UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS PROF. DR. SÉRGIO JACINTHO LEONOR
MESTRADO PROFISSIONAL EM MATEMÁTICA

FREDERICO TORRES DE MOURA

NÚMEROS PRIMOS: UMA FÓRMULA GERADORA

Arraias - TO
2018

UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS PROF. DR. SÉRGIO JACINTHO LEONOR
MESTRADO PROFISSIONAL EM MATEMÁTICA

FREDERICO TORRES DE MOURA

NÚMEROS PRIMOS: UMA FÓRMULA GERADORA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Robson Martins de Mesquita

Arraias - TO
2018

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

M929n MOURA, FREDERICO TORRES DE.
NÚMEROS PRIMOS: : UMA FÓRMULA GERADORA . / FREDERICO TORRES DE MOURA. – Arraias, TO, 2018.
67 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Arraias - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2018.
Orientador: ROBSON MARTINS DE MESQUITA

1. NÚMEROS PRIMOS. 2. MATEMÁTICA. 3. INVESTIGAÇÃO. 4. TEOREMAS. I. Título

CDD 510

Elaborado pelo sistema de geração automatica de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

FREDERICO TORRES DE MOURA

NÚMEROS PRIMOS: UMA FÓRMULA GERADORA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Robson Martins de Mesquita.

Data de Aprovação 04/07/2018

BANCA EXAMINADORA:

Prof. Dr. Robson Martins de Mesquita (Orientador)
Universidade Federal do Tocantins-(UFT)

Prof. Dr. Thiago Rodrigues Cavalcante
Universidade Federal do Tocantins-(UFT)

Prof. Dr. Ronaldo Antônio dos Santos
Universidade Federal de Goiás-(UFG)

Ao futuro dos meus filhos
e a realização de seus sonhos.

Agradecimentos

Agradeço primeiramente a Deus pelas coisas maravilhosas que aconteceram em minha vida desde o começo deste curso e por me ajudar todos os dias a superar as dificuldades apresentadas em meu caminho.

Agradeço também à minha esposa Ieda pela compreensão e paciência, tendo em vista que durante sua primeira gravidez tive que deixá-la em várias sextas-feiras para viajar até a Universidade Federal do Tocantins -UFT-, em Arraias.

Agradeço aos meus pais Carlos Roberto e Maria Eli por sempre me apoiarem no que diz respeito aos meus sonhos e por ajudar em minha casa nos momentos em que estive ausente.

Agradeço a todos os professores do PROFMAT da UFT, campus de Arraias, pela aprendizagem. A alguns deles são devidos agradecimentos especiais pelo simples prazer de estar em sua presença, visto que são pessoas com altíssimo conhecimento (e como isso faz bem para quem tem vontade de aperfeiçoar seus conhecimentos!), em especial, a meu orientador, Prof. Dr. Robson Martins de Mesquita, com quem tive a satisfação de concluir duas disciplinas tendo-o como regente.

Agradeço a todos os meus colegas pelos grupos de estudos que são muito importantes nesta etapa e pelos momentos de distração. Em especial aos colegas Moisés, Juliana e Luciano com quem dividi despesas de viagem, hotel e alimentação durante todo o curso e com quem tive o prazer de dividir experiências de vida e aprender muito com eles.

"Não é o conhecimento, mas o ato de aprender, não a posse
mas o ato de chegar lá, que concede a maior satisfação".
Carl Friedrich Gauss (1777-1855)

Resumo

O trabalho aqui apresentado tem por objetivo fazer uma investigação sobre os números primos e algumas de suas características e propriedades, dentre elas uma fórmula geradora de números primos. Para isto foram realizadas pesquisas bibliográficas e assim introduzidos conceitos de aritmética bem como teoremas e suas respectivas demonstrações com intuito de esclarecimento acerca do assunto abordado. No contexto do programa este trabalho é direcionado ao professor regente, como uma forma de aprimorar seus conhecimentos, para estudantes em nível de olimpíada ou mesmo para alunos de nível médio que tenham interesse no assunto em questão. Nesse sentido, foi desenvolvido um questionário contendo perguntas básicas sobre os números primos e aplicado para os estudantes que compõe a terceira série do Colégio Iesgo, na cidade de Formosa-GO, afim de identificar o que se conhece sobre os números primos no ensino básico.

Palavras-chaves: Números. Primos. Matemática. Investigação. Teoremas.

Abstract

The work presented here aims to investigate the prime numbers and some of their characteristics and properties, among them a formula generating prime numbers. For this purpose, bibliographical researches were carried out, thus introducing concepts of arithmetic as well as theorems and their respective demonstrations in order to clarify the subject matter. In the context of the program this work is directed to the regent teacher, as a way to improve his knowledge, for students at the level of the Olympiad or even for students of medium level who have an interest in the subject in question. In this sense, a questionnaire containing basic questions about primes was developed and applied to the students who make up the third series of the Iesgo College, in the city of Formosa-GO, in order to identify what is known about prime numbers in elementary education.

Keywords: Numbers 1. Prime 2. Mathematic 3. Investigation 4. Theorems 5.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

TFA	Teorema Fundamental da Aritmética
F_n	Número de Fermat
M_n	Número de Mersenne
GIMPS	Great Internet Mersenne Primo Search
PTF	Pequeno Teorema de Fermat
$\pi(m)$	Quantidade de números primos menores que m
PMI	Princípio do menor inteiro

Sumário

Introdução

No decorrer de minha carreira acadêmica as disciplinas com as quais mais me identifiquei foram: Geometria Euclidiana, Cálculo e Teoria dos Números. Pelo pouco aprofundamento na graduação não pude conhecer melhor as maravilhas que cada uma delas ainda tinham para me mostrar. Por sorte, ao ingressar no curso de Mestrado profissional pude aprender mais sobre cada uma dessas disciplinas e escolhi na Teoria dos Números, os números primos para realizar esta pesquisa. De acordo com os objetivos do programa PROFMAT, este trabalho seria destinado a alunos do Ensino Básico e acredito que alunos mais curiosos, ou, ainda, aqueles que queiram aprofundar seus conhecimentos sobre os números primos e os estudantes que participam de competições matemáticas, podem fazer bom uso do presente estudo.

O primeiro capítulo traz um pouco da história dos números até chegar na primeira ideia de número primo. Após a definição de número primo são apresentadas propriedades de divisibilidade dos números e o Algoritmo de Euclides para calcular o *mdc*. Ao final do capítulo, são apresentados dois teoremas importantes, o Teorema Fundamental da Aritmética e o teorema da existência de infinitos números primos.

No segundo capítulo são apresentadas as conjecturas de Fermat e de Mersenne para os números primos. Como curiosidade também são definidos os números perfeitos e uma relação deles com os números de Mersenne. Ao final, são enunciados dois teoremas fundamentais para o resultado final desta pesquisa, o Pequeno Teorema de Fermat e o Teorema de Wilson.

O terceiro capítulo faz uma breve descrição da procura por uma fórmula que descreva o conjunto dos números primos e são apresentadas algumas expressões matemáticas que na verdade eram tentativas de representação dos números primos, perseguida arduamente por muitos matemáticos.

No quarto capítulo é apresentada uma aplicação de parte do trabalho para uma turma de 3ª série do Ensino Médio. Para estes alunos foi passado um questionário para analisar o que eles sabiam sobre números primos durante o período do Ensino Básico. Após responderem, foi ministrado um momento de aula sobre os números primos de forma a responder o questionário aplicado anteriormente.

1 Conhecendo os números primos

1.1 O inicío dos números

No início da história do homem surge naturalmente a necessidade de contar e por consequência associa os números às quantidades de coisas ao seu redor. Segundo DOMINGUES (1991) a antropologia confirma através do estudo de culturas primitivas que não importa o quão limitados eram os indivíduos da época os mesmo tinham um embrião da ideia de número. Dessa forma nossos antepassados passaram a se preocupar com os registros quantitativos das coisas que tinham para terem uma referência quanto às suas necessidades.

Com o desenvolvimento de uma sociedade surge a necessidade da contagem mais precisa e dos cálculos, o que não era viável sem a criação dos sistemas de numeração. Dessa maneira naquela época os egípcios desenvolveram um sistema de numeração de base decimal chamado hieróglifico o qual usava símbolos para representar as quantidades. Na mesma época os mesopotâmios desenvolveram um sistema de base sexagesimal também escrito por símbolos. Os gregos por sua vez usaram dois sistemas de numeração dentre eles o jônico, ou sistema cifrado, que também era na base 10 e tinha como símbolos as 24 letras do alfabeto grego e mais 3 símbolos. Um sistema de numeração antigo que ainda é apresentado no ensino básico é o sistema de numeração Romano também de base decimal. DOMINGUES (1991)

Há muitos anos que os números primos são investigados e vistos como enigmas na matemática. Ao certo não se sabe quando se deu o início do estudo dos números primos, mas os gregos os conheciam e os chamavam de números indivisíveis. A palavra "primo" não tem nenhuma ligação com grau de parentesco, mas com o termo do latim "primus" que significa primeiro. Na Grécia antiga os matemáticos consideravam que tudo eram números, também os pitagóricos, compreendiam que haviam números indivisíveis e os chamavam primários.

Sabemos que se k é divisor de p então o resto da divisão de p por k é igual a zero, ou ainda $p = k \cdot q$ para algum q inteiro. Vejamos a definição de número primo.

Definição 1.1. *Um número $n > 1$, tal que $n \in \mathbb{N}$, é primo quando possui apenas dois divisores, sendo eles, o 1 e o próprio n.*

Pelo conceito de número primo pode-se, de forma simples, listar os 5 ou 10 primeiros primos. A título de curiosidade serão listados abaixo todos os números primos até mil:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997.

Observando a lista acima pode-se contar 168 números de forma que de 0 a 100 tem-se 25 primos, de 100 a 200 são 21 primos, de 200 a 300 são 16, e sucessivamente, a lista vai diminuindo e no intervalo de 900 a 1000 são apenas 14 números primos. Dessa forma, observando a listagem dos números acima temos a ideia de que os números primos vão diminuindo a quantidade de acordo com o crescimento dos números naturais. Mas afinal, existe um último número primo? A quantidade de números primos é finita? De acordo com BOYER (1974), Euclides de Alexandria, autor de *Os Elementos*, publicou por volta de 300 A.C. que a quantidade de números primos é infinita. Da infinitude dos números primos é interessante observar que existem intervalos arbitrariamente grandes que contém apenas números compostos como por exemplo, para $N > 1$, $(N+1)!+2, (N+1)!+3, (N+1)!+4, \ldots, (N+1)!+(N+1)$. Antes de provar a infinitude dos números primos veremos algumas propriedades básicas de divisibilidade nos números inteiros.

