de capacidades cognitivas distintas e aplicando desafios as equipes: Quem efetua a divisão mais rápido? Qual equipe pode fatorar esse número mais rápido? Qual o maior divisor primo desse número? Quantos são os divisores naturais "m" ?

No entanto, o professor deve permitir que os alunos sempre procurem suas estratégias para a resolução de problemas sobre divisões. O professor deve lembrar aos alunos que a divisão exata é apenas um caso particular em que o resto da divisão é nulo e problemas cuja solução depende da manipulação do resto da divisão são tão fundamentais quanto problemas envolvendo o quociente.

Daí em diante, o aluno deve entrar em contato com temas que consolidam o estudo da divisão:

a) **Algoritmo da Divisão**: que fundamenta resultados importantes para o estudo da divisão como o lema dos restos, lema de Euclides e propriedades importantes sobre *mdc* e *mmc* de números inteiros;

b) **Teorema Fundamental da Aritmética**: fundamental para a demonstrar muitas propriedades concernente ao números inteiros tais como a obtenção dos divisores de qualquer número inteiro, fundamenta a demonstração da infinitude dos números primos, justifica o algoritmo para cálculo do *mdc* e *mmc* de dois números inteiros, entre outras.

Entretanto apesar da importância desses temas, eles são apresentados para os alunos de forma bem resumida e sem justificativa ainda no 3º ciclo do Ensino Fundamental, e

nos anos posteriores, esses temas são simplesmente esquecidos comprometendo não só a consolidação da aprendizagem sobre números inteiros como também a aprendizagem dos outros conjuntos numéricos (racionais, reais e complexos). Isso evidencia que a organização atual do ensino de Aritmética é inadequado ao nível de preparo dos alunos para a sua assimilação. Nesse contexto, se faz necessário rever o currículo de Aritmética na educação básica. O ensino precoce de temas centrais no estudo da Aritmética como o "Algoritmo da Divisão" e "Teorema Fundamental da Aritmética" não se mostra eficaz. É necessário desenvolver o ensino de Aritmética nas escolas durante toda a educação básica, e assim, dar tempo para que o professor ajude o aluno a consolidar esse conhecimento. A Aritmética é o primeiro ramo da Matemática ensinado aos alunos nas escolas, mas isso não quer dizer que deva ser o primeiro a ter o seu ensino encerrado.

6.1 O Ensino da Divisão e as Olimpíadas de Matemática

Uma das políticas públicas voltadas para a educação (em especial a educação matemática) é o incentivo a participação dos alunos em olimpíadas escolares.

No Brasil temos em destaque a OBM (Olimpíada Brasileira de Matemática) e a OBMEP (Olimpíada Brasileira de Matemática Para Escolas Públicas) nessa última participam na 1ª fase praticamente 100% dos alunos matriculados no 3º e 4º ciclos do Ensino Fundamental e no Ensino Médio em escolas públicas brasileiras e os 5% melhores na 1ª fase da olimpíada vão para a 2ª fase[1].

O objetivo dessas olimpíadas é encontrar potenciais talentos em matemática. Entretanto sem uma preparação adequada fica inviável a boa participação dos alunos em tais olimpíadas.

Questões sobre tópicos de Aritmética, dentre eles a divisão, estão sempre presente em tais olimpíadas. Segue algumas recomendações úteis para resolução de questões de olimpíadas envolvendo os estudos sobre divisão:

a) Muitos dos problemas sobre divisão envolvem o Teorema Fundamental da Aritmética;

b) O lema dos restos facilita muito o cálculo de restos de divisões de potências, multiplicações e somas por um número natural;

c) Em problemas envolvendo divisões de expressões algébricas por um número natural n, é de boa praxe examinar todos os restos possíveis da divisão pelo número n, ou seja, fazer um estudo de caso;

d) O lema de Euclides é muito utilizado para resolver problemas envolvendo *mdc* de expressões algébricas;

[1] Fonte: http://www.obmep.org.br. Acesso em 20 de Abril de 2014.

e) Muitos problemas envolvendo quadrados perfeitos podem ser resolvidos pelo o resto da divisão por 3 e 4. Quadrados perfeitos quando divididos por 3 ou 4 deixam resto 0 ou 1 (o leitor pode se sentir convidado a demonstrar esse resultado);

f) Apesar de sua simplicidade o algoritmo da divisão é um instrumento poderoso para resolver problemas e demonstrar resultados importantes.

Segue alguns exemplos de questões da OBM (Olimpíada Brasileira de matemática) abordando os tópicos estudados até aqui[2]:

Exemplo 6.1. (OBM – 2008) Quantos números inteiros positivos menores que 500 têm exatamente 15 divisores inteiros positivos?
A) 0 B) 1 C) 2 D) 3 E) 4

Solução: Pelo princípio fundamental da contágem bem como pelo Corolário 4.2, para um inteiro positivo ter exatamente 15 divisores positivos, os número precisam ser da seguinte forma: p^{14} e $p^2 \cdot q^4$. Como p^{14} é maior que 500 para todo $p > 2$, logo os números procurados são $2^2 \cdot 3^4 = 324$, $3^2 \cdot 2^4 = 144$, e $5^2 \cdot 2^4 = 400$. Portanto há 3 números que satizfazem as condições do problema.

Exemplo 6.2. (OBM – 2008) O quociente e o resto na divisão de 26097 por 25 são, respectivamente:
A) 1043 e 22 B) 1044 e 3 C) 143 e 22 D) 1044 e 22 E) 144 e 3

Solução: Como $26097 = 1043 \cdot 25 + 22$, o quociente procurado é 1043 e o respectivo resto é 22.

Exemplo 6.3. (OBM -2011) Quantos são os pares ordenados (a, b), com a, b inteiros positivos, tais que $a + b + mdc(a, b) = 33$?

Solução: Seja $d = mdc(a, b)$. A expressão acima fica da forma: $\frac{a}{d} + \frac{b}{d} + 1 = \frac{33}{d}$.
Como o primeiro membro é uma soma de números inteiros, sabemos que $d \mid 33$. Pelo lema de Euclides

$$\begin{aligned} mdc\left(\frac{33}{d} - 1, \frac{a}{d}\right) &= mdc\left(\frac{a}{d} + \frac{b}{d}, \frac{a}{d}\right) = mdc\left(\frac{b}{d}, \frac{a}{d}\right) = 1 \\ mdc\left(\frac{33}{d} - 1, \frac{b}{d}\right) &= mdc\left(\frac{a}{d} + \frac{b}{d}, \frac{b}{d}\right) = mdc\left(\frac{b}{d}, \frac{a}{d}\right) = 1. \end{aligned}$$

Agora basta encontrar os pares de inteiros (x, y) tal que $x+y = \frac{33}{d}-1$ com $mdc(\frac{33}{d}-1, x) = 1$ para cada d obtendo como solução $(a, b) = (dx, dy)$:

a) Se $d = 1$, então $x + y = 32$ tem 16 soluções (tomamos x ímpar);

[2] Fonte: Provas e Gabaritos em (13) www.obm.org.br. Acesso em 20 de Abril de 2014.

b) Se $d = 3$, então $x + y = 10$ tem 4 soluções (x não pode ser par nem múltiplo de 5);

c) Se $d = 11$, então $x + y = 2$ tem 1 solução;

d) Se $d = 33$, então $x + y = 0$ não tem solução (pois a e b devem ser positivos).

Portanto, existem 21 pares de soluções.

Exemplo 6.4. (OBM – 2006) O máximo divisor comum de todos os termos da seqüência $a_n = n^3 - n$, $n = 1, 2, 3, ...$ é:
A) 2 B) 3 C) 4 D) 5 E) 6

Solução: Fatorando a expressão $a_n = n^3 - n$, obtemos

$$a_n = n^3 - n = (n-1)n(n+1).$$

Logo o valor de $a_n = n^3 - n$ com $n = 1, 2, 3, ...$ é formado por três números consecutivos, ou seja, é divisível por 2 e por 3 consequentemente por 6. Como $6 = 2^3 - 2$ pela caracterização do *mdc* concluimos que 6 é o *mdc* da sequência pois nenhum $a_n = n^3 - n$ com $n > 2$ divide 6.

Exemplo 6.5. (OBM – 2011)O maior inteiro positivo n tal que (2011!)! é divisível por ((n!)!)! é:
A)3 B)4 C)5 D)6 E)7

Solução: Pela propriedade (viii) do divisor, se $a \mid b$ com a e b inteiros não negativos, então $a \leqslant b$. Mas se $a \leqslant b$, então $a! \leqslant b!$. No caso se $((n!)!)! \mid (2011!)!$, então $((n!)!)! \leqslant (2011!)!$. Por outro lado, como o fatorial é uma função crescente em $\mathbb{N}$ ocorre que $((n!)!)! \leqslant (2011!)! \Leftrightarrow n! \leqslant 2011$. Como $6! < 2011 < 7!$ concluimos que o valor máximo de n é 6.

Exemplo 6.6. (OBM – 2011) Os inteiros positivos 30, 72 e N possuem a propriedade de que o produto de quaisquer dois é divisível pelo terceiro. Qual o menor valor possível de N?

Solução: Pela propriedade (v) do divisor, se $30 \mid 72N$, então $5 \mid 12N$. Como $5 \nmid 12$ temos que $5 \mid N$. Do mesmo modo, se $72 \mid 30N$, então $12 \mid 5N$. Como $12 \nmid 5$ temos que $12 \mid N$. Logo N deve ser mútiplo de 60, ou seja, $N \geqslant 60$. Portanto o número procurado é 60.

Exemplo 6.7. (OBM – 2012) Os dois menores números primos da forma $n^2 + 5$ são $36 + 5 = 41$ e $144 + 5 = 149$. Qual é o terceiro menor primo dessa forma?

Solução: Se n é ímpar então $n^2 + 5$ é par e maior do que 2, ou seja, não é primo. Logo n é par. Pelo algoritmo da divisão, tomando o inteiro $k > 1$, n pode ser escrito das formas $3k$, $3k + 1$ e $3k + 2$. Analisando as duas últimas formas:

a) $n = 3k + 1$: Nesse caso, $n^2 + 5 = 9k^2 + 6k + 6$ que é um múltiplo de 3 maior do que 3, ou seja, não é primo;

b) $n = 3k + 2$: Do mesmo modo $n^2 + 5 = 9k^2 + 12k + 9$ que também é um múltiplo de 3 e maior do que 3, ou seja, não é primo.

Logo n é múltiplo de 3, e, portanto, é múltiplo de 6. Assim, os próximos candidatos a primo são

$$\begin{aligned} 18^2 + 5 &= 18^2 – 3^2 + 14 = (18 – 3)(18 + 3) + 14 = 15 \cdot 21 + 14 \\ 24^2 + 5 &= 24^2 – 3^2 + 14 = (24 – 3)(24 + 3) + 14 = 21 \cdot 27 + 14. \end{aligned}$$

Mas ambos são múltiplos de 7. O número $30^2 + 5$ é múltiplo de 5. O próximo número a ser testado é $36^2 + 5 = 1301$ que é o número primo procurado.

Exemplo 6.8. (OBM-2012) Quantos números inteiros positivos têm o número 9 como seu maior divisor, diferente do próprio número?

Solução: Todo múltiplo de 9 é múltiplo de 3, ou seja, é da forma $3k$ com $k \in \mathbb{Z}$. Dessa forma, k é um dos divisores desse número. Como k é menor do que $3k$, e pelos dados do problema, 9 é o maior divisor de $3k$ que é diferente de $3k$, então $k \leqslant 9$, ou seja, $3k \leqslant 27$. Os inteiros positivos que satisfazem essas condições são o 9, 18 e 27. Como o números deve ser diferente de 9 então apenas o 18 e o 27 satisfazem as condições do problema, ou seja, são 2 números.

Exemplo 6.9. (OBM – 2009) Considere o número inteiro positivo n tal que o número de divisores positivos do dobro de n é igual ao dobro do número de divisores positivos de n. Podemos concluir que n é:
a)um número primo
b)um número par
c)um número ímpar
d)um quadrado perfeito
e)um potência inteira de 2

Solução: Sendo $n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ a fatoração de n, então $2n = 2^{\alpha+1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Pelo Corolário 4.2, a quantidade de divisores positivos de n é

$$(\alpha + 1)(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1).$$

E a quantidade de divisores positivos de $2n$ é

$$(\alpha + 1 + 1)(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1).$$

Essa quantidade é o dobro da anterior quando

$$(\alpha+2)(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1) = 2(\alpha+1)(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1) \Rightarrow \alpha+2 = 2(\alpha+1) \Rightarrow \alpha = 0.$$

Logo, n não tem fatores 2. Portanto n é ímpar.

7 CONGRUÊNCIAS

Na educação básica, o aluno pode se deparar com perguntas do tipo:

a) O 112º e 235º dias do ano caem no mesmo dia da semana?

b) Qual o resto da divisão de 4^{100} por 6?

c) É possível saber se o números 56382639246293269632532 é divisível por 4 sem efetuar a divisão?

A primeira pergunta pode ser respondida com duas divisões simples, a segunda pergunta pode ser respondida com o lema dos restos e a terceira pergunta pode ser respondida com o critério de divisibilidade por 4. A noção de congruência, que foi apresentada por C. F. Gauss, na sua obra "Disquisitiones Arithmeticae" no ano de 1801, responde todas essas perguntas.

Como proposta para a continuação do estudo sobre divisão e suas propriedades dedicaremos atenção ao resto das divisões de números inteiros. O estudo de congruência é relegado ao ensino superior, entretanto as demonstrações e resultados apresentados aqui utilizam ideias ou conceitos oriundos das operações elementares, ou seja, com algumas restrições, é possível desenvolver o estudo das congruências na educação básica dando maior significado ao ensino da divisão.

O estudo das congruências é voltado para o resto das divisões e o ensino tradicional sobre divisão é focado em problemas cuja solução é a obtenção do quociente. Portanto, podemos dizer que o estudo das congruências na educação básica complementa o estudo da divisão.

Um dos objetivos desse trabalho é fornecer meios para o professor inserir o estudo das congruências como continuidade, desdobramento ou extensão do ensino da divisão. Essa proposta tem com objetivo de amadurecer a definição de divisão entre números inteiros, além do fato de que a congruência é útil em uma grande quantidade de aplicações práticas principalmente em olimpíadas de matemática.

Definição 7.1. (Congruência módulo m) Sejam a, b e $m \in \mathbb{Z}$ com $m > 1$. Dizemos que o número a é congruente a b módulo m, se m divide a diferença entre a e b, ou seja, $m \mid (a - b)$.

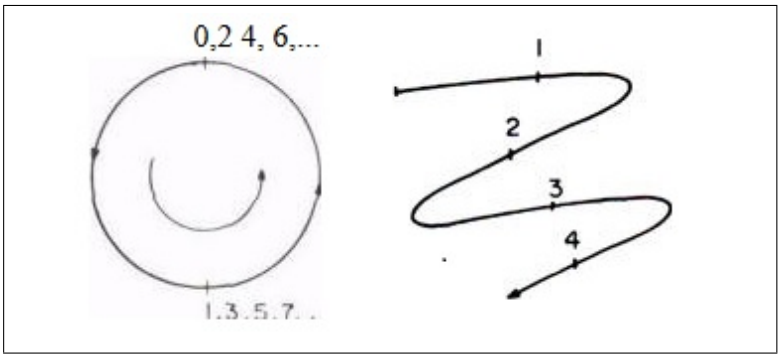
A notação $a \equiv b \; mod \; m$ representa que "a é congruente a b módulo m", ou seja,

$$a \equiv b \; mod \; m \Leftrightarrow m \mid (a - b) \Leftrightarrow a - b = mt \text{ para } t \in \mathbb{Z}.$$

Nesse trabalho usaremos as notação já consagrada para representar congruências. Caso um professor esteja interessado em trabalhar algumas propriedades das con-

gruências na educação básica, ele pode utilizar ou inserir símbolos e terminologia novos, mais simples e sugestivos aos alunos.

Figura 3 – Notações alternativas para as congruências



Fonte: Revista do Professor de Matemática Nº 10

Exemplo 7.1. $24 \equiv 6 \; mod \; 3$, pois $3 \mid (24 - 6)$.

