UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA

NÚMEROS PRIMOS UMA ABORDAGEM EDUCACIONAL

Edson Ribeiro Machado

MANAUS
2015

UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA

Edson Ribeiro Machado

NUMEROS PRIMOS UMA ABORDAGEM EDUCACIONAL

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Roberto Antonio Cordeiro Prata

MANAUS
2015

EDSON RIBEIRO MACHADO

NUMEROS PRIMOS UMA ABORDAGEM EDUCACIONAL

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em 30 de Abril de 2015.

BANCA EXAMINADORA

Prof. Dr. Roberto Antonio Cordeiro Prata
Presidente

Prof. Dr. Valtemir Martins Cabral
Membro

Prof. Dra. Jeanne Moreira de Sousa
Membro

AGRADECIMENTOS

Agradeço a Deus por tudo concedido até hoje, pelo dom da vida e bênçãos a mim concedidas e por sempre guiar meus passos para realizar com sucesso os meus objetivos.

Ao meu orientador Prof. Dr. Roberto Prata, pela confiança e dedicação, por toda liberdade no desenvolvimento deste estudo e por ter acreditado em meu potencial e me conduzindo para esta realização, obrigado pelas horas e apoio disponibilizados.

A todos os meus professores do PROFMAT, pela arte de ensinar, por aceitar o desafio de nos ensinar e acreditar em nossa capacidade de aprender.

RESUMO

Neste trabalho buscou-se fazer uma nova abordagem na construção dos números primos, na forma de encarar os números naturais, e na diferenciação de números compostos e primos, bem como mostrar sua distribuição ao longo do conjunto dos números naturais com a finalidade de aprimoramento dos nossos alunos do Ensino Fundamental e Médio no estudo do Conjunto dos Números, apresentando-lhes em forma de subconjuntos e cisão de conjuntos concluindo finalmente no Teorema Fundamental da Álgebra (TFA). Inicialmente fazendo um resumo histórico e em seguida uma introdução onde destacamos o princípio da boa ordenação, divisibilidade, congruência, MDC, MMC, definição de números primos e números composto e também o TFA. Logo depois dividimos o trabalho em cinco capítulos nos quais tratamos a infinitude dos números primos, aplicações, como achar números primos, como saber se um número é primo e por fim um trabalho feito com os alunos do Colegio Militar de Manaus junto ao Clube de Matemática lá existente.
Palavras-Chave: Conjuntos; Números Primos ; Números Compostos; Congruência; Divisibilidade.

ABSTRACT

In this study we attempted to take a new approach in the construction of primes in the form of facing the natural numbers, and differentiating compounds and prime numbers and show their distribution over the set of natural numbers with the improvement of our purpose students of primary and secondary education in the study of the numbers set by presenting them in the form of sub-assemblies and fission products finally emptying into the Fundamental Theorem of Algebra (TFA). Initially making a historical summary then an introduction where we emphasize the principle of good order, divisibility, congruence, MDC, MMC, definition of prime numbers and composite numbers and also the TFA. Soon after divided the work into five chapters in which we treat the infinity of prime numbers, applications, how to find prime numbers, how to tell if a number is prime and for the end work done with the students of Colegio Militar de Manaus with the math club there existing.

Keywords: Sets; Prime Numbers; Compounds numbers; congruence; Severability.

Sumário

LISTA DE SÍMBOLOS

$\mathbb{N} = \{1, 2, 3, 4, ...\}$	Conjunto dos Números Naturais
$\mathbb{Z} = \{... - 3, -2, -1, 0, 1, 2, 3, ...\}$	Conjunto dos Números Inteiros
$\mathbb{Z}^+ = \{0, 1, 2, 3, 4, ...\}$	Conjunto dos Números Inteiros não negativos
$\mathbb{Z}_m = \{[1], [2], [3], ..., [m-1]\}$	Classe Residual modulo m

Capítulo 1

Introdução

Nós professores de matemática, em geral, trabalhamos muito pouco as características dos números primos com nossos alunos. Dentre alguns dos motivos para que este fato ocorra, temos a dificuldade por parte dos alunos em determinar se um número é primo ou composto, faltando muitas vezes estruturação e método, e a falta de aplicação no cotidiano dos alunos e, juntando a isso temos as experiências negativas que envolvem esta matéria e a maneira como os professores abordam esse tema.

Pensando nisso, deve-se escolher uma maneira motivadora para que sejam abordados os temas relacionados aos números primos, tentando envolver o conteúdo o máximo possível com a realidade do aluno, procurando sua aplicabilidade, de modo a tornar o processo ensino-aprendizagem mais tranquilo e satisfatório, em termos de resultados.

Neste texto, apresentamos uma proposta de abordagem do tema dos Números Primos no Ensino Fundamental e Médio. Acreditamos que este tema é muito importante, trazendo situações-problema para a sala de aula, onde o aluno será motivado a utilizar o raciocínio e a criatividade. Além disso, verificamos que alguns conteúdos, que a princípio são trabalhados no Ensino Superior,podem ser iniciados nas séries anteriores ao curso universitário, como por exemplo o estudo das congruências, o algoritmo de Euclides, método de fatoração de Fermat, os crivos e as classes residuais, que pode trazer

maior interesse por parte dos alunos com relação aos números primos.

Sendo assim com a finalidade de destacar os números primos iremos organizar o conjunto dos números naturais $\mathbb{N} = \{1, 2, 3, 4, ...\}$ em três conjuntos, o conjunto $\{1\}$, conjunto dos números primos $P = \{2, 3, 5, 7, ...\}$ e o conjunto dos números compostos $C = \{4, 6, 8, 9, 10, ...\}$ e posteriormente trataremos de suas distinções e relações, e importância de cada um deles e como obter elementos de cada um desses conjuntos.

Nesse contexto a unidade não pode ser considerado um número primo pois contraria o Teorema Fundamental da Álgebra, quando diz que todo número natural diferente do 1 pode ser escrito de uma única forma através do produto de potencias de números primos. A titulo de exemplo podemos observar, caso considerarmos o número 1 como um número primo teríamos $6 = 2 \times 3 = 1 \times 2 \times 3$, sendo assim adotar o número 1 como primo contrariaria esse teorema. Por outro lado o número 1 não pode ser considerado composto pois é o único número natural que não pode ser escrito através dos números primos, desse modo temos o conjunto dos números naturais, através destes 3 conjuntos, atendendo as condições de cisão onde a união é o próprio conjunto dos naturais e a interseção é vazia. É importante observar que os números primos são números positivos, mas muitas vezes e ao longo deste trabalho a presença dos números inteiros positivos e negativos com suas operações serão amplamente utilizados.

Estrutura do TCC

Além dos capítulos - Um pouco de História e a introdução - este trabalho está organizado como segue.

Considerações inciais:

Onde são dadas as noções iniciais que serão importantes para o entendimento e aplicação dos números primos.

Existem infinitos números primos ?

Quantos números primos existem? Existem infinitos números primos?

onde se procura utilizar as demonstrações mais simples que nos permite entender a existência de infinitos números primos dentro do contexto do ensino médio e fundamental.

A importância dos Números Primos

Porque os números primos são importantes? Neste tópicos é colocado situações em que os números primos são importantes para soluções de alguns problemas ou para gerar soluções particulares ou para garantir a existência delas.

Esse número é primo?;

Como identificar se um número é primo? Onde será tratado alguns métodos de se identificar se um números é primo mostrando as vantagens e desvantagens de cada um.

É possivel gerar Números Primos ?

Como gerar números primos? Nesse último tópico é feito um estudo sobre os vários métodos de se gerar números primos citando os aspectos positivos e negativos de cada método.

Trabalhando com os Alunos:

Trabalho feito sobre o estudo dos números primos com os alunos do Clube de matemática do Colégio Militar de Manaus.

Capítulo 2

Um pouco de História

Introduzimos um pouco de História segundo a referencia [08], [14] e [16].

Os gregos, em particular os pitagóricos, estudaram os números extensivamente e perceberam a importância dos números primos. Eles tinham um profundo interesse pelos números perfeitos e pelos pares de números amigáveis. Posteriormente, Eratostenes descobriu como determinar todos os números primos através de um crivo.

Os Elementos de Euclides (cerca de 300 a.C) possuem importantes teoremas sobre números primos, inclusive uma prova de que os números primos são infinitos, utilizando uma demonstração pelo método da contradição.

Euclides demonstra também a Teoria Fundamental da Aritmética que diz que qualquer inteiro pode ser decomposto como produto de potencias de números primos de forma única. Euclides também mostrou como construir um número perfeito a partir de um primo Mersenne.

A palavra primo significa primeiro, e sua origem está na concepção numérica da escola pitagórica por volta do século V a.C. Nessa época, os matemáticos gregos dividiam os números inteiros naturais em três classes: a monad (unidade, 1); os protói arithmói (significa números primos) ou asynthetói aritmói (números não compostos), ou seja,aqueles que não podem ser gerados pelo produto de outros números além da unidade. $\{2, 3, 5, 7, 11, ...\}$ e os deuterói arithmói (números compostos): aqueles que podem ser gerados pelo produto dos protói arithmói. $\{4, 6, 8, 10, 12, 14, ...\}$.

Durante a Idade Media, o desenvolvimento da Teoria dos Números Primos

ficou estagnado, assim como praticamente todas as outras áreas do conhecimento. Somente no seculo XVII, apos estudar a Aritmética de Diofanto (escrita provavelmente no seculo III), Pierre de Fermat ressuscitou a questão, e é considerado o fundador da moderna Teoria dos Números. Fermat não era matemático profissional. Mesmo assim, encontrava tempo para se dedicar a matemática. Algumas de suas conjeturas posteriormente provaram-se falsas, como a de que seria primo todo numero da forma $Fn = 2^{2^n} + 1$, os quais ficaram conhecidos como Números de Fermat, que ele fez baseado na observação de que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65.537$ são primos onde em 1732, Leonhard Euler mostrou que $F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \times 6.700.417$, portanto, composto, desmentindo assim a afirmação de Fermat.

Outra conjetura, hoje conhecida como Pequeno Teorema de Fermat, revelou-se verdadeira e diz que se p é primo, e a e p são primos entre si (dizemos que dois números a e p são primos entre si quando seu único divisor comum é o 1), então $a^{p-1} - 1$ é divisível por p. Utilizando esse teorema, podemos concluir, por exemplo, que $2^{100} - 1$ é divisível por 101, sem termos que calcular o valor desse número.

Euler, desta vez, demonstrou sua veracidade, e percebeu, inclusive, que esse teorema na verdade é um corolário de um teorema mais geral.

Euler, como bem se sabe, foi extremamente ativo na sua produção científica. Durante sua vida publicou mais de 500 artigos em quase todas as áreas da matemática. Entre suas contribuições, que depois tiveram consequências na historia dos números primos, esta o estudo da funcão ζ, conhecida como Funcão Zeta de Euler.

Até então ninguém havia conseguido ver um padrão na distribuição dos números primos. Essa distribuição, aparentemente aleatória, ensejou a questão de saber se era possível prever a localização precisa do próximo numero primo. Foi Gauss quem deu o primeiro e decisivo passo nesse sentido, aos 15 anos de idade. A tabela de números primos contida na contracapa de seu livro de logaritmos parece ter sido a responsável por esse passo. Onde em vez de tentar prever a localização precisa do próximo primo, ele buscou ao

menos descobrir quantos primos haveria entre os primeiros 100 números, os primeiros 1.000 e assim por diante. Ou seja, se tomássemos o numero N, haveria alguma maneira de estimar quantos primos encontraríamos entre os números 1 e N?

Ao se perguntar quantos primos existiam entre 1 e N, isto é, qual é o valor da função $\pi(n)$ para $n = N$, Gauss percebeu que parecia existir uma relação entre esse valor e os logaritmos. Assim, parecia haver uma conexão entre a função logarítmica e a distribuicão dos números primos, que o levou, por fim, até a descoberta da integral logarítmica. Gauss, de fato, foi um dos grandes propulsores da Teoria dos Números. Em 1798, aos 21 anos, produziu uma das obras-primas da matemática, o livro Disquisitiones Arithmeticae, publicado em 1801, onde, entre outras novidades, introduziu o conceito de congruência, que consiste em uma aritmética com os restos da divisão euclidiana por um numero fixado, e que acabou por ter uma utilidade pratica, descoberta somente após cerca de 200 anos.

Analisando os estudos de Gauss, e estudando a Função Zeta de Euler, estendendo-a para números complexos, Riemann deparou-se com algo que parecia acabar com a impossibilidade de prever a localização exata dos números primos. Ele visualizou uma relação entre os zeros não triviais da função zeta e a localização dos números primos. Tal relação teve como consequência uma conjetura, ate hoje não provada, conhecida como a Hipótese de Riemann. Se sua conjetura estiver correta, a estimativa de Gauss sobre a distribuição dos números primos será cada vez mais precisa a medida que se avança na contagem.

Capítulo 3

Considerações Iniciais

3.1 Princípio da boa Ordenação

Por muitos milênios os números foram considerados entes intuitivos e algumas de suas propriedades, como a comutatividade e associatividade da adição e da multiplicação, consideradas inerentes à sua própria natureza, sem a necessidade de demonstração.

Com o desenvolvimento da matemática surgiram novos problemas que, para melhor serem compreendidos e solucionados, precisavam de uma fundamentação mais rigorosa do conceito de número. Este trabalho foi realizado pelos matemáticos do século XIX.