1.2 Divisibilidade em $\mathbb{Z}$

Tratar de divisibilidade dos números inteiros é continuar a falar de múltiplos e divisores de uma forma semelhante ao que foi feito em $\mathbb{N}$, mas com consequências muito mais abrangentes. Para iniciar, serão enunciadas duas extensões conceituais do que já foi feito no conjunto dos naturais para o conjunto dos números inteiros, a saber, o conceito de divisibilidade, virtualmente com a mesma semântica e o conceito de número primo. Em seguida é apresentado o Princípio do Menor Inteiro (PMI), considerado neste trabalho como um postulado e, posteriormente, é enunciado e demonstrado o Algoritmo da Divisão de Euclides, que é conhecido e muito utilizado em sala de aula e servirá para facilitar o entendimento das proposições e notações posteriores.

Definição 1.2. *Dados $a, b \in Z$, dizemos que b divide a e escrevemos $b \mid a$, se existir $c \in Z$ tal que $a = bc$. Neste caso, também se diz que a é um múltiplo de b.*

Exemplo: $5 \mid 15$, pois $15 = 5 \cdot 3$.

Definição 1.3. *Um número $p \in \mathbb{Z}$ onde $p \notin \{0, 1, -1\}$, é primo se e somente se os únicos números naturais que o dividem são $|p|$ e 1.*

Portanto, quando um número $n \in \mathbb{Z}$ não é primo existem números inteiros não nulos e ambos diferentes de 1 e de n, b e c, tais que $n = bc$ e, neste caso, n é dito um número composto e b e c são os fatores de n. Se algum dos fatores de um número composto for um número primo, será dito que tal fator é um fator primo de n.

A argumentação que escolhemos para a demonstração do Algoritmo da divisão faz uso do Princípio da Boa Ordenação dos Inteiros, também conhecido como Princípio do Menor Inteiro, que assumiremos como um postulado. Antes, apresentamos uma definição para não restar dúvidas sobre o que diz o Princípio.

Definição 1.4. *Seja S um subconjunto não vazio de $\mathbb{Z}$. Todo elemento $k \in \mathbb{Z}$ tal que $k \leq x$, para todo $x \in S$, chama-se cota inferior de S. Uma cota inferior de S que pertença a S chama-se mínimo de S e é denotado por* $\min(S)$.

É fácil ver que o mínimo de S, quando existe, é único.

Postulado 1.1. *O Princípio do menor Inteiro: Seja $S \neq \emptyset$ um subconjunto de $\mathbb{Z}$. Se S admite alguma cota inferior em $\mathbb{Z}$, então S possui um mínimo.*

O teorema seguinte é dado como o Algorítmo da Divisão de Euclides que é muito usual no ensino básico quando se trabalha com múltiplos e divisores e fundamental para o entendimento da "Congruência"que é apresentada no capítulo 2.

Teorema 1.1. *Para quaisquer inteiros a e b com $b \neq 0$, existe um único par de inteiros (q, r) tais que $a = bq + r$ onde $0 \leq r < |b|$. Os números q e r são chamados, respectivamente, de quociente e resto da divisão de a por b.*

Demonstração. Precisamos mostrar duas coisas: i) a existência e ii) a unicidade.

(i) Existência.
Seja $b > 0$ e $a \in \mathbb{Z}$, mostraremos que existe $n \in \mathbb{N}^*$ de modo que $nb > a$. Tomando $n = |a| + 1$, como $b \geq 1$ então $nb \geq n = |a| + 1 > a$. Logo, se tomarmos o conjunto $S = \{n \in \mathbb{N}^*; nb > a\}$ temos que S é não vazio. Observando que $S \subset \mathbb{N}^*$, então 0 é uma cota inferior de S. Assim, pelo princípio do menor inteiro existe $q + 1 = min(S)$. Então:

$$qb \leq a < (q + 1)b$$

Somando $-(qb)$ temos:

$$0 \leq a - qb < b$$

e tomando $a = qb + r$ temos $0 \leq r < b$.

Caso $b < 0$.
Aplicamos o teorema no caso já demonstrado em (i) para determinar q_1 e $r \in \mathbb{Z}$, com $0 \leq r < |b|$ para escrever:

$$a = q_1|b| + r. \tag{1.1}$$

Fazendo $q = -q_1$ e observando que $|b| = -b$, pois $b < 0$, obtemos de (1.1) $a = qb + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < |b|$
(ii) Unicidade.
Suponha que $a = qb + r = q_1 b + r_1$ com $0 \leq r < |b|$ e $0 \leq r_1 < |b|$. Assim,

$$|r - r_1| = |q_1 - q||b| \tag{1.2}$$

Afirmamos que $r = r_1$. De fato, pois se $r \neq r_1$, tem-se que

$$0 < |r - r_1| < |b|, \tag{1.3}$$

uma vez que $r,\ r_1 \in [0,\ |b|)$ implica que a distância entre um e o outro é menor que o comprimento do intervalo, que é $|b| - 0 = |b|$.
De (1.2) em (1.3) segue que $0 < |q - q_1||b| < |b|$ implicando que $0 < |q - q_1| < 1$, o que é um absurdo, pois sendo $|q - q_1|$ um inteiro diferente de zero, não pode ser menor que 1. Portanto $r = r_1$ e, por (1.2), $q = q_1$. E isto demonstra o teorema.

□

Agora vejamos algumas proposições importantes para entendermos algumas demonstrações subsequentes.

Proposição 1.1. *Se $a \mid b$ e $b \mid a$ então $a = b$ ou $a = -b$. (Lê-se: Se a divide b e b divide a, então a é igual a b ou a é igual a -b)*

Demonstração. Se $a \mid b$ então existe um $f \in \mathbb{Z}$ tal que $b = a \cdot f$ (*). Da mesma forma se $b \mid a$ então existe um $k \in \mathbb{Z}$ tal que $a = b \cdot k$ (**). Substituindo (**) em (*) vemos que $b = (b \cdot k) \cdot f$ o que nos dá $k \cdot f = 1$ e como k e f são inteiros $k = 1$ e $f = 1$, ou $k = -1$ e $f = -1$. □

Proposição 1.2. *Se $a \mid b$ e $b \mid c$ então $a \mid c$. (Lê-se: Se a divide b e b divide c, então a divide c)*

Demonstração. Se $a \mid b$ então existe m inteiro tal que $b = a \cdot m$(*). Se $b \mid c$ então existe um n inteiro tal que $c = b \cdot n$(**). Subtituindo (*) em (**) temos $c = a \cdot m \cdot n$ e como m e n são inteiros o produto $m \cdot n$ também resulta em um número inteiro j. Assim, temos que $c = a \cdot j$ e então $a \mid c$. □

Proposição 1.3. *Se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$*

Demonstração. Se $a \mid b$ então existe um $j \in \mathbb{Z}$ tal que $b = a \cdot j$. Se $a \mid c$ então existe um $k \in \mathbb{Z}$ tal que $c = a \cdot k$. Somando as duas igualdades temos $b + c = a \cdot j + a \cdot k$ e colocando a em evidência $b + c = a(j + k)$. Como j e k são inteiros $j + k = h$ também é inteiro, o que nos dá $b + c = a \cdot h$. Da última igualdade temos que $a \mid (b + c)$.

□

Proposição 1.4. *Se $a \mid b$ então $a \mid b \cdot m$ (Lê-se: Se a divide b então a divide um múltiplo de b)*

Demonstração. Se $a \mid b$ sabemos que existe um k inteiro tal que $b = a \cdot k$. Multiplicando m em ambos os lados da igualdade temos $b \cdot m = a \cdot k \cdot m$ e tomando o produto $k \cdot m = t$ chegamos em $b \cdot m = a \cdot t$ o que nos leva à conclusão de que $a \mid b \cdot m$. □

Proposição 1.5. *Se $a \mid b$ e $a \mid c$ então $a \mid (bx + cy)$, para quaisquer inteiros x e y.*

Demonstração. Pela proposição 1.4 sabemos que se $a \mid b$ então $a \mid bx$ e também que se $a \mid c$ então $a \mid cy$. Pela proposição 1.3 temos que se $a \mid bx$ e $a \mid cy$ então $a \mid (bx + cy)$ que é exatamante o que queríamos mostrar. □

Além das propriedades de divisibilidade o Máximo Divisor Comum (mdc) também será importante para chegarmos a resultados importantes.

1.2.1 Máximo divisor comum

Definição 1.5. *Sejam a e $b \in \mathbb{Z}$. Um número d inteiro é o máximo divisor comum de a e b, ou ainda, $mdc(a, b) = d$ se:*

i) $d \mid a$ e $d \mid b$

ii) se existe c inteiro tal que $c \mid a$ e $c \mid b$, então $c \mid d$

Por exemplo, seja D_n o conjunto de divisores inteiros de n e tomemos os divisores dos números 16 e 24, $D_{16} = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$ e $D_{24} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$. Podemos observar que o maior número que divide 16 e 24 é 8, ou seja, $8 \mid 16$ e $8 \mid 24$ então se existe um outro número c tal que se $c \mid 16$ e $c \mid 24$ temos que $c \mid 8$ como é o caso dos números 4 e 2 neste exemplo. Notemos que este método para calcular o *mdc* se torna cansativo quando a quantidade de divisores é muito grande. Um método mais prático é o Algorítmo de Euclides que veremos mais adiante.

Podemos observar que tomando a e b inteiros temos as igualdades $mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b)$ e dessa forma, podemos supor sempre a e b inteiros não negativos sem perda de generalidade. Mais precisamente:

Definição 1.6. *Se a,b* $\in \mathbb{Z}$*, então, por definição,* $mdc(a,b) = mdc(|a|,|b|)$

Definição 1.7. *Dois números inteiros a e b são ditos primos entre si se* $mdc(a,b) = 1$.

Podemos observar essa definição tomando os números 10 e 21. Sabemos que ambos não são primos mas como $mdc(10,21) = 1$, ou seja, o máximo divisor entre eles é 1, dizemos então que 10 e 21 são primos entre si.

Proposição 1.6. *Sejam* a *e* $b \in \mathbb{Z}$*, se* $a \mid b$ *então* $mdc(a,b) = |a|$.

Demonstração. Sabemos que $a \mid a$ e por hipótese $a \mid b$, o que implica em $a \leq b$. Como não há um número maior que a que o divida então o maior número que divide simultaneamente a e b é o próprio a.