A notação $a \not\equiv b \; mod \; m$, diz que a não é congruente (a é incongruente) a b módulo m, ou seja,

$$a \not\equiv b \; mod \; m \Leftrightarrow m \nmid (a - b).$$

Exemplo 7.2. $25 \not\equiv 8 \; mod \; 2$, pois $2 \nmid (25 - 8)$.

7.1 Aplicações da Definição de Congruências

Proposição 7.1. (Caracterização das congruências módulo m) Dois números inteiros a e b são congruentes modulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m.

Demonstração.
($\Rightarrow$) Supondo que $a \equiv b \; mod \; m$, resulta, pela definição de congruência, que

$$m \mid (a - b), \text{ ou seja } a - b = mt \text{ com } (t \in \mathbb{Z}). \tag{7.1}$$

Pelo algoritmo da divisão, se r é o resto da divisão de a por m então

$$a = mq + r \text{ com } (0 \leqslant r < m). \tag{7.2}$$

Substituindo (7.2) em (7.1) obtemos

$$(mq + r) - b = mt, \text{ ou ainda, } b = mq - mt + r = m(q - t) + r.$$

Portanto, a e b tem o mesmo resto quando divididos por m.

($\Rightarrow$) Reciprocamente, seja r o resto da divisão de a e b por m. Logo,

$$a = mk + r, \text{ com } k \in \mathbb{Z} \tag{7.3}$$

$$e$$

$$b = mt + r, \text{ com } k \in \mathbb{Z}. \tag{7.4}$$

Subtraindo (7.4) de (7.3) obtemos $a-b = (k-t)m$. Portanto, pela definição de congruência segue que $a \equiv b \ mod \ m$. □

A proposição acima evidencia a relação entre congruência e o resto da divisão. Notemos que todo número inteiro é congruente módulo m ao resto de sua divisão por m. De fato

$$(D = dm + r \text{ com } 0 \leqslant r < m) \Leftrightarrow (D \equiv r \ mod \ m).$$

Proposição 7.2. A congruência módulo m define uma relação de equivalência.

Demonstração. Basta mostrar que a congruência módulo m é reflexiva, simétrica e transitiva:

a) (Reflexiva) Com efeito, $a - a = 0$ e como $m \mid 0$ concluimos que $a \equiv a \ mod \ m$.

b) (Simétrica) Se $a \equiv b \ mod \ m$ então $a - b = tm$ com $(t \in \mathbb{Z})$. Como $b - a = -(tm) = (-t)m$ segue que $b \equiv a \ mod \ m$

c) (Transitiva) Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$ então $a-b = tm$ e $b-c = km$ com $(t, k \in \mathbb{Z})$. Portanto, $a - c = (a - b) + (b - c) = tm + km = (k + t)m$, ou seja, $a \equiv c \ mod \ m$.

□

7.2 Propriedades Operatórias das Congruências

A proposição abaixo mostra que a soma, subtração e multiplicação dos inteiros preservam a congruência módulo m.

Proposição 7.3. Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$. São válidas as seguintes propriedades:

a) Se $a \equiv b \ mod \ m$ então $a \pm c \equiv b \pm c \ mod \ m$ e $ac \equiv bc \ mod \ m$;

b) Se $a \equiv b \ mod \ m$ e se $c \equiv d \ mod \ m$, então $a \pm c \equiv b \pm d \ mod \ m$ e $ac \equiv bd \ mod \ m$.

Demonstração.

a) Pela definição de congruência, como $a \equiv b \; mod \; m$ temos que $a - b = tm$ para t inteiro. Como $a - b = (a \pm c) - (b \pm c)$, segue que $(a \pm c) \equiv (b \pm c) \; mod \; m$.

   Para a multiplicação, como $a \equiv b \; mod \; m$ temos que $a - b = tm$ para t inteiro. Logo $ac - bc = ctm$ o que implica em $m \mid (ac - bc)$. Portanto $ac \equiv bc \; mod \; m$.

b) Como $a \equiv b \; mod \; m$ e $c \equiv d \; mod \; m$ segue que $a - b = tm$ e $c - d = km$. Somando e subtraindo as expressões membro a membro obtemos $(a + c) - (b + d) = (t + k)m$ e $(a - c) - (b - d) = (t - k)m$. Portanto $a \pm c \equiv b \pm d \; mod \; m$.

   Para a segunda parte, multiplicamos a expressão $a - b = tm$ por c e a expressão $c - d = km$ por b. Em seguida somamos membro a membro obtendo $(a - b)c + (c - d)b = ctm + bkm$, o que implica em $ac - bd = (ct + bk)m$. Portanto $ac \equiv bd \; mod \; m$.

□

Corolário 7.1. Dados $a, b, m \in \mathbb{Z}$ (com $m > 1$), se $a \equiv b \; mod \; m$ com $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}^*$, então $a^n \equiv b^n \; mod \; m$;

Demonstração. Usaremos indução sobre n. Para $n = 1$ o resultado é óbvio. Suponhamos que o resultado seja válido para $k > 1$, onde k é um inteiro, ou seja, $a^k \equiv b^k \; mod \; m$. Usando o item (b) da Proposição 7.3 obtemos $(a^k)a \equiv (b^k)b \; mod \; m$, ou seja, $a^{k+1} \equiv b^{k+1} \; mod \; m$. Portanto $a^n \equiv b^n \; mod \; m$ para $a, b, n, m \in \mathbb{Z}$. □

Proposição 7.4. Se $ac \equiv bc \; mod \; m$ e $mdc(c, m) = d$, então $a \equiv b \; mod \; \frac{m}{d}$.

Demonstração. Se $ac \equiv bc \; mod \; m$, então $ac - bc = (a - b)c = km$, com $k \in \mathbb{Z}$. Se $mdc(c, m) = d$, então existe inteiros r e s tais que $c = dr$ e $m = ds$, onde r e s são primos entre si (veja o Corlário 5.2). Logo, $(a-b)dr = kds \Rightarrow (a-b)r = ks$. Mas isso implica que $s \mid (b-a)r$. Como o $mdc(r, s) = 1$ segue que $s \mid (b - a) \Rightarrow a \equiv b \; mod \; s$ com $s = \frac{m}{d}$. Portanto $a \equiv b \; mod \; \frac{m}{d}$. □

Corolário 7.2. Se $ac \equiv bc \; mod \; m$ e se $mdc(c, m) = 1$, então $a \equiv b \; mod \; m$.

Demonstração. Basta fazer $d = 1$ na Proposição 7.4. □

Essa propriedade garante o cancelamento de fatores em ambos os membros de uma congruência se eles são primos com o módulo.

Proposição 7.5. Seja $a, b, n, m \in \mathbb{Z}$, com $m, n > 1$, então:

a) Se $a \equiv b \; mod \; m$ e $n \mid m$, então $a \equiv b \; mod \; n$.

b) Se $a \equiv b \; mod \; m$, então $mdc(a, m) = mdc(b, m)$.

Demonstração. Sem perda de generalidade, tomaremos $b \leqslant a$.

a) Pela definição de congruência, vale que $m \mid (a - b)$. Como $n \mid m$, resulta que $n \mid (a - b)$. Portanto $a \equiv b \; mod \; n$.

b) Pela definição das congruências, se $a \equiv b \ mod \ m$, então $a-b = mk$, ou seja, $a = mk+b$ para $k \in \mathbb{Z}$. Pelo lema de Euclides obtemos $mdc(a,m) = mdc(mk+b,m) = mdc(b,m)$.

□

Segue abaixo alguns exemplos sobre congruência que o professor pode aplicar aos seus alunos de Ensino Médio.

Exemplo 7.3. Mostre que $10^{200} - 1$ é divisível por 11.

Solução: Usando a congruência módulo m obtemos

$$10 \equiv -1 \ mod \ 11 \Rightarrow 10^{200} \equiv (-1)^{200} \ mod \ 11 \Rightarrow 10^{200} \equiv 1^{200} \ mod \ 11 \Rightarrow 10^{200} - 1 \equiv 0 \ mod \ 11.$$

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

Exemplo 7.4. (FOMIN, D. 2012, p. 105) Encontre o resto da divisão de $10^{10} + 10^{100} + 10^{1000} + ... + 10^{10000000000}$ por 7.

Solução: Provemos por indução em $n \in \mathbb{N}$ que $10^{10^n} \equiv 4 \ mod \ 7$.

a) Para $n = 1$: $10^{10^1} \equiv 3^{10} = (3^2)^5 \equiv 2^5 \equiv 4 \ mod \ 7$, ou seja, o resultado é verdadeiro;

b) Supondo que o resultado seja verdadeiro para algum $k \in \mathbb{N}$: $10^{10^k} \equiv 4 \ mod \ 7 \Rightarrow 10^{10^{k+1}} \equiv 4^{10} = 16^5 \equiv 2^5 \equiv 4 \ mod \ 7$. Portanto $10^{10^n} \equiv 4 \ mod \ 7$ para $n \in \mathbb{N}$.

Voltando a questão, pela Proposição 7.3 e pelo reultado anterior, $10^{10} + 10^{100} + 10^{1000} + ... + 10^{10000000000} \equiv 4.10 \equiv 5 \ mod \ 7$. Portanto o resto da divisão de $10^{10} + 10^{100} + 10^{1000} + ... + 10^{10000000000}$ por 7 é 5.

Exemplo 7.5. Calculando a soma dos algarismos de 2^{100}, em seguida calculando a soma dos algarismos do número resultante, e assim por diante, até sobrar um só algarismo. Qual o algarismo que sobrou?

Solução: Pelo critério de divisibilidade por 9 (que será visto logo mais adiante), um número é divisível por 9 se a soma dos algarismos desse número também o for. Logo

$$\begin{aligned} 2^5 &\equiv 5 \ mod \ 9 \Rightarrow 2^{10} \equiv 5^2 \ mod \ 9 \Rightarrow 2^{10} \equiv 7 \ mod \ 9 \Rightarrow 2^{20} \equiv 7^2 \ mod \ 9 \Rightarrow \\ 2^{20} &\equiv 4 \ mod \ 9 \Rightarrow 2^{100} \equiv 4^5 \ mod \ 9 \Rightarrow 2^{100} \equiv 7 \ mod \ 9. \end{aligned}$$

Portanto o último algarismo restante é 7.

Exemplo 7.6. (REVISTA EUREKA nº 4) Determine todos os valores do natural n, para os quais $2^n + 1$ é múltiplo de 3.

Solução: Observe que $2 \equiv (-1) \ mod \ 3$. Logo, pela Proposição 7.3 e pelo Corolário 7.1, segue que $2 \equiv (-1) \ mod \ 3 \Rightarrow 2^n \equiv (-1)^n \ mod \ 3 \Rightarrow 2^n + 1 \equiv (-1)^n + 1 \ mod \ 3$.

Portanto, $2^n + 1 \equiv 0 \ mod \ 3$ se n é ímpar.

7.3 Congruências Lineares

Na educação básica, mais especificamente no 3º e 4º ciclo do Ensino Fundamental, o professor inicia o estudo das equações do primeiro grau com duas variáveis da forma $ax + by = c$ com $a, b, c \in \mathbb{Z}$. Essas equações são utilizadas para resolver problemas tais como:

a) De quantos modos podemos organizar 30 bolinhas em grupos de 4 ou 5 bolinhas?

b) Uma garota recebeu R$ 50,00 para comprar dois tipos de lanches. Depois de pesquisar, conseguiu o preço de R$ 4,00 por hambúrguer e de R$ 6,00 por um sorvete. De quantas maneiras ela pode comprar esses lanches?

c) Para levar 200 turistas para um passeio, dispomos de carros e vans. Cada carro pode levar 4 turistas e cada van pode levar 18 turistas. De quantos modos podemos distribuir os turistas nos carros e vans? Se o custo do da van é o triplo do carro, qual a quantidade mas vantajosa financeiramente de levar os turista?

O ensino das equações de duas variáveis em $\mathbb{Z}$ na educação básica tradicional é feita usando o método das tentativas. Esse modo é cansativo para os alunos e não mostra a estrutura das soluções. Mas usando a notação de congruência obtemos

$$ax + by = c \Leftrightarrow ax - c = b(-y) \Leftrightarrow ax \equiv c \ mod \ b. \tag{7.5}$$

Logo os problemas acima podem ser estudados com as congruências. A equação obitida em (7.5) é chamada de congruência linear.

Definição 7.2. Chama-se congruência linear toda equação da forma $ax \equiv b \ mod \ m$, onde $a, b, m \in \mathbb{Z}$ com $m > 1$.

Se um inteiro x_0 satatisfaz a relação $ax_0 \equiv b \ mod \ m$ então x_0 é uma solução da congruência linear $ax \equiv b \ mod \ m$.

7.3.1 *Relação das Congruências Lineares e Equações Diofantinas*

Definição 7.3. Chama-se equação diofantina linear do primeiro grau com duas incógnitas, as equações da forma $ax + by = c$, onde a, b e c são números inteiros e x e y são incógnitas a serem determinadas em $\mathbb{Z}$.

Precisamos agora de uma ferramenta que nos permita definir se uma equação diofantina linear tem ou não solução. Os próximos dois resultados logo abaixo são dados em Filho (9).

Teorema 7.1. [1] A equação diofantina linear $ax + by = c$ tem solução se e somente se, d divide c, sendo $mdc(a, b) = d$.

[1] FILHO, 1981 p. 138

Demonstração. Supondo que a equação $ax + by = c$ tem uma solução, isto é existe um par de inteiros (x_0, y_0) tal que $ax_0 + by_0 = c$. Por ser $mdc(a, b) = d$, existem inteiros p e q tais que $a = dp$ e $b = dq$, logo $c = ax_0 + by_0 = dpx_0 + dqy_0 = d(px_0 + qy_0)$. Como p, x_0, q, y_0 são inteiros, segue que $px_0 + qy_0$ é um inteiro, portanto $d \mid c$.

Reciprocamente, suponhamos que d divide c ($d \mid c$) isto é, $c = dt$, onde t é um inteiro. Por ser $mdc(a, b) = d$, existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$. O que implica, $c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0)$. Isto é, o par de inteiros $x = tx_0 = \frac{c}{d}x_0$ e $y = ty_0 = \frac{c}{d}y_0$, é solução da equação $ax + by = c$. □

Se c for o maior divisor comum de a e b, então esta equação associa-se a **Identidade de Bézout**, o que a caracteriza como uma equação diofantina com soluções.

A proposição a seguir nos fornece um meio para encontrar as soluções de equações diofantinas lineares de duas variáveis e isso é dado pela proposição a seguir.

Proposição 7.6. [2] Se d divide c sendo $mdc(a, b) = d$ e se o par de inteiros x_0 e y_0 é uma solução particular da equação diofantina $ax + by = c$, então todas as demais soluções dessa equação são da forma

$$x = x_0 + \frac{b}{d}t \quad \text{e} \quad y = y_0 - \frac{a}{d}t, \text{ com } t \in \mathbb{Z}.$$

Demonstração. Suponhamos que o par de inteiros x_0 e y_0 uma solução particular da equação $ax + by = c$, e seja x_1 e y_1 outra solução da equação. Logo,

$$ax_0 + by_0 = ax_1 + by_1 = c \Rightarrow a(x_1 - x_0) = b(y_0 - y_1). \tag{7.6}$$

Como $mdc(a, b) = d$, existem inteiros p e q coprimos tais que $a = dp$ e $b = dq$. Substituindo esses valores em (7.6) e cancelando d obtemos

$$p(x_1 - x_0) = q(y_0 - y_1).$$

Como p e q coprimos, temos que $q \mid (x_1 - x_0)$ e $p \mid (y_0 - y_1)$, ou seja, $(x_1 - x_0) = qt$ e $(y_0 - y_1) = pt$. Portanto,

$$\begin{aligned} p(x_1 - x_0) &= q(y_0 - y_1) \Rightarrow x_1 - x_0 = qt \Rightarrow x_1 = x_0 + \frac{b}{d}t; \\ p(x_1 - x_0) &= q(y_0 - y_1) \Rightarrow y_0 - y_1 = pt \Rightarrow y_1 = y_0 - \frac{a}{d}t. \end{aligned}$$

Esses valores de x_1 e y_1 satisfazem realmente a equação $ax + by = c$, para qualquer inteiro t, pois temos

$$a_1 + by_1 = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 + a\frac{b}{d} - b\frac{a}{d} = c$$

□

[2] FILHO, 1981 p. 140

Corolário 7.3. Se o par de inteiros x_0 e y_0 é uma solução particular da equação diofantina $ax + by = c$, com $mdc(a, b) = 1$, então todas as demais soluções dessa equação são da forma

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

Demonstração. Basta substituir o $mdc(a, b) = 1$ em d no resultado da Proposição 7.6 obtendo o resultado. □

Na prática, para se resolver uma equação diofantina linear da forma $ax + by = c$, calculamos o $mdc(a, b) = d$. Se $d \nmid c$ paramos o processo (a equação não tem solução). Se $d \mid c$, ou seja $c = kd$ para k inteiro, continuamos o procedimento. Em seguida utilizamos o algoritmo de Euclides para encontrar uma solução particular de $ax + by = d$, que pela identidade de Bézout, sempre tem solução. Para encerrar o procedimento, se x_1 e y_1 é uma solução particular de $ax + by = d$, então $ax_1 + by_1 = d$, logo basta multiplicar a equação anterior por k para obter $x_0 = kx_1$ e $y_0 = ky_1$ que é uma solução particular da equação original. Finalmente usamos a Proposição 7.6 ou o Corolário 7.3, se for o caso.