1. Todo Número Natural tem um sucessor, que ainda é um número natural;

2. Números Naturais diferentes têm sucessores diferentes;

3. Existe um único Natural 1 que não é sucessor de nenhum outro natural;

Definição 3.1. *Desta forma o conjunto númerico que contém o número 1 e contém também o seu sucessor e possui também o sucessor de cada um de seus elementos, esse conjunto contém todos os números chamados naturais.* $\mathbb{N} = \{1, 2, 3, 4, 5, 6, ...\}$ *tem um elemento mínimo* 1 *e uma relação de ordem, ou seja, dado dois elementos do conjunto acima* a *e* b *temos* $a < b$ *ou* $a > b$ *ou* $a = b$*. Diante do exposto qualquer coleção finita de elementos deste conjunto sempre teremos um menor e um maior elemento, e toda coleção infinita de elementos deste conjunto sempre haverá um menor elemento.*

Exemplo 1. *seja o conjunto dos divisores naturais do número* 12 *maiores que* 1*, representado por* $D(12) = \{2, 3, 4, 6, 12\}$ *neste caso é um conjunto finito de números naturais e tem um menor elemento o* 2 *e o maior elemento o* 12*.*

3.2 Divisibilidade

Definição 3.2. *Sejam* a *e* b *dois inteiros com* $a \neq 0$ *se* a *divide* b *tem-se a notação* $a|b$ *se somente se existe um inteiro* k *de modo que* $b = a \times k$ *e chamamos* b *um múltiplo de* a*. Se* a *divide* b *temos que* $a|b$ *,* $a|-b$ *e* $-a|-b$*. Se* $a|1$ *então* $a = \pm 1$*, pois se* $1 = a \times k$ *implica* $a = k = \pm 1$*.*

Proposição 3.1. *Se* $a|b$ *e* $c|d$ *então* $a \times c|b \times d$

Demonstração: 1. *Pois se* $b = a \times k_1$ *e* $d = c \times k_2$ *temos* $b \times d = a \times c \times k_1 \times k_2$ *logo* $ac|bd$

Proposição 3.2. *Se* $a|b$ *e se* $a|d$ *então* $a|b \times k_1 \pm d \times k_2$ *para todo* k_1*,* k_2 *inteiros*

Demonstração: 2. *Pois se* $b = a \times k_1$ *e* $d = a \times k_2$ *logo* $b \times x \pm d \times y = a \times k_1 \times x \pm a \times k_2 \times y = a \times (k_1 \times x \pm k_2 \times y)$

Proposição 3.3. *Se* $a|b$ *e* $b|c$ *então* $a|c$

Demonstração: 3. *Se* $b = a \times k$ *e* $c = b \times k_1$ *então* $c = a \times k \times k_1$ *logo* $a|c$*.*

3.3 Números primos e números compostos

Como já citado o conjunto dos números naturais pode ser dividido em três grupos chamados: 1, o conjunto dos números primos $(p, p_1, p_2, .., p_n)$ e conjunto dos números compostos $(a, b, c, ..)$.

Definição 3.3. *Um número natural* p *é primo, se para todo* c *natural em que* $1 < c < p$*,* c *não divide* p*. Por outro lado, um número composto,* a*, é aquele em que existe um* c *natural tal que* $1 < c < a$ *e* $c|a$*.*

3.4 Divisão Euclidiana

Teorema 3.1. *Dados inteiros d e D com $d \neq 0$, existem inteiros q e r tais que*

$$D = d.q + r \ \ e \ \ 0 \leq r < |d|. \tag{3.1}$$

Além disso, q e r são unicamente determinados pelas condições acima.

Demonstração. Considere o conjunto limitado inferiormente,

$$S = \{x \in \mathbb{Z}^+ | x = D - d.n \ \ para \ \ algum \ \ n \in \mathbb{Z}\}.$$

Este conjunto é não vazio pois existe um inteiro n tal que $n.(-d) \geq D$, portanto $x = D - n.d \in S$.

Pelo Princípio da Boa Ordenação, segue que S possui um menor elemento r. Logo $r = D - d.q$, para algum $q \in \mathbb{Z}$. É claro que $r \geq 0$ pois $r \in S$. Vamos agora provar que $r < |d|$.

Suponha por absurdo que $r \geq |d|$, logo $r = |d| + s$ para algum s tal que $0 \leq s < r$. Portanto

$$D = d.q + |d| + s = d.(q \pm 1) + s,$$

e consequentemente,

$$s = D - d(q \pm 1) \in S.$$

Como $s \in S$ e $s < r$, temos uma contradição pois r era o menor elemento de S.

Para provar a unicidade suponha que

$$D = d.q_1 + r_1 = d.q_2 + r_2,$$

com $0 \leq r_1 < |d|$ e $0 \leq r_2 < |d|$. Por estas últimas desigualdades segue que

$$-|d| < -r_2 \leq r_1 - r_2 \ \ e \ \ r_1 - r_2 < |d| - r_2 \leq |d|,$$

e portanto

$$-|d| < r_1 - r_2 < |d|.$$

Consequentemente, temos que $|r_1 - r_2| < |d|$. Como

$$d(q_1 - q_2) = r_2 - r_1,$$

Segue que

$$|d|.|q_1 - q_2| = |r_2 - r_1| < |d|.$$

Isto só é possível se $q_1 = q_2$ e $r_1 = r_2$.

Portanto é possível em $\mathbb{Z}$ efetuar a divisão de um número D por outro número $d \neq 0$ com resto pequeno.

Os números D, d, q e r são chamados respectivamente de dividendo, divisor, quociente e resto.

Observação 3.1. *Na divisão euclidiana, se $D \geq 0$ e $d > 0$, então $q \geq 0$. De fato, se valesse $q < 0$, teriamos*

$$D = d.q + r < d.q + d = d(q + 1) \leq 0,$$

Logo $D < 0$, absurdo.

Por tudo que foi dito acima podemos fazer a seguinte definição.

Definição 3.4. *Na divisão de a por b onde b não divide a de forma inteira definimos: $a = bq + r$...(1) restringindo r a $0 < r < |b|$.... (2) Onde a relação (2) impõe a unicidade da igualdade (1).*

Vejamos um exemplo:

Exemplo 2. *Vejamos um exemplo seja $a = -8$ e $b = 3$ na divisão de -8 por 3 utilizando apenas (1) podemos ter: $-8 = 3(-3)+1$ ou $-8 = -3\times 2+(-2)$ ou $-8 = 3(-4) + 4$. Utilizando também (2) temos apenas:$-8 = 3(-3) + 1$. Um outro exemplo seria $a = -8$ e $b = -3$ logo temos apenas $-8 = (-3)3 + 1$ obedecendo a relação (1) e (2). Nesse contexto da divisibilidade podemos identificar os dois conjuntos: primos e compostos. Os primos*

como o conjunto dos números p, natural, onde para todo inteiro significativo $b = \{\pm 1, \pm 2, \pm 3, .., \pm(p-1)\}$ *temos que* $p = bq + r$ *o resto* r *sempre* $0 < r < |b|$. *Por outro lado identificamos o conjunto dos números composto dentro do contexto da divisibilidade como aquele natural* a *onde existe um inteiro significativo* $b = \{\pm 1, \pm 2, \pm 3, .., \pm(a-1)\}$ *tal que* $a = b.k$ *para algum número* k *inteiro.*

Observação 3.2. *O resto também é denotado por* $a \bmod b$ *na divisão de* a *por* b *tratamento que será dado posteriormente.*

Exemplo 3. $43\,(mod\,12) = 43 \div 12 = 3\,com\,resto 7 \; -- > 43\,(mod\,12) = 7$
$59\,(mod\,5) = 59 \div 5 = 11\,com\,resto\,4 \; -- > 59\,(mod\,5) = 4$
$2 + 3(mod 7) = 5$ *porque* $5 \div 7 = 0 \quad com \quad resto \quad 5$
$2 + 9(mod\,7) = 4$ *porque* $11 \div 7 = 1$ *com resto* 4
$3 \times 3(mod\,7) = 2$ *porque* $9 \div 7 = 1$ *com resto* 2

3.5 Teorema Fundamental da Aritmética

Este importante teorema mostra que os números primos são os construtores dos inteiros, ou seja, todo número inteiro pode ser escrito de forma única como um produto de potências de números primos.

Teorema 3.2. *(Teorema Fundamental da Aritmética (TFA)). Todo inteiro maior que um se escreve de maneira única como um produto de primos.*

Lema 3.1. *O menor divisor de um número natural é um número primo.*

Demonstração: 4. *Seja* a *um número natural maior que* 1 *e seja* d *seu menor divisor se* d *não é primo existe* c *tal que* $1 < c < d$ *então* $c|d$ *logo pelas propriedades demostradas acima* $c|a$ *logo* $c < d$ *contradição.*

Lema 3.2. *(Lema de Euclides) Se* p *é um primo que divide* $a.b$ *então* p *divide* a *ou* p *divide* b.

Demonstração: 5. *Suponha que* p *é um primo que divide* $a.b$ *mas que* p *não divide* a. *Como* p *é primo podemos afirmar que* p *e* a *são relativamente*

primos. Assim existem inteiros r e s tais que $ra + sp = 1$. *Então* $r(ab) + sb(p) = b$. *Como p divide ab e p divide p temos que p divide b.*

Existência - TFA.

Seja $S \subset \mathbb{Z}$ formado de inteiros maiores que 1 que são primos ou um produto de primos. É claro que $2 \in S$. Supondo agora que para algum inteiro n, S contém todos os inteiros k com $2 \leq k < n$. Devemos mostrar que $n \in S$. Se n é primo, então $n \in S$ por definição. Se n não for primo, n poderá ser escrito na forma $n = a.b$ onde $1 < a < n$ e $1 < b < n$.

Como estamos assumindo que a e b pertencem a S, eles são primos ou produtos de primos. Assim, n também é um produto de primos. Existência provada.

Unicidade - TFA

Sejam duas fatorações em primos de n:

$$n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$$

. Pelo Lema de Euclides $p_1 | q_i$ para algum q_i e como p_1 e q_i são primos temos que $p_1 = q_i$ para algum $i \in \{1, 2, ..., s\}$. Analogamente $p_2 = q_j$ para algum $j \in \{1, 2, ..., s\}$ e assim por diante. Pela propriedade do cancelamento teremos $1 = q_{i_1} ... q_{i_k}$ se $s > r$. Mas isso é um absurdo pois nenhum produto de números primos pode ser igual a 1. Analogamente se $s < r$ também chegamos a um mesmo absurdo. Logo $s = r$ e os primos são os mesmos.

Também podemos observar que dado um número a composto seja p seu menor divisor diferente de 1 tal que $b = a/p$ sendo assim se b primo temos $a = b.p$ sendo assim terminada a fatoração de a. Caso b seja composto temos p_1, menor elemento que divide b diferente de 1, um número primo (que pode ser igual a p ou não) tal que $c = b/p_1$ se c um numero primo temos $a = c.p.p_1$ terminamos a fatoração, caso contrario seguimos sucessivamente dessa forma até obtermos a fatoração final do número a como:$a = p.p_1.p_2...p_n$.

Quanto a unicidade, seja a um composto dado, seja p o menor divisor de a pelo principio da boa ordenação ele é único, partindo dai seja b, onde $b = a/p$, e $1 < p_1 \leq b$ o menor divisor de b, é único pelo principio da boa ordenação,

desta forma e assim sucessivamente segue a unicidade:$a = p.p_1.p_2...p_n$.

Diante do exposto e estendendo um pouco mais o raciocínio podemos dizer:

Proposição 3.4. *Dado número natural a diferente de* 1 *é composto se e somente se possui algum divisor primo p cujo quadrado é maior do que* 1 *e menor ou igual a a.*

Demonstração: 6. *Se existe p o menor divisor primo de a tal que:* $1 < p < p^2 \leq a$ *então a é composto. Por outro lado, se a é composto, ele possui um divisor natural q cujo quadrado e maior do que* 1 *e menor do que ou igual a a. Se q é primo basta colocar p igual a q. Se q é composto ele possui um menor divisor primo p tal que:* $1 < p^2 < q^2 \leq a$.

Exemplo 4. *Tomemos por exemplo o número* 1638 *o seu menor divisor é 2 então:* $1638/2 = 819$, *agora o menor divisor é* 3 *e daí* $819/3 = 273$ *daí* $273/3 = 91$ *daí* $91/7 = 13$ *daí* $13/13 = 1$ *dessa forma temos* $1638 = 2 \times 3 \times 3 \times 7 \times 13$ *não havendo outra forma senão pela troca de ordem dos fatores.*

Observação 3.3. *Agora utilizando TFA podemos demostrar, outra vez, que se p um número primo e* $p|a \times b$ *se e somente se* $p|a$ *ou* $p|b$, *basta decompor a e b em fatores primos algum deles (ou os dois) terá de ter o fator primo p.*

3.5.1 Método de fatoração de Fermat

Por fim apresentaremos nessa seção este método simples que nos permite fatorar um número impar identificando até se ele é um número primo. O método consiste basicamente em: dado um número natural ímpar N, vai se somando a ele os primeiros números impares $L = \{1, 3, 5, ..\frac{N-1}{2}\}$ em cada linha. Até se encontrar um quadrado perfeito n^2 neste momento temos:

$$N = (n + L)(n - L)$$

.Caso seja a ultima linha um quadrado perfeito, ou seja, a linha $L = \frac{N-1}{2}$ temos que N é um número primo.

Agora vejamos um exemplo:

Exemplo 5. *Seja* $N = 33$ *temos que:*

$$1 : 33 + 1 = 34$$

$$2 : 34 + 3 = 37$$

$$3 : 37 + 5 = 42$$

$$4 : 42 + 7 = 49 = 7^2$$

logo temos: :

$$33 = (7 - 4) \times (7 + 4)$$

Não é um número primo.

Exemplo 6. *Seja* $N = 43$ *temos que:*

$$1 : 43 + 1 = 44$$

$$2 : 44 + 3 = 47$$

$$3 : 47 + 5 = 52$$

$$.$$

$$.$$

$$22 : 441 + 43 = 484 = 22^2$$

Logo temos:

$$43 = (22 + 21) \times (22 - 21)$$

Um número primo.

3.6 MDC e MMC

Definição 3.5. *Dados dois ou mais números inteiros (que não sejam nulos ao mesmo tempo) chamamos de MDC desses dois ou mais números ao maior divisor comum a ambos.*

Existência: Considere os divisores desses números pelos menos teremos o 1 como elemento comum.

Unicidade: Como o conjunto dos divisores de qualquer inteiro é limitado temos que o conjunto formado pela interseção desses conjuntos também é limitado, logo haverá um maior elemento.

Exemplo 7.

$$D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

$$D(18) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$$

$$D(12) \cap D(18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

Logo o $mdc(12, 18) = 6$.

Pela definição dada acima o mdc entre dois ou mais números sempre sera um número positivo afinal sendo o número 1 sempre um dos divisores de qualquer número, com certeza o mdc será maior ou igual a unidade. Por outro lado um número jamais vai poder ser dividido por um valor maior que seu valor absoluto pela definição de divisibilidade logo, podemos escrever:$1 \leq mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b) \leq min(|a|, |b|)$.

Definição 3.6. *Dados dois ou mais números inteiros (todos não nulos), chamamos de seu MMC ao menor múltiplo positivo comum a eles.*

Existência: Considere os múltiplos desses números teremos pelos menos como elemento comum o produto dos números dados.

Unicidade: Como o conjunto dos múltiplos positivos são naturais temos que o conjunto formado pela interseção desses conjuntos também é limitado, logo haverá um menor elemento.

Exemplo 8.

$$M(12) = \{\pm 12, \pm 24, \pm 36, \pm 48, \pm 60, \pm 72, ...\}$$

$$M(18) = \{\pm 18, \pm 36, \pm 54, \pm 72, ...\}$$

$$M(12) \cap M(18) = \{\pm 36, \pm 72, \pm 108, ...\}$$

Logo o $mmc(12, 18) = 36$.

Por definição o mmc tem que ser positivo e como é um múltiplo comum aos números dados temos que o mmc de dois ou mais números não poderá ser menor que o valor absoluto do menor valor sobre os quais se calcula o mmc. Por outro lado sempre vai ser menor ou igual ao módulo do produto de todos os valores envolvidos. Para o caso de dois valores a e b temos:$min(|a|, |b|) \leq mmc(a, b) = mmc(-a, b) = mmc(-a, -b) \leq |a.b|$.

Lema 3.3. *Se* $a = bq + r$, *então* $mdc(a, b) = mdc(b, r)$.

Demonstração: 7. *Se* $c = mdc(a, b)$ *temos* $c|a$ *e* $c|b$, *logo* $c|a - bq \leftrightarrows c|r$ *e portanto* $c \in Db \cap Dr$. *Da mesma forma, se* $c \in Db \cap Dr$ *temos* $c|b$ *e* $c|r$, *logo* $c|bq + r \Leftrightarrow c|a \quad e \quad assim \quad c \in Db \cap Dr$.

3.7 Algoritmo de Euclides

O algoritmo de Euclides é um método que tem por finalidade determinar o mdc entre dois números inteiros dados e que por fim irá determinar a solução de Equações Diofantinas que são equações da seguinte forma: $a.x + b.y = c$ com a, b, c inteiros assunto tratado no capítulo "A importância dos números primos". É um método simples de possível inserção no Ensino Fundamental, e uma ferramenta útil no Ensino Fundamental e Médio. O método segue a seguinte regra: divide-se o maior pelo menor, este pelo primeiro resto obtido, em seguida o segundo resto pelo primeiro e assim sucessivamente até encontrar um resto nulo, nesse ponto o ultimo resto encontrado diferente de zero é o mdc procurado. Este metodo se baseia no seguinte lema:

Lema 3.4. *Seja* a *e* b *tais que* $a = b.q + r$, *com* $r \geq 0$ *então* $mdc(a, b) = mdc(b, r)$.

Demonstração: 8. *Se* $mdc(a, b) = d$ *então* $d|(a - b.q)$, *logo* $d|r$ *e sendo assim* $d|b$ *e* $d|r$, *mas se existe um* c *que divida* b *e* r *então* $c|b.q + r$ *logo* $c|a$ *então* $c \leq d$.

Observação 3.4. $mdc(a, b) = mdc(b.r_1) = mdc(r_1, r_2) = \ldots = mdc(r_{n-1}, r_n)$.

Observação 3.5. *Se $b|a$ então $mdc(a,b) = b$.*

Exemplo 9. *Vamos determinar o $mdc(963, 657)$. Dai temos:*

$$963 = 657 \times 1 + 306$$

$$657 = 306 \times 2 + 45$$

$$306 = 45 \times 6 + 36$$

$$45 = 36 \times 1 + 9$$

$$36 = 9 \times 4 + 0$$

Logo o mdc procurado é 9 que pode ser escrito como uma combinação linear dos números 963 e 657 da seguinte forma:

$$9 = 45-36 = 45-(306-45\times6) = -306+7\times45 = -306+7\times(657-306\times2)$$

$$= 7 \times 657 - 15 \times (963 - 657) = 963 \times (-15) + 657 \times 2$$

ou seja, $963 \times (-15) + 657 \times 2 = 9$

3.8 Fatorial

Definição 3.7. *O fatorial de um numero natural n é definido por $n!$ onde*

$$n! = 1.2.3...n \tag{3.2}$$

Exemplo 10. $3! = 1.2.3 = 6$ *e* $1! = 0! = 1$.

3.9 Teorema de Wilson

Proposição 3.5. *Seja p um número natural diferente de 1 tal que:*

$$p|[(p-1)! + 1] \tag{3.3}$$

Então p é primo.

Demonstração: 9. *Se p é menor do que 6, ele não pode ser composto, pois 4 não divide 7, ou seja, $4 \nmid [3!+1]$. Se p e maior ou igual a 6, ele também não pode ser composto, pois se n e um número composto maior ou igual a seis, $n|(n-1)!$ pois seja $n = a.b$, um produto de dois inteiros (a e b) tal que $1 < a, b < n$. Se a e b são distintos, eles são fatores distintos do fatorial acima, donde segue o resultado. Se b e igual a a, quer dizer que n e igual a a^2 e que a e um fator do fatorial acima. Vamos mostrar agora que $2a$ e um fator distinto do mesmo fatorial, o que e suficiente para o que foi pedido. Como a é maior do que dois: $2 < a < 2a < a^2 = n$. Se p é composto então $p|(p-1)!$ logo $p \nmid [(p-1)!+1]$.*

Exemplo 11. *Uma das aplicações mais conhecidas é dada a seguir: Seja:*

$$K = M \times (N+1) - (N!+1) \tag{3.4}$$

com M e N naturais. em seguida aplica-se :

$$P = \frac{1}{2} \times (N-1)[|K^2-1| - (K^2-1)] + 2 \tag{3.5}$$

Nesta aplicação os primos P aparecem muito lentamente, ou seja, para $M = 1$ e $N = 2$ temos o primo $P = 3$, para $M = 5$ e $N = 4$ temos o primo $P = 5$, para achar o primo $P = 7$ temos que ter $M = 103$ e $N = 6$, e para o primo $P = 11$ temos $M = 329891$ e $N = 10$. Isso deve-se ao fato de que a expressão $|K^2-1|-(K^2-1)$ só assumir dois valores:0 ou 2, respectivamente para $K \neq 0$ e para $K = 0$. Sendo assim temos que fazer escolhas adequadas para M e N utilizando o teorema de Wilson. Pois para termos $K = 0$ na primeira formula teremos:

$$M \times (N+1) = N!+1 \tag{3.6}$$

Ou seja, $(N+1)|(N!+1)$ o teorema de Wilson. Desta forma no momento que se escolher para N um valor igual a um número primo menos 1 acha-se M e temos para P um primo.

3.10 Congruência

Definição 3.8. *Seja a,b e m naturais temos que se* $m|(a-b)$ *ou* $m|(b-a)$ *escrevemos:* $a = b(mod\, m)$ *ou* $b = a(mod\, m)$

Proposição 3.6. *Se* $a = b(mod m)$ *e* $c = d(mod m)$ *então* $a.c = b.d(mod m)$

Demonstração: 10. *Se* $m|(a-b)$ *e* $m|(c-d)$ *então* $m|a.(c-d)+d.(a-b)$ *então* $m|(a.c-b.d)$ *escrevemos* $a.c = b.d\ (mod\, m)$.

Consequência: *logo* $a = b(mod\, m) \Leftrightarrow\ a.n = b.n(mod\, m)$.

Proposição 3.7. *Se* $m|(a-b)$ *e* $m|(c-d)$ *então* $a \pm c = b \pm d\ (mod\, m)$

Demonstração: 11. $m|[(a-b)+(c-d)] \Rightarrow m|[(a+c)-(b+d)] \Rightarrow (a+c) = (b+d)(mod\, m)$ *da mesma forma como* $m|(d-c)$ *temos* $m|(a-c)-(b-d)$ *sendo assim* $(a-c) = (b-d)(mod\, m)$.

Consequência: *Se* $a \pm c = b \pm c(mod\, m) \Leftrightarrow a = b(mod\, m)$.

Proposição 3.8. *Se* $a.c = b.c\ (mod\ m)$ *e o* $mdc(c,m) = d$ *então* $a = b\ (mod\, m/d)$.

Demonstração: 12. *Observe que se* $a.c = b.c(mod m)$ *então* $m|(a.c-b.c) = c.(a-b)$ *dado* r *e* s *tal que* $m = r.d$ *e* $c = s.d$ *e* $mdc(r,s) = 1$ *logo* $r.d|s.d(a-b)$ *logo* $r|s.(a-b)$ *logo* $r|(a-b)$ *então* $a = b\ (mod\, r)$ *ou seja* $a = b(mod\, m/d)$.

Consequência: *Seja* $a.c = b.c(mod m)$ *de tal modo que* $mdc(m,c) = 1$ *vale a simplificação* $a = b\ (mod\, m)$.

3.11 Pequeno Teorema de Fermat

Lema 3.5. *Se* p *é primo e não divide a então* $p|a^{p-1} - 1$ *então escrevemos:*

$$a^{p-1} = 1(mod p) \tag{3.7}$$

Demonstração: 13. *Sejam os múltiplos positivos de* a, $\{a, 2a, 3a, 4a, ..., (p-1)a\}$ *todos eles não são divisíveis pelo primo* p *e são incongruentes* 2 *a* 2,

ou seja, dado r e s tal que $1 \leq r < s \leq p-1$ então p não divide $r-s$ logo também não divide $ar-as$. Sendo assim os $a, 2a, 3a, 4a, ..., (p-1)a$, cada um deles é congruente a algum dos termos $1, 2, 3, 4..., p-1$. Daí podemos escrever:

$$a, 2a, 3a, 4a, ..., (p-1)a = 1.2.3.4...(p-1) \ (mod\, p)$$

$$a^{p-1}.(p-1)! = (p-1)! \ (mod\, p)$$

$$a^{p-1} = 1 \ (mod\, p)$$

Exemplo 12. *Seja $p = 7$ e $a = 8$, temos $8.1, 8.2, 8.3, 8.4, 8.5, 8.6$. Teremos $8.1 = 1(mod\ 7)$, $8.2 = 2(mod\ 7)$, $8.3 = 3(mod\ 7), 8.4 = 4(mod\ 7)$, $8.5 = 5(mod\ 7)$ e $8.6 = 6(mod\ 7)$. Logo temos :*

$$8.1.8.2.8.3.8.4.8.5.8.6 = 1.2.3.4.5.6 \ (mod\, 7)$$

$$8^6.1.2.3.4.5.6 = 1.2.3.4.5.6 \ (mod\, 7)$$

$$8^6.6! \ = 6! \ (mod\, 7)$$

$$8^6 = 1 \ (mod\, 7)$$

Proposição 3.9. *Se p é um primo qualquer e seja a um inteiro então $p|a^p - a$ então escrevemos:*

$$a^p = a(mod\, p) \tag{3.8}$$

Demonstração: 14. *Podemos escrever $p|a^p - a$ ou $p|a.(a^{p-1} - 1)$ então $p|a$ ou $p|a^{p-1} - 1$ pelo lema anterior.*

3.12 Classes Residual Modulo m

Definição 3.9. *Seja $\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}$ onde $[n] = \{mk + n; k \in \mathbb{Z})\}$ chamado de sistema completo de resíduo modulo m.*

Exemplo 13. *Para $m = 3$, ou seja, $\mathbb{Z}_3$ temos:*

$$[0] = \{... - 6, -3, 0, 3, 6, 9, 12, 15, ...\} = 3k + 0$$

$$[1] = \{... - 5, -2, 1, 4, 7, 10, 13, 16, ...\} = 3k + 1$$

$$[2] = \{... - 4, -1, 2, 5, 8, 11, 14, 17, ...\} = 3k + 2$$

Proposição 3.10. *Dada uma classe residual modulo m, $\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}$ a união $[0] \cup [1] \cup [2], ..., \cup [m-1]$ é o conjunto dos inteiros e a interseção $[1] \cap [2]...[m-2] \cap [m-1]$ a dois é vazia.*

Exemplo 14. *Conforme o conjunto $\mathbb{Z}_3$ a união de $[0] \cup [1] \cup [2] = \mathbb{Z}$ (conjunto dos inteiros) e interseção dois a dois dos conjuntos $[0], [1] e [2]$ é vazia.*

Operações: *Adição: $[a] + [b] = [a + b]$ Multiplicação: $[a] \times [b] = [a \times b]$*

Exemplo 15. *Para $\mathbb{Z}_3$ temos: $[1]+[2] = [1+2] = [0]$ e $[2]\times[2] = [2\times2] = [1]$.*

Definição 3.10. *Um elemento $[a] \in \mathbb{Z}_m$ é chamado de invertível quando existe um $[b] \in \mathbb{Z}_m$ de forma que $[a] \times [b] = [1]$ com a e b diferente de zero.*

Exemplo 16. *Em $\mathbb{Z}_m$ temos : $[1] \times [1] = [1]$, $[2] \times [2] = [1]$.*

Observação 3.6. *Seja p primo no conjunto $\mathbb{Z}_p^* = \{[1], [2], ..., [p-1]\}$ todos os elementos são invertíveis e o produto de quaisquer dois elementos desse conjunto nunca é $[0]$. Por outro lado seja m onde $\mathbb{Z}_m^* = \{[1], [2], ..., [m-1]\}$ não primo haverá pelo menos dois elementos desse conjunto cujo produto seja $[0]$.*

Exemplo 17. *Em*

$$\mathbb{Z}_4 : \ [2] \times [2] = [0] \quad \mathbb{Z}_6 : \ [2] \times [3] = [0]$$

.

$$\mathbb{Z}_8 : \ [2] \times [4] = [0] \quad \mathbb{Z}_9 : \ [3] \times [3] = [0]$$

.

3.13 Curiosidades sobre números primos e compostos

Nesta seção é tratado sob a forma de observação algumas curiosidades sobre números primos e compostos, citando algumas conjecturas que ainda não foram provadas.

Primos gêmeos são inteiros positivo ímpares consecutivos que são primos por exemplo: 17 *e* 19, 29 *e* 31, 41 *e* 43,.., 857 *e* 859,.., 22961 *e* 22963,.., 140.737.488.353.699 *e* 140.737.488.353.701. *Não se sabe ainda a existência desses pares de números primos é infinita.*

O menor número primo é o 2 *e é o único primo par, e o menor número natural composto é o* 4. *Os primeiros números primos são:* $\{2, 3, 5, 7, 11, 13, 17, 19, ...\}$.