□

Lema 1. *(Lema de Euclides) Sejam* $a, b, n \in \mathbb{Z}$*. Se existe* $mdc(a, b - na)$*, então* $mdc(a,b)$ *existe e*

$$mdc(a,b) = mdc(a, b - na)$$

Demonstração. Considerando $mdc(a, b - na) = d$ sabemos que $d \mid a$ e $d \mid b - na$. Pela Proposicão 1.5, temos que se $d \mid b - na \Rightarrow b \mid b - na + na = b$. Logo, d é divisor comum de a e b. Supondo agora um c que seja divisor comum de a e b, temos que c é divisor de a e $b - na$ e então $c \mid d$. Isto prova que $d = mdc(a,b)$.

□

Proposição 1.7. *Se* $a = bq + r$ *e* $d = mdc(a,b)$*, então* $d = mdc(b,r)$.

Demonstração. Como $d = mdc(a,b)$ sabemos que $d \mid a$ e $d \mid b$. Se $d \mid b$ então $d \mid bq$ e também $d \mid a - bq$. Note que $a - bq = r$ e portanto $d \mid r$. □

1.2.2 Algoritmo de Euclides

O Algoritmo de Euclides é o método prático para se calcular o *mdc* entre dois números. De acordo com HEFEZ (2013) pouco conseguiu-se aprimorar este método por milênios. Tomemos a e b naturais e supomos $b \leq a$. Se $b = 1$ então $mdc(a,1) = 1$ e também se $b = a$ temos que $mdc(a,b) = a$. Dessa forma assumimos que $1 < b < a$ e $b \nmid a$ pela divisão euclidiana temos

$$a = bq_1 + r_1, \quad com \quad 0 < r_1 < b.$$

Para a igualdade acima temos duas possibilidades:

i) $r_1 \mid b$ e então $mdc(b,r_1) = r_1$ e pelo Lema 1 $mdc(b,r_1) = mdc(b, a - bq_1) = mdc(b,a) = mdc(a,b)$.

ii) $r_1 \nmid b$ e então, dividindo b por r_1 teremos $b = r_1q_2 + r_2$, com $0 < r_2 < r_1$.

Para $b = r_1q_2 + r_2$ teremos as mesmas possibilidades acima para o resto r_2 e o divisor r_1 e prosseguindo sucessivamente dessa forma até que cheguemos em um $r_n \mid r_{n-1}$ onde $mdc(a,b) = r_n$. Para sistematizar este método usaremos os que chamamos de "grade"para organizar os elementos da divisão da seguinte forma:

	q_1	
a	b	
r_1		

Prosseguindo de forma análoga, faz-se a divisão de b por r_1 colocando os valores na grade:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo sucessivamente da mesma forma teremos:

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

Como exemplo, vamos calcular o *mdc* dos números 416 e 352.

	1	5	2
416	352	64	32
64	32	0	

Portanto $(416, 352) = 32$.

Proposição 1.8. *(Relação de Bézout) Dados inteiros a e b diferentes de zero, existem dois inteiros m e n tais que* $mdc(a,b) = am + bn$.

Demonstração. Consideremos a combinação linear $ax + by$ onde x e y percorrem todos os inteiros. Denotamos este conjunto por $I = \{ax + by; x, y \in \mathbb{Z}\}$. Note que, sendo $I = \{ax + by; x, y \in \mathbb{Z}\}$ vê-se que ele possui elementos positivos considerando $x = a$ e $y = b$. Como a e b são não nulos por hipótese, $a^2 + b^2 > 0$ e então, pelo PMI, podemos escolher m e n tais que $d = am + bn$ seja o menor inteiro positivo contido no conjunto I. Agora mostraremos que $d \mid a$ e $d \mid b$. Provaremos que $d \mid a$ e o outro é análogo. A prova

será feita por redução ao absurdo de forma que vamos supor $d \nmid a$ e obteremos uma contradição. Pela divisão euclidiana, se $d \nmid a$ então existem q e r tais que $a = dq + r$ com $0 < r < d$. Portanto temos,

$$r = a - dq = a - q(am + bn) = a(1 - qm) + b(-qn)$$

e dessa forma temos que $r \in I$, contradizendo a hipótese de d ser o menor elemento positivo do conjunto I. □

Proposição 1.9. *Se $mdc(a, b) = d$ então $mdc(sa, sb) = sd$ para todo s natural.*

Demonstração. Utilizando o algorítmo da divisão para calcular $mdc(a, b)$ e tomando $a > b$ temos:

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1q_2 + r_2 \\
r_1 &= r_2q_3 + r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

Multiplicando as igualdades por s temos:

$$\begin{aligned}
sa &= sbq_1 + sr_1 \\
sb &= sr_1q_2 + sr_2 \\
sr_1 &= sr_2q_3 + sr_3 \\
&\vdots \\
sr_{n-2} &= sr_{n-1}q_n + sr_n \\
sr_{n-1} &= sr_nq_{n+1}
\end{aligned}$$

De acordo com as proposições 1.1 e 1.2 temos que:

$sd = sr_n = mdc(sr_{n-1}, sr_n) = \ldots = mdc(sb, sr_1) = mdc(sa, sb)$

□

Corolário 1. *Se $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.*

Demonstração. Se temos como hipótese que $mdc(a,b) = 1$ da Proposição 1.9 acima temos que $mdc(ac,bc) = c$. Como, por hipótese, $a \mid bc$ e com certeza $a \mid ac$, então $a \mid mdc(ac,bc) = c \Rightarrow a \mid c$.

□

Conhecendo as propriedades de divisibilidade e máximo divisor comum anteriores, vejamos uma propriedade importante de divisibilidade envolvendo um número primo.

Proposição 1.10. *Seja p um número primo e $p \mid ab$. Então, $p \mid a$ ou $p \mid b$.*

Demonstração. É suficiente provar que se $p \mid ab$ e $p \nmid a$ então $p \mid b$. Como p é primo temos as seguintes possibilidades para $mdc(a,p)$: se $p \mid a$ então $mdc(a,p) = p$ e se $p \nmid a$ então $mdc(a,p) = 1$. Supondo que $p \nmid a$ temos que $mdc(p,a) = 1$. Dessa forma, pelo corolário 1, temos que $p \mid b$.

□

Com os conhecimentos de divisibilidade e *mdc* podemos mostrar dois teoremas fundamentais para o estudo da aritmética e igualmente dos números primos. Segue abaixo o Teorema Fundamental da Aritmética (TFA) e o resultado que mostra a infinidade dos números primos.

Teorema 1.2. *(Teorema Fundamental da Aritmética) Seja $n \in \mathbb{N}$, com $n \geq 2$, então n pode ser escrito de forma única (a não ser pela ordem dos fatores) como o produto*

$$n = p_1 \dots p_m$$

onde $m \geq 1$ e p_i é primo para $1 \leq i \leq m$.

Demonstração. Mostramos a existência da fatoração de n em primos por indução. Se n é primo não há o que provar (escrevemos $m = 1, p_1 = n$). Se n é composto podemos escrever $n = ab$, com a e b $\in \mathbb{N}$, tal que $1 < a < n$ e $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n. Vamos agora mostrar a unicidade. Suponhamos que n possui duas fatorações diferentes

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \cdots \leq p_m$, $q_1 \leq \cdots \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 \mid q_1 \cdots q_{m'}$ temos $p_1 \mid q_i$ para algum valor de i pelo Corolário 1. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \geq p_1$, donde $p_1 = q_1$. Mas

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, pela minimalidade de n, donde $m = m'$ e $p_i = q_i$ para todo i o que contradiz o fato de n ter duas fatorações. □

Teorema 1.3. *Existe uma infinidade de números primos.*

Demonstração. Suponhamos que o conjunto P de todos os números primos seja finito, ou seja, que existe $r \in \mathbb{N}$ tal que $P = \{p_1, p_2, \cdots, p_r\}$. Neste caso, tomando o produto de todos os primos $A = p_1 \cdot p_2 \cdot \ldots \cdot p_r$, teríamos que seu sucessor $A + 1$ não poderia ser um número primo, pois evidentemente não pertenceria a P e nem poderia ser um número composto, pois não seria divisível por número primo algum (a divisão por qualquer número primo daria resto 1), contrariando o que diz o TFA. Como todo número inteiro é um número primo ou um número composto, teríamos um absurdo. Sendo a única hipótese considerada a da finitude de P, o conjunto dos números primos não pode ser finito.

□

Tomando $p\#$ como sendo o produto de todos os primos menores ou iguais a p, temos que $p\#$ é chamado o primorial de p. Sobre a ideia de primorial segue abaixo dois problemas em aberto:

i) Existe uma infinidade de números primos p tais que $p\# + 1$ seja primo ?

ii) Existe uma infinidade de números primos p tais que $p\# + 1$ seja composto ?

Sabendo que os números primos são infinitos é comum pensarmos em como identificá-los e como encontrá-los. Veremos agora um método para identificar números primos.

1.3 Como identificar os números primos ?

No ensino básico pouco se fala sobre os números primos. Os alunos até compreendem que para um número ser primo ele só pode ser divisível por um e por ele mesmo. Também sabem fazer a decomposição de um número composto em fatores primos. Mas como reconhecer um número primo? Segundo BOYER (1974), o matemático Eratóstenes, por volta do século III A.C., teve a ideia de construir um método que leva seu próprio nome, o "Crivo de Eratóstenes". O crivo serve para determinar os

números primos inferiores a um número N bem como seus múltiplos menores que N. Inicialmente faz-se a listagem dos números menores que N e risca todos os múltiplos de 2, depois de 3 e assim sucessivamente até que restem apenas os números primos. Abaixo, segue o Crivo de Eratóstenes para $N = 51$:

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11
~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~
~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31
~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	39	~~40~~	41
~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~	~~51~~

Tabela 1 – Crivo de Eratósteles

De acordo como crivo acima observamos que os números primos N tal que $2 \leq N \leq 51$ são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 39, 41, 43 e 47. O Lema a seguir é referente ao critério de parada do Crivo de Eratóstenes:

Lema 2. *Seja n composto, então n possui um fator primo p tal que* $p \leq \sqrt{n}$.

Demonstração. Suponhamos, que n é um número composto tal que $n = ab$. Sem perda de generalidade admitimos que $a \leq b$. Dessa forma, devemos ter $a \leq \sqrt{n}$, pois se $a > \sqrt{n}$ então

$$n = ab > \sqrt{n} \cdot \sqrt{n} = n$$

o que é absurdo. Sabemos que a pode ser primo ou composto. Se a é primo está mostrado. Se a é composto então pelo TFA pode ser escrito como produto $a = p_i \cdot \alpha$ onde p_i é primo e menor que a.

□

Além do crivo de Eratóstenes, um outro método de identificar um número primo é o da decomposição em fatores primos que é apresentada aos estudantes no ensino básico. Um número que ao ser decomposto não possui mais do que dois divisores com certeza será primo. Assim como Eratóstenes, outros matemáticos iniciam suas buscas por relações e fórmulas que se referem aos números primos como será apresentado na sequência.