Exemplo 7.7. Um aluno foi encarregado de remanejar todos os livros de uma estante da biblioteca de sua escola. Se ele retirar os livros de dois em dois sobrará um livro na estante e se ele retirar os livros de três em três sobrará dois livros na estante. Quantos livros havia nessa estante se cada estante da biblioteca cabem no máximo 50 livros e por economia de espaço cada estante deve ter pelo menos 40 livros?

Solução: Seja n o número de livros dessa estante. Pelos dados do problema e usando o algoritmo da divisão segue que

$$n = 2x + 1 \text{ e } n = 3y + 2 \Rightarrow 2x + 1 = 3y + 2 \Rightarrow 2x - 3y = 1. \tag{7.7}$$

Por inspeção, uma solução particular da equação (7.7) é $x_o = 2$ e $y_o = 1$. Logo a solução geral é $x = 2 - 3t$ e $y = 1 + 2t$ para $t \in \mathbb{Z}$. Como cada estante tem pelo menos 40 livros e no máximo 50 isso acarreta que:

$$n = 2x + 1 = 2(2 - 3t) + 1 = 5 - 6t \Rightarrow 40 \leqslant 5 - 6t \leqslant 50 \Rightarrow -7 \leqslant t \leqslant -6$$

Portanto temos duas possibilidade para o valor de t:

a) Para $t = -6$: o número de livros é $n = 5 - 6t = 5 - 6(-6) = 41$;

b) Para $t = -7$: o número de livros é $n = 5 - 6t = 5 - 6(-7) = 47$.

Exemplo 7.8. Mostre que nenhum número inteiro pode deixar resto 5 quando dividido por 12 e resto 4 quando dividido por 15.

Solução: Supondo que exista um número inteiro n que deixa resto 5 quando dividido por 12 e resto 4 quando dividido por 15. Pelo algoritmo da divisão segue que

$$n = 15x + 4 \text{ e } n = 12y + 5 \Rightarrow 15x + 4 = 12y + 5 \Rightarrow 15x - 12y = 1. \tag{7.8}$$

Mas o $mdc(15, 12) = 3$ e $3 \nmid 1$ e pelo Teorema 7.1 a equação diofantina (7.8) não tem solução. Contradição.

Voltando ao estudo das congruências, o número x_0 é solução da congruência linear $ax \equiv b \; mod \; m$ se e somente se $m \mid (ax_0 - b)$, logo, existe um inteiro y_o tal que $ax_0 - b = my_0$, ou seja, $ax_0 - my_0 = b$. Portanto, para encontrar todos os inteiros que satisfazem a congruência linear $ax \equiv b \; mod \; m$, basta obter as soluções da equação diofantina $ax - my = b$.

7.3.2 *Soluções das Congruências Lineares*

Toda congruência linear tem solução? A pergunta, é respondida pelo seguinte teorema dado em Filho(9):

Teorema 7.2. [3] A congruência linear $ax \equiv b \; mod \; m$ tem solução, se e somente se, d divide b ($d \mid b$), sendo $d = mdc(a, m)$.

Demonstração.
Supondo que a solução da congruência linear $ax \equiv b \; mod \; m$, tem como solução o inteiro x_0, isto é, $ax_0 \equiv b \; mod \; m$. Então existe um inteiro y_0 tal que $ax_0 - b = my_0$ o que implica em $ax_0 - my_0 = b$. Pelo Teorema 7.1 o resultado segue.

Reciprocamente, suponhamos que $d \mid b$, isto é, $b = dt$ com $t \in \mathbb{Z}$. Como o $mdc(a, m) = d$, existem inteiros x_0 e y_0 tais que $ax_0 + my_0 = d$. Agora multiplicando ambos os membros dessa última igualdade por t temos

$$a(tx_0) + m(ty_0) = dt = b \Rightarrow a(tx_0) - b = m(-ty_0) \Rightarrow a(tx_0) \equiv b \; mod \; m.$$

Isso mostra que a congruência $ax \equiv b \; mod \; m$ tem solução. □

As soluções de uma congruência linear estão associadas as soluções de uma equação diofantina linear. Se o $mdc(a, m)$ divide b, então a equação diofantina $ax - my = b$ tem infinitas soluções, o que implica que a congruência linear $ax \equiv b \; mod \; m$ tem infinitas soluções.

Exemplo 7.9. (HEFEZ, 2006, p. 144) Pode o dobro de um número natural deixar resto igual a 9 quando dividido por 26? E quando dividido por 25?

Solução:

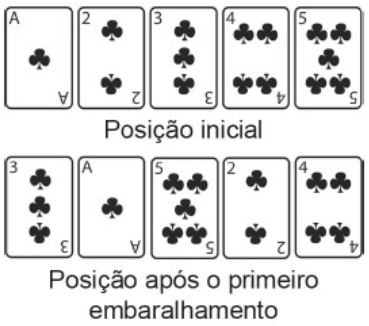
[3] FILHO, 1981, p. 167

a) Suponha que existe $x \in \mathbb{N}$ tal que $2x$ deixa resto igual a 9 quando dividido por 26. Logo $2x \equiv 9 \ mod \ 26$. Pelo Teorema 7.2 deveria ocorrer que $mdc(2, 26) \mid 9$. Mas isso é uma contradição. Portanto, o dobro de um número natural não pode deixar resto igual a 9 quando dividido por 26.

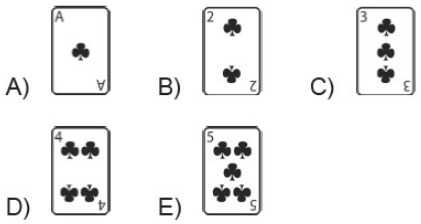
b) Suponha que existe $x \in \mathbb{N}$ tal que $2x$ deixa resto igual a 9 quando dividido por 25. Logo $2x \equiv 9 \ mod \ 25$. Pelo Teorema 7.2 deveria ocorrer que $mdc(2, 25) \mid 9$, o que é verdadeiro. Com efeito, $2x \equiv 9 \ mod \ 25 \Leftrightarrow 2x - 25y = 9$. Essa equação diofantina tem como solução particular os valores $x_0 = -108$ e $y_0 = -9$. Logo a solução geral da congruência linear é $x = -108 - 25t$ para $t \in \mathbb{Z}$. Como queremos soluções naturais, segue que $-108 - 25t \geqslant 0 \Rightarrow t \leqslant -5$. Portanto $-108 - 25 \cdot (-5) = 17$ é menor número natural cujo o dobro deixa resto igual a 9 quando dividido por 25.

Segue logo abaixo exemplos de aplicação das congruências lineares em questões de olimpíadas de matemática aplicadas no Ensino Médio.

Exemplo 7.10. (OBMEP 2012) Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas.



Em cada embaralhamento, a primeira carta passa a ser a segunda, a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira. Qual será a primeira carta após 2012 embaralhamentos?



Solução:De acordo com as regras do embaralhamento obtemos as seguintes posições das cartas:

a) A posição original das cartas: A2345;

b) 1º embaralhamento: 3A524

c) 2º embaralhamento: 534A2

d) 3º embaralhamento: 4523A

e) 4º embaralhamento: 24A53

f) 5º embaralhamento: A2345, no caso a posição original das cartas.

Como a cada 5 embaralhamentos a posição das cartas se repete, a solução do problema é dada pela menor número natural que é solução da congruência linear $2012 \equiv x \ mod \ 5$, ou seja:

$$\begin{aligned} 10 &\equiv 0 \ mod \ 5 \Rightarrow \\ 2010 &\equiv 0 \ mod \ 5 \Rightarrow \\ 2012 &\equiv 2 \ mod \ 5 \end{aligned}$$

Logo a posição das cartas após 2012 embaralhamentos é igual a posição após o 2º embaralhamento que é 534A2. Portanto a 1ª carta é o 5.

Exemplo 7.11. (Banco de Questões - OBMEP) As figuras △, ♣, ♢, ♠, ♡ e □ são repetidas indefinidadente na sequência

$$△, ♣, ♢, ♠, ♡, □, △, ♣, ♢, ♠, ♡, □, ...$$

a) Que figura aparecerá ná 1000ª posição da sequência?
b) Em que posição aparece o milésimo ♢?

Solução:
a) Devemos encontrar o menor número natural que é solução da congruência linear $1000 \equiv x \ mod \ 6$. Partindo de $10 \equiv 4 \ mod \ 6$ segue que

$$\begin{aligned} 10 &\equiv 4 \ mod \ 6 \Rightarrow \\ 10^3 &\equiv 4^3 \ mod \ 6 \Leftrightarrow \\ 1000 &\equiv 64 \ mod \ 6 \Rightarrow \\ 1000 &\equiv 4 \ mod \ 6 \end{aligned}$$

Portanto o símbolo procurado é o 4º, ou seja , ♠.
b) Como o 1º ♢ está na 3ª posição, o 2º ♢ está na $1 \cdot 6 + 3 = 9$ª posição,o 3º está na $2 \cdot 6 + 3 = 15$ª posição e assim por diante, o número procurado está na $999 \cdot 6 + 3 =$ posição . Portanto o milésimo ♢ ocupa a 5997ª posição.

7.4 Critérios de Divisibilidade

Os critérios de divisibilidade são ensinados no início do 3º ciclo do Ensino Fundamental para servir como ferramenta para o estudo posterior sobre divisões. No entanto o ensino dos critérios de divisibilidade são justificados apenas com exemplos de casos particulares . A justificativa para o uso de tal metodologia consiste no fato de que sem a teoria das congruências fica inviável efetuar as demonstrações de grande parte dos critérios de divisibilidade, contudo, durante toda educação básica tal assunto não é abordado e as regras de divisibilidade são apenas decoradas pelos alunos, privando-os de desenvolver sua criatividade e raciocínio lógico-matemático.

O estudo das congruências módulo m, permite que o aluno tenha ferramentas para demonstrar os critérios de divisibilidade contido nos livros bem como tentar estabelecer seus próprios critérios. O professor pode iniciar com as demonstrações dos primeiros critérios de divisibilidade no início do Ensino Médio quando os alunos já tem domínio sobre as propriedades e ideias oriundas da divisão.

Alguns dos critérios de divisibilidade abaixo podem ser demonstrados apenas com as propriedades de divisão porém, as congruências facilitam o trabalho.

Para discutir e demonstrar os critérios de divisibilidade é necessário que os alunos compreendam o sistema de numeração decimal posicional representado pela identidade

$$n = n_r n_{r-1} n_{r-2} n_1 n_0 = n_r 10^r + n_{r-1} 10^{r-1} + ... + n_1 10^1 + n_0 10^0 \tag{7.9}$$

O número escrito a direita é o número natural n escrito com algarismos na ordem estabelecida.

Basicamente, para demonstrar critérios de divisibilidade por um número natural m, devemos em cada parcela da soma do último membro de (7.9) aplicar a congruência módulo m e somar todas as congruências. Lembrando que um critério de divisibilidade é eficaz apenas se ele for mais fácil de utilizar do que a própria divisão. Não é de nosso interesse exibir vários critérios de divisibilidade, pois essa tarefa é interminável, mas sim, mostrar uma ideia comum para a obtenção de todos os critérios e assim obter um método eficiente de construção.

7.4.1 *Critério de divisibilidade por 2,5 e 10*

Tomando o número n na base 10, $n = n_r 10^r + n_{r-1} 10^{r-1} + \cdots + n_1.10 + n_0$, basta observar que $10 \equiv 0 \; mod \; 2$, $10 \equiv 0 \; mod \; 5$, $10 \equiv 0 \; mod \; 10$. Pela Proposição 7.3 bem como pelo Corolário 7.1 da congruências, segue que

$$\begin{aligned} n_i 10^i &\equiv 0 \; mod \; 2 \\ n_i 10^i &\equiv 0 \; mod \; 5 \\ n_i 10^i &\equiv 0 \; mod \; 10. \end{aligned}$$

Onde $i \in \mathbb{N}$. Logo, $n_r 10^r + n_{r-1}10^{r-1} + \cdots + n_1 10 + n_0 \equiv n_0 \; mod \; 2, mod \; 5, mod \; 10$.

Portanto, n_0 (no caso o último algarismo de n) deve ser divisível por 2, 5 ou 10.

7.4.2 *Critério de divisibilidade por 3,9*

Tomando o número n na base 10, $n = n_r 10^r + n_{r-1}10^{r-1} + \cdots + n_1.10 + n_0$, basta observar que $10 \equiv 1 \; mod \; 3$ e $10 \equiv 1 \; mod \; 9$. Pela Proposição 7.3 bem como pelo Corolário 7.1, segue que

$$\begin{aligned} n_i 10^i &\equiv n_i \; mod \; 3 \\ n_i 10^i &\equiv n_i \; mod \; 9. \end{aligned}$$

Onde $i \in \mathbb{N}$. Agora observe que

$$\begin{aligned} n_0 &\equiv n_0 \; mod \; 3, mod \; 9 \\ n_1 10^1 &\equiv n_1 \; mod \; 3, mod \; 9 \\ &\vdots \\ n_{r-1} \; 10^{r-1} &\equiv n_{r-1} \; mod \; 3, mod \; 9 \\ n_r 10^r &\equiv n_r \; mod \; 3, mod \; 9. \end{aligned}$$

Somando membro a membro as congruências acima segue que

$$n \equiv n_r + n_{r-1} + \cdots + n_1 + n_0 \; mod \; 3, mod \; 9.$$

Portanto, n é divisível por 3 ou 9 se $n_r + n_{r-1} + \ldots + n_1 + n_0$ (a soma dos algarismos de n) é divisível por 3 ou por 9.

7.4.3 *Critério de divisibilidade por 7*

Pelo Corolário 7.1 tem-se que $1000 = 10^3 \equiv -1 \; mod \; 7$. Tomando o número n na base 10, $n = n_r 10^r + n_{r-1}10^{r-1} + \cdots + n_1 10 + n_0$ e $i \in \mathbb{N}$ tem-se

$$\left(10^3\right)^i \equiv (-1)^i \; mod \; 7 \Rightarrow \begin{cases} 10^{3i} \equiv 1 \; mod \; 7, \text{ se i for par} \\ 10^{3i} \equiv -1 \; mod \; 7, \text{ se i for impar} \end{cases}$$

Separando as classes (unidades simples, milhar, milhão,...) de n e aplicando as congruências obtemos

$$\begin{aligned} n &\equiv \left(\cdots + n_8 n_7 n_6 \left(10^3\right)^2 + n_5 n_4 n_3 \left(10^3\right)^1 + n_2 n_1 n_0 \left(10^3\right)^0\right) \; mod \; 7 \\ &\Rightarrow \quad n \equiv (... + n_8 n_7 n_6 - n_5 n_4 n_3 + n_2 n_1 n_0) \; mod \; 7 \end{aligned}$$

Portanto, n é divisível por 7 se a soma das classe ímpares menos a soma das classes pares de n for divisível por 7.

