UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS UNIVERSITÁRIO DE PALMAS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL – PROFMAT

ANTONIO MACIEL GÓES

ARITMÉTICA: DIVISIBILIDADE, CONGRUÊNCIAS E NÚMEROS PRIMOS – UMA PROPOSTA PARA O ENSINO MÉDIO

PALMAS - TO
2015

ANTONIO MACIEL GÓES

ARITMÉTICA: DIVISIBILIDADE, CONGRUÊNCIAS E NÚMEROS PRIMOS – UMA PROPOSTA PARA O ENSINO MÉDIO

Trabalho de Conclusão de Curso apresentado ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para a obtenção do título de Mestre - Área de Concentração: Matemática. Orientadora: Prof. Dr^{a}. Hellena Christina Fernandes Apolinário.

PALMAS - TO
2015

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

G598a Goes, Antonio Maciel.

Aritmética: divisibilidade, congruências e números primos - uma proposta para o ensino médio. / Antonio Maciel Goes. – Palmas, TO, 2015.

74 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2015.

Orientadora : Hellena Christina Fernandes Apolinário

1. Divisibilidade. 2. Equações diofantinas. 3. Curiosidades. 4. Mundo estranho dos códigos de barras. I. Título

CDD 510

ANTONIO MACIEL GÓES

ARITMÉTICA: DIVISIBILIDADE, CONGRUÊNCIAS E NÚMEROS PRIMOS – UMA PROPOSTA PARA O ENSINO MÉDIO

Trabalho de Conclusão de Curso apresentado ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para obtenção do título de Mestre – Área de Concentração: Matemática. Orientadora: Dra. Hellena Christina Fernandes Apolinário.

Aprovada em 24 / 09 / 2015

BANCA EXAMINADORA

Hellena Apolinário

Prof. Dra. Hellena Christina Fernandes Apolinário (Orientadora-UFT)

Rogério Azevedo Rocha

Prof. Dr. Rogério Azevedo Rocha (UFT)

Prof. Dr. Cláudio de Castro Monteiro (IFTO)

Dedico este trabalho a minha esposa Mirinalda,
ao meu filho Wéblen
e também in memorian da minha tia Beatriz pela qual sempre tive um carinho especial.

Agradecimentos

Primeiramente, a Deus por todas as graças alcançadas, pois creio que sempre posso contar com sua proteção.

Aos meus pais, Milton e Valdeci, pelo incentivo e pela compreensão e por me ensinarem o caminho certo. Sei que sempre que preciso posso contar com vocês. Obrigado!

À minha esposa Mirinalda e ao meu filho Wéblen pelo incentivo, compreensão e carinho que sempre tiveram comigo. Obrigado!

À minha irmã Jaquilene e ao meu cunhado Josilei. Pelos conselhos plausíveis que sempre teve comigo em momentos difíceis ao longo desse caminho. Obrigado!

Ao meu tio Raimundo e a minha tia Davina. Valeu pela torcida e incentivo. Sempre torceram pela conclusão deste curso. Obrigado!

Aos meus primos Gilberto e Raidoney pelo apoio e incentivo e por saber que sempre posso contar com vocês. Obrigado!

Aos meus vizinhos Macedo e Antônia Francisca pelas sugestões principalmente ajuda que sempre me deram no decorrer deste trabalho. Obrigado!

Aos professores da Universidade Federal do Tocantins Campus de Palmas: Msc. Gilmar, Dr. Rogério, Dr. Andrés, Dr. Christian, Dr. Pedro, Drª. Betty. Obrigado!

À minha orientadora a Profª. Drª Hellena Christina Fernandes Apolinário, pela colaboração, compreensão e paciência que teve comigo no decorrer deste trabalho. Obrigado!

Aos meus colegas de curso, amigos sempre vou me lembrar de vocês com um carinho muito especial, pois sem vocês eu não tinha conseguido chegar até aqui! Obrigado!

Aos motoristas das vans que tiveram sempre uma atenção especial para que eu chegasse com segurança e sem atraso para as aulas do curso. Obrigado a todos!

A CAPES pela bolsa que foi fundamental para que eu pudesse terminar esse trabalho! Obrigado!

A todos que direta ou indiretamente contribuíram para o término deste trabalho

Só sei que nada sei, e o fato de saber isso,
me coloca em vantagem sobre aqueles que
acham que sabem alguma coisa... (Sócrates)

Resumo

O presente trabalho vem com o intuito de impulsionar a curiosidade dos estudantes, buscando uma interação entre o que é ensinado e o que constitui seu âmbito familiar, utilizando-se de uma pesquisa didático-pedagógica que propõe uma sequência de atividades experimentais e investigativas para trabalhar a aritmética modular e consequentemente a questão da divisibilidade utilizando-se como ferramentas as equações diofantinas como sendo um importante instrumento nesta questão. Essas atividades experimentais ocorreram em duas turmas de 1ª e 3ª série de uma escola pública rural no interior do Tocantins. Essa pesquisa propõe também o estudo dos números primos e algumas curiosidades, além de sugerir a implementação da aritmética dos restos, trazendo consigo algumas situações que torna seu uso importante, como para o entendimento do mundo misterioso dos códigos de barras. Sendo que essas atividades investigativas apontam que esta proposta de trabalho pode corroborar para uma aprendizagem por meio de aulas mais agradáveis e participativas para os alunos do Ensino Médio.

Palavras-chaves: Aritmética, Divisibilidade, Equações diofantinas, Curiosidades, Códigos de barras.

Abstract

This work comes in order to boost the curiosity of students, seeking an interaction between what is taught and what is your family environment, using a didactic and pedagogical research which proposes a series of experimental and investigative activities to work modular arithmetic and consequently the question of severability using as tools the Diophantine equations as an important tool in this question.Being understood that these experimental activities occurred in two classes 1st and 3rd series of a rural public school in the interior of Tocantins. That research also proposes the study of prime numbers and their curiosity, besides suggesting the implementation of the arithmetic of the remains, i.e. congruence, bringing some situations that makes its important use, such as for understanding the mysterious world of barcodes. And these investigative activities show that this proposed work could help to a learning through more pleasant and participative classes for high school students.

Key-words: Arithmetic, Severability, Diophantine equations, Curiosities, Bar codes.

Lista de ilustrações

Sumário

1 INTRODUÇÃO

O presente trabalho pretende contribuir com propostas curriculares para o Ensino Médio com o objetivo de impulsionar a curiosidade dos estudantes em sala de aula de Matemática, em particular de Aritmética, buscando uma interação entre o que é ensinado e o que constitui seu espaço familiar.

Apesar dos esforços por parte dos governantes e educadores, o Ensino Médio ainda deixa muito a desejar, em muitos aspectos, como falta de materiais adequados, profissionais comprometidos e com formação adequada a sua área de atuação e como também ambientes agradáveis, entre outros.

Outro grande problema enfrentado pelos governantes e profissionais de educação, é encontrar maneiras de trabalharem conteúdos importantes para o Ensino Médio e, ao mesmo tempo adaptar esses conteúdos a realidade de cada comunidade, sem que haja perda de conhecimentos predominantes.

No que diz respeito ao caráter instrumental da Matemática no Ensino Médio, ela deve ser vista pelo aluno como um conjunto de técnicas e estratégias para serem aplicadas a outras áreas do conhecimento, assim como para a atividade profissional.

Não se trata dos alunos possuírem muitas e sofisticadas estratégias, mas sim, de desenvolverem a iniciativa e a segurança, para adaptá-las a diferentes contextos, usando-as adequadamente no momento oportuno. Neste sentido, é preciso que o aluno perceba a Matemática, como um sistema de códigos e regras, que a torna uma linguagem de comunicação de ideias, que permite modelar a realidade e interpretá-la (BRASIL[1]).

Segundo a Lei de diretrizes e bases da educação no seu art. 35:

> "O Ensino Médio, etapa final da educação básica, com duração mínima de três anos, terá como finalidade a preparação básica para o trabalho e a cidadania do educando, para continuar apreendendo, de modo a ser capaz de se adaptar com flexibilidade, a novas condições de ocupação ou aperfeiçoamento posteriores". (BRASIL [2])

Assunto discutido amplamente, no presente estudo. Porém este trabalho não pretende resolver o problema da matemática do Ensino Médio, e sim contribuir para o processo de evolução desse ensino, com ideias novas a serem trabalhadas, no decorre desse período.

Em síntese, como objetivo do presente trabalho, ressalta-se a chamada de atenção para a necessidade de se elaborar ideias novas, para otimizar o ensino da aritmética nas escolas de Ensino Médio. Com mais criatividade e consequentemente poder de atração e persuasão entre os jovens estudantes da matemática contemporânea.

Defende-se no presente estudo, a importância de se aspergir as noções aritméticas, para além de seu resumido universo, no qual tem sido restrita, principalmente no Ensino Médio, quando o estudo desta fascinante matéria, sofre uma espécie de estagnação e redução de seus horizontes potenciais, para poder ser colocada no currículo oficial e consequentemente, reduzir suas chances de aplicabilidade, em todos os seguimentos de estudos, nos quais a aritmética, exerce um imensurável fator de novas e inusitadas probabilidades.

No ensino fundamental, o aluno completamente inocente sobre a matemática, se deslumbra com sua humilde expressão que é a aritmética. Dos dedos às equações no papel, tudo é novidade e é simplicidade. E quando este mesmo aluno, entra no Ensino Médio, depara-se com um resumo mal formado, de uma matéria escolar, que o havia encantado no ensino fundamental.

E a matemática acaba por ser "taxada" de "matéria difícil", quando na verdade deveria ser justamente a partir do Ensino Médio, que o aluno chegasse ao que em linguagem poética, se resumiria no "sublime da matemática". Quando ele começaria a descobrí-la em tudo o mais.

A aritmética está em tudo, na arte, na física, na química, na linguagem, no universo. Porque não nos corações dos jovens estudantes brasileiros?

O trabalho científico em pauta, procura humildemente, alcançar esta resposta. Ou ao menos, dar os primeiros passos para alcançá-la. O leitor pesquisador, encontrará nas próximas páginas, do presente estudo científico, o resultado de uma árdua tentativa honesta, de propor um debate sobre o mencionado tema.

Como metodologia elegeu-se a mais simples utilização de problemas do cotidiano dos educandos com o intuito de informar, explorar e ensinar os conteúdos propostos, além de atividades diferenciadas e a apresentação de algumas curiosidades do mundo dos números.

O segundo capítulo apresenta algumas proposições importantes para o estudo da aritmética, o terceiro vem expor um método para o cálculo do máximo e do mínimo divisor comum, o quarto começa por introduzir o conteúdo de equações diofantinas onde o mesmo estende-se a apresentações de algumas atividades diferenciadas que podem servir de alicerces para tal conteúdo, prosseguindo vem-se números primos e suas curiosidades, no quinto capítulo e finalmente vem o sexto e último capítulo propondo o estudo de congruências mostrando algumas de suas múltiplas aplicações como no entendimento do mundo estranho dos códigos de barras assuntos esses que poderão serem trabalhados no decorrer do ensino médio.

2 PRELIMINARES

2.1 Algumas propriedades importantes

Os números naturais foram um dos pensamentos mais antigo que se pode conceber, entrementes o seu desenvolvimento de uma concepção intuitiva para uma caracterização mais elaborada foi muito devagar. Somente nos últimos anos do século XIX, quando os alicerces até então da matemática começaram a ser discutidos e intensamente reconsiderados, é que a concepção de número passou ser apoiada em conceitos da teoria dos conjuntos, estimados como mais primordiais.

Para incorporar mais precipitadamente o objeto de estudo deste trabalho, que são as divisibilidades, as equações diofantinas e os números primos é importante entender as propriedades sobre os números naturais, que serão apresentadas a seguir, devido que, para resolver qualquer problema é essencial, conhecer as técnicas exigidas em cada caso.

Note que as propriedades assim como as definição que serão apresentadas ao longo desse trabalho poderão ser encontradas em sua maioria no livro Elementos de Aritmética [3].

Antes da apresentação da primeira propriedade vêm-se definir duas notações: Definiremos que a divide b e, que a não divide b pelas respectivas notações: $a \mid b$ e $a \nmid b$.

Proposição 2.1.1. *Sejam a e b números naturais não nulos e seja c um outro número natural se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Se $a \mid b \Rightarrow b = a \cdot k$ (I), $k \in \mathbb{N}$; se $b \mid c \Rightarrow c = b \cdot w$ (II), $w \in \mathbb{N}$, substituindo (II) em (I). Tem-se, $c = (a \cdot k) \cdot w = a \cdot (k \cdot w) \Rightarrow a|c$ □

Proposição 2.1.2. *Tomando os números a e c naturais, com $a \neq 0$. Vale então que:*

(i) $1 \mid c$

(ii) $a \mid a$

(iii) $a \mid 0$

Demonstração. A prova para (i), (ii) e (iii) vem-se das respectivas igualdades: $c = 1 \cdot c$, $a = a \cdot 1$ e $0 = a \cdot 0$. □

Tem-se um detalhe que não pode passar sem sua atenção que é a seguinte: $a \mid 0$ porém $0 \nmid a$.

Note que ao longo deste trabalho serão apresentadas algumas propriedades juntamente com sua demonstração, porém, não será necessário que apresente todas as demonstrações aos alunos. Esses testemunhos servirão, apenas para que o professor tenha segurança para apresentá-las junto aos educandos.

Proposição 2.1.3. *Sejam a, b, c e $d \in \mathbb{N}$ com $a \neq 0$, Então:*

(i) $a \mid b$ *e* $c \mid d \Rightarrow a \cdot c \mid b \cdot d$ *(quando* $c \neq 0$*)*

(ii) $a \mid b \Leftrightarrow a \mid c$ *(quando* $a \mid (b+c)$*)*

(iii) $a \mid b \Leftrightarrow a \mid c$ *(quando* $a \mid (b-c)$ *e* $b \geq c$*)*

Demonstração. De (i), como $a \nmid b$ então existe $f \in \mathbb{N}$, tal que $b = f \cdot a$ (I) do mesmo modo têm a igualdade $d = g \cdot c$ (II), com $g\mathbb{N}$. Multiplicando (I) e (II) lado a lado, ou seja,

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

Portanto, $a \cdot c \mid b \cdot d$.

De (ii) apresenta-se aqui a ida da proposição, pois a volta é totalmente análoga.

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

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

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

$$b = g \cdot a \tag{2.2}$$

Substituindo 2.2 em 2.1, tem-se

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

Como $c \in \mathbb{N}$, logo $f \cdot a > g \cdot a$, ou seja, $f - g > 0$ e portanto,

$$c = (f - g) \cdot a \Rightarrow a \mid c$$

De (iii) a Demonstração idêntica ao item anterior provocando sua volta. Tomando que $a \mid c$, então $\exists f \in \mathbb{N}$ tal que

$$c = f \cdot a \tag{2.3}$$

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

$$b - c = g \cdot a \tag{2.4}$$

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

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

□

Proposição 2.1.4. *Sejam a,b,c,f e g todos números naturais com $a\neq 0$ e satisfazendo $a\mid b$ e $a\mid c$, então*

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

(ii) $a\mid(f\cdot b-g\cdot c)$ *desde que* $f\cdot b\geq g\cdot c$

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

Para (i)

Como $a\mid b$ e $a\mid c$, então existem m e $n\in\mathbb{N}$, tais que

$$b=m\cdot a\Rightarrow f\cdot b=f\cdot m\cdot a \tag{2.5}$$

$$c=n\cdot a\Rightarrow g\cdot c=g\cdot n\cdot a \tag{2.6}$$

Somando as equações 2.5 e 2.6 obtem-se,

$$f\cdot b+g\cdot c=f\cdot m\cdot a+g\cdot n\cdot a$$
$$f\cdot b+g\cdot c=a\cdot(f\cdot m+g\cdot n)$$

Como $(f\cdot m+g\cdot n)\in\mathbb{N}$, conclui-se, que $a\mid(f\cdot b+g\cdot c)$ □

Para as propriedades seguintes usa-se o último axioma de Peano[1] , no qual afirma que para uma sentença ser válida para todo n natural, tem-se que verificar a validade das 3 propriedades a seguir:

i) $P(0)$ ser verdadeira;

ii) $P(n)$ ser verdadeira, para algum, $n\geq 0$, $n\in\mathbb{N}$ *(hipótese auxiliar!)*

iii) Provar que $P(n+1)$ é verdadeira *(tese!)*

[1] Giuseppe Peano foi um matemático italiano. Autor de dezenas de livros e artigos, ele foi um dos fundadores da lógica matemática e da teoria dos conjuntos, para as quais ele também contribuiu bastante na notação

Esse tipo de demonstração é conhecido como método da Indução Finita. Essa propriedade é exclusiva dos números naturais, ou seja, não se aplica aos racionais e muito menos aos reais. Tendo consultado alguns livros didáticos do Ensino Médio como: SILVA[4], GIOVANNI[5] DANTE[6], entre outros, o único que propõe, e assim mesmo de maneira superficial indução finita no Ensino Médio é o último autor.