Todo número inteiro par maior que 4 *é a soma de dois primos (Conjectura de Goldbach) como se observa:* $6 = 3 + 3$; $8 = 3 + 5$; ...; $20 = 3 + 17$.... *essa conjectura já foi verificada para acima dos* 100.000 *primeiros números naturais e é utilizada como verdadeira mesmo sem a demonstração.*

Temos também que todo inteiro impar $n > 5$ *pode ser escrito na forma:* $n = p + 2 \times q$ *onde* p *e* q *são primos (Conjectura de Lagrange) como se observa:* $7 = 3 + 2 \times 2; ...; 29 = 7 + 2 \times 11; ....; 47 = 13 + 2 \times 17; ...; 71 = 13 + 2 \times 29$;... *também essa propriedade é utilizada sem demonstração.*

A soma de números pares é sempre um número par logo não é primo. Por outro lado a soma de uma quantidades par de números impares é par logo não é primos (exceção 1+1), e também a soma dos primeiros números impares é um quadrado perfeito logo não é primo.

Conjectura de TSCHEBISCHEFF onde afirma que para todo inteiro $n > 3$ *existe pelo menos um primo entre* n *e* $2.(n - 1)$.

Exemplo 18. *Para* $n = 4$ *temos* $p = 5$; *para* $n = 5$ *temos* $p = 7$;

para $n = 6$ *temos* $p = 7$; *para* $n = 7$ *temos* $p = 11$;

para $n = 8$ *temos* $p = 11$ *e* $p = 13$

O número p *é um primo de Sophie Germain se* $2p + 1$ *também for um número primo. Atualmente conjectura-se que existam infinitos primos de Sophie Germain, mas ainda também não se conseguiu demostrar. Um fato*

interessante sobre este tipo de número é que se p é um primo de Sophie Germain, então existem inteiros x, y e z, diferentes de zero, tais que $x^p + y^p = z^p$. *Este é o primeiro caso para o último teorema de Fermat. Demostração essa que não cabe neste trabalho.*

Por fim uma sequência curiosa de alternância de números primos e números compostos:

91 *composto*

9901 *primo*

999001 *composto*

99990001 *primo*

9999900001 *composto*

999999000001 *primo*

99999990000001 *composto*

9999999900000001 *primo*

.

Ocorrendo assim uma curiosa sequência de números primos e composto da seguinte forma:

$$N = 10^{2n} - 10^n + 1$$

onde n natural. E se n-impar o número N é composto e se n-par então o N é primo.

Capítulo 4

Existem infinitos números primos?

Neste capítulo iremos demostrar a existência de infinitos números primos e dentro de uma narrativa histórica analisar a sua distribuição no conjunto dos números naturais.

Proposição 4.1. *Existe uma infinidade de números primos.*

Demonstração: 15. *Suponha que exista apenas uma quantidade n de números primos sejam eles* $p_1, p_2..., p_n$ *e também seja* $N = p_1.p_2....p_n \pm 1$. *Se* N *é primo então temos um primo diferente de* $p_1, p_2, ...p_n$ *caso* N *composto seja* p *um primo tal que: se* $p|N$ *e* $p \in \{p_1, p_2, ...p_n\}$ *então* $p| \pm 1$ *sendo assim* $p = \pm 1$ *o que contraria o fato de p ser primo logo p é diferente de* $p_1, p_2, ...p_n$.

Faremos agora duas outras demostração:

Demonstração: 16. *Podemos também demostrar a infinitude como se segue:seja N um natural resultado do produto de todos os n primos e como o* $m.d.c(N, N-1) = 1$ *logo os fatores primos de N e* $N-1$ *são distintos, então existe p primo diferente dos* $p_1, p_2, ..., p_n$ *que divide* $N-1$, *dai segue também a infinitude dos números primos.*

Demonstração: 17. *para cada número natural* $n > 1$ *defina* $x(n) = n! + 1$. *Como* $x(n)$ *é um número natural (para cada n natural) , então existe um primo p fator de* $x(n)$. *Esse primo p não pode dividir um número menor do que ou igual a n, pois neste caso, dividiria n! e daí, dividiria* $x(n) - n! = 1$ *então dividiria a unidade o que é uma contradição. Sendo assim dado*

qualquer natural $n > 1$, sempre existe um primo $p > n$ concluindo então que há uma infinidade de números primos!. Esta demostração se deve ao matemático francês Charles Hermite que viveu de 1822 a 1901.

Proposição 4.2. *Seja n número natural com $n > 4$ ele será composto se e somente se $n|(n-p)!$ onde p é o menor divisor primo de n.*

Demonstração: 18. *Provaremos inicialmente que n composto divide $(n-1)!$.De fato, suponha que $n = n_1.n_2$ com $n_1 < n$ e $n_2 < n$. Se $n_1 \neq n_2$,podemos supor que $n_1 < n_2$, e portanto, $(n-1)! = 1...n_1....n_2....(n-1)$; o que mostra que $n|(n-1)!$, neste caso. Suponhamos que $n_1 = n_2 > 2$. Logo, Suponhamos que $n_1 = n_2 > 2$. Logo, $(n-1)! = 1....n_1....2 \times n_1.....(n-1)$; o que implica também que $n = n_1 \times n_1$ divide $(n-1)!$. Agora, note que $m.d.c(n; n-1) = 1$ e que $n|(n-2)!(n-1)$; portanto, $n|(n-2)!$. Generalizando como se segue: Seja p o menor número primo que divide n; então, $n|(n-p)!$ De fato, temos que $m.d.c(n-1; n) = 1$; $m.d.c(n-2; n) = 1$ e $m.d.c(n-(p-1), n) = 1$; ,. Logo, segue que $((n-1)(n-2).....(n-p+1); n) = 1$, o que, em vista do fato de $n|(n-1)!$ Então se conclui que $n|(n-p)!$.*

É possível gerar números compostos de várias maneiras dentre as mais interessantes é gerar uma quantidade finita de números compostos consecutivos utilizando o seguinte recurso: Dado n natural maior ou igual a 2 temos $(n+1)!+2$, $(n+1)!+3$,...,$(n+1)!+(n+1)$ todos números compostos e divisíveis por $2, 3, 4, ..., n+1$ essa sequencia de números naturais consecutivos onde não aparecem nem um número primo são chamados de desertos de números primos.

Exemplo 19. *Seja $4!+2$, $4!+3$ e $4!+4$; são números compostos consecutivos. Caso tivéssemos escolhido um natural maior que 3 teríamos encontrado uma sequencia muito maior de números compostos.*

Isso mostra que apesar dos números primos serem infinitos a medida que os números crescem encontramos maiores desertos de números primos ficando cada vez mais rara a sua frequência.

4.0.1 A Distribuição dos Números Primos

Utilizando uma narrativa histórica apresentaremos um modelo capaz de mostrar a distribuição dos números primos de 1 a N natural de acordo com o texto abaixo da referencia [25].

Muitos matemáticos ao longo do tempo estiveram dedicados tentando resolver dois problemas um era localizar de forma precisa o próximo primo a partir da posição de um primo conhecido, e o outro era de determinar quantos primos existiam entre 1 e N. Entre eles, Gauss, que se dedicou a saber quantos primos existiriam entre 1 e um número N qualquer. Afirma-se que Tal percepção tenha sido motivada pela leitura de um livro de logaritmos que continha na sua contracapa uma tábua de números primos nessa oportunidade percebeu, então, que parecia haver uma forte regularidade. Nessa oportunidade ele foi estudar uma função, que posteriormente foi denotada por $\pi(x)$, definida como o número de primos p tais que $p \leqslant x$, chamada de função de contagem dos números primos. Assim temos:

Exemplo 20. $\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, *etc. Não é necessário que* x *seja um número natural,* $\pi(\sqrt{2}) = 0$, $\pi(e) = 1$, $\pi(\pi) = 2$, *etc. Desse modo, a proporção de números primos entre* 1 *e* x *é dada por* $\pi(x)/x$.

Dessa forma foi feita uma análise do comportamento deste quociente para uma quantidade relativamente grande de números naturais, dessa forma Gauss buscou encontrar uma função de comportamento bem conhecido que se aproximasse de $\pi(x)/x$ para x suficientemente grande. Com uso dos computadores atuais construiu-se a Tabela abaixo alguns valores do quociente $x/\pi(x)$.

Na época foram construídas varias tabelas muitas utilizadas e construídas por Gauss. Ele observou que, sempre que multiplicava seu espaço amostral por 10, o valor do quociente $x/\pi(x)$ era acrescido em cerca de $2,3$.

Essa propriedade de transformar produtos em somas é a que caracteriza

x	π(x)	x/ π(x)
10	4	2,5
100	25	4,0
1000	168	6,0
10.000	1229	8,1
100.000	9592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.511	22,0

Figura 4.1: A Distribuição dos Números Primos

as funções logarítmicas. Logo se levou a crer que, então, haveria uma base a de modo que: $x/\pi(x) = log_a x \Leftrightarrow \pi(x)/x = 1/log_a x$ Analisando tabelas, concluiu-se que essa base poderia ser o numero e, e assim conjeturou:

$$\pi(x)/x \approx 1/lnx \Leftrightarrow \pi(x) \approx x/lnx \tag{4.1}$$

Em 1896, Poussin e Hadamard, independentemente, demonstraram que:

$$\lim_{x\to\infty} \frac{\pi(x).lnx}{x} = 1 \tag{4.2}$$

Esse resultado ficou conhecido como Teorema dos Números Primos, provando a igualdade assintótica das duas funções. A demonstração desse teorema é bastante difícil e não será apresentada neste trabalho pois utiliza ferramentas de Análise Complexa que não tem significado neste compendio apesar de ser uma área que atualmente é muito importante no desenvolvimento da Teoria dos Números.

Em 1949, Selberg recebeu a Medalha Fields, um dos maiores reconhecimentos de um matemático, por ter simplificado de forma substancial a demonstração original desse teorema. Por meio dele, podemos obter uma boa aproximação para o n-esimo número primo p_n, vendo que:

$$p_n = n.ln(n) \tag{4.3}$$

Inconformado com a aparente incorreção da estimativa de Gauss, e analisando as tabelas de primos existentes até então, Legendre apresentou o que seria uma melhoria na estimativa, onde Legendre substituiu a aproximação $\frac{N}{lnN}$ por $\frac{N}{lnN-1,08366}$, introduzindo assim uma pequena correção que tinha o efeito de desviar a curva de Gauss em direção ao número verdadeiro de primos. Considerando-se os valores dessas funções situados dentro do alcance computacional da época, era impossível distinguir os gráficos de $\pi(N)$ da estimativa de Legendre. Além do mais, no século XIX havia uma grande preocupação com a aplicação prática da matemática, que deveria dar resultados mais precisos quanto possível, independentemente do método empregado, o que pesava a favor da estimativa de Legendre. O termo $1,08366$ introduzido na fórmula, porém, era pouco consistente, e considerado totalmente artificial, o que fez com que alguns matemáticos acreditassem que deveria haver algo melhor e mais natural. Anos mais tarde, o próprio Gauss apresentou um refinamento na sua estimativa, que ficou conhecida como a integral logarítmica, denotada por:

$$\int_2^n 1/ln(x)dx \tag{4.4}$$

Segundo a justificativa teórica da nova estimativa de Gauss baseava-se na ideia de probabilidade. Como a distribuição (dos primos) parecia tão aleatória, o lançamento de uma moeda talvez fosse um bom modelo para a escolha dos primos. [...] Porém, pensou Gauss, a moeda teria que ser viciada, de modo que não caísse em cara a metade das vezes, e sim com a probabilidade de $\frac{1}{ln(N)}$. Assim como, em N lançamentos de uma moeda não viciada, espera-se que o número de caras seja $\frac{1}{2} + \frac{1}{2} + ... + \frac{1}{2}$ com total de n-termos. Gauss supôs que, para a moeda viciada dos primos, o número de caras, ou seja, o número de primos até N, seria algo como: $\frac{1}{ln2} + \frac{1}{ln3} + \frac{1}{ln4} + ... + \frac{1}{ln(N)}$.
Considerando cada um destes termos como a área de um retângulo com base

igual a 1 e altura igual a $\frac{1}{ln(n)}$, para $n = 2, ..., N$, Gauss seguiu os passos naturais que o levaram até a integral logarítmica, que é a área exata sob a curva $\frac{1}{ln(x)}$, limitada pelas retas $x = 2$, $x = N$ e o eixo-x. Dessa forma assim foi possível comparar as estimativas sobre a quantidade de primos até x.

x	Erro (%) de **x/ ln x**	Erro (%) de ***x*/(ln *x*- 1,08366)**	Erro (%) de **∫lt/ln t**
10	8,57	105,10	28,00
10^2	-13,14	13,59	16,32
10^3	-13,83	2,20	5,10
10^4	-11,65	0,12	1, 31
10^5	-9,44	-0,04	0,38
10^6	-7,79	0,06	0,16
10^7	-6,64	0,08	0,05
10^8	-5,77	0,11	0,01
109	-5,09	0,14	0,003
10^{10}	-4,56	0,15	0,0007

Figura 4.2: A Distribuição dos Números Primos

A nova estimativa de Gauss passou a ser mais precisa do que a de Legendre, a medida que as tabelas de números primos começaram a ficar mais extensas.

A análise teórica de Gauss havia triunfado sobre a tentativa de Legendre de manipular sua fórmula para se adequar aos dados disponíveis, segundo a tabela acima. Prevalecendo até os dias atuais.

Capítulo 5

A importância dos Números Primos

É natural perceber a importância dos números primos em várias aplicações matemáticas tanto na álgebra, aritmética e geometria. A presença desses números nos permite ver até aonde podemos simplificar os processos, a identificar unicidades e até em alguns casos determinar a impossibilidade.

Primeira Aplicação:

Buscando o caso em que os números primos tornam sempre possível a solução de um problema, podemos citar o caso, por exemplo, das equações diofantinas em que toda equação diofantina na forma $a.x + b.y = c$ com a, b, c constantes inteiras, só haverá solução, ou seja,só haverá valores x e y que atendam a equação, se e somente se c for um múltiplo do $\text{mdc}(a, b)$ sendo assim sempre haverá solução se o $\text{mdc}(a, b) = 1$ e isso sempre vai acontecer se a ou b for um número primo, ou se forem primos entre si, nesse caso a equação terá sempre solução independente do valor de c. Se também a e b forem números de Fermat também atende para qualquer c conforme veremos no capítulo 7.

Segunda Aplicação:

Um caso em que os números primos são determinantes, seja $\mathbb{Z}_m$ a classe residual modulo m (natural), ou seja, $\mathbb{Z}_m = \{[0], [1], [2], .., [m-1]\}$,onde $[r]$ são todos os números naturais que divididos por m da resto r. $\mathbb{Z}_m$ é um corpo se, e somente se, m é primo, pois nesse caso todos os seus elementos

diferentes de zero são invertíveis, dessa forma o conjunto $\mathbb{Z}_m$ deixa de ser um anel e passe a ser um corpo.

Terceira Aplicação:

Se formarmos um produto de frações onde os numeradores são os números primos $\{3, 5, 7, 11, ...\}$ e os denominadores são os vizinhos do numerador desde que seja diferente de um múltiplo de 4 achamos uma forma de determinar o valor π . Assim temos $\frac{3}{2} \times \frac{5}{6} \times \frac{7}{6} \times \frac{11}{10} \times \frac{13}{14} .... = \frac{\pi}{2}$.

Quarta Aplicação:

Hoje em dia a grande aplicação dos números primos é na criptografia. Bem vamos a uma breve explicação, Para interpretar uma mensagem codificada, temos duas formas: decodifica-la ou decifra-la Decifrar significa interpretar uma mensagem codificada sem possuir a receita de decodificação. Obviamente, esta opção é utilizada por quem não é o destinatário legítimo da mensagem. Assim, o objetivo dos criadores de códigos criptográficos é dificultar ao máximo o trabalho dos decifradores. Hoje em dia é muito utilizado um sistema de criptografia conhecido como RSA. Em breves palavras o RSA funciona da seguinte forma:

1. Escolhemos dois números primos p e q.
2. Para codificar uma mensagem, utilizamos o número $n = p \times q$.
3. Para decodificar uma mensagem, precisamos conhecer p e q.

Como já foi dito, a segurança do método reside na dificuldade de fatorar n, ou seja, na dificuldade de se obter p e q, mesmo possuindo n. Isto é fácil de se compreender, quando se está falando de números grandes, com centenas de algarismos, como os que são usados atualmente para a segurança da Internet pela criptografia RSA. Números grandes pois apesar de apresentarem algum trabalho para um ser humano decompostos facilmente e rapidamente por um computador de mesa com software adequado.

Capítulo 6

Esse Número é Primo ?

Mesmo sabendo que existem infinitos números primos na maioria das vezes não é muito fácil concluir que um determinado número é primo ou não, a tarefa se torna ainda mais difícil quanto maior for o número.

Ao longo do tempo foram desenvolvidos alguns métodos que ajudam nessa tarefa, mas em geral não tem uma aplicação pratica razoável para alunos do ensino médio, esses métodos muitas vezes precisam da utilização de computadores e boas calculadoras para realização de cálculos repetitivos e enfadonhos, afastando assim os alunos e professores deste tema. Neste capitulo colocaremos algumas ideias que podem ajudar a estruturar o estudo deste assunto.

A partir desse momento vamos traçar discussões que facilitarão o entendimento do que foi dito acima.

Metodo: Seja N um número natural composto de forma que podemos escrever $N = a \times b$ e sem perda de generalidade seja, $1 < a \leqslant b$, sendo assim temos, $a^2 \leq N$ logo $a \leq \sqrt{N}$, dessa forma observamos que basta dividirmos o numero N por todo os primeiros números primos $p \leq a$, se nenhum deles dividir N de forma inteira temos que N é primo.

Exemplo 21. *Seja* $N = 1517$ *e sua raiz* $38 < \sqrt{N} < 39$*, logo os primos a serem considerados são* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$*. Nos casos de* $2, 3, 5$ *usando critério de divisibilidade é direto, nos números maiores se realiza da seguinte maneira, por exemplo para o* 17 *temos:* $1517 - 17 \times 100 = -183 + 10 \times 17 = -13$ *logo não divisível por* 17*, procedendo assim para cada*

primo chegamos que em $1517 = 37 \times 41$*, logo* 1517 *não é primo.*

Podemos também utilizar algumas outras regras de divisibilidade por números primos que permitiram facilitar a identificação se o numero natural qualquer N é um numero primo. De acordo com o texto "Outros critérios de divisibilidade"de Mario Gustavo Pinto Guedes, referência [2], podemos usar o seguinte critério de divisibilidade:

Lema 6.1. *Seja o número* m *um número natural e* k *um número inteiro, escrito da seguinte forma* $m = a + k \times b$*, onde* a *é o número* m *sem o algarismo das unidades e* b *o algarismo da unidade, se esse número* m *é divisível pelo primo* $p > 5$*, então para uma escolha conveniente de* k*, se* $p|m$ *então* $p|(a + k \times b)$*.*

Demonstração: 19. *Se* $m = a \times 10 + b = 10 \times (m - k \times b) + b$ *o que implica em* $m = 10 \times m + (1 - 10 \times k) \times b$*. E como* $p|m$ *escolhendo* k *convenientemente temos* $p|(1 - 10 \times k)$*. Logo se quisermos que o número seja divisível por* 7*, por exemplo, basta usar:* $k = -2$ *ou* $k = 5$ *temos então* $m = a - 2 \times b$ *ou* $m = a + 5 \times b$*.*

Exemplo 22. *Desejando saber se* $N = 1378$ *é divisível por* 7 *basta* $137 - 16 = 121$ *;* $12 - 2 = 10$ *logo não divisível por* 7 *caso fosse* $N = 1372$*, aplicando o método temos* $137 - 4 = 133$*;* $13 - 6 = 7$ *logo divisível.*

Abaixo temos uma relação para todos os números primos de 7 a 97, para identificar ser divisível pelos números dados: Utilizando o caso $a - k \times b$ temos:

Utilizando o caso $a + k \times b$ temos:

Infelizmente, para valores pequenos funciona rápido mas, por exemplo, para um número maior que 10.000 o processo não se torna tão simples e a realização de muitas contas o torna enfadonho. Consequentemente para números muito maiores se torna impraticável manualmente, e mesmo utilizando algoritmos em computadores o tempo de processamento se torna muito longo.

7: a -2b	**11: a - b**	**13: a – 9b**	**17: a – 5b**	**19: a -17b**	**23: a – 16b**
29: a – 26b	**31: a – 3b**	**37: a – 11b**	**41: a – 4b**	**43: a – 30b**	**47: a – 14b**
53: a – 37b	**59: a – 53b**	**61: a – 2b**	**67: a – 20b**	**71: a – 7b**	**73: a – 51b**
79: a – 71b	**83: a – 58b**	**89: a – 80b**	**97: a – 29b**		

Figura 6.1: Como saber se um Número é Primo

7: a + 5b	**11: a +10b**	**13: a + 4b**	**17: a + 12b**	**19: a -17b**	**23: a – 16b**
29: a – 26b	**31: a – 3b**	**37: a – 11b**	**41: a – 4b**	**43: a – 30b**	**47: a – 14b**
53: a – 37b	**59: a – 53b**	**61: a – 2b**	**67: a – 20b**	**71: a – 7b**	**73: a – 51b**
79: a – 71b	**83: a – 58b**	**89: a – 80b**	**97: a – 29b**		

Figura 6.2: Como saber se um Número é Primo

Pequeno Teorema De Fermat:

Uma outra forma é usar o pequeno teorema de Fermat, onde para todo primo p tal que p não divide a natural, temos:

$$a^{p-1} \equiv 1(mod\, p) \tag{6.1}$$

Neste caso para termos um número p primo, basta tomarmos todo a tal que $1 < a < p$, e calcularmos a formula acima. Se p for primo teremos que para todo a, $a^{p-1} \equiv 1(mod\, p)$ é verdadeiro; caso contrário indica que p é um número composto.

Observação 6.1. *No entanto, este teste falha se p for um número de Car-*

michael (falsos primos ou pseudoprimo). O menor número de Carmichael é 561. *Para provar isso, verifica-se que:*

$$a^{561} \equiv a(mod\,561)\ para\ todo\ a = 2, ..., 559$$

Mas observe que $561 = 3 \times 11 \times 17$. *Logo se mostrarmos que* $a^{561} - a$ *é divisível por* 3, 11 *e* 17 *então temos que* $561|a^{561} - a$.

Hoje em dia para determinação da primalidade de um número é feito por algoritmos em sistemas computacionais em duas classes de métodos: os determinísticos (Afirmam com 100% de certeza a primalidade de um número), e os probabilísticos. Em geral os métodos probabilísticos são mais rápidos feitos em tempo polinomial com probabilidade de 99%, enquanto os determinísticos são realizados em tempo exponencial vamos tratar neste momento finalizando este capitulo sobre dois teste o AKS e o teste de Monte Carlo de acordo com as referencias [23] e [24].

6.0.2 Metodo AKS

O AKS é o primeiro algoritmo determinístico a executar este teste em tempo polinomial.

Teorema 6.1. *Seja p número primo então:*

$$(x + a)^p = x^p + a(mod\,p) \tag{6.2}$$

Demonstração: 20. *Seja* $(x + a)^p = x^p + C_{p,1}.x^{p-1} \times a + C_{p-2} \times x^{p-2} \times a^2 + ... + a^p$ *todos os coeficientes* $C_{p,1}, C_{p,2}, ..., C_{p,p-1}$ *são todos divisíveis pelo primo p, facilmente verificável dividindo-se os binômios de uma linha n do Triângulo de Pascal por n e constatando que todos os termos são divisíveis se e somente se n é primo.*

sendo assim temos:

$$(x + a)^p = x^p + a^p(mod\,p) \tag{6.3}$$

0: 1

1: 1 1

2: 1 2 1

3: 1 3 3 1

4: 1 4 6 4 1

5: 1 5 10 10 5 1

6: 1 6 15 20 15 6 1

7: 1 7 21 35 35 21 7 1

8: 1 8 28 56 70 56 28 8 1

9: 1 9 36 84 126 126 84 36 9 1

10:1 10 45 120 210 252 210 120 45 10 1

Figura 6.3: Metodo AKS

Mas como $a^p = a(mod p)$ concluímos que $(x+a)^p = x^p + a(mod\, p)$.
Assim, para se testar a primalidade de um número p, bastaria demonstrar a congruência acima para todo a que não divide p. No entanto, tal operação pode consumir um tempo exponencial e, para contornar este problema, é proposto realizar o teste de congruência primeiro em módulo $(x^r - 1)$ e depois em módulo p da seguinte forma:

$$(x-a)^p = x^p - a(mod\, x^r - 1, p) \tag{6.4}$$

Esta segunda congruência é válida para todos os primos p e valores de a e r. Porém, é também satisfeita para alguns p não-primos para alguns valores de a e r. Por isso, ainda temos que testar muitos valores para a.

Exemplo 23. *Seja $p = 7$, $a = 2$ e $r = 3$: Agora vejamos para o primeiro polinômio:*

$$(x^7 - 2)/(x^3 - 1) = (x^4 + x)$$

resto $(x-2)$ logo $(x-2)(mod\ 7) = 5 + x$ Agora vejamos para o outro

polinômio:

$$(-128 + 448x - 672x^2 + 560x^3 - 280x^4 + 84x^5 - 14x^6 + x^7)/(x^3 - 1) =$$

$$= x^4 - 14x^3 + 84x^2 - 279x + 546$$

resto $(418 + 169x - 588x^2)(mod\, 7) = 5 + x$

Este resultado é válido sempre que p é primo.

6.0.3 Teste Monte Carlo

É um algoritmo para teste de primalidade em tempo polinomial mas não-determinístico, ou seja, para determinar se um número p grande tem uma probabilidade p de ser primo. Para tanto, escolhe-se aleatoriamente um número inteiro a no intervalo $(2, p-1)$ e aplica-se dois testes:

$$a^{p-1} = 1(mod\, p) \tag{6.5}$$

$$para\ algum\ inteiro\ k, 1 < mdc(a^{(p-1)/2k} - 1, p) < p \tag{6.6}$$

O primeiro teste é baseado no Pequeno Teorema de Fermat, enquanto o segundo procura achar um fator comum entre dois números, sendo um deles p, o que implicaria p ser composto. Se a for aprovado em ambos os testes, então p é composto. Mais da metade dos números do intervalo estão neste caso. Caso contrário, se um número a não passa no teste, então p pode ser primo com probabilidade $P = 50\%$. Neste caso, escolhe-se um novo a e aplica-se o teste também. Se o novo a também não passa no teste, a probabilidade de que p seja primo sobe para 75%; seguindo assim no máximo em 10 iterações teremos 99% de certeza sobre a primalidade do número dado.

Exemplo 24. *Utilizando o número* 5063*, ele é indicado como primo com apenas uma iteração (*50% *de certeza). Ao fazermos uma nova iteração, descobrimos que ele na verdade se trata de um número composto* $5063 = 61 \times 83$.

Observação 6.2. *Bem sendo este teste probabilístico mesmo as vezes com várias iterações é possível se chegar a resultados enganosos como por exemplo com o número* $3.215.031.751 = 151 \times 751 \times 28351$. *A probabilidade de que ele fosse primo utilizando o método é acima de* $93,75\%$.

Os testes de Monte Carlo apesar de ser probabilístico continuara a ser aplicados em softwares criptográficos por terem um desempenho superior aos outros teste. Há também outros teste de menos conhecidos que utilizam também algoritmos como os citados abaixo conforme dito na referencia [25].

6.0.4 Metodo ECPP

ECPP significa, em inglês: *curve primality proving* . Foi desenvolvido por A. O. L. Atkin e F. Morain em 1993, no artigo Ellipitc Curves and Primality Proving. Teste de primalidade modelo, criou uma nova classe de avaliação de primalidade de um número. Totalmente justificado utilizando curvas elípticas sobre corpos finitos. É determinístico, aplicável a qualquer inteiro e executado em provável tempo polinomial. Pode ser executado em computadores comuns. Apresenta resultados intermediários cuja lista é chamada de certificado de primalidade para um determinado número primo testado. Resumimos abaixo as característica deste teste:

i. O algoritmo utiliza a teoria das curvas elípticas com multiplicação sobre corpos finitos;

ii. O algoritmo tem complexidade polinomial, e possui excelente desempenho prático, pois demonstra a primalidade de números de 100 a 1.5000 algarismos;

iii. Ele realiza o teste para um número de até 400 dígitos, em poucos dias, utilizando uma estação de trabalho simples;

iv. Para números de mais de 800 dígitos é utilizado processamento distribuído em dez estações de trabalho e gasta um tempo real de uma semana;

Assim é sugerida a seguinte estratégia para um computador com uma determinada velocidade média de processamento:

1. Peneiramento e posterior fatorização dos números de pontos da curva;
2. Utilizar exponenciação módulo p ;
3. Exponenciação de uma curva elíptica módulo p ;
4. Solução de polinômios utilizando congruências módulo p ;

A análise matemática deste teste de primalidade está além das possibilidades deste trabalho. A dificuldade para analisar este tipo de prova é que em sua concepção é utilizada uma linguagem matemática bastante atual e sofisticada. O grande avanço conceitual e técnico conseguido pelos autores é a introdução das curvas elípticas no estudo dos números primos e a utilização de linguagem e resultados mais atuais sobre álgebra abstrata e sua aplicação à teoria dos números. O ECPP criou uma nova classe de testes de primalidade. As provas de primalidade utilizando curvas elípticas. Mas não deixou de utilizar congruências.