7.4.4 *Critério de divisibilidade por 8*

Tomando o número n na base 10, $n = n_r 10^r + n_{r-1}10^{r-1} + \cdots + n_1 10 + n_0$ e aplicando a congruência módulo 8 as potências de 10 obtemos

$$\begin{aligned} 10^0 &\equiv 1 \ mod\ 8 \\ 10^1 &\equiv 2 \ mod\ 8 \text{ ou } 10^1 \equiv -6 \ mod\ 8 \\ 10^2 &\equiv 4 \ mod\ 8 \text{ ou } 10^2 \equiv -4 \ mod\ 8 \\ 10^3 &\equiv 0 \ mod\ 8 \text{ ou } 10^3 \equiv 0 \ mod\ 8 \\ 10^4 &\equiv 0 \ mod\ 8 \text{ ou } 10^4 \equiv 0 \ mod\ 8 \\ &\vdots \end{aligned}$$

Mas pela Proposição 7.3, isso implica que

$$\begin{aligned} n_0 10^0 &\equiv 1n_0 \ mod\ 8 \\ n_1 10^1 &\equiv 2n_1 \ mod\ 8 \text{ ou } n_1 10 \equiv -6n_1 \ mod\ 8 \\ n_2 10^2 &\equiv 4n_2 \ mod\ 8 \text{ ou } n_2 10^2 \equiv -4n_2 \ mod\ 8 \\ n_3 10^3 &\equiv 0 \ mod\ 8 \text{ ou } n_3 10^3 \equiv 0 \ mod\ 8 \\ n_4 10^4 &\equiv 0 \ mod\ 8 \text{ ou } n_4 10^4 \equiv 0 \ mod\ 8 \\ &\vdots \\ n = n_0 10^0 + n_1 \cdot 10^1 + n_2 10^2 + n_3 10^3 + ... &\equiv 1n_0 + 2n_1 + 4n_2 \ mod\ 8 \\ &ou \\ n = n_0 10^0 + n_1 10^1 + n_2 10^2 + n_3 10^3 + ... &\equiv 1n_0 - 6n_1 - 4n_2 \ mod\ 8 \end{aligned}$$

Portanto, n é divisível por 8 se

a) O algarismo da unidade somado com duas vezes o algarismo da dezena e a quatro vezes o algarismo da centena for divisível por 8;

b) O algarismo da unidade menos seis vezes o algarismo da dezena menos quatro vezes o algarismo da centena for divisível por 8.

7.4.5 *Critério de divisibilidade por 11*

Basta observar que $11 = 10 + 1 \equiv 0 \ mod\ 11$ e pelo Corolário 7.1, com $i \in \mathbb{N}$ temos que $10^{2i} \equiv 1 \ mod\ 11$(I). Usando a relação $10^{2i+1} + 1^{2i+1} = (10+1)\cdot(10^{2i} - 1 \cdot 10^{2i-1} + ... - 1^{2i-1}10 + 1^{2i})$ e que $11 \mid (10+1)$, acarreta que $11 \mid (10^{2i+1} + 1^{2i+1})$. Portanto $10^{2i+1} + 1 \equiv 0 \ mod\ 11$(II).

Tomando o número n na base 10, $n = n_r 10^r + n_{r-1}10^{r-1} + \cdots + n_1 \cdot 10 + n_0$ e os resultados de (I) e (II), bem como pela Proposição7.3, obtemos,

$$\begin{aligned} n_0 &\equiv n_0 \ mod\ 11 \\ n_1(10+1) = 10n_1 + n_1 &\equiv 0 \ mod\ 11 \\ 10^2 n_2 &\equiv n_2 \ mod\ 11 \\ n_3(10^3+1) = 10^3 n_3 + n_3 &\equiv 0 \ mod\ 11 \\ &\vdots \end{aligned}$$

Somando membro a membro as congruências segue que

$$n + n_1 + n_3 + \cdots \equiv n_0 + n_2 + \cdots \ mod\ 11.$$

Como n é divisível por 11 se e somente se, $n \equiv 0 \ mod\ 11$, pela expressão acima segue que

$$n_1 + n_3 + \cdots \equiv n_0 + n_2 + \cdots \ mod\ 11.$$

Portanto, o número n é divisível por 11, se a soma dos seus algarismos de ordem par menos a soma de seus algarismos de ordem ímpar é divisível por 11.

7.4.6 *Critério de divisibilidade por 13*

Tomando o número n na base 10, $n = n_r 10^r + n_{r-1}10^{r-1} + \cdots + n_1.10 + n_0$ e aplicando a congruência módulo 13 as potências de 10 obtemos

$$\begin{aligned} 10^0 &\equiv 1 \ mod\ 13 \\ 10^1 &\equiv 10 \ mod\ 13 \text{ ou } 10^1 \equiv -3 \ mod\ 13 \\ 10^2 &\equiv 9 \ mod\ 13 \text{ ou } 10^2 \equiv -4 \ mod\ 13 \\ 10^3 &\equiv 12 \ mod\ 13 \text{ ou } 10^3 \equiv -1 \ mod\ 13 \\ 10^4 &\equiv 3 \ mod\ 13 \text{ ou } 10^4 \equiv -10 \ mod\ 13 \\ 10^5 &\equiv 4 \ mod\ 13 \text{ ou } 10^5 \equiv -9 \ mod\ 13 \\ 10^6 &\equiv 1 \ mod\ 13 \text{ ou } 10^6 \equiv -12 \ mod\ 13 \\ 10^7 &\equiv 10 \ mod\ 13 \text{ ou } 10^7 \equiv -3 \ mod\ 13 \\ 10^8 &\equiv 9 \ mod\ 13 \text{ ou } 10^8 \equiv -4 \ mod\ 13 \\ 10^9 &\equiv 2 \ mod\ 13 \text{ ou } 10^9 \equiv -1 \ mod\ 13 \\ 10^{10} &\equiv 3 \ mod\ 13 \text{ ou } 10^{10} \equiv -10 \ mod\ 13 \\ &\vdots \end{aligned}$$

Mas pela Proposição 7.3, isso implica que

$$\begin{aligned}
n_0 10^0 &\equiv 1n_0 \ mod\ 13 \\
n_1 10^1 &\equiv 10n_1 \ mod\ 13 \text{ ou } n_1 10^1 \equiv -3n_1 \ mod\ 13 \\
n_2 10^2 &\equiv 9n_2 \ mod\ 13 \text{ ou } n_2 10^2 \equiv -4n_2 \ mod\ 13 \\
n_3 10^3 &\equiv 12n_3 \ mod\ 13 \text{ ou } n_3 10^3 \equiv -1n_3 \ mod\ 13 \\
n_4 10^4 &\equiv 3n_4 \ mod\ 13 \text{ ou } n_4 10^4 \equiv -10n_4 \ mod\ 13 \\
n_5 10^5 &\equiv 4n_5 \ mod\ 13 \text{ ou } n_5 10^5 \equiv -9n_5 \ mod\ 13 \\
n_6 10^6 &\equiv 1n_6 \ mod\ 13 \text{ ou } n_6 10^6 \equiv -12n_6 \ mod\ 13 \\
n_7 10^7 &\equiv 10n_7 \ mod\ 13 \text{ ou } n_7 10^7 \equiv -3n_7 \ mod\ 13 \\
n_8 10^8 &\equiv 9n_8 \ mod\ 13 \text{ ou } n_8 10^8 \equiv -4n_8 \ mod\ 13 \\
n_9 10^9 &\equiv 2n_9 \ mod\ 13 \text{ ou } n_9 10^9 \equiv -1n_9 \ mod\ 13 \\
n_{10} 10^{10} &\equiv 3n_{10} \ mod\ 13 \text{ ou } n_{10} 10^{10} \equiv -10n_{10} \ mod\ 13 \\
&\vdots
\end{aligned}$$

Agrupando os segundos membros de cada uma das congruências acima podemos concluir que o número n é divisível por 13 se o número abaixo for divisível por 13.

$$(n_0 + 3n_4 + 4n_5 + n_6 + 2n_9) - (3n_1 - 4n_2 - 1n_3 - 3n_7 - 4n_8) + \ldots$$

7.4.7 *Critério de divisibilidade por 16*

Tomando o número n na base 10, $n = n_r 10^r + n_{r-1} 10^{r-1} + \cdots + n_1 10 + n_0$ e aplicando a congruência módulo 16 as potências de 10, obtemos

$$\begin{aligned}
10^0 &\equiv 1 \ mod\ 16 \\
10^1 &\equiv 10 \ mod\ 8 \text{ ou } 10^1 \equiv -6 \ mod\ 8 \\
10^2 &\equiv 4 \ mod\ 16 \text{ ou } 10^2 \equiv -12 \ mod\ 8 \\
10^3 &\equiv 8 \ mod\ 16 \text{ ou } 10^3 \equiv -8 \ mod\ 16 \\
10^4 &\equiv 0 \ mod\ 16 \text{ ou } 10^0 \equiv 0 \ mod\ 8 \\
&\vdots
\end{aligned}$$

Mas pela Proposição 7.3, isso implica que

$$\begin{aligned}
n_0 10^0 &\equiv 1n_0 \ mod\ 16 \\
n_1 10^1 &\equiv 10n_1 \ mod\ 16 \text{ ou } n_1 10^1 \equiv -6n_1 \ mod\ 16 \\
n_2 10^2 &\equiv 4n_2 \ mod\ 16 \text{ ou } n_2 10^2 \equiv -12n_2 \ mod\ 8 \\
n_3 10^3 &\equiv 8n_3 \ mod\ 16 \text{ ou } n_3 10^3 \equiv -8n_3 \ mod\ 16 \\
n_4 10^4 &\equiv 0 \ mod\ 16 \text{ ou } n_4 10^4 \equiv 0 \ mod\ 16 \\
&\vdots \\
n = n_0 10^0 + n_1 10^1 + n_2 10^2 + n_3 t 10^3 + \cdots &\equiv n_0 + 10n_1 + 4n_2 + 8n_3 \ mod\ 16 \\
&ou \\
n = n_0 10^0 + n_1 10^1 + n_2 10^2 + n_3 10^3 + \cdots &\equiv n_0 - 6n_1 - 12n_2 - 8n_3 \ mod\ 16
\end{aligned}$$

Portanto n é divisível por 16 se

a) O algarismo da unidade mais dez vezes o algarismo da dezena mais quatro vezes o algarismo da centena mais oito vezes o algarismo da milhar é divisível por 16;

b) O algarismo da unidade menos seis vezes o algarismo da dezena menos doze vezes o algarismo da centena menos oito vezes o algarismo da milhar é divisível por 16;

As demonstrações dos critérios divisibilidade representam uma maneira para o aluno associar as propriedades da congruência ao estudo da divisão. Os critérios, antes apresentados de forma obscura no 3º ciclo do Ensino Fundamental, justificados apenas com casos particulares, agora pedem ser compreendidas mediante o conhecimento das propriedades das congruências. O professor pode apresentar esses critérios já na educação básica e incentivar seus alunos a tentar encontrar outros critérios não apresentados nesse trabalho como por exemplo os critérios de divisibilidade por 17, 19, 23 entre outros.

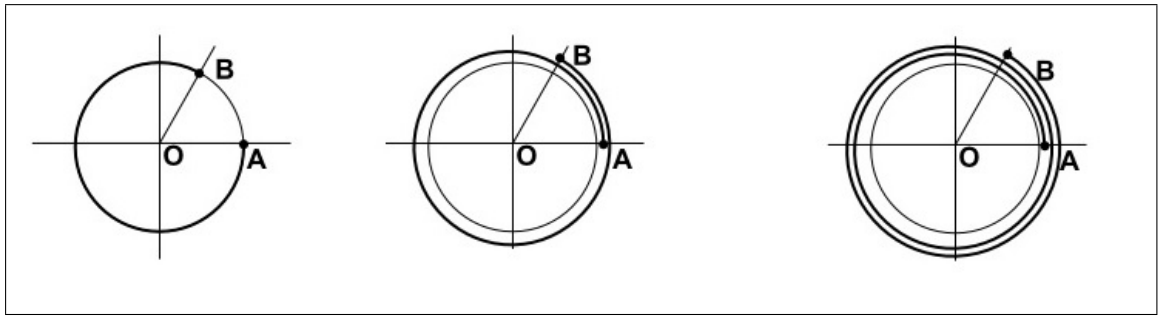
8 O ENSINO DAS CONGRUÊNCIAS NA EDUCAÇÃO BÁSICA

No ensino de Aritmética convencional, o resto da divisão é apenas tratado como a "sobra" da divisão. Mas o resto da divisão tem significado em situações práticas bem como em conteúdos curriculares de matemática que tem como características, fenômenos periódicos ou cíclicos. Uma sequência de valores ou propriedades é periódica quando, no seu desenvolvimento, a partir de um determinado instante (período) a sequência volta a apresentar os mesmos valores ou propriedades a cada período. Fenômenos periódicos são comuns na natureza tais como as estações do ano e as fases da lua. Na matemática, conteúdos como a trigonometria, números complexos, progressões aritméticas, alguns subconjuntos dos números inteiros (por exemplo pares e ímpares) dentre outros, apresentam características periódicas.

8.1 O Ensino das Congruências em Trigonometria e Números Complexos

O estudo das congruências módulo m pode ajudar na compreensão dos arcos côngruos em um ciclo trigonométrico. Dado um arco AB de medida α, ao dar voltas completas no ciclo trigonométrico são gerados outros arcos com a mesma extremidade do arco AB. Esses arcos são chamados de arcos côngruos. A determinação de arcos côngruos é uma aplicação do Algoritmo da Divisão à trigonometria, consequentemente um problema sobre divisão.

Figura 4 – Representação de ângulos côngruos no ciclo trigonomêtrico



Fonte: O Autor

No caso todo os arcos de medida $\alpha + 360^o \cdot k$ com $k \in \mathbb{Z}$ são arcos côngruos que tem a mesma representação no ciclo trigonométrico.

A notação da congruência pode ser utilizada para melhor representar as medidas de arcos côngruos.

Exemplo 8.1. A notação $\alpha + 360^o k$ com $k \in \mathbb{Z}$ ficaria $x \equiv \alpha \ mod \ 360^o$

As congruência lineares podem ser utilizadas para resolver problemas envolvendo arcos côngruos.

Exemplo 8.2. Determine a menor determinação positiva de -810^o.

Solução: Devemos encontrar o menor valor para x tal que $x \equiv 810^o \ mod \ 360^o$ com $0^o \leqslant x < 360^o$. Utilizando as propriedades das congruências

$$-810^o \equiv -720^o - 90^o \equiv -90^o \equiv -90^o + 360^o \equiv 270^o \ mod \ 360^o.$$

Portanto a menor determinação positiva de -810º é 270º.

Em relação aos números complexos, as potências da unidade imaginária i com expoente natural n tem características periódicas. Basta observar a sequência

$$\begin{aligned}
i^0 &= 1 \\
i^1 &= i \\
i^2 &= -1 \\
i^3 &= i^2 \cdot i = -i \\
i^4 &= i^2 \cdot i^2 = 1 \\
i^5 &= i^3 \cdot i^2 = i \\
&\vdots \\
i^{4n} &= (i^4)^n = 1 \\
i^{4n+1} &= (i^4)^n \cdot i = i \\
i^{4n+2} &= (i^4)^n \cdot i^2 = -1 \\
i^{4n+3} &= (i^4)^n \cdot i^3 = -i.
\end{aligned}$$

Analisando a propriedade periódica das potências de i, assim como os arcos côngruos da trigonometria, podemos ver facilmente que é um problema envolvendo restos de divisões; podendo ser estudado utilizando as congruências. É possível mostrar que

$$i^n = \begin{cases} 1, \text{se } n \equiv 0 \ mod \ 4 \\ i, \text{se } n \equiv 1 \ mod \ 4 \\ -1, \text{se } n \equiv 2 \ mod \ 4 \\ -i, \text{se } n \equiv 3 \ mod \ 4 \end{cases}$$

entretanto não demonstraremos a propriedade pois foge dos objetivos desse trabalho.

8.2 O Ensino das congruências e as Olimpíadas de Matemática

As afirmações e propriedades envolvendo o resto das divisões são mais simples e fáceis de se manipular quando escritas usando a linguagem das congruências, tornando

esse assunto uma poderosa ferramenta para resolução de problemas de olimpíadas de matemática envolvendo números inteiros.

Algumas recomendações úteis para resolução de questões de olimpíadas envolvendo congruências:

a) Problemas envolvendo o resto de divisões com dividendos elevados são fortes candidatos a serem resolvidos com congruências;

b) Podemos tentar utilizar as congruências na resolução de problemas cujos dados tem características cíclicas (fases da lua, calendários, relógios), etc;

c) Problemas envolvendo critérios de divisibilidade, em geral, podem ser resolvidos usando as congruências.