2 Alguns Primos Específicos

2.1 Primos de Fermat e Mersenne

O matemático amador Pierre de Fermat nasceu na França em (1601-1665) e tinha como interesse na matemática a Teoria do Números. De acordo com HEFEZ (2013), Fermat trocava correspondências com Marin Mersene mandando desafios matemáticos e havia enviado a ele, até então, uma conjectura para a fórmula os primos na qual dizia que todos os números da forma $2^{2^n}+1$ eram primos. Apenas no ano de 1732, o matemático Suíço Leonhard Euler mostrou que a conjectura dos números primos de Fermat não era válida para $n = 5$, pois $2^{2^5}+1 = 4.294.967.297$ trata-se de um número composto que pode ser escrito $641 \times 6.700.417$.

Definição 2.1. *Todo número da forma $F_n = 2^{2^n}+1$ com $n \in \mathbb{N}$ é chamado número de Fermat.*

De fato, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65.537$ são primos, mas não se sabe se existem outros primos de Fermat além dos cinco primeiros. Os matemáticos Hardy e Wrigth conjecturaram que existem infinitos primos de Fermat. Alguns problemas que estão em aberto, relacionados aos primos de Fermat, são:

i) Existem uma infinidade de Números de Fermat primos?

ii)Todo número de Fermat não possui um fator quadrado.

iii) Existem uma infinidade de Números de Fermat compostos ?

Definição 2.2. *Todo número da forma $M_q = 2^q - 1$, onde q é um número primo, é chamado número de Mersenne.*

Também aos Números de Mersenne são relacionados problemas ainda em aberto:

i) Existe algum Número de Mersenne par?

ii) Existem infinitos números de Mersenne?

iii) Existem infinitos primos de Mersenne?

Teorema 2.1. *Se $2^q - 1$ é primo então q é primo.*

Demonstração. Suponha $q = ab$ com $a, b > 1$. Como $2^a - 1 > 1$, segue que $2^q - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \mod (2^a - 1)$, provando que $2^q - 1$ é composto. □

Até Abril de 2010, os nove maiores números primos conhecidos eram da forma M_q para os valores de $q = 443112609, 42643801, 37156667, 32582657, 30402457, 25964951, 24036583, 200996011, 13466917$. Até então, estes eram os únicos números primos conhecidos com mais de 4000000 dígitos. Desta data até novembro de 2017, os seis maiores primos conhecidos são primos de Mersenne e o maior deles é o $M_{74207281}$. Esse número foi encontrado graças a um projeto chamado Great Internet Mersenne Prime Search (GIMPS) que é destinado à busca pelos primos de Mersenne e eles vem se superando cada vez mais. Por último, em janeiro de 2018, encontraram mais um primo de Mersenne, o $M_{77232917}$ com quase um milhão de algarismos a mais que o $M_{74207281}$.

2.2 Números Perfeitos

Definição 2.3. *Um número $n \in \mathbb{N}$ é dito perfeito quando for igual à soma de seus divisores naturais distintos de si mesmo. Ou seja, tomando $S(n)$ como sendo a soma dos divisores de $n \in \mathbb{N}$, n é perfeito quando $S(n) = 2n$.*

Vejamos por exemplo o número 6. Seus divisores são 1, 2, 3 e 6. Temos então que a soma dos divisores de 6 é igual a 12 e portanto 6 é um número perfeito.

Observação: Seja $n \in \mathbb{N}$. Tem-se que $S(n) = n + 1$ se, e somente se, n é um número primo.

Proposição 2.1. *Seja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ um número natural escrito na forma fatorada. Se n' é um divisor positivo de n, então*

$$n' = p_1^{\beta_1} \cdots p_r^{\beta_r},$$

onde $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \cdots, r$.

Demonstração. Seja n' um divisor positivo de n e seja p^β a potência de um primo p que figura na decomposição de n' em fatores primos. Como $p^\beta \mid n$, segue que p^β divide algum $p_i^{\alpha_i}$, por ser primo com os demais $p_j^{\alpha_j}$, e, consequentemente, $p = p_i$ e $0 \leq \beta \leq \alpha_i$. □

Proposição 2.2. *Seja $n = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ a decomposição de n em fatores primos. Então,*

$$S(n) = \frac{P_1^{\alpha_1+1}-1}{P_1-1} \cdots \frac{P_r^{\alpha_r+1}-1}{P_r-1}$$

Demonstração. Considere a igualdade

$$(1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_r + \cdots + p_r^{\alpha_r}) = \sum p_1^{\beta_1} \cdots p_r^{\beta_r},$$

onde o somatório do lado direito da igualdade é tomado sobre todas as r-uplas $(\beta_1, \cdots, \beta_r)$ ao variar cada β_i no intervalo $0 \leq \beta_i \leq \alpha_i$, para $i = 0, \cdots, r$. Como tal somatório, pela proposição 2.1, representa a soma de todos os divisores de n, a fórmula para $S(n)$ resulta aplicando a fórmula da soma de uma progressão geométrica a cada soma do lado esquerdo da igualdade acima. □

2.2.1 Relação entre primos de Mersenne e números perfeitos

Proposição 2.3. *Se M_p é um primo de Mersenne então $2^{p-1}M_p$ é perfeito. Além disso, todo número perfeito par é da forma $2^{p-1}M_p$ para algum primo p, sendo M_p um primo de Mersenne.*

Demonstração. Se M_p é primo então

$$S(2^{p-1}M_p) = S(2^{p-1}) \cdot S(M_p) = (2^p - 1)(M_p + 1) = 2 \cdot 2^{p-1}M_p$$

Por outro lado seja $n = 2^k b$, com $k > 0$ e b ímpar, um número perfeito par. Temos $S(n) = 2n = S(2^k)S(b)$ donde $2^{k+1}b = (2^{k+1} - 1)S(b)$. Como mdc $(2^{k+1} - 1, 2^{k+1}) = 1$, temos $b = (2^{k+1} - 1)c$ para algum inteiro c e assim $S(b) = 2^{k+1}c$. Mas $1, 2^{k+1} - 1, c, b$ são divisores de $b = (2^{k+1} - 1)c$; se $c > 1$ então $S(b) = 2^{k+1}c \geq 1 + 2^{k+1} - 1 + b$, o que implica $c \geq 2^{k+1}$, mas neste caso $S(b) = 2^{k+1}c \geq 1 + 2^{k+1} - 1 + b + c$, um absurdo. Logo $c = 1$ e $b = 2^{k+1} - 1$ é primo pois $S(b) = 2^{k+1}$. Pelo teorema 1.3, $p = k + 1$, é primo, $b = M_p$ e $n = 2^{p-1}M_p$.

□

2.3 O Pequeno Teorema de Fermat e Teorema de Wilson

Alguns resultados importantes para testar a primalidade e também para o resultado final deste estudo são os teoremas de Fermat e Wilson. Como ambos os teoremas apoiam-se na congruência, serão mostradas algumas proposições importantes antes dos teoremas principais. Iniciaremos este assunto com um problema:

O dia 10 de maio de 2018 foi uma quinta feira. O dia 5 de novembro do mesmo ano será em qual dia da semana?

Para iniciar a resolução deste problema observamos que a partir do dia 10 de maio, a cada 7 dias, será uma quinta feira. Então, primeiro precisamos saber quantos dias existem entre 10 de maio e 1 de novembro. Vejamos:

10 a 31 de maio $\rightarrow$ 21 dias
1 a 30 de junho $\rightarrow$ 30 dias
1 a 31 de julho $\rightarrow$ 31 dias

$$1 \text{ a } 31 \text{ de agosto} \rightarrow 31 \text{ dias}$$
$$1 \text{ a } 30 \text{ de setembro} \rightarrow 30 \text{ dias}$$
$$1 \text{ a } 31 \text{ de outubro} \rightarrow 31 \text{ dias}$$
$$1 \text{ a } 5 \text{ de novembro} \rightarrow 5 \text{ dia}$$

Totalizando 179 dias do dia 10 de maio até 1 de novembro de 2018. Desta maneira, se a cada 7 dias é uma quinta-feira, o importante aqui é saber o resto da divisão de 179 por 7. Logo temos $179 = 7 \cdot 25 + 4$, ou seja, o resto da divisão é 4. Observe que se o resto fosse igual a 0 o dia 5 de novembro seria novamente uma quinta-feira. Como o resto é 4, temos que contar 4 dias da semana após a quinta, o que nos dá uma segunda-feira. No sentido em que vamos falar abaixo, neste exemplo dizemos que $179 \equiv 4 \mod 7$, e lemos "179 é congruente a 4 módulo 7".

Definição 2.4. *Sejam $a, b, n \in \mathbb{Z}$, dizemos que a é congruente a b módulo n, e escreve-se*

$$a \equiv b \mod n$$

se $n \mid a - b$, ou seja, se a e b deixam o mesmo resto na divisão por n.

Para ficar mais clara esta definição tomemos por exemplo que $10 \equiv 2 \mod 4$ pois 10 deixa resto 2 na divisão por 4. Algumas consequências desta definição seguem abaixo, onde temos a, b e $c \in \mathbb{Z}$ e $n \in \mathbb{N}$:

Proposição 2.4. *$a \equiv a \mod n$.*

Proposição 2.5. *Se $a \equiv b \mod n$, então $b \equiv a \mod n$.*

Proposição 2.6. *Se $a \equiv b \mod n$ e $b \equiv c \mod n$, então $a \equiv c \mod n$.*

Também tem-se a flexibilidade com a soma e diferença com duas congruências de mesmo módulo, pode somar ou subtrair em ambos os lados da congruência, muito parecido com o procedimento nas equações. Veja:

Proposição 2.7. *Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então $a + c \equiv b + d \mod n$.*

Proposição 2.8. *Se $a \equiv b \mod n$, então $ka \equiv kb \mod n$ para todo $k \in \mathbb{Z}$.*

Muito parecido com a proposição 2.7 pode ser feita a multiplicação dos membros correspondentes entre duas congruências de mesmo módulo. Veja:

Proposição 2.9. *Se $a \equiv b \mod n$ e $c \equiv d \mod n$ então $ac \equiv cd \mod n$ e ainda, se $a \equiv b \mod n$ então $a^k \equiv b^k \mod n$ para todo $k \in \mathbb{Z}$.*

Também é válida a regra do cancelamento.

Proposição 2.10. *Seja* $mdc(c,n) = 1$, *então* $ac \equiv bc \mod n \Rightarrow a \equiv b \mod n$.

