UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

DISSERTAÇÃO DE MESTRADO

Introdução à Teoria dos Números: Uma Nova Proposta para Educação Básica

Nicholas Ursulino da Silva

Instituto de Matemática

Maceió, Março de 2019

PROFMAT

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

INTRODUÇÃO À TEORIA DOS NÚMEROS: UMA NOVA PROPOSTA PARA EDUCAÇÃO BÁSICA

NICHOLAS URSULINO DA SILVA

MACEIÓ - AL
2019

NICHOLAS URSULINO DA SILVA

INTRODUÇÃO À TEORIA DOS NÚMEROS: UMA NOVA PROPOSTA PARA EDUCAÇÃO BÁSICA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade Federal de Alagoas, como requisito parcial para a obtenção do grau de mestre em Matemática.

Orientador: Prof. Dr. Rinaldo Vieira da Silva Júnior

MACEIÓ - AL
2019

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Bibliotecário Responsável: Helena Cristina Pimentel do Vale – CRB4 - 661

S586i Silva, Nicholas Ursulino da.
Introdução à teoria dos números : uma nova proposta para educação básica / Nicholas Ursulino da Silva. – 2019.
58 f. ; il.

Orientador: Rinaldo Vieira da Silva Júnior.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal de Alagoas. Instituto de Matemática. Maceió, 2019.

Bibliografia: f. 53.
Apêndices: f. 54-58.

1. Matemática – Estudo ensino. 2. Números – Teoria. 3. Educação básica. 4. Aritmética – Resolução de problemas. I. Título.

CDU: 511:372.47

Folha de Aprovação

NICHOLAS URSULINO DA SILVA

INTRODUÇÃO A TEORIA DOS NÚMEROS: UMA NOVA PROPOSTA PARA A EDUCAÇÃO BÁSICA

Dissertação submetida ao corpo docente do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Instituto de Matemática da Universidade Federal de Alagoas e aprovada em 15 de março de 2019.

Banca Examinadora:

Rinaldo V. da S/ni

Prof. Dr. Rinaldo Vieira da Silva Junior – UFAL (Presidente)

Márcio Cavalcante de Melo

Prof. Dr. Márcio Cavalcante de Melo - UFAL

Márcio Silva Santos

Prof. Dr. Márcio Silva Santos – UFPB

MACEIÓ – 2019

Dedicatória

Dedico este trabalho a todos os meus familiares e em especial aos meus pais e minha esposa que sempre estiveram do meu lado e me incentivaram a estudar e a nunca dessistir de meus objetivos, dedico também a todos os que acreditaram e estiveram junto comigo durante todo esse processo de aprendizagem.

"Deus dá as batalhas mais difíceis aos seus melhores soldados."
Papa Francisco

Agradecimentos

Agradeço, primeiramente a Deus pelo Dom da Vida, pois sem ela não seria possível chegar até aqui e por ter me dado uma nova oportunidade de trilhar esse caminho acadêmico.

Agradeço a minha família em especial aos meus pais, Maria Bernadete e Sebastião Ursulino e a minha esposa Elaine Santana, por sempre terem me dado força, apoio emocional e me incentivado a nunca desistir, além de toda paciência que tiveram comigo quando eu estava estudando, pois foram várias horas dedicada ao estudo.

Agradeço aos meus colegas de curso, em particular e especialmente a David, Alyrio, Hilário, Claúdio e Edgar, pela atenção, companhia, conselhos, por todos os dias dedicados aos estudos e conhecimento passados por esses Mestres da matemática. Além de me fazer enxergar a matemática de várias formas.

Agradeço a todos aqueles que torceram por mim e me ajudaram ao longo dessa caminhada.

Agradeço a todos os professores deste programa de mestrado que me fizeram crescer matematicamente, em especial ao meu orientador Rinaldo Vieira da Silva Júnior, por todo o ensinamento matemático e por confiar no meu potencial.

E por fim, agradeço aos professores Isnaldo Issac(Diretor do Instituto de Matemática da UFAL) e Adina Rocha por suas dicas e ajuda na primeira correção da dissertação, dando opiniões e sugestões importantíssimas nos desdobramentos das pesquisas.

Resumo

O presente trabalho apresenta resultados de uma investigação que teve como objetivo implementar o conteúdo de Teoria dos Números no ensino básico, buscando e implementando esses novos conhecimentos com o objetivo de melhorar o desempenho dos alunos nas soluções de problemas matemáticos, além de reduzir o tempo gasto para a solução destes problemas. Optamos por uma abordagem qualitativa, utilizando pesquisa documental e de campo. Realizamos entrevistas semiestruturadas com 20 professores de matemática que lecionam na educação básica e com 70 alunos do ensino médio. O estudo permitiu concluir que a implementação da Teoria dos Números na educação básica, melhorou o conhecimento matemático dos alunos, além de diminuir o tempo para solução de problemas. A educação básica constitui-se em um espaço propício para o desenvolvimento de novas habilidades e de ideias matemáticas relevantes.

Palavras-chave: Ensino da Teoria dos Números, Educação Básica, Resolução de Problemas, Aritmética.

Abstract

The present work presents results of an investigation that had as objective to implement the content of Number Theory in basic education, seeking and implementing this new knowledge with the objective of improving students' performance in the solutions of mathematical problems, besides reducing the time spent solutions to these problems. We opted for a qualitative approach, utilizing documentary and field research. We conducted semi-structured interviews with 20 mathematics teachers who teach in basic education and 70 high school students. The study allowed to conclude that the implementation of Number Theory in basic education improved the students' mathematical knowledge, as well as reducing the time for solving problems. Basic education is a space conducive to the development of new skills and relevant mathematical ideas.

Keywords: Teaching of Number Theory, Basic Education, Problem Solving, Arithmetic.

Sumário

Introdução

Desde a antiguidade existia a necessidade de contar objetos e coisas e esta necessidade existe há mais de 30.000 anos, muito antes de haver escrita e civilização. Os homens nessa época viviam em cavernas e grutas e não existia a ideia de números, mas eles tinham a carência de contar e representar quantidades e com a evolução humana, de uma vida primitiva para uma vida em sociedade, englobaram – se novos desafios sociais e econômico e diante disso o homem tinha de pensar numericamente. No início o homem desenvolveu a capacidade de comparar conjuntos de objetos e estabelecer entre eles uma correspondência um a um, porém isto não era suficiente para construir um sistema de contagem. Seria necessário ainda introduzir a noção de ordem e daí surgiram os primeiros números.

> *A princípio os números inteiros eram suficientes para representar quantidades. Mas não foi só de contar que o homem teve necessidade. A agricultura fez o homem desenvolver sua percepção de tempo e de espaço que o levou a estabelecer, a partir das observações feitas ao seu redor, noções relativas às fases da Lua e às estações do ano que se constituíram nos primeiros indícios de um calendário. (GONGORRA; SODRÉ, 2005).* [2]

Analisando um pouco da história percebeu –se os sumérios, por volta de 2500 a.C., eles já possuíam um calendário e faziam o uso da base sexagesimal. Além de desenvolverem algum tipo de aritmética no estudo da astronomia.

No Antigo Egito encontra-se o Papiro de Rhind ou Papiro de Ahmes. Esse documento egípcio é datado de 1650 a.C., onde um escriba de nome Ahmes detalha a solução de 85 problemas de aritmética, frações, cálculo de áreas, volumes e progressões. É um dos documentos antigos mais famosos que descreve registros onde é possível perceber como a Matemática era praticada naquela época.

Com isso percebemos que o estudo de aritmética é muito antigo e com o passar dos tempos e a evolução do sistema de numeração, consequentemente as civilizações também evoluíram e isso propiciou muitas mudanças desde o início das civilizações até os dias atuais; pois os números estão presentes em basicamente todas nossas atividades. Tudo isso contribuiu para o avanço e evolução da matemática de modo que o estudo das propriedades dos números inteiros evoluiu e evolui, fascinando a mente humana, pois suas propriedades desafiaram inúmeros estudiosos através de seus conceitos e propriedades que vão além de qualquer simplicidade. Em razão da necessidade do avanço da matemática, para ajudar o homem no dia a dia, os matemáticos foram deixando um legado de registros documentados, que com o passar dos anos, foram transmitidos de geração para geração, contribuindo cada vez mais para o avanço da matemática. Parte desta herança é constituída de aritmética, o qual será um dos nossos objetos de estudo, pois vamos descobrir relações que diferentes tipos de números podem estabelecer.

Muitos desses algoritmos tornaram-se parte da literatura da teoria dos números, e muitos desses estão presentes nos livros didáticos atuais, livros esses utilizados diariamente nas unidades escolares.

Contudo, é notório que atualmente, não se deve aplicar os conteúdos de forma direta. É necessário apresentar os conteúdos em sala de aula de forma contextualizada, aplicando os conteúdos a situações do cotidiano do aluno, para que o processo de ensino aprendizagem se torne mais fácil.

O presente trabalho pretende contribuir com propostas curriculares para o Ensino Básico com o objetivo de impulsionar, melhorar os resultados em matemática nos vestibulares e minimizar o tempo gasto nas soluções de questões de vestibulares e concursos, garantindo ao aluno um melhor desempenho e um conforto maior na hora de fazer uma prova, além de ajudar aos professores a desenvolverem essa técnica e em qual momento é ideal aplicarem esses conteúdos específicos da disciplina de teoria dos números e quais são eles. Pois esses conteúdos irão ajudar os alunos a responderem questões de matemática de uma forma mais rápida aplicando essa técnica, além de aumentar a curiosidade dos estudantes em sala de aula na disciplina de matemática e melhorar os desempenho deles. É ideal que esse conteúdo seja aprofundado de duas formas ou no inicio do ano letivo quando o professor esta fazendo revisão ou a medida que ele ministra cada conteúdo ele encaixe essa noção de teoria dos números, mostrando aos alunos novas maneiras de resolver problemas. Contudo este trabalho não pretende resolver o problema da matemática do Ensino básico, mas sim contribuir para o processo de evolução desse ensino, com ideias novas a serem trabalhadas, no decorrer da educação básica. Aplicaremos conceitos de divisibilidade e congruência, buscando uma interação entre o que é ensinado e situações-problemas de matemática no cotidiano, tornando o ensino de matemática mais atraente e surpreendente através dos resultados apresentados.

Em muitos problemas do cotidiano a congruência modular é uma ferramenta de extrema importância. O estudo irá mostrar várias situações-problemas em que a aplicação de congruência é essencial para resolver o problema de forma prática. Porém, o estudo de aritmética modular é um conteúdo que acaba não sendo visto na educação básica. Sendo visto apenas no ensino superior por estudantes que seguem alguns ramos das ciências exatas. E este conteúdo irá ajudar os alunos a resolverem problemas de matemática de maneira mais rápida, logo acredita - se que é ideal que seja visto ao menos noções na educação básica.

Utilizando como motivação o ensino da matemática como ferramenta de formação de um cidadão crítico, capaz de compreender pensamentos conceituais, este trabalho irá propor a inserção de uma introdução ao ensino de "teoria dos números" na educação básica, mostrando e discutindo que suas aplicações são de extrema importância para resolução de problemas de forma mais rápida e prática.

Em síntese, o principal objetivo do trabalho, ressalta em chamar a atenção para as necessidades de se elaborarem novas ideias, para otimizar o ensino da aritmética nas escolas de ensino básico, aplicando mais criatividade no cotidiano do aluno no que tange o ensino de matemática que consequentemente aumentará o poder de atração e persuasão entre os jovens estudantes da matemática contemporânea. Pois o ensino de teoria dos números aplicados em momentos cruciais durante a vida escolar se torna uma ferramenta fantástica para o desenvolvimento da matemática e na resolução de problemas.

Defende-se no presente estudo, a importância de se estender o ensino de noções de

aritméticas, para além de seu resumido universo do nível superior, estendendo esse conhecimento para todo ensino básico, no qual tal conhecimento tem sido restrito. Esta restrição tem reduzido a capacidade de aplicabilidade dos alunos, impedindo-os que avancem cada vez mais no conhecimento matemático para resolução de problemas, no qual à aritmética exerce uma imensurável probabilidade de novas ideias para resolução de problemas.

A falta de expansão desse conhecimento tem contribuído de forma indireta para a matemática acabar sendo "taxada" de "matéria difícil", quando na verdade deveria ser vista como matéria sublime e incrível, pois é uma disciplina essencial para o crescimento tecnológico e científico. Acredita – se que a aplicação desse conhecimento no ensino básico facilitaria no ensino da resolução de muitos problemas. E isso foi testado e aplicado em uma sala de aula da educação básica no município de Arapiraca, e foi obtido um resultado bem satisfatório e surpreendente, o qual será descrito e demonstrado nos capítulos a seguir.

Fica aqui a seguinte reflexão: A aritmética está em tudo, na arte, na física, na química, na linguagem, no universo. Por que não como um conteúdo obrigatório para o ensino básico?

Esta dissertação em tese, procura alcançar esta resposta. Além de obter conclusões sobre a adequação deste conteúdo nesta fase de aprendizagem e mostra que é uma proposta necessária e condizente e útil neste ciclo escolar. O leitor encontrará nas próximas páginas, do presente estudo, o resultado de uma árdua tentativa de propor um debate sobre o mencionado tema.

Como metodologia elegeu-se a mais simples utilização de problemas do cotidiano dos educandos focados principalmente em questões de vestibulares e concurso, aos quais os futuros alunos irão se submeter. Essa metodologia tem o intuito de informar, explorar e ensinar os conteúdos propostos, além de atividades diferenciadas e a apresentação de algumas curiosidades do mundo dos números. A seguir explanaremos alguns conteúdos e resultados básicos para o conhecimento do professor afim de que ele seja capaz de desenvolver as atividades necessárias proposta no trabalho para atingir o resultado desejado.