Segue abaixo alguns problemas da OBM (Olimpíada Brasileira de matemática) resolvidos cujo o foco é o resto da divisão de números inteiros, consequentemente utilizando as congruências módulo m[1].

Exemplo 8.3. (OBM -2009) Seja $N = 8^{8^{\cdot^{\cdot^{\cdot^{8}}}}}$, em que aparecem 2009 números 8. Agilulfo ficou de castigo: ele deve escrever a soma dos dígitos de N, obtendo um número M; em seguida, deve calcular a soma dos dígitos de M; e deve repetir o procedimento até obter um número de um único dígito. Vamos ajudar Agilulfo: esse dígito é:
A) 1 B) 2 C) 3 D) 7 E) 8

Solução: Pelo pelo critério de divisibilidade por 9, um número é divisível por 9 se a soma de seus algarismos tambem o for, logo, pelos dados do problema podemos escrever a seguinte congruência

$$8 \equiv (-1) \; mod \; 9 \Rightarrow 8^{8^{\cdot^{\cdot^{\cdot^{8}}}}} \equiv (-1)^{8^{\cdot^{\cdot^{\cdot^{8}}}}} \; mod \; 9 \Rightarrow 8^{8^{\cdot^{\cdot^{\cdot^{8}}}}} \equiv 1 \; mod \; 9.$$

Ou seja, a soma dos dígitos de todos os números que Agilulfo deve escrever é congruente a 1 módulo 9. Portanto, o último dígito desse número será 1.

Exemplo 8.4. (OBM – 2010) O professor Piraldo tem dois relógios, ambos digitais de 24 horas. Nenhum dos dois funciona: um muda de horário com o dobro da velocidade normal e o outro vai de trás para frente, na velocidade normal. Ambos mostram corretamente 13 : 00. Qual é a hora certa na próxima vez em que os dois relógios mostrarem o mesmo horário?

A) 05:00 B) 09:00 C) 13:00 D) 17:00 E) 21:00

[1] Fonte: Provas e Gabaritos em (13) www.obm.org.br. Acesso em 20 de Abril de 2014.

Solução: Seja x o tempo que o segundo relógio voltou no tempo. Então queremos resolver a congruência $2x \equiv -x \; mod \; 24$. Pelas Proposições 7.3 e 7.4 obtemos

$$2x \equiv -x \; mod \; 24 \Rightarrow 3x \equiv 0 \; mod \; 24 \Rightarrow x \equiv 0 \; mod \; 24 \Rightarrow x \equiv 0 \; mod \; 8.$$

Logo o menor inteiro positivo que satisfaz essa congruência é 8. Portanto a hora certa será 13:00 + 8:00 = 21:00.

Exemplo 8.5. (OBM – 2010) Seja N o menor número inteiro positivo que multiplicado por 33 resulta em um número cujos algarismos são todos iguais a 7. Determine a soma dos algarismos de N.

Solução: Pelo critério de divisibilidade por 11, se o número $33N$ possui todos os seus algarismos iguais e é divisível por 11, então ele deve possuir um número par da algarismos. Por outro lado, o critério de divisibilidade por 3 garante que a soma dos algarismos deve ser múltiplo de 3, ou seja, a quantidade de algarismos 7 deve ser divisível por 3. Logo o menor número que satisfaz as condições é 777777, ou seja, $N = \frac{777777}{33} = 23569$. Portanto A soma dos algarismos de N é 2 + 3 + 5 + 6 + 9 = 25.

Exemplo 8.6. (OBM-2012)) Qual é a maior potência de 2 que divide $2011^{2012}–1$?
A) 2 B) 4 C) 8 D) 16 E) 32

Solução: A expressão $2011^{2012}–1$ pode ser fatorada da na forma

$$2011^{2012}–1 = (2011^{1006}–1)(2011^{1006} + 1) = (2011^{503} + 1)(2011^{503}–1)(2011^{1006} + 1).$$

Utilizando as congruências módulo m obtemos

$$\begin{aligned} 2011 &\equiv -1 \; mod \; 4 \Rightarrow 2011^{503} - 1 \equiv (-1)^{503} - 1 \; mod \; 4 \Rightarrow 2011^{503} - 1 \equiv 2 \; mod \; 4 \\ 2011 &\equiv -1 \; mod \; 4 \Rightarrow 2011^{1006} + 1 \equiv (-1)^{1006} + 1 \; mod \; 4 \Rightarrow 2011^{1006} + 1 \equiv 2 \; mod \; 4 \\ 2011 &\equiv 3 \; mod \; 8 \Rightarrow 2011^{1503} + 1 \equiv 3^{503} + 1 \; mod \; 8 \Rightarrow 2011^{5036} + 1 \equiv 4 \; mod \; 8. \end{aligned}$$

Logo, as maiores potências de 2 que dividem $(2011^{503}–1)$, $(2011^{1006} + 1)$ e $(2011^{503} + 1)$ são 2, 2 e 4 respectivamente. Portanto, a maior potência de 2 que divide $2011^{2012}–1 = (2011^{1006}–1)(2011^{1006} + 1) = (2011^{503} + 1)(2011^{503}–1)(2011^{1006} + 1)$ é $2 \cdot 2 \cdot 4 = 16$.

9 APLICAÇÃO DA ATIVIDADE EM SALA DE AULA E AVALIAÇÃO DE RESULTADOS

Descreveremos agora uma experiência de aplicação em sala de aula de alguns Tópicos de Aritmética apresentados nesse trabalho. O objetivo desse minicurso de cunho extracurricular é averiguar a viabilidade da proposta desse trabalho em inserir tópicos de teoria dos números no currículo do Ensino Médio relacionados com o estudo da divisão.

Para isso, é necessário observar o processo de ensino e aprendizagem dos alunos sobre Aritmética Básica a partir do aprofundamento do conteúdo visto no Ensino Fundamental bem como o ensino de novos conceitos de aritmética, reaproveitando, sempre que possível, o conhecimento prévio dos alunos. A justificativa da escolha do minicurso ao invés das aulas convencionais se deve ao fato de que o currículo de Matemática da escola onde será aplicado o minicurso não contempla estudos de Aritmética no Ensino Médio.

9.1 Metodologia de Aplicação

Para a aplicação do referido minicurso, foi pedido autorização (Apêndice A) à Direção da Escola de Ensino Médio Governador Adauto Bezerra. A referida escola, de esfera estadual, situa-se no município de Juazeiro do Norte CE e tem aproximadamente 2100 alunos matriculados. Segundo dados da direção, a instituição de ensino funciona nos três turnos atendendo alunos de baixa renda, tanto da zona urbana quanto rural. Vale salientar que a clientela do turno noturno, em sua maioria é composta pela classe trabalhadora.

Após a autorização dada pela direção, foi feito um convite formal aos alunos das turmas do 3º anos A,B,C e D do turno vespertino, cujo professor de Matemática regente é o próprio mestrando, a participar do minicurso de "Aritmética Básica". Para garantir a concentração nos trabalhos de classe bem como atenção adequada do regente a todos os alunos, foram oferecidas apenas dez vagas que foram rapidamente preenchidas. A escolha dos alunos se deve apenas ao desejo dos próprios em participar do curso, não sendo utilizado como critério de seleção as notas nem a participação dos mesmos em sala de aula. Entretanto, como motivação para a persistência dos alunos no curso, foi dado uma nota extra em Matemática para cada aluno que compareceu a todos os encontros.

Após a seleção dos alunos, foi enviado um pedido de autorização por escrito (Apêndice B) aos pais ou responsáveis dos mesmos para participação do minicurso. Posteriormente, foi aplicado o questionário socioeconômico e o teste de sondagem aos alunos cursistas, cujo objetivo foi averiguar o conhecimento prévio dos alunos a res-

peito dos conteúdos ministrados no minicurso, bem como verificar condições externas que favoreçam ou não a aprendizagem dos discentes.

As atividades foram aplicadas em um minicurso de Aritmética Básica de 16 horas/aula dividido em quatro encontros presenciais de 4 horas/aula cada. Os dois primeiros encontros foram utilizados para aprofundar conceitos que os alunos aprenderam no Ensino Fundamental (divisão, números primos, *mdc* e *mmc*) e os dois últimos encontros trataram de atividades complementares, que tradicionalmente não são ensinados na educação básica (Equações Diofantinas e Introdução as Congruências Módulo m). O método escolhido para aplicação do minicurso foi a aula expositiva dialogada.

Como critério de avaliação quantitativa, ao final de cada encontro foi aplicado um pequeno exercício de classe sobre o conteúdo visto no encontro. Esse exercício foi recolhido ao final de cada encontro e utilizado para a análise de resultados, descrita adiante, e em seguida arquivado.

A bibliografia principal utilizada para a aplicação do minicurso foram os tópicos contidos nos capítulos 3 a 6 desse trabalho e, pela falta de livros didáticos para o ensino de Aritmética no Ensino Médio, foram usados como material de apoio os livros "Iniciação à Aritmética"(14), "Círculos Matemáticos - A Experiência Russa"(15) e "Teoria Elementar dos Números"(9); que apesar de serem utilizados em cursos de nível superior e para preparação de alunos para olimpíadas de Matemática, esses livros tem uma linguagem acessível aos alunos dessa faixa etária.

9.2 Aplicação do Minicurso

9.2.1 *Avaliação Preliminar*

O objetivo da avaliação prévia é conhecer o perfil socioeconômico bem como os conhecimentos de Aritmética dos alunos, para então avaliar quais as dificuldades e limitações que os mesmos enfrentarão durante o curso e preparar um plano de aulas adequado para a turma.

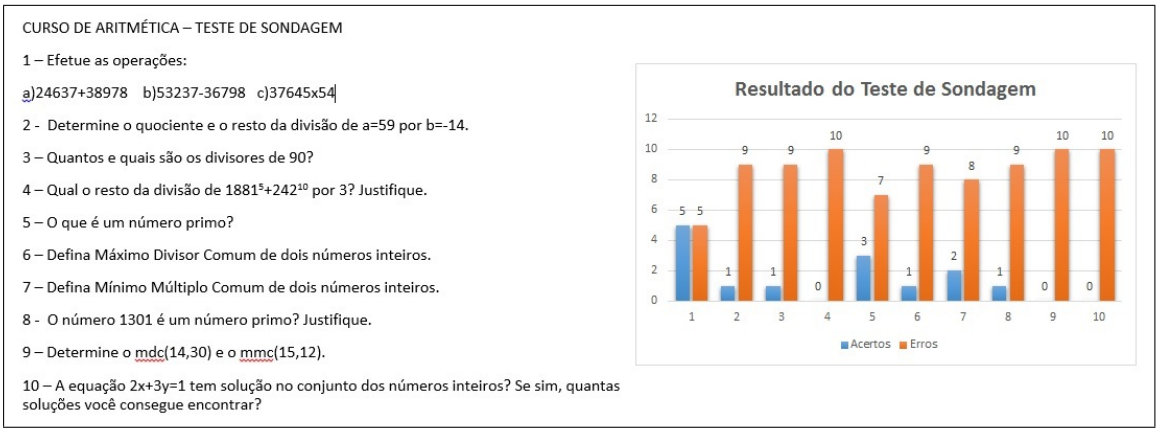
O teste de sondagem versa sobre operações aritméticas elementares, noção de números primos, equações diofantinas lineares e manipulação do resto de divisões. Nesse teste foi evitado de propósito as situações-problema contextualizadas para verificar somente as habilidades de cálculo; pois elas é que são o foco do estudo da Aritmética no Ensino Fundamental, ou seja, o conhecimento prévio do aluno foi nosso ponto de partida para decidir quais os conteúdos e práticas de ensino foram adotadas no decorrer do curso.

> "Também a importância de levar em conta o conhecimento prévio dos alunos na construção de significados geralmente é desconsiderada. Na maioria das vezes, subestimam-se os conceitos desenvolvidos no decorrer das vivências práticas dos alunos, de suas interações sociais imediatas, e parte-se para um tratamento escolar, de forma esquemática,

> privando os alunos da riqueza de conteúdos proveniente da experiência pessoal."(BRASIL, 1998,p.23)

O gráfico abaixo mostra as questões aplicadas e a quantidade de acertos e erros. Por questão de comodidade para o leitor, as questões sem resposta nesse gráfico e nos gráficos subsequentes, serão consideradas erradas.

Figura 5 – Resultado do teste de sondagem



Fonte: O Autor

O teste de sondagem revela que apenas metade dos alunos tem domínio das operações elementares; a maioria absoluta dos alunos não conhecem definições básicas de aritmética tais como *mdc* e *mmc* de números inteiros e números primos; nenhum dos alunos conhecem métodos para manipular restos de divisões nem conhecimento sobre propriedades dos divisores; e o que é mais intrigante é que nenhum dos alunos, apesar de estarem cursando 3º ano do Ensino Médio, conhecem os métodos de cálculo do *mdc* e *mmc* de dois números inteiros.

O questionário sócioeconômico evidencia que a maioria dos alunos que participaram do curso tem idade entre 16 e 18 anos, não são repetentes, tem local apropriado para estudos, moram na mesma cidade onde estudam, tem bom aproveitamento na disciplina de Matemática, não tem limitações físicas que comprometam a capacidade de estudo. Portanto não há fatores aparentes que interfiram na rotina de estudos dos alunos que participaram do curso. Esses dados reforçam que um dos motivos para o baixo rendimento dos alunos no teste de sondagem se deve à interrupção precoce dos estudos de Aritmética no Ensino Fundamental.

9.2.2 *Primeiro Encontro*

OBJETIVOS

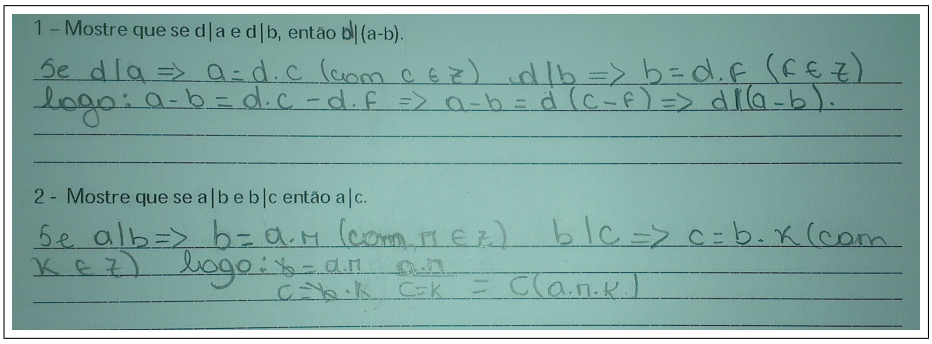
Que os alunos estejam aptos a aplicar a definição de divisor em demonstrações elementares; reconhecer se um número natural é primo ou composto como também aplicar o Teorema Fundamental da Aritmética para encontrar os divisores de um certo número natural; aplicar o algoritmo da divisão e o lema dos restos em aplicações envolvendo o estudo de caso.

RELATO DA AULA

A aula foi iniciada com o mestrando expondo a definição de Aritmética[1] e, em seguida, a divulgação aos alunos dos conteúdos que seriam abordados durante a aula: Definição de Divisor e propriedades; Números Primos; Algoritmo da Divisão e Lema dos Restos.

O mestrando mostrou a Definição de divisor 3.1 aos alunos que a receberam com naturalidade, apesar do embaraço dos mesmos quando viram a aplicação da definição na demonstração das propriedades (ii), (iii) e (iv) dos divisores, pois na educação convencional de Matemática, as demonstrações dos resultados quase não são utilizadas. Entretanto, os alunos se adaptaram rapidamente com a notação ($a \mid b$) conseguindo aplicá-la em alguns exercícios básicos de demonstrações com argúcia.