Demonstraremos as proposições 2.7 e 2.8. O restante se prova por meio de argumentos semelhantes.

Demonstração. (2.7) Supondo que $a \equiv b \mod n$ temos que $n \mid b-a$ e também, se $c \equiv d \mod n$ temos que $n \mid d-c$. Dessa forma temos que $b-a = nk$ para algum k inteiro e $d-c = nf$ com f inteiro. Somando as duas equações temos $(b-a)+(d-c) = n(f+k)$, ou ainda, $(b+d)-(a+c) = n(f+k)$ que nos dá $(a+c) \equiv (b+d) \mod n$.

□

Demonstração. (2.8) Supondo $a \equiv b \mod n$ temos que $n \mid b-a \Rightarrow b-a = nf$ para algum f inteiro. Multiplicando um k inteiro em ambos os lados da igualdade chegamos a $bk-ak = nfk$, que implica $n \mid bk-ak$ ou ainda $ak \equiv bk \mod n$.

□

As proposições apresentadas acima fazem da congruência uma ferramenta muito poderosa na matemática. Podemos por exemplo encontrar o resto da divisão 6561^{2018} por 4 da seguinte maneira:

- fazendo a fatoração de 6561 temos 9^4

- $9 \equiv 1 \mod 4$

- então $9^4 \equiv 1^4 \mod 4$ (pela proposição 2.7)

- Logo temos $6561^{2018} \equiv 1^{2018} = 1 \mod 4$

Dessa forma encontramos resto 1 para a divisão de 6561^{2018} por 4. Conhecendo esta parte das congruências enuncia-se abaixo O Pequeno Teorema de Fermat (PTF).

Teorema 2.2. *Se* p *é um número primo e* $a \in \mathbb{Z}$, *então* $a^p \equiv a \mod p$ *e ainda, se* $p \nmid a$, *então* $a^{p-1} \equiv 1 \mod p$

Demonstração. Por indução em a, temos que por hipótese o resultado é válido para a. Então temos que para $a+1$ usamos o binômio de Newton para expandir

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1$$

Na expansão acima temos que $\binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a$ tem todas as parcelas inteiras e múltiplas de p e dessa forma na divisão de $(a+1)^p$ por p teremos resto igual a a^p+1, ou seja, $(a+1)^p \equiv a^p + 1 \equiv a+1 \mod p$.

Logo temos que $a^p \equiv a \mod p$, para todo $a \in \mathbb{Z}$.

□

Pode-se utilizar este teorema para resolver problemas de divisibilidade como encontrar o resto de divisão de 12^{12} por 5 . Para resolver este exemplo sabemos que pelo PTF $12^4 \equiv 1 \mod 5$ e então $(12^4)^3 = 12^{12} \equiv 1^3 \mod 5 \Rightarrow 12^{12} \equiv 1 \mod 5$.

O próximo resultado é chamado Teorema de Wilson e é fundamental para o objetivo final desta pesquisa.

Teorema 2.3. *(Teorema de Wilson) Se p é um número primo, então*

$$(p-1)! \equiv -1 \pmod{p}$$

.

Demonstração. O teorema é verdadeiro para $p = 2$ e para $p = 3$, pois:

$$(2-1)! = 1! = 1 \equiv -1 \pmod{2}$$

$$(3-1)! = 2! = 2 \equiv -1 \pmod{3}$$

De modo que podemos supor que $p \geq 5$. Consideremos a congruência $aX \equiv 1 \pmod{p}$ onde $a \in \{1, 2, \ldots, p-1\}$, ou seja, a é um dos $p-1$ primeiros números primos. Em particular, a e p são primos entre si, o que implica que $(a, p) = 1$. Então a congruência acima sendo equivalente à equação diofantina $aX + pY = 1$, possui solução, de acordo com a Relação de Bézout (Proposição 1.8). Por um lado, observe que se x e x_0 são soluções de $aX \equiv 1 \pmod{p}$, então $ax \equiv ax_0 \pmod{p}$, o que implica que $x \equiv x_0 \pmod{p}$ pela proposição 2.10 acima. E reciprocamente, se x_0 é solução de $aX \equiv 1 \pmod{p}$ e $x \equiv x_0 \pmod{p}$, então x também é solução da congruência $aX \equiv 1 \pmod{p}$, pois $ax \equiv ax_0 \pmod{p}$, desta vez de acordo com a proposição 2.8 acima. Ora, o que acabamos de ver é que as soluções da congruência em questão estão sempre na mesma classe de congruência e, portanto, são essencialmente a mesma solução da equação $aX \equiv 1 \pmod{p}$. Concluímos então que se $a \in \{1, 2, \ldots, p-1\}$, existe único $b \in \{1, 2, \ldots, p-1\}$ tal que $ab \equiv 1 \pmod{p}$. Como p é primo, tem-se que $b = a$ se e somente se $a = 1$ ou $a = p-1$, pois $a = b$ implica $a^2 \equiv 1 \pmod{p}$ que acarreta $(a-1)(a+1) \equiv 0 \pmod{p}$, e daí, $a - 1 \equiv 0 \pmod{p}$ ou $a + 1 \equiv 0 \pmod{p}$, isto é, $a = 1$ ou $a = p-1$. O que tudo isto quer dizer? Isto significa que se omitirmos os inteiros 1 e p-1, com os p-3 restantes: $2, 3, \ldots, p-2$ podemos formar $\frac{1}{2}(p-3)$ pares a e b com $a \neq b$, tais que $ab \equiv 1 \pmod{p}$. Então, multiplicando convenientemente todas essas $\frac{1}{2}(p-3)$ congruências obtemos que $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$ ou, o que é o mesmo, $(p-2)! \equiv 1 \pmod{p}$. Multiplicando por $p-1$:

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$$

□

Um exemplo da formação dos pares discutida na demonstração do Teorema de Wilson: considerando $p = 13$:

A	1	2	3	4	5	6	7	8	9	10	11	12
B	1	7	9	10	8	11	2	5	3	4	6	12

Descartando 1 e $p - 1 = 12$, os dez inteiros $2, 3, \ldots, 11$ dão lugar a $\frac{p-3}{2} = 5$ pares tais que o produto dos inteiros de cada par é congruente a 1 módulo 13:

$2 \cdot 7 \equiv 1 \pmod{13}$, $3 \cdot 9 \equiv 1 \pmod{13}$, $4 \cdot 10 \equiv 1 \pmod{13}$, $5 \cdot 8 \equiv 1 \pmod{13}$ e $6 \cdot 11 \equiv 1 \pmod{13}$

Multiplicando ordenadamente estas congruências obtemos:

$$(2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

ou seja, $(p-1)! \equiv p - 1 \equiv -1 \mod p$, para $p = 13$.

A recíproca do Teorema de Wilson é verdadeira, ou seja, o teorema de Wilson pode ser utilizado para testar se um número é primo ou não. Se o número p satisfaz a congruência $(p-1)! \equiv -1 \pmod{p}$, então p é primo. Vejamos:

Proposição 2.11. *Seja $p \geq 2$ um inteiro. Se $(p-1)! \equiv -1 \pmod{p}$, então p é primo.*

Demonstração. Suponha agora que p seja um número composto e que

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$$

então p possui um divisor primo d tal que $1 < d < p$, de maneira que d é um dos fatores do produto $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = (p-1)!$ e, portanto, $d \mid (p-1)!$. Como por hipótese $p \mid [(p-1)! + 1]$ e d é um divisor de p, segue que $d \mid [(p-1)! + 1]$ e, então, $d \mid 1$, o que é um absurdo, visto que $d > 1$. Logo, p não pode ser composto, tem que ser primo. □

Desta forma vamos verificar como exemplo se o número é primo ou não.

O número 11 é primo ou composto? Já temos certeza que o número 11 é primo. Verificando pelo teorema de Wilson temos que $(11-1)! \equiv -1 \pmod{11}$. Desenvolvendo as contas $3628800 \equiv -1 \pmod{11}$ e essa congruência é equivalente a $3628801 \equiv 0 \pmod{11}$. Dessa forma, o número 3628801 tem que ser divisível por 11 e é verdadeiro pois $3628801 = 329891 \cdot 11$.

3 Polinômios e funções que geram números primos

Os números primos são um verdadeiro enigma da matemática pois não existe nenhuma fórmula precisa que os caracterize por completo nem tão pouco que explique sua distribuição. Alguns matemáticos trabalharam muito tempo para tentar resolver estes problemas com primos. Neste capítulo vamos tratar das funções e polinômios que são conhecidos para mostrar algo sobre os primos.

Inicialmente serão mostrados alguns polinômios com coeficientes inteiros que tem forte relação com os primos e o primeiro deles, segundo RIBENBOIM (2012) deve-se a Euler que em 1772 descobriu um polinômio com uma sucessão de valores primos. Para esses polinômios, existem números naturais m e n, com $0 \neq m < n$ tais que $f(k)$ seja primo, para todo k, com $m \leq k \leq n$. O famoso polinômio de Euler é:

Seja $f(X) = X^2 + X + 41$. Para $X = 0, 1, 2, 3, ..., 39$, todos seus valores são números primos. A título de curiosidade segue a listagem destes resultados: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 e 1601. Se tomarmos $X = 40$ temos $f(40) = 1681 = 41^2$. Considerando a função polinomial $f(X) = X^2 + X + q$, onde q é primo gera números primos para q = 2, 3, 5, 11, 17 ou 41 onde os valores de $X \in \{0, 1 \ldots, q-2\}$ sendo o que apresenta a maior quantidade é quando q = 41. Neste mesmo polinômio de Euler existe uma variação curiosa. Se tomarmos o polinômio $f(x) = x^2 - x + 41$, que se diferencia do $f(X)$ apenas na mudança de sinal da variável com expoente 1, com os valores de $x = 1, 2, 3, ..., 40$ os primos encontrados são os mesmos.

Euler também considerou o polinômio $2X^2 + p$ com p = 3, 5, 11 e 29 e mostrou resultados em números primos para todo $X \in \{0, 1, \ldots, p-1\}$ como também $f(X) = 2X^2 + 2X + \frac{p+1}{2}$, sendo p um primo da forma $4k + 1$ para $k \in \mathbb{Z}$, tal que $x \in \left\{0, 1, \ldots, \frac{p-3}{2}\right\}$ gera números primos para p = 5, 13 e 37.