Capítulo 1

CONCEITOS PRELIMINARES

A seguir iremos apresentar conceitos de divisibilidade e suas propriedades, conceitos esses muito importantes para dar base ao leitor da pesquisa além de ser importante para o entendimento do leitor. Posteriormente espera-se que esses conceitos sejam ferramentas úteis para um melhor desenvolvimento nas soluções de problemas matemáticos.

1.1 Inteiros e Divisibilidade

Os números naturais é um modelo matemático, que permite a operação de contagem. A sequência desses números é uma antiga criação do homem e essa tecnica será chamada de contagem. **Giussepe Peano** (1858-1932), produziu toda a teoria dos números naturais a partir de quatro axiomas, conhecida como axiomas de Peano.

P1. Todo número natural tem um único sucessor, que também é um número natural.

P2. Números naturais diferentes tem sucessores diferentes.

P3. Existe um único número natural, designado por 1, que não é sucessor de nenhum outro.

P4. Seja X um conjunto de números naturais, tais que $X \subset \mathbb{N}$. Se $1 \in X$ e se, além disso, o sucessor de cada elemento de X ainda pertence a X, então $X \subseteq \mathbb{N}$.

Assim, designaremos o conjunto dos números naturais através do símbolo $\mathbb{N}$, onde $\mathbb{N} = \{0, 1, 2, 3, 4, 5, ...\}$. É comum adotar o 0 como ponto de partida do conjunto dos naturais, porém é uma questão de gosto e conveniência.

O conjunto dos números naturais $\mathbb{N}$ possui uma função s: $\mathbb{N} \rightarrow \mathbb{N}$ chamada **função sucessor**, para cada número $n \in \mathbb{N}$, o número s(n), é o valor que a função "s"assume no ponto n, chamado de sucessor.

Embora todos os axiomas de Peano sejam essenciais para a caracterização dos números naturais, o último axioma, o qual chamaremos de **Axioma da indução** , se destaca. Pois ele fornece um mecanismo que garante que dado um subconjunto X de $\mathbb{N}$, inclui todos os elementos de $\mathbb{N}$. Sendo uma ferramenta primordial para construir definições e demonstrar teoremas.

Antes de falar do princípio da indução finita é necessário introduzir uma propriedade dos números inteiros, que é o *Princípio da Boa Ordenação*.

Definição 1.1.1. *Todo subconjunto $S \subset \mathbb{N}$ é limitado inferiomente, se existir um $c \in S$ tal que $c \leq x$, $\forall\, x \in S$.*

Assim diremos que $a \in S$ é *um menor elemento* de S, se $a \leq x$, $\forall\, x \in S$.

Princípio da Boa Ordenação: Todo subconjunto não vazio de $S \subset \mathbb{N}$ possui um menor elemento.

Demonstração: Considere $I_n = \{k \in \mathbb{N};\, k \leq n\}$, onde I_n é o conjunto dos números naturais menores ou iguas a n. Note que, se $1 \in S$ nada a se fazer pois 1 é o menor elemento de S. Porém, se $1 \notin S$, então existe um conjunto X dos números naturais n tais que $I_n \subset \mathbb{N} - S$. Como $I_1 = \{1\} \subset \mathbb{N} - S$, vemos que $1 \in X$. Por outro lado, como S não é vazio, então X $\neq \mathbb{N}$. E isto contradiz o axioma P_4 de *Peano*. Logo, deve existir $n \in S$ tal que n $+ 1 \notin X$. Então $I_n = \{1, 2, ..., n\} \subset \mathbb{N} - S$. Portanto, c é o menor elemento do conjunto A.

Princípio de Indução Matemática: Sejam S um subconjunto de $\mathbb{Z}$ e a $\in \mathbb{Z}$ tais que

i) $a \in S$

ii) S é fechado com respeito ao sucessor de seus elementos, ou seja, $\{\forall\, n, n \in S\} \Rightarrow n + 1 \in S$. Então,$\{x \in \mathbb{Z}; x \geqslant a\} \subset S$.

Demonstração:
Tomemos $S' = \{x \in \mathbb{Z}; x \geqslant a\}$ e supohamos por absurdo que $S' \not\subset S$, logo $S' \setminus S \neq \emptyset$. Como esse conjunto é um conjunto limitado inferiormente por a,então pelo princípio da boa ordenação, existe um menor elemento c em $S' \setminus S$. Como $c \in S'$ e $c \notin S$, temos que $c > a$. Então, $c - 1 \in S'$ e $c - 1 \in S$. Mas por hipótese, temos que $c = (c - 1) + 1 \in S$, mas $c \in S'$, logo absurdo! Portanto $c \in S' \setminus S$.

A seguir vamos definir a importante noção de valor absoluto, pois será usada em alguns resultados.
Seja $a \in \mathbb{Z}$, definimos

$$|a| = \begin{cases} a, \ se\ a \geq 0 \\ -\ a, \ se\ a < 0 \end{cases}$$

Note que para todo $a \in \mathbb{Z}$, tem - se que $|a| \geq 0$ *e* $|a| = 0$ se, e somente se, a $= 0$. O número inteiro $|a|$ é chamado de valor absoluto de a.

Proposição 1.1.1. *Não existe nenhum número intereiro n tal que 0 < n <1.*

Demonstração: Suponha por absurdo que exista um n com essa propriedade. Então o conjunto S $= \{x \in \mathbb{Z}; 0 < x < 1\}$ é não vazio, além de ser limitado inferiormente. Portanto, S possui um menor elemento s, com $0 < s < 1$. Multiplicando esta desigualdade por s, temos $0 < s^2 < s < 1$, logo $s^2 \in S$ e $s^2 < s$, logo absurdo, pois s é o menor elemento. Portanto, $S = \emptyset$.

Corolário 1.1.1 (Propriedade Arquimediana)**.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > 0$.*

Demonstração: Como o $|b| \neq 0$, então pela proposição acima, temos que $|b| \geq 1$, multiplicando a desigualdade por $(|a| + 1)$. logo

$$(|a| + 1)\ |b| \geq |a| + 1 > |a| \geq a.$$

Assim tomando $n = |a| + 1$, o resultado segue. Se $b < 0$, basta tomar $n =$ - $(|a| + 1)$.

1.2 Divisibilidade

Dados dois números inteiros a e b, diremos que a divide b, denotado por $a|b$, quando existe um $c \in \mathbb{Z}$ tal que $b = ca$. Assim, dizemos que a é um divisor de b, ou que b é um múltiplo de a, ou seja, b é divisível por a.

Observe que a negação da sentença $a|b$, será representada por $a \nmid b$, significando que não exite nennhum inteiro c tal que $b = ca$.

Proposição 1.2.1. *Sejam $a, b, c \in \mathbb{Z}$. Temos que*

i. $1 \mid a,\ a \mid a \ \ e \ \ a \mid 0$.

ii. $0 \mid a \Leftrightarrow a = 0$.

iii. a divide b se, e somente se, $|a|$ divide $|b|$

iv. se $a \mid b$ e $b \mid c$, então $a \mid c$

Demonstração.

(i) Basta notar que $a = 1a,\ a = a1\ e\ 0 = 0a$.

Para mostrar o item (ii), vamos enunciar e demonstrar a seguinte lema.

Lema 1.2.1. *$a0 = 0$ para todo $a \in \mathbb{Z}$.*

Demonstração:

$$a0 = a(0 + 0) = a0 + a0$$
Somando -$(a0)$ em ambos os membros da igualdade, temos que
$$0 = \text{-}(a0) + a0 = \text{-}(a0) + (a0 + a0)$$
$$= (\text{-}(a0) + a0) + a0 = 0 + a0$$
$$= a0$$

(ii) Se $0|a$, então existe $c \in \mathbb{Z}$ tal que $a = c0$. Pelo lema 1 conclui-se que $a = 0$. A recíproca basta notar que $0|0$, que foi mostrado no item (i).

(iii) Se $a|b$, então existe um $c \in \mathbb{Z}$, tal que $b = ca$.
Logo, |b| = $|ca| \Rightarrow |b| = |c|\ |a| \Rightarrow |a|$ divide $|b|$.
Reciprocamente, sejam $a < 0$ e $b < 0$, se $|a|$ divide $|b|$, então $|b| = c|a| \Rightarrow$
-b = c(-a) $\Rightarrow$ -b = -(ca)$\Rightarrow$ $b = ca$, portanto $a|b$. O resultado segue para $a \geq 0$ e $b \geq 0$.

(iv) Se a divide b e b divide c, existem $k_1 e k_2 \in \mathbf{Z}$, tais que $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$ temos $c = k_2 k_1 a$ isto implica que $a \mid c$.

Exemplo 1.1. Se 3|12 e 12|48, então 3|48.

Proposição 1.2.2. *Se $a, b, c, d \in \mathbb{Z}$, então*

$$a|b \ e \ c|d \Rightarrow ac|bd.$$

Demonstração: Se $a \mid b$ e $c \mid d$, então $\exists\ k_1 e k_2 \in \mathbf{Z}$, tal que $b = k_1 a$ e $d = k_2 b$. Assim $bd = (k_1 k_2)(ac) \Rightarrow ac|bd$.

Proposição 1.2.3. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b \pm c)$. Então*

$$a|b \Leftrightarrow a|c.$$

Demonstração: Suponhamos que $a|(b+c)$. Logo, existe $k_1 \in \mathbb{Z}$ tal que $b+c = k_1 a$. Por outro lado, se $a|b$, então existe um $k_2 \in \mathbb{Z}$ tal que $b = k_2 a$.
Substituindo uma equação na outra temos que $k_2 a + c = k_1 a \Rightarrow c = (k_1$ - $k_2)a$, logo $a|c$. De modo análogo, se $a|c$, $\exists\ k_3 \in \mathbb{Z}$, tal que $c = k_3 a$. Substituindo na primeira equação temos $b + k_3 a = k_1 a \Rightarrow b = (k_1$ - $k_3)a$, logo $a|b$.
O caso em que $a|(b$-$c)$ é demonstrado de forma análoga.

Proposição 1.2.4. *Se $a, b, c \in \mathbb{Z}$, são inteiros tais que $a|b$ e $a|c$, então para todo $m, n \in \mathbb{Z}$*

$$a|(mb + nc).$$

Demonstração: Se $a|b$ e $a|c$, então $b = k_1 a$ e $c = k_2 a$, com $k_1 e k_2 \in \mathbb{Z}$. Assim $mb + nc$= m($k_1 a$) + n($k_2 a$) = m$k_1 a$ + n$k_2 a$ = (mk_1)a) + (nk_2)a) = (mk_1 + nk_2)a.

Exemplo 1.2. Como 3|15 e 3|42, então 3| $(8 \times 15 - 7 \times 42)$.

A seguir vamos introduzir um importante resultado da obra de Euclides que é o teorema da divisão Euclidiana. A divisão euclidiana, também conhecida como divisão inteira ou divisão com resto, é um assunto essencial nos primeiros anos de aprendizado. Ele é definido de forma que todos os números inteiros podem ser divididos por um inteiro natural diferente de zero e ter como resultado um quociente e um resto, no qual o resto sempre deve ser menor que o divisor.

Teorema 1.2.1 (Divisão Euclidiana)**.** *Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que $a = bq + r$, com $0 \leq r < |b|$.*

Demonstração: Seja

$$\mathrm{S} = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Pelo Corolário 1.1.1, existe $n \in \mathbb{Z}$ tal que n(-b) > -a, logo a - $nb > 0$, o que mostra que S é não vazio. Note que o conjunto S é limitado inferiormente por 0, então pelo Princípio da Boa Ordenação, S possui um menor elemento r. Suponhamos então que $r = a$ - bq, como r ≥ 0, por hipótese vamos mostrar que $|r| < b$.
Suponha por absurdo que r $\geq |b|$. Logo existe um s $\in (\mathbb{N} \cup \{0\})$ tal que r = $|b|$ + s, ou seja, 0 $\geq$ s $<$ r. Mas isso contradiz o fato de r ser o menor elemento de S, pois s = a - (q $\pm$ 1)b $\in$ S, com s $<$ r.

Unicidade: Suponhamos que $a = bq + r = = bq' + r'$, onde q, q', r, r' $\in \mathbb{Z}$, 0 $\leq$ r $<$ $|b|$ e 0 $\leq$ r' $<$ $|b|$. Assim, temos que -$|b|$ $<$ -r $\leq$ r'- r $\leq$ r' $<$ $|b|$. logo, |r' - r| $<$ $|b|$. Por outro lado, **b**(q - q') = r' - r $\Rightarrow$ |**b**||(q - q')| = |r' - r| $<$ |**b**|, que somente é possível se q = q' $\Leftrightarrow$ r = r'.
Com isso, os números q e r são chamados, respectivamente, de quociente e resto da divisão de a por b. E o resto desta divisão é zero se, e somente se, b divide a.

A demonstração acima da existência e unicidade do quociente q e do resto r são encontradas em muitos textos e já eram conhecidas de Euclides no terceiro século antes de Cristo. Usamos a demonstração feita por [3]

Exemplo 1.3: Suponha que se deseje dividir 55 por 7. Note que não será possível nos números naturais. Porém podemos admitir um resto natural r = $55 - 7 \times 7 = 6$. De modo que a representação dessa operação na forma do algoritmo da divisão euclidiana fica assim:

$$55 = 7 \times 7 + 6.$$

1.3 Máximo Divisor Comum

Sejam dados dois inteiros a e b, distintos ou não. Um número inteiro d é dito *divisor comum* de a e b se $d \mid a$ e $d \mid b$.
A definição a seguir é dada no livro VII dos Elementos de Euclides e consiste em ums dos pilares da teoria dos números.