Figura 6 – Resolução do exercício do aluno sobre propriedades do divisor - 1º encontro



Fonte: O Autor

Em seguida houve um debate rápido sobre a definição de números primos entre os alunos e o mestrando com o propósito de aperfeiçoar a definição que os alunos obtiveram no Ensino Fundamental. Ao perguntar aos alunos a definição sobre números primos um deles afirmou que "números primos são todos os números que terminam com o algarismo 1", outro aluno afirmou que "números primos são todos os números ímpares", entretanto a maioria dos alunos afirmaram que números primos são os

[1] Palavra de origem grega, que significa número. É o ramo da Matemática que lida com os números e com as operações possíveis entre eles. A palavra aritmética é também usada para se referir à Teoria dos Números que estuda as propriedades dos números em geral. Fonte: http://pt.wikipedia.org/wiki/Aritmética.

números inteiros com dois divisores. Nessa etapa da aula o mestrando interferiu na discussão afirmando que a quantidade de divisores de um número primo é relativa ao conjunto numérico adotado, ou seja, são dois divisores positivos distintos. Após a definição e alguns exemplos de números que são primos, foi enunciado o Teorema Fundamental da Aritmética 4.1. A demonstração desse Teorema foi aplicada parcialmente, no caso apenas a parte da "Existência" da fatoração (que não precisa necessariamente ser mostrada por indução), não sendo demonstrada a parte da "Unicidade" pois o "Princípio da Indução", que é um resultado essencial para a demonstração, não foi apresentado aos alunos.

Continuando a aula, o mestrando perguntou aos alunos como reconhecer se certo número é primo ou composto. Não houve resposta a essa pergunta. Entretanto, um dos alunos indagou se era possível conhecer todos os números primos.

Para responder aos alunos sobre a infinitude dos números primos o mestrando aproveitou a oportunidade de trabalhar com alunos do 3º ano do Ensino Médio, que já conhecem a definição de fatorial, para aplicar a demonstração de "Hermite"sobre a infinitude dos números primos.

Foi dada a incumbência para os alunos pesquisarem e apresentarem a demonstração de Euclides sobre a infinitude dos números primos no próximo encontro. Em seguida foi apresentado o Teorema 4.2 como teste de primalidade e base para a construção do Crivo de Eratóstenes.

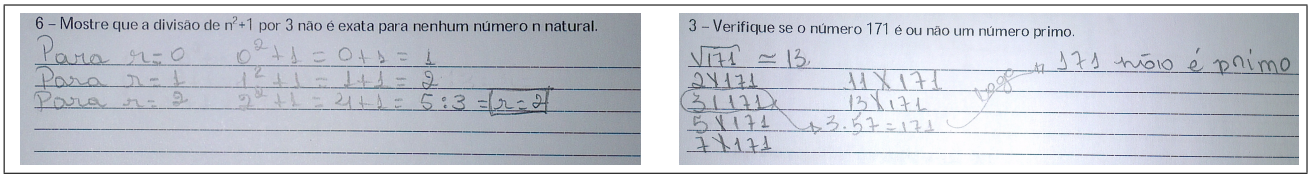
Figura 7 – Aluno resolvendo o exercício - 1º encontro

Fonte: O Autor

Após a verificação do entendimento do Teorema 4.2 como teste de primalidade, foi apresentado e demonstrado para os alunos, os Corolários 4.1 e 4.2 que mostram como encontrar os divisores de um número inteiro a partir do Teorema Fundamental da Aritmética. Para terminar a parte teórica, o mestrando apresentou aos alunos o Algoritmo da Divisão 3.3 e o Lema dos Restos 3.1, sem no entanto efetuar a

demonstração formal em virtude do não conhecimento dos alunos sobre o "Princípio da Boa Ordenação", bem como o tempo de aula que estava adiantado.

Figura 8 – Resolução de parte do exercício de dois alunos - 1º encontro. Fonte: O Autor



Fonte: O Autor

Para finalizar as atividades foi iniciado o estudo dirigido onde o mestrando colocou os alunos em duplas para realizarem a lista de exercícios propostas para esse dia. A realização dos exercícios foi feita sem o auxílio do mestrando, onde os alunos contavam apenas com a conceituação e seu colega de dupla.

9.2.3 *Segundo Encontro*

OBJETIVOS

Que os alunos estejam aptos a calcular o *mdc* e *mmc* de dois números inteiros pelo processo da decomposição em fatores primos bem como a sua aplicação em situações-problema; utilizar o Algoritmo de Euclides para escrever o *mdc* de dois números inteiros como combinação linear desses números; conhecer e utilizar a Identidade de Bézout para verificar se alguns tipos de equações lineares de duas variáveis tem solução.

RELATO DA AULA

A aula foi iniciada com o seminário proposto pelo mestrando no último encontro. O seminário foi ministrado por um dos alunos onde o mesmo expôs sua pesquisa sobre a infinitude dos números primos, em seguida, a aluna apresentou aos colegas e ao mestrando a demonstração de Euclides para a infinitude dos números primos. Nesse seminário, o papel do mestrando foi voltado a corrigir erros de notação e expressão oral da aluna. A aluna foi muito sagaz na explicação da demonstração de Euclides. Na sua explicação ela supõe que o conjunto dos números primos tem apenas dois elementos, os números 2 e 3, em seguida , expressa o números $p = 2 \cdot 3 + 1$ que não tem fatores 2 e 3; em seguida ela supõe que o conjunto dos números primos tem apenas três elementos, os números 2,3 e 5 e expressa o número $p = 2 \cdot 3 \cdot 5 + 1$ que não tem fatores 2, 3 e 5; ela segue com esse raciocínio até expressar o número $P = p_1 p_2 p_3 \cdots p_n + 1$ terminando a demonstração.

Em seguida, o mestrando fez a divulgação aos alunos dos conteúdos que seriam abordados durante a aula: Máximo Divisor Comum e Mínimo Múltiplo Comum de números inteiros; Lema de Euclides e Algoritmo de Euclides; Identidade de Bézout.

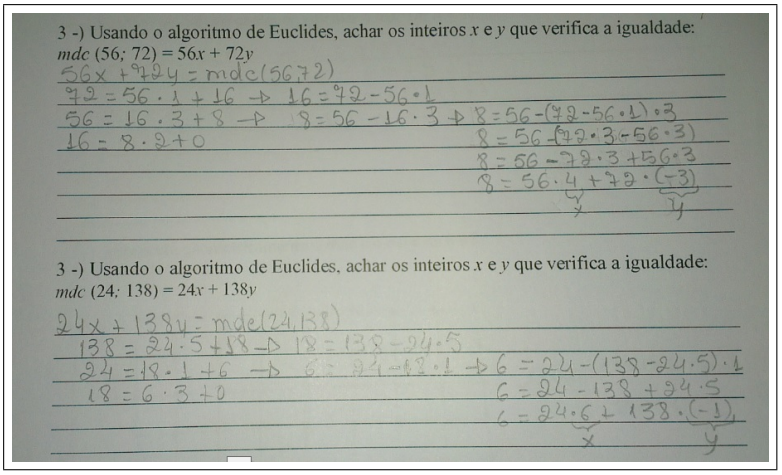
A aula prosseguiu com a apresentação das definições e caracterizações do *mdc* e *mmc* de dois números inteiros e a descrição do método de cálculo do *mdc* e *mmc* pela decomposição em fatores primos. As demonstrações das caracterizações do *mdc* e *mmc* foram omitidas. Para terminar a primeira parte da aula o mestrando mostrou aos alunos como interpretar geometricamente o *mdc* e *mmc* de dois números naturais.

Figura 9 – Seminário sobre e infinitude os números primos e da demonstração do Lema de Euclides - 2º encontro

Fonte: O Autor

Com o objetivo de justificar o funcionamento do Algoritmo de Euclides, foi apresentado o Lema de Euclides como um método de que permite a substituição do $mdc(a, b)$ pelo mdc de a e b menos um múltiplo de a. Em seguida, o Lema de Euclides foi demonstrado. O objetivo da apresentação do algoritmo de Euclides aos alunos foi dar meios para a resolução das equações diofantinas, assunto ministrado no terceiro encontro entre o mestrado e seus alunos. Foi evidenciado o fato de que o Algoritmo de Euclides é eficiente para encontrar o *mdc* de dois valores elevados sem a necessidade de efetuar fatorações. A identidade de Bézout foi apresentada aos alunos pelo mestrando sem demonstração. O objetivo da identidade de Bézout nesse minicurso foi introduzir o conceito de combinação linear e associá-la a uma equação linear de duas variáveis com soluções.

Figura 10 – Resposta do exercício de um aluno sobre aplicações do MDC e MMC - 2º encontro



Fonte: O Autor

Para finalizar a aula, foi entregue a lista de exercícios sobre os tópicos ensinados. Cada aluno foi orientado a fazer sua atividade sem ajuda dos colegas. Durante as atividades coube ao mestrando dar orientação individual se fosse solicitado pelos alunos sem no entanto interferir no desenvolvimento das estratégias e cálculos efetuados pelo aluno em cada item do exercício. Nessa tarefa os alunos apresentaram dificuldades em resolver questões envolvendo o Algoritmo de Euclides e o Lema de Euclides, entretanto as questões envolvendo as definições e método de aquisição do *mdc* e *mmc* foram resolvidas sem maiores dificuldades.

9.2.4 *Terceiro Encontro*

OBJETIVOS

Que os alunos estejam aptos a verificar se as equações diofantinas lineares tem ou não solução; encontrar a solução geral das equações diofantinas, desde que tenham solução; aplicar as equações diofantinas lineares na resolução de problemas contextualizados.

RELATO DA AULA

A aula foi iniciada com a revisão de combinação linear iniciado no encontro anterior tomando como exemplo o Algoritmo de Euclides que escreve o resto das divisões como combinação linear do dividendo e divisor. Em seguida o mestrando fez uma rápida revisão sobre a Identidade de Bézout. Tanto o Algoritmo da Divisão quanto a Identi-

dade de Bézout são ferramentas importantes para o estudo das equações diofantinas lineares.

Em seguida foi dada a definição das Equações Diofantinas Lineares, bem como a etimologia da palavra Diofantina[2].

Em seguida foi apresentado e demonstrado aos alunos o Teorema 7.1 que mostra a condição necessária e suficiente para as equações diofantinas admitirem ou não soluções inteiras, bem como a Proposição 7.6 que mostra a solução geral de uma equação diofantina linear da forma $ax + by = c$ com $mdc(a, b) = 1$ a partir de uma solução particular.

Figura 11 – Demonstração da Proposição 7.6 e desenvolvimento de trabalhos em equipe - 3º encontro

Fonte: O Autor

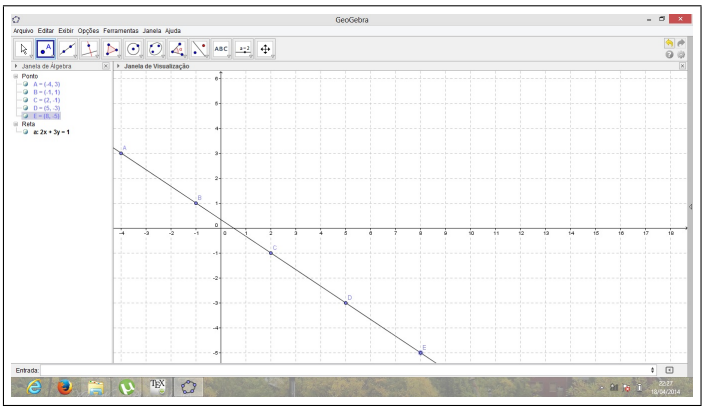
Para terminar a parte teórica, o mestrando apresentou aos alunos alguns exemplos de aplicações da teoria sobre as equações diofantinas lineares.

Exemplo 9.1. Represente geometricamente no plano cartesiano a equação $2x + 3y = 1$.

Solução: Para deixar claro aos alunos que as soluções inteiras de uma equação diofantina linear são colineares, o mestrando associou as definições de equações diofantinas lineares e função afim. Em seguida foi utilizado o programa Geogebra para dar a representação geométrica da equação.

[2] No caso desse curso, são equações de duas incógnitas com soluções inteiras. A palavra diofantina, de origem grega, mais especificamente de Diofanto de Alexandria, que é considerado o maior algebrista grego.

Figura 12 – Representação geométrica da equação $2x+3y = 1$ no Geogebra - 3º encontro



Fonte: O Autor

Exemplo 9.2. Determinar o menor inteiro positivo que dividido por 8 e por 15 deixa os restos 6 e 13, respectivamente.

Solução: Chamando de "D" o número procurado, usando as condições do problema no algoritmo da divisão obtemos

$$D = 8x + 6 \text{ e } D = 15y + 13 \Rightarrow 8x + 6 = 15y + 13 \Rightarrow 8x - 15y = 7. \tag{9.1}$$

Ou seja, o número procurado é solução da equação diofantina dada em (9.1). Uma solução particular da equação diofantina é $x_0 = 14$ e $y_0 = 7$, logo a solução geral da equação é dada por $x = 14 - 15t$ e $y = 7 - 8t$, com $t \in \mathbb{Z}$.

Como D é menor inteiro que satisfaz as condições do problema, então deve ocorrer que,

$$D > 0 \Rightarrow 8 \cdot (14 - 15t) + 6 > 0 \Rightarrow 118 - 120t > 0 \Rightarrow t = 0.$$

Portanto o número procurado é $D = 8x + 6 = 8 \cdot (14 - 15t) + 6 = 118$.

Exemplo 9.3. Uma estudante foi a uma papelaria comprar esferográficas e lapiseiras para sua coleção. Cada esferográfica custa R$ 5,00 e cada lapiseira custa R$ 4,00. Se ela pretende gastar R$ 50,00 nas compras de quantos modos a estudante pode comprar esse material de modo que não sobre troco?

Solução: Chamando de "x" o número de esferográficas e "y" o números de lapiseiras, usando as condições do problema no algoritmo da divisão obtemos a equação $5x + 4y = 50$. Uma solução particular da equação diofantina é $x_0 = 14$ e $y_0 = 7$, logo a solução geral da equação é dada por $x = 50 + 4t$ e $y = -50 - 5t$, com $t \in \mathbb{Z}$. Como o número de esferográficas e lapiseiras é um número inteiro não negativo, segue que,

$$50 + 4t \geqslant 0 \text{ e } -50 - 5t \geqslant 0 \Rightarrow -12 \leqslant t \leqslant -10.$$

Portanto temos três possibilidades:

a) Para $t = -12$: A estudante pode comprar 2 esferográficas e 10 lapiseiras;

b) Para $t = -11$: A estudante pode comprar 6 esferográficas e 5 lapiseiras;

c) Para $t = -10$: A estudante pode comprar 10 esferográficas e 0 lapiseiras.

Para encerrar as atividades foi distribuído a lista de exercícios para serem realizadas pelos alunos em classe. Com o objetivo de motivar os alunos, foi proposto uma competição entre duas equipes com uma premiação simbólica. O mestrando, com o objetivo de proporcionar equilíbrio às equipes, colocou os dois alunos com maior rendimento nos encontros anteriores em equipes distintas, o restante dos componentes de cada equipe foram escolhidos pelos dois alunos apontados pelo mestrando. Em seguida foram definidas as regras da competição:

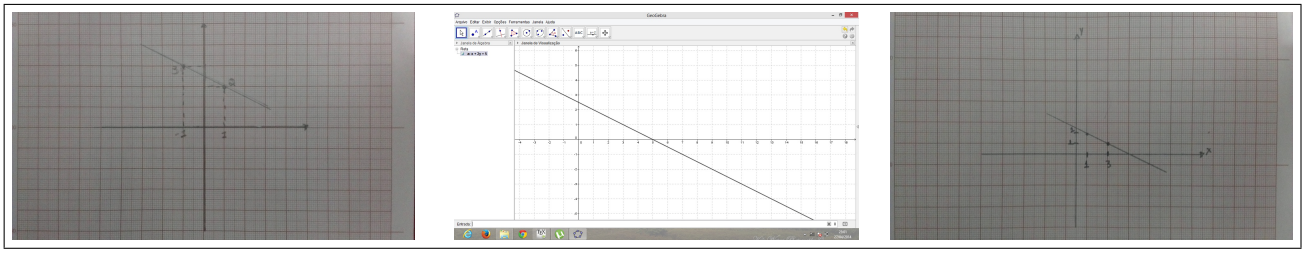
a) As equipes terão cem minutos para resolver as questões;

b) Cada item da 1ª questão valerá um ponto; cada item da 2ª questão valerá dois pontos; a 3ª e 4ª questões valerão três pontos e a 5ª questão valerá dois pontos;

c) Serão consideradas questões com acerto total, acerto parcial (metade da pontuação) e erradas;

d) Em caso de empate ganhará a equipe que entregar primeiro o exercício.

Figura 13 – Interpretação geométrica da equação $3x + 6y = 15$ feita pelas duas equipes concorrentes - 4º encontro



Fonte: O Autor

Encerrado o tempo para a resolução dos exercícios, o mestrando corrigiu a lista de cada equipe com a fiscalização dos chefes de equipe. Após a correção foi dado um prêmio simbólico (uma caixa de bombons) aos alunos da equipe campeã.

9.2.5 *Quarto Encontro*

OBJETIVOS

Que o alunos estejam aptos a aplicar a definição e as propriedades operatórias das congruências na resolução de problemas envolvendo o resto de divisões com dividendo elevado, e aplicar as congruências lineares na resolução de problemas contextualizados.

RELATO DA AULA

Antes de iniciar as atividades, o mestrando incentivou o uso de calculadoras nas atividades para que todo o tempo da aula fosse reservado à compreensão dos conceitos e propriedades das congruências módulo m.

A aula foi iniciada com uma revisão sobre as propriedades do divisor, que foram fundamentais para o prosseguimento dos trabalhos em sala de aula. Em seguida o mestrando expôs a Definição de Congruência 7.1 seguido de uma rápida arguição sobre eventos cíclicos conhecidos pelos alunos (horas do dia, meses do ano, estações do ano, entre outro), objetos de aplicação das congruências. Concomitante às explicações dadas, foi solicitado aos alunos que aplicassem a definição de congruência na verificação dos itens do exemplo abaixo.

Exemplo 9.4. Determine se é verdadeiro ou falso cada item abaixo:
a) $2 \equiv 4 \ mod\ 2$ b) $5 \equiv 8 \ mod\ 3$ c) $3 \not\equiv 1 \ mod\ 2$ d)$17 \equiv 6 \ mod\ 9$

Após a verificação do entendimento da definição de congruência pelos alunos, o mestrando apresentou a demonstração da Proposição 7.1. Em seguida o mestrando utilizou a Proposição 7.1 e o algoritmo da divisão para relacionar congruência com o resto da divisão.

Figura 14 – Demonstração das propriedades das congruências - 4º encontro

Fonte: O Autor

Em seguida foi apresentado aos alunos as propriedades operatórias das congruências contidas na Proposição 7.3 e no Corolário 7.1. Entretanto o mestrando apresentou aos alunos apenas a demonstração da Proposição 7.3 em virtude da falta de conhecimento dos alunos sobre o princípio da indução.

Após a exposição das propriedades operatórias das congruências o mestrando as aplicou na resolução dos exemplos abaixo.

Exemplo 9.5. Ache o resto da divisão de 2^{50} por 7.

Solução: $2^5 \equiv 4 \; mod \; 7 \Rightarrow 2^{10} \equiv 4^2 \; mod \; 7 \Rightarrow 2^{50} \equiv 2^5 \; mod \; 7 \Rightarrow 2^{50} \equiv 4 \; mod \; 7$. Portanto o resto da divisão é 4.

Exemplo 9.6. Calcule o resto da divisão de 1001^{1001} por 5.

Solução: $1001^{1001} \equiv 1^{1001} \; mod \; 5 \Rightarrow 1001^{1001} \equiv 1 \; mod \; 5$ Portanto o resto da divisão é 1. Foi explicado aos alunos que a justificativa das implicações abaixo são oriundas do lema dos restos 3.1 e pela caracterização das congruências 7.1.

Exemplo 9.7. Sabendo que o dia 01/01/2014 foi um dia de quarta-feira, em que dia da semana será o dia 06/07/2014?

Solução: O mestrando argumentou com os alunos que problemas envolvendo horas do dia, dias da semana e estações do ano tem características cíclicas, portanto podem ser interpretados usando as congruências. Ha 187 dias entre as datas 01/01/2014 e 06/07/2014, ou seja, o problema pode ser representado pela congruência $187 \equiv 5 \; mod \; 7$. Logo o 187º dia do ano coincide com o 5º dia do ano na semana, portanto o dia procurado é segunda-feira.

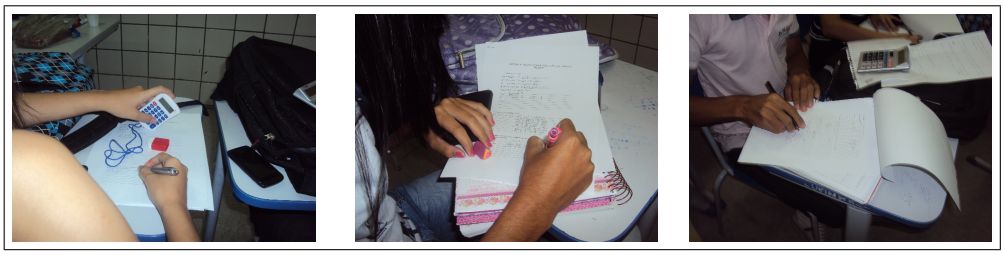
Exemplo 9.8. Verifique se $40^{40} + 81^{81}$ é divisível por 41.

Solução: Do mesmo modo que o 2º exemplo dado na aula, foi explicado aos alunos que as implicações dadas adiante são decorrentes da caracterização das congruências módulo m 7.1 e do lema dos restos 3.1. Logo segue que,

$$40^{40} + 81^{81} \equiv (-1)^{40} + (-1)^{81} \; mod \; 41 \Rightarrow 40^{40} + 81^{81} \equiv 1 - 1 \; mod \; 41 \Rightarrow 40^{40} + 81^{81} \equiv 0 \; mod \; 41.$$

Portanto $40^{40} + 81^{81}$ é divisível por 41.

Figura 15 – Resolução do exercícos de sala - 4º encontro



Fonte: O Autor

Entretanto, os alunos tiveram dificuldades na aplicação da caracterização das congruências na resolução dos exemplos citados, especialmente o segundo exemplo, que utiliza propriedades das potenciações. Nesse momento houve a necessidade do mestrando redirecionar a aula para uma revisão sobre propriedades da potenciação e maiores esclarecimentos sobre as propriedades das congruências. Esse contratempo comprometeu grande parte do tempo da aula.

Para encerrar as atividades em sala de aula, o mestrando distribuiu as listas de exercícios aos alunos. Os exercícios que contemplavam estudos sobre congruências lineares foram retirados pois não houve tempo para trabalhar o assunto. Os alunos foram deixados à vontade para resolver os exercícios de forma individual ou em duplas. O mestrando participou das resoluções dos exercícios ajudando os alunos com a notação das congruências e com uma pequena revisão sobre as propriedades das potenciações, necessária para resolução de alguns problemas.

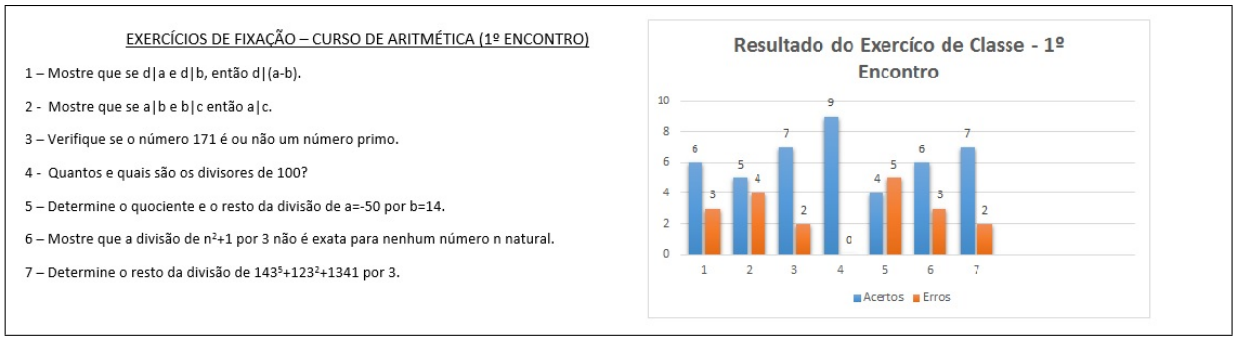
9.3 Análise dos Resultados

Para a análise de resultados serão considerados e examinados a execução do plano de curso em sala de aula, bem como as avaliações quantitativas dos exercícios dos alunos. Será levado em consideração as opiniões dos alunos no decorrer das aulas contidas nas gravações das mesmas e entrevistas com os alunos após o curso, para maiores esclarecimentos sobre as dificuldades encontradas no decorrer das aulas. Essa análise servirá para reformular o roteiro de estudos e assim indicar uma sequência didática mais adequada sobre o Tópicos de Aritmética a ser aplicada no Ensino Médio.

Ao analisar o comportamento dos alunos no decorrer da aula do primeiro encontro, podemos constatar que nenhum dos alunos conheciam a definição de divisor, entretanto conseguiram interagir e aplicar de modo satisfatório a definição na demonstração de algumas propriedades básicas. Alguns alunos não conheciam a definição de números primos nem sua infinitude, entretanto no seminário realizado no início do segundo encontro conseguiram, apesar de alguns erros de notação, demonstrar a infinitude dos números primos utilizando a demonstração de Euclides. Quase todos os objetivos do

encontro foram cumpridos, entretanto, ainda havia alunos que não conseguiam aplicar o algoritmo da divisão em problemas com dividendo e divisor negativos. Esse fato é evidenciado observando a maior quantidade de acertos da questão seis do exercício de classe do primeiro encontro que tem um grau de dificuldade maior em relação a questão cinco. Existem muitas dificuldades de ordem epistemológica que justificam a dificuldade dos alunos em lidar com números negativos, entretanto esse assunto foge aos objetivos desse trabalho.

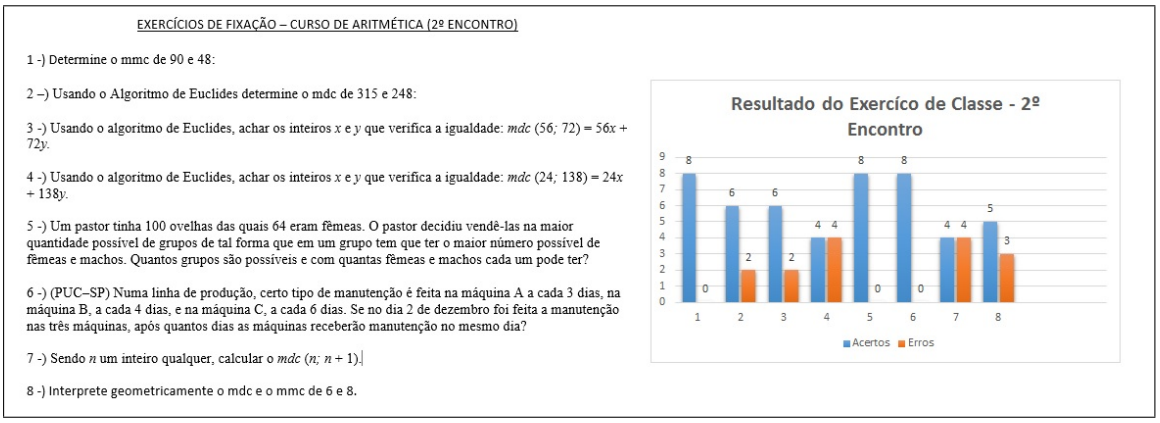
Figura 16 – Resultado exercíco de classe - 1º Encontro



Fonte: O Autor

No segundo encontro, podemos observar que todos os alunos conseguiram aplicar as definições e o método de cálculo do *mmc* e *mdc* de números inteiros pelo método da decomposição simultânea em situações-problema contextualizados. Entretanto, apesar dos objetivos do encontro terem sido alcançados, uma parte dos alunos apresentaram dificuldades em exprimir o *mdc* de dois números inteiros como combinação linear desses números. Isso se deve em parte à dificuldade que os alunos apresentaram em entender que o algoritmo da Divisão permite a escrita do resto como combinação linear do dividendo e divisor e na interpretação do lema de Euclides como método que permite a substituição, quantas vezes for necessário, do *mdc* de dois números inteiros por um *mdc* de números menores, mais simples de serem manipulados.

Figura 17 – Resolução do exercício de classe - 2º Encontro



EXERCÍCIOS DE FIXAÇÃO – CURSO DE ARITMÉTICA (2º ENCONTRO)

1 -) Determine o mmc de 90 e 48:

2 –) Usando o Algoritmo de Euclides determine o mdc de 315 e 248:

3 -) Usando o algoritmo de Euclides, achar os inteiros x e y que verifica a igualdade: $mdc\ (56;\ 72) = 56x + 72y$.

4 -) Usando o algoritmo de Euclides, achar os inteiros x e y que verifica a igualdade: $mdc\ (24;\ 138) = 24x + 138y$.

5 -) Um pastor tinha 100 ovelhas das quais 64 eram fêmeas. O pastor decidiu vendê-las na maior quantidade possível de grupos de tal forma que em um grupo tem que ter o maior número possível de fêmeas e machos. Quantos grupos são possíveis e com quantas fêmeas e machos cada um pode ter?

6 -) (PUC–SP) Numa linha de produção, certo tipo de manutenção é feita na máquina A a cada 3 dias, na máquina B, a cada 4 dias, e na máquina C, a cada 6 dias. Se no dia 2 de dezembro foi feita a manutenção nas três máquinas, após quantos dias as máquinas receberão manutenção no mesmo dia?

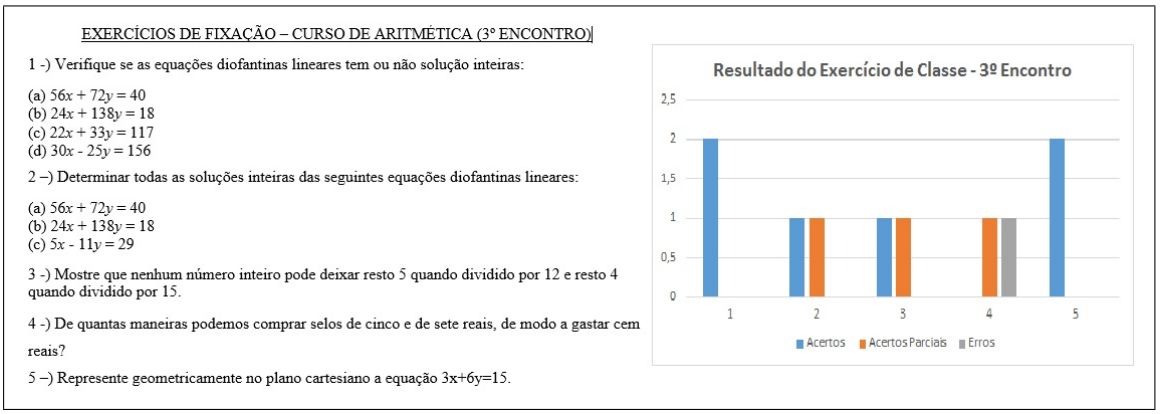
7 -) Sendo n um inteiro qualquer, calcular o $mdc\ (n;\ n + 1)$.

8 -) Interprete geometricamente o mdc e o mmc de 6 e 8.

Fonte: O Autor

No terceiro encontro, os objetivos foram atingidos parcialmente. As duas equipes demoraram bastante tempo para desenvolver os exercícios desse encontro. Avaliando as resoluções das questões das duas equipes fica claro que os alunos conseguem verificar se as equações diofantinas tem solução e conseguem encontrar a solução geral, conseguiram representar geometricamente as equações no plano cartesiano com desenvoltura, entretanto, tiveram muitas dificuldades em aplicar a teoria em situações-problema contextualizadas(questões 3 e 4 do exercício). Essa deficiência na aprendizagem se deve ao fato dos alunos terem dificuldades em trabalhar com inequações do 1º grau com uma variável.

Figura 18 – Resultado exercíco de classe - 3º Encontro



EXERCÍCIOS DE FIXAÇÃO – CURSO DE ARITMÉTICA (3º ENCONTRO)

1 -) Verifique se as equações diofantinas lineares tem ou não solução inteiras:

(a) $56x + 72y = 40$
(b) $24x + 138y = 18$
(c) $22x + 33y = 117$
(d) $30x - 25y = 156$

2 –) Determinar todas as soluções inteiras das seguintes equações diofantinas lineares:

(a) $56x + 72y = 40$
(b) $24x + 138y = 18$
(c) $5x - 11y = 29$

3 -) Mostre que nenhum número inteiro pode deixar resto 5 quando dividido por 12 e resto 4 quando dividido por 15.

4 -) De quantas maneiras podemos comprar selos de cinco e de sete reais, de modo a gastar cem reais?