6.0.5 Algoritmo de Fatoração de Shor

Por fim citamos o algoritmo de P. Shor (Shor, 1994) que apresentou o seu algoritmo para fatoração em computadores quânticos. Não é um algoritmo para identificar se um número é primo e sim um algoritmo de fatoração. Foi elaborado para ser processado em um computador quântico, cujas bases teóricas já se havia definido. Trabalha com complexidade polinomial. Este algoritmo mostra qualquer número composto pode ser fatorado dentro de uma probabilidade suficientemente segura. É também uma metodologia probabilística. A utilização do computador quântico não está só na velocidade de processamento, mas principalmente na forma de processar, chamada de superposição quântica. Matematicamente o algoritmo está basicamente fundamentado em uma definição e duas proposições que não cabe no contexto deste compendio, onde exige um método de fatoração complexo, mas tem tempo polinomial para um computador quântico. O cálculo do mdc é feito pelo algoritmo de Euclides, que leva tempo, muito tempo.

Capítulo 7

É possível gerar Números Primos ?

Neste capitulo introduzimos os métodos criados com finalidade de se obter os números primos. Começaremos falando sobre os números primos de Fermat devido a grande importância desse matemático.

Definição 7.1. *Um número primo de Fermat é da seguinte forma:*

$$F_n = 2^{2^n} + 1 \tag{7.1}$$

Exemplo 25. *Os primeiros primos de Fermat são:* $F_0 = 3; F_1 = 5; F_2 = 17, F_3 = 257, F_4 = 65537 F_5 = 4.294.967.297 = 641 \times 6700417.$

Observação 7.1. *Os primos de Fermat podem ser escritos como:*

$$F_n - 2 = F_1 \times F_2 \times ... \times F_{n-1} \tag{7.2}$$

Demonstração: 21. *Basta observar a indução para* $n = 1$ *temos:* $F_1 - 2 = F_0$ *pois* $5 - 2 = 3$. *Considere valido* $n = p$ *natural maior que um, observe que vale para* $n = p + 1$, *pois,*

$F_{p+1} - 2 = F_1 \times F_2 \times .. \times F_{p-1} \times F_p => 2^{2(p+1)} + 1 - 2 = (F_p - 2)F_p$

$=> 2^{2(p+1)} - 1 = (2^{2p} + 1 - 2) \times (2^{2p} + 1)$

Desta forma: $2^{2(p+1)} - 1 = (2^{2p} - 1) \times (2^{2p} + 1)$

Observação 7.2. *A principal vantagem dos primos de Fermat é o fato todos os seus termos serem primos entre si é fácil provar por indução isso, partindo*

do fato que:

$$F_n - 2 = F_1 \times F_2 \times ... \times F_{n-1} \tag{7.3}$$

Pois se F_n fosse divisivel por alguns dos $F_{1...n-1}$ então o número 2 tamém seria divisivel por esse F absurdo, pois, o números 2 não é divisivel por nenhum $F_{1..n-1}$.

Observação 7.3. *Apesar da importância desses números ao longo da história eles tem a desvantagens de gerarem poucos números primos pequenos (pois os números crescem rapidamente), falha já nos primeiros números e além disso seus cálculos a mão livre são enfadonhos.*

Definição 7.2. *Números primos de Mersenne são números da forma:*

$$M_n = 2^n - 1 \tag{7.4}$$

com n-primo.

Exemplo 26. *Fornecem os seguintes números iniciais: :* $M_2 = 3, M_3 = 7, M_5 = 31, M_7 = 127$ *(este último não é primo).*

$$2^{19} - 1 = 524287$$

$$2^{61} - 1 = 2305843009213693951$$

$$2^{89} - 1 = 618970019642690137449562111$$

$$2^{107} - 1 = 162259276829213363391578010288127$$

Observação 7.4. *Vamos mostrar que o número de Mersenne $M_{83} = 2^{83} - 1$ não é primo, apesar de 83 ser primo.*

Demonstração: 22. *De fato, temos que:*

$$2^8 = 256 = 89(mod\, 167)$$

$$2^{16} = 2^8 \times 2^8 = 89.89 = 72(mod\, 167)$$

$$2^{32} = 2^{16} \times 2^{16} = 72.72 = 7(mod\, 167)$$

$$2^{64} = 2^{32} \times 2^{32} = 49 = 49(mod\,167)$$

Daí, segue-se que: $2^{83} = 2^{64} \times 2^{16} \times 2^3 = 49.72.8 = 1(mod\,167)$*; o que implica que* $2^{83} - 1$ *é divisível por* 167.

Os números de Mersenne: M_{11} , M_{23} , M_{29}, M_{37} ,M_{41}, M_{43} não são númros primos.

Observação 7.5. *Um número natural* n *é um número perfeito par se* n *for da forma* $n = 2^{p-1}(2^p - 1)$*, onde* $2^p - 1$ *é um primo de Mersenne.*

Observamos que:$M(M_2) = M_3$ *;* $M(M_3) = M_7$*;* $M(M_5) = M_{31}$*;* $M(M_7) = M_{127}$*... Mas* $M(M_{13})$ *não primo.*

Observação 7.6. *Existem atualmente* 47 *Primos de Mersenne conhecidos. Ainda não foi provado se existem finitos ou infinitos primos desse tipo.*

7.0.6 O Crivo de Erastótenes

Um dos meios mais simples de achar todos os números primos pequenos, por exemplo os menores do que 10.000.000, é usando o Crivo de Erastótenes ($\pm 240 a.c.$). Basta fazer uma lista com todos os inteiros maiores que um e menores ou iguais a n e riscar os múltiplos de todos os primos menores ou iguais à raiz quadrada de $n(\sqrt{n})$. Os números que não forem riscados são os números primos.

Exemplo 27. *Vamos determinar os primos menores ou iguais a* 20*: 1. Inicialmente faz-se a lista dos inteiros de* 2 *a* 20.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

2. O primeiro número 2 *é primo. Vamos mantê-lo e retirar todos os seus múltiplos. Desta forma, obtemos:*

2 3 5 7 9 11 13 15 17 19

3. O próximo número "livre"é o 3*, outro primo. Vamos mantê-lo e retirar*

os seus múltiplos:

$$2\ 3\ 5\ 7\ 11\ 13\ 17\ 19$$

4. O próximo número primo é 5*, porém não é necessário repetir o procedimento porque 5 é maior que a raiz quadrada de* $20(\sqrt{20} = 4,4721)$*. Os números restantes são primos, destacados abaixo:*

$$2\ 3\ 5\ 7\ 11\ 13\ 17\ 19$$

Existem outras maneiras de gerar números primos mas nenhuma delas consegue formar todos os números, nem sua aplicação gera sempre números primos. Uma forma simples de gerar novos números primos é utilizar a ideia da prova da infinitude deles:

7.0.7 Um Novo Crivo Para Gerar Números Primos

Temos um novo crivo publicado na $RPM71$ de Severino Toscano Melo - IME-USP, onde apresenta o seguinte crivo:

(1) Elimine todos os números naturais os números pares e os quadrados perfeitos. (2) Elimine também os $P^2 - I^2$ e os $I^2 - P^2$ onde P é par e I é impar sendo $|P - I| > 1$.

Após eliminar esses números os restantes são primos.

Observe que se $N = P^2 - I^2 = (P - I) \times (P + I)$ produto de dois números impares maiores que 1. Logo N é composto. Excluindo todos esses números compostos é possível obter todos os primos menores que 10.000, obtendo neste caso os 1229 primos.

Exemplo 28.

$$15 = (4 + 1)(4 - 1)$$

$$21 = (5 + 2)(5 - 2)$$

$$27 = (6 + 3)(6 - 3)$$

$$33 = (7 + 4)(7 - 4)$$

7.0.8 Com a infinitude de Números Primos

Podemos achar $P_n = p_n+1$ gerando os seguintes primos: $3, 7, 11, 31, 211, 2311, ...$

Vejamos: $P_1 = 2 + 1 = 3$; $P_2 = 2 \times 3 + 1 = 7$; $P_3 = 2 \times 3 \times 5 + 1$.... mas $P_7 = 30.031$ ja não é primo pois $30.031 = 59 \times 509$.

O método é simples fácil de utilizar mas encontra muitos primos mas nem sempre diretamente, muitas vezes é preciso fatorar o P_n em novos primos como no caso do P_7.

A partir desse momento exibiremos algumas tentativas feitas ao longo do tempo por muitos matemáticos com a intensão de se criar uma formula simples para gerar números primos de acordo com a referencia [22]. Formulas essas que nem sempre geram números primos e nem geram todos eles, vejamos:

NÚMERO PRIMO DE PRIERPONT...

Os números primos de Prierpont foram assim chamados em homenagem a James Prierpont. Os números primos Prierpont são todos que tem a forma:

$$2^a \times 3^b + 1 \tag{7.5}$$

Com a e b naturais. Tem-se encontrado vários números primos de Prierpont. Observa-se que todo número primo é da forma: $6 \times k \pm 1$ com k um número natural caso de $a = b$. Aplicando $b = 0$ encontramos alguns números primos de Fermat.

NÚMERO PRIMO DE PROTH...

Os primos de Proth. são Aqueles número primos que tem a forma:

$$k \times 2^n + 1 \tag{7.6}$$

Com k e n naturais. Estes números primos são um caso especial dos números primos de Prierpont. Todos iguais que os números primos de Cullen. E para $k = 1$ achamos também primos de Fermat.

NÚMEROS PRIMOS DE CULLEN...

São todos aqueles primos que se escrevem da forma:

$$n \times 2^n + 1 \tag{7.7}$$

Com n natural.

É um caso particular da fôrmula de Proth obtendo assim uma variedade menor de números.

NÚMEROS PRIMOS DE WAGSTAFF...

São todos aqueles que se escrevem da forma:

$$P = \frac{(2n+1)}{3} \tag{7.8}$$

Onde n natural.

E através de escolhas adequadas de n o resultado P deve ser um número inteiro. Temos os primos: $3, 5, 7, 11, 13, ...$ Achando números como 9, 15 e outros números não primos, mas muito promissor para pequenos números.

Capítulo 8

Trabalhando com os alunos

Dentro do contexto que a escola existe para formar sujeitos preparados para sobreviver nesta sociedade e desenvolver capacidades cognitivas para se apropriar criticamente dos benefícios da ciência e da tecnologia. Este ultimo capitulo retrata um trabalho desenvolvido com os alunos voluntários do Clube de matemática do Colegio Militar de Manaus com esta finalidade.

Entre as várias abordagens didáticas neste capitulo, buscamos clarificar a teoria e a prática como objetos do ensino da matemática com ênfase nos números primos na formação dos nossos alunos do ensino fundamental e médio, e para isso foi utilizado estratégias de ação educativa com alunos voluntários e com autonomia de ação e pensamento.

Apesar do trabalho ter muitos aspectos práticos o seu objetivo final evidencia o desenvolvimento do pensamento abstrato na busca de solução de problemas.

A organização didática das aulas foi extremamente simples, apresentando, via de regra, a utilização dos capítulos anteriores deste compêndio, utilizado, e organizado, para dar instrumentos aos discentes para que os mesmos pudessem atingir o objetivo fim.

Deste modo didaticamente as aulas ocorreram dentro de uma cooperação entre docente e discente, para que realmente ocorresse a apropriação do conhecimento na relação dinâmica de ensinar e de aprender. Para isso, foi muito importante o comportamento de ambos para que o conhecimento realmente acontecesse. Em muitos momentos, se tornou assim natural, aparecer

o caráter questionador do aluno em uma nova relação baseada nos questionamentos.

A estrutura do Clube de Matemática, realizado fora do período normal das aulas, sem o compromisso de concluir conteúdos em determinado prazo, e com a vantagem de se trabalhar com alunos voluntariamente interessados, sem a costumeira obrigatoriedade da sala de aula e liberto da estrutura regular de ensino, propiciou um ambiente adequado para o desenvolvimento dos objetivos. Refutando assim influências externas que poderiam mascarar o resultado do trabalho.

Vários são os fatores comportamentais que impedem o aluno a assimilar o que é ensinado em sala de aula. A inibição e a dispersão são problemas que se sobressaem notadamente e prejudicam o relacionamento professor $\times$aluno.

Acreditando que a inserção de um novo comportamento com mais liberdade para o aluno possa ser um dos recursos facilitadores da aprendizagem, essa ideia se tornou uma ferramenta de grande relevância, por outro lado é preciso que o professor tenha um controle muito maior sobre o ambiente e sobre seu próprio comportamento, para que as atividades se desenvolvam de forma consistente e prazerosa ao aluno proporcionando diferentes formas de aquisição de conhecimentos.

Com isso podemos afirmar que uma aula dinâmica, aparentemente informal e descompromissada com livros didáticos e roteiros, com certeza renda muito mais e gera melhores resultados do que uma aula formal. Nesse contexto, observou-se que os resultados didáticos devem se afastar das aulas convencionais e das enfadonhas estruturas conteudistas e buscar ambientes mais descontraídos e férteis.

O curso foi desenvolvido com 20 alunos de variadas séries do Ensino Fundamental e Médio, no chamado Clube de matemática do Colégio Militar de Manaus, onde foram realizadas 4 aulas sobre o estudo dos números primos.

Outro ponto positivo deste trabalho é o fato de se conseguir trabalhar com vários alunos de diversos anos, permitindo que eles troquem informações em diversos níveis de conhecimento e de maturidade. Ao contrário do que se poderia esperar essa interação entre alunos do ensino médio e fundamental

foi enriquecedora em vários aspectos que contribuíram de sobremaneira para o desenvolvimento do grupo.

Nessas 4 aulas foi utilizado os capítulos anteriores deste compendio, conforme a estrutura e organização sugerida, com o objetivo de identificar o sucesso ou o fracasso dos alunos no estudo dos números primos como proposto.

Neste capitulo iremos destacar cada aula, de acordo com os planos de aula, mostrando as atividades e apresentando as dificuldades encontradas, conclusões e observações. No decorrer das aulas foram propostos vários exercícios, em geral de cunho prático, e muitos resolvidos com os discentes durante a aula, com a finalidade de preparar esses alunos para uma atividade com característica mais abstrata.

É importante assinalar que mais do que aprender e aplicar o conhecimento objetivo, é preciso que os discentes progridam no raciocínio abstrato à medida que se empenham em alcançar solução para os problemas.

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COLÉGIO MILITAR DE MANAUS

(Ato de criação n° 68.996, de 02 de agosto de 1971).

CLUBE DE MATEMÁTICA

Ano: 2014

Nível: Ensino Fundamental e Médio

Profº: Edson Ribeiro Machado

Plano de Aula do dia 16 de Outubro de 2014

Duração: 120 minutos

1. Referência: Sequência didática - Números Primos:

2. Competência Discursiva a ser trabalhada: Leitura e debate do texto introdutório -Um pouco de História- extraído da tese de mestrado - Números primos: uma abordagem educacional.

3. Mediação:

a.Introdução à atividade: Duração: 20 minutos.

- Identificação dos números naturais e inteiros

- Principio da boa ordenação.

b. Desenvolvimento: Duração: 85 minutos.

- Divisibilidade: conceitos e aplicações.

- Divisão Euclidiana: identificação do resto.

- Caracterização e distinções entre números primos e compostos.

- Teorema Fundamental da Aritmética.

.- Fatoração e quadrados perfeitos.

- Método de fatoração de Fermat - exemplos.

c. Processo Avaliativo: Duração: 15 minutos.

- Diagnóstica participação de todos na aula e apresentação de dúvidas na resolução de exercícios.

- Verificação dos exercícios.

- A atividade tem apenas finalidade formativa, sem mensuração.

8.0.9 A Primeira Aula

Em um primeiro momento foi falado sobre a história do desenvolvimento da teoria dos números primos,observando o quanto de tempo os números primos são estudados por grandes matemáticos, sua importância dentro do conjunto dos números naturais e em toda a teoria moderna da matemática, destacando a luta de tantos estudiosos em encontrar uma formula precisa e geradora de números primos, a tentativa de descobrir como ocorre a sua distribuição dentro dos naturais e a localização de cada um deles. Toda essa parte foi feita em uma apresentação em slides onde se destacou as fotos dos matemáticos e de seus trabalhos.

Essa introdução teve um impacto muito positivo pois o envolvimento dos alunos pela historia, pela luta dos matemáticos na busca de soluções, despertou neles curiosidades e interesse pelo tema.

Apresentando os números naturais observou-se a sua construção, a relação de ordem, propriedades e o princípio da boa ordenação, em seguida feita a extensão para os números inteiros observou-se mais uma vez sua estrutura, propriedade e limitações desse conjunto.

Em seguida foi falado sobre a divisão de números inteiros destacando todas as propriedades citadas na seção de divisibilidade e a também fatoração dos números naturais compostos e os números primos já apresentando aqui suas definições.

Em seguida tratou da divisão Euclidiana destacando importância e a unicidade do resto, mostrando a formula de Euclides $a = b \times q + r$ onde $r \geq 0$ e mostrando que $r = a - b \times q$ ja visando o estudo de congruência. Ao final desse estudo procurou-se definir bem o TFA.

No estudo de divisão Euclidiana uma pequena mudança de foco, ou seja passar a olhar o resto como uma coisa significativa nessa operação, deu uma impressão para os alunos que estávamos falando de uma coisa nova. Normalmente os discentes dão pouca importância ao resto nessas operações, pode-se observar que eles nunca tiveram uma noção clara sobre sua importância. Como citado por alguns alunos "resto é resto".

Por fim, procuramos colocar uma atividade prática, buscando um instrumento de fatoração, utilizou-se o Método de Fatoração de Fermat. Onde através desse método pode-se distinguir os números primos dos números compostos. Este método utilizado de forma lúdica, despertou nos alunos uma competição na identificação desses números.

Durante toda aula, e devido a liberdade dada no trabalho e a inexistência de criticas aos erros dos alunos, eles em muitos momentos realizaram as tarefas com desenvoltura e com muita participação, reforçando assim um comportamento, que contagiou até os mais discretos e criou um ambiente de estudo que se propagou para todas as aulas.

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COLÉGIO MILITAR DE MANAUS

(Ato de criação n° 68.996, de 02 de agosto de 1971).

CLUBE DE MATEMÁTICA

Ano: 2014

Nível: Ensino Fundamental e Médio

Prof°: Edson Ribeiro Machado

Plano de Aula do dia 21 de Outubro de 2014

Duração: 120 minutos

1. Referência: Sequência didática - Números Primos:

2. Competência Discursiva a ser trabalhada: Leitura e debate de textos relacionados aos números primos da tese de metrado - Números Primos: Uma abordagem educacional.

3. Mediação:

a. Introdução à atividade: Duração: 20 minutos.

- MMC e MDC: revisão de conteúdo já conhecidos

b. Desenvolvimento: Duração: 85 minutos.

- MMC e MDC: importância e relacionamento com números primos. - Relação entre MMC e MDC.

- Algoritmo de Euclides: resolução equações diofantinas - Aplicações práticas.

- Congruência: conceitos, operacionalidade e propriedades básicas.

c. Processo Avaliativo: Duração: 15 minutos.

- Diagnóstica participação de todos na aula e apresentação de dúvidas na resolução das aplicações

- Verificação dos exercícios.

- A atividade tem apenas finalidade formativa, sem mensuração.

8.0.10 A Segunda Aula

Nesta segunda aula começando com questionamento com os alunos sobre MMC e MDC, procurando sempre achar as diferenças, apesar de terem nomes muito próximos, aos poucos eles foram se tornando muito diferentes.

A partir do ponto em que as diferenças estavam bem evidentes, foi se introduzindo as propriedades, e por fim estudada a relação entre o MMC e o MDC. Todo esse assunto foi desenvolvido passo-a-passo onde em cada etapa eram realizados exercícios ou exemplos. Destacou-se nesse estudo a definição de números primos entre si que depois será utilizada com os números primos de Fermat e em outras situações.

E como instrumento de operacionalização fizemos o algoritmo de Euclides para determinar o MDC entre dois números. Nesta oportunidade introduzimos as equações diofantinas, pegando exemplo com solução com números pequenos. Com o desenvolvimento de forma simples e introduzindo as soluções e depois com o fato de verificarmos as soluções encontradas materializou o conhecimento, em seguida foram mostrados exemplos com inexistência de soluções, assim tratamos as limitações, e por fim foi deixado outros exemplos para que os alunos pudessem resolver. Apesar do conteúdo e das operações em si não ser nenhuma novidades, a construção da solução da equação causou em certo momento embaraço dos alunos, mas com auxilio do professor e dos colegas entre si, as duvidas foram se dissipando.

Por fim foram resolvidos algumas aplicações semelhantes aos exercícios abaixo : Dispondo de 100 reais, quais são as quantias que se podem gastar comprando selos de 5 reais e de 7 reais? (Utilizando dois baralhos, um azul o outro vermelho, o azul representado os selos de 5 reais e as cartas vermelhas representando os selos de 7 reais, encontramos a solução inicial: $x = 6$ e $y = 10$ gerando $x = 6 + 7t$ e $y = 10 - 5t$ obtemos também $x = 13$ e o $y = 5$ e $x = 20$ e $y = 0$ como soluções maiores que zero)

Numa criação de coelhos e galinhas, contaram-se 60 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível? (continuamos a usar o baralho como instrumento

e se observou a utilização do mesmo raciocínio em diferentes contexto)

Em um segundo momento, foi tratado o estudo das congruências, de forma objetiva e com aplicação direta das propriedades, fazendo apenas as demostração simples, e destacando a importância do resto. Foram apresentadas diversas situações onde se apresenta aplicações do dia a dia sobre congruência. Como, por exemplo, a distribuição dos dias do mês num calendário, é um exemplo do uso do conceito de congruência. Vejamos o calendário do mês de Junho do ano de 2014: Junho de 2014:

D - S - T - Q - Q - S - S

1 - 2 - 3 - 4 - 5 - 6 - 7

8 - 9 - 10 - 11 - 12 - 13 - 14

15 - 16 - 17 - 18 - 19 - 20 - 21

22 - 23 - 24 - 25 - 26 - 27 - 28

29 - 30

Observe a segunda coluna, a das segundas-feiras, ela começa com o 2 e todos os outros números dessa coluna deixam resto 2 quando divididos por 7. A coluna da sexta-feira, começa com 6 e todos os outros números deixam resto 6 quando divididos por 7. Ou seja, em todas as colunas os números são côngruos entre si módulo 7. Em seguida se estudou o Pequeno Teorema de Fermat e no Teorema de Wilson, onde foi feita uma breve revisão da fatorial dos números naturais. Feitas algumas aplicações semelhantes aos exemplos abaixo:

O mágico senta-se numa cadeira, de costas voltadas para a audiência. Alguém pensa num número natural(logicamente ja testado) não superior a 100. Divide o número por um número primo e diz o número primo e o resto da divisão ao mágico. Em seguida, divide o número inicialmente pensado por outro número primo e fala o número primo e o resto da divisão ao mágico. O mágico, conhecendo apenas os dois números primos e os restos, advinha o menor número pensado. (Nesta atividade um aluno era escolhido como mágico e um outro aluno fazia as escolha prévia do número a ser adivinhado e transmitia ao mágico os divisores e os restos. Por exemplo um número que por 3 da resto 1 e por 5 da resto 2 o mágico encontrou 11.)

A importância de se ter chegado no pequeno Teorema de Fermat e no Teorema de Wilson ganhou magnitude pois nos permitiu durante a aula usando o Excel identificarmos alguns números primos pequenos utilizando esses dois teoremas.

Nessa oportunidade em que foi colocado um slide com os primeiros 1000 números primos, aproveitamos a oportunidade para observar que a presença deles se torna cada vez menor a medida que os números irão crescendo, e no intuito de deixar bem claro essa caracteristica realizamos uma contagem dos números primos entre os 100 primeiros números naturais havendo 25, depois entre os números de 100 ao 200 tendo 21, depois de 200 a 300, 300 e 400 e 600 e 700 havia 16, entre 400 e 500 tinha 17, entre 600 e 700 havia 16, entre 500 e 600, 700 e 800 e 900 e 1000 tinha 14 e por fim entre 800 e 900 havia 15.

Nessa aula foi observado pelos alunos que se faz muita em matemática com poucas ferramentas, que muitos problemas são resolvidos muitas vezes com a mesma ferramenta. E que aparentes formulas simples podem apresentar soluções inesperadas.

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COLÉGIO MILITAR DE MANAUS

(Ato de criação n° 68.996, de 02 de agosto de 1971).

CLUBE DE MATEMÁTICA

Ano: 2014

Nível: Ensino Fundamental e Médio.

Profº: Edson Ribeiro Machado.

Plano de Aula do dia 23 de Outubro de 2014. Duração: 120 minutos

1. Referência: Sequência didática - Números Primos.

2. Competência Discursiva a ser trabalhada: Leitura e debate de textos relacionados aos números primos da tese de metrado - Números Primos: Uma abordagem educacional.

3. Mediação:Duração: 15 minutos.

a. Introdução à atividade:

- Classe residual modulo m - operações.

b. Desenvolvimento: Duração: 75 minutos.

- Números primos de Fermat: exemplos e exceções.

- Números primos de Mersenne: exemplos e aplicações com Torre de Hanoi.

- Distribuição dos números primos: história e analise.

- Crivo de Erastótenes: realização de cortes em numerações com projeção com slides.

- Um novo crivo: critérios, realização de cortes em numerações com projeção com slides.

- Identificação se um número é primo ou composto por divisões por primo conhecido.

c. Processo Avaliativo. Duração: 30 minutos.

- Definição dos Grupos 1 e 2.

- Determinação das atividades a serem desenvolvidas por cada grupo para semana seguinte:

Grupo 1: tinha o objetivo de buscar ou criar um método de como gerar números primos.

Grupo 2: tinha objetivo de procurar, descobrir ou criar um métodos de como identificar se um números era primo.

- A atividade tem apenas finalidade formativa, sem mensuração.

8.0.11 A Terceira Aula

Esta terceira aula foram aprofundado um pouco o conceito de congruência com a introdução das Classes residuais Modulo m, onde foram apresentadas alguns tabelas das operações de soma e multiplicação, e posteriormente os discentes fizeram as tabelas para outros números identificando as diferenças de quando o m-composto e quando m-primo.

Logo em seguida começamos a trabalhar formulas que geram números primos. Esses alunos que ja haviam tido uma breve introdução de algumas formulas na primeira aula quando se falou na parte histórica não tiveram dificuldades na introdução desse tema, partimos, então, direto para as formulas de Fermat e de Mersenne.

Começamos apresentando o número de Fermat, para que os alunos se familiarizassem com ele calculamos os primeiros números, e logo se deparou com um crescimento vertiginoso nos cálculos, tanto que para calcular F_5 foi utilizado uma calculadora. Nesse momento, o professor, aproveitou para mostrar que esse número F_5 não é primo que ele é divisível por 641.

Como exemplo foram projetados outros números de Fermat que não são primos, apenas por curiosidade. E por fim foi mostrado que os números de Fermat são todos primos entre si ou seja que o $\text{mdc}(F_m, F_n) = 1$ para $m \neq n$, e que para $n \geq 2$ o dígito das unidade de F_n é sempre 7 utilizando, neste caso, uma demostração com operações simples de congruência.

de hanoi.png 

Figura 8.1: Torre de hanoi

O número de Mersenne foi muito mais atraente e interessante, como a formula do Número de Mersenne coincide com a solução minimal da Torre de Hanoi (figura 8.1 abaixo), e como alguns alunos ja conheciam esse jogo foi mais fácil a familiarização com esse número. Aproveitamos a oportunidade para realizar esse jogo, que ja faz parte do arsenal dos nossos alunos do Clube de matemática.

Por fim como fizemos com o número de Fermat identificamos que o $M_7 = 127$ não é primo, e mostramos vários outros que também são de Mersenne mas não são primos. Foi o bastante para os alunos entenderem o quanto é difícil encontrar uma formula para se achar sempre números primos.

Em um terceiro momento estudamos o modo tradicional de se achar os primeiros números primos utilizando o Crivo de Erastóstenes. Assim foi possível descobrir os primeiros números primos. E com essa tabela criada usando o Crivo de Erastótenes podemos utilizando o capitulo 7 deste compendio apresentar um novo Crivo. Esse foi um momento oportuno pois todos os alunos ja conheciam o Crivo de Erastótenes, e sua construção não trouxe nenhuma novidades a esses alunos. Com o novo Crivo sim permitiu que os discentes fizessem os corte dos números composto utilizando operações simples e constatando uma forma mais moderna de construir um crivo.

Por fim, como aplicação foi colocado um número relativamente grande ($>$ 1.000) e buscou identificar se tal número era primo ou não, para isso procurou saber se o número dado era um quadrado perfeito, que no caso não era, em seguida buscou-se o intervalo entre as raízes quadradas inteiras e tomou-se o menor desses valores, já se utilizando os primos encontrado no tópico anterior, cada aluno dividiu o numero dado por cada um dos primos menores que a raiz inteira escolhida. Como nenhum deles dividiu de forma inteira o número dado concluiu-se que o número era primo. Conforme abaixo:

Exemplo 29. *Dado o número* 3.061 *cuja raiz quadrada aproximada a menos é* 55*, olhando o crivo montado anteriormente pegamos os primos:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 \text{ e } 53$$

. Pela simples observação (e regra de divisibilidade) se identificou que o número não era divisível nem por: $2, 3, 5, 7$ *e* 11*. E foi feita as contas com os primos restantes. Como em nenhum caso o número era divisível pelo primo concluiu-se que o número era primo. Como o grupo era formado em sua maioria por alunos do ensino fundamental ficou a duvida do porque não testar os outros primos maiores que a raiz. Nesse momento mostrou que todo numero inteiro* N *pode ser escrito na forma:* $N = a \times b$ *onde* $a \leq b$ *logo,* $a \times a \leq N$ *logo,* $a \leq \sqrt{N}$ *então sempre haverá esse* a*, caso o número seja primo esse* $a = 1$*.*

Por fim a turma foi divida em 2 grupos com dez alunos, com escolha livre de parceiros entre eles. Onde formou-se dois grupos:

GRUPO 1: tinha o objetivo de buscar ou criar um método de como gerar números primos diferente daquele trabalhado em sala de aula.

GRUPO 2: tinha objetivo de procurar, descobrir ou criar um métodos de como identificar se um números era primo, claro que diferente daquele dado em sala de aula.

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

COLÉGIO MILITAR DE MANAUS

(Ato de criação n° 68.996, de 02 de agosto de 1971).

CLUBE DE MATEMÁTICA

Ano: 2014.

Nível: Ensino Fundamental e Médio

Prof°: Edson Ribeiro Machado

Plano de Aula do dia 28 de Outubro de 2014. Duração: 120 minutos

1. Referência:

Sequência didática - Números Primos.

2. Competência Discursiva a ser trabalhada: Leitura e debate de textos relacionados aos números primos da tese de metrado - Números Primos: Uma abordagem educacional.

3. Mediação:

a. Introdução à atividade. Duração: 20 minutos.

- Resumo de todo trabalho feito até a presente data. b. Desenvolvimento:

-Apresentação do trabalho do Grupo 1: objetivo de buscar ou criar um método de como gerar números primos diferente daquele trabalhado em sala de aula. Duração: 35 minutos.

- Apresentação do trabalho do Grupo 2: objetivo de procurar, descobrir ou criar um métodos de como identificar se um números era primo, claro que diferente daquele dado em sala de aula. Duração: 35 minutos.

c. Processo Avaliativo: Duração: 30 minutos.

- Discussões, perguntas, interpretações entre os grupos.

- Autocritica.

- Comentários do professor.

- Premiação dos melhores alunos na atividade prevista.

8.0.12 A Quarta Aula

Esta quarta aula foi marcada pela exposição dos grupos sobre as repostas obtidas em busca da solução dos problemas propostos. GRUPO 1: trouxe como solução a ideia da prova da infinitude dos números primos $P_n = p_n + 1$ gerando os seguintes primos:

$$3, 7, 11, 31, 211, 2311, ...$$

Também foi colocado nesse aspecto que o uso de $N = p_1 \times p_2 \times .. \times p_n - 1$ também gera números primos e falha também mais ou menos com a mesma frequência. Observado também por alguns alunos que se juntássemos as duas formulas teríamos melhores resultados, ou seja, usando $N = p_1 \times p_2 \times .. \times p_n \pm 1$ geraríamos muito mais primos rapidamente, mas sempre teríamos que fazer os testes para poder garantir que os valores achados seriam mesmos primos. Depois ainda percebemos que se começarmos pelo primeiro primo $\{2\}$ e utilizando apenas operações básicas na forma: $\{2, 3\} \times p_2 \pm \{1, 2, 3\}$ semelhante a um algoritmo podemos encontrar todos os próximos primos, da seguinte forma: achando o primo 3 utilizando operações basicas com o 2 e o 3 achamos o primo 5 e assim por diante, sempre utilizando apenas os primos achados anteriormente. Com isso achávamos todos os primeiros primos de 3 ao 97.

Exemplo 30.

$$2.1 + 1 = 3 \qquad 2.2 + 1 = 5 \qquad 2.3 + 1 = 7$$

$$2.5 + 1 = 11 \qquad 3.5 - 2 = 13 \qquad 3.5 + 2 = 17$$

$$3.7 - 2 = 19 \qquad 3.7 + 2 = 23 \qquad 2.13 + 3 = 29$$

$$3.11 - 2 = 31 \qquad 3.13 - 2 = 37 \qquad 3.13 + 2 = 41$$

$$2.23 - 3 = 43 \qquad 2.23 + 1 = 47 \qquad 3.17 + 2 = 53$$

$$3.19 + 2 = 59 \qquad 2.29 + 3 = 61 \qquad 3.23 - 2 = 67$$

$$3.23 + 2 = 71 \qquad 2.37 - 1 = 73 \qquad 2.41 - 3 = 79$$

$$2.41 + 1 = 83 \qquad 3.29 + 2 = 89 \qquad 2.47 + 3 = 97$$

Seguindo assim sucessivamente como uma brincadeira testando o raciocínio dos alunos envolvidos. Obtendo assim os primeiros números primos de 2 a 97. Buscando a ideia de que podemos escrever todos os números primos na forma citada acima.

Alunos de GRUPO1 também buscaram na internet métodos vulgarizados na rede sem muita importância tipo completamento de tabelas achando os primeiros primos, que foram facilmente descartada com regras simples para achar os primeiros números primos. O GRUPO2 encontrou mais problemas para desenvolver sua atividade buscando sempre na divisibilidade e na fatoração como um método para descobrir se um numero é primo ou não. Por fim utilizando "Um novo Crivo para gerar números primos"já desenvolvido no capitulo 7 encontramos os primeiros números primos dentre os números de 1 a 100 utilizando uma tabela e fazendo os cortes dos números compostos de acordo com o crivo.

Reconhecendo que foi uma experiência extremamente satisfatória acreditamos que o estudo de números primos deve tomar um novo tratamento no ensino médio e fundamental principalmente quando se da ênfase a um tratamento didático lúdico, que torna o assunto atraente e permite uma maior absorção por parte dos discentes.

Por outro lado observou-se que alunos do ensino fundamental e médio carecem de conteúdo relacionado ao estudo de congruência, encontram dificuldade de compreender que o conjunto dos números inteiros podem ser organizados de acordo com classes de números. E principalmente falta um estudo organizado sobre números primos, compostos e divisibilidade.

Considerações Finais

Observando a realidade do ensino no país, o estudo dos números primos ficaram ofuscados e distanciados dos alunos do ensino fundamental e médio em função da falta de sistematização do estudo, conceitos e aplicações desses números e a dificuldade de se encontrar um modo simples para caracterizar quando um número é primo ou composto.

Constata-se que encontrar um modelo que gere alguns números primos se apresenta atualmente muito mais fácil do que determinar se um número é primo ou não o que foi facilmente observado através do trabalho feito em sala de aula com os alunos do Clube de matemática como tratado no último capitulo.

Também é muito comum as escolas de nível médio e fundamental, infelizmente, não apresentar um estudo sobre congruências ficando esse tema como tópico de uma cadeira universitária de álgebra, e mais ainda, a ideia de algoritmos e o uso de computadores para gerar soluções e resultados em matemática ainda se encontra muito distante dos nossos alunos, apesar do tão corriqueiro uso de computadores e internet pelos nossos jovens.

Com a intenção que este trabalho busque um retorno ao tema trabalhado neste compendio, entendemos que uma valorização e sistematização do conteúdo aqui relacionado, vai trazer um modelo didático de como introduzir o estudo dos números primos no primeiro e segundo ciclos de estudo, e fazendo isso acreditamos termos contribuído de certa forma para educação dos nossos alunos.

Por fim gostaria de ressaltar que existem várias curiosidades e estudo sobre números primos com várias questões que ainda não foram respondidas, como por exemplo: se existem infinitos primos da forma $n^2 + 1$? ou se sempre

existe um número primo entre n^2 e $(n+1)^2$? ou se existem infinitos primos de Fermat (da forma $2^{2^n}+1$)? E outros questionamentos citados neste trabalho. Dessa forma observa-se que a teoria em torno dos números primos oferece uma vasta gama de oportunidade de trabalhos e estudos que podem estimular a curiosidade dos nossos discentes e despertar-lhes o interesse por essa fronteira da matemática a ser vencida.

Referências Bibliográficas

[1] Santos, José Plínio de Oliveira - Introdução a Teoria dos Números - Coleção Matemática Universitária

[2] Revista Professor Matemática nº 70,71 e 73 - Sociedade Brasileira de Matemática e USP ? Universidade de São Paulo

[3] Gowers, Thimothy - Matemática: Uma breve introdução - Ed Gradiva, 2008

[4] Avila, Geraldo Severo de Souza ? Várias Faces da matemática - São Paulo: Ed Blucher, 2007

[5] Courant, Richard e Robbins, Herbert , O que é a matemática? - Rio de Janeiro: Ed Ciencia Moderna Ltda, 2000

[6] Alencar Filho, Edgar de, 1913 - Aritmética dos inteiros / Edgar de Aelncar Filho - São Paulo ; Nobel, 1987.

[7] GHAGRAWAL, Manindra, KAYAL, Neeraj e SAXENA, Nitin. Primes is in P. Disponível em *http* : *//www.cse.iitk.ac.in/ manindra/algebra/primality*$_v$*6.pdf* Acesso em: 04 jun. 2008.

[8] BOYER, Carl B. História da matemática. Tradução: Elza F. Gomide. São Paulo: Edgard Blucher Ltda., 1974. 488p.

[9] COUTINHO, S. C. Números inteiros e criptografia RSA. 2. ed. Rio de Janeiro: IMPA, 2001. 213 p.

[10] COUTINHO, S. C. Primalidade em tempo polinomial: uma introdução ao algoritmo AKS. Rio de Janeiro:Sociedade Brasileira de Matemática, 2004. 105 p.

[11] FILHO, EDGARD DE ALENCAR, Teoria Elementar dos Números. São Paulo - Ed Nobel - 1981. 383p.

[12] DEVLIN, Keith. Os problemas do milênio. Tradução: Michelle Dysman. Rio de Janeiro: Record, 2004. 308 p.

[13] EUCLIDES. Elementos de geometria. Tradução: Frederico Commandino. São Paulo: Edições Cultura, 1944. Vol.1. Adicionados e ilustrado por Roberto Simsom, professor de Matemática da Academia de Glasgow, Escócia.

[14] EVES, Howard. Introdução à história da matemática. Tradução: Higyno H. Domingues. Campinas: Editora da UNICAMP, 2004. 844 p.

[15] GRANVILLE, Andrew. It is eeasy to determine whether a given integer. Bulletin (New Series) of the AmericanMathematical Society, 2004. 1: Vol. 42. p. 3-38.

[16] IFRAH, Georges. Os números: história de uma grande invenção. Tradução: Stella Maria de Freitas Senra. 2. ed. Rio de Janeiro: Globo S.A., 1989. 368 p.

[17] JOYCE, D. E. Euclide's elements. Ed. University Dept. Math. & Comp. Sci. Clark. 1997. Disponivel http://aleph0.clarku.edu/ djoyce/java/elements/elements.html> Acesso em: 6 abr. 2008.

[18] KHUN, Thomas S. A estrutura das revoluções científicas. 3. ed. São Paulo: Perspectiva, 1982. 257 p.

[19] RIBENBOIN, Paulo. Números primos: mistérios e recordes. Rio de Janeiro: IMPA, 2001. 280 p.

[20] SAUTOY, Marcus du. A música dos números primos: a história de um problema não resolvido na matemática.Tradução: Diego Alfaro. Rio de Janeiro: Jorge Zahar Editora, 2007. 352 p.

[21] Posted in Demostraciones, MegaPost, Números primos, Teoría Analítica de números by ZetaSelberg on 4 noviembre, 2013

[22] Bruno da Rocha Braga - Ravel / COPPE / UFRJ - Algoritmo AKS Primalidade de um Número em Tempo Polinomial brunorb@ravel.ufrj.br - http://www.ravel.ufrj.br/ - 11 de Setembro, 2002.

[23] De farias, Fernando - Uma analise comparativa entre os testes de primalidade AKS e MiIller-Rabin - Universidade católica de Brasilia.

[24] Aluízio Ferreira Lima, José e Braga de Freitas, Sinval - Primalidade: Fundamentos, testes e Perspectivas - Microsoft Word - TCC II - Primalidade - Vers43º Final.doc.

[25] Spenthof, Roberto Luiz e Souza, Josiney Alves - Primos: da aleatoriedade ao padrão - Sociedade Brasileira de Matemática

[26]] SINGH, S. O Ultimo Teorema de Fermat. Rio de Janeiro: Record, 1998.

[27] COUTINHO, S. C. Numeros Inteiros e Criptografia RSA. Rio de Janeiro: IMPA / SBM, 1997.