Definição 1.3.1. *Um número inteiro $d \geq 0$ é um máximo divisor comum (mdc) de a e b, se possui as seguintes Propriedades:*

i) d é um divisor comum de a e b

ii) d é divisível por todo divisor comum de a e b. Em outras palavra, se c é um divisor comum de a e b, então $c|d$.

Observação: O mdc de dois números a e b, será denotado por (a,b).

Exemplo 1.4: O mdc de 12 e 18 é 6, que será denotado da seguinte forma (12,18) = 6.

Pela condição ii) acima, se d e d' são dois mdc de um mesmo par de números , então $d|d'$ e $d'|d$, que juntamente com o fato de $d \geq 0$ e $d' \geq 0$, implica que $d = d'$. Ou seja, o mdc de dois números quando existe é único.

Lembre que o mdc de a e b não depende da ordem que a e b são tomados, então temos que

$$(a,b) = (b,a)$$

Exemplo 1.5: Se a é um número inteiro, é fácil verificar que $(0,a) = |a|$, $(1,a) = 1$ e que $(a,a) = |a|$.

Mais ainda, $\forall\ b \in \mathbb{Z}$, temos que

$$a|b \Leftrightarrow (a,b) = |a|.$$

De fato, se $a|b$, temos que $|a|$ é um divisor comum de a e b, e se c é um divisor comum de a e b, então c divide $|a| \Rightarrow |a| = (a,b)$. Análogamente, se $(a,b) = |a| \Rightarrow |a|$ divide b. Logo, $a|b$.

O mdc de dois números inteiros é o maior número inteiro que divide ambos sem deixa resto. O algoritmo de Euclides é baseado no princípio que o mdc não muda se o menor número for subtraído ao maior.

Como o maior dos dois números é reduzido, a repetição deste processo irá gerar sucessivamente números menores, até convergir em zero. Nesse momento, o MDC é o outro número inteiro, maior que zero. A mais antiga descrição que se conhece do método usado no algoritmo de Euclides é da sua obra "Elementos de Euclides"(300 a.C.), o que o torna um dos algoritmos numéricos mais antigos ainda em uso corrente. O algoritmo original foi descrito apenas para números naturais e comprimentos geométricos, mas foi generalizado no século XIX para outras classes de números como os inteiros gaussianos e polinómios de uma variável. Em matemática, o algoritmo de Euclides é um método simples e eficiente de encontrar o máximo divisor comum entre dois números inteiros diferentes de zero.

Isto conduziu a noções da moderna álgebra abstrata tais como os domínios euclidianos. O algoritmo de Euclides foi ainda generalizado mais a outras estruturas matemáticas, como os nós e polinómios multivariados.

O algoritmo tem muitas aplicações teóricas e práticas. Ele pode ser usado para gerar quase todas as importantes aplicações tradicionais usados em diferentes culturas em todo o mundo. Ele é um elemento-chave dos algoritmos RSA, um método de criptografia de chave pública usado no comércio eletrônico. Ele é usado para resolver as equações de diofantina, tal como na descoberta de números que seja safistatório em múltiplas congruências (teorema chinês do resto) ou inverso multiplicativo de um número finito. Ele pode também ser usado para construir frações contínuas, em um método para o teorema de Sturm para descobrir raízes reais em um polinômio, e em vários algoritmos modernos em fatoração de inteiros. Finalmente, é uma ferramenta básica para obter na teoria dos números modernas, tal como teorema de Fermat-Lagrange e no teorema fundamental da aritmética. Diante de tudo isso que foi exposto da pra perceber que o algoritmo de Euclides é um importante resultado para matemática. Para construir a existência do mdc dada por Euclides, vamos enunciar e demontrar um lema que será essencial para o resultado.

Lema 1.3.1. *Sejam a, b, n ∈ ℤ, se existe (a,b - na), então (a,b) existe e (a,b) = (a,b - na).*

Demonstração: Seja d = (*a,b - na*), então d|*a* e d|(*a,b - na*), daí *b = b - na + na.* Logo, d é um divisor comum de *a e b.* Suponha agora que existe um *c* que seja divisor comum de *a e b.* Logo, *c* é um divisor comum de *a* e (*a,b - na*), portanto *c*|*d.* O que prova que d = (*a,b*).

A seguir vamos fazer uma aplicação e mostrar como esse lema é útil pra soluções de questões que envolvem divisão.

Exemplo 1.6: Mostre que $\frac{21n+4}{14n+3}$ é irredutível para todo $n \in \mathbb{N}$.

Para resolver o problema, basta mostrar que o mdc é 1.
Temos que $(21n + 4, 14n + 3) = (21n + 4 - 14n - 3, 14n + 3) = (7n + 1, 14n + 3) = (7n + 1, 14n + 3 - 14n - 2) = (7n + 1, 1) = 1$.
Seja $d = (21n+4, 14n+3)$, então $d \mid 21n+4$ e $d \mid 14n+3 \Rightarrow d \mid 21n+4-(14n+3) = 7n+1$, e $d \mid (21n + 4) - 3(7n + 1) = 1$, ou seja, $d \mid 1$.

Diante do exposto vamos apresentar a prova construtiva da existência do mdc dada por Euclides.

Algoritmo de Euclides

Dados *a* e *b* ∈ ℕ, supondo sem perda de generalidade que $b \leq a$. Temos que, se $b=1$ ou $b = a$, ou ainda $b \mid a$, então (*a,b*) = *a* como foi visto no exemplo 1.5. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela deivisão euclidiana podemos escrever

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b.$$

Assim, temos duas possibilidades: Ou $r_1 \mid b$ ou $r_1 \nmid b$

i Se $r_1 \mid b$, então $r_1 = (b,r_1)$ e pelo lema 1.1.2,

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

e daí o algoritmo termina.

ii Se $r_1 \nmid b$, então podemos efetuar a divisão de *b* por r_1, obtendo

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

E novamente temos duas possibilidades: Ou $r_2 \mid r_1$ ou $r_2 \nmid r_1$

iii Se $r_2 \mid r_1$, então $r_2 = (r_1,r_2)$ e pelo lema 1.1.2,

$$r_2 = (r_1,r_2) = (r_1,b - q_2r_1) = (r_1,b) = (a - q_1b,b) = (a,b)$$

e daí o algoritmo termina.

iv Se $r_2 \nmid r_1$, então podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3 \text{ , com } 0 < r_3 < r_2.$$

Continuamos esse processo até que pare. E isso sempre ocorre, pois caso contrário, teriámos uma sequência de números naturais tais que $b > r_1 > r_2 > ...$ que não possui menor elemento, contradizendo o Princípio da Boa Ordenação. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $(a,b) = r_n$.

Vamos sintetizar o algoritmo acima, realizando o metodo das divisões sucessivas. Sejam a e b dois números inteiros e efetuando a divisão obtemos $a = bq_1 + r_1$, colocando os números no seguinte diagrama

	q_1	
a	b	
r_1		

Continuando a divisão temos que b $= r_1 q_2 + r_2$, colocando os números no diagrama

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Continuando a divisão enquanto for possível, teremos

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

Ou seja, suponhamos que $r_{i+1} \mid r_i$ somente para i = n - 1. Assim obtemos a seguinte sequência

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b. \\ b &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 \text{ ,} & 0 < r_3 < r_2. \end{aligned}$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \text{ ,} \qquad 0 < r_n < r_{n-1}.$$

$$r_{n-1} = r_n q_n$$

Exemplo 1.7. Calcule o mdc de 23732 e 180.

	131	1	5	2	3
23732	180	152	28	12	4
152	28	12	4	0	

Assim, o mdc(23732,180) = 4.

Note que esse método é muito útil para números grandes. Pois caso fosse preciso fatorar o número 23732, daria um pouco mais de trabalho.
Além de ser possível escrever 4 como múltiplo de 23732 e 180. Através do algoritmo de Euclides pode-se observar que
4 = 28 - 2 × 12
12 = 152 - 5 × 28
28 = 180 - 1 × 152
152 = 23732 - 131 × 180

Donde segue que 4 = 28 - 2×12 = 28 -2×(152 - 5×28) = - 2×152 + 11×28 = -2×152 +11×(180 - 1×152) = 11×180 - 13×152 = 11×180 - 13×(23732 - 131×180) = 1714×180 - 13×23732.

Então, temos que

$$(23732,180) = 4 = (1714)\times 180 + (-13)\times 23732.$$

Note que o algoritmo de Euclides nos fornece um meio de escrever o mdc de dois números como soma de múltiplos dos dois números em questão. Ou seja, $(a,b) = ma + nb$, com $m, n \in \mathbb{Z}$. Que será de grande valia para encontrar soluções de equações diofantinas. O teorema a seguir é uma das ferramentas básicas na resolução de problemas que envolvem o mdc entre dois números. O resultado foi provado pela primeira vez por Claude-Gaspard Bachet de Méziriac (1581-1638) e mais tarde generalizado para polinômios por Étienne Bézout Bachet (1730-1783). Frequentemente, na literatura se enuncia este resultado como teorema (ou identidade) de Bézout.

Propriedade do mdc: Sejam $a,b \in \mathbb{Z}$. Definimos o conjunto

$$I(a,b) = \{xa + yb; x, y \in \mathbb{Z}\}$$

Note que se a e b não são simultaneamente nulos, então $I(a,b) \cap \mathbb{N} \neq \emptyset$. De fato, temos que $a^2 + b^2 = a \cdot a + b \cdot b \in I(a,b) \cap \mathbb{N}$

Teorema 1.3.1. *Sejam $a,b \in \mathbb{Z}$, ambos não nulos. Sed $= minI(a,b) \cap \mathbb{N}$, então*

i) d é o mdc de a e b;

ii) $I(a,b) = d\mathbb{Z}$, com $d\mathbb{Z} = \{ld; l \in \mathbb{Z}\}$.

Demonstração: (i) Suponha que exista um c tal que c divide a e b, então c divide todos os números naturais da forma xa + yb. Logo, c divide todos os elementos de I(a,b) e, isto implica que c|d.
Agora vamos mostrar que d divide todos os elementos de I(a,b). Seja p $\in$ I(a,b) e suponha por absurdo, que d $\nmid$ p. Pela divisão euclidiana, temos que p = dq + r, com 0 < r < d. Como p = xa + yb e d = ma + nb, para alguns x, y, n, m $\in \mathbb{Z}$, e como

$$\text{r = p - dq} \Rightarrow \text{r = x}a + \text{yb - (m}a + \text{nb)q} \Rightarrow \text{r = x}a + \text{yb - qm}a - \text{qnb} \Rightarrow$$
$$\text{r = (x - qm)}a + \text{(y - qn)}b \in \text{I}(a,b) \cap \mathbb{N},$$

logo absurdo , pois d= min I(a,b) $\cap \mathbb{N}$ e r < d. Em particular, d|a e d|b.
Portanto, d é o mdc de a e b.

(ii) Para mostrar a igualdade, vamos mostrar que ld $\in$ $d\mathbb{Z}$ e que $d\mathbb{Z}$ $\subset$ I(a,b). Se todo elemento de I(a,b) é divisível por d, temos que I(a,b) $\subset$ $d\mathbb{Z}$. Por outro lado, para todo ld $\in$ $d\mathbb{Z}$, temos que

$$\text{ld} = \text{l(m}a + \text{nb)} = \text{(lm)}a + \text{(ln)b} \in \text{I}(a,b)$$

Portanto, $d\mathbb{Z}$ $\subset$ I(a,b). Logo concluí - se que I(a,b) = $d\mathbb{Z}$.

Definição 1.3.2. *Dois números inteiros a e b serão chamados de primos entre si, ou coprimos, se (a,b) = 1. Ou seja, se o maior divisor comum entre a e b é 1.*

Proposição 1.3.1. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que ma + nb = 1.*

Demonstração: Dado dois números inteiros a e b primos entre si, então (a,b) = 1. Pelo teorema acima temos que existem inteiros m e n tais que ma + nb = (a,b) = 1.
Reciprocamente, suponha que existam inteiros m e n tais que ma + nb = 1, e seja d = (a,b), logo d|(ma + nb), o que implica que d|1 e portanto d = 1.

1.4 Equações Diofantinas

Vamos ultilizar a noção de mdc para resolver equações diofantinas lineares.Chama-se equação diofantina do primeiro grau a duas variáveis, a toda equação da forma aX + bY = c, onde X e Y são variáveis inteiras e a, b e c são números inteiros. Vemos, pois, que numa equação diofantina, tanto as variáveis como os coeficientes são números inteiros.
Tais equações são chamadas equações diofantias lineares em homenagem a Diofanto de Alexandria.

Proposição 1.4.1. *Sejam a, b, c $\in \mathbb{Z}$. A equação $aX + bY = c$ admite solução em números inteiros se, e somente se, (a,b)|c.*

Demonstração: Pelo teorema de *Bezout*, temos que

$$\text{I}(a,b) = \{ma + nb; m, n \in \mathbb{Z}\} = (a,b)\mathbb{Z}$$

Portanto, a equação aX + bY = c possui solução se, e somente se, c $\in$ I*(a,b)* $\Leftrightarrow$ c $\in$ I*(a,b)*$\mathbb{Z}$ $\Leftrightarrow$ I*(a,b)*|c. Basta verificar que a equação aX + bY = c, com a$\neq$0 ou b$\neq$0 e I*(a,b)*|c

Proposição 1.4.2. *Seja x_0 e y_0 uma solução particular da equação aX + bY = c, onde (a, b) = 1. Portanto as soluções x e y nos inteiros são*

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

Demonstração: Seja x e y uma solução de aX + bY = c, logo,

$$ax_0 + by_0 = ax + by = c \Rightarrow ax_0 - ax = by_0 - by = c \Rightarrow a(x_0 - x) = b(y_0 - y)$$

Como $(a, b) = 1$, então $b|(x - x_0) \Rightarrow x - x_0 = tb$, com $t \in \mathbb{Z}$.

Substituindo $x - x_0$ em $a(x_0 - x) = b(y_0 - y)$, temos que $atb = b(y_0 - y) \Rightarrow y_0 - y = ta$

Com isso, mostramos que a solução é da forma referida acima.
Por outro lado, como x, y é solução pois

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

Daí segue que a equações diofantinas da forma aX + bY = c, com $(a, b) = 1$, admite infinitas soluções nos inteiros.

A seguir através do exemplo vejamos como o estudo de equações diofantinas é importante, principalmente nos casos em que temos apenas uma equação e duas incognitas.

Exemplo 1.8: A secretaria de educação de certo município disponibilizou para uma escola 5000 reais para compra de livros de matemática e livros de português. Sabendo que o livro de matemática custa 26 reais a unidade e o livro de português custa 24 reais a unidade. Encontre todas as possibilidades possíveis para a compra desses dois livros, gastando todo o valor disponível.

Seja x o número de livros de matemática e y o número de livro de português, assim temos que

$$26x + 24y = 5000$$

Simplificando a equação por 2, obtemos a equação equivalente 13x + 12y = 2500
O (13,12) = 1, e como (13,12) = 1|2500, observamos pela proposição 1.1.7 que a equação diofantina possui solução. Vamos encontrar uma solução particular x_0 e y_0 para essa equação.
$1 = 13 \cdot (1) + 12 \cdot (-1)$, multiplicando tudo por 2500
$2500 = 13 \cdot (2500) + 12 \cdot (-2500) = 13 \cdot (12 \cdot 208 + 4) + 12 \cdot (-2500) = 13 \cdot (4) + 13 \cdot (12 \cdot 208) + 12 \cdot (-2500) = 13 \cdot (4) + (12 \cdot 2704) + 12 \cdot (-2500) = 13 \cdot (4) + (12 \cdot 204) = 2500.$
Logo, $x_0 = 4$ e $y_0 = 204$ é uma solução particular da equação, assim as soluções são

$$x = 4 + 12t \text{ e } y = 204 - 13t \text{ , com } t \in \mathbb{Z}.$$

Como procuramos soluções naturais devemos ter que x = 4 + 12t $\geqslant$ 0 $\Rightarrow$ t$\geqslant \frac{-1}{3} \Rightarrow$ t$\geqslant$0 e y = 204 - 13t $\geqslant$ 0 $\Rightarrow$ t$\leqslant$15.
Assim as soluções devem está entre 0$\leqslant$ t $\leqslant$ 15, portanto 16 possibilidades.

Apesar de ser um tópico abordado apenas no Ensino Superior ou com alunos que se preparam para as olímpiadas de matemática, nota-se por meio dos exemplos apresentados, que Equações Diofantinas Lineares pode ser um conteúdo apresentado no Ensino Básico, pois os conceitos envolvidos são plenamente acessíveis aos alunos da Educação Básica.

Capítulo 2

NÚMEROS PRIMOS E CONGRUÊNCIA MODULAR

Neste capítulo iremos apresentar um estudo sobre números primos, que é um dos conceitos mais importantes de toda a matemática, além de apresentar alguns conceitos de congruência modular e de suas propriedades, dando ferramentas necessárias aos leitores para o desenvolvimento nas soluções de problemas matemáticos tornando - os mais fáceis de se resolver, além de ser um conceito muito interessante e sofisticado que apresenta resultados significativos.

2.1 Breve histórico dos Números Primos

A descoberta dos números primos surgiu na Grécia pelo matemático Euclides de Alexandria. Mas é possível que os primeiros estudos venham da escola pitagórica por volta de 530 a.c.. que já entendia a ideia de primalidade e já estudava os números perfeito. Os números primos eram conhecidos por eles como lineares, por ser representado por pontos agrupado em linha. Já os números não-primos (compostos) poderiam ser representado por pontos formando retângulos, dando a ideia que os números lineares (primos) seriam os geradores dos outros. Outro fato importante é que os pitagóricos não consideravam o número 2 como número primo, porque para eles os números 1 e 2 não eram números verdadeiros, mas geradores de números ímpares e pares.

Os gregos antigos tinham conhecimento muito importante sobre o que envolvia os números primos. Mas, foi com o matemático de Alexandria Euclides que tomaram a forma que são encontrada nos livros didáticos.

Um dos fatores da teoria dos números primos forma: o cálculo de máximo divisor comum, a determinação dos números primos maiores que um número inteiro dado e a infinitude dos números primos.

Esse fatores são encontrados num dos trabalho mais famosos da matemática, Os Elementos de Euclides. Euclides nasceu em Alexandria por volta de 300 a.C.. e sua obra Os Elementos é composta por 13 livros e são os livros VII, VIII e IX que se encontra questões com teoria dos números.

No livro VII encontra definições dos números primos, como "protós arithmós estin monadi mone metroymenos"que significa números primos são tudo aquilo que só pode ser

medido através da unidade. Ainda nesse livro se encontra uns dos principais teoremas, hoje conhecido como "Algoritmo de Euclides"(método para achar o máximo divisor comum entre dois números).
O livro VIII fala das propriedade das progressões geométricas, já o livro IX tem muitos teoremas interessantes, desses, o mais famoso é a proposição 20:
"Números primos são mais do que qualquer quantidade fixada de números primos." Em outras palavras existem infinitos números primos.

> Isto é, Euclides dá aqui a prova elementar bem conhecida do fato de que há infinitos números primos. Segundo BOYER (P.79) "A prova é direta, pois mostra a hipótese de haver somente um número finito de primos leva a uma contradição".[1]

Outro grego que trabalhou com os números primos foi Erastóstenes de Alexandria no século III a.c. ele foi o primeiro a criar a tabela de números primos: O Crivo de Erastóstenes.

O motivo deste nome é que seu método de montar uma tabela com os números de 2 até N, onde N era um número natural qualquer. Como o 2 era um número primo, o número 1 não satisfazia as definições de primos. Porque, tinha-se em mente que todos os múltiplos de 2 excerto o próprio 2, eram crivados na tabela e o próximo seria o três, logo todos os múltiplos de três era crivados, com exceção do próprio 3. que é primo. O próximo era o 5, que também é primo. Fazendo a tabela nessa sequência, todos os números composto eram "crivados", sobrando só os números finitos até o N.

Na Europa o francês Pierre de Fermat que depois de ler o texto de Diofanto, (esse texto foi traduzido do grego para o latim que era a língua estudado por muitos intelectuais da época), o despertou para o aprofundamento de muitos resultados matemáticos, levou a se tornar o fundador da matemática moderna na teorias dos números. BOYER (p258).

Embora sua teorias tenham sido provadas como falsas, com afirmação que todos os números da forma$[2^(2^n)] + 1$ seriam primos, o que ficou conhecido como número de Fermat.
Hoje essas teorias foram tão exploradas que os matemáticos acreditam que só existem quatro números de Fermat que são primos, 0, 1, 2, 3, 4. Outro estudo de Fermat foi o que hoje conhecemos como "pequeno teorema de Fermat", que mostrou-se verdeiro ao demostrar que diz que se p é primo e a e p são primos entre se (dois números são primos entre se quando um único divisor comum entre se for 1) então $a^(p-1) - 1$é divisível por p.

Foi Leonhard Euler(1007-1783) que provou que o teorema era verdadeiro, e a parte dele, percebeu um teorema mais geral, mas apesar de suas contribuições para o estudo da teoria dos números, Euler não publicou nenhum tratado sobre esse assunto, divulgou seu resultado só por cartas e artigos.

Outro matemático que contribui no estudos dos números primos foi Carl Friedrich Gauss (1777-1855), que no início da sua carreira matemática, estabeleceu a conjectura sobre a distribuição dos números primos, que tornou-se posteriormente conhecido como "TEOREMA DOS NÚMEROS PRIMOS". Foi ele que deu um formato definitivo á teoria dos números, a parte de sua obra Disquisitiones Arithmeticae, publicada em 1801.

Antes de seu tratado, a teoria dos números era um conjunto isolado de teoria e conjecturas. Gauss organizou o trabalho dos seus antecessores, preencheu lacunas, corrigiu demonstrações, incluiu ideias extremamente inovadoras e deu uma estrutura sistemática

para a teoria dos números e é considerado por muitos historiadores como o fundador da moderna teoria dos números.

Segundo [BOYER, 1996], durante parte da história, grandes matemáticos como Euclides, Erastóstenes, Pierre de Fermat, Leonhard Euler, Carl Friedrich Gauss e Georg Friedrich Bernhard Riemann(1826-1866), entre outros desenvolveram pesquisas envolvendo teorias dos números, particularmente os números primos. E seus trabalhos acabaram por estruturar esse ramo da matemática e por influenciar várias outras áreas como por exemplo na matemática computacional.

Os números primos ainda serão um objeto de trabalho por muito matemáticos ao redor do mundo. Nos dias atuais são citados números primos com até 17 milhões de dígitos.

2.2 Teorema Fundamental da Aritmética

Nesta seção iremos apresentar e demonstrar mais um grande resultado da matemática que é o Teorema Fundamental da Aritmética. Antes vamos definir alguns conceitos.

Definição 2.2.1. *Chamaremos de número primo todo número natural maior que 1 que só possui como divisores 1 e ele próprio.*

Daí decorre o seguinte fato: Dado dois números primos p e q e um número inteiro a temos que:

i) Se p|q, então p = q. De fato, como p|q se q é primo, então p = 1 ou p = q. Sendo p primo, tem - se que p > 1 $\Rightarrow$ p = q.

ii) Se p$\nmid a$, então (p,a) = 1.
De fato, se (p,a) = d, temos que d|p e d|a. Portanto, d = p ou d = 1. Mas d$\neq$ p, pois p$nmida$, emtão d = 1.

Se um número é maior que 1 e não é primo, ele será chamado de *composto*.
Se n > 1 é composto, então exite um divisor natural n_1 de n tal que $1 < n_1 <$ n. Logo, existe um $n_2 \in \mathbb{N}$ tal que n = $n_1 n_2$, com $1 < n_1 <$ n e $1 < n_2 <$ n.

Exemplo 2.1. Os números 2, 3, 5, 7, 11, 13, 17 são primos, enquanto que os números 4, 6, 8, 9, 10, 12, 14, 15 são compostos.

Definição 2.2.2. *Seja p > 1, se p divide o produto de dois números naturais quaisquer, então p divide um dos fatores.*

Em outras palavras, sejam a, b, p $\in \mathbb{Z}$, com p primo. Se p|ab, então p|a ou p|b.
Antes de demonstrar o resultado vamos enunciar e demonstrar o seguinte lema.

Lema 2.2.1. *Sejam a, b e c números inteiros. Se a|bc e (a,b) = 1, então a | c.*

Demonstração: De fato, pois se a|bc, então $\exists$ r $\in \mathbb{Z}$, tal que bc = ar.
Se (a, b) = 1, então pela proposição 1.1.6, temos que existem m, n $\in \mathbb{Z}$ tais que

$$\text{m}a + \text{nb} = 1$$
Multiplicando ambos os lados da igualdade, temos
$$\text{c} = \text{m}a\text{c} + \text{nbc}$$
Substituindo bc por ar, obtemos
$$\text{c} = \text{m}a\text{c} + \text{nar} = a(\text{mc} + \text{nr})$$

e, portanto $a|$c.

Agora para mostra que: Se p|ab, então p|a ou p|b, basta provar que, se p $\nmid$ a, então p|b. Mas, se p|a, temos que (p, a) = 1 e pelo lema acima o resultado segue.

Corolário 2.2.1. *Se p,p_1,...,p_n são números primos e, se p|* $p_1 \cdots p_n$ *, então p = p_i para algum i = 1,...,n.*

Demonstração: Usando a definição acima e aplicando indução sobre n e o fato de que se p| p_i, então p = p_i.

Teorema 2.2.1 (Teorema Fundamental da Aritmética)**.** *Todo número natura maior que 1 ou é primo ou se escreve de modo único como um produto de números primos.*

Demonstração: Usaremos o segunda forma do princípio da indução. Se n = 2, e como 2 é primo o resultado é verificado.

Agora suponha que o resultado é válido para todo número natural menor do que n e mostraremos que vale para n. Temos então dois casos ou n é primo ou n é composto. (i) Se n é primo, nada a demonstrar. (ii) Se n é composto, então existem n_1 e n_2 naturais tais que n = $n_1 n_2$, como $1 < n_1 <$ n e $1 < n_2 <$ n. Pela hipótese de indução, temos que existem números primos $p_1...p_r$ e $q_1...q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, n = $p_1 \cdots p_r q_1 \cdots q_s$.

Agora, vamos mostrar que se escreve de forma única. Suponha que tenhamos n = $p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_1 e os q_j são números primos. Como $p_1 \mid q_1 \cdots q_s$ e pelo corolário acima temos que $p_1 = q_j$ para algum j, e reordenado os $q_1 \cdots q_s$, podemos supor que seja q_1. Logo, $p_2 \cdots p_r = q_2 \cdots q_s$ e como $p_2 \cdots p_r <$ n, a hipótese de indução aarreta que r = s e os p_i e q_j são iguais dois a dois.

Exemplo 2.2. Decomponha em fatores primos o número 60.
$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$

Vamos denotar por d(n) o número de divisores positivos do número natural n, ou seja, decompondo n em fatores primos obtemos n = $p_1^{\alpha 1} \cdots p_r^{\alpha r}$, onde $p_1, ..., p_r$ são números primos e $\alpha_1 \cdots \alpha_r \in \mathbb{N}$ então

$$\text{d(n)} = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

Assim essa escrita nos mostra que um número natural n = $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ possui uma quantidade ímpar de divisores positivos se, e somente se, cada α_i é par, ou seja, se e somente se, n é uma quadrado perfeito.