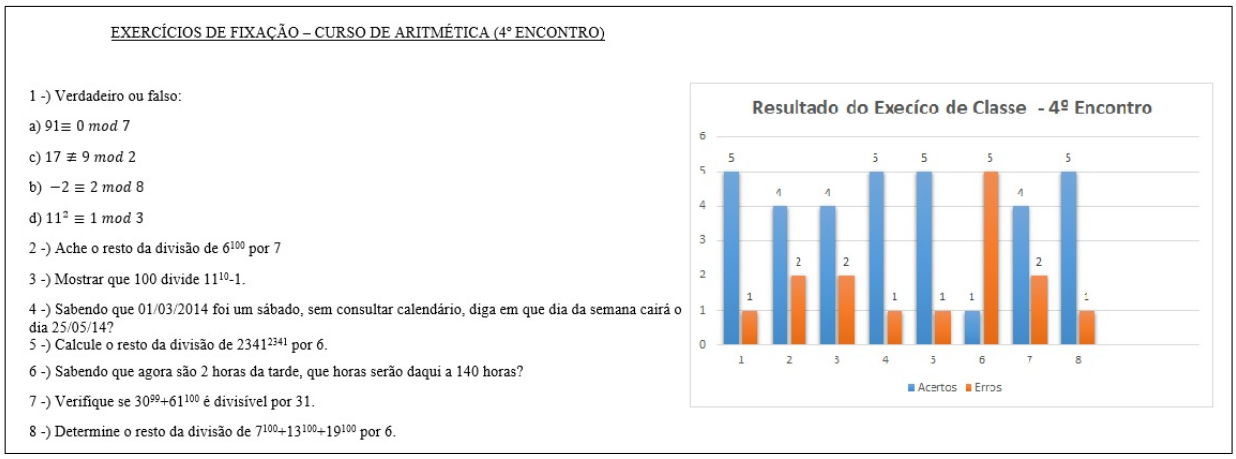
5 –) Represente geometricamente no plano cartesiano a equação 3x+6y=15.

Fonte: O Autor

No quarto encontro podemos verificar que não houve dificuldade para os alunos se adaptarem à notação usual das congruências módulo m, entretanto houve dificuldades para os alunos aplicarem as propriedades das congruências na resolução de problemas. Outro problema detectado para a compreensão dos problemas propostos,

foi a falta de conhecimento das propriedades das potenciações. Esses contratempos comprometeram a exposição de parte do conteúdo programado.

Figura 19 – Resultado exercíco de classe - 4º Encontro



EXERCÍCIOS DE FIXAÇÃO – CURSO DE ARITMÉTICA (4° ENCONTRO)

1 -) Verdadeiro ou falso:

a) $91 \equiv 0\ mod\ 7$

c) $17 \not\equiv 9\ mod\ 2$

b) $-2 \equiv 2\ mod\ 8$

d) $11^2 \equiv 1\ mod\ 3$

2 -) Ache o resto da divisão de 6^{100} por 7

3 -) Mostrar que 100 divide 11^{10}-1.

4 -) Sabendo que 01/03/2014 foi um sábado, sem consultar calendário, diga em que dia da semana cairá o dia 25/05/14?

5 -) Calcule o resto da divisão de 2341^{2341} por 6.

6 -) Sabendo que agora são 2 horas da tarde, que horas serão daqui a 140 horas?

7 -) Verifique se $30^{99}+61^{100}$ é divisível por 31.

8 -) Determine o resto da divisão de $7^{100}+13^{100}+19^{100}$ por 6.

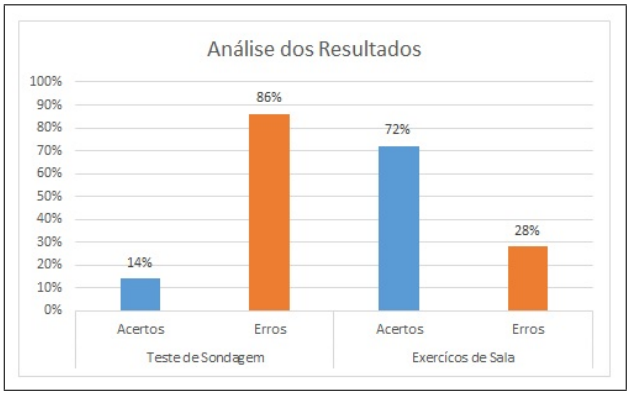
Fonte: O Autor

Os objetivos do quarto encontro não foram atingidos de forma satisfatória pois o tempo se mostrou insuficiente para iniciar o estudo das congruências lineares em virtude da revisão sobre as propriedades das potenciações. Entretanto, por mais bem fundamentado que esteja o planejamento de qualquer curso, imprevistos acontecem.

9.4 Avaliação Geral e Conclusões

Confrontando quantitativamente o aproveitamento das questões aplicadas aos alunos no teste de sondagem com os exercícios de sala de aula no decorrer dos quatro encontros, podemos avaliar o saldo das atividades como positivo.

Figura 20 – Confronto do aproveitamento quantitativo entre o teste de sondagem e as tarefas de sala



Fonte: O Autor

O ensino de Aritmética ministrado nesse minicurso se mostrou eficaz não apenas no caráter quantitativo, mas também em outros quesitos tais como:

a) Consolidou o conteúdo visto no Ensino Fundamental;

b) Proporcionou ao aluno o conhecimento de diversos tipos de demosntrações matemáticas, tais como a direta (dedução), absurdo (contradição) e contra-positiva;

c) Melhorou a capacidade de cálculo, raciocínio e argumentação dos alunos;

Entretanto, alguns problemas impediram que o curso fosse dado de modo mais satisfatório. Algumas demonstrações importantes como a do Teorema Fundamental da Aritmética e do Algoritmo da Divisão foram aplicadas parcialmente ou omitidas em virtude da falta de conhecimento dos alunos sobre o Princípio da Indução e o Princípio da Boa Ordenação. Portanto, há necessidade de inserir esses dois tópicos em um curso de Aritmética Básica. Há livros do Ensino Médio que contemplam esses assuntos que o professor pode utilizar para trabalhar o tema, como por exemplo o texto de Iezzi(16) e de Hefez (10).

Apesar do bom rendimento dos alunos nas tarefas de classe, o conhecimento prévio dos alunos sobre as operações elementares foi insatisfatório para uma transposição didática adequada dos tópicos do curso. Alguns alunos não conheciam os termos da divisão e tinham dificuldades para efetuar divisões onde o dividendo era menor do que o divisor. Propriedades das potenciações, necessárias na resolução de problemas, também eram desconhecidas. Esses conhecimentos não foram avaliados no teste de sondagem e, como consequência, houve a necessidade de efetuar desvios de rota no conteúdo ministrado em sala. Portanto, o teste de sondagem não se mostrou eficaz para conhecer a o nível real de conhecimentos sobre Aritmética dos alunos.

Para sanar as dificuldades apontadas, sugerimos ao leitor interessado em aplicar o minicurso em outras turmas, a inclusão de pelo menos dois novos encontros de 4 horas/aula contemplando uma revisão sobre as Operações Elementares (Divisão, Potenciação e Radiciação), Princípio da Indução Finita e o Princípio da Boa Ordenação para uma transposição didática eficiente, totalizando uma carga horária mínima de 24 horas/aula dividida em seis encontros.

As entrevistas audiografadas[3] com os alunos que frequentaram todos os encontros do minicurso mostraram que os alunos aceitaram bem a proposta de estudar Aritmética no Ensino Médio, a maioria compreendeu o conteúdo estudado e tem interesse na aprendizagem extracurricular de matemática. Ainda, de acordo com a opinião dos discentes, constatamos como principal ponto positivo a oportunidade de rever

[3] As gravações das aulas, fotografias, exercícios resolvidos dos alunos em sala de aula, autorizações dos pais e da direção da escola para a aplicação do minicurso de Aritmética Básica e a entrevista com os alunos que concluíram o curso, estão à disposição para maiores esclarecimentos.

e aprofundar conhecimentos importantes ensinados no Ensino Fundamental e como ponto negativo a falta de tempo para consolidar os assuntos vistos nos encontros.

A seguir, será apresentada uma sequência didática revista a partir das análises das atividades aplicadas nesse minicurso para que o leitor interessado possa aplicá-la em sala de aula. Os tópicos ministrados na proposta original foram reformulados de acordo com as observações contidas na análise de resultados.

SEQUÊNCIA DIDÁTICA:

- 1º Encontro
  - Operação de Divisão (Ideias sobre quotização e partição)
  - Potenciação e Radiciação (Definição e Propriedades)
- 2º Encontro
  - Princípio da Indução
  - Princípio da Boa Ordenação
- 3º Encontro
  - Definição de Divisor e Propriedades
  - Números Primos
  - Teorema Fundamental da Aritmética
  - Algoritmo da Divisão e Lema dos Restos
- 4º Encontro
  - Definição e Caracterização do MDC e MMC
  - Lema de Euclide e Algoritmo de Euclides
  - Combinação Linear e Identidade de Bezout
- 5º Encontro
  - Equações Diofantinas Lineares
- 6º Encontro
  - Definição de Congruência Módulo m
  - Caracterização das Congruências
  - Propriedades Operatórias das Congruências
  - Congruências Lineares

10 CONSIDERAÇÕES FINAIS

Nesse trabalho foi apresentada uma proposta para o ensino de Tópicos de Aritmética, em especial o ensino da divisão, no Ensino Médio. É inegável que as escolas trabalham a Aritmética a partir da educação infantil, pois desde cedo as crianças adquirem certas competências aritméticas intuitivas no seu próprio meio. Mas é papel da escola de ensino básico desenvolver essa competência durante toda a vida escolar do aluno, tanto no Ensino Fundamental quanto no Ensino Médio, pois a Aritmética faz parte de uma educação de base, ajuda na formação de novos conceitos e desenvolve o pensamento analítico dos alunos.

Foi visto que o estudo da divisão, ensinado no início do 3º ciclo do Ensino Fundamental a partir de situações-problema que trabalham as ideias de quotização e partição e que priorizam a obtenção do quociente da divisão, podem ser aprofundadas no Ensino Médio com a demonstração formal do algoritmo de divisão e complementadas com o estudo das congruência e o lema dos restos que focam situações-problema envolvendo o resto da divisão.

O estudo dos números primos, máximo divisor comum e mínimo múltiplo comum que são trabalhados no 3º ciclo do Ensino Fundamental pode ganhar novo significado no Ensino Médio, quando o aluno pode conhecer e aplicar na resolução de situações-problema alguns teoremas elementares, mas de importância significativa como o lema de Euclides e a identidade de Bézout; a aplicação do importantíssimo Teorema Fundamental da Aritmética em muitos resultados, tais como a obtenção dos divisores bem como o número de divisores de um número natural, demonstrações da infinitude dos números primos, na caracterização do *mdc* e no estudo das congruências lineares.

A Aritmética pode ser coadjuvante em outros assuntos da matemática como por exemplo a contribuição dos números primos ao estudo da análise combinatória (fatoração do fatorial); o estudo das congruências na compreensão do ciclo trigonométrico bem como na demonstração de resultados envolvendo números complexos; e as equações diofantinas como instrumento de transição entre a Aritmética e a Álgebra.

Por fim, propomos uma abordagem mais abrangente do ensino da Aritmética do que as propostas tradicionalmente apresentadas nos livros didáticos da educação básica, uma proposta para o ensino de Aritmética que contribua para que os educadores formem uma escola que cumpra os objetivos oriundos das leis da LDB e diretrizes dos PCNs: "possibilitar ao aluno conhecimentos que o permita continuar sua aprendizagem após o Ensino Médio, que ele reconheça a Matemática como uma ferramenta importante para a compreensão do mundo à sua volta e tenha capacidade de contrubuir para a construção do conhecimento."

REFERÊNCIAS

[1] BRASIL. *Parâmetros Curriculares Nacionais: Matemática - Ensino de Quinta à Oitava Série*. Brasília: MEC/SEF, 1998. 148 p.

[2] BRASIL. *Parâmetros Curriculares Nacionais: Matemática - Ensino de Primeira à Quarta Série*. Brasília: MEC/SEF, 1997, 142 p.

[3] BRASIL. *Lei de Diretrizes e Bases da Educação Nacional*. Brasília: Senado Federal, Subsecretaria de Edições Técnicas, 2010.

[4] BRASIL. *Parâmetros Curriculares Nacionais - Ensino Médio: Parte 3*. Brasília: MEC/SEF, 1999.

[5] OLIVEIRA, S. José Plínio de. *Introdução à Teoria dos Números*. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2000.

[6] HEFEZ, A. *Elementos de Aritmética*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006.

[7] LIMA, E. L. et al. *A Matemática do Ensino Médio-Volume 1*. Rio de Janeiro: Sociedade Brasileira de Matematica, 2006.

[8] OLIVEIRA, K. I. M.; FERNANDEZ, A. J. C. *Iniciação à Matemática: um curso com problemas e soluções*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2010.

[9] FILHO, E. de A. *Teoria Elementar dos Números*. São Paulo: Nobel, 1981.

[10] HEFEZ, A. Indução matemática. *Programa de Iniciação Científica da OBMEP*, Niterói, 2009.

[11] RIBENBOIM, P. *Números primos: mistérios e recordes*. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, 2001.

[12] POLEZZI, M. Como obter o mdc e mmc sem fazer contas? *Revista do Professor de Matemática*, v. 51, p. 29–31, 2003.

[13] MATEMÁTICA, P. e gabaritos da Olimpíada Brasileira de. *Olimpíada Brasileira de Matemática*. Sociedade Brasileira de Matematica. Disponível em: ⟨http://www.obm.org.br/opencms/provas_gabaritos/⟩. Acesso em: 20 abr. 2014.

[14] HEFEZ, A. Iniciação à aritmética. *Programa de Iniciação Científica da OBMEP*, Niteroi, 2009.

[15] FOMIN, D.; GENKIN, S.; ITENBERG, I. *Círculos Matemáticos: A Experiência Russa*. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada, 2012.

[16] IEZZI, M. *Fundamentos de Matemática Elementar, vol. 1*. São Paulo: Atual Editora, 1993.

A APÊNDICES

A.1 Autorização da Escola

TERMO DE AUTORIZAÇÃO

Eu, **Francisco Ailton Alcantara**, professor de matemática do EEM Governador Adauto Bezerra situada na cidade de Juazeiro do Norte, solicito autorização para realizar pesquisa sobre "o ensino da aritmética na educação básica" com alunos das turmas do 3º ano A, B, C, D do turno vespertino da referida escola. Essa pesquisa faz parte do Trabalho de Conclusão de Curso que está sob orientação do professor **Flávio França Cruz**, professor do Curso de Matemática da Universidade Regional do Cariri (URCA).

Para desenvolvimento desse trabalho serão ministrados quatro encontros no turno matutino, no contra turno das aulas convencionais nos dias 09,12,16 e 23 de abril de 2014 de 07:00 as 11:00 horas.

O curso, fotografado e audiografado, tem como objetivo acadêmico analisar o processo de ensino e aprendizagem da aritmética básica tendo como base o aprofundamento do conteúdo visto no ensino fundamental que é amparando pelo Artigo 35, Inciso I da Lei de Diretrizes e Bases da Educação Nacional.

Vale ressaltar que os alunos participante foram autorizados por escrito pelos seus respectivos responsáveis legais a participar do curso e que na referida pesquisa, por força da lei, não constará nenhum meio para identificação dos alunos participantes.

_____

Professor Francisco Ailton Alcantara

_____

Direção da EEM Governador Adauto Bezerra

A.2 Autorização dos Pais

AUTORIZAÇÃO

Eu _____ portador do documento de identidade nº _____, e inscrição no CPF sob nº _____, residente e domiciliado no(a) _____, declaro para os devidos fins que AUTORIZO meu(minha) filho(a) _____ a participar do curso de "Iniciação a Aritmética", na data de 09,12,16 e 23 de abril de 2014, na EEM Governador Adauto Bezerra de 07:00 as 11:00 horas sob a tutela do Professor de Matemática da referida escola **Francisco Ailton Alcantara** portador do documento de identidade nº 96029467467 e inscrição no CPF sob nº 790.004.793-04.

Por ser a expressão da verdade, firmo o presente.

_____, ____ de _____ de 2014

_____
(Nome do pai, ou mãe ou responsável legal)