Além de Euler outros matemáticos trabalharam na procura de polinômios geradores. Fung e Ruby (1990) encontraram o polinômio $36x^2 - 810x + 2753$, que gera 45 primos distintos, e ainda $47x^2 - 1701x + 10181$ que tem 43 primos distintos. Em 2005 Ruiz encontrou $3x^3 - 183x^2 + 3318x - 18757$ que gera 43 primos distintos. Speiser (2005) também encontrou o polinômio $103x^2 - 4707x + 50383$ que gera 43 primos distintos. Dress e Landreau em 2003 acharam polinômios de grau superior sendo um deles $f(X) = 66X^3 + 83X^2 - 13735X + 30139$ o qual $\mid f(X) \mid$ é primo quando

$-26 < X < 19$, obtendo 46 números primos; e o outro é $f(X) = 16X^4 + 28X^3 - 1685X^2 - 2380X + 110647$ que também para $\mid f(X) \mid$ gera 46 números primos com $-2 < X < 22$. Como a quantidade de polinômios deste tipo é grande, os mostrarei em uma tabela ao final deste capítulo.

Entretanto, em uma carta de Goldbach à Euler em 1743 já havia sido apresentado um resultado um tanto interessante:

Teorema 3.1. *Se $f(X)$ é um polinômio não-constante, de coeficientes inteiros e em uma variável, existe uma infinidade de inteiros n tais que $\mid f(n) \mid$ não seja um número primo.*

Demonstração. Como o polinômio não é constante, seria trivial se todos os seus valores fossem números compostos. Então pode-se supor que exista um inteiro $n_0 \geq 0$ tal que $\mid f(n_0) \mid = p$ seja número primo. Como o polinômio não é constante, $\lim_{x\to\infty} \mid f(x) \mid = \infty$ existe então $n_1 > n_0$ tal que , se $n \geq n_1$, então $\mid f(n) \mid > p$. Para todo inteiro h tal que $n_0 + ph \geq n_1$, tem-se que $f(n_0 + ph) = f(n_0)+$ (múltiplo de p) = (múltiplo de p).

Sendo suposto $\mid f(n_0 + ph) \mid > p, \mid f(n_0 + ph) \mid$ é então um número composto. □

De acordo com o resultado acima, sabemos que um polinômio com coeficientes inteiros não fornece somente números primos.

O matemático MILLS (1946), mostrou que existe um número real $\gamma > 0$ onde $[\gamma^{3^n}]$ é primo para $n \in \mathbb{Z}; n \geq 1$ e o valor de γ é aproximadamente igual a 1,3064. Os números primos da forma $[\gamma^{3^n}]$ são chamados primos de Mills. Os números $[\gamma^{3^{11}}]$ e $[\gamma^{3^{12}}]$ foram calculados por P. Carmody e têm respectivamente, 20562 e 61684 algarismos.

Indicando por $\pi(x)$ a quantidade de primos menores que x, tem-se uma fórmula para $\pi(m)$ dada por Willans em 1964 baseando-se no Teorema de Wilson (Teorema 3.3).

Definição 3.1. *Para todo inteiro $j \geq 1$, seja*

$$F(j) = \left[Cos^2 \pi \frac{(j-1)!+1}{j}\right]$$

onde $[x]$ é o maior inteiro n tal que $n \leq x$ sendo x um número real positivo.

Pelo Teorema 2.3 sabemos que se j é primo então $j \mid (j-1)! + 1$ e então $F(j) = [Cos^2 \pi k]$ onde k é inteiro será sempre igual a 1 tendo em vista que $Cosk\pi = 1$ ou -1 mas como em $F(j)$ temos Cos² será sempre 1. Tomando j composto em $F(j) = [Cos^2 \pi k]$ onde k não é inteiro fazendo $0 < F(j) < 1$ e então $F(j) = 0$. Com isso, temos a seguinte fórmula de Willans para $\pi(m)$:

$$\pi(m) = -1 + \sum_{j=1}^{m} F(j)$$

O mesmo Willans ainda expressou $\pi(m)$ em uma fórmula utilizando seno ao invés de cosseno. Minác apresentou também uma $\pi(m)$ onde não utilizava valores de seno ou cosseno mas também baseada no Teorema de Wilson. Como esta foi publicada pela primeira vez em RIBENBOIM (2012) pág: 131 e é onde também encontra-se sua demonstração, será apresenta aqui. Segue:

$$\pi(m) = \sum_{j=2}^{m} \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right]$$

Dadas as definições, o que temos agora é a fórmula de Willans para o enésimo número primo:

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left(\frac{n}{1+\pi(m)} \right)^{\frac{1}{n}} \right]$$

3.1 Função que gera todos os números primos

Os matemáticos Putnam, Davis, J. Robinson e Matijasevic desenvolveram uma teoria sobre números primos que permite concluir:

Existe um polinômio de coeficientes inteiros, cujo qual o conjunto dos números primos coincide com o conjunto dos valores positivos assumidos por esse polinômio quando as variáveis percorrem o conjunto dos números inteiros positivos.

Na tradução deste trabalho por JONES (1976) eles foram os primeiros a explicitar um polinômio de grau 25 e com 26 variáveis a, b, c, . . ., z de forma que quando números inteiros não negativos são substituídos nessas variáveis os valores positivos coincidem exatamente com o conjunto de todos os números primos. Segue o polinômio:

$$\begin{aligned}
&(k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2\\
&-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2\\
&-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2\\
&-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))-1)(n+4dy)^2\\
&+1-(x+cu)^2]^2-[n+l+v-y]^2-[(a^2-1)l^2+1\\
&-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a\\
&-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap+2a-p^2-2p\\
&-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}$$

Durante muito tempo muitos matemáticos se dedicaram arduamente procurando alguma fórmula que gerasse os números primos. Muitos professores ainda afirmam que não existe tal feito, mas segundo HONSBERGER (1976) a função que veremos agora diz exatamente o contrário.

Proposição 3.1. *Sejam x e y números naturais com $y \neq 0$ e $a = x(y+1) - (y!+1)$, então*

$$f(x,y) = \tfrac{y-1}{2}\left[\left|a^2-1\right| - (a^2-1)\right] + 2$$

nos dá todos os números primos e somente estes.

Vejamos alguns exemplos:

Para $x = 1$ e $y = 1$ temos $a = 1(1+1) - (1!+1) = 0$. Então $f(1,1) = \frac{1-1}{2}\left[\left|0^2-1\right| - (0^2-1)\right] + 2 = 2$

Para $x = 3$ e $y = 2$ temos $a = 3(2+1) - (2!+1) = 6$. Então $f(3,2) = \frac{2-1}{2}\left[\left|6^2-1\right| - (6^2-1)\right] + 2 = 2$

Para $x = 1$ e $y = 2$ temos $a = 1(2+1) - (2!+1) = 0$. Então $f(1,2) = \frac{2-1}{2}\left[\left|0^2-1\right| - (0^2-1)\right] + 2 = 3$

Para $x = 5$ e $y = 4$ temos $a = 5(4+1) - (4!+1) = 0$. Então $f(5,4) = \frac{4-1}{2}\left[\left|0^2-1\right| - (0^2-1)\right] + 2 = 5$

Após alguns testes admitindo valores quaisquer para x e y e observando as condições apresentadas percebemos que sempre que $a = 0$ o primo encontrado é o 2, o que acontece em muitas tentativas.

Nesse sentido, vamos mostrar que para x e y naturais a função $f(x,y)$ gera todos os primos e apenas estes.

Demonstração. Inicialmente notemos que o valor de a admite valores inteiros já que x e y são naturais, logo a^2 é positivo. Desta forma temos dois casos: i) $a^2 \geq 1$ e ii) $a^2 = 0$.

i) Se $a^2 \geq 1$ temos que $a^2 - 1 \geq 1$ e então $\mid a^2-1 \mid = a^2 - 1$. Logo, neste caso teremos $f(x,y) = 2$ que é primo.

ii) Se $a^2 = 0$ teremos:

$$f(x,y) = \tfrac{y-1}{2}[\mid -1 \mid -(-1)] + 2 = y + 1$$

O interessante é que se $a^2 = 0$ então $x(y+1) - (y!+1) = 0$ e ainda que $x(y+1) = (y!+1)$ o que nos dá $y+1 \mid y!+1$ ou ainda, se chamarmos $y = p-1$ temos exatamente o teorema de Wilson $p \mid (p-1)!+1$. Logo $y+1$ é um número

primo. Desta forma concluímos que para quaisquer valor natural de x e y a função $f(x,y)$ sempre será um número primo.

Sabendo que para $a = 0$ $f(x,y)$ é primo tomemos $x(y+1) - (y!+1) = 0$ de modo a encontrar x em função de y. Logo teremos $x = \frac{y!+1}{y+1}$ e chamando $y = p-1$ temos $x = \frac{(p-1)!+1}{p}$ o que nos dá $f\left(\frac{(p-1)!+1}{p}, p-1\right)$. Como pelo Teorema de Wilson $x = \frac{(p-1)!+1}{p}$ é natural e $y = p-1$ também é natural então $f(x,y)$ fornece todos os números primos.

□

Conhecendo os valores a serem atribuídos para x e y que fornecerão primos diferentes de 2 vamos fazer alguns testes de modo a encontrar x e y que geram os números primos que queremos encontrar.

Para $p = 11$ temos $x = \frac{(11-1)!+1}{11} = 329891$ e $y = 11-1 = 10$. Dessa forma $f(329891, 10) = 11$

Para $p = 13$ temos $x = \frac{(13-1)!+1}{13} = 36846277$ e $y = 13-1 = 12$. Dessa forma $f(36846277, 12) = 13$

Para $p = 17$ temos $x = \frac{(17-1)!+1}{17} = 1230752346353$ e $y = 17-1 = 16$. Logo, $f(1230752346353, 16) = 17$

Analisando os testes apresentados percebemos que o valor de x tende a aumentar rapidamente da mesma forma em que aumentamos o número primo que se deseja procurar e isso faz que com $f(x,y)$ seja algo pouco praticável. Entretanto, o fato é que existe sim uma função matemática sobrejetora cujo conjunto imagem é o conjunto dos números primos.

Tabela 2 – Polinômios que geram primos

Polinômios	primos de 0 a n	primos distintos	Referências
$\frac{1}{4}(n^5 - 133n^4 + 6729n^3 - 158379n^2 + 1720294n - 6823316)$	56	57	Dress e Landreau (2002),Gupta (2006)
$\frac{1}{36}(n^6 - 126n^5 + 6217n^4 - 153066n^3 + 1987786n^2 - 13055316n + 34747236)$	54	55	Wroblewski e Meyrignac (2006)
$n^4 - 97n^3 + 3294n^2 - 45458n + 213589$	49	49	Beyleveld (2006)
$n^5 - 99n^4 + 3588n^3 - 56822n^2 + 348272n - 286397$	46	46	Wroblewski e Meyrignac (2006)
$-66n^3 + 3845n^2 - 60897n + 251831$	45	46	Kazmenko e Trofimov (2006)
$36n^2 - 810n + 2753$	44	45	Fung e Ruby
$3n^3 - 183n^2 + 3318n - 18757$	46	43	S. M. Ruiz (2005)
$47n^2 - 1701n + 10181$	42	43	Fung e Ruby
$103n^2 - 4707n + 50383$	42	43	Speiser (2005)
$n^2 - n + 41$	40	40	Euler
$42n^3 + 270n^2 - 26436n250703$	39	40	Wroblewski e Meyrignac
$43n^2 - 537n + 2971$	34	35	J.Brox (2006)
$8n^2 - 488n + 7243$	61	31	F. Gobbo (2005)
$6n^2 - 342n + 4903$	57	29	J.Brox (2006)
$2n^2 + 29$	28	29	Legendre (1798)
$7n^2 - 371n + 4871$	23	24	F.Gobbo (2005)
$n^4 + 29n^2 + 101$	19	20	E. Peeg Jr. (2005)
$3n^2 + 39n + 37$	17	18	A. Bruno (2009)
$n^2 + n + 17$	15	16	Legendre
$4n^2 + 4n + 59$	13	14	Honaker

Fonte: WolframMathWorld

4 Aplicando em sala de aula

Esta etapa expõe a aplicação deste trabalho para alunos do ensino médio com intuito de observar o quanto eles sabem sobre os números primos. De fato, sabemos que no ensino básico os números primos são vistos logo no início dos números naturais, normalmente em turmas de 6º ano, onde é passado aos alunos que os números são compostos ou primos e consequentemente sua definição. Daí em diante, no processo de decomposição dos números volta-se a falar sobre primos. De modo geral, o que eles realmente sabem responder quando perguntado é que os números primos são aqueles divisíveis por um e por ele mesmo. A ideia desta aplicação é então verificar o que estes estudantes aprenderam sobre os números primos no período em que estiveram na escola.

Nesse sentido, foi montado um questionário com 5 perguntas simples sobre números primos destinados especificamente aos alunos da 3ª série do Colégio Iesgo, situado na cidade de Formosa-GO, escola em que atuo como professor vigente. Os alunos foram pegos de surpresa em relação ao questionário visto que a ideia era de identificar o que cada um sabia acerca do assunto em questão e não possibilitar nenhuma pesquisa que os ajudasse a responder. O questionário era anônimo e tinha apenas identificação 01 e 02 pois foi aplicado duas vezes em momentos distintos. Logo, entende-se que o questionário identificado por 01 foi o que responderam no primeiro momento e 02 no segundo momento.

Figura 1 – Aplicação do questionário

O questionário respondido pelos alunos continha as seguintes perguntas: 1- O que você sabe sobre os números primos?, 2 - Qual a impressão que você tem sobre o conceito "números primos"?, 3 - O que você sabe sobre a infinitude dos números primos?, 4 - Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?, 5 - Você sabe se existe uma fórmula cujos resultados são números primos?.

Após responderem estas perguntas, foram recolhidos os questionários 01 e então uma aula explicativa acerca dos assuntos contidos no questionário. Nesta aula, procurei responder as questões do questionário não de forma direta, mas fazendo uma explicação de parte deste trabalho a qual se tem as respostas para as perguntas do questionário. Apresentei à eles o crivo de Eratóstenes como um método para se obter números primos mas sem utilizar linguagem técnica. Falei um pouco sobre a procura por uma fórmula para terem uma ideia de como é difícil até hoje trabalhar com os números primos e finalizei mostrando a fórmula $f(x, y)$ e pedi a eles que substituíssem alguns pares (x, y) e resolvessem.

Figura 2 – Aula explicativa

Na sequência da aula foi passado à eles novamente o questionário, desta vez identificado por 02, o qual eles tiveram uma nova chance de responder as questões mas com mais noção do assunto.

4.1 Apresentação e análise dos resultados

No total foram respondidos 10 questionários 01 e 02. Esta etapa da pesquisa tem por objetivo analisar os erros e acertos referentes aos questionamentos em questão e fazer a exposição gráfica destes resultados. No que se refere a cada questão do questionário 01, evidencia-se através dos gráficos a seguir todas as informações obtidas após a análise.

4.1.1 Análise do questionário 01

Questão 1: O que você sabe sobre os números primos?

De início questinou-se o que cada um dos estudantes sabiam sobre os números primos. Assim, observou-se que 100% responderam o que se esperava sobre a definição dos números primos.

Figura 3 – Gráfico 1

A partir do Gráfico 1 percebe-se que todos os entrevistados sabiam a definição dos números primos.

Questão 2: Qual a impressão que você tem sobre o conceito "números primos"?

A segunda questão foi observado o que pensam quando escutam dizer números primos e verificou-se que 11% não respondeu a pergunta e 89% não responderam conforme se esperava.

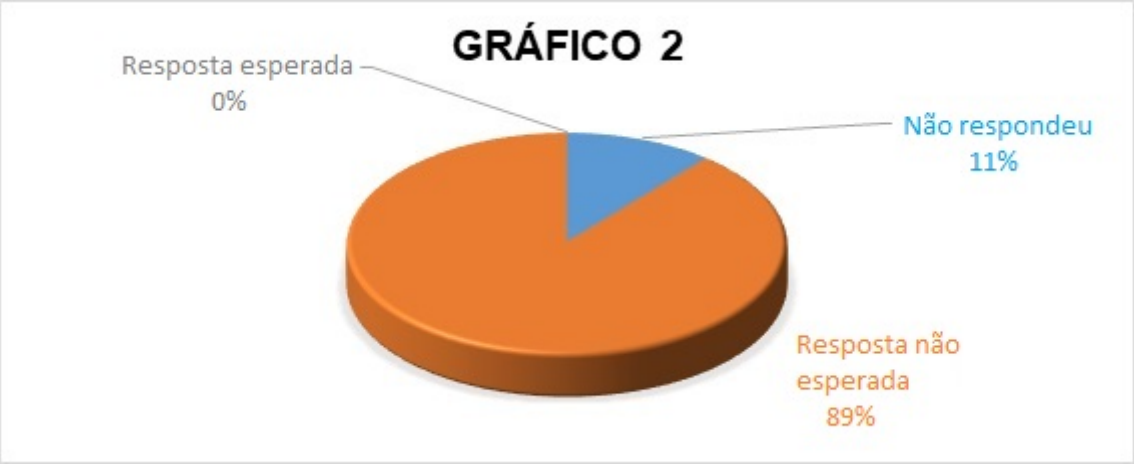

Figura 4 – Gráfico 2

Analisando o Gráfico 2 nota-se que nenhum dos entrevistados sabia algo relacionado ao à expressão "números primos". O esperado era que respondessem em relação à um grau de parentesco entre os números.

Questão 3: O que você sabe sobre a infinitude do números primos?

No terceiro questionamento é levantada a questão sobre a infinitude dos números primos, se sabiam que eram finitos ou infinitos. Dos resultados tem-se que 22% não sabiam nada, 22% não responderam, 22% responderam corretamente, e 34% não responderam conforme se esperava.

Figura 5 – Gráfico 3

Observando o gráfico 3 pode-se perceber que alguns arriscaram dizer que os números primos são infinitos, outros que não são e outros não quiseram responder.

Questão 4: Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Nesta questão almeja-se saber se os entrevistados conheciam o TFA, que é

muito importante na Matemática. Observando os resultados nota-se que nenhum dos estudantes que participaram da pesquisa conhece o TFA.

Figura 6 – Gráfico 4

Analisando o gráfico 4 nota-se que os estudantes não conhecem o TFA que normalmente é apresentado a eles antes de aprenderem a fazer a decomposição em fatores primos ainda no ensino fundamental II.

Questão 5: Você sabe se existe alguma fórmula cujos resultados são números primos?

A questão 5 pergunta se os entrevistados conhecem fórmulas que gerem números primos e identifica se algum dos estudantes é mais curioso e conhece sobre o assunto. Dos resultados 11% não responderam, 11% responderam errado e 78% não sabem.

Figura 7 – Gráfico 5

Observando o gráfico acima pode-se notar que nenhum dos entrevistados tem algum conhecimento sobre fórmulas que geram números primos.

4.1.2 Análise do questionário 02

Após observar os resultados do questionário 01 almeja-se agora um melhor desempenho do questionário 02 tendo em vista que todas as perguntas foram respondidas ao longo da aula explicativa. Nesse sentido apresenta-se os resultados do questionário 02.

Questão 1: O que você sabe sobre os números primos?

Desde o questionário 01 houve 100% das respostas corretas. Nesta etapa não foi diferente, 100% dos entrevistados responderam corretamente, conforme mostra o gráfico a seguir.

Figura 8 – Gráfico 6

Analisando o gráfico 06 pode-se observar que todos os entrevistados concluíram que realmente sabiam acerca da definição de números primos.

Questão 2: Qual a impressão que você tem sobre o conceito "números primos"?

Na segunda questão o resultado vem bem melhor do que o correspondente do questionário 01. Os resultados mostram que 90% responderam corretamente e apenas 10% responderam errado.

Figura 9 – Gráfico 7

Questão 3: O que você sabe sobre a infinitude dos números primos ?

Neste questionamento tivemos resultado de 100% de respostas corretas, todos afirmam que os números primos são infinitos e alguns ainda citam a prova por Euclides.

Figura 10 – Gráfico 8

Analisando o gráfico acima pode-se notar que os entrevistados absorveram bem na aula explicativa sobre a infinitude dos números primos e a prova feita por Euclides.

Questão 4: Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Questionados sobre o TFA, os entrevistados ainda tiveram dificuldades para esta resposta apresentando resultados: 11% não respoderam, 22% responderam errado e 67% responderam corretamente. Ainda assim o desempenho é satisfatório comparado ao questionário 01.

Figura 11 – Gráfico 9

Observando o gráfico 9 pode-se perceber que os alunos não absorveram muito bem a explicação sobre TFA e seu enunciado.

Questão 5: Você sabe se existe alguma fórmula cujos resultados são números primos?

Para o quinto questionamento 100% dos entrevistados responderam que existe sim uma fórmula cujos resultados são números primos.

Figura 12 – Gráfico 10

Como foi mostrado à eles na aula explicativa a função $f(x, y)$ e aplicados alguns pares (x, y) todos responderam que existe uma fórmula cujos resultados são números primos, como mostra o gráfico acima, pensando na mesma função.

Considerações Finais

Desde os primórdios da história humana percebe-se a presença dos números a princípio apenas para contagem. Diante de tantos algarismos os números primos destacam-se pela beleza de suas propriedades. A procura por algo que caracterizasse os números primos sempre foi do interesse de muitos e ainda é, mas nada fácil de se conseguir. Depois de saber que existem infinitos números primos muitos pensam em alguma expressão que possa ser utilizada para encontrar esses números.

Tantos foram os matemáticos que dedicaram anos de suas vidas na procura de uma fórmula que gerasse todos os números primos até que aparecesse a função $f(x,y)$ que é um achado na matemática mesmo não sendo prática a sua utilização. Com certeza a falta de algo concreto que expresse os números primos é o que mais atraia pessoas a estudar sobre este assunto. É normal do homem se interessar por coisas que parecem estar ocultas.

A experiência da aplicação de um trabalho sobre números primos em sala de aula é bem interessante.Iniciando pela definição e o crivo de Eratóstenes parece ser algo simples pois todos conseguem entender bem. Logo que se começa a falar sobre infinitude e algumas propriedades todos ficam intrigados. Por já terem trabalho com sequências numéricas e progressões aritmética e geométrica os alunos pensam que uma expressão que represente a sequência dos números primos é algo simples.

Ao final da aplicação dos questionários foi possível notar certo interesse desses alunos acerca do assunto abordado e pareciam estar satisfeitos em ter aprendido algo que não conheciam na Matemática.

Referências

BOYER, Carl Benjamin, **História da Matemática**; tradução: Elza F. Gomide. São Paulo, Ed. da Universidade de São Paulo, 1974. Citado nas páginas 15 e 23.

DOMINGUES, Hygino H., 1934- **Fundamentos de Aritmética** / Hygino H. Domingues. - São Paulo: Atual, 1991. Citado na página 14.

HEFEZ, Abramo. **Aritmética** / Abramo Hefez - Rio de Janeiro: SBM, 2013. Citado nas páginas 19 e 25.

HONSBERGER, Ross. **Mathematical Gems II**. The Mathematical Association of America, 1976. Citado na página 35.

JONES, James P; et al. **Diophantine Representation of the Set of Prime Numbers**. Mathematical Association of America, 1976. Citado na página 34.

MILLS, W.H., **A Prime-Representing Function**. Princeton University, 1946. Citado na página 33.

MOLLIN E WILLIANS, **Prime-Generating Polynomial**. Disponível em: http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html. Citado na página 37.

RIBENBOIM, Paulo. **Números primos. Velhos mistérios e novos recordes** / Paulo Ribenboim. 1 ed. Rio de Janeiro: IMPA, 2012. Citado nas páginas 32 e 34.

ANEXOS

Anexos - Questionário 1 respondido

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Que o número primo é divisível por 1 e por ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Que os números primos não torna possível a divisão por qualquer número, tem que ser por número específico

3 – O que você sabe sobre a infinitude dos números primos?

nada

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Não

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Não

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Seja $n \in \mathbb{Z}$ / n é divisível apenas por 1 e n. Se se estendido para os números inteiros com (-1) e (-n) como divisores também

2 – Qual a impressão que você tem sobre o conceito "números primos"?

São números que tem alguma ligação entre si

3 – O que você sabe sobre a infinitude dos números primos?

Não se sabe qual o último número primo

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sabia

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Não existe! Existe até um físico para quem descobrir uma P.A cuja razão seja que gerará um número primo.

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

São números divisíveis por 1 e por ele mesmo

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Por serem números divisíveis por 1 e por ele mesmo, não considerados "primos" devido a sua afinidade com ele mesmos ou com os iguais, como se fosse em uma família, em que você tem afinidade com os parentes.

3 – O que você sabe sobre a infinitude dos números primos?

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Não

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Não

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Que os números primos são todos os números naturais divisíveis por 1 e pelo próprio número, ou seja, por ele mesmo

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Que são números próximos um do outro e por eles serem divisíveis pelos mesmos e esta regra ser utilizada por todos

3 – O que você sabe sobre a infinitude dos números primos?

Não se sabe ao certo qual é o último número primo, logo há uma infinitude de números.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Não.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Não.

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

são numeros que são divisiveis apenas por um e por ele mesmo

2 – Qual a impressão que você tem sobre o conceito "números primos"?

não tenho impressão, pois não sei a origem ou significado da palavra "primo".

3 – O que você sabe sobre a infinitude dos números primos?

Pouca coisa, apenas que não se sabe quantos números primos existem

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

não

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

não

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

São números que dividem-se apenas por 1 e pelo próprio número

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Que o conceito "números primos" não remete a ideia "central" que esse termo teria.

3 – O que você sabe sobre a infinitude dos números primos?

Que até hoje há pesquisas que buscam o último número primo.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Nada.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Não.

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Que são números divisiveis por 1 e por ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Números que tem algo em comum.

3 – O que você sabe sobre a infinitude dos números primos?

Nada.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Não.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Não.

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Números primos são números que dividem por ele mesmo, um, menos um e seu respectivo negativo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

A impressão que eu tenho é que esses números tem características em comum.

3 – O que você sabe sobre a infinitude dos números primos?

Até onde eu me recordo, ainda acredita-se que os números primos são infinitos.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Não conheço.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Não sei.

01

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

São todos os números que só se divide por ele e por 1.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

3 – O que você sabe sobre a infinitude dos números primos?

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Anexos - Questionário 2 respondido

02

UFT
UNIVERSIDADE FEDERAL
DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

São números que são divisíveis somente por um e por ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

O significado de "primos" vem do latim que significa primário.

3 – O que você sabe sobre a infinitude dos números primos?

Eles são infinitos, porém, a medida que os números crescem, a quantidade de números primos vai diminuindo.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sim, diz que todos os números compostos podem ser decompostos unicamente em produto de fatores primos.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

sim

02

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Todo $m \in \mathbb{N}^*$ que é divisível por 1 e N / $m \neq 1$.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

São primeiros números, que teve sua descoberta há aproximadamente 300 A.C, o termo "primo" vem da latim "primi", que significa "primeiro", e/ou "primário".

3 – O que você sabe sobre a infinitude dos números primos?

Que são infinitos! Provado por absurdo pelo matemático Euclides.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sim, ele afirma que todo $m \in \mathbb{N}^*$ é primo ou composto.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Sim! Entretanto, a fórmula não é muito útil, pois o número 2 sempre está se repetindo.

02

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Todos os numeros que não divisivel por 1 e por ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Que a palavra "primo" deriva do latim, "primeiro". Em que os numeros primos são infinitos e não é possivel encontrar todos.

3 – O que você sabe sobre a infinitude dos números primos?

Que ou pares dos números, ou seja, Conforme os números vão ~~passando~~ aumentando os números primos vão diminuindo, porém os números primos são infinitos e não é possivel encontrar todos.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

$$F(x;y) = \frac{y-1}{2} \cdot \left[|a^2 - 1| - (a^2 - 1) \right] + 2$$

$$a = x.(y+1) - (y! + 1)$$

02

UFT
UNIVERSIDADE FEDERAL
DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Os números primos são números naturais ($n>1$) em que são divisíveis por 1 e pelo próprio n, que é ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Os números primos em relação ao conceito não se interliga com o "grau de parentesco" dos números, mas sim que são números derivados do grego "primus" que quer dizer primeiro, indivisível.

3 – O que você sabe sobre a infinitude dos números primos?

Que os números primos são infinitos, isto foi provado por Euclides através de um Teorema.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sim, este Teorema enuncia que os números compostos (não primos) em sua decomposição, o resultado para que se chegue é na multiplicação de números primos.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Sim, existe uma fórmula que foi encontrada em um livro de séculos atrás.

02

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

São números que possuem apenas dois divisores, sendo eles 1 e o próprio número

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Primo vem da palavra "primus", que significa primeiro ou primário, dando ideia de que ele não seria divisível.

3 – O que você sabe sobre a infinitude dos números primos?

Que, apesar da quantidade de números primos diminuirem através de intervalos com a mesma quantidade de números ainda não conseguiram ~~dar provas~~ provar que os números primos são finitos, acreditando que eles sejam infinitos.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sim, diz que números compostos podem ser decompostos de maneira única através do produto entre números primos

5 – Você sabe se existe alguma fórmula cujos resultados são números primos?

Sim, existe uma fórmula $f(x,y)$ que os resultados são sempre números primos

02

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Numeros que não divisiveis apenas por 1 e por ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Que primo deriva do latim primus que significa primeiro, primogenito, primatio.

3 – O que você sabe sobre a infinitude dos números primos?

Que é algo ainda não provado a limitude deles, tendo então infinitos.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sim. Que numeros compostos podem ser decompostos unicamente em fatores primos.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Sim.

02

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Que são números naturais que tem como divisor 1 e ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Numeros indivisiveis, pois deriva do grego "primus".

3 – O que você sabe sobre a infinitude dos números primos?

Ainda não se sabe, pois devido ao decrescimento de primos ao longo do passar dos números, diz-se que são infinitos, entretanto Euclides provou o contrário por absurdo, assim provando a infini

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sim. Enuncia que os números primos vão ficando em menor quantidade com o passar dos números.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Sim, entretanto as mesmas não são totalmente funcionais e práticas.

02

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

Pertencem aos naturais, onde $n \neq 0$, que dividem por 1 e ele mesmo.

2 – Qual a impressão que você tem sobre o conceito "números primos"?

Números primos vem da nomenclatura ~~do~~ do latim "primus" que quer dizer primário, indivisível.

3 – O que você sabe sobre a infinitude dos números primos?

Foi comprovado por Euclides que números primos são infinitos.

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

Sim, ele enuncia que números compostos podem ser unicamente decompostos em fatores primos.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

Sim, possui uma fórmula, porém ela é inviável, por ter números relativamente grandes na maioria dos casos.

02

UNIVERSIDADE FEDERAL DO TOCANTINS

Questionário para verificação do aprendizado sobre números primos de estudantes da 3ª série do Colégio Iesgo em Formosa-GO visando identificar o que os alunos do ensino básico sabem sobre números primos. Realizada pelo discente do Mestrado Profissional em Matemática, Frederico Torres de Moura, tendo em vista a elaboração de seu Trabalho final (dissertação), orientado pelo professor Dr. Robson Martins de Mesquita.

1 – O que você sabe sobre os números primos?

são numeros que só podem ser divididos por 1 e por ele mesmo

2 – Qual a impressão que você tem sobre o conceito "números primos"?

que são numeros que compartilhão alguma coisa entre des.

3 – O que você sabe sobre a infinitude dos números primos?

Que até hoje eles são infinitos e já foi provado por alguns matematicos

4 – Você conhece o Teorema Fundamental da Aritmética? Se sim, o que ele enuncia?

sim, Quando um por comporto de podera ser descomportos num produto de numeros primos.

5 – Você sabe se existe alguma fórmula cujos resultadossão números primos?

sim, mas ela apresenta falhas.