Exemplo 2.3. Mostre que se ab é um quadrado perfeito, então a e b são quadrados perfeitos.

Demonstração: Se ab é um quadrado perfeito, então ab $= X^2$ onde $X = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$ e ab $= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, onde α_i é par.
Logo,

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n} = (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n})^2 = p_1^{2\beta_1} \cdot p_2^{2\beta_2} \cdots p_n^{2\beta_n}, \text{ isto implica que}$$
$$\alpha_1 = 2\beta_1,\ \alpha_2 = 2\beta_2, \cdots, \alpha_n = 2\beta_n$$

e como (a,b) = 1, então não existem divisores comum de a e b.
Assim ,

$$a = \prod_{i=1}^{n} p_i^{\alpha_i} \text{ e b} = \prod_{j=1}^{n} p_j^{\alpha_j} \text{ , com i,j} = \{1, 2, ..., n\} \text{ e } i \neq j.$$

$$\text{Ou seja, } a = \prod_{i=1}^{n} p_i^{2\beta_i} \text{ e b} = \prod_{j=1}^{n} p_j^{2\beta_j},$$

isto é a e b são quadrados perfeitos.

Este exemplo pode ser generalizado para a r-ésima potência, o qual deixamos a generalização a cargo do leitor, pois é feita de forma análoga.

2.3 Decomposição do Fatorial em Primos

Antes de iniciar, denotaremos por $[\frac{a}{b}]$ o quociente da divisão de a por b, que é o maior inteiro menor ou igual do que o número racional $\frac{a}{b}$. O qual será chamada de parte inteira do número racional.
Além disso, denotaremos por $E_p(n)$ o expoente da maior potência de p que divide n, com p primo. Ou seja, o expoente da potência de p que aparece na fatoração de n em fatores primos.
Em particular, $E_p(n!)$ representara a maior potência de p que aparece na fatoração de n! em fatores primos.

Nesta seção iremos aprender a fatorar em números primos o número n!, onde n é um número natural arbitrário. Assim nota-se que se a e b são maiores que zero, então $[\frac{a}{b}] > 0$.

Proposição 2.3.1. *Sejam a, b e c* $\in \mathbb{N}$. *Temos que*

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

Demonstração: Sejam

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

Logo,

$$a = \text{b}q_1 + r_1, \quad \text{com } 0 \leq r_1 \leq \text{b -1}$$

e

$$\left[\frac{a}{b}\right] = q_1 = \text{c}q_2 + r_2, \quad \text{com } 0 \leq r_2 \leq \text{c -1}.$$

Portanto,

$$a = \text{b}q_1 + r_1 = \text{b}(\text{c}q_2 + r_2) + r_1 = bcq_2 + br_2 + r_1$$

Como

$$0 \leq br_2 + r_1 \leq b(c-1) + b - 1 = \text{bc - 1},$$

Segue-se que q_2 é o quociente da divisão de a por bc, ou seja

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

Assim, o resultado acima mostra que o quociente da divisão de a por b por c é igual ao quociente da divisão de a por b vezes c. A seguir, temos um resultado que vai nós mostrar como decompor um número fatorial em fatores primos. Algo fantástico não acham? Pois indago a seguinte pergunta aos leitores como vocês fariam a decomposição em fatores primos de um número fatorial grande? O teorema de Legendre será uma importante ferramente para facilitar esse cálculo.

Teorema 2.3.1 (Legendre)**.** *Sejam n um número natural e p um número primo. Então,*

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

Demonstração: Inicialmente, note que a soma acima aparentemente infinita, é sempre finita, pois a partir de uma certa potência i de p, $p^i > n$, e todas as pontências maiores de p também serão maiores que n, portanto $\left[\frac{n}{p^i}\right] = 0$, se i $\geq$ m. Vamos usar a indução sobre n para mostar o resultado.
(i) Para n = 1 é fácil ver. (ii) Suponha que o resultado vale para algum m natural com m $<$ n. Sabemos que os múltiplos de p entre 1 e n são

$$\text{p, 2p, ... , } \left[\frac{n}{p}\right] p$$

Portanto,

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

Pela hipótese de indução, temos que

$$E_p\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p_2}\right] + \left[\frac{\left[\frac{n}{p}\right]}{p_3}\right] + ...$$

E pela proposição 2.1.1 acima, o resultado decorre.

Note que, na prática é fácil calcular $E_p(n!)$, usando o algoritmo abaixo temos que:

$$\begin{gathered} n = pq_1 + r_1 \\ q_1 = pq_2 + r_2 \\ q_2 = pq_3 + r_3 \\ \cdots \\ q_{s-1} = pq_s + r_s \\ \cdots \end{gathered}$$

Como $q_1 > q_2 > \cdots$, segue - se que, para algum s, tem-se que $q_s < p$. Portanto, temos

$$E_p(n!) = q_1 + q_2 + \cdots + q_s$$

Exemplo 2.4. Determine a decomposição de 20! em fatores primos e descubra com quantos zeros termina a representação decimal desse número.

Para resolver o problema devemos achar $E_p(20!)$ para todo primo $p \leq 10$.
Sendo que

$$E_2(20!) = \left[\frac{20}{2}\right] + \left[\frac{20}{2^2}\right] + \left[\frac{20}{2^3}\right] + \left[\frac{20}{2^4}\right] = 10 + 5 + 2 + 1 = 18$$

$$E_3(20!) = \left[\frac{20}{3}\right] + \left[\frac{20}{3^2}\right] = 6 + 2 = 8$$

$$E_5(20!) = \left[\frac{20}{5}\right] = 4, \quad E_7(20!) = \left[\frac{20}{7}\right] = 2, \quad E_{11}(20!) = \left[\frac{20}{11}\right] = 1$$

$$E_{13}(20!) = \left[\frac{20}{13}\right] = 1 \quad E_{17}(20!) = \left[\frac{20}{17}\right] = 1, \quad E_{19}(20!) = \left[\frac{20}{19}\right] = 1.$$

Segue-se que 20! em fatores primos será

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

Consequentemente, existem dezoito fatores iguais a 2 e quatro fatores iguas a 5 na decomposição de 20! em fatores primos, vê-se, imediatamente, que 20! termina com 4 zeros. Pois os zeros são formados pelos fatores 2 e 5.

Exemplo 2.5. É possível repartir exatamente $\binom{2357}{528}$ objetos entre 49 pessoas?

Sabemos que $\binom{2357}{528} = \dfrac{2357!}{528!\,1829!}$

Agora vamos encontrar $E_7\left(\binom{2357}{528}\right)$ = $E_7(2357!)$ - $E_7(538!)$ - $E_7(1829!)$.

$$E_7(2357!) = \left[\frac{2357}{7}\right] + \left[\frac{2357}{49}\right] + \left[\frac{2357}{343}\right] = 336 + 48 + 6 = 390$$

$$E_7(528!) = \left[\frac{528}{7}\right] + \left[\frac{528}{49}\right] + \left[\frac{528}{343}\right] = 75 + 10 + 1 = 86$$

$$E_7(1829!) = \left[\frac{1829}{7}\right] + \left[\frac{1829}{49}\right] + \left[\frac{1829}{343}\right] = 261 + 37 + 5 = 303$$

Logo, $E_7\left(\binom{2357}{528}\right)$= 390 - 86 - 303 = 1, e como $49 = 7^2$ não divide 1. Assim $\binom{2357}{528}$ não é múltliplo de 49.

2.4 Congruência

Em Teoria dos Números, algo que ajuda muito na hora de resolver problemas é a famosa "aritmética modular", que é equivalente à análise de restos. Você irá ver aqui o básico sobre aritmética modular e relações de congruência. Estas noções de Teoria dos Números foram introduzidas por Gauss no livro *Disquisitiones Arithmeticae*, de 1801.

Definição 2.4.1. *Dado um número natural m. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais.*

Quando dois números inteiros são congruentes escreve - se

$$a \equiv \text{b mod m.}$$

Exemplo 2.6. Mostre que $27 \equiv 19$ mod 2.

De fato são, pois o resto da divisão de 27 por 2 é 1, e o resto da divisão de 19 por 2 também é 1. Logo como eles possuem o mesmo resto na divisão por 2, dizemos que são congruentes módulo 2.
Quando a relação é falsa, dizemos que são incogruentes, módulo m e denotamos por

Proposição 2.4.1. *Seja m$\in \mathbb{N}$. Para todos a, b e $\in \mathbb{Z}$, tem - se que*
(i) $a \equiv a$ mod m.
(ii) Se $a \equiv b$ mod m, então $b \equiv a$ mod m.
(iii) Se $a \equiv b$ mod m e $b \equiv c$ mod m, então $a \equiv c$ mod m

Demonstração:
Para verificar a congruência entre dois números, basta aplicar o seguinte resultado.

Proposição 2.4.2. *Suponha que a, b e m $\in \mathbb{Z}$, com m > 1. Tem - se que $a \equiv b$ mod m se, e somente se, m$|a$ - b.*

Demonstração: Dividindo a por m e b por m, temos que a = mq + r, com $0 \leq r \leq m$ e b = mq' + r' , com $0 \leq r' \leq m$. Logo:
Se r = r'

a - b = mq + r - (mq' + r') = m(q - q') + (r - r'), como r = r' por hipótese então
a - b = m(q - q') + 0 $\Rightarrow$ a - b = m(q - q')
Logo, m| a - b

Reciprocamente, a - b = m(q - q') + (r - r'), por hipótese temos que a - b é divisível por m e m(q - q') é divisível por m, pois é multiplo de m, então r - r' é divisível por m, mas - m < r - r' < m, então r - r' = 0 $\Rightarrow$ r = r'. Assim a e b deixam o mesmo resto quando divisível por m.

Proposição 2.4.3. *Sejam a, b, c, d, e m* $\in \mathbb{Z}$*, com m > 1.*
(i) Se a $\equiv$ *b mod m e c* $\equiv$ *d mod m, então a + c* $\equiv$ *b + d mod m.*
(ii) Se a $\equiv$ *b mod m e c* $\equiv$ *b mod m, então ac* $\equiv$ *bd mod m.*

Demonstração: Suponhamos que $a \equiv$ b mod m e c $\equiv$ d mod m, logo pela proposição 2.1.2, temos que m| b - a e m| d - c.
(i) Como $a \equiv$ b mod m e c $\equiv$ d mod m, temos que m| b - a e m| d - c então m| (b - a) + (d - c) $\Rightarrow$ m|(b + d) - (a + c) $\Rightarrow$ $(a + c) \equiv (b + d)$ mod m.
(ii) Note que, bd - ac = bd - da + da - ac = d(b - a) + a(d - c), mas m| b - a e m| d - c, logo m| d(b - a) e m|a(d - c) $\Rightarrow$ m|d(b - a) + a(d - c) $\Rightarrow$ m| bd - ac. Ou seja, $ac \equiv$ bd mod m.

Corolário 2.4.1. *Para todo n* $\in \mathbb{N}$*, a, b* $\in \mathbb{Z}$*, se a* $\equiv$ *b mod m, então tem - se que* $a^n \equiv b^n$ *mod m.*

Demonstração: Vamos ultilizar indução sobre n.

$a \equiv$ b mod m, então
$a \cdot a \equiv$ b $\cdot$ b mod m $\Rightarrow$ $a^2 \equiv b^2$ mod m
$a \cdot a^2 \equiv b \cdot b^2 mod m \Rightarrow a^3 \equiv b^3$ mod m
$\vdots$
Se $a^k \equiv b^k$ mod m, por hipótese de indução

Então, $a^{k+1} = a^k \cdot a \equiv b^k \cdot b = b^{k+1}$ mod m.

Exemplo: Calcule o resto da divisão de 4^{100} por 3.

Note que $4 \equiv 1$ mod 3, e aplicando o corolário acima, elevando ambos os membros a 100, temos $4^{100} \equiv 1^{100} = 1$ mod 3.
Assim, 4^{100} deixa resto 1, quando dividido por 3.

2.5 Pequeno Teorema de Fermat

Há exatos 377 anos, Pierre de Fermat anunciou em carta ao colega matemático Bernard Frenicle de Bessey que tinha criado um *pequeno teorema de Fermat*, capaz verificar se um número é ou não primo.

Apesar da grande importância, a primeira demonstração do chamado "pequeno teorema de Fermat" levou quase cem anos para ser divulgada. Foi publicada apenas em 1736, pelo grande Leonhard Euler.

Fermat não era nada vaidoso em relação a suas descobertas, a ponto de nunca tê-las publicado. Apenas fazia referências a elas nas trocas de cartas com amigos. Apesar de ter criado a Geometria Analítica (1629) e dado importantes contribuições à Matemática, tinha a disciplina como um hobby.

Jurista e magistrado por profissão, dedicava-se à Matemática nas horas de lazer. Em razão disso, é considerado o "Príncipe dos Amadores". Apesar desse amadorismo, era tido por Blaise Pascal o maior matemático de seu tempo.

Seu último teorema foi solucionado 357 anos após sua proposição. Coube ao inglês Andrew Wiles, professor da Universidade de Oxford, resolver uma das charadas mais difíceis da história da álgebra. Agora iremos enunciar e demonstrar o pequeno teorema de Fermat.

Teorema 2.5.1 (Pequeno Teorema de Fermat)**.** *Seja p é um número primo. Se $p \nmid a$, então $a^{p-1} \equiv 1 \ mod \ p$*

Demonstração: Sabemos que o conjunto formado pelos p números 0, 1, 2,$\cdots$, p - 1 constitui um sistema de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjuto $\{0, 1, 2, \ldots, p-1\}$. Seja B = $\{a, 2a, ...(p-1)a\}$ o conjunto de todos os restos não nulos. Vamos mostrar que cada npumero quando divisível por p, deixa resto diferente de 0 e diferentes entre si.
De fato, o mdc(a, p) = 1, pois p é primo e o mdc(k, p) = 1, $\forall k \leq p-1$ então mdc(ka, p) = 1, logo deixam resto não nulo. Suponha que ka $\equiv$ la (mod p), "dividindo ambos os membros por a", temos que k $\equiv$ a (mod p), logo k = l.
Assim,

$$a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \text{ (mod p)} \Rightarrow$$
$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \text{ (mod p), dividindo ambos os membros por (p-1)!}$$
$$a^{p-1} \equiv 1 \text{ (mod p).}$$

Usamos a demonstração feita por [5].

Exemplo: Qual o resto da divisão de 2^{257} por 7.

Note que $257 = 6 \cdot 42 + 5$, logo $2^{257} = 2^{6 \cdot 42+5} = (2^6)^{42} \cdot 2^5$
Por Fermat, $a^{p-1} \equiv 1$ mod p, então $2^6 \equiv 1 \text{ mod } 7 \Rightarrow (2^6)^{42} \equiv 1^{42} \text{ mod } 7 \Rightarrow 2^{252} \equiv 1 \text{ mod } 7 \Rightarrow 2^{252} \cdot 2^5 \equiv 1 \cdot 2^5 \text{ mod } 7 \Rightarrow 2^{257} \equiv 32 = 4 \text{ mod } 7$, ou seja $2^{257} \equiv 4 \text{ mod } 7$.
Portanto o resto da divição de 2^{257} por 7 é 4.

Corolário 2.5.1. *Se p é um número primo e se a é um número inteiro positivo, então $a^p \equiv a(mod p)$.*

Demontração: Vamos analisar doi casos, se $p \mid a$ e se $p \nmid a$. Se $p \mid a$, então $p \mid (a(a^{p-1} - 1))$ e, portanto $a^p \equiv a(mod p)$. Por outro lado, se $p \nmid a$, pelo teorema de Fermat $p \mid (a^{p-1} - 1)$ e, portanto, $p \mid (a^p - a)$. Logo, em ambos os casos, $a^p \equiv a(mod p)$.

Gostariamos de indicar ao leitor a ver também um importante resultado para o estudo de teoria dos números, que é a generalização do Pequeno Teorema de Fermat. O autor da

primeira demonstração do Pequeno Teorema de Fermat, também foi o autor da primeira e mais conhecida generalização, a qual é também usualmente referida como Teorema de Euler e neste resultado você irá conhecer a função de Euler.

Capítulo 3

APLICAÇÃO DA TEORIA DOS NÚMEROS EM SALA

Diante das dificuldades relacionadas à aprendizagem de conceitos matemáticos, no cotidiano dos alunos, levando - os a se desmotivarem, o professor precisa investir na busca de novas formas de aprimorar as atividades de ensino. Nessa direção, os recursos de ensino constituídos por novas técnicas, como a *Teoria dos Números*, precisam ser implementadas no cotidiano do aluno. Esta seção apresenta uma proposta de sequências didática de atividades para evolução do aluno, sequência essa de autoria própria, abordando conteúdos matemáticos de Teoria dos Números e relacionando - os com conteúdos estudados na vida escolar do aluno. Além de uma comparação do desempenho do aluno antes e depois de estudar Teoria dos Números.
Assim, as atividades aqui propostas buscam ser motivadoras e levam à construção de um novo conhecimento para o aluno, que para desenvolvê-las precisaram dedicar um tempo maior para estudo de matemática, tempo este que os ajudará, a obterem um melhor desempenho ao prestar vestibulares e concursos.
A aplicação da pesquisa foi desenvolvida em algumas Escolas do Município de Arapiraca com alunos do ensino médio do turno matutino e entre professores do ensino básico. Os professores foram ouvidos através de questionários, buscando através das perguntas uma troca de experiências com professores que lecionam matemática no ensino básico. A pesquisa foi realizada com cerca 70 jovens e com cerca de 20 professores de matemática de diferentes instituições. Foram realizadas três etapas previamente definidas de atividades, "as quais serão descritas a seguir"para chegarmos às primeiras conclusões dessa aplicação de teoria dos números no ensino básico.

O primeiro momento foi aplicado um questionário para professores de matemática em diferentes escolas, perguntando acerca da pesquisa além de outras questões consideradas importantes para o desenvolvimento do trabalho. O questionário encontra - se no anexo.

Num segundo momento, foi aplicado um teste com algumas questões de vestibulares inclusive do ENEM, tomando como padrão questões de vestibulares de Universidades conceituadas no Brasil. O motivo de ter escolhido questões de vestibulares, está no fato de ser uma prova em que a maioria dos alunos do ensino básico precisaram prestar, pois é a porta de entrada para muitas Universidades. As questões escolhidas para o teste foram

aquelas em que aparecem aplicações de teoria dos números. Após a aplicação das questões foi feita uma coleta de informações sobre o teste.
Este teste de sondagem foi realizado para verificar o conhecimento matemático a cerca das questões, o tempo gasto por eles para se resolver as questões, qual era o nível de dificuldade do teste para eles, qual a estratégia usada pelos alunos para resolverem as questões e até que ponto eles eram interessados em resolver aquelas questões e estudar matemática. Considero que analisar o grau de conhecimento matemático dos alunos é importante, pois muitas vezes a matemática torna - se desmotivadora, devido as dificuldades relacionadas à aprendizagem de conceitos matemáticos, que acabam daí desmotivando o aluno. É aí que o professor precisa investir na busca de novas formas de aprimorar as atividades de ensino e como implementar uma nova forma de aprendizagem para o aluno, aplicando conceitos novos e novas formas de resoluções.
Nessa direção, as ideias construídas nesse trabalho tem o objetivo de mostrar aos professores, alunos e em particular os leitores dessa dissertação o quanto o conhecimento dos alunos em Teoria dos Números é importante. Pois além de ser conceitos extremamente relevantes para a resoluções de problemas matemáticos, irá diminuir o tempo de resolução em alguns problemas encontrados nos vestibulares.

No terceiro momento foi trabalhado durante duas semanas, uma oficina dos números, ou seja, uma breve explanação de teoria dos números com alguns conceitos, exemplos e exercícios importantes para aprimorar a solução de problemas. Ao final da quinzena, no último dia da oficina, foi reaplicado um teste semelhante ao primeiro, mudando apenas algumas coisas. O resultado foi acima do esperado e pôde-se observar que: O conhecimento matemático, as estratégias usadas, o interesse em responder o teste, a quantidade de acertos, o tempo de resolução e a empolgação aumentaram de maneira bastante positiva. Mostrando que em apenas 15 dias de trabalho, muita coisa mudou e em particular os alunos evoluíram mostrando que essa intervenção foi importantíssima para o desempenho e crescimento matemático do aluno.
A seguir será explicado com detalhes cada fase do processo e seus resultados.

3.1 Pré Teste

Como já exposto anteriormente, foram aplicados três testes para quantificar e qualificar o impacto do ensino de *Teoria dos Números* na interpretação e resolução de problemas. Antes de ir até a sala de aula desenvolver a pesquisa com os alunos, foi feito um questionário para os professores e entregue a eles durante o intervalo das aulas para que os mesmo respondessem a cerca do tema, buscando uma troca de experiências e informações. O primeiro teste teve o objetivo de ouvir e coletar ideias dos professores que lecionam matemática no ensino básico.
Os dados foram coletados e expostos nos gráficos como mostra a tabela abaixo.

Perguntas	Sim	Não
Considera que o tempo para resolver questões de matemática em vestibulares é pouco?	90%	10%
Considera que administrar o tempo para responder questões de matemática em vestibulares é importante?	100%	0%
Você é a favor dos alunos aprenderem noções de teoria dos números no ensino básico?	85%	15%
Você está disposto a ajudar seu aluno a diminuir o tempo para solução de problemas ?	100%	0%

Assinale cada uma das seguintes frases, de acordo com o seu grau de acordo/desacordo, numa escala entre 1 (discordo em absoluto) e 5 (concordo totalmente).

Perguntas	1	2	3	4	5
Gosto de ensinar Matemática.	0%	0%	5%	5%	90%
Alguns conteúdos de matemática são desnecessários no ensino básico.	0%	0%	5%	0%	95%
Conheço bem os temas a desenvolver.	20%	15%	5%	0%	60%
Os meus alunos gostam de Matemática.	80%	10%	10%	0%	0%
A Matemática é uma disciplina independente das outras.	60%	8%	20%	0%	12%
Você considera o sucesso do seus alunos importante.	0%	10%	0%	0%	90%
Você é a favor de mudanças em temas da matemática do ensino básico.	0%	0%	5%	0%	95%

Assim diante do exposto é possível observar e tirar algumas conclusões importantes a respeito do tema, nota - se que 100% dos professores consideram que o tempo para resolver questões em vestibulares é importante e se mostram dispostos a ajudar os alunos a melhorarem seu desempenho, pois torcem pelo sucesso de seus alunos. Observa - se também que mais de 85% dos professores são a favor do ensino de teoria dos números no ensino básico e uma quantidade ainda maior optam por desnecessários alguns tópicos matemáticos ensinados no ensino básico. Que aproveito a ocasião e sugiro uma análise na possibilidade de haver algumas mudanças na Base Comum Currícular-BNCC em relação a esses temas por teoria dos números, que acredito ser de um aproveitamento melhor para o cotidiano do aluno.

Essas conclusões considero muito relevantes, pois são informações dadas por professores que estão em contato direto com o aluno, ou seja, em sala de aula diariamente. E não apenas por teóricos, que apesar de ter uma capacidade intelectual incontestável, muitas vezes não ministram aulas e nem estão em sala de aula diariamente vivenciando o dia a dia escolar.

O segundo momento foi aplicado questões para os alunos com propósito de verificar o conhecimento prévio dos alunos acerca do tema, o tempo gasto para solução dos problemas, entre outros. Neste momento, foi proposto um questionário como questões de vestibulares para que cada um resolver - se 5 questões em tempo total de 30 minutos, ficando em média 6 minutos para solução de cada questão, tempo que considero suficiente pois em vestibulares o tempo médio por questão é de 2 minutos. Ressaltamos que todos os alunos resolveram as mesmas 5 questões para que assim pudéssemos comparar a

relação entre erros e acertos, e o modo como buscavam solucionar os problemas. Tomaremos como acerto o fato do aluno ter encontrado pelo menos uma solução que satisfaz o problema. Como atividade inicial foi feita a leitura em voz alta das questões e os alunos foram orientados a resolver os problemas da maneira que achassem melhor. Inicialmente já dava pra observar que os estudantes de posse das informações propostas nos problemas, apresentaram muitas dúvidas a respeito da interpretação das questões.
O gráfico a seguir discrimina o resultado quantitativo (acertos, erros e brancos) por questão do questionário avaliativo.
Lembrando que os alunos responderam todas as questões, e aquelas que eles não sabia responder foi permitido a eles chutarem ou deixarem em branco, ficando a critério de cada aluno.

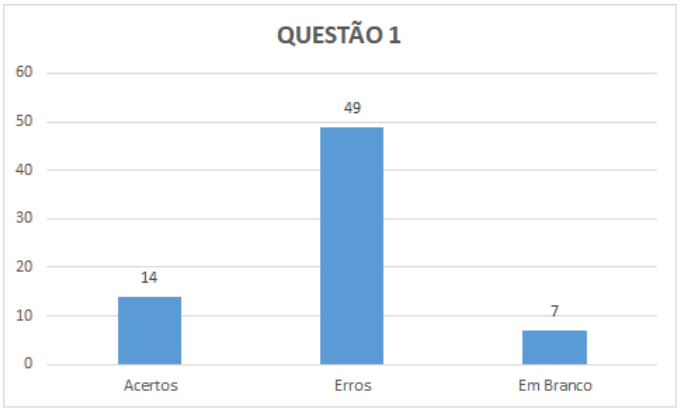

Figura 3.1: O maior número x tal que $\frac{60!}{7^x}$ seja um número natural é:

Na questão 1 tivemos um total de 20% de acertos, 70% de erros e 10% deixaram em branco.

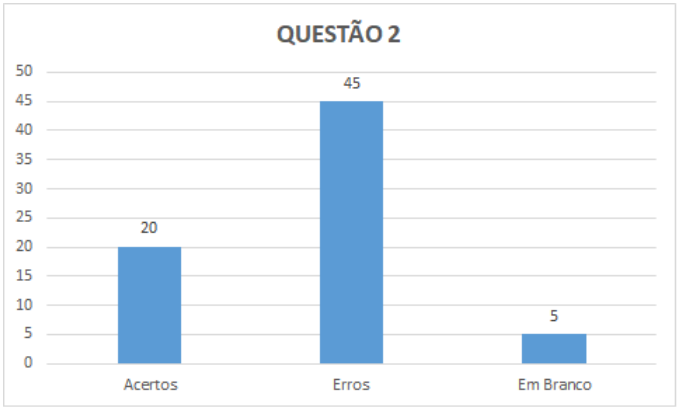

Figura 3.2: Se $4^{16} \cdot 5^{25} = \alpha \cdot 10^n$, com $1 \leq \alpha \leq 9$, então n é:

Na questão 2 tivemos 29% de acertos, 64% de erros e 4% deixaram em branco.

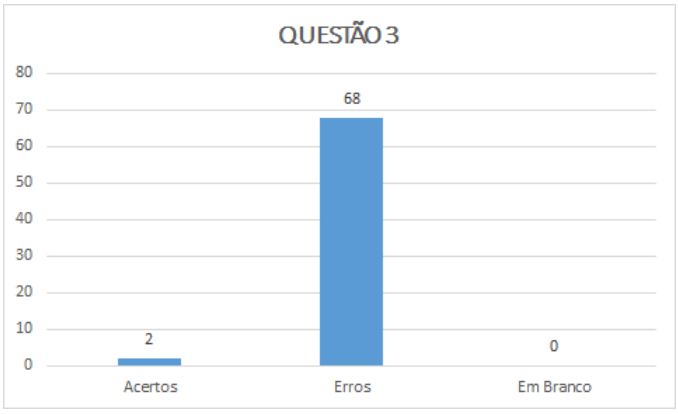

Figura 3.3: Em um estacionamento existem carros e motos num total de 84 rodas quantos carros podem existir neste estacionamento, sabendo que existe no mínimo 30 veículos:

Na questão 3 tivemos apenas 3% de acertos, e consequentemente 97% de erros, e não houve nenhuma questão em branco. Vale ressaltar que essa foi a questão que os alunos mais erraram.

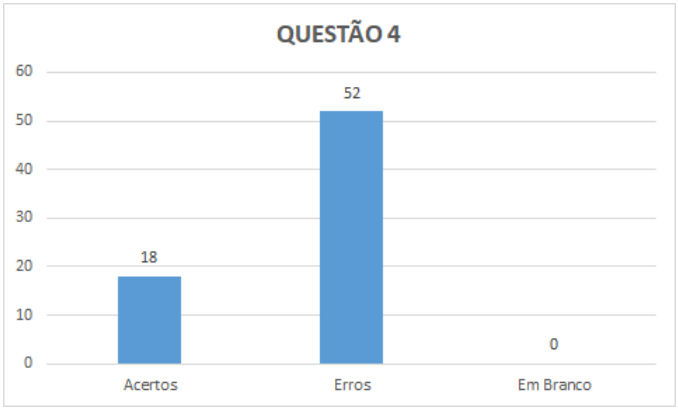

Figura 3.4: Um número dividido por 5 deixa resto 4, e dividido por 7 deixa resto 3. Qual o resto da divisão desse número por 35?

Na quarta questão foi obtido 25% de acertos, 75% de erros e ninguém deixou a questão em branco.

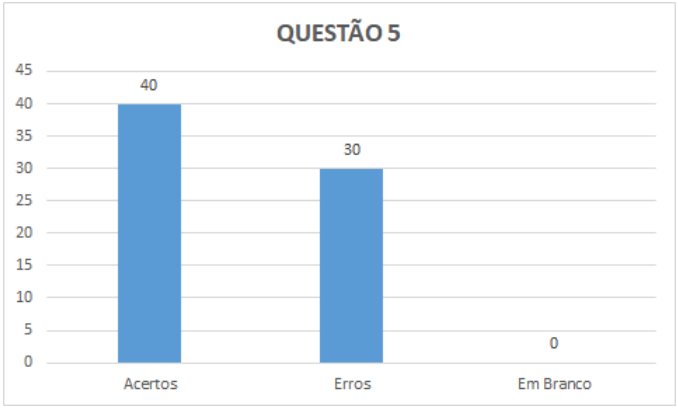

Figura 3.5: Suponha que João tenha perdido seus documentos, inclusive o cartão de CPF e, ao dar queixa da perda na delegacia, não conseguisse lembrar quais eram os dígitos verificadores, recordando-se apenas que os nove primeiros algarismos eram 123.456.789. Neste caso, os dígitos verificadores d1 e d2 esquecidos são, respectivamente:

Por fim na quinta questão obtivemos 58% de acertos, 42% de erros e nenhuma questão deixada em branco. De fato essa foi a questão que obtivemos o maior percentual de acertos.

Após isso, foi entregue aos alunos outro questionário, agora de sondagem para saber a opinião dos alunos a respeito de alguns pontos que considero importante para a discursão do trabalho. Este questionário se encontra no anexo, mais iremos mostrar através de gráficos as opiniões dos alunos a respeito das perguntas feitas.

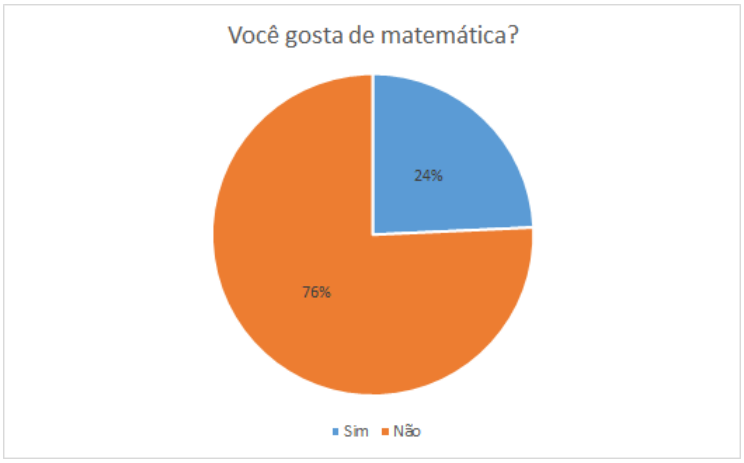

Figura 3.6: Gráfico Relacionado a Primeira Pergunta

Note que grande parte dos alunos do ensino básico não gostam de matemática e isso é fator preocupante e em análise a outras pesquisas realizadas sobre o tema, nota - se que diferente são os motivos que vêm desde da metodologia aplicada pelo professor até a falta de conhecimento do aluno.

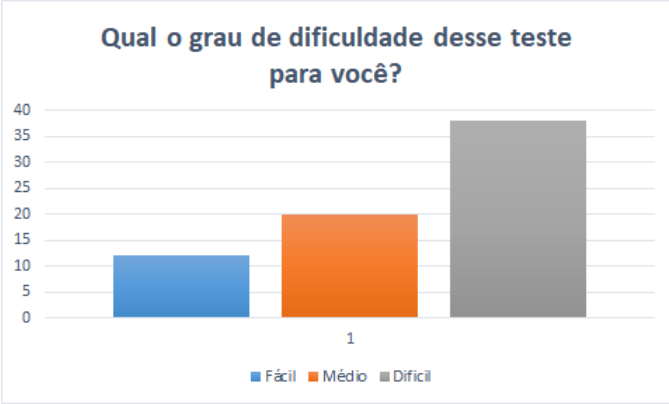

Figura 3.7: Gráfico Relacionado a Segunda Pergunta

Ao analisar o resultado dessa pergunta, percebemos que a maior parte dos alunos acharam o teste difícil ou médio, isto mostra que grande parte deles não preparados o suficiente para o vestibular e muitos ao terminar o ensino médio, vão para cursos pre - vestibulares para aprimorar seus conhecimentos. O que de fato esse conhecimento poderia ser ministrado em sala de aula, dando a cada aluno um conceito mais bem apurado e rico em técnicas para soluções de problemas.

Figura 3.8: Gráfico Relacionado a Terceira Pergunta

Ao análisar essa pergunta a resposta "SIM"foi unânime entre eles e todos os alunos questionados gostariam de aprender novas técnicas para responder questões de matemática de forma mais rápida e eficiente. Porém vale ressaltar que nem em todas as questões é possível, aplicar teoria dos números.

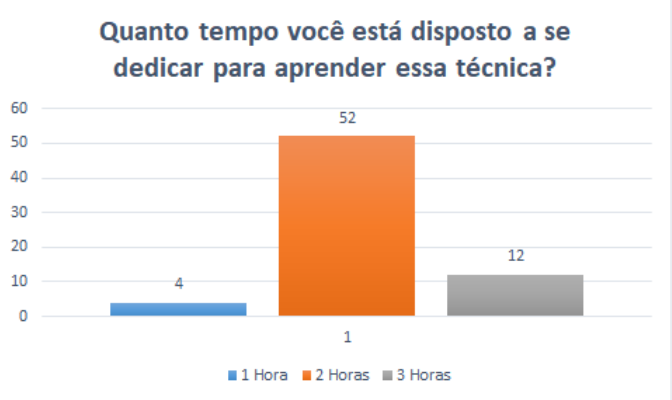

Figura 3.9: Gráfico Relacionado a Quarta Pergunta

Essa resposta acima é muito importante, pois a priori teríamos que saber se o aluno gostaria de aprender Teoria dos Números em seguida era preciso saber quanto tempo ele estava disposto a se dedicar para isso. E como mostra o gráfico a maioria está disposto a se dedicar em média duas horas por dia para aprender novas formas de aprender matemática. E isso é um fato, pois quando falamos que aprender teoria dos números ajuda a Ele a responder as questões de forma mais rápida, o aluno fica interessado e consequentemente seu desempenho tende a melhorar.

Figura 3.10: Gráfico Relacionado a Quinta Pergunta

Como já era esperado todos os alunos e os professores pesquisados consideram importante o tempo para solução de problemas em provas. E o mais legal é que eles (Alunos) estão dispostos a dedicarem um tempo maior para aprender novos métodos de solução de problemas. Acredito que o leitor também deve concordar que o tempo é um fator relevante para se sair bem em uma prova, seja ela, uma simples avaliação ou um vestibular, concurso, entre outros.

3.2 Sequência Didática

Depois de aplicado o questionário, tivemos um terceiro momento, o qual foi proposto aos alunos um momento de aprendizado sobre tópicos que irão ajuda - los nas soluções de problemas de matemática. Esse terceiro momento foi durante duas semanas no contra turno 3 vezes por semana "segunda, quarta e sexta"com duas horas aulas sobre *Noções de Teoria dos Números*, exemplos e soluções de exercícios, voltadas para tópicos que considero relevante para solução de problemas e que estão expostos no trabalho e serão mostrado aqui.

Inicialmente, foi definido que a metodologia usada nesta pesquisa é de abordagem qualitativa, pautada nos pressupostos teóricos e práticos da Engenharia Didática. A noção de Engenharia Didática emergiu na Didática da Matemática (enfoque na didática francesa) no início dos anos 80. Segundo Almouloud, Queiroz e Coutinho (2008) caracteriza-se por um esquema experimental baseado em realizações didáticas em sala de aula. Basicamente, a pesquisa se subdivide nas vertentes qualitativa e quantitativa. Sobre isso Pommer (2013) afirma que:

> *A Engenharia Didática possui dupla função: pode ser utilizada como metodologia qualitativa de pesquisa na área da matemática, mas também é extremamente útil para a elaboração de situações didáticas que configurem um quadro de aprendizagem significativa em sala de aula (p. 21)* [4]

A metodologia da Engenharia Didática foi desenvolvida e amplamente descrita por Artigue (1996) que a nomeou desta forma por se assemelhar ao trabalho do engenheiro que se apoia e aceita o controle científico, mas também está ciente da maior complexidade

dos problemas didáticos.
Ainda segundo Artigue (1996) esta metodologia está dividida em quatro fases.

i) Estudos Prévios: levam em consideração o quadro teórico didático geral, envolvendo o campo de domínio a ser estudado.

ii) Análises a Priori: o investigador identifica as variáveis didáticas para subsidiar a tomada de decisões.

iii) Experimentação: consiste basicamente no desenvolvimento e aplicação da sequência didática pretendida.

iv) Análises a Posteriori: se caracteriza pelo tratamento dos dados obtidos anteriormente, permitindo a interpretação dos resultados.

É importante ressaltar que essas fases não ocorrem, obrigatoriamente, de forma sequencial e isolada. Ao contrário, é comum a antecipação, junção e até sobreposição dos elementos caracterizadores destas quatro fases.
Nas próximas subseções apresentaremos de que modo a pesquisa foi realizada, de acordo com as fases da Engenharia Didática.

Experimentação e Aplicação da Sequência Didática

Como já exposto acima a aplicação da sequência foi dispostos em 6 encontros ao todo. Sendo 3 encontros na primeira semana e os outros na segunda semana no contra turno. Os encontros aconteceram no período de 03 de dezembro de 2018 a 14 de dezembro de 2018. Com a primeira turma em que o teste foi aplicado e de 04 de fevereiro a 15 de fevereiro com uma segunda turma, totalizando 70 alunos. Cada encontro teve duração de 120 minutos, sempre as Segundas feiras, Quartas feiras e Sextas feiras no turno vespertino.
No primeiro encontro foi falado sobre conceitos preliminares e Divisibilidade. Além de um momento de motivação para os alunos, mostrando a eles o número de erros aplicado anteriormente no teste e motivando - os a melhorar esse resultado e mostrando que eles podem fazer melhor e ser melhores. Este primeiro encontro teve como propósito aprofundas conceitos de divisibilidade e Máximo divisor Comum, conceitos esses já adquiridos pelos alunos no decorrer da vida escolar.
Estavam presentes cerca de 30 alunos, que foram organizados em círculo, com o intuito de promover a troca de conhecimento entre os alunos. Pois um ao lado do outro o acesso ao colega o lado era mais fácil.

No segundo encontro foi dado início à oficina de Equações Diofantinas. Pois esse conceito está intrisicamente ligado aos ministrados na primeira aula. Foram abordados conceitos iniciais tais como: múltiplos, divisores, m.d.c.,m.m.c., divisão euclidiana.
Foram resolvidos exercícios para exemplificar os conceitos abordados. A maioria dos estudantes apresentou certa dificuldade com esses conceitos, mostrando apenas o domínio da aplicação mecanizada de algoritmos. Mas entusiasmados por estarem aprendendo uma nova técnica para soluções de problemas.
Questionados sobre o verdadeiro significado dessas definições, nenhum deles soube explicar o real sentido dos cálculos efetuados. Foi percebido por exemplo, que nenhum deles

conseguia identificar, na divisão euclidiana, a relação entre dividendo, divisor, quociente e resto. Apesar de todos eles saberem o nome de cada fator envolvido. Problema sanado após a intervenção do pesquisador mediador. Notando que não é apenas ensinar a responder as questões, mas o verdadeiro significado que está por trás dessa técnica, aprendendo bem as definições e deixando tudo claro sem nenhuma dúvida.

O terceiro encontro iniciou-se a discussão sobre o que é número primo e como seria decompor um número fatorial em fatores primos como por exemplo 10!.Daí foi proposto aos alunos decompor em fatores primos o número 10!. Os alunos tentaram resolver multiplicando $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 3628800$, para daí decompor em fatores primos. Eles relataram que teriam que gastar muito tempo para acharem uma solução. E já se mostravam ansiosos por aprenderem uma nova forma de fazer isso. Antes de aplicar essa nova forma, foi solicitado a um aluno que fizer - se no quadro da forma "bruta"e seus colegas de sala poderiam ajudar. Com isso houve participação dos estudantes deixando a aula mais participativa.
A partir daí foram abordados conceitos de decomposição de fatorial em números primos, o Teorema Fundamental da Aritmética e consequentemente o Teorema de Legendre. Desde então percebemos uma mudança de postura dos alunos, que se mostravam muito mais interessados neste novo conteúdo e participaram ativamente inclusive fazendo perguntas e tirando dúvidas.

O quarto encontro foi o dia de se inserir conceitos de congruência modular e o pequeno teorema de Fermat, foi propostos problemas para encontrar restos, entre outras atividades.

O quinto encontro foi dedicado à resolução das questões vistas durante a semana buscando exemplificar e retomar os conceitos vistos em toda a oficina de conhecimento, bem como tirar as dúvidas dos alunos. Foram feitas duplas e os alunos participaram intensamente fazendo perguntas e expondo estratégias próprias de resolução. Ao final deste quinto encontro foi informado aos alunos que no sexto encontro eles fariam outro teste avaliátivo aos moldes do primeiro teste, para descobrir se eles evoluíram.

Por fim no sexto encontro foi dedicada a finalização da sequência didática e foi entregue aos alunos o mesmo teste aplicado no início da pesquisa em sala de aula, apenas com algumas modificações de valores. Foi dado o mesmo tempo 30 minutos para que eles resolverssem e ao me entregarem foram feitas perguntas e daí o teste foi corrigido em sala de aula com todos eles. Os resultados serão expostos na próxima seção, fazendo uma comparação com o primeiro teste.

3.3 Pós Teste

Após as aulas ministradas uma das principais preocupações foi: Se os alunos teriam avançado de um estado de menor para um de maior conhecimento sobre o que foi ensinado e se o objetivo do tempo para soluções das questões seria diminuído satisfazendo um dos principais objetivo da pesquisa.
Para verificar tal fato, foi aplicado um teste semelhante ao primeiro fazendo apenas algumas adaptações de valores. "Vale ressaltar que durante a primeira aplicação foram

recolhidas todas as folhas e não foi passado para os alunos gabaritos ou comentários sobre as questões aplicadas". Durante a segunda aplicação, avaliou - se os progressos de cada estudante, observando como ele se saiu nas atividades da sondagem inicial - que já é uma situação de aprendizagem - até a etapa final. Em seguida foi feita uma comparação com o primeiro resultado, que será demonstrado aqui.

Quantitativo	**Questão 1**	**Questão 2**	**Questão 3**	**Questão 4**	**Questão 5**
Número de Acertos (Antes)	20%	29%	3%	25%	58%
Número de Acertos (Depois)	60%	75%	60%	70%	80%

De fato, houve um crescimento bastante positivo e expressivo em relação ao número de acertos, quando comparado a primeira aplicação. Mostrando que as aulas surtiram efeitos como desejado, que os alunos compreenderam melhor os conteúdos e que a técnica desenvolvida foi bem aceita e compreendida pelos alunos. Posso dizer que foi um sucesso, pois se analisando os casos o leitor pode perceber que em quase todas as questões houve um crescimento de mais de 100% no número de acertos, sendo assim um resultado excelente.

Quantitativo	**Questão 1**	**Questão 2**	**Questão 3**	**Questão 4**	**Questão 5**
Número de Erros (Antes)	70%	64%	97%	75%	42%
Número de Erros (Depois)	40%	25%	40%	30%	20%

Ao analisar esses registros, ficou claro como os alunos evoluíram, e perceber que essa grande evolução aconteceu com apenas 12 horas de trabalho. Fica aqui minha indagação e se você incluir - se esse método durante todo o ano letivo ao final de cada conteúdo, quanto o seu aluno não iria evoluir?

Vale ressaltar também que alguns fatores influenciaram nos resultados obtidos, que poderiam ser ainda bem melhores do que, o quê, já foi. Cito alguns fatores que influenciaram: Poucos encontros disponíveis, o fato do tema ter sido ministrado concomitantemente a outros conteúdos programáticos, pois acredita - se que se fosse aplicado concomitantemente com cada conteúdo específico o resultado seriam muito mais satisfatório do que, o quê, já se foi.

Apesar de todos as adversidades, os resultados obtidos a partir dos testes I e II mostram que tivemos um crescimento de 94 acertos no geral para 240 acertos, aumento de mais de 150% nos acertos, e uma diminuição de mais de 110% nos erros, caindo de 256 erros para 110 erros. Portanto fica evidente que houve uma interferência bastante positiva da oficina de conhecimento sobre Teoria dos Números no resultado do aluno.
Então, é possível concluir que o ensino, ainda que superficial, de conceitos relacionados a Teoria dos Números influenciam positivamente na forma como os alunos interpretam e solucionam problemas matemáticos.

3.4 Considereções Finais

Através deste trabalho, conclui-se que a aplicação de Teoria dos números como uma complementação do conteúdo ou até mesmo sendo um assunto visto regularmente é uma ferramenta extremamente importante para resolver algumas situações problemas e consequentemente melhorar o desempenho do aluno na resolução de problemas. A pesquisa mostrou que nas aulas de Matemática o professor pode propiciar momentos para incluir conteúdos mais aprofundados, criar espaços de aprendizagens criativos e significativos, valorizando a participação do aluno e mostrando sempre onde se pode aplicar aquele conteúdo.

Foi observado durante a realização desse trabalho, que a cada conteúdo novo implementado mostrando como esse conteúdo se aplica na resoluções de problemas, os alunos se sentiam estimulados a participar mais e mais, a se desafiar e a participar com intervenções orais motivados pela empolgação de aprender algo novo. Foi-lhes proporcionado entender que com a aplicação de Teoria dos Números seria possível fazer questões de forma mais rápida, que a atividade se mostrou uma oportunidade de ampliar o conhecimento do aluno. Esse avanço foi realmente gratificante. Pode-se concluir que a pesquisa tornou - se manifesto de um vasto campo de conhecimento e possibilidades onde os conteúdos matemáticos podem ser explorados, através de resoluções de questões de vestibulares e isso ajudou a muitos alunos a passarem a gostar de estudar Matemática.

Torna-se indispensável ressaltar que atualmente pelas experiências vivenciadas em sala de aula e pelos testemunhos de muitos colegas de trabalho é muito importante 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 na obtenção das melhores estratégias de solução e os mesmos consigam progredir. Ou seja, é preciso criar maneiras para que os alunos aumentem o conhecimento matemático. 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 dificuldades na resolução de problemas, pricipalmente em relação ao tempo, buscando trabalhar de maneira mais atraentes aos olhos dos estudantes, mostrando meios diferentes de soluções e de preferência meios mais rápidos. Mas sem perca de conhecimentos predominantes e importantes.

Espera - se deste trabalho é que ele auxilie o professor na prática docente no que diz respeito ao desenvolvimento de conteúdos e principalmente nas resoluções de problemas. Pois acredita-se veemente que essas ideias poderá facilitar o aprendizado dos alunos, em muitas situações e principalmente na hora de ir fazer uma prova de vestibular.
Em consonância com o exposto espera - se também que espelhados por essa proposta, os professores possam aderir a essa pesquisa e consequentemente possam surgir outros trabalhos nesta linha, buscando ajudar os alunos e melhorar o ensino da matemática. Trazendo assim outras aplicações interessantes que poderão se utilizadas no ensino básico tanto pelo professor como pelo aluno.

Capítulo 4

APÊNDICE

4.1 Anexo I

No âmbito da dissertação de Mestrado Profissional em Matemática – com o título **"Introdução à teoria dos números: Uma nova proposta para educação básica"** estou realizando um trabalho colaborativo entre professores da área de matemática na escolha de um melhor processo didático para aplicação da Teoria dos números em sala de aula no dia a dia. O presente questionário tem como objetivo a recolha de informações relativa à atitude dos professores face à aplicação da teoria dos números em seu ensino. O questionário está organizado da seguinte maneira algumas perguntas direcionada para a opinião pessoal dos professores sobre a disciplina e algumas perguntas relacionadas com a aplicação da teoria dos números na sala de aula. Solicita-se a sua colaboração no preenchimento individual do questionário, garantindo-se que os dados serão tratados de forma totalmente anónima.

Desde já obrigado.

QUESTIONÁRIO - PROFESSORES

1.Considera que o tempo para resolver questões de matemática em vestibulares é pouco?
( ) Sim ( ) Não

2. Considera que administrar o tempo para responder questões de matemática em vestibulares é importante?
( ) Sim ( ) Não

3.Você é favor de que os alunos aprendam noções de teoria dos números no ensino básico?
( ) Sim ( ) Não

4.Durante quanto tempo você estudou ou estuda matemática, incluindo graduação, pós-graduação e cursos de aperfeiçoamento? ( )4 anos ( ) Entre 4 e 6 anos

( ) Entre 6 e 10 anos ( ) Mais de 10 anos

5.Você está disposto a ajudar seu aluno a diminuir o tempo para solução de problemas ? Além de aumentar o conhecimento matemático dele?
( ) Sim ( ) Não

6.Quanto tempo você estária disposto para aprender Teoria dos números para passar para seus alunos?
( )Nenhuma ( ) 2 horas semanais ( ) Entre 2 e 5 horas semanais
( ) Mais de 5 horas semanais

7. Quais momentos você considera importante para inserir novos conhecimentos, extra curriculares ao seu aluno?
( ) Início do Ano ( ) Nas férias "Curso de Férias" ( ) Final do Ano ( ) A medida que se ministra cada conteúdo ( ) No contra horário

8. Você concorda em inserir conhecimentos matemáticos que ajude o aluno a ter capacidade de responder questões de outra maneira "mais rapidamente"?
( ) Sim ( ) Não

9. Assinale cada uma das seguintes frases, de acordo com o seu grau de acordo/desacordo, numa escala entre 1 (discordo em absoluto) e 5 (concordo totalmente).

Perguntas	**1**	**2**	**3**	**4**	**5**
Gosto de ensinar Matemática.					
Ensino Matemática por obrigação.					
Conheço bem os temas a desenvolver.					
Os meus alunos gostam de Matemática.					
A Matemática é uma disciplina independente das outras.					
Você considera o sucesso do seus alunos importante.					
Você é a favor de mudanças em temas da matemática do ensino básico.					

4.2 Anexo II

QUESTIONÁRIO - ALUNOS

Foram feitas as seguintes Perguntas:

1.Você gosta de matemática?

( ) Sim ( ) Não

2.Qual o grau de dificuldade desse teste para você?

( ) Fácil ( ) Médio ( ) Difícil

3.Você gostaria de saber responder essas questões de uma forma mais rápida?

( ) Sim ( ) Não

4.Se sim, Quanto tempo você está disposto a se dedicar para aprender essa técnica?

( ) 1 hora ( ) 2 horas ( )3horas

5. você considera importante o tempo para se responder um teste?

( ) Sim ( ) Não

6.Em que situações lhe parece que a Matemática é um instrumento facilitador?

( )Nunca ( ) As vezes ( ) Sempre

4.3 Anexo III

QUESTIONÁRIO PARA SONDAGEM

1. (UFCE) O maior inteiro x tal que $\frac{60!}{7^x}$ seja uma número natural é:
a) 7
b) 8
c) 9
d) 10
e) 11

2. (FUVEST – SP) Se $4^{16} \cdot 5^{25} = \alpha \cdot 10^n$ com $1 \leq \alpha \leq 9$, então n é:
a) 24
b) 25
c) 26
d) 27
2) 28

3. (UFF) Em um estacionamento existem carros e motos num total de 84 rodas quantos carros podem existir neste estacionamento?
a) 12
b) 15
c) 18
d) 20
e) 30

4. (UNIT) Um número dividido por 5 deixa resto 4, e dividido por 7 deixa resto 3. Qual o resto da divisão desse número por 35?
a) 24
b) 59
c) 17
d) 19
e) 29

5. (ENEM) Suponha que João tenha perdido seus documentos, inclusive o cartão de CPF e, ao dar queixa da perda na delegacia, não conseguisse lembrar quais eram os dígitos verificadores, recordando-se apenas que os nove primeiros algarismos eram 123.456.789. Neste caso, os dígitos verificadores d1 e d2 esquecidos são, respectivamente:
a) 0 e 9.
b) 1 e 4.
c) 1 e 7.
d) 9 e 1.
e) 0 e 1.

Referências Bibliográficas

[1] Mariano Martínez Boyer, Carl B e Pérez. *História da Matemática.* Alianza e Madrid, 1986.

[2] Miriam e Gongorra Sodré. *Ensino Fundamental: A origem dos números.* ENCEEJA, Brasília - MEC/INEP, 2006.

[3] Abramo Hefez. *Aritmética.* Coleção PROFMAT, Rio de Janeiro: SBM, 2016.

[4] Wagner Marcelo Pommer. *A Engenharia Didática em sala de aula: Elementos básicos e uma ilustração envolvendo as Equações Diofantinas Lineares.* São Paulo:[sn], 2013.

[5] José Plínio de Oliveira Santos. *Introdução à teoria dos números*, volume 3. Rio de Janeiro: IMPA, 2009.

[6] Almouloud, S. A.; Queiroz, C. de; Coutinho, S. Engenharia didática: características e seus usos em trabalhos apresentados no gt-19/anped. Revemat: Revista Eletrônica de Educação Matemática, v. 3, n. 1, p. 62–77, 2008.

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

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