Entendemos que esse conteúdo é muitíssimo importante para a formação do aluno do Ensino Médio, pois faz com que o educando busque estratégia de solução de problemas deste tipo, melhore seu raciocínio elevando assim seu conhecimento para demonstrar outros tipos de problemas ou questões matemáticas que necessitam de tal aplicação como por exemplo para provar a validade das fórmulas das progressões aritméticas e geométricas nas quais podem-se, utilizar deste método de demonstração, assim como utilizaremos, para as três propriedades seguintes:

Proposição 2.1.5. *Sejam $a,b,n \in \mathbb{N}$, com $a > b > 0$. Tem-se, $a-b \mid a^n - b^n$.*

Demonstração. Provaremos por indução finita sobre n.

i) $P(0)$ é verdadeira, pois $a-b \mid a^0 - b^0 = 0$.

ii) Suponha-se, que $a-b \mid a^n - b^n$ é verdadeira *(hipótese auxiliar)*

Tem-se, que $a^{(n+1)} - b^{(n+1)} = a^n \cdot a - b \cdot a^n + b \cdot a^n - b \cdot b^n = a^n \cdot (a-b) + b(a^n - b^n)$
Como $a-b \mid a^n - b^n$ *(hipótese auxiliar)* decorre da proposição 2.1.4 que

$$a-b \mid a^{(n+1)} - b^{(n+1)}$$

□

Proposição 2.1.6. *Sejam $a,b,n \in \mathbb{N}$ com $a+b \neq 0$. Tem-se que , $a+b \mid a^{(2n+1)} + b^{(2n+1)}$*

Demonstração. O leitor interessado nesta demonstração poderá encontrá-la, no livro Elementos de Aritmética [3]. □

Proposição 2.1.7. *Sejam $a,b,n \in \mathbb{N}$, com $a \geq b > 0$. Tem-se que $a+b \mid a^{2n} - b^{2n}$.*

Demonstração. Mais uma vez, usa-se indução sobre n para demonstrá-la. Porém não a faremos aqui mais o leitor interessado poderá encontrá-la no livro Aritmética [7]. □

Proposição 2.1.8. *(Propriedade da Boa Ordem). Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.*

Demonstração. A demonstração desta proposição se encontra no livro Elementos de Aritmética [3]. □

3 UM MÉTODO PARA O ESTUDO DA DIVISÃO

Apesar de que um número natural a nem sempre divide outro número natural b, mesmo sendo $b > a$. EUCLIDES[8], afirma em seus Elementos que em qualquer ocasião é possível executar a divisão de b por a, com resto menor que a, sendo este também um número natural. Como consequência disso, no qual será mostrado mais adiante, é que a divisão euclidiana tem um apreço muito grande na obra de Euclides, e portanto é essencial para a teoria dos números e também para a aritmética em geral.

3.1 A divisão no contexto do ensino médio

Ensinar a dividir não é uma tarefa muito fácil, principalmente com a tecnologia que existe nos tempos atuais como calculadoras, celulares, computadores que executam esse processo com a velocidade da luz. Sendo este um problema enfrentado por muitos docentes em sala de aula quando se quer uma divisão com resto, pois os alunos em sua maioria detêm pelo menos um destes aparatos citados acima o que dificulta o trabalho de aprendizagem dos mesmos que estão habituados a utilizá-los, e não querem fazer e as vezes nem sabem ou se esqueceram do processo tradicional que utilizavam no Ensino Fundamental.

Por exemplo, quando o docente vai lecionar na 3ª série do Ensino Médio encontra-se, muita dificuldade por parte dos educandos nas atividades propostas de números complexos, pois o processo de simplificar as potências exige a divisão com resto. Então sabendo disso, vem-se aqui nesta seção tentar minimizar esses problemas com a apresentação da divisão euclidiana, procurando assim chamar a atenção dos alunos para a importância da divisão com resto.

O educador talvez esteja se perguntando, como revisar a divisão euclidiana e não causar situações inconvenientes como a seguinte, "isso é conteúdo do Ensino Fundamental"? Mesmo eles tendo muitas dificuldades para realizar tal tarefa, uma de nossas sugestões é contextualizar as questões com problemas do cotidiano destes alunos, bem diferente do nosso tempo no qual era usado apenas os números sem um contexto, sem uma aplicação prática.

A seguir apresentaremos um teorema que dará início ao processo da implementação da revisão da divisão euclidiana no Ensino Médio.

Teorema 3.1.1. *(Divisão Euclidiana) Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que*

$$b = a \cdot q + r, \ com \ r < a$$

Demonstração. A demonstração apresentada a seguir pode ser encontrada no livro Elementos de Aritmética[3].

Suponha que $b > a$ e considere, enquanto forem números naturais, a lista descrita abaixo:

$$b, \ b-a, \ b-2a, \ \cdots, \ b-na, \ \cdots$$

Pela proposição 2.1.8 (Propriedade da Boa Ordem) o conjunto T formado pelos elementos acima tem um menor elemento $r = b - q \cdot a$. Tem-se que provar que r tem a requerida propriedade, ou seja, que $r < a$.

Se $a \mid b$, então $r = 0$ e nada mais tem-se, a provar. Por outro lado se $a \nmid b$, então $r \neq a$, e , portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isso ocorresse existiria um número natural $c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - q \cdot a$ Tem-se

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

Contradição pelo fato de r ser o menor elemento de T.

Portanto, tem-se, que $b = a \cdot q + r$ com $r < a$, o que mostra a existência de q e r.

Agora, provaremos a unicidade.

Observe-se, que dados dois elementos distintos de T, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Logo se

$r_1 = b - a \cdot q_1$ e $r_2 = b - a \cdot q_2$, com $r_1 < r_2 < a$, teríamos $r_2 - r_1 \geq a$ o que acarrentaria $r_2 \geq r_1 + a \geq a$, (absurdo!).

Portanto , $r_1 = r_2$.

Daí, segue que $b - a \cdot q_1 = b - a \cdot q_2 \Rightarrow a \cdot q_1 = a \cdot q_2$ e portanto $q_1 = q_2$

□

Observe que a demonstração desse teorema acima produz um algoritmo para o cálculo do quociente e do resto da divisão de um número natural por outro, fazendo uso de subtrações consecutivas. No Ensino Médio, este processo evitará problemas como a dificuldade em divisão, como veremos no exemplo a seguir:

Exemplo 3.1.1: Um professor pretende formar grupos com 6 integrantes em uma sala que contém 22 alunos. Determine quantos grupos serão formados com 6 componentes e, quantos alunos restarão para formar um outro grupo menor, formado pelo restante dos educandos?

Solução: Seja q a quantidade de grupos com 6 integrantes e r o restante dos alunos. Tem-se que dos 22 alunos da sala, serão retirados $1 \cdot 6 = 6$ alunos, para formar o primeiro grupo, ou seja, restarão $22 - 1 \cdot 6 = 16$ alunos, veja que o produto $1 \cdot 6$ tem o primeiro número como a quantidade de grupos formados até aquele instante e o segundo número representa a quantia de componentes em cada grupo. Seguindo têm-se que ao formar o segundo grupo $22 - 2 \cdot 6 = 10$ alunos restarão, veja que mais uma vez o produto é estabelecido respectivamente como sendo o número da quantidade de grupos 2 verso o número que representa a quantia de componentes em cada grupo 6. Então percebe-se que o problema pode ser resolvido utilizando-se de subtrações sucessivas, ou seja,

$$22 - 1 \cdot 6 = 16;\ 22 - 2 \cdot 6 = 10;\ 22 - 3 \cdot 6 = 4 < 6$$

De onde segue que $q = 3$ (quantidade de grupos de 6 componentes) e $r = 4$ (representa a quantidade de alunos do grupo menor).

Aparentemente, tem-se a sensação de não haver a obrigatoriedade de se demonstrar a unicidade de q e r no teorema 3.1.1, visto que o resultado da subtração em cada passagem é único e, por consequência, r e q têm valores bem definidos. verdade é que exibe-se, um meio de calcular q e r, cumprindo as condições do teorema, porém de modo algum garante que fazendo-se, uso de outro método não teríamos outros valores para q e r. Por isso a exigência de se demonstrar a unicidade.

Note que no exemplo 3.1.1 não foi feito nenhuma divisão porém chegou-se, no resultado da divisão desejada, ou seja, se o aluno tem dificuldade na divisão, o teorema 3.1.1 abre um leque de possibilidade para esse estudante conseguir resolver problemas de divisão. Não vem-se aqui defender que não se deve ensinar a dividir, ou que a divisão não é importante, e sim que diante das dificuldades de alguns educandos que não foram bem sucedidos na aprendizagem da divisão, eles possam acompanhar o conteúdo proposto naquele instante utilizando esse outro método.

3.2 Um método para o cálculo do MDC

Os conceitos e resultados contidos nesta seção encontram-se, em sua maioria, no Livro elementos de Euclides [8]. É notável a sua atualidade, apesar dos quase dois mil anos que nos separam de sua criação.

Denota-se, que um número d é o máximo divisor comum de dois números a e b ambos naturais se conter as seguintes propriedades:

i) d é divisor comum de a e b

ii) Se c é divisor comum de a e b, então $c \mid d$

O máximo divisor comum de dois números a e b, se existir, é único, e será denotado aqui de duas maneiras (a,b) ou $mdc(a,b)$ procurando a melhor maneira de representá-lo em cada caso.

Encontrar o Máximo Divisor Comum (MDC) entre dois números nem sempre é uma tarefa fácil como vem-se mostrar mais adiante, pois quando esses números são pequenos, pode-se fazer como se faz no Ensino Fundamental, ou seja, encontra-se todos os divisores de cada número e verifica qual é o maior divisor comum a esses dois números.

Por exemplo, os divisores comuns entre 12 e 18, são 1,2,3 e 6, logo o Máximo Divisor Comum, ou seja, $mdc(12,18) = 6$.

Porém esse método se torna ineficaz quando se trata de números muito grandes como o exemplo a seguir

Exemplo 3.2.1: Um aluno pesquisador chega ao seu professor de Matemática com a seguinte pergunta: Sempre é possível determinar o Máximo Divisor Comum de dois números naturais? O professor mesmo surpreso com a pergunta respondeu que SIM, é só fatorar esses números em fatores primos. Então o aluno, lhe mostrou uma questão que tinha encontrado em suas pesquisas, fazendo uma outra pergunta: como vou fatorar esses números?

$$mdc\left(\frac{2^{120}-1}{2^{10}-1}, 2^{10}-1\right)$$

O professor respondeu que esse tipo de problema tem uma sofisticada solução para resolvê-lo, e que o mesmo não é possível fatorar, e sim utilizar um outro método, o lema de Euclides que também serve para os números menores, iguais aos vistos no Ensino Fundamental.

A solução apresentada pelo professor a esse aluno será apresentada mais adiante onde o mesmo utilizou o lema de Euclides.

Por isso Euclides em seus estudos sobre algoritmo chegou em uma propriedade (lema) muito importante para o estudo de Máximo Divisor Comum (MDC) e que nos levou a propor esse novo método no Ensino Médio, pois apresenta propriedades importantes tanto para o cálculo do mdc como para o algoritmo de Euclides, sendo que este método não deixa nada a desejar aos métodos utilizados no Ensino Fundamental pelo contrário esse método é mais eficaz pois, servirá para um campo maior que os métodos antecessores. Apresenta-se a seguir, o lema citado anteriormente:

Lema 3.2.1. *(Lema de Euclides) Sejam* $a,b,n \in \mathbb{N}$ *com* $a < n \cdot a < b$*. Se existe* $(a, b - n \cdot a)$*, então* (a,b) *existe e*

$$(a,b) = (a, b - n \cdot a)$$

Demonstração. Seja $d = (a, b - n \cdot a)$. Como $d \mid a$ e $d \mid (b - n \cdot a)$, segue que d divide $b = b - n \cdot a + n \cdot a$. Logo , d é um divisor comum de a e b. Consequentemente c é um divisor comum de a e $b - n \cdot a$ e, portanto, $c \mid d$. Isso prova que $d = (a,b)$

□

Observe que o mesmo método usado na demonstração do Lema de Euclides, servirá para mostrar que, para quaisquer $a,b,n \ \in \mathbb{N}$,

$$(a,b) = (a, b + n \cdot a)$$

Ou se $n \cdot a > b$, segue se que

$$(a,b) = (a, n \cdot a - b)$$

Essa sentença torna positiva para o cálculo do *mdc*, como nota-se, no seguinte exemplo, e será essencial para instituirmos o algoritmo de Euclides que permitirá, com muita eficácia, calcular o *mdc* entre dois números naturais quaisquer.

Segundo os Parâmetros Curriculares Nacionais:

> "As situações de aprendizagem devem se desenvolver a partir das experiências significativas vividas anteriormente por eles, na escola ou fora dela, pois elas os levam a construir, mais facilmente, ideias a respeito dos fenômenos. Além disso, por estarem baseadas em experiências cotidianas, essas ideias costumam ser sólidas e, muitas vezes, incompatíveis com os conceitos científicos que o professor pretende lhes apresentar. Por esse motivo, é necessário que se estabeleçam vínculos entre o conteúdo pedagógico, que é apresentado ao aluno, e aqueles conhecimentos que já integram a sua estrutura cognitiva".(BRASIL [9]).

Pensando nisso procuramos dar significados a esses conteúdos propostos com exemplos “problemas” do cotidiano desses educandos de um modo geral, como se pode perceber no exemplo seguinte:

Exemplo 3.2.2:(Ver [10]) Uma indústria de tecidos fabrica retalhos de mesmo comprimento. Após realizarem os cortes necessários, verificou-se que duas peças restantes tinham as seguintes medidas: 156 centímetros e 234 centímetros. O gerente de produção ao ser informado das medidas, deu a ordem para que o funcionário cortasse o pano em partes iguais e de maior comprimento possível. Como ele poderá resolver essa situação?

Solução:

Como o funcionário designado a fazer os cortes tem-se que fazê-lo de maneira que os pedaços sejam todos iguais e que sejam os maiores possíveis o problema em questão trata-se de encontrar o MDC de 156 e 234. Como $234 = 156 + 78$, então têm-se,

$$mdc(156, 234) = mdc(156, 156 + 78)$$

Utilizando o Lema de Euclides 3.2.1 obtem-se

$$mdc(156, 156 + 78) = mdc(156, 78) = 78$$

Logo o funcionário terá que fazer cortes com 78 cm de comprimento.

Proposição 3.2.1. *Dados* $a, m \in \mathbb{N}$ *com* $a > 1$*, tem-se que*

$$\left(\frac{a^m - 1}{a - 1}, a - 1 \right) = (a - 1, m)$$

Demonstração. A demonstração dessa propriedade poderá ser encontrada no livro Elementos de Aritmética[3]. □

3.2.1 Algoritmo de Euclides

O algoritmo de Euclides é um dos conceitos mais importante para o estudo da divisibilidade sendo que existem inúmeras aplicabilidades para tal algoritmo, e uma dessas aplicação é o seu uso para encontrar as soluções de problemas que recaem em equações diofantinas assunto este que será abordado no próximo capítulo.

Segundo HEFEZ [3]: "a demonstração construtiva da vivência do mdc colocada por Euclides em Os elementos (Livro VII, prop.2) tem uma perfeição do ponto de vista computacional que pouco se fez para complementá-lo em mais de vinte séculos".

Teorema 3.2.1. *(Algoritmo de Euclides) Dados* $a, b \in \mathbb{N}$*, podemos supor* $a \leq b$*. Se* $a = 1$ *ou* $a = b$*, ou ainda* $a \mid b$*, sabemos que* $(a, b) = a$*.*

Demonstração. Suponhamos, então, que $1 < a < b$ e que $a \nmid b$. Logo, pela divisão euclidiana, podemos escrever

$$b = a \cdot q_1 + r_1 \quad \text{com } r_1 < a$$

Tem-se duas possibilidades:

a) $r_1 \mid a$, e em tal caso, pelo lema de Euclides

$$r_1 = (a, r_1) = (a, b - q_1 a) = (a, b)$$

E termina assim o algoritmo, ou

b) $r_1 \nmid a$,e em tal caso podemos efetuar a divisão de a por r_1, obtendo

$$a = r_1 \cdot q_2 + r_2 \text{ tendo } r_2 < r_1$$

Outra vez têm-se duas possibilidades:

a') $r_2 \mid r_1$ e, em tal caso, outra vez pelo lema de Euclides

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

E assim não vai além disso, ou

b') $r_2 \nmid r_1$ e, em tal caso pode-se, efetuar a divisão de r_1 por r_2, obtendo-se

$$r_1 = r_2 \cdot q_3 + r_3 \text{ tendo } r_3 < r_2$$

Esse método não poderá continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > r_3 > \cdots$ que não possui menor elemento, o que não é possível pela Propriedade da Boa Ordem. Logo, para algum n, têm-se que $r_n \mid r_(n-1)$ o que implica que $(a, b) = r_n$.

$\square$

O algoritmo acima pode ser esquematizado da seguinte forma primeiro, fazemos a divisão $b = a \cdot q_1 + r_1$, depois utilizarmos um diagrama para representa-la:

	q_1	
b	a	
r_1		

Tabela 1 – Algoritmo de Euclides

Prosseguindo faz-se, a divisão $a = r_1 \cdot q_2 + r_2$ e colocamos os números no diagrama

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Tabela 2 – Algoritmo de Euclides

Continuando o procedimento sob o aspecto de ser possível a divisão, tem-se

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

Tabela 3 – Algoritmo de Euclides

Exemplo 3.2.3: Antônio e Carlos são grandes amigos e empresários bem sucedidos, em certo final de ano resolveram distribuir presentes a comunidade do local em que moram. Para isso, Antônio conseguiu 381 presentes e Carlos outros 273. Combinaram entre eles, de dividir esses presentes em kits com o máximo possível de presente em cada um, de maneira que não sobrasse nenhum presente, e que cada kit contasse com a mesma quantidade de presente, ou seja, um kit de Antônio possuía a mesma quantidade de presente que os de Carlos. Sabendo que cada um fez seus próprios kits, sem troca de presente entre eles, pergunta-se quantos presentes possuíam cada kit?

Solução: Observe que cada kit terá a quantidade de presente igual ao Máximo Divisor comum entre 381 e 273. Portanto, utilizando a tabela 3, ou seja, o Algoritmo de tem-se,

	1	2	1	2	8	2
381	273	108	57	51	6	$3 = mdc$
108	57	51	6	3		

Tabela 4 – Algoritmo de Euclides

Logo cada kit possuirás 3 presentes.
Veja que o Algoritmo de Euclides nos gera:

$$3 = 51 - 8 \cdot 6$$
$$6 = 57 - 1 \cdot 51$$
$$51 = 108 - 1 \cdot 57$$

$$57 = 273 - 2 \cdot 108$$
$$108 = 381 - 1 \cdot 273$$

Do qual procede que

$$3 = 51 - 8 \cdot 6 = 51 - 8 \cdot (57 - 1 \cdot 51) = 9 \cdot 51 - 8 \cdot 57$$

Daí segue que

$$3 = 9 \cdot (108 - 1 \cdot 57) - 8 \cdot 57 = 9 \cdot 108 - 17 \cdot 57$$

Consequentemente

$$3 = 9 \cdot 108 - 17 \cdot (273 - 2 \cdot 108) = 43 \cdot 108 - 17 \cdot 273$$

Continuando com o procedimento tem-se,

$$3 = 43 \cdot (381 - 1 \cdot 273) - 17 \cdot 273$$

Portanto,

$$3 = 43 \cdot 381 - 60 \cdot 273$$

Observe que através do Algoritmo de Euclides pode-se escrever $3 = (273, 381)$ como múltiplo de 381 subtraído por um múltiplo de 273.

Note que o algoritmo euclidiano tem um papel importantíssimo neste procedimento, e o mesmo servirá para que possamos resolver o exemplo 3.2.1 apresentado anteriormente.

Para resolveremos este exemplo utilizaremos a proposição 3.2.1 e o teorema 3.2.1.

Solução (Do Exemplo 3.2.1):

Pela propriedade 3.2.1 tem-se

$$\left(\frac{2^{120}-1}{2^{10}-1}, 2^{10}-1\right) = \left(\frac{\left(2^{10}\right)^{12}-1}{2^{10}-1}, 2^{10}-1\right) = \left(2^{10}-1, 12\right) = (1023, 12)$$

Consequentemente pelo teorema 3.2.1 tem-se que

	85	4
1023	12	$3 = mdc$
3		

Tabela 5 – Algoritmo de Euclides

Logo

$$(1023, 12) = 3$$

Portanto

$$\left(\frac{2^{120}-1}{2^{10}-1}, 2^{10}-1\right) = 3$$

Este método exposto por Euclides facilita o cálculo do *mdc* tanto no Ensino Fundamental como no Ensino Médio, pois ao contrário dos procedimento anteriores nos quais eram necessário expor todos os divisores, para assim encontrar o maior divisor comum ou utilizar a decomposição em fatores de primos, esse procedimento só necessita de fazer divisões sucessivas facilitando o cálculo do Máximo Divisor Comum. Por isso "compramos" este procedimento como um marco que facilitará o trabalho do professor do Ensino Médio, principalmente quando o docente for introduzir equações diofantinas que é uma das nossas propostas na qual será levantada no próximo capítulo.

Apresentaremos aqui algumas propriedades importantes, nas quais acreditamos serem essenciais para um melhor entendimento por parte dos estudantes do método apresentado para o cálculo do máximo divisor comum de dois ou mais números naturais.

Corolário 3.2.1. *Dados $a, b \in \mathbb{N}$, tem-se que*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

Demonstração. A demonstração desse corolário poderá ser encontrada no livro elemento de aritmética [3]. $\square$

Note que quando o Máximo Divisor Comum entre dois números naturais é 1, logo os mesmo serão proferido como co-primos ou primos entre si.

Proposição 3.2.2. *Dois números naturais a e b são primos entre si se, e somente se, existem números naturais n e m tais que $n \cdot a - m \cdot b = 1$.*

Demonstração. A demonstração dessa propriedade mais uma vez encontra-se no livro elementos de artimética[3]. $\square$

Perceba que essa proposição acima é uma ferramenta muito importante que permitirá resolver vários problemas entre eles para verificar se uma equação do tipo $ax - by = c$, tem ou não solução, assunto este que será tratado no próximo capítulo como já foi mencionado anteriormente.

Proposição 3.2.3. *Dados números naturais* $a_1, a_2, \cdots, a_n$ *, existe o seu mdc e*

$$(a_1, \cdots, a_n) = (a_1, \cdots, (a_{n-1}, a_n))$$

Demonstração. A demonstração dessa proposição se faz por indução finita, não a faríamos aqui porém o leitor interessado poderá encontrá-la no livro Elementos de Aritmética[3]. □

Observe que calcular o *mdc* de $a_1, a_2, \cdots, a_n$, n números naturais é o mesmo que encontrar o Máximo Divisor Comum de dois desses números, depois tornar fazer o *mdc* do *mdc* calculado anteriormente com o próximo número. Fazendo-se, esse procedimento até fazer o *mdc* com o último número da lista, encontrando assim o *mdc* de $a_1, a_2, \cdots, a_n$.

O exemplo a seguir ilustra com mais detalhes o procedimento apresentado por essa proposição.

Exemplo 3.2.4: (Ver [11]) No almoxarifado de certa repartição pública há três lotes de pastas iguais: o primeiro com 60, o segundo com 105 e o terceiro com 135 pastas. Um funcionário deve empilhá-las, colocando cada lote de modo que, ao final de seu trabalho, ele tenha obtido pilhas com igual quantidades de pastas. Nestas condições, qual é o menor número de pilhas que ele obterá?

Solução:

Note que essa é uma aplicação do MDC. Pois se o funcionário quer todas as pilhas com a mesma quantidade de pastas iguais, vai ter que descobrir quantas terás em cada pilha, só então, vai ter como descobrir o número total de pilhas. Sendo que ele pretende ter o máximo número de pastas em cada pilha, ou seja, o valor máximo que divide os três lotes que é

$$mdc(60, 105, 135)$$

Utilizando a proposição 3.2.3 tem-se que

$$mdc(60, 105, 135) = mdc((60, 105), 135)$$

Consequentemente do lema 3.2.1 tem-se, $mdc(60, 105) = mdc(60, 2 \cdot 60 - 15) = mdc(60, 15) = 15$ segue que

$$mdc(60,105,135) = mdc((60,105),135) = mdc(15,135)$$

Novamente usando o lema 3.2.1 segue que

$$mdc(15,135) = mdc(15, 8\cdot 15 + 15) = 15 \text{ número de pastas em cada pilha}$$

Como queremos o número de pilhas basta dividir cada lote pelo Máximo Divisor Comum que é 15.

Fazendo o cálculo tem-se, $\frac{60}{15} + \frac{105}{15} + \frac{135}{15} = 4 + 7 + 9 = 20$ pilhas

3.3 Um método para o cálculo do MMC

O conteúdo de Mínimo Múltiplo Comum muitas das vezes é deixado de lado por professores do Ensino Fundamental e principalmente do Ensino Médio, nos quais não é dado a sua merecida importância.

No entanto esse conteúdo se torna importante e necessário quando tem-se que somar duas ou mais frações que é uma dificuldade encontrada por muitos alunos do Ensino Fundamental e também do Ensino Médio, sendo que para tal cálculo é indispensável saber um multiplo comum aos denominadores dessas frações. Consequentemente o cálculo do *mmc* se tornar viável por ser o menor desses múltiplos facilitando os cálculos posteriores.

Diz-se que um número é um múltiplo comum de dois números a e b ambos naturais se, a divide esse número e b também o divide.

Observe que $a \cdot b$ é sempre múltiplo comum de a e b ambos naturais.

Denota-se, que um número m é o mínimo múltiplo comum de dois números naturais a e b se conter as seguintes propriedades:

i) m é múltiplo comum de a e b

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

Exemplo 3.3.1: (Ver [10]) Um médico, ao prescrever uma receita, determina que dois medicamentos sejam ingeridos pelo paciente de acordo com a seguinte escala de horários: remédio A, de 4 em 4 horas, remédio B, de 6 em 6 horas. Caso o paciente utilize os dois remédios às 7 horas da manhã, qual será o próximo horário de ingestão dos mesmos?

Solução:

Observe que 24 é múltiplo de 4 e 6. Porém, não é de maneira nenhuma o Mínimo Múltiplo Comum desses números e sim o número 12. Logo os remédios serão ingeridos novamente às 19h.

Voltaremos neste exemplo mais adiante para mostrar como chegou se a essa conclusão.

O mínimo múltiplo comum de dois números a e b, se existir, é único, e é denotado por $[a,b]$.

Note que o mínimo múltiplo comum só existe se os números são naturais.

Proposição 3.3.1. *Dados dois números naturais a e b, tem-se que $[a,b]$ existe e*

$$[a,b]\cdot(a,b)=a\cdot b$$

Demonstração. Escrevendo $m=\dfrac{a\cdot b}{(a,b)}$. Como $m=a\cdot\dfrac{b}{(a,b)}=b\cdot\dfrac{a}{(a,b)}$ tem-se, que $a\mid m$ e $b\mid m$.

Seja c um múltiplo comum de a e b; segue $c=n\cdot a=n'\cdot b$. Prossegue daí que

$$n\cdot\frac{a}{(a,b)}=n'\cdot\frac{b}{(a,b)}$$

Como $\dfrac{a}{(a,b)}$ e $\dfrac{b}{(a,b)}$ pelo corolário 3.2.1 são coprimos procede que $\dfrac{a}{(a,b)}\mid n'$, e , portanto, $m=\dfrac{a}{(a,b)}\cdot b$ divide $n'\cdot b$ que, é igual a c.

$\square$

Note que em legitimidade a propriedade anterior, o Mínimo Múltiplo Comum pode ser descoberto pelo Algoritmo de Euclides, visto que, bastará dividir o produto dos dois números naturais pelo seu Máximo Divisor Comum no qual este necessita somente desse algoritmo para ser encontrado.

Exemplo 3.3.2: Um comerciante tem uma certa quantidade de copos, e deseja guardá-los em pequenas caixas, de maneira que todas fiquem com a mesma quantia de copos. O mesmo notou que necessitava de 27 caixas para colocá-los com uma certa quantidade A ou 36 com uma certa quantidade B. Diante dessa situação pergunta-se quantos copos existiam no mínimo?

Solução:

Observe que a quantidade de copos tem que ser divisível por 27 e 36. Como que a mínima quantia possível, a solução do problema trata-se, de encontrar o mínimo múltiplo comum de 27 e 36. Daí segue

$$[27,36]=\frac{27\cdot 36}{(27,36)}=\frac{27\cdot 36}{9}=108$$

Observe que este método utilizado no exemplo 3.3.2 não é a única maneira de encontrar o *mmc* entre dois números naturais, pois poderíamos encontrá-lo pela fatoração em números primos, porém não a utilizaremos aqui, por considerar esse procedimento mais complicado para o entendimento dos alunos. E também pela dificuldade de aplicá-lo em muitas situações. E até mesmo por não ser utilizável em muitos problemas como no seguinte exemplo:

Exemplo 3.3.3: Seja $n \in \mathbb{N}$; encontre $\left[n^2+1, n+1\right]$.

Solução:

Note que este dois números são impossíveis de serem fatorados, pois n é um número natural arbitrário. Daí para resolvermos vamos utilizar o lema de Euclides 3.2.1, ou seja, que

$$(n^2+1, n+1) = (n+1, n^2+1) = (n+1, (n+1)\cdot n - n + 1) = (n+1, -n+1) =$$
$$(n+1, -(n+1)+2) = (n+1, 2)$$

Logo

$$(n^2+1, n+1 = (n+1, 2) = \begin{cases} 2 \text{ se } n \text{ é impar} \\ 1 \text{ se } n \text{ é par} \end{cases}$$

Segue que

$$\left[n^2+1, n+1\right] = \frac{(n^2+1)\cdot(n+1)}{(n^2+1, n+1)} = \frac{n^3+n^2+n+1}{(n^2+1, n+1)}$$

Portanto

$$\left[n^2+1, n+1\right] = n^3+n^2+n+1 \text{ se } n \text{ é par}$$

e

$$\left[n^2+1, n+1\right] = \frac{n^3+n^2+n+1}{2} \text{ se } n \text{ é ímpar.}$$

Observação 3.3.1: Talvez, o leitor esteja se perguntando, onde será aplicado o conhecimento adquirido neste exemplo? Em qual situação esse problema terá uma utilidade prática para o educando? Pois bem, como já foi mencionado na introdução desta proposta, o Ensino Médio tem como uma das suas finalidades a preparação do aluno para poder continuar apreendendo, ou seja, buscando novos saberes, sendo que um deles poderá ser de encontrar uma situação problema, no qual esse tipo de questão terá seu apreço.

Resolvendo o problema 3.3.1 utilizando a proposição 3.3.1:

Como os remédios foram ingeridos ás 7h e um dos remédios deve ser ingerido de 4 em 4h e o outro de 6 em 6h para saber a próxima ingestão deverás ser após a soma do MMC entre 4 e 6. Daí, segue que

$$[6,4] = \frac{6 \cdot 4}{(6,4)} = \frac{24}{2} = 12$$

Logo serão ingeridos 12h após a ingestão anterior, ou seja, ás 19h.

Tem-se que dois números a e b ambos naturais primos entre si, para o cálculo do *mmc* dos mesmos basta multiplicá-lo um pelo outro, ou seja, como o Máximo Divisor Comum é 1, logo não é necessário fazer a divisão, pois o número 1 é o elemento neutro da divisão, assim como é da multiplicação.

Exemplo 3.3.4: Uma certa escola irá participar de uma competição nos quais existirão variados Jogos: Futsal (5 atletas), Futebol soçaite (7 atletas) e Futebol de campo (11 atletas). Sendo que os alunos (atletas) poderão participar de quantas modalidades quiserem, e cada escola pode ter uma quantidade ilimitada de times para cada modalidade. O professor responsável por escolher os atletas pretende que todos os alunos participem de todas as modalidades sem precisar substituir nenhum atleta durante os jogos. Pergunta-se, no mínimo quantos alunos esse professor terá que selecionar para essa competição?

Solução:

Como o professor não pretende substituir nenhum atleta durante os jogos e quer que todos participem de todas as modalidades, então o número de atletas tem que ser divisível pelas quantidades de atletas em cada modalidade. Daí, segue que o mínimo múltiplo comum é o menor desses números, ou seja, o mínimo múltiplo comum de 5,7,11.

Segue que como os números 5, 7 e 11 são primos o máximo divisor comum dois a dois deles é 1, então o mínimo múltiplo comum é o produto desses números.

Portanto,

$$[5,7,11] = 5 \cdot 7 \cdot 11 = 385$$

Logo serão levados 385 alunos (atletas).

4 APLICAÇÃO DO MÁXIMO DIVISOR COMUM

Uma das aplicações importante do máximo divisor comum são as equações diofantinas, na qual o mdc é utilizado para verificar se essas equações têm soluções no conjunto dos números naturais ou não, e até mesmo para encontrar essas soluções através de substituições entre as equações encontrada pelo algoritmo euclidiano.

4.1 Equações diofantinas lineares com duas incógnitas

A aritmética praticamente não progrediu após Euclides por quase cinco séculos, ressurgindo com Diofanto de Alexandria, que viveu por volta de 250 D.C. A obra que Diofante nos deixou recebe o nome de Aritmética, essa escrevedura conteve treze volume, mas somente sete nos alcançaram. Esse trabalho de diofanto é o primeiro estudo de que se tem conhecimento sobre álgebra, pois a maneira que ele abordava era completamente algébrica, não sendo coberta de nenhuma interpretação geométrica, como praticavam todos os matemáticos predecessores. Em sua maioria os problemas de Diofante em Aritmética, mirava descobrir desfecho em números racionais, satisfazendo-se, ao encontrar unicamente uma solução particular de equações algébricas com uma ou mais variáveis.

Vários problemas em aritmética reincidem na capacidade de resolver, em números naturais, equações do tipo

$$aX - bY = c \text{ ou ainda}$$
$$aX + bY = c \text{ com } a, b, c \in \mathbb{N}$$

Estas equações são conhecidas como equações diofantinas lineares em homenagem a Diofante de Alexandria (300 D.C.).

Segundo CAMPOS [12] a história da vida de Diofante está resumida em seu túmulo e, que está escrito sob a forma de um enigma Matemático:

“Caminhante!
Aqui jazem os restos de Diofante.
Os números podem mostrar, oh maravilha, a duração da sua vida, cuja sexta parte constou da encantadora infância.
Tinha passado mais uma duodécima parte da sua vida quando lhe apareceu a barba.
A partir daí, a sétima parte da sua existência passou-a num matrimônio sem filhos.

> *Passou um quinquénio mais quando o fez feliz o nascimento do seu primogênito.*
> *Este entregou o seu corpo e a sua encantadora existência à terra, tendo vivido metade do que seu pai viveu.*
> *Quanto a Diofante desceu à sepultura com profunda mágoa, tendo sobrevivido apenas quatro anos a seu filho.*
> *Diz-me, caminhante, quantos anos viveu Diofante até que a morte lhe chegou?"*

Segundo esse enigma, considerando os anos vividos por Diofante como D, tem-se:

$$\frac{D}{6}+\frac{D}{12}+\frac{D}{7}+F+4=D$$

E como seu primogênito viveu a metade de sua vida, tem-se:

$$F=\frac{D}{2}$$

Daí, segue que

$$\frac{D}{6}+\frac{D}{12}+\frac{D}{7}+\frac{D}{2}+4=D$$

Resolvendo tem-se $D=84$.

Portanto, Diofante viveu 84 anos.

Agora faremos as seguintes perguntas: Para que estudar essas equações? Essas equações possuem soluções? Se existem, como encontrá-las? Em quais situações poderemos recorrer a esse tipo de equações, para solucionar problemas? Procura-se, nesta seção responder as essas indagações entre outras que possam surgir, ao longo do trabalho do docente a frente de tal conteúdo.

Segundo Pommer [13]:

> "O uso das equações Diofantinas lineares no Ensino Médio possibilita reexplorar situações problemas envolvendo números inteiros. No ensino médio, a concepção vigente é tratar os inteiros simplesmente como subconjuntos dos números reais, o que conduz a simplificações que não consideram aspectos fundamentais dos números inteiros. [...] este tema permite articular a partir da tentativa e erro, outras estratégias de enfoque aritmético. Estabelecendo uma natural transição entre a aritmética e a álgebra"

Note que não é sempre que este tipo de equações tem solução, por exemplo, as equações

$$6x+8y=2 \text{ e } 8x-6y=3$$

não possuem nenhuma solução nos naturais, (x_0, y_0) visto que, do contrário, para a primeira equação, tem-se, $6x_0 + 8y_0 > 2$, e na segunda equação, tem-se, $8x_0 - 6y_0$ é par, daí nunca será igual a 3.

As duas proposições seguintes nos dá uma ideia de quando esse tipo de equação tem ou não solução, e como representá-las de modo geral.

Proposição 4.1.1. *Sejam $a, b \in \mathbb{N}^*$ e $c \in \mathbb{N}$. A equação $ax - by = c$ admite solução em números naturais se, e só se, $(a, b) \mid c$.*

Demonstração. A demonstração dessa proposição poderá ser encontrada pelo leitor no livro Elementos de Aritmética [3]. □

Proposição 4.1.2. *Seja (x_0, y_0) a solução mínimal da equação $ax - by = c$ sendo que $(a, b) = 1$. Então a solução (x, y) pertencente aos naturais da equação é:*

$$x = x_0 + tb,\ y = y_0 + ta \qquad t \in \mathbb{N}$$

Demonstração. A demonstração dessa propriedade poderá ser encontrada pelo leitor no livro Elementos de Aritmética [3]. □

Repare que a equação $ax - by = c$, com $(a, b) = 1$, aceita soluções infindáveis.

Prosseguindo, apresentaremos um método para a solução mínimal das equações do tipo $ax - by = c$, desde que $(a, b) = 1$.

Seja a, b e c números naturais pequenos, a solução poderá ser encontrada por vistoria. Abrangentemente o método apresentado a seguir, em qualquer ocasião consentirá encontrar a solução mínimal.

Utilizando-se do algoritmo de Euclides, é possível exprimir

$$na - mb = (a, b) = 1 \text{ ou } m'b - n'a = (a, b) = 1$$

No caso em que $1 = m'b - n'a$, escolha $p \in \mathbb{N}$ tal que $pb > n'$ e $pa > m'$, logo

$$1 = (pb - n')a - (pa - m')b$$

Logo, em qualquer ocasião poderá denotar $1 = na - mb$, para $n, m \in \mathbb{N}$. Fazendo-se, multiplicar a igualdade por c, tem-se

$$c = cna - cmb$$

Daí, tem-se,
$x_1 = cn$ e $y_1 = cm$ é uma solução particular da equação. Pela proposição 2.1.2, tem-se, que a solução mínimal é do tipo $x_0 = x_1 - tb$ e $y_0 = y_1 - ta$ para o maior valor de t, desde que se tenha

$$cn - tb = x_1 - tb \geq 0 \text{ e } cm - ta = y_1 - ta \geq 0$$

Exemplo 4.1.1: Carlos e Mário são grandes amigos, ambos feirantes, com estabelecimentos próximos. Em certo dia numa de suas conversas, sobre suas vendas, Carlos contou alegremente a Mário que naquele dia tinha vendido 22 pacotes de laranjas (todos iguais). Por outro lado Mário estava triste naquele momento pois, somente 14 pacotes (mesma quantidade de laranjas) o mesmo tinha conseguido vender. Resolveram então fazer o cálculo de quantas laranjas cada um tinha vendido naquele dia, após esse procedimento perceberam que Carlos tinha vendido somente 18 laranjas a mais que Mário. Pergunta-se, no mínimo quantas laranjas existam em cada pacote?

Solução:

Sejam X e Y os números respectivamente de laranjas em cada pacote de Carlos e Mário. Então a equação que representa essa sentença é a seguinte:

$$22X - 14Y = 18$$

Portanto uma equação diofantina. Como o $(22,14) = 2$ e $2 \mid 18$, então existe solução e é equivalente a resolver a equação

$$11X - 7Y = 9$$

Vamos encontrar a solução mínimal (x_0, y_0) desta última equação. Recorrendo ao algoritmo de Euclides tem-se,

$$\begin{aligned} 11 = 7 \cdot 1 + 4 &\Rightarrow 4 = 11 - 7 \cdot 1 \\ 7 = 4 \cdot 1 + 3 &\Rightarrow 3 = 7 - 4 \cdot 1 \\ 4 = 3 \cdot 1 + 1 &\Rightarrow 1 = 4 - 3 \cdot 1 \end{aligned}$$

Substituindo as equações a direita umas nas outras, obtêm-se

$$1 = 11 \cdot 2 - 7 \cdot 3$$

e portanto,

$$9 = 11 \cdot (18) - 7 \cdot (27)$$

logo $x_1 = 18$ e $y_1 = 27$ é uma solução particular da equação. Diante desta solução e com o apoio do método apresentado acima iremos determinar a solução mínimal

$$x = 18 - 7t \quad y = 27 - 11t$$

Determinando o maior valor de t tais que x e $y \in \mathbb{N}$. Isso ocorre quando $t = 2$, tendo assim, que a solução mínimal é $x_0 = 4$ e $y_0 = 5$.

E portanto as soluções da equação são do tipo

$$x = 4 + 7t \quad y = 9 + 11t$$

Logo existiam no mínimo, 4 laranjas em cada pacote de Carlos e 5 laranjas em cada pacote de Mário.

Note que as equações diofantinas podem serem usadas para trabalhar outras habilidades com os alunos entre elas para expor suas culturas, contextualizando as mesmas com questões do próprio cotidiano dos alunos, como foi feito no problema apresentado a seguir:

Exemplo 4.1.2: Vários côcos de babaçu foram reunidos por três homens, Carlos, Mário e Tiago, além de um menino, formando assim um monte de côco. No dia seguinte Carlos voltou ao local desse monte juntamente com o menino, repartiu o monte em três partes iguais, sobrando dois cocos que foram dados ao menino, escondeu uma dessas partes, reuniu-se as outras duas partes nas quais foram deixadas no local sem que ninguém pudesse perceber o ocorrido. Esse processo foi repetido novamente por Mário e Tiago nos respectivos segundo e terceiro dia após os três terem reunido o monte. Continuadamente no quarto dia voltaram ao local dividiram o restante mais uma vez em partes iguais, sobrou dois côcos que foram dados mais uma vez ao menino, cada um dos três homens levou uma dessas partes para sua casa terminando assim o processo. Pergunta-se, no mínimo quantos côcos existiam no monte antes do início do processo para que pudesse ser realizado?

Solução: Observe pela Figura 1 que em cada passagem é feita uma divisão por 3.

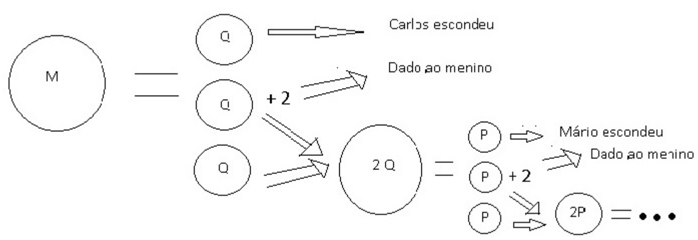


Figura 1 – Esquema prático

Seja M a quantidade de côco no monte inicial. E sejam ainda Q,P, R e V os respectivos quocientes das divisões sucessivas feitas por: Carlos, Mário, Tiago e pelos três durante esse processo como mostra o esquema prático acima. Logo têm-se as seguintes equações:

$$M = 3Q + 2$$

$$2Q = 3P + 2$$

$$2P = 3R + 2$$

$$2R = 3V + 2$$

Da última equação tem-se,

$$R = \frac{3V + 2}{2}$$

Substituindo-o valor de R na equação logo acima e, fazendo esse processo retrocedente até a primeira equação, obtém-se

$$8M - 81V = 130$$

Utilizando-se a divisão euclidiana tem-se

$$1 = 81 - 8 \cdot (10) = 8 \cdot (-10) - 81 \cdot (-1)$$

Multiplicando a igualdade por 130 obtém-se

$$8 \cdot (-1300) - 81 \cdot (-130) = 130$$

Como queremos soluções nos naturais segue que

$$\begin{cases} M = -1300 + 81t \geq 0 \\ V = -130 + 8t \geq 0 \end{cases}$$

Resolvendo o sistema tem se que $t \geq 17$, de onde segue que o menor valor de M é para $t = 17$, portanto $M = 77$. Logo existia no mínimo 77 côco no monte inicial.

Observação 4.1.1: Em nossa região, norte do Tocantins (bico do papagaio) apresenta-se, o cultivo do babaçu como fonte de renda para famílias com pouco poder aquisitivo, do qual é extraído azeite, retirado a casca do coco para fabricação de bombons, sua madeira é usada para fazer carvão assim como as palhas são utilizadas para construção de barracas, entre outros, ou seja, está presente no cotidiano dos nossos alunos. Por esse motivo, acreditamos que questões como a apresentada no exemplo acima poderá chamar a atenção dos alunos, é claro que ela poderá ser adaptada pra qualquer região do Brasil, pois invés de coco poderia ser banana, melão, laranja, entre outros. Ficando dependente apenas da criatividade do professor à frente do conteúdo.

Para prosseguirmos com nosso estudo sobre equações diofantinas necessitamos da proposição a seguir:

Proposição 4.1.3. *Sejam $a, b \in \mathbb{N}^*$, com $(a,b) = 1$. Todo número natural c pode ser escrito (de modo único) de uma e, somente uma, das formas seguintes:*

$$c = na + mb \quad ou \quad c = na - mb, \; com \quad n < b$$

Demonstração. A demonstração dessa propriedade poderá ser encontrada no livro Elementos de Aritmética [12].

□

Note que as equações diofantinas tem soluções no conjunto dos números inteiros sempre que $(a,b) = 1$. Assim tendo encontrado uma solução nos inteiros (x_1, y_1), para achar a solução mínimal (menores naturais) basta resolver as inequações

$$\begin{cases} x = x_1 - bt > 0 \\ y = y_1 + at > 0 \end{cases}$$

Se a equação for do tipo ax+by=c com (a,b)=1, porém se o sistema não tiver solução a equação também não terá solução nos naturais . E para as equações do tipo $ax - by = c$, com $(a,b) = 1$.

$$\begin{cases} x = x_1 + bt > 0 \\ y = y_1 + at > 0 \end{cases}$$

Note que um aluno do Ensino Médio ao se deparar com uma equação do tipo apresentado acima, se não for conhecedor do método de Diofanto terá muitíssima dificuldade para resolver tais equações. No entanto problemas que recaem neste tipo de equações são muito frequentes na matemática e no cotidiano dos estudantes, como nas situações dos dois exemplos seguinte.

Exemplo 4.1.3: O valor da entrada de um cinema é R$ 8,00 e da “meia” entrada é de R$ 5,00. Qual é o menor número de pessoas que podem assistir a uma sessão de maneira que a bilheteria seja de R$ 500,00? (IEZZI [14]).

Solução:

Sejam x e y, respectivamente os números de pessoas que pagam o valor total da entrada e os que pagaram “meia” entrada , a equação que representa o número de pessoas e a seguinte

$$8x+5y=500$$

Utilizando o algoritmo de Euclides tem-se $mdc(8,5)=1$ e como $1 \mid 500$ a equação tem solução, observe a tabela do algoritmo

	1	1	1
8	5	3	2
3	2	1	

Daí, segue que

$$\begin{cases} 1=3-2\cdot 1 \\ 2=5-3\cdot 1 \\ 3=8-5\cdot 1 \end{cases}$$

Substituindo retroativamente as equações anteriores obtem-se,que $8\cdot(2)+5\cdot(-3)=1$ consequentemente multiplicando a igualdade por 500, tem-se

$$8\cdot(1000)+5\cdot(-1500)=500$$

Logo

$$\begin{cases} x=1000-5t \\ y=-1500+8t \end{cases}$$

Sabendo que x e y são números naturais, pois representam números de pessoas tem-se que

$$\begin{cases} x=1000-5t\geq 0 \\ y=-1500+8t\geq 0 \end{cases}$$

Resolvendo o sistema de inequações obtêm-se, que $188\leq t\leq 200$. Seja S a soma entre quem pagou "meia" entrada e quem pagou valor total da entrada, utilizando-se, uma tabela tem-se que:

t	188	189	190	191	192	193	194	195	196	197	198	199	200
x	60	55	50	45	40	35	30	25	20	15	10	5	0
y	4	12	20	28	36	44	52	60	68	76	84	92	100
S	64	67	70	73	76	79	82	85	88	91	94	97	100

Portanto, o menor número de pessoas que assiste uma sessão do cinema é 64.

Exemplo 4.1.4: Um observador estando próximo a um semáforo resolve contar a quantidade de pneus que passava naquele local, tendo passado 5 minutos verificou que tinha contado 80 pneus e que só passaram carros de passeio (4 pneus) e motos (2 pneus) e que a diferença entre esses dois tipos de transporte foi o mínimo possível. Diante do ocorrido, pergunta-se quantas motos e quantos carros passaram por aquele local no período mencionado acima?

Solução:

Sejam x e y os números respectivamente de carros e motos , a equação que representa o número de pneus e a seguinte

$$4x + 2y = 80$$

Como $(4,2) = 2 \mid 80$ a equação tem-se, solução e é equivalente a resolver a equação

$$2x + y = 40$$

Veja que $x_1 = 80$ e $y_1 = -120$ são números inteiros porém são solução da equação acima, pois $2 \cdot (2) + 1 \cdot (-3) = 1$ segue que, multiplicando a igualdade por 40, têm-se

$$2 \cdot (80) + 1 \cdot (-120) = 40, \quad \text{logo}$$

$$\begin{cases} x = 80 - t \\ y = -120 + 2t \end{cases}$$

Sabendo que x e y são números naturais, pois representam respectivamente o número de carros e motos, têm-se

$$\begin{cases} x = 80 - t > 0 \\ y = -120 + 2t > 0 \end{cases}$$

Resolvendo o sistema de inequações obtêm-se, que $60 < t < 80$. Seja D a diferença entre carros e motos, utilizando-se, uma tabela segue que

t	61	62	63	$\cdots$	66	67	68	$\cdots$	77	78	79
x	19	18	17	$\cdots$	14	13	12	$\cdots$	3	2	1
y	2	4	6	$\cdots$	12	14	16	$\cdots$	34	36	38
D	17	14	11	$\cdots$	2	1	4	$\cdots$	31	34	37

Portanto observando a tabela acima concluímos que passaram exatamente 13 carros e 14 motos naquele local.

Note que os valores $x_1 = 80$ e $y_1 = -120$ no exemplo 4.1.4 foram encontradas por tentativa e não utilizando o algoritmo euclidiano, mas poderíamos também ter utilizado-o no qual chegaríamos ao mesmo resultado. Porém vale lembrar que o método euclidiano nos dará uma certeza que iremos conseguir com êxito o resultado procurado.

Note que nem sempre as expressões do tipo $ax + by = c$ tem soluções nos números naturais, ou seja, existem valores para c em que o conjunto de soluções é vázio. Para encontrar esses valores chamados de "lacunas"basta encontrar todas as combinações $na - mb$ com n e b naturais e com $n < b$.

4.2 Atividades diferenciadas de equações diofantinas

A objeção sobre sua aplicabilidade e a falta de interesse representam um dos principais fenômenos que geram dificuldades na esfera escolar quanto ao ensino da Matemática e em particular da Aritmética. Tal fenômeno é caracterizado de várias formas, porém, as ideias acerca de como solucionar esse problema estão longe de se tornar consensuais. Procuramos solucionar esses problemas atribuídos por alunos do Ensino Médio ao fenômeno “falta de interesse e objeção a Aritmética”, procurando dar significado aos conteúdos motivando os educandos com atividades diferenciadas e contextuais que possam ser utilizadas para compreender, resolver ou amenizar problemas de seu âmbito familiar. Partimos do pressuposto que, se desejamos sobrevir na realidade educacional de nossos alunos, devemos conhecer, de antemão, a realidade que constitui seus entornos, a sua comunidade, os dilemas que vivenciam e as alternativas de modificação dessa situação.

Os sentidos atribuídos pelos alunos ao fenômeno revelam uma pluralidade de terminologias. Não é um problema que poderá ser resolvido de forma isolada, somente abrangendo a esfera escolar, ou seja, sem existir, um olhar para a comunidade envolvida. No que diz respeito a buscar, uma maior aproximação entre a escola e seu contexto familiar visando um trabalho integrado, não apenas discutindo as dificuldades existentes no contexto escolar, mas com a inserção desses novos olhares possibilitarem uma restruturação das formas e modelos existente no processo de aprendizagem do Ensino Fundamental e principalmente do Médio.

Uma das maneiras de chamar a atenção para um conteúdo é trabalhar com atividades diferenciadas, para propiciar esse ambiente ao apresentar equações diofantinas, propomos aqui algumas atividades como sendo um diferencial para a aprendizagem do aluno.

De antemão sugerimos que as atividades 1 e 2 que serão apresentadas mais adiante, assim como todo o conteúdo de equações diofantinas, sejam apresentados aos alunos logo após estes terem estudados equação geral da reta, pois, observar-se uma relação estreita entre equações da reta e as diofantinas. Entre outros, esse é um dos motivos que defendemos a presença das equações diofantinas no Ensino Médio, para sanar algumas dificuldades neste tipo de habilidades e por resolver outras situações problemas do cotidiano dos educandos nos quais as equações da reta não os resolvem.

Essas atividades devem ser desenvolvidas de preferência em uma sala que contenha no máximo 30 alunos, para que o professor tenha maior disponibilidade de sanar as dúvidas gerada no decorrer das atividades e que estas sejam em grupos contendo 2 ou 3 alunos.

> "Há um ditado chinês que diz que, 'se dois homens vêm andando por uma estrada, cada um carregando um pão, e, ao se encontrarem, eles trocam os pães, cada homem vai embora com um; porém, se dois homens veem andando por uma estrada, cada um carregando uma ideia e, ao se encontrarem, eles trocam as ideias, cada homem vai embora com duas'. Quem sabe é esse mesmo o sentido do nosso fazer: repartir ideias, para todos terem pão"[...] (CORTELLA, 1998, p. 159 [15]).

O ditado acima citado por Cortella explica a importância do trabalho em grupo, porém trabalhar com alunos em grupos não é uma tarefa fácil, pois muitos deles utilizam este momento para dialogar assuntos que não são direcionados as atividades propostas, o que solicita uma maior atenção pelo professor. Porém, certifica-se, que trabalhos em grupos como mencionado por Cortella disponibiliza uma troca de ideias, prevalecendo assim uma aprendizagem superior ao estudo individualizado.

ATIVIDADE 1:

Objetivo Geral:

O objetivo geral dessa atividade é a compreensão das equações diofantinas utilizando o contexto familiar, com exemplo.

Objetivos específicos:

Saber diferenciar se é possível um saque que contenha apenas algumas cédulas.

Utilizar equações diofantinas para resolver problemas do cotidiano.

Procedimento:

Para a realização dessa atividade precisou-se de separá-la em dois momentos. O primeiro serviu para apresentação aos estudantes dos conceitos primordiais de equações diofantinas, como também para mostrar sua importância na solução de algumas situações do cotidiano desses estudantes. Na segunda etapa, ou seja, momento da aplicação da atividade ocorreu o seguinte: a distribuição da tabela 5.2.1 a cada grupo (2 alunos em cada), depois pediu-se para os grupos discutirem se é possível realizar certo saque em um caixa que contém apenas alguns tipos de notas, segunda coluna, sendo que cada nota tem a quantidade indicada na primeira coluna da tabela. Após essa verificação marcar na quarta coluna SIM ou NÃO, se há solução, ou seja, a resposta é SIM, caso contrário é

Não, após isso descrever uma solução na quinta e última coluna caso o grupo responder que SIM.

Quantidade	cédulas	Quantidade a sacar	Pode ser sacado?	Se, SIM descreva uma maneira
10	R$ 20, 00	R$ 138, 00	☐ SIM ☐ NÃO	
10	R$ 5,00			
20	R$ 10, 00	R$ 630, 00	☐ SIM ☐ NÃO	
8	R$ 50, 00			
3	R$ 2, 00	R$ 608, 00	☐ SIM ☐ NÃO	
10	R$ 100, 00			
12	R$ 5, 00	R$ 250, 00	☐ SIM ☐ NÃO	
10	R$ 20, 00			
12	R$ 10, 00	R$ 800, 00	☐ SIM ☐ NÃO	
13	R$ 20, 00			
10	R$ 50, 00			

Figura 2 – Tabela 4.2.1

<u>Dados estatísticos da Atividade 1</u>

Abaixo estão representados gráficamente os resultados da atividade 1 sendo que 64 % dos grupos conseguiram responder corretamente todos os questionamentos propostos na atividade.

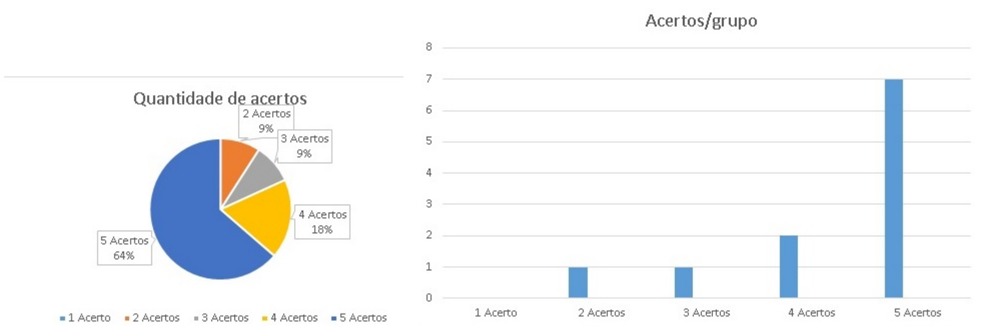


Figura 3 – Dados estatístico da atividade 1

<u>Conclusão:</u>

Esta atividade foi desenvolvida aos alunos da 3ª série do Ensino Médio (22 alunos) do Colégio Estadual Inês Viana Costa, município de Carrasco Bonito – TO. O tempo necessário para o desenvolvimento dessa atividade foi de aproximadamente 1h40min. Separados da seguinte forma 60 minutos para primeira etapa (explanação dos princípios básicos do conteúdo de equações diofantinas) e 40 minutos para a segunda etapa (tempo médio para atividade). Em princípio, alguns grupos encontraram um pouco de dificuldade em relacionar a atividade proposta aos conceitos de equações diofantinas, não compreendendo em um primeiro momento quais conceitos serviriam para obter com êxito a solução, porém rapidamente após uma breve explicação onde procurou-se, estabelecer esses conceitos relacionando a atividade proposta aos conceitos de equações diofantinas, quase que a totalidade dos grupos conseguiram chegar no resultado esperado. Sendo que essa atividade foi de suma importância para que os alunos aqui pesquisados passassem a compreender a importância das equações diofantinas para resolver problemas do nosso cotidiano.

ATIVIDADE 2:

Objetivo Geral:

O objetivo geral desta atividade é relacionar as equações diofantinas e as tarefas corriqueiras dos educandos, como também saber identificar situações em que sejam possíveis a aplicação dessas equações como método para resolver problemas.

Objetivo Especificos:

Identificar a relação entre equações diofantinas e no cotidiano.
Saber utilizar as equações diofantinas para controlar suas finanças.
Compreender a importância das equações diofantinas no cotidiano das pessoas.

Procedimentos:

Distribuir a tabela 4.2.2 para cada grupo. Pedir para os grupos observar o exemplo, da tabela, depois o professor faz uma breve explanação explicando o que significa as duas últimas colunas citando o exemplo nela exposto. Após isso cada grupo deve preencher o restante da tabela.

Produtos	Quantidade	Preço por unidade ou Kg	Uma eq. p/ o cálculo do custo	Custo parcial da compra (C)
Arroz (Tipo1)	5	R$ 12, 00	5 X 12 + 3 X 6 = C	C = 60 + 18 = 78,00
Feijão (Tipo 2)	3	R$ 6, 00		
Farinha	2	R$ 5, 00		
Cebola	2	R$ 4, 00		
Detergente	3	R$ 3, 00		
Sabão em pó	4	R$ 2, 00		
Margarina	2	R$ 3, 00		
Bollacha	3	R$ 2, 00		
Papel Higienico	3	R$ 1, 00		
Vasoura	1	R$ 5, 00		
Cera líquida	2	R$ 4, 00		
Refrigerante	3	R$ 6, 00		
Macarrão	2	R$ 2,00		
Extrato de Tomate	2	R$ 3, 00		
Custo total da compra de todos os produtos listados acima				

Figura 4 – Tabela 4.2.2

Dados estatísticos da Atividade 2

Abaixo estão representados gráficamente os resultados da atividade 2 sendo que 82 % dos grupos conseguiram responder corretamente todos os questionamentos propostos na atividade.

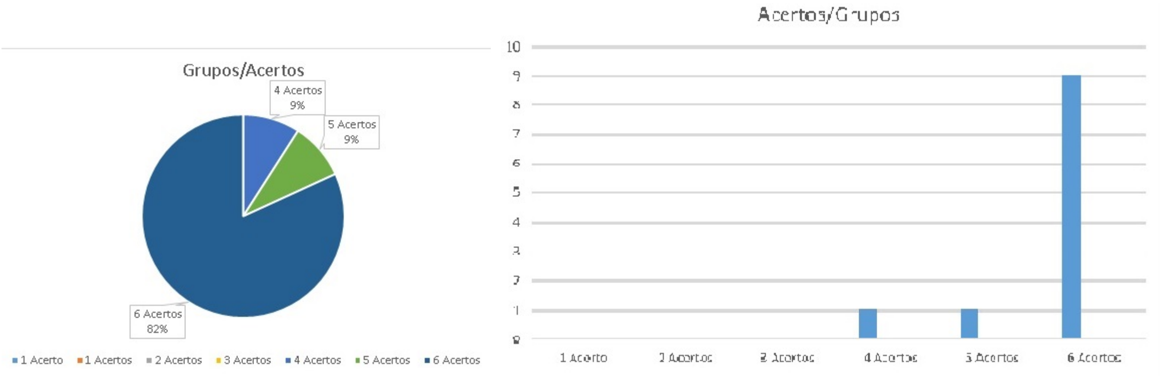


Figura 5 – Dados estatístico da atividade 2

<u>Conclusão:</u>

Esta segunda atividade foi aplicada novamente a 3ª série EM, sendo para a resolução da mesma foi exigido um tempo médio de 30 minutos. Essa atividade proposta acima, foi considerada pelos alunos mais simples que a primeira, acredita-se que por já estarem adaptados aos conceitos de equações diofantinas não tiveram muitas dificuldades, sendo que 82% dos grupos conseguiram relacionar facilmente a atividade com os conceitos das equações diofantinas e com isso, resolver corretamente a mesma sem maiores dificuldades. O restante conseguiram relacionar o conteúdo com as equações porém fizeram manipulações equivocadas em alguns momentos não tendo êxito na resposta.

5 OS ÁTOMOS DA MATEMÁTICA E ALGUMAS CURIOSIDADES

Dedicamos este capítulo ao estudo dos números primos por seu importante papel no estudo da aritmética e da matemática em geral. Segundo Marcus SAUTOY [16]"os números primos desempenham um papel importante em vários ramos na matemática, são como o hidrogênio e o oxigênio do mundo dos números, eles são os átomos da matemática".

Apesar do grande acervo de estudos sobre os números primos até hoje existem muitas indagações sobre eles que ainda não tem respostas conclusivas entre elas a mais importante que intriga os principais matemáticos é a busca por uma fórmula para encontrar todos os números primos.

Tendo analisado o Referencial Curricular do Ensino Fundamental[17] entende-se, a dificuldade dos alunos do Ensino Médio quanto ao conteúdo de números primos, pois observa que os números: naturais, inteiros, racionais, irracionais e reais, são minuciosamente estudados do 7º ano até o 9º ano e ainda é revisado na 1ª série do Ensino Médio. Porém, os números primos são vistos de maneira superficial, ou seja, só para o estudo de radiciação nos quais são utilizados para fatorar o radicando não tendo uma abordagem específica para esses números tão importante quanto os demais, e até com mais destaque no estudo da matemática em geral.

5.1 Um teorema fundamental para aritmética

Vem-se aqui nesta seção definir algumas propriedades e/ou teoremas importantes para o estudo dos números primos, entre esses o teorema fundamental da aritmética.

Definição 5.1.1. *Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado primo.*

Então a partir da Definição 5.1.1 ocorrem duas situações entre dois números p e q ambos primos e um número a um inteiro qualquer:

1) Se $p \mid q$, então $p = q$.

2) Se $p \nmid a$, então $(p, a) = 1$.

Demonstração. As demonstrações dessas duas situações acima poderão, serem encontradas no livro aritmética[13]. $\square$

Note que um número quando não é primo e proferido como composto, e todos os números compostos podem serem formados a partir de produtos de números primos. Daí, que se entende o porquê de todo o estudo acerca dos números primos tornando eles tão especiais.

Por exemplo os números 2, 3, 5, 7 e 11 são primos. Por outro lado 4, 6, 10, 33 são compostos. Entretanto, esses números compostos podem serem escritos como: $4 = 2 \cdot 2$; $6 = 3 \cdot 2$; $10 = 2 \cdot 5$; $33 = 3 \cdot 11$, ou seja, produtos de primos.

Eratóstenes de Cirene, matemático grego do século II a.C. em seus estudos sobre números primos conseguiu provar que se um número n natural maior que 1 for composto, então n possui um divisor primo p, tal que $p \leq \sqrt{n}$ caso contrário n é primo. Sendo este um grande salto para a aritmética daquela época. Ele também foi responsável por um excelente trabalho que conseguira medir indiretamente o diâmetro da Terra com uma precisão impressionante para sua época.

A seguir apresentaremos duas propriedades importantes sobre os números primos que são de utilidades para a apresentação do teorema fundamental da aritmética.

Proposição 5.1.1. *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. O leitor interessado poderá encontrá-la, no livro Aritmética[7]. □

Corolário 5.1.1. *Se $p, p_1, p_2, \cdots, p_n$ são números primos e, se $p \mid p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, \cdots, n$.*

Demonstração. Mais uma vez o leitor interessado poderá encontrar a sua demonstração no livro Aritmética[7]. □

Até o aparecimento de Euclides com Os elementos[8] por volta de 300 a.C, muito já se sabiam sobre os números primos. No entanto, Euclides no livro IX de Os elementos consegue provar que existem infinitos números primos, utilizando pela primeira vez até onde se tem relatos sobre a história da aritmética o método da contradição, com um intensão clara de obter-se, um resultado. Sendo que Euclides utilizou de maneira indireta o corolário 5.1.1 para encontrar esse fascinante resultado.

Teorema 5.1.1. *(Teorema Fundamental da Aritmética): Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. A demonstrção desse teorema poderá ser encontrado pelo leito interesado no livro Elementos de Aritmética[3]. □

Com relação o teorema fundamental da aritmética 6.1.1, tem-se a seguinte definição: Se $n \in \mathbb{Z} \setminus \{0\}$ e seja p um número primo, denota-se, por $E_p(n)$ o expoente da maior potência de p que divide $n!$. Sendo que $E_p(n)$ pode ser encontrado da seguinte maneira:

$$E_p(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^r}\right]$$

Sendo que $\left[\frac{n}{p^i}\right]$ significa, a parte inteira da divisão de n por p^i com i variando de 1 a r, em ordem crescente para cada parcela enquanto houver uma parte inteira.

Teorema 5.1.2. *Dado um número inteiro* $n \neq 0$*, 1, -1, existem primos* $p_1 < \cdots < p_r$ *e* $\alpha_1 \cdots \alpha_r \in \mathbb{N}$*, univocamente determinados, tais que*

$$n = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Demonstração. A demonstração desse teorema é basicamente uma verificação do teorema 5.1.1. □

Note que quando houver necessidade pode-se, acrescentar fatores da seguinte forma $p^0 (= 1)$, sendo p um primo qualquer, para decomposição em números primos.

Sendo denotado por $d(n)$ o número de divisores de um número natural $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, sendo que $p_1, \cdots, p_r$ são números primos e $\alpha_1, \cdots, \alpha_r \in \mathbb{N}$, então

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

Essa propriedade torna importante para o ensino médio quando estão diante de problemas como o seguinte:

Exemplo 5.1.1: (ENEM-2014) Durante a segunda Guerra Mundial, para decifrarem as mensagens secretas, foi utilizada a técnica de decomposição em fatores primos. Um número N é dado pela expressão $2^x \cdot 5^y \cdot 7^z$, na qual x, y e z são números inteiros não negativos. Sabe-se que N é múltiplo de 10 e não é múltiplo de 7. Qual a expressão que representa o número de divisores diferente de N, em função de x, y e z?

Solução:

Como a quantidade de divisores do número N é $d(N) = (x+1)(y+1)(z+1)$, daí segue que devemos encontrar os divisores diferentes de N, então basta subtrair um (o divisor N). Portanto, o número de divisores de N diferente de N é $(x+1)(y+1)(z+1) - 1$.

5.2 Curiosidades sobre os números primos

Nesta seção apresentaremos algumas curiosidades sobre os números primos com o intuito de mostrar aos educandos que estes números vão muito além de uma simples definição de que possuem apenas dois divisores.

Curiosidade 5.2.1: Criptografia e os números primos:

Essa pequena história poderá ser encontrada, em partes no link [18]

Em todas as épocas houve necessidade de mandar mensagem secretas que deveriam ser lidas apenas pelo destinatário da mensagem, motivando o aparecimento de determinados processos que impedissem terceiros de conhecer o conteúdo da mensagem. Esses processos compõe um ramo da matemática chamado criptografia (do grego Kryptós "escondido", gráphein, "escrita"). Hoje em dia, a criptografia está presente em vários momentos do nosso cotidiano, na maioria das vezes sem que percebemos. Por exemplo, quando nos cadastramos em um site da internet a senha é criptografada antes de ser armazenada no banco de dados. Assim, se um hacker roubar o banco de dados com as senhas, ele não conseguirá lê-las. Portanto os codificadores têm um papel muito importante nesse processo de esconder dados secretos, e atualmente usam os fatores primos de números monstruosos como chave de criptografia. E esses fatores primos quando descobertos, são guardados "a sete chaves" pois fazem parte da segurança nacional de muitos países inclusive de transações bancárias dos mesmos. Daí, a importância dada pelos matemáticos aos números primos e consequentemente, há uma busca incansável por esses números.

Por que isso? Porque, quando o número for tremendamente grande, o processo de fatoração é praticamente impossível.

Por exemplo, o número $2^{193}-1$ é um número gigantesco. Os fatores primos desse número, ou seja, os números primos que multiplicados resultam em $2^{193}-1$ são:

$p = 13.821.503;$

$q = 61.654.440.233.248.340.616.559;$

$r = 14.732.265.321.145.317.331.353.282.383$

Ou seja,

$p \cdot q \cdot r = 2^{193} - 1$

Evidentemente, esse resultado foi obtido por computador.

Todavia, para um número da ordem de 10^{130}, um computador comum levaria 50 anos para efetuar a sua fatoração. E para um número da ordem de 10^{308}, mesmo com os esforços combinados de 100 milhões de computadores, seriam necessários mais de 1000 anos!

Os maiores gênios da criptografia são pessoas desconhecidas, pois, em geral, trabalham em serviços secretos de seus países.

Martin Gardner, famoso matemático americano, fez um desafio para a decodificação de um texto cifrado por ele em agosto de 1977, e forneceu para a chave um número enorme:

$N = 114.381.625.757.999.967.669.235.779.976.146.612.010.218.296.721.242.362.562.561.842$

$935.706.935.245.733.897.830.597.123.563.958.705.058.989.075.147.599.290.026.879.543.541$

Para decifrar o texto seria necessário obter os fatores primos desse número. E isso só foi conseguido dezessete anos depois, pelo esforço conjunto de 600 pessoas de várias nacionalidades e com a utilização de computadores e supercomputadores, em de 26 abril de 1994.

Os fatores de N:

$p = 3.490.529.510.847.650.949.147.849.619.903.898.133.417.764.638.493.387.846.990.820.$

577

$q = 32.769.132.993.266.709.549.961.988.190.834.461.413.177.642.967.992.942.539.798.299.$

533

Ou seja, $N = p \cdot q$

O texto de Gardner decifrado e traduzido era: “as palavras mágicas são estruturas sensíveis”.

Na verdade, este método de encriptação é fruto da aplicação engenhosa de conceitos ligados a Teoria dos Números, como, por exemplo, o Algoritmo de Euclides e o Teorema de Euler-Fermat. Deste modo, conclui-se que os números primos sabem “guardar um segredo”, pois estão associados a processos de codificação na Internet.

Curiosidade 5.2.2: Seleção brasileira de 1994 e os números primos.

Figura 6 – gloogle [19]

Quando o Bebeto chegou a seleção em 1994 para a copa comecei a meditar, acerca do motivo que teria levado o “craque” a escolher a camisa número 7 e não a camisa 10. Achei uma opção estranha uma vez que sempre o “craque” cérebro da seleção jogava com a camisa número 10, exemplo disso o rei Pelé.

Questionei muito com meus amigos sobre o motivo do craque ter utilizado a camisa 7 entre as respostas que me surgiu a mais aplausível era que ele não se sentia bem utilizando uma camisa que tantos “craques” já tinham vestido, como foi mencionado acima, até o rei Pelé já a utilizou. Outra teoria seria pelo motivo da copa ser nos Estados Unidos, os americanos gostam de basquetes e futebol americano, pois esses jogos sempre há um vencedor, pois eles não admite assistir 90 minutos de uma partida e o placar não sair do 0X0, sem que ninguém marque um gol e nem tenha um vencedor.

Imagine-se uma outra hipótese que seria que a seleção brasileira poderia ter feito uma pesquisa e descobrira que o jogador mais famoso nos Estados Unidos era Michael Jordan, jogador do Chicago Bulls. A seleção brasileira pretendia contar com a energia do “craque” americano, e teria verificado que ele utilizava a camisa 23. Porém, a numeração para a copa era fixa de 1 à 22, então a seleção tinha percebido que 23 era um número primo. Logo a comissão técnica resolvestes utiliza-se, os números primos nas camisas de seus principais jogadores Bebeto e Romário, escolhendo assim os números 7 e 11 para os respectivos jogadores, não sei ao certo se foi a magia dos números primos que ajudaram, mais o Brasil foi campeão, o Romário foi artilheiro e para muitos o Bebeto foi o melhor jogador desta copa.

Os números primos são os tijolos para a construção de todos os números inteiros como se fosse os “craques” dos números, ou seja, a base. Assim como as moléculas são compostas de átomos como nitrogênio, hélio, sódio, oxigênio, e carbono, os números inteiros são formados a partir de produtos de primos.

Comecei a desconfiar que a seleção tinha um “matemático” na comissão técnica. Pois, seu principal zagueiro Aldair, camisa 13 (mais de 80 jogos pela seleção apenas 5 derrotas), principal cabeça de área (volante) Mário Silva, camisa 5, lateral direito Jorginho, camisa 2. Observe que os principais jogadores da seleção estavam sempre com um número primo na sua camisa.

Mas, talvez o leitor esteja perguntando: E o goleiro da seleção Taffarel, que foi decisivo, pois defendeu um pênalti na grande final? Qual era o número de sua camisa? Esse número era primo? Bem, sim e não (precisamente este é o tipo de questionamento que todo matemático adora, e as duas respostas estão corretas). A dois séculos atrás o número 1 fazia parte das tabelas de números primos. Enfim, este não é divisível por outro natural, além de se próprio. Mas, nos dias atuais não consideramos o número 1 primo pelo motivo que os números primos servem para composição dos outros números inteiros através de produtos de dois ou mais primos, e como o número 1 é o elemento neutro da multiplicação ele acabou sendo excluído da lista, começando assim com o número 2.

Evidentemente, na existência de um "matemático" na seleção, o mesmo considerava o número 1 primo, pois num time de futebol o goleiro tem um papel muitíssimo importante na composição do time como pode ser visto nos relatos anteriormente, logo ele creditava o número 1 como primo.

Curiosidade 5.2.3: A religião e os números primos

Provavelmente você esteja se perguntando o que a Religião tem a ver com os números primos? Talvez, sua relação seja muito mais forte que a gente possa imaginar, segundo o livro Sagrado (Bíblia) na Santa Ceia, última ceia feita por Jesus antes de ser crucificado morto e sepultado, estavam presente Ele e seus doze Apóstolos, num total de 13 integrantes, portanto um número primo de pessoas. Porém, não fica só neste grande acontecimento a relação entre a religião e os números primos, segundo a Bíblia mais precisamente em Gênesis capítulo 41: 27 e 29, a terra passou 7 anos de farturas e 7 anos de vacas magras (número primo de anos!).

Certamente Deus é um grande apreciador dos números primos isso torna-se, evidente quando observamos o nome de seu primogênito JESUS CRISTO 11 letras, mais uma vez um número primo. Jesus também foi crucificado juntamente com 2 homens (ladrões). Lembre-se, 2 é o único número par primo.

Curiosidade 5.2.4: As progressões aritméticas e os números primos:

Em 2 de março de 1998. M. Topic, encontrou uma progressão aritmética que possui dez termos consecutivos primos. A razão da progressão aritmética é 210. O primeiro destes termos é o número

$p =$ 1000996972469714247637786655587969840329599324689190041803603417758904341703348882159067229719. (DIAS[20])

A história completa dessa pesquisa sobre as cigarras exóticas pode ser encontrada em REIS[21].

Curiosidade 5.2.5: Cigarras Exóticas

Bilhões de cigarras emergem nos Estados Unidos após 17 anos no solo

Figura 7 – National Geographic - 10/05/2015

As cigarras americanas **Magicicada** tem estimulado a curiosidade de muitos pesquisadores, pois durante muito tempo elas ficam no subsolo, alimentando-se de raízes. E o mais curioso é que de tempos em tempos elas emergem do subsolo prontas para acasalar nos céus americanos, curiosadamente em ciclos que variam de 17 ou 13 anos, portanto números primos.

Segundo o pesquisador Paulo Campos: "É difícil acreditar que a natureza tenha escolhido aleatoriamente esses números".

No entanto nada se pode afirmar sobre isso, o que se pode utilizar como justificativa é que esse procedimento evitam os predadores (como por exemplo: os passáros).

Essa pesquisa foi submetida para publicação no periódico científico "Physical Review Letters". (Ver[22])

5.3 Atividade diferenciada sobre números primos

Pré-requisito: Números Primos

Objetivo Geral:

Estabelecer uma relação entre os números primos e a raiz quadrada.

Objetivo específico:

Criar um ambiente favorável para expor o conteúdo de números primos.

Instigar os educandos ao importante estudo sobre os números primos.

Procedimentos:

Repartir as sala em grupos contendo 2 alunos por grupo. Entregar a cada aluno a tabela 5.3.1 e pedir para os mesmos utilizando o procedimento feito por Eratóstenes verifique um a um se os números da tabela 5.3.1 seguinte, são primos ou compostos.

2	3	4	5	6	7	8	9	10	11	Listar os números primos
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	

Figura 8 – tabela 5.3.1

Conclusão:

Está atividade foi desenvolvida na 1ª série do EM do Colégio Estadual Inês Viana, sendo que esta turma contém apenas 10 alunos, sendo que os alunos conseguiram encontrar corretamente os números primos sem maiores dificuldades, tendo como auxílio uma calculadora, conseguiram colocar de maneira correta os números compostos como produto de números primos. O tempo médio para desenvolvimento desta atividade foi de 1h 30min.

5.4 Uma incansável busca

Uma das buscas mais instigantes na área da matemática em geral é encontrar números primos, como também fórmulas que possam facilitar este trabalho tão árduo. Em torno desses trabalhos dois matemáticos do século XVII se destacaram por fazerem afirmações impressionante para época. Foram eles Pierre de Fermat e Marin Mersenne.

Em 1640, Fermat escreveu a Mersenne que acreditava que todos os números da forma seguinte eram primos:

$$F_n = 2^{2^n} + 1$$

De fato $F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$ e $F_4 = 65537$ são todos primos. Porém, em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417,$$

Portanto um número composto.

Até os dias atuais não se sabe ao certo se existem outros números primos ditos de Fermat, ou se eles são em quantidade finita.

Nesta busca por encontrar números primos Mersenne tem um destaque notáveis, pois os maiores números primos encontrados até o presente momento são da forma:

$$M_p = 2^P - 1$$

onde p é um número primo, estes números representados pela fórmula acima são conhecidos, no mundo da matemática, como números de Mersenne, em sua homenagem. Assim como os primos desta fórmula são os primos de Mersenne.

5.4.1 Outras curiosidades sobre números primos

A seguir apresentaremos mais algumas curiosidades sobre os números primos:

Curiosidade 5.4.1: Os valores de $p(p < 5000)$ para os quais tem-se, primos de Mersenne são:

$p = 2$, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253 e 4423.

Curiosidade 5.4.2: Maior número primo encontrado:

O maior número primo já calculado é de Mersenne e, é um "monstro" de 17 milhões de dígitos que, se fosse escrito por extenso, ocuparia 3,4 mil páginas impressas com 5 mil caracteres cada. Assim, a única maneira de representá-lo de forma prática é como uma potência de dois subtraindo um, mais precisamente 2 elevado a 57.885.161 menos 1. O gigante foi descoberto por Curtis Cooper, da Universidade Central do Missouri em Warrensburg, EUA, em janeiro de 2013 como parte do Great Internet Mersenne Prime Search (GIMPS), um projeto internacional que computação compartilhada desenhada para encontrar números primos de um tipo que foi descrito pela primeira vez no século XVII. Só para confirmar o status de primo do novo número, a máquina passou 39 dias inteiros fazendo os cálculos. Os números primos são divisíveis apenas por si próprios e por um e os primos do tipo Mersenne tem a forma de 2 elevado a "p" menos 1, em que "p" também é um número primo. O novo maior primo conhecido é apenas o 48º do tipo Mersenne já descoberto e o primeiro encontrado nos últimos quatro anos. O recordista anterior, também achado pelo GIMPS, tinha 13 milhões de dígitos e é expresso como 2 elevado a 43.112.609 − 1. Além deles, todos os dez maiores primos conhecidos foram encontrados pelo projeto. Fonte: o globo[23].

Chris Caldwell, professor da Universidade do Tennessee (EUA) comparou:

> "É como encontrar um diamante! Ele também mantém uma base de dados dos maiores números primos conhecidos. Por alguma razão, as pessoas decidiram que gostam de diamantes, e por isso eles são valiosos. Da mesma maneira, algumas gostam de grandes primos, e assim eles também têm seu valor".

E esse valor se traduz ainda em um prêmio em dinheiro. Cooper recebera US$ 3 mil da Electronic Frontier Foundation (EFF), uma organização não-governamental dedicada a defender a liberdade na internet, por ter achado o novo número. A EFF também oferece prêmios de US$ 150 mil e US$ 250 mil à primeira pessoa ou grupo que descobrir os primeiros números primos com 100 milhões e 1 bilhão de dígitos respectivamente. Prêmios anteriores destinados aos descobridores dos primos com 1 milhão e 10 milhões de dígitos já foram concedidos pela organização. Fonte: o globo[23]

Curiosidade 5.4.3: A lista dos 5 maiores números primos conhecidos:

1^{o} lugar: $2^{57885161} - 1$ (jan;2013) 17 425 170 dígitos;

2^{o} lugar: $2^{43112609} - 1$ (ago;2008) 12 978 189 dígitos;

3^{o} lugar: $2^{42643801} - 1$ (abr;2009) 12 837 064 dígitos;

4^{o} lugar: $2^{37156667} - 1$ (set;2008)11 185 272 dígitos;

5^{o} lugar: $2^{32582657} - 1$ (set;2006) 9 808 358 dígitos.

Note que todos os cinco maiores números primos listados acima são de Mersenne. E vale ainda ressaltar que dos dez maiores primos apenas um não é de Mersenne. Este ocupa a nona posição da lista de maiores primos.

Lembre-se que Euclides[8] demonstrou a existência de uma infinidade de números primos. Consequentemente, há sempre um número primo maior que todos os já encontrados. Então, pergunta-se: quem se habilita a encontrar um primo ainda maior?

6 NOVIDADE PARA O ENSINO MÉDIO

Um dos temas que compõe essa proposta de dissertação é a inclusão da aritmética dos restos como uma oferta de ensino para os alunos do Ensino Médio com o propósito de favorecer o processo de maturação da divisão euclidiana como também de abrilhantar concepções que têm o próprio resto de uma divisão euclidiana nos naturais ou inteiros.

6.1 Noções de Congruências

No momento em que dois números, ou um grupo maior de números, têm o atributo de possuir o mesmo resto em uma divisão por um determinado número inteiro, é possível assentar certas similaridades. A exemplo disso 18 e 22 que deixam resto 2 quando divididos por 4. Se aos dois somarmos ou subtrairmos um número exatamente igual, os novos restos da divisão por 4 permaneceram os mesmos, observe que $18+9=27$ e $22+9=31$ deixam o mesmo resto 3 na divisão por 4. Note que 9 deixa resto 1 na divisão por 4, nesta circunstância o resto 2, das divisões de 18 e 22 por 4 somado com o resto 1 da divisão de 9 por 4 resulta em 3.

Hefez[7] faz a seguinte definição:

Definição 6.1.1. *Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se*

$$\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$$

Por exemplo, $22 \equiv 18 \bmod 4$, já que os restos da divisão euclidiana de 22 e de 18 por 4 são iguais a 2.

Escreve-se, a negação da definição acima, ou seja, quando a e b não são congruentes módulo m da seguinte forma $\mathrm{a} \not\equiv \mathrm{b} \bmod \mathrm{m}$.

Para continuarmos nosso estudo sobre congruências apresentaremos algumas proposições a seguir:

Proposição 6.1.1. *Seja $m \in \mathbb{N}$. Para todos a, b, $c \in \mathbb{Z}$, tem-se que*

(i) $\mathrm{a} \equiv \mathrm{a} \bmod \mathrm{m}$*,*

(ii) Se $\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$*, então* $\mathrm{b} \equiv \mathrm{a} \bmod \mathrm{m}$*,*

(iii) Se $\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$ *e* $\mathrm{b} \equiv \mathrm{c} \bmod \mathrm{m}$*, então* $\mathrm{a} \equiv \mathrm{c} \bmod \mathrm{m}$*.*

Para verificar se um número é congruente a outro módulo m, não é necessário realizar a divisão euclidiana desses números para comparar os restos obtidos. É suficiente aplicar a seguinte propriedade:

Proposição 6.1.2. *Suponha que a, b,* $m \in \mathbb{Z}$, *com* $m > 1$. *Tem-se que* $\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$ *se, e somente se,* $m \mid b-a$.

Demonstração. A demonstração dessa propriedade poderá ser encontrada no livro Aritmética [7]. □

Proposição 6.1.3. *Sejam a, b, c, d,* $m \in \mathbb{Z}$, *com* $m > 1$.

i) *Se* $\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$ *e* $\mathrm{c} \equiv \mathrm{d} \bmod \mathrm{m}$, *então* $\mathrm{a}+\mathrm{b} \equiv \mathrm{b}+\mathrm{d} \bmod \mathrm{m}$.

ii) *Se* $\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$ *e* $\mathrm{c} \equiv \mathrm{d} \bmod \mathrm{m}$, *então* $\mathrm{a}\cdot\mathrm{b} \equiv \mathrm{b}\cdot\mathrm{d} \bmod \mathrm{m}$.

Demonstração. A demonstração dessa propriedade não será apresentada aqui o leitor interessado poderá encontrá-la no livro Aritmética [7]. □

Corolário 6.1.1. *Para todos* $n \in \mathbb{N}$, *a,* $b \in \mathbb{Z}$, *se* $\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$, *então tem-se que*

$$\mathrm{a}^{\mathrm{n}} \equiv \mathrm{b}^{\mathrm{n}} \bmod \mathrm{m}$$

Demonstração. A demonstração se faz sem maiores problemas utilizando indução finita sobre n. □

Vamos utilizar os conceitos de congruência para mostrar que o quinto número de Fermat como afirmou Euler não é primo, ou seja, que $F_5 = 2^{2^5}+1$ é composto.

Perceba que da igualdade $641 = 5\cdot 2^7+1$, tem-se, que $5\cdot 2^7 \equiv -1 \bmod 641$. Portanto pelo corolário 6.1.1, segue que

$$(5\cdot 2^7)^4 \equiv (-1)^4 \; mod \; 641 \Leftrightarrow 5^4\cdot 2^{28} \equiv 1 \; mod \; 641.$$

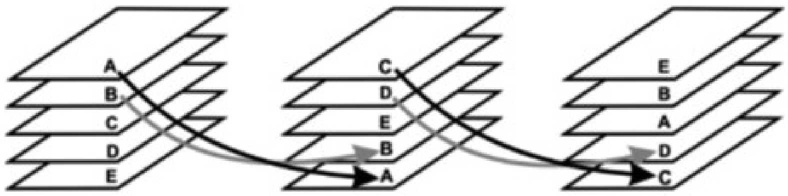
A partir disso, e da igualdade $641 = 5^4+2^4$, tem-se, que

$$5^4\cdot 2^{28}+2^{32} = 2^{28}(5^4+2^4) \equiv 1 \; mod \; 641.$$

Como $5^4\cdot 2^{28} \equiv 1 \; mod \; 641$ decorre que $2^{32} = 2^{2^5} \equiv -1 \; mod \; 641$, ou seja, pela proposição 6.1.2 tem se que $641 \mid 2^{2^5}+1$, o que mostra que $641 \mid F_5$.

Nota-se, que um dos motivos de estudar congruências no Ensino Médio é dar a verdadeira importância aos restos da divisão euclidiana e não ter esses valores como apenas uma sobra como é ensinado no Ensino Fundamental por professores e normalmente estão sendo expostos por livros didáticos. No exemplo seguinte verifica-se, esta importância.

Exemplo 6.1.1: (OBMEP-2012 Banco de questões): Estefânia tem cinco cartas marcadas com as letras A,B,C,D e E empilhadas nessa ordem de cima para baixo. Ela embaralha as cartas pegando as duas de cima e colocando-as, com a ordem trocada, embaixo da pilha. A figura mostra o que acontece nas duas primeiras vezes em que ela embaralha as cartas.



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

Solução:

Observe na tabela abaixo o que acontece nas 6 primeiras embaralhadas de Estefânia.

Posição inicial	1ª	2ª	3ª	4ª	5ª	6ª
A	C	E	A	C	E	A
B	D	B	D	B	D	B
C	E	A	C	E	A	C
D	B	D	B	D	B	D
E	A	C	E	A	C	E

Segue daí, que a cada 6 embaralhadas as cartas voltam a posição inicial, ou seja, o baralhamento torna-se periódico de período 6, basta então encontrar o resto da divisão de 74 por 6, o que é equivalente a

$$74 = 6 \cdot 12 + 2 \equiv 2 \ mod\ 6$$

Logo é a carta E que estará no topo.

A seguir apresentamos dois conteúdos, da Proposta Curricular do Ensino Médio que no uso de congruência pode trazer alguns benefícios na aprendizagem dos estudantes: Em primeiro lugar a potência do número complexo $i = \sqrt{-1}$ e o outro é o estudo de arcos côngruos.

Note que na exposição de potência do número complexo $i = \sqrt{-1}$ têm-se, os seguinte valores:

$$i^0 = 1;\ i^1 = i;\ i^2 = -1;\ i^3 = -i;\ i^4 = 1;\ i^5 = i;\ i^6 = -1;\ i^7 = -i;\ i^8 = 1;\cdots$$
$$\cdots i^{4n} = 1;\ i^{4n+1} = i;\ i^{4n+2} = -1;\ i^{4n+3} = -i;\cdots$$

Tem-se, que a potência do número i^n com $i = \sqrt{-1}$ é cíclica, ou seja, um ciclo que se repete de 4 em 4, logo pode-se, encontrar os valores destas potências do seguinte modo:

Se n $\equiv 0$ mod 4 $\Longrightarrow i^n = 1$
Se n $\equiv 1$ mod 4 $\Longrightarrow i^n = i$
Se n $\equiv 2$ mod 4 $\Longrightarrow i^n = -1$
Se n $\equiv 3$ mod 4 $\Longrightarrow i^n = -i$

Exemplo 6.1.2: Determine o valor de:

(a) i^{36} (b) i^{143} (c) $2i^{70} - i^{29}$

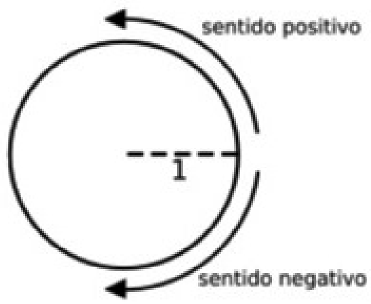
Solução:

(a) Como $36 \equiv 0$ mod $4 \Rightarrow i^{36} = i^0 = 1$.
(b) Como $143 = 4 \cdot 35 + 3 \equiv 3mod4 \Rightarrow i^{143} = i^3 = -i$
(c) Como $70 \equiv 2$ mod 4 e $29 \equiv 1$ mod $4 \Rightarrow 2i^{70} - i^{29} = 2i^2 - i = -2 - i$.

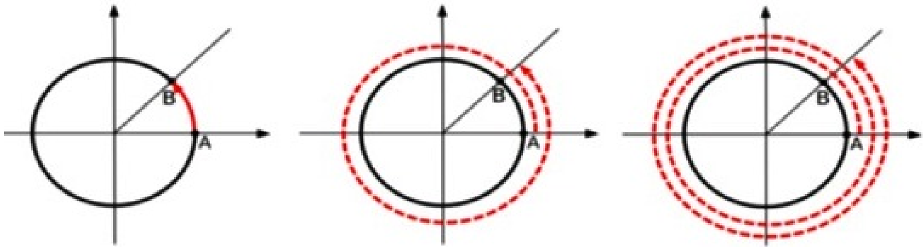
Com relação a ângulos côngruos primeiramente iremos revisar alguns conceitos acerca de trigonometria no círculo.

Segundo DANTE [6]:

> "Denomina-se circunferência trigonométrica a circunferência orientada cujo raio tem 1 unidade de comprimento e na qual o sentido positivo é o anti-horário".



Observando as figuras seguintes, têm-se uma noção do que representa um ângulo côngruo



Consequentemente para um ângulo θ(em graus) os ângulos da forma $\theta + 360 \cdot k$, com $k \in \mathbb{Z}$ estes são denominados de ângulos congruentes a θ, e suas exibições na circunferência acima são idênticas.

Note que a notação de congruência $\equiv$ pode ser favorável, permitindo uma melhor visibilidade para o problema. Como veremos do exemplo a seguir:

Exemplo 6.1.3: Nos X-Games Brasil, em maio de 2004, o skatista brasileiro Sandro Dias, apelidado "mineirinho" conseguiu realizar a manobra denominada "900", na modalidade skate vertical, tornando-se o segundo atleta no mundo a conseguir esse efeito. A denominação "900" refere-se ao número de graus que o atleta gira no ar em torno de seu próprio corpo, que, no caso, corresponde a duas voltas e meia. Considerando que a cada volta o atleta voltou a posição inicial, qual o verdadeiro ângulo do atleta em relação a posição inicial após essa façanha?

Solução:
Como $720 \equiv 0 \mod 360$ e $900 = 720 + 180$ segue que

$$720 + 180 \equiv 180 \mod 360$$

Ou seja

$$900 \equiv 180 \mod 360$$

Logo a posição final do "mineirinho" era de 180º em relação inicial.

6.2 O mundo estranho dos códigos de barras

Uma das múltiplas aplicações da aritmética modular é para detectar problemas com os misteriosos códigos de barras, presente por exemplo, em produtos comercias. Sendo que as congruências são utilizadas para detectar erros humanos de dígitação , ou seja, quando o leitor óptico não consegue fazer a leitura por algum motivo, e o operador tem que colocar manualmente esse código, pode ocorrer erros de dígitação dos algarismos, no entanto o leitor óptico é capaz de detectar alguns tipos de erros, através de um programa instalado na máquina que tem como base as congruências.

Antes de entrar no mérito dessa questão que é a relação entre as congruências e os códigos de barras iremos conhecer um pouco sobre esse misteiroso mundo dos códigos de barras, pois isso permitirá mais clareza a nossa aplicação.

Segundo o dicionário o código de barras é:

> "Uma representação de sequências alfanuméricas por barras impressas de diferentes larguras, alinhadas paralelamente, e que podem ser lidas mediante dispositivo eletrônico de leitura óptica".

Numa explicação prática, o código de barras é uma reprodução gráfica de dados. Ele permite uma ligeira compreensão de dados, oportuna rapidez nas operações, perfeição nas informações e aceita atualização quase instantânea e tudo isso origina em maior domínio, subtração de erros, gerenciamento remoto, assegurando rapidez no atendimento de pedidos e clientes, além da expressiva diminuição nos custos.

Compreendendo todos esses benefícios proporcionados pela inclusão dos códigos de barras, especialmente na área comercial, manifesta-se, a motivação para trabalhar este assunto no Ensino Médio, pois o mesmo representa uma ótima lição de aplicação de *Aritmética Modular*.

Nos dias atuais os códigos de barras se tornaram indispensáveis em todo o mundo, pois, eles permitem fazer identificações em várias áreas como, indústrias, comércio, transportes, correios entre outras.

Os códigos de barras do tipo que é conhecido hoje, com listras brancas e pretas no formato vertical foi introduzido a princípio por George J. Laurer no começo da década de setenta. O código exposto por Laurer continha 12 algarismos (números situados na parte de baixo das listras) e foi acreditado em 1973 recebendo o nome de Universal Product Code, em outras palavras Código Universal de Produtos (UPC), como mostra a Figura 9.

0 36000 29145 2

Figura 9 – UPC

Laurer em 1976, adicionou um novo número ao código, no intuito que dessa maneira, existisse a possibilidade de identificação da procedência do produto quanto ao país de fabricação do mesmo. Tornando-o em um novo código com treze dígitos, esse recebeu o nome de EAN-13 (European Article Numbering system).

Figura 10 – EAN-13

Essas barras são todas verticais e como podemos verificar na Figura 10 são alternadas, nas cores pretas e brancas, assim como são de várias espessuras, ou seja, finas, médias, grossas, ou muito grossas, que representam o número que aparece abaixo das listras. Essa leitura, é feita da seguinte maneira:

Listras	Finas	Médias	Grossas	Muito Grossas
Brancas	0	00	000	0000
Pretas	1	11	111	1111

Tabela 6 – Significado das listras

Como existe uma diferença de dígitos entre os dois sistemas o UPC e o EAN-13, e cada dígito é representado por uma sucessão de zeros e uns. Para que possam serem lidos por uma mesma leitora óptica o primeiro dígito do sistema EAN-13 é prescrito pelos 6 algarismos posteriores.

Quanto ao dígito de verificação sua função é muitíssima importante, pois nos casos em que houver um problema, que impede a leitura óptica do código, então o operador é obrigado a digitar a sequência do código e nos casos que existam erros no procedimento de digitação. Este dígito de verificação tem, recursos para detectar a presença de erros. E esse recurso é através de programas que utilizam congrências.

Admita que $w_1, w_2, \cdots, w_{12}, w_{13}$ seja a sequência de dígitos de um código qualquer do EAN-13. Como já mencionado nesta seção os 12 primeiros dígitos permitem identificar o país, o fabricante, além de caracterizar o produto, ou seja, esses números são pré-determinados. Quanto ao último dígito dos sistemas EAN-13 e UPC, será estabelecido pelos outros 12 ou 11 dígitos anteriores a ele dependendo de qual espécie é o código de barras, se for EAN-13 são 12 se for UPC serão 11.

Seja A o dígito verificador do código EAN-13, ou seja o décimo terceiro dígito da sequência, que em forma de vetor apresenta-se como: $\beta = (w_1, w_2, \cdots, w_{12}, w_{13}, A)$.

Este sistema EAN-13, emprega um vetor pré-determinado, v, apelidado de vetor de pesos, apresentado por:

$$v = (1,3,1,3,1,3,1,3,1,3,1,3,1).$$

Determinando o produto escalar dos dois vetores anteriores tem-se:

$$\beta \cdot v = (w_1, w_2, \cdots, w_{12}, w_{13}, A) \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1) = w_1 + 3w_2 + \cdots + 3w_{12} + A.$$

Como o dígito de verificação, $A \in 0,1,2,3,4,5,6,7,8,9$, de maneira que $\beta \cdot v \equiv 0 \ mod \ 10$.

Exemplo 6.2.1: Determine o valor de X para a Figura 10, no qual esse valor corresponde ao dígito de verificação do código de barras.

Solução:

Como X representa o código de verificação, o número relativo ao código de barras da Figura 10 é $489166832668X$. Utilizando uma tabela da seguinte maneira colocando esse dígitos na primeira linha com seus respectivos pesos na segunda linha e fazendo-se, o produto da primeira linha pela segunda, obtêm-se:

Digitos do códigos de barras	4	8	9	1	6	6	8	3	2	6	6	8	X
Vetor de Pesos EAN-13	1	3	1	3	1	3	1	3	1	3	1	3	1
Resultado do produto	4	24	9	3	6	18	8	9	2	18	6	24	X

Deve-se cumprir a seguinte sentença:

$\beta \cdot v = 4+24+9+3+6+18+8+9+2+18+6+24+X \equiv 0 \mod 10$. Reordenando essa soma tem-se,

$$\underbrace{6+24+6+24+18+2}_{\equiv 0 \text{ mod } 10} + 4+3+8+9+9+18+X \equiv 0 \text{ mod } 10$$

Daí segue que

$$4+8+9+9+18+3+X = \underbrace{12+18}_{\equiv 0 \text{ mod } 10} + 18+3+X \equiv 0 \text{ mod } 10$$

Então tem-se

$$21 + X \equiv 0 \text{ mod } 10$$

Como o valor de X (dígito de verificação) pertence ao conjunto: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Logo $X = 9$, ou seja, é o valor do código de verificação da figura 10. E isso se cumpriu veementemente.

Para o caso de um código UPC que contém apenas 12 dígitos o vetor terá uma coordenada a menos e se iniciará com o algarismo 3 e alternando assim com o dígito 1.

No entanto, no momento da leitura do código de barras, pode ocorrer alguma situação indesejável que faça com que o leitor óptico, ou outra circunstância que obstrui a leitura óptica do código, então será preciso que o operador efetue a leitura manualmente, ou seja, ele precisará digitar os algarismos encontrados na parte inferior do código de barras. Nesse instante será possível que aconteça uma "falha humana" e o número digitado pode não estar em concordância como o reprimido no código de barras. Se algum dos dígitos for incluído de maneira incorreta ou fora da ordem correta, provavelmente o resultado da verificação não apresente um número congruente a zero módulo dez, neste caso o processador desferirá um sinal de alerta, chamando a atenção para o erro cometido. Sugere aqui salientar, que há possibilidade de que uma falha de digitação aconteça e não seja percebida, porém essa chance é mínima.

Prosseguindo apresentaremos algumas situações onde isso acontece:

Se somente um algarismo for digitado incorretamente, pratica-se, um erro chamado erro singular, decerto o produto $\beta \cdot v$, não será congruente a zero módulo dez, neste caso o erro será percebido. Na ocorrência em que dois ou mais dígitos são inseridos incorretamente, existe há possibilidade dos erros cometido se contrapesarem uns aos outros e o resultado de $\beta \cdot v$ ser congruente a zero módulo dez. Para esse caso o erro não será detectado pelo leitor óptico.

Por outro lado podem ocorrer outros tipos de erros diferentes dos citados anteriormente, como por exemplo quando há uma transposição adjacente entre alguns dígitos, neste caso essas falhas podem ou não serem detectadas.

Exemplo 6.2.2 Considere que o número do código de barras da figura seguinte foi digitado incorretamente, nos dois casos abaixo:

7 898357 410015

Figura 11 – Código de barras [ver [24]]

1^o Caso:78983574100$\underbrace{51}$

Note que o código é um EAN-13, então o vetor de pesos é:

$$\beta = (1,3,1,3,1,3,1,3,1,3,1,3,1)$$

Como $v = (7,8,9,8,3,5,7,4,1,0,0,5,1)$. Consequentemente,

$$\beta \cdot v = 7+24+9+24+3+15+7+12+1+0+0+15+1$$

.

Daí segue que $\beta \cdot v = 118 \not\equiv 0 \ mod \ 10$, logo o erro será detectado.

2^o caso: 789$\underbrace{38}$57410015

Neste segundo caso tem-se,

$$v = (7,\ 8,\ 9,\ 3,\ 8,\ 5,\ 7,\ 4,\ 1,\ 0,\ 0,\ 1,\ 5)$$

De onde segue que,

$$\beta \cdot v = 7+24+9+9+8+15+7+12+1+0+0+3+5$$

Daí segue que $\beta \cdot v = 100 \equiv 0 \ mod \ 10$, logo o erro não será detectado.

Uma observação importante para os códigos EAN-13 e UPC é que quando dois dígitos adjacente são digitados incorretamente o erro será detectados se, e somente se o módulo da diferença entre esses dígitos for diferente de 5.

Para mais informações sobre erros detectáveis e não detectáveis sugiro consultar os livros [25] e [26].

6.3 Boletos bancários

Quitar as contas em tempos de crises, não é para ninguém uma tarefa fácil, porém é impossível livra-se delas. Mais cedo ou mais tarde será necessário obter um boleto para pagamento, da escola dos filhos, da conta de luz, das compras pela internet, entre outras.

Ao receber um boleto o mesmo poderá ser pago utilizando o código de barras. Mas, nas compras online não há necessidade da impressão do documento para fazer tal pagamento.

Pois, subsiste um número chamado “linha digitável”, constantemente na parte superior do boleto com 48 ou 44 dígitos separados em 5 grupos, e é somente esses grupos, que são necessários para o pagamento do boleto precisando apenas que o pagador anote e o leve a um caixa automático para realizar a operação. Utilize a opção pagamento com código de barras e peça para digitar o número em vez de fazer a leitura com o Scanner.

Apesar de ser muito apreciado no pagamento de boletos, sem a necessidade de imprimir o documento, a procedência e a acepção desta sequência de números não são tão conhecidos pela população em geral. São algarismos casuais? Se ocorrer a digitação de algum algarismo errado o caixa irá detectar? Um número sequencial grande? Para que serve o dígito verificador? Será que existe algo escondido por traz desse código?

Compreendendo a "linha digitável":

Figura 12 – Ilustração de boletos

Para compreender o que cada algarismo da “linha digitável” simboliza, perceba na imagem acima a separação dos algarismos em grupos, ou seja, em 5 campos. (Sugestão: o professor deverá levar alguns boletos de preferência que sejam pagáveis em qualquer banco para os alunos acompanhe o raciocínio na prática, podendo ser conta de luz, mensalidades, compras online, entre outras).

Resumindo:

BBB = código do banco emissor do boleto.
M = código da moeda (se for em reais o código é 9 se for moeda extrangeira é 8).
L = campo livre.
d = dígito verificador de campo.
D = dígito verificador geral.
V = vencimento e o valor do documento sendo que os quatro primeiros representam o vencimento, posteriormente vem uma sequência de zeros e finalmente o valor do documento sem vírgulas.

Agora fazemos a seguite pergunta: Como é obtido os dígitos de verificação de campo e o dígito de verificação geral?

Para boletos com 43 dígitos (excluído é claro o dígito de verificação geral) o cálculo desse dígito, deve-se utilizar o módulo 11 da seguinte maneira:

1) Multiplique cada um dos números que compõem o código de barras, iniciando da direita para a esquerda pela sequência $2, 3, 4, 5, 6, 7, 8, 9, 2, 3, 4 \ldots$ e assim por diante;

2) Some o resultado de cada produto obtido na multiplicação do item anterior obtendo-se um total ”X”;

3) Encontre o resto da divisão de X por 11, ou seja, $r < 11$ tal que $X \equiv r \mod 11$.

4) Calcule o dígito verificador geral através da expressão $D = 11 - r$.

Observação: caso r seja 0 (zero), 1 ou 10 o valor atribuido a D será 1.

Explicaremos agora como é determinado o dígito de verificação de cada campo, ou seja, d para boletos com 48 dígitos na "linha dígitável". Para esse cálculo, por conveniencia é usado o módulo 10, utilizando o seguinte procedimento:

1) Multiplique cada dígito de cada campo, iniciando-se da direita para a esquerda pela sequência de $2, 1, 2, 1, 2, 1, 2, \ldots$

2) Soma individualmente os algarimos dos resultados obtendo-se um total "X";

3) Divida o valor "X"por 10 $10(Y = X/10)$ e determine o resto da divisão (R);

4) Calcule o dígito verificador de campo d através da expressão: $d = 10 - R$.

Observação: Caso o resto da divisão R seja 0 (zero), para o dígito verificador de campo d deverá ser atribuido o valor 0 (zero).

Torna-se, relevante informar que os módulos nas operações acima foram escolhidos por conveniência pelos seus criadores, não tendo nenhum problema que imposibilite o uso de outros métodos (módulos) em tais operações. No entanto formalizou-se esses módulos para que não ocorresse aberração ao sistema óptico do leitor de Scanner.

6.4 O calendário e as congruências

Como aplicação de congruência, vem-se estabelecer uma fórmula para descobrir qual é o dia da semana correspondente a uma determinada data passada ou futura.

Há vários problemas a serem enfrentados ao elaborar um calendário, sendo o mais importante o fato de que o ano solar não é um número exato de dias, sendo aproximadamente de $365,242199$ dias. Este fato torna necessário que a cada tanto se deva corrigir o número de dias do ano, daí a razão da existência dos anos bissextos, que corrigem parcialmente esse defeito.

Desde o tempo do imperador romano Júlio César até o ano de 1482 vigorava no mundo ocidental o calendário Juliano, nome dado em homenagem ao imperador que o havia instituído, e que estimava a duração do ano em $365,25$ dias, segundo as medições realizadas pelos egípcios em cerca de 300 a.C. Com a medida mais apurada da duração do ano em dias e frações, a diferença entre as duas medidas resultava em um dia a menos a cada 128 anos. E para corrigir a diferença que ainda sobra foi estabelecido que os anos múltiplos de 4 e também de 100, portanto múltiplos de 400 não são bissextos.

Para simplificar as contas, a fórmula que será estabelecida posteriormente terá validade a partir do ano de 1601 e ainda, devido à irregularidade do mês de fevereiro, para dar maior uniformidade à fórmula, o colocaremos no final da contagem dos meses, ou seja, o mês 1 de um ano será março, seguindo de abril, etc., até chegar aos meses 11 e 12, que são janeiro e fevereiro (do ano seguinte). Assim os meses de janeiro e fevereiro de um determinado ano serão considerados como os meses 11 e 12 do ano anterior.

Uma data (d,m,A) será constituída por três números, onde d representa o dia, m o mês, com a conversão acima (março= 1), e A um ano posterior a 1600, ou seja, $A \geq 1601$. Por exemplo, 20 de janeiro de 1958 será representado por $(20,11,1957)$ e, 29 de fevereiro de 2016 por $(29,12,2015)$. Vem-se ainda enumerar os dias da semana como segue: domingo (1), segunda(2),…, sábado(7).

Para determinar o dia da semana $s(d,m,A)$ da data (d,m,A), procede-se da seguinte forma:

$$s(d,m,A) = d+1+\left[\frac{13m-1}{5}\right]+A+\left[\frac{A}{4}\right]-\left[\frac{A}{100}\right]+\left[\frac{A}{400}\right] \equiv mod\ 7$$

Note que o símbolo $\left[\frac{a}{b}\right]$ significa a parte inteira da divisão de a por b como já foi mencionado na seção 6.1. E vale resaltar também que o módulo 7 é utilizado na fórmula acima devido a semana ter sete dias.

Exemplo 6.4.1: A segunda Guerra Mundial foi o conflito mais sangrento e letal da história da humanidade resultando em aproximadamente 70 milhões de mortos. Não existe um consenso sobre a data final do conflito, porém o Japão fez sua rendição formal em 2 de setembro de 1945. Considerando essa data como a data oficial do fim da Segunda Guerra Mundial, pergunta-se, em que dia da semana ocorreu essa capitulação, ou seja, o fim dos conflitos?

Solução:

Como setembro é o mês 7 do cronograma para o cálculo do dia da semana, tem-se, que

$$s(2,7,1945) = 2+1+\left[\frac{13\cdot 7-1}{5}\right]+1945+\left[\frac{1945}{4}\right]-\left[\frac{1945}{100}\right]+\left[\frac{1945}{400}\right] \equiv mod\ 7$$
$$s(2,7,1945) = 2+1+18+1945+486-19+4 = 2437 \equiv 1\ mod\ 7$$

Logo a data de 2 de setembro de 1945 tão especial para a humanidade foi um belo domingo.

7 CONSIDERAÇÕES FINAIS

Através deste trabalho, conclui-se que as equações diofantinas é uma ferramenta importante para resolver algumas situações do nosso cotidiano, sendo que as vezes as utilizamos sem nenhuma percepção, como por exemplo: ao verificar se é possível sacar certa quantidade de dinheiro em um caixa eletrônico. Por outro lado essas equações mostram que o máximo divisor comum e consequentemente o algoritmo euclidiano, tem um papel de destaque neste senário, sendo que os mesmos deixam de existirem apenas para identificar qual é o máximo divisor comum de dois números inteiros, para tornar-se importante no procedimento de encontrar as soluções das equações citadas acima, como pôde ser visto ao longo desse trabalho.

Torna-se indispensável ressaltar que atualmente pelas experiências vivenciadas e pelos testemunhos de muitos colegas de trabalho em todas as ocasiões (escolas), uma empreitada muito intensa para nós educadores é oferecer um ensino de qualidade e ao mesmo tempo praticar uma matemática mais prazerosa de maneira que os alunos tomem gosto pelo estudo, e se concentrem apenas na obtenção das melhores estratégias de solução e os mesmos consigam progredir. Em outras palavras criar maneiras para que os alunos raciocinem. De maneira mais geral, favorecer isso, ou despertar o interesse é muito gratificante, é a realização dos sonhos didáticos e pedagógicos que muitos docentes possuem, porém pelas condições de trabalhos e do sistema de ensino tornam essas metodologias impraticáveis.

Com o intuito de tentar mudar essa realidade trouxe aqui uma metodologia interessante na qual procurou suprir essas dificuldades buscando trabalhar de maneira mais atraentes aos olhos dos estudantes, mas sem perca de conhecimentos predominantes como pôde ser visto por exemplo: na apresentação do quarto capítulo sobre números primos e suas curiosidades. Deixando de ensinar apenas que um número primo é aquele que possui apenas dois divisores naturais. E sim indo muito além disso, mostrando de fato a importância dos números primos para o mundo contemporâneo.

Quanto as congruências, acredita-se veemente que seu conceito poderá facilitar o aprendizado dos alunos, em muitas situações como no estudo de ângulos congruentes, e também de números complexos. Uma situação importante que merece um crédito a esse conceito é a apresentação do misterioso mundo dos códigos de barras, pois sua notação facilita a visualização do problema, isso quando queremos verificar se um erro é detectável ou não, como foi apresentado durante o último capítulo desse trabalho. Essa aplicação é importante, pois mais cedo ou mais tarde será preciso pegar um boleto para pagar uma conta, em um caixa eletrônico, seja de água, energia, faculdade, entre outros. Tornando esse procedimento corriqueiro e que esse conhecimento pode trazer certa comodidade e confiança para exercer tal tarefa sem dificuldades.

Espera-se, também que espelhados por essa proposta possam surgirem outros trabalhos nesta linha, nos quais levantem outras aplicações interessantes que poderão ser utilizadas no ensino básico.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BRASIL. Ministério da Educação, Secretaria de Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais** (PCN): Ensino Médio. -Brasília: MEC/SECTEC, 2002, p.253.

[2] BRASIL. Ministério da Educação. **Leis de Diretrizes e Bases da Educação**. – Brasília-DF: Senado Federal. p.33.

[3] HEFEZ, Abramo. **Elementos de Aritmética**. 2 ed. –Rio de Janeiro: SBM, 2011. (Coleção do professor de matemática).

[4] SILVA, Claudio Xavier da; FILHO, Benigno Barreto. **Matemática aula por aula** – 2.ed.renov. – São Paulo: FTD, 2005. (Coleção matemática aula por aula)

[5] GIOVANNI, José Ruy; BONJORNO, José Roberto. **Matemática Completa**. – 2.ed.renov. – São Paulo: FTD, 2005. (Coleção matemática completa).

[6] DANTE, Luiz Roberto. **Matemática: Contexto e Aplicações**. – São Paulo: Ática, 2010. (coleção).

[7] HEFEZ, Abramo. **Aritmética**. –Rio de Janeiro: SBM, 2013. (Coleção PROFMAT).

[8] EUCLIDES. **Os Elementos**. Tradução e Introdução de Irineu Bicudo. –São Paulo, SP: editora: UNESP, 2009.

[9] BRASIL. Secretária de Educação Fundamental. **Parâmetros curriculares nacionais: introdução aos parâmetros curriculares nacionais**. – Brasília: MEC/SEF, 1997.(PCN+)

[10] Máximo divisor comum: <https://www.google.com.br/?gfe_rd=cr&ei=ctJnVa3dKyp8we35YCABQ&gws_rd=ssl#q=aplica%C3%A7%C3%A3o+maximo+divisor+comum > acesso em: 29 de maio de 2015.

[11] Vídeo sobre máximo divisor comum <https://www.youtube.com/watch?v=-A-_kA12a9U > acesso em: 29 de maio de 2015.

[12] CAMPOS, Gisele D. Marciano. **Equações Diofantinas Lineares**. – Universidade Federal de Mato Grosso: Instituto de Ciências Exatas e da Terra (Programa de pós graduação em Matemática), Cuiabá, 2013.

[13] O uso das equações diofantinas no EM: < http://stoa.usp.br/wmpommer/files/3810> acesso em 20 de maio de 2015.

[14] IEZZ, G et.al., Coleção: **Matemática, Ciências e Aplicações**. 2. – São Paulo: Atual, v2, 2004.

[15] CORTELLA, Mário Sergio. **A Escola e o Conhecimento: Fundamentos Epistemológicos e Políticos**. - São Paulo, Editora Cortez, 1998. p.159.

[16] SAUTOY. Marcus du. **A Música dos Números Primos: A história de um problema não resolvido na matemática**. Tradução: Diego Alfaro, 2007.

[17] **Referencial Curricular do Ensino Fundamental das escolas públicas do Estado do Tocantins**: Ensino Fundamental do 1º ao 9º ano. 2 ed. Secretaria de Estado da Educação e Cultura. Palmas-TO: 2008. 281 p.

[18] História sobre números primos: <http://www.testonline.com.br/curprimos.htm> acesso em 25 de junho de 2015.

[19] Fotos da seleção brasileira: <https://www.google.com.br/?gfe_rd=cr&ei=jPZqVYhw6ZTxB_yFgdgI&gws_rd=ssl#q=foto+da+sele%C3%A7%C3%A3o+brasileira+de+1994>acesso em:12 de maio de 2015.

[20] DIAS, Cristina Helena Bovo Batista. **Números primos e Divisibilidade: Estudo de propriedades**. Universidade Estadual Paulista – Instituto de Geociências e Ciências Exatas. Campos de Rio Claro, 2013.

[21] REIS. Carlos Costa do. **Oficina de aritmética: o uso dos números primos na resolução de problemas e algumas curiosidades**. Universidade Federal do Espirito Santo – 2014 (Dissertação de mestrado).

[22] Pesquisa sobre as abelhas exóticas: <http://www1.folha.uol.com.br/folha/ciencia/ult306u_11973.shtml> acesso em 10 de maio de 2015

[23] Maior número primo encontrado: <http://oglobo.globo.com/sociedade/ciencia/maior-numero-primo-ja-calculado-tem-17-milhoes-de-digitos-7499486> acesso em 30 de maio de 2015.

[24] Mundo estranho dos códigos de barras: <http://mundoestranho.abril.com.br/materia/como-funciona-o-codigo-de-barras> acesso em 23 de maio de 2015.

[25] DIAS, Eduardo Marques. **Código de barras**. Universidade Católica de Brasília – Departamento de Matemática.

[26] MILIES, César Polcino. **A matemática dos códigos de barras**. 19 f. São Paulo: IME/USP – Departamento de Matemática – SP.