INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA BAHIA
CURSO DE LICENCIATURA EM MATEMÁTICA

MAURICIO OLIVEIRA DO NASCIMENTO

O fascinante e misterioso mundo dos Números Primos. Sua importância e suas aplicações.

Salvador-BA
2025

MAURICIO OLIVEIRA DO NASCIMENTO

O fascinante e misterioso mundo dos Números Primos.
Sua importância e suas aplicações.

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia da Bahia como requisito parcial para obtenção do grau de Licenciado em Matemática.

Orientador: Prof. M. Sc. Acelio Rodrigues Souza

Salvador-BA
2025

FICHA CATALOGRÁFICA ELABORADA PELO SISTEMA DE BIBLIOTECAS DO IFBA, COM OS DADOS FORNECIDOS PELO(A) AUTOR(A)

N244f Nascimento, Mauricio Oliveira do

O fascinante e misterioso mundo dos números primos: sua importância e suas aplicações / Mauricio Oliveira do Nascimento; orientador Acelio Rodrigues Souza -- Salvador, 2025.

34 p.

Trabalho de Conclusão de Curso (Licenciatura em Matemática) -- Instituto Federal da Bahia, 2025.

1. Números primos. 2. Máximo divisor comum. 3. Criptografia. I. Souza, Acelio Rodrigues, orient. II. TÍTULO.

CDU 511.313

MAURICIO OLIVEIRA DO NASCIMENTO

O fascinante e misterioso mundo dos Números Primos. Sua importância e suas aplicações.

A banca examinadora, abaixo listada, aprova o Trabalho de Conclusão do curso "O fascinante e misterioso mundo dos números primos", sua importância e suas aplicações . Elaborado por Mauricio Oliveira Do Nascimento como requisito parcial para obtenção do grau de Licenciado em Matemática, pelo Instituto Federal de Educação, Ciência e Tecnologia da Bahia.

Salvador-BA, 10/02/2025

Comissão Examinadora

Documento assinado digitalmente
gov.br ACELIO RODRIGUES SOUZA
Data: 15/04/2025 13:48:23-0300
Verifique em https://validar.iti.gov.br

Prof. M. Sc. Acelio Rodrigues Souza
IFBA
(Orientador)

Fellipe A. dos S. C. Leite

Prof. M. Sc. Fellipe Antonio dos Santos Cardoso Leite
IFBA

Documento assinado digitalmente
gov.br RENATA DE MOURA ISSA VIANNA
Data: 13/04/2025 23:52:03-0300
Verifique em https://validar.iti.gov.br

Profª. M. Sc. Renata de Moura Issa Vianna
IFBA

Joseph N. Yartey

Prof. Dr. Joseph Nee Anyah Yartey
UFRB

Dedico este trabalho ao glorioso Deus o Todo poderoso, que mesmo nos ambientes e circunstâncias totalmente desfavoráveis para os estudos, ele com suas mãos poderosas abriu caminhos e criou possibilidades em meio aos contratempos da vida me enchendo de paixão e disposição para o estudos de matemática como se fosse combustível onde me fez chegar até aqui. Dedico também aos meus genitores José Vieira do Nascimento e Edna Pinto de Oliveira (in memorian), minha querida esposa Cristiane Bomfim Ribeiro do Nascimento por ter suportado meus momentos de ausência .

Agradecimentos

Primeiramente agradeço ao meu Glorioso Deus El Shaddai minha fonte de inspiração, aos professores e amigos Joseph Yartey, Cristiano, José Nelson, e amigos da turma de mestrado acadêmico em Matemática Pura da UFBA: Joedson, Djavan, Yuri, Leandro, Jonatas, eles me ensinaram os primeiros passos na matemática superior quando ainda estava engatinhando .

Por fim ao IFBA e seus professores como Reinaldo Lima que me incentivou a não desistir e dizia que para ele também não tinha sido fácil, Fellipe Antonio que sempre estava disposto a responder as dúvidas, e jamais não poderia deixar de falar do meu orientador Professor Acelio um homem totalmente dedicado e apaixonado pela matemática e que me ensinou os primeiros passos de demonstrações de pequenos resultados matemáticos.

"Deus é o grande geômetra.
Deus geometriza sem cessar.
Por toda a parte, existe geometria (Platão 428-348 a.c)
As leis da Natureza são apenas os pensamentos matemáticos de Deus. (Euclides 300 a.c.)
."

Resumo

Esse trabalho propõe-se a refletir a importância do estudo dos números primos, através da investigação de como o conteúdo tem sido aprendido por estudantes e professores. Nosso objetivo é conscientizar a comunidade da riqueza e a aplicabilidade dessa temática, bem como das fragilidades percebidas na aprendizagem dela.Com este intento, realizou-se uma revisão bibliográfica na qual resgatamos brevemente aspectos históricos relacionados ao estudo dos números primos, definições e propriedades estabelecidas em torno deste conceito. Um dos maiores mistérios sobre os números primos é a dificuldade dos matemáticos em descobrir se um dado número é ou não primo. De fato, até o presente momento, não está resolvido se não existe um padrão de ocorrência entre esses números ou se tal padrão existe, mas ainda não foi descoberto. Conjecturam-se como os estudos de hoje que não há tal padrão, embora a prova formal ainda não tenha sido estabelecida. Curiosamente, esta mesma dificuldade, de decidir se um dado número é primo,foi brilhantemente utilizada na ciência de codificar mensagens (a criptografia) para proteger informações importantes como senhas de banco e de cartões de créditos e dados sigilosos. Por outro lado observa-se que muitas pessoas não associam o estudo dos Números Primos a nada além da matemática escolar. Com isto, resolvemos investigar com aplicações de formulários eletrônicos de nossa autoria o domínio deste assunto entre estudantes e professores nos mais diversos níveis de ensino.

Palavras-chave: Números primos. Máximo Divisor Comum. Criptografia.

Abstract

This work aims to reflect on the importance of studying prime numbers by investigating how the content has been learned by students and teachers.

Our goal is to raise awareness in the community about the richness and applicability of this topic, as well as the weaknesses perceived in its learning.

To this end, a bibliographic review was carried out in which we briefly reviewed historical aspects related to the study of prime numbers, definitions and properties established around this concept. One of the greatest mysteries about prime numbers is the difficulty mathematicians have in discovering whether a given number is prime or not. In fact, to date, it has not been resolved whether there is no pattern of occurrence among these numbers or whether such a pattern exists but has not yet been discovered. It is speculated, as in current studies, that there is no such pattern, although formal proof has not yet been established. Interestingly, this same difficulty in deciding whether a given number is prime has been brilliantly used in the science of encoding messages (cryptography) to protect important information such as bank and credit card passwords and confidential data. On the other hand, it is observed that many people do not associate the study of Prime Numbers with anything other than school mathematics. With this in mind, we decided to investigate, using electronic forms of our own, the mastery of this subject among students and teachers at the most diverse levels of education.

Keywords: Prime Numbers. Greatest Common Divisor . Crytography.

Lista de figuras

Lista de tabelas

Sumário

1 Introdução

Os Números Primos foram e sempre serão sem dúvidas, um objeto de pesquisa que fascina muitos matemáticos durante anos , entre eles : Pitágoras, Euclides, Eratóstenes, Carl Friedrich Gauss, Pierre de Fermat e outros. Isso porque até os tempos de hoje ninguém conseguiu desenvolver uma fórmula que identifique todos . A palavra "Primo"não tem haver com grau de parentesco e sim, derivada da palavra "Primordial", isto é ,que se destaca dos demais, neste caso os números compostos. no conjunto dos números naturais, eles possuem por definição dois e apenas dois divisores, ele mesmo e o numero 1. Falaremos também neste trabalho de fatos interessantes como os números primos de Fermat, Mersenne, formula de Carl Friedrich Gauss que estima e prever a densidade de um número primo em termos da Integral definida, fórmula fracassada de Fermat e outras curiosidades.A proposta desta pesquisa é mostrar para professores e estudantes de matemática os conceitos , propriedades, teoremas e aplicações através de resultados importantes desses números. A metodologia aplicada foi trabalhar por meio de revisões, trechos de bibliografias de alguns autores que descorrem sobre o assunto, somada a um questionário construído na plataforma google Forms por meio do aplicativo WhatsApp disparados para os variados níveis de ensino (fundamental II, médio, superior e professores) em matemática, por onde através das respostas erradas destes grupos, pudemos avaliar e relacionar o quanto eles erraram (trabalhamos em cima dos erros) e desse jeito ,concluímos o quanto eles desconhecem sobre os números primos. Outra característica interessante destes números é que eles não obedecem nenhum tipo de padrão no tocante a seu ordenamento (na reta real), o que contribui para sua complexidade (dificuldade) durante os estudos e pesquisas em busca de determinar o que será ou não um número primo.

Encontrar números primos cada vez maiores, é de interesse dos pesquisadores nos tempos atuais, o que representa um recurso fortíssimo utilizado para codificações e segurança de dados as quais atende o mercado financeiro entre outros seguimentos da sociedade . Buscar números primos é uma tarefa desafiadora, pois não existe fórmula para encontrá-los e nem determiná-los . Existem vários algoritmos de testes de primalidade disponíveis, como o teste de divisão simples, o teste de Fermat, o teste de Miller-Robin, o teste de Lucas –Lehmer (para os números de Mersenne) o que podemos lá na frente conhecê-los (alguns em anexo) . A busca por número primo cada vez maior é frequentemente uma atividade colaborativa que envolve várias pessoas e instituições de pesquisas do mundo inteiro .Existem projetos de computação distribuídos ,como o projeto GIMPS que se concentra em encontrar números primos específicos como o número primo de Mersenne. Com certeza essa tarefa requer uma computação poderosíssima, pois os cálculos envolvidos podem ser

extremamente exaustivos e demorados, isso geralmente envolve o uso de computadores de última geração e de altos desempenho de processadores.

2 RELAÇÕES HISTÓRICAS E CURIOSIDADES

Poderíamos citar aqui inúmeros matemáticos de muitas regiões do mundo e de varias civilizações da história, que estudaram os números primos, mas foi o povo da antiga Grécia que deu início ao estudos desses números em especial os matemáticos da escola Pitagórica (500 a 300 a.c.) que se tem registro , e estavam interessados nos números primos por suas propriedades e sentido a numerologia, isto é, a relação dessas propriedades matemáticas com os seres vivos e forças físicas e também suas características místicas.

Quando o matemático Euclides escreveu sua obra clássica "OS ELEMENTOS" (300 a.c.) os resultados que envolviam esses números já estavam presentes nas formulações dos axiomas e dos teoremas de geometria, entre esses resultados dois bastante conhecidos "Existem Infinitos Números Primos" e o Teorema Fundamental da Aritmética "Qualquer inteiro pode ser escrito como Produto de números primos em essencialmente uma única maneira".

O matemático grego Eratóstenes por volta de 200 a.c. criou um algoritmo para encontrar números primos chamado de "O crivo de Erastóstenes" em um período em que se estudavam muito esses números pelo qual ficou conhecido como Idade Negra.

Muitas pesquisas em torno desses números foram realizadas, o Matemático Pierre Fermat (século XVII) também fez grandes contribuições a saber ,um resultado bastante conhecido hoje na matemática, na área da Teoria dos números, uma que antes era uma conjectura feita por Álbert Girard que diz :
"Todo número primo da forma $4n+1$ poderia ser inscrito de um só modo como a soma dos quadrados de dois números inteiros" , daí em diante veio também a fatoração de números primos e ainda por Fermat "O grande Teorema de Fermat" que diz : "se p for um número primo então para qualquer inteiro x vale x^p congruo a x ou x^{p-1} congruo 1 mod p".

Como também o resultado $F_n = 2^{2^n} + 1$ que descrevia os números primos , tese essa que foi derrubada pelo Matemático Leonhard Euler quando descobriu uma falha para um $n = 5$, $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ um número composto , portanto não primo.

Não poderíamos deixar de falar dos números de Mersenne , Marin Mersenne (1588 – 1648) foi um Padre , filósofo , teólogo, músico , astrônomo e matemático francês que criou uma forma para achar números primos do tipo $2^n - 1$.

Cujo notação é M_n com "n" um número primo onde hoje em dia é usada para descobrir muitos, mas vale lembrar que nem todos dessa forma serão primos a exemplo de $2^{11} - 1 = 2047 = 23 \cdot 89$ um número composto.

Outros grandes matemáticos da história também usaram esses números primos em seus desenvolvimentos de pesquisa a exemplo de Leonhard Euler (1707-1783) quando provou que a série Harmônica é divergente para "n" primo

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

E também Carl Friedrich Gauss (1777-1855), estimou ao numero $\pi(n) \approx \dfrac{n}{\log n}$ do matemático Adrien-Marie Legendre em termos da integral

$$\pi(n) = \int_2^n \frac{1}{\log n}\, dt$$

e previu que a densidade de um número primo igual a $\dfrac{1}{\log n}$ onde hoje é conhecido com Teorema dos Números Primos.

Além das grandes descobertas e contribuições na matemática pura em torno dos números primos, destacamos em meio a muitas curiosidades o ciclo de vidas das cigarras magicicadas nos subsolos do Canadá e também dos estados unidos que curiosamente só sobem para a superfície da terra sobre uma variação de períodos entre 13 e 17 anos evitando todo tipo de períodos pares para se proteger de seus predadores. Os biólogos e estudiosos entendem que os períodos pares de tempo geram na natureza uma espécie de padrão como um ciclo vicioso em que os predadores ficariam de sentinela esperando para dar o bote, logo números primos aparecem como intervalos de tempo o que livrariam das armadilhas com a exceção do número 2 que é o único número primo par. Outra curiosidade é uma composição de uma música clássica do compositor Francês Oliver Messiaen onde os intervalos que são escritas as divisões dos instrumentos como clarineta, violino e violão são compostos em números de compasso entre 17 e 29 compassos rítmicos produzindo assim uma sensação de tempo interminável, como se a música nunca fosse acabar de ser tocada, pois era essa a intenção do Maestro. São muitas curiosidades, aplicações que se dão aos estudos dos números primos que não caberia falar de todas elas. Uma das mais fabulosas artes que envolvem esses números nesse século é a incansável busca cada vez pelo um maior número primo, pesquisadores usam computadores de grandes potências para calcular a maior quantidade de dígito que compõem o maior número primo, prêmios de milhões é oferecidos a quem os encontra-lo. Afinal por que essa busca implacável em encontrar cada vez um maior número primo ? Essa resposta se deve ao fato de que cada vez maior esse número maior será a dificuldade de sua fatoração se transformando em códigos que serão quase impossíveis de serem descobertos. O que estamos falando é da Criptografia, a arte de codificar dados pessoais como senhas de cartões entre outras chaves de segurança cibernética da criptografia RCA cujas siglas homenageiam seus criadores(Rivest-Shamir-Adleman).

3 METODOLOGIA APLICADA

A metodologia aplicada consistiu em uma revisão bibliográfica dos livros [1], [2], [3], [4], [5] e [6], que forneceram a fundamentação teórica utilizada na pesquisa. Somado a isto , foi elaborado o mesmo questionário para alunos do ensino fundamental, médio, superior em matemática e professores de matemática, onde tiveram de responder sim ou não.

Dessa forma pudemos avaliar o grau de desconhecimento dos participantes da pesquisa sobre o tema números primos, através das respostas que cada grupo forneceu . A quantidade de participantes desta pesquisa foi distribuída da seguinte forma: 31 pessoas do ensino fundamental, 42 do ensino médio, 36 foram estudantes do ensino superior em matemática e 49 foram professores de matemática de todos os graus de ensino. Em seguida , através da coleta de dados (as respostas dos participantes) foi construído um gráfico para auxiliar na análise, e na leitura crítica destas respostas , o que pudemos através disto, avaliar os conhecimentos dos candidatos (seção 7).

4 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, iremos introduzir definições, teoremas, lemas ,proposições que irão fundamentar toda a teoria. Baseado em algumas literaturas, utilizando como fonte de consulta tais livros [1], [2] e [4] entre outros citados nas referências bibliográficas .

4.1 Divisibilidade

A noção de divisibilidade dialoga com dois temas importantes: divisão exata (resto zero) e a noção de números primos. Como veremos a seguir, os resultados desta seção são utilizados para provar propriedades especiais dos números primos. Em especial: todo número tem ao menos um número primo como divisor primo!

Definição 4.1.1. Sejam a, b números inteiros. Dizemos que a **divide** b, denotado por $a \mid b$, se existe um número inteiro c tal que

$$b = ac.$$

Nesse caso, dizemos ainda que "a é um divisor de b" ou "b é um múltiplo de a". O número c é chamado de quociente de b por a.

Exemplo 4.1.1. Os divisores de 18 são os inteiros

$$\pm 1,\ \pm 2,\ \pm 3, \pm 6,\ \pm 9,\ \pm 18.$$

Por outro lado, estes inteiros são também os divisores de -18.

Proposição 4.1.1. *Sejam $a, b, c \in \mathbb{Z}$. Então,*

(a) $1 \mid c, \quad a \mid a \quad e \quad a \mid 0.$

(b) $a \mid b,\ b \neq 0$, *se, e somente se,* $|a| \leq |b|$.

(c) *se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.
Essas propriedades insinuam que em $\mathbb{N}$ a divisibilidade é uma relação de ordem (reflexiva, anti-simétrica e transitiva)

Demonstração.

(a) $1 \mid c$, pois $c = 1 \cdot c, \quad a \mid a$ pois $a = a \cdot 1 \quad$ e $\quad a \mid 0$ pois $0 = a \cdot 0$.

(b) Se $a \mid b$, então, existe $q \in \mathbb{Z}$ tal que $b = a \cdot q$. Assim, $|b| = |a| \cdot |q|$. Como $b \neq 0,\ |q| \geq 1$, tem-se $|a| \leq |b|$.

(c) Se $a \mid b$ e $b \mid c$, então, por definição, existem $m, n \in \mathbb{Z}$ tais que $b = am$ e $c = bn$. Assim,

$$c = (am)n = a(mn). \quad \text{Logo,} \quad a \mid c.$$

□

Proposição 4.1.2. *Se $a,\ b,\ c,\ d \in \mathbb{Z}$, com $a \neq 0$ e $c \neq 0$, então*

$$a \mid b \ \ e \ \ c \mid d \Longrightarrow ac \mid bd$$

Demonstração. Se $a \mid b$ e $c \mid d$, então existem $m, n \in \mathbb{Z}$ tais que $b = am$ e $d = cn$. Então,

$$bd = (am) \cdot (cn) = (ac) \cdot (mn).$$

Portanto, $ac \mid bd$. □

Proposição 4.1.3. *Sejam $a,\ b,\ c \in \mathbb{Z}$ tais que $a \mid b$ e $a \mid c$, então para todo $x, y \in \mathbb{Z}$, $a \mid (xb + yc)$*

Demonstração. Se $a \mid b$ e $a \mid c$, então existem $m,\ n \in \mathbb{Z}$ tais que $b = a \cdot m$ e $c = a \cdot n$. Então,

$$xb + yc = xam + yan = a \cdot (xm + yn).$$

Logo, $a \mid (xb + yc)$.

□

4.2 Máximo Divisor Comum

A ideia de máximo divisor comum também será importante para perceber propriedades especiais de números primos e até generalizar algumas delas.

Definição 4.2.1 (Máximo Divisor Comum). Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos. O máximo divisor comum de a e b, denotado por (a, b) é um elemento $d \in \mathbb{Z}$ tal que

(i) $d \,|\, a$ e $d \,|\, b$

(ii) $d \geq 1$

(ii) Se d' é outro elemento de $\mathbb{Z}$ satisfazendo (i) e (ii), isto é $d' \,|\, a$ e $d' \,|\, b$, então d' divide d.

Exemplo 4.2.1.

$$(4, 6) = 2, \qquad (17, 17) = 17, \qquad (42, 0) = 42, \qquad (12, -15) = 3.$$

O Teorema a seguir demonstra a existência do (a, b) para $a, b \in \mathbb{Z}$, não simultaneamente nulos. A força do lema de Bèzout está em garantir que o mdc é combinação linear de a e b, ou seja, uma soma de múltiplos deste. Esta combinação não é única. O resultado é uma ferramenta muito útil na Teoria dos números.

Teorema 4.2.1 (Bézout). *Dados números inteiros a, b ambos não nulos, existe um único máximo divisor comum $d = (a, b)$. Além disto, existem inteiros x, y tais que*

$$d = ax + by \quad (\textit{combinação linear de } a \quad e \quad b)$$

Exemplo 4.2.2.

(a) $(4, 6) = 2 \quad$ e $\quad 2 = 6 \cdot 1 + 4 \cdot (-1)$

(b) $(12, -15) = 3 \quad$ e $\quad 3 = -15 \cdot (-1) + 12 \cdot (-1)$

Observação 1.

(a) Temos $(12, -15) = 3$, logo o Teorema 4.2.1, afirma que o conjunto de todas as combinações lineares de 12 e -15 - isto é o conjunto de todos os números da forma $-15x + 12y$ - é o conjunto de todos os múltiplos de 3:

$$\cdots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \cdots .$$

Observe que o máximo divisor comum é o menor número positivo neste conjunto.

(b) Notamos no Teorema de Bezout os inteiros x e y não são únicos.

De fato, $2 = (6, 4)$. Mas

$$6 \cdot 1 + 4 \cdot (-1) = 2 \qquad e \qquad 6 \cdot 3 + 4 \cdot (-4) = 2.$$

(c) Em geral, também não vale a recíproca do Teorema de Bezout, pois

$$6 \cdot 2 + 4 \cdot (-2) = 4 \qquad e \qquad (6, 4) \neq 4.$$

Entretanto, vamos provar adiante que:

$$(a, b) = 1 \iff \quad \textit{existirem inteiros } x \textit{ e } y \textit{ tais que } xa + yb = 1.$$

Esse é o único caso em que a recíproca do Teorema de Bezout é verdadeira.

Lema 4.2.2. *Se a e b são inteiros não ambos nulos, então $(a, b) = 1$ se, e somente se, existem números inteiros x e y tais que $ax + by = 1$.*

Demonstração. Suponha que $(a, b) = 1$. Pelo Teorema 4.2.1, existem números inteiros x e y tais que

$$ax + by = (a, b), \quad \text{isto é,} \quad ax + by = 1.$$

Reciprocamente, suponha que existam números inteiros x e y tais que $ax + by = 1$. Seja $d = (a, b)$. Então, como $d \mid a$ e $d \mid b$, tem-se $d \mid (ax + by)$, ou seja, $d \mid 1$ e portanto, $d = 1$. □

Lema 4.2.3. ***[Lema de Gauss]*** *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração. Se $a \mid bc$, então existe $k \in \mathbb{Z}$ tal que $bc = ak$. Pelo Lema 4.2.2, como $(a, b) = 1$, existem inteiros x, y tal que $ax + by = 1$. Então, multiplicando por c ambos os lados da igualdade,

$$axc + byc = c \Longrightarrow axc + yak = c \Longrightarrow (xc + yk)a = c \Longrightarrow a \mid c.$$

□

Lema 4.2.4. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid c$, $b \mid c$ e $(a, b) = 1$, então $ab \mid c$.*

Demonstração. Se $a \mid c$ e $b \mid c$, então existem k_1, $k_2 \in \mathbb{Z}$ tais que $c \overset{(i)}{=} ak_1$ e $c \overset{(ii)}{=} k_2 b$. Pelo Lema 4.2.2, como $(a, b) = 1$, existem inteiros x, y tal que $ax + by \overset{(iii)}{=} 1$. Então, multiplicando por c ambos os lados da igualdade (iii), temos

$$axc + byc = c \overset{(i) \text{ e } (ii)}{\Longrightarrow} ax(k_2 b) + by(ak_1) = c \Longrightarrow (xk_2 + yk_1)ab = c \Longrightarrow ab \mid c.$$

□

Observação 2. *Observe que no Lema 4.2.4, o resultado é falso se $(a, b) \neq 1$. Por exemplo:*

$$8 \mid 24 \quad e \quad 6 \mid 24, \quad mas \quad 48 = 8 \cdot 6 \nmid 24.$$

Definição 4.2.2. (Inteiros primos entre si ou coprimos ou relativamente primos)
Dizemos que dois inteiros a e b são **primos entre si**, ou **relativamente primos** ou são **coprimos**, quando $(a, b) = 1$.

Exemplo 4.2.3. 25 e 42 são coprimos pois $(25, 42) = 1$.

4.3 Números Primos

4.3.1 Definição e Propriedades

Definição 4.3.1. Um número inteiro $a \neq \pm 1$ é um número **primo** quando só tem dois divisores positivos: 1 e $|a|$.
Os números inteiros $a \neq \pm 1$ que não são primos são chamados de números **compostos**.

Exemplo 4.3.1.

(a) Os inteiros 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 são os 10 primeiros inteiros primos positivos.

(b) Os inteiros -2, $-3, -5, -7, -11$, -13, $\cdots$ são inteiros primos negativos.

(c) Os inteiros ± 4, ± 6, $\pm 8, \pm 10$ são números compostos.

Lema 4.3.1. *Qualquer inteiro positivo $n > 1$ tem um divisor primo.*

Demonstração. Seja $S = \{n \in \mathbb{Z} \mid n > 1 \text{ e } n \text{ não tem divisores primos}\}$
Se $S \neq \emptyset$, como S é limitada inferiormente, pelo Principio da Boa Ordenação[1] S possui um menor elemento, digamos, $n_0 \in S$.

Como $n_0 > 1$ e n_0 não tem divisores primos, então n_0 é composto, e existem inteiros $a_0, b_0 \in \mathbb{Z}$ tal que

$$n_0 = a_0 \cdot b_0$$

onde $1 < a_0 < n_0$ e $1 < b_0 < n_0$.

Entretanto, como $1 < a_0 < n_0$ e n_0 é o menor elemento em S, então $a_0 \notin S$, que implica que a_0 tem um divisor primo, digamos que $p \mid a_0$, mas então $p \mid n_0$ também. Contradição.
Portanto, a afirmação que $S \neq \emptyset$ leva a uma contradição, e devemos ter $S = \emptyset$, e portanto qualquer inteiro positivo $n > 1$ tem pelo menos um divisor primo. □

Teorema 4.3.2 (Infinitude dos números primos)**.** *Existem infinitos números primos.*

Demonstração. Suponha que não, isto é que $p_1, p_2 \cdots, p_N$ são os únicos primos. Agora considere o inteiro

$$M = p_1 \cdot p_2 \cdots p_N + 1.$$

Então pelo Lema 4.3.1, M possui um divisor primo, e ele deve ser portanto um dos primos $p_1,\ p_2, \cdots, p_N$. Contradição, pois nenhum dos primos divide M. □

4.3.2 Teorema Fundamental da Aritmética

Esse Teorema é importante porque estabelece que com números primos podemos gerar todos os números. Em verdade, primo tem a ver com primordial, o que vem primeiro e não com grau de parentesco. Outra coisa, esse Teorema tem inúmeras aplicações, como estabelecer importância dos primos, cálculo de mdc e mmc, extração de raiz quadrada.

[1] Todo subconjunto não-vazio $A \subset \mathbb{N}$ possui um menor elemento, isto é, um elemento $a_0 = \min(A)$ em A tal que $a_0 \leq a$ para todo $a \in A$.

Teorema 4.3.3 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Por exemplo,

$$36 = 2^2 \cdot 3^2, \quad 4312 = 2^3 \cdot 7^2 \cdot 11, \quad 19 = 19^1.$$

Para provar o Teorema Fundamental da Aritmética, vamos precisar dos seguintes lemas.

Lema 4.3.4. *Qualquer inteiro $n > 1$ ou é primo ou é produto de números primos.*

Demonstração. Por indução sobre n.
O resultado é valido para $n = 2$, pois 2 é primo.
Vamos assumir que ele e válido para qualquer inteiro positivo k, com $2 \leq k < n$.

Se n não é primo, então ele possui um divisor positivo d com $d \neq 1$ e $d \neq n$. Portanto, $n = m \cdot d$, onde $m \neq n$.

Mas como, $1 < m, d < n$, pela hipótese de indução, m e d são produtos de primos, portanto n é também um produto de primos. Isto completa o processo de indução. □

Lema 4.3.5. *Se p é primo tal que $p \nmid a$, então $(p, a) = 1$.*

Demonstração. De fato, se $(p, a) = d$, então $d \mid a$ e $d \mid p$. Assim, $d = p$ ou $d = 1$. Porém, $d \neq p$, pois $p \nmid a$. Portanto, $d = 1$. □

Lema 4.3.6. *Sejam $a, b \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$. Mais geral, se $p \mid a_1 a_2 \cdots a_n$ então $p \mid a_i$ para algum i.*

Demonstração. Por hipótese, $p \mid ab$. Suponha que $p \nmid a$. Assim, $(p, a) = 1$. Daí, como $p \mid ab$ e $(p, a) = 1$, pelo Lema 4.2.3, Lema de Gauss, $p \mid b$.
A demonstração no caso mais geral, segue de indução. □

Exemplo 4.3.2.

$$7 \mid 154 \quad \text{e} \quad 154 = 11 \cdot 14.$$

Tem-se que $7 \nmid 11$ e $7 \mid 14$.

Corolário 1. *Se $p, p_1, \cdots, p_n$ são números primos e, se*

$$p \mid p_1 \cdots p_n,$$

então $p = p_i$, para algum $i = 1, \cdots, n$.

Usando esses resultados, vamos provar o Teorema Fundamental da Aritmética.

Demonstração. (Teorema Fundamental da Aritmética). Para demonstrar o Teorema Fundamental da Aritmética, será utilizado o Segundo Princípio de Indução[2]
Se $n = 2$, então n é primo. Suponhamos o resultado válido para todo número natural menor que n, vamos mostrar que vale para n.
Se n é primo, nada a mostrar.
Se n é composto, então existem números naturais n_1, n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Assim, pela hipótese de indução, existem números primos $p_1, p_2 \cdots, p_r$ e $q_1, q_2 \cdots, q_s$ tais que $n_1 = p_1 p_2 \cdots p_r$ e $n_2 = q_1 q_2 \cdots q_s$. Logo,

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

Agora, suponhamos que n admita duas decomposições em números primos, isto é:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

em que p_i e q_j são números primos, para $i = 1, \cdots, r$ e $j = 1, \cdots, s$.
Pelo corolário acima, $p_1 = q_j$, para algum j, pois $p_1 \mid q_1 \cdots q_s$. Vamos supor que $p_1 = q_1$. Assim,

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

Como $p_2 \cdots p_r < n$, a hipótese de indução implica que $r = s$ e $p_i = q_j$. □

Observação 3. *Na fatoração de um inteiro n, um primo p pode ocorre varias vezes. Se os fatores primos distintos de n são $p_1,\ p_2, \cdots, p_k$, e se p_i ocorre α_i vezes para $1 \leq i \leq k$ então podemos escrever*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Isto é,

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

chamado de fatoração de n de potências primos.

Lema 4.3.7. *Sejam $k,\ n,\ a_1,\ a_2, \cdots, a_k$ números naturais tais que $(a_i,\ n) = 1\ \forall i$. Então*

$$(a_1 a_2 \ldots a_k, \quad n) = 1.$$

Demonstração. Basta notar que sendo $(a_i,\ n) = 1$, as decomposições em fatores primos de a_i e n não possuem fator comum e, portanto, as decomposições do produto $a_1 a_2 \ldots a_k$ e n não possuem fator comum o que nos leva a $(a_1 a_2 \ldots a_k,\ n) = 1$. □

[2] Seja $P(n)$ uma proposição sobre $A = \{n \in \mathbb{N}; n \geq a, a \in \mathbb{N}\}$, o Segundo Princípio da Indução pode ser definido como segue:

a) $P(a)$ é verdadeira.

b) Para todo n tal que $a \leq n \leq k$ vale $P(n) \rightarrow P(k+1)$.

Então para qualquer $n \in A, P(n)$ é verdadeira.

4.3.3 Descobrindo primos

Existem várias maneiras de encontrar números primos. Um dos métodos mais antigos para encontrá-los foi dado por Eratóstenes (276-194 A.C.), antigo bibliotecário da grandiosa biblioteca de Alexandria.

O método de Eratóstenes para achar primos chama-se Crivo de Eratóstenes. O Crivo de Eratóstenes consiste em organizar os números em ordem crescente em uma tabela e remover os múltiplos de cada primo que encontrar. Os primos são dados pelos números que não forem removidos.

Tabela 1 – Crivo de Eratóstenes.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	50	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~
73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~
97	~~98~~	~~99~~	~~100~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~

Fonte: Produzida pelo autor

Uma consequência dos trabalhos sobre o crivo de Eratóstenes leva ao resultado sobre identificar a primaridade de um número qualquer com mais facilidade.

Note que todos os múltiplos de primos no Crivo estão eliminados na verificação do próximo primo. Isto significa que um número n não teria mais chances de ser composto se não houver divisores dele menores que $\sqrt{n}$.

Teorema 4.3.8. *Se n é inteiro positivo, então n possui um divisor primo p tal que $p \leq \sqrt{n}$.*

Demonstração. Se n é composto, então $n = a \cdot b$, onde $1 < a \leq b < n$. Se $a \geq \sqrt{n}$, então $b \geq a > \sqrt{n}$ e isto implica que

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$$

que uma contradição. Portanto $a \leq \sqrt{n}$ e como $a > 1$, então a possui um divisor primo p tal que $p \leq a \leq \sqrt{n}$ e como $p \mid a$ e $a \mid n$, então $p \mid n$ também. □

Exemplo 4.3.3. Quais primos devemos usar para dividir 127 para testar que ele é primo ou não? Para verificar que 127 é primo, devemos somente verificar ele possui um fator primo $\leq \sqrt{127} \approx 11,27$. Então podemos verificar 127 não é divisível por 2, 3, 5, 7, ou 11. Portanto , 127 é primo.

4.4 Aritmética modular

Aprestamos uma breve introdução referente à congruência módulo m, ou "a aritmética dos restos de uma divisão por $n \in \mathbb{Z}$.

Definição 4.4.1. Sejam $a, b, n \in \mathbb{Z}$ com $n \neq 0$. Dizemos que a é congruente b módulo n e escrevemos

$$a \equiv b \pmod{n} \quad \text{ou} \quad a \equiv_n b$$

se, e somente se, $a - b$ é um múltiplo de n, isto é, se, e somente se $a - b = kn$, para algum $k \in \mathbb{Z}$.

Exemplo 4.4.1.

1. $13 \equiv 18 \pmod{5}$ pois $(13 - 18) = 5 = 5 \cdot 1$
2. $152 \equiv_7 5$ pois $(152 - 5) = 147 = 7 \cdot 21$.
3. $7 \equiv_8 15$ pois $(7 - 15) = -8 = 8 \cdot (-1)$.
4. $-101 \equiv_3 1$ pois $(-101 - 1) = -102 = 3 \cdot (-34)$.
5. $16 \equiv -1 \pmod{17}$ pois $(16 - (-1)) = 17 = 17 \cdot 1$.

A congruência módulo n é uma relação de equivalência. Isto é

Proposição 4.4.1. *Seja $n \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se:*

(a) $a \equiv a \pmod{n}$ (reflexiva)

(b) Se $a \equiv b \pmod{n}$ então $b \equiv a \pmod{n}$ (simétrica)

(c) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então $a \equiv c \pmod{n}$ (transitiva)

Portanto $\equiv_n$ é um relação de equivalência.

Proposição 4.4.2 (Propriedades básicas de congruências).

(a) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então $a + c \equiv b + d \pmod{n}$

(b) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então $a - c \equiv b - d \pmod{n}$

(c) Se $a \equiv b \pmod{n}$ e c é inteiro não negativo, então $ac \equiv bc \pmod{n}$

(d) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$ então $ac \equiv bd \pmod{n}$

(e) Se $a \equiv b \pmod{n}$ e k é um inteiro positivo, então $a^k \equiv b^k \pmod{n}$

(f) Se $a + c \equiv b + c \pmod{n}$ então $a \equiv b \pmod{n}$

(g) Se $da \equiv db \pmod{dn}$ então $a \equiv b \pmod{n}$.

4.5 A Função fi, ϕ de Euler

Definição 4.5.1. Para qualquer inteiro positivo n, definimos a função phi de Euler, denotado por ϕ como a quantidade de inteiros positivos menores que n e coprimos com n.
Em outras palavras,

$$\phi(n) = \#\{x \in \mathbb{N};\ \ 1 \leq x < n \ \text{ e } \ (x, n) = 1\}$$

Exemplo 4.5.1.

(1) Seja $n = 12$. Os inteiros menores que 12 e são coprimos com 12 são $\{1, 5, 7, 11\}$. Portanto $\phi(12) = 4$.

(2) Seja $n = 15$. Os inteiros menores que 15 e são coprimos com 15 são $\{1, 2, 4, 7, 8, 11, 13, 14\}$. Portanto $\phi(15) = 8$.

(3) A tabela abaixo mostra os valores da função $\phi(n)$ para os 20 primeiros inteiros positivos.

Tabela 2 – Os 20 primeiros valores de ϕ

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Fonte: Produzida pelo autor

A seguir, verificaremos algumas propriedades da função fi que tornam seu cálculo mais simples.

Lema 4.5.1. *Se p é um número primo, então $\phi(p) = p - 1$.*

Demonstração. Por definição, $\phi(p)$ é a quantidade de inteiros positivos x menores que p e coprimos como p. Mas, como p é primo, os únicos divisores positivos são 1 e p, logo todo inteiro $x,\ 1 \leq x \leq p - 1$ é coprimo com p. Assim $\phi(p) = p - 1$. □

Exemplo 4.5.2. $\phi(29) = 29 - 1 = 28$, pois 29 é primo.

Lema 4.5.2. *Sejam p um número primo e $n \in \mathbb{N}$. Então*

$$\phi(p^n) = p^{n-1}(p - 1) = p^{n-1} \cdot \phi(p).$$

Demonstração. Temos que contar a quantidade de inteiros entre 1 e p^n que são coprimos com p^n. Faremos isso de uma maneira indireta: contaremos quantos inteiros entre 1 e p^n

não são coprimos com p^n, pois os divisores de p são apenas 1 e p, logo os divisores de p^n são as potências de p. Consequentemente os inteiros que não são coprimos com p^n são exatamente os múltiplos de p. Os múltiplos de p entre 1 e p^n são:

$$p,\ 2p,\ 3p, \cdots, p^n. \qquad (*)$$

O conjunto $(*)$ é uma progressão aritmética de razão p e primeiro termo p. Portanto existem, p^{n-1} múltiplos de p entre 1 e p^n.
Logo

$$\begin{aligned}\phi(p^n) &= \#\{x \in \mathbb{N};\ \ 1 \leq x \leq p^n \ \text{ e } \ (x, p^n) = 1\} \\ &= \ \#\{x \in \mathbb{N};\ \ 1 \leq x \leq p^n\} \ - \ \#\{x \in \mathbb{N};\ \ 1 \leq x < p^n \ \text{ e } \ (x, p^n) \neq 1\} \\ &= p^n - p^{n-1} = p^{n-1}(p-1) = p^{n-1}\phi(p).\end{aligned}$$

□

Exemplo 4.5.3.

(i) $\phi(27) = \phi(3^3) = 3^2\phi(3) = 9 \cdot 2 = 18$

(ii) $\phi(625) = \phi(5^4) = 5^3\phi(5) = 125 \cdot 4 = 500.$

Lema 4.5.3. *A função de Euler é multiplicativa, isto é, quaisquer que sejam n e m números naturais satisfazendo $(n, m) = 1$ (m e n são primos entre si) teremos*

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n)$$

Corolário 2. *Sejam $p_1,\ p_2, \cdots, p_k$ números primos distintos e $n_1,\ n_2, \cdots, n_k$ números naturais. Então:*

$$\begin{aligned}\phi\left(p_1^{n_1} \cdot p_2^{n_2} \cdots p_n^{n_k}\right) &= \phi\left(p_1^{n_1}\right) \cdot \phi\left(p_2^{n_2}\right) \cdots \phi\left(p_n^{n_k}\right) \\ &= p_1^{n_1-1}\phi(p_1) \cdot p_2^{n_2-1}\phi(p_2) \cdots p_k^{n_k-1}\phi(p_k)\end{aligned}$$

Exemplo 4.5.4.

(a) $$\begin{aligned}\phi(100) &= \phi(2^2 \cdot 5^2) \\ &= \phi(2^2) \cdot \phi(5^2) \\ &= 2^1\phi(2) \cdot 5^1\phi(5) \\ &= 2 \cdot 1 \cdot 5 \cdot 4 = 40\end{aligned}$$

(b) $$\begin{aligned}\phi(120) &= \phi(2^3 \cdot 3 \cdot 5) \\ &= \phi(2^3) \cdot \phi(3) \cdot \phi(5) \\ &= 2^2\phi(2) \cdot 2 \cdot 4 \\ &= 4 \cdot 1 \cdot 2 \cdot 4 = 32\end{aligned}$$

4.6 Exemplos de Aplicações Interessantes

Problema 1: (Canguru Matemático sem Fronteiras 2014 - Categoria Junior) Na figura ao lado esta um dado especial. A soma dos números em quaisquer duas faces opostas é sempre a mesma. Os números que não estão visíveis na figura são todos números primos. Que numero esta na face oposta à face com o número 14?

(A) 11 (B) 13 (C) 17 (D) 19 (E) 23

Resolução:

Temos que $35 + x = 14 + y = 18 + z$, sendo x, y, z primos. Apenas 2 e -2 são primos pares e nenhum deles poderia se opor a 14 ou 18, pois a soma dos números nas faces opostas seria menor do que 35. Portanto, os primos opostos às faces 14 e 18 são ambos ímpares, logo o número oposto à face 35 tem forçosamente que ser par, já que as somas nas faces consideradas anteriormente são ímpares. Esse número não pode ser -2, pois $53 + (-2) = 33$, o que forçaria a face oposta a 18 ter números 15, qu não é primo. Mas se $x = 2$, então $y = 23$ e $z = 19$. Logo, o número oposto ao número 14 é 23.

Problema 2:

Quais são os números cujos triplos somados com 1 dão um número primo entre 70 e 110 ?

Resolução:

Os primos entre 70 e 110 são 71, 73, 79, 83, 89, 97, 101, 107, 109 e que subtraindo 1 de cda um desses números teremos : 70, 72, 78, 82, 88, 96, 100, 102, 106, 108 Desta lista os múltiplos de 3 será : 72, 78 ,96 ,102 ,108. Daí :

$$72 \div 3 = 24,\ 78 \div 3 = 26,\ 96 \div 3 = 32,\ 102 \div 3 = 34,\ 108 \div 3 = 36$$

Portanto, os números procurados são $24, 26, 32, 34, 36$

Problema 3:

Outra Aplicação é a codificação de mensagens RCA, em que sua fundamentação é puramente baseadas nos números primos justamente por eles serem impossíveis de serem fatorados e consequentemente difíceis de serem encontrados .Traremos um exemplo com etapas de decodificação como mostraremos abaixo . Segundo Coutinho (2003), a primeira etapa do método é a pré-codificação que consiste em converter a mensagem desejada em uma sequência de números. No caso em 48 que ilustraremos tomaremos nossa mensagem sem números grandes, para simplificar a descrição das etapas. Para a conversão das letras em números como desejamos utilizaremos o quadro abaixo : O espaço entre duas palavras

Δ	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

será substituído pelo número 99, quando fizermos a conversão. A frase que utilizaremos como exemplo será TEORIA DOS NÚMEROS. Feita a conversão para números segundo

o quadro acima temos:

$$2051518914151421135181519.$$

Os parâmetros dos sistema RSA são dois números primos que denotaremos por p e q, faremos $n = pq$. A última parte do processo de pré-codificação consiste em dividir o número obtido em blocos menores de n.

Assim, fazendo $p = 11$ e $q = 17$ temos $n = 11 \cdot 17 = 187$ e os blocos do número acima podem ser:

$$2 - 91 - 42 - 42 - 7 - 18 - 10 - 99 - 132 - 42 - 89 - 92 - 3 - 30 - 22 - 142 - 72 - 42 - 8.$$

Esses blocos poderiam ser escritos de outras formas, porém é preciso ter cuidado com aqueles que começam com o número 0, pois é mais fácil surgir problemas no momento da decodificação. Assim é finalizada a etapa de pré-codificação.

A segunda etapa é chamada de codificação, segundo Coutinho (2003). Nesta etapa precisaremos de n, assim como um número e que seja inversível módulo $\phi(n)$, ou ainda, $\text{mdc}(e, \phi(n)) = 1$. Como temos p e q definidos é fácil calcular $\phi(n)$, pois $\phi(n) = (p-1)(q-1)$. O par (n, e) será chamado de chave de codificação. Cada bloco que obtemos na etapa da pre-codificação será codificado separadamente e a mensagem codificada será a sequencia dos blocos codificados.

Em nosso caso temos $\phi(n) = \phi(187) = \phi(11 \cdot 17) = (11-1)(17-1) = 160$. Nosso número e será o menor primo que não divide 160, logo $e = 3$, assim temos a chave de codificação $(n, e) = (87, 3)$. A codificação de um bloco b será dada por

$$C(b) = \text{resto da divisão de } be \text{ por } n, \text{ sendo } b \text{ um bloco da mensagem.}$$

Em termos de aritmética modular temos,

$$C(b) \equiv b^e \mod n \text{ com } 0 < C(b) < n.$$

Codificando cada bloco obtemos:

- Como $2^3 = 8$ e $8 \equiv 8 \mod 187$, logo, $C(2) = 8$.
- Como $91^3 = 91^2 \cdot 91$, $91 \equiv 91 \mod 187$ e $91^2 \equiv 53 \mod 187$ então, $91^3 \equiv 91 \cdot 53 \equiv 148 \mod 187$. Logo, $C(91) = 148$.
- Como $42^3 = 42^2 \cdot 42$, $42 \equiv 42 \mod 187$ e $42^2 \equiv 81 \mod 187$ então, $42^3 \equiv 81 \cdot 42 \equiv 36 \mod 187$. Logo, $C(42) = 36$.
- Como $7^3 = 343$ e $343 \equiv 156 \mod 187$, logo, $C(7) = 156$.
- Como $18^3 = 18^2 \cdot 18$, $18 \equiv 18 \mod 187$ e $182 \equiv 137 \mod 187$ então, $183 \equiv 137 \cdot 18 \equiv 35 \mod 187$. Logo, $C(18) = 35$.

- Como $10^3 = 1000$ e $1000 \equiv 65 \mod 187$, logo, $C(10) = 65$.
- Como $99^3 = 99^2 \cdot 99$, $99 \equiv 99 \mod 187$ e $99^2 \equiv 77 \mod 187$ então, $99^3 \equiv 77 \cdot 99 \equiv 143 \mod 187$. Logo, $C(99) = 143$.
- Como $132^3 = 132^2 \cdot 132$, $132 \equiv (-55) \mod 187$, $132^2 \equiv 33 \mod 187$ então, $132^3 \equiv 33 \cdot (-55) \equiv -132 \equiv 55 \mod 187$. Logo, $C(132) = 55$.
- Como $89^3 = 89^2 \cdot 89$, $89 \equiv 89 \mod 187$ e $89^2 \equiv 67 \mod 187$ então, $89^3 \equiv 67 \cdot 89 \equiv 166 \mod 187$. Logo, $C(89) = 166$.
- Como $92^3 = 92^2 \cdot 92$, $92 \equiv 92 \mod 187$ e $92^2 \equiv 49 \mod 187$ então, $92^3 \equiv 49 \cdot 92 \equiv 20 \mod 187$. Logo, $C(92) = 20$.
- Como $3^3 = 27$ e $27 \equiv 27 \mod 187$, logo, $C(3) = 27$.
- Como $30^3 = 30^2 \cdot 30$, $30 \equiv 30 \mod 187$ e $30^2 \equiv 152 \mod 187$ então, $30^3 \equiv 152 \cdot 30 \equiv 72 \mod 187$. Logo, $C(30) = 72$.
- Como $22^3 = 22^2 \cdot 22$, $22 \equiv 22 \mod 187$ e $22^2 \equiv 110 \mod 187$ então, $22^3 \equiv 110 \cdot 22 \equiv 176 \mod 187$. Logo, $C(22) = 176$.
- Como $142^3 = 142^2 \cdot 142$, $142 \equiv 142 \mod 187$ e $142^2 \equiv 155 \mod 187$ então, $142^3 \equiv 155 \cdot 142 \equiv 131 \mod 187$. Logo, $C(142) = 131$.
- Como $72^3 = 72^2 \cdot 72 \equiv 72 \mod 187$ e $72^2 \equiv 135 \mod 187$ então, $72^3 \equiv 135 \cdot 72 \equiv 183 \mod 187$. Logo, $C(72) = 183$.
- Como $8^3 = 512$ e $512 \equiv 138 \mod 187$, logo, $C(8) = 138$.

Assim, a sequência dos blocos codificados é:

$$8-148-36-36-156-35-65-143-55-36-166-20-27-72-176-131-183-36-138$$

5 Distribuição dos números primos

Afinal, quantos serão os números primos? Essa pergunta perdurou nos antepassados, quando foi respondida e provada que sua quantidade seria infinita por um dos maiores matemáticos que existiu aproximadamente 400 a.c Euclides , que deixou registrado em seu livro "Elementos".

Apresentamos uma tabela em que exibe o ordenamento desses números no conjunto dos números naturais conhecida como Crivo Erastóstenes que geram números primos. Mas é importante salientar que esses e outros métodos de primalidades não são eficientes e são extremamentes lentos e muito trabalhosos. Erastótenes foi um matemático grego e bibliotecário da biblioteca de Alexandria (275-194)

Esse método consiste em encontrar números primos dentro um determinado intervalo limitado de números por exemplo:

Tomado um intervalo limitado $[1, 120] \subset \mathbb{N}^*$ como mostra na figura abaixo: Tomando o primeiro primo 2, encontramos e marcamos todos seus múltiplos dentro deste intervalo em seguida o processo se repete para o próximo primo o 3 e assim sucessivamente até o último primo 11 onde seus múltiplo se limitam dentro do intervalo. Com isso os números que não foram marcados (sobram) são números primos.

6 Questionário

Foi feita uma pesquisa com o questionário abaixo em que alunos do ensino fundamental, médio, curso superior em matemática e professores de matemática tinham que responder apenas "SIM" ou "NÃO" para assim avaliar o nível de desconhecimento sobre os números primos.

QUESTIONÁRIO

NÚMEROS PRIMOS - O fascinante e misterioso mundo dos números primos. Sua importância e suas aplicações.

1. Pra você existe alguma fórmula que encontre somente números primos?
   ◯ Sim ◯ Não
2. Voçê sabe o que diz o Teorema Fundamental da Aritmética?
   ◯ Sim ◯ Não
3. Você conhece os números de Fermat?
   ◯ Sim ◯ Não
4. Você conhece os números de Mersenne?
   ◯ Sim ◯ Não
5. Pra você todos os números primos são ímpares?
   ◯ Sim ◯ Não
6. O número 1 é primo?
   ◯ Sim ◯ Não
7. Você conhece os números primos gêmeos?
   ◯ Sim ◯ Não
8. Você conhece os números primos trigêmeos?
   ◯ Sim ◯ Não
9. Você conhece alguma aplicação dos números primos?
   ◯ Sim ◯ Não
10. Dentre as seguintes áreas de pesquisa: sistemas dinâmicos, criptografia RCA e robótica, voçê identificaria qual delas seria uma aplicação de números primos?
    ◯ Sim ◯ Não

11. O conjunto dos números primos é infinito?

    ◯ Sim ◯ Não

12. Dado um número natural, você conhece algum método que identifique se esse tal número é ou não um número primo?

    ◯ Sim ◯ Não

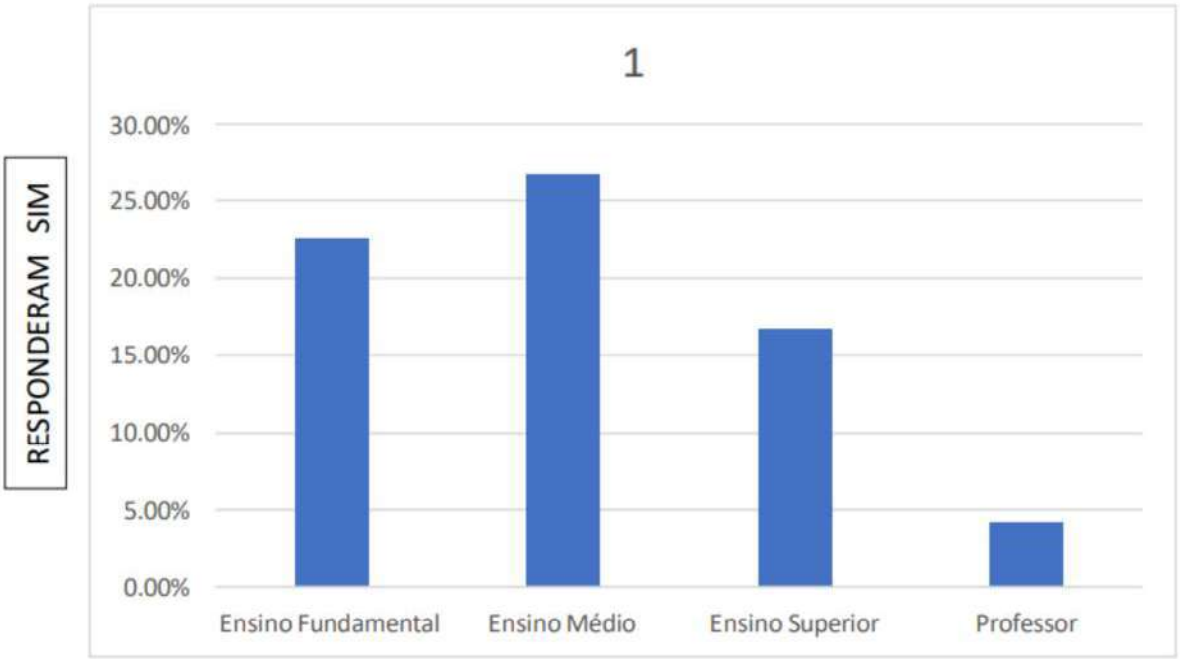
13. Dos seguintes números : 2, 33, 119, 149, e 193, você concorda que apenas três deles é primo?

    ◯ Sim ◯ Não

7 Análise de Dados

A partir de agora vamos analisar os gráficos com as perguntas feitas a vários níveis de ensino onde o eixo das ordenadas vai representar a porcentagem de erros dos grupos em geral e iremos fazer a associação com o nível de desconhecimento de cada grupo sobre os números primos.

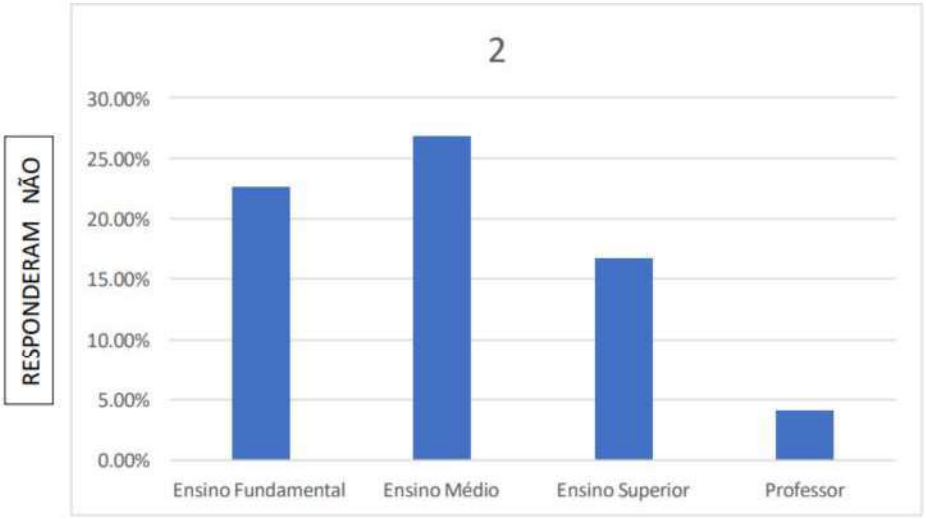
1) Pra você existe alguma fórmula que encontre somente números primos?



A resposta certa é não. Podemos perceber através do gráfico por exemplo que mais de 20% do ensino fundamental acreditam que possa existir uma fórmula que so encontre números primos, e que por incrível que pareça quase 5% dos professores também acreditam.

Figura 1 – Analise das respostas da Questão 1

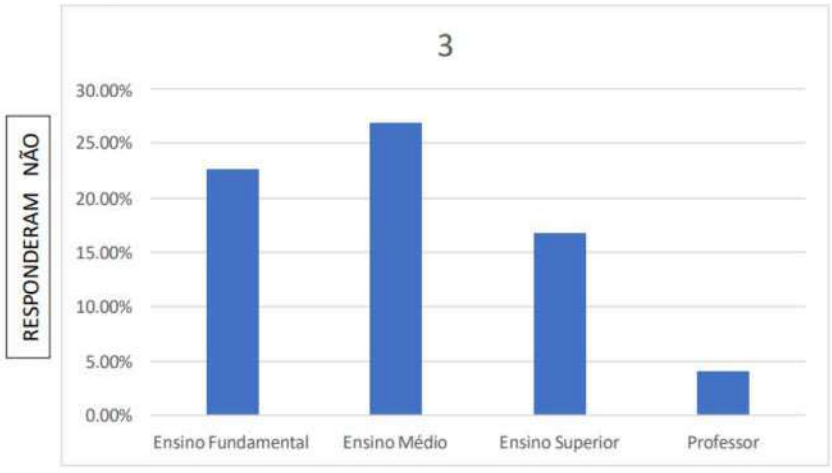
2) Você sabe o que diz o teorema fundamental da Aritmética?



Neste caso mais de 15% dos estudantes não conhecem o teorema fundamental da aritmética, seria comum o desconhecimento para os alunos do fundamental e médio, já que esse tema é ofertado no ensino superior, porém alguns alunos e professor desconhecem.

Figura 2 – Analise das respostas da Questão 2

3) Você conhece os Números de Fermat ?



Esse foi o método para encontrar números primos mais conhecido no mundo da pesquisa em matemática. Isso devido ao equívoco no entendimento do Matemático Fermat, quando ele acreditou que sua fórmula $F_n = 2^{2^n} - 1$, fosse gerar todos os núeros primos, só que 100 anos depois foi derrubada essa afirmação pelo Matemático Euler, que mostrou o erro para n = 5.

Figura 3 – Analise das respostas da Questão 3

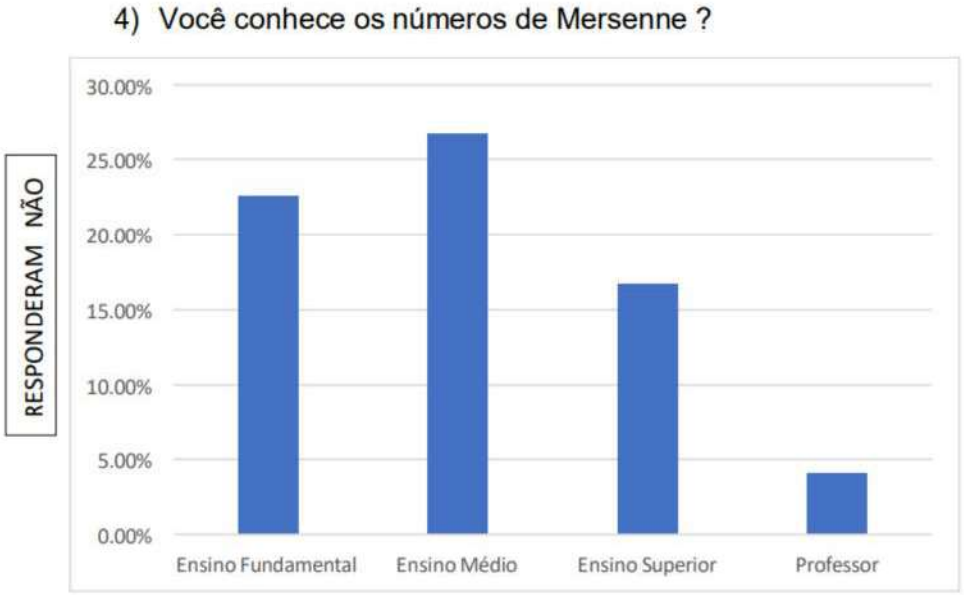


Figura 4 – Analise das respostas da Questão 4

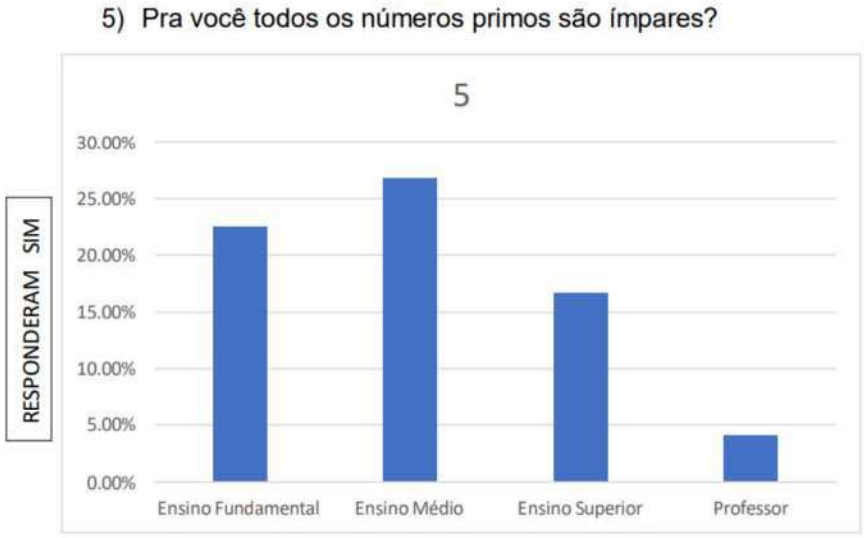


Figura 5 – Analise das respostas da Questão 5

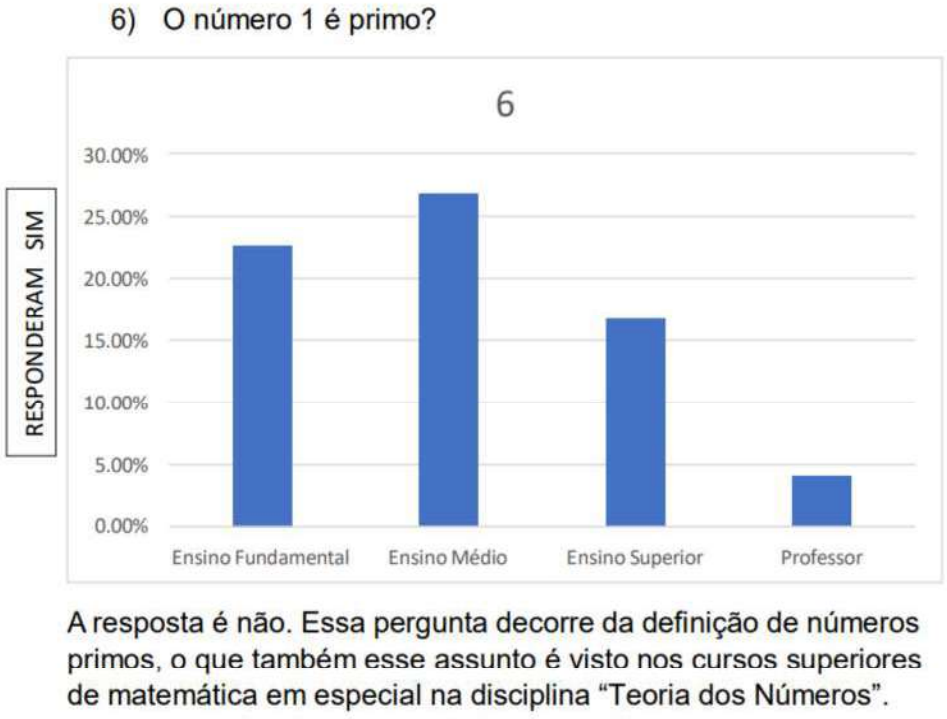


Figura 6 – Analise das respostas da Questão 6

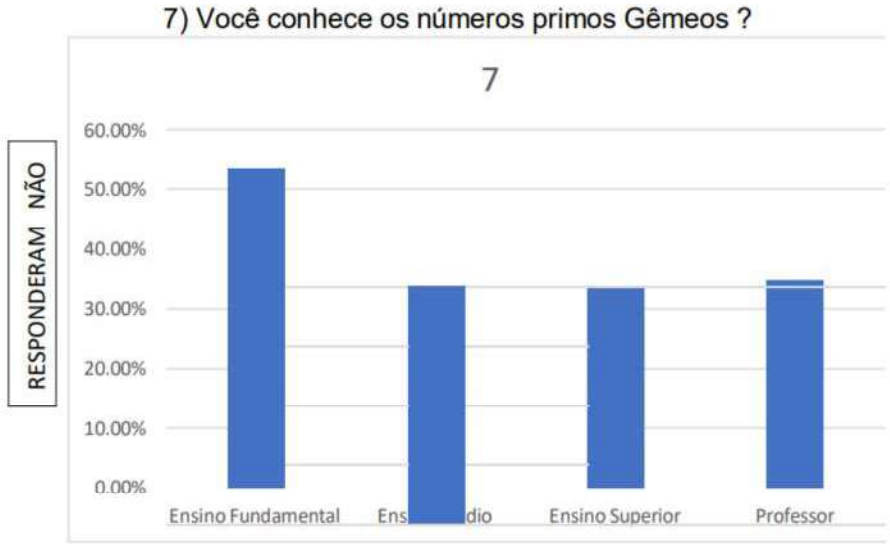


Figura 7 – Analise das respostas da Questão 7

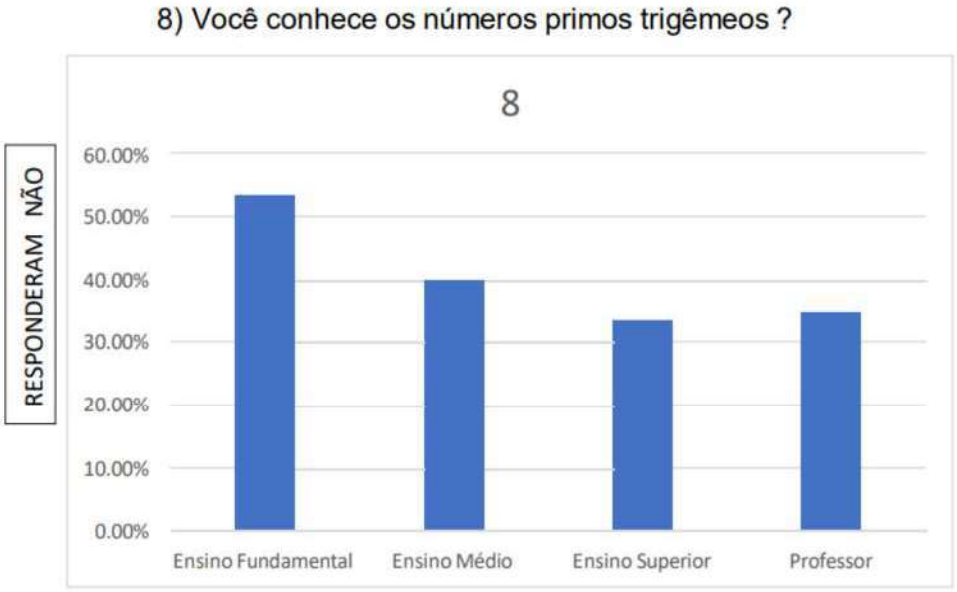


Figura 8 – Analise das respostas da Questão 8

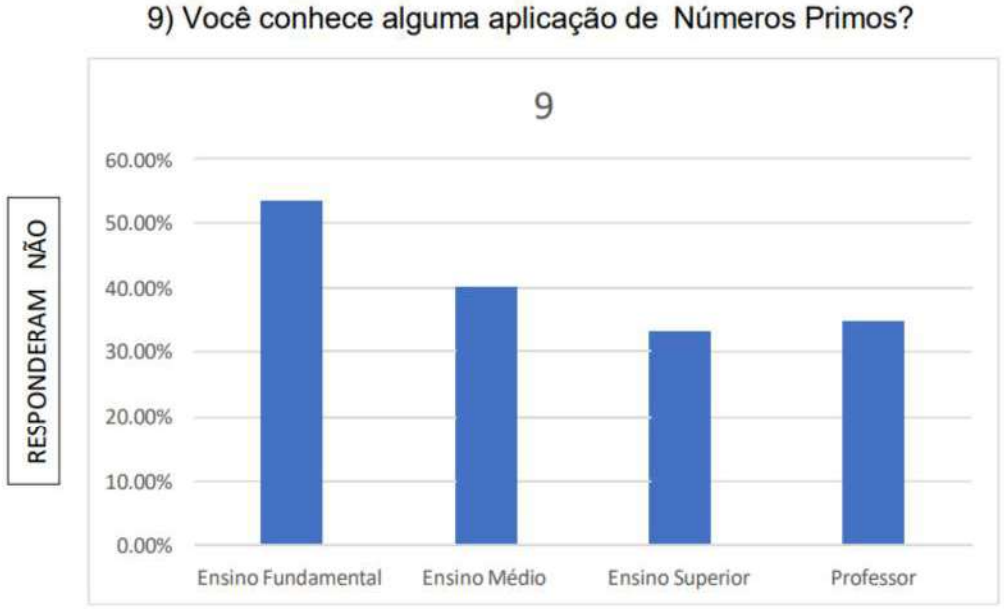
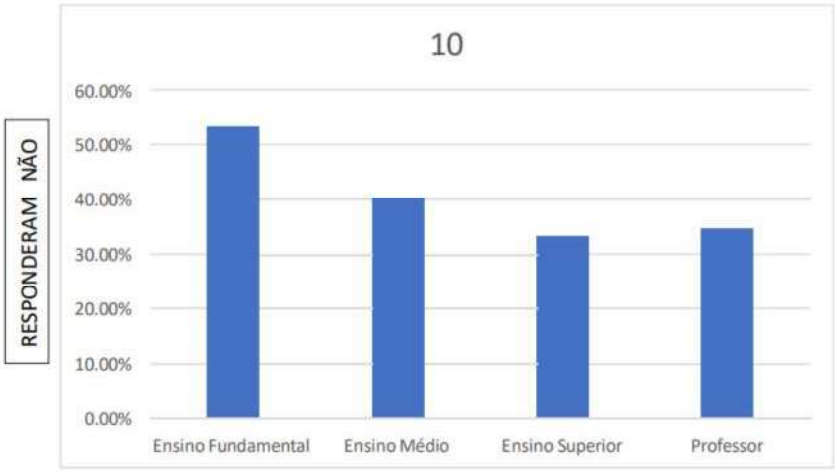


Figura 9 – Analise das respostas da Questão 9

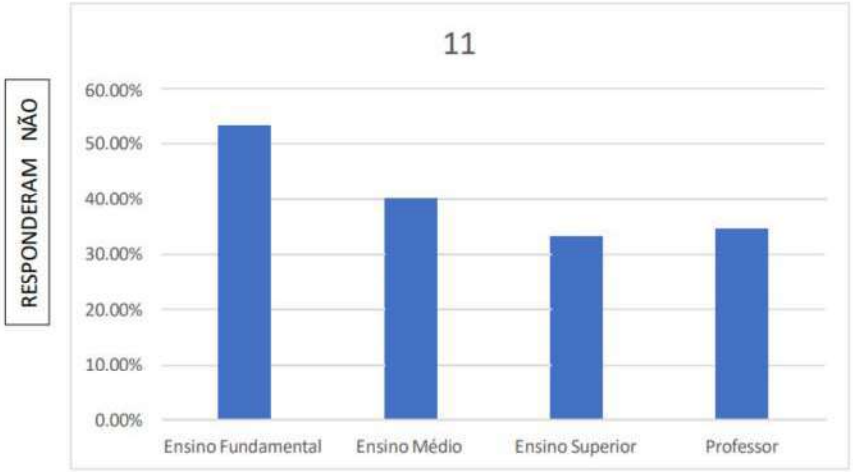
10)Entre as seguintes áreas de pesquisa: Sistemas dinâmicos, criptografia RCA e robótica, você identificaria qual delas seriam aplicações de números primos?



Uma das áreas que envolvem pesquisas sobre os números primos é a criptografia RCA . É uma pergunta específica, era de se esperar muitos erros.

Figura 10 – Analise das respostas da Questão 10

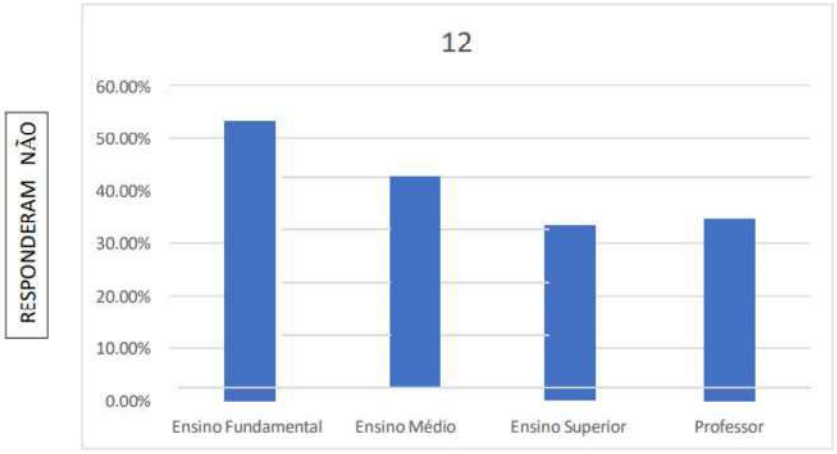
11) O conjunto dos números primos é infinito?



Essa é a pergunta talvez mais clássica do mundo dos números primos. Esse resultado que vem do teorema mais conhecido deste tema, provado pelo um dos matemáticos mais notáveis de todos os tempos “Euclides “que está em seu livro “Os elementos “um livro que possui mais de 300 anos de existência. A resposta sim.

Figura 11 – Analise das respostas da Questão 11

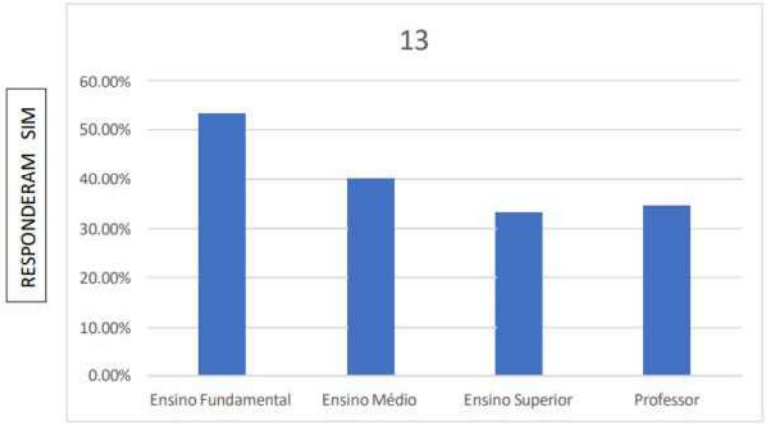
12) Dado um número natural, você conhece algum método que identifique se esse tal número é ou não um número primo ?



Existem vários métodos, o da raiz, o do Matemático Lucas entre outros. O que já era de se esperar, é que o nível fundamental e médio viessem a desconhecer mais que os outros, e que os níveis superior e professores conhecessem mais.

Figura 12 – Analise das respostas da Questão 12

13) Dos seguintes números: 2 , 33 , 119, 127 , 149 e 193 , Você concorda que apenas três deles é primo?



Para essa pergunta os alunos e professores poderiam fazer uma consulta do crivo de Eratóstenes, por se tratar de números formados por poucos dígitos o que ficaria mais difícil para números formados de quatro dígitos em diante que teriam que usar recursos computacionais. Parece que todos os níveis não buscaram fazer a pesquisa e logo muitos não acertaram e que existem quatro números primos, restando os compostos 33 e 119.

Figura 13 – Analise das respostas da Questão 13

8 Conclusão

É de impressionar que inúmeros alunos, e até professores que ensinam matemática, venham a desconhecer definições e elementos básicos que envolvem a teoria dos números primos. Era de se esperar que os estudantes do nível fundamental e médio viessem errar perguntas referentes ao nível superior . Por outro lado, , era também de se esperar que os estudantes do nível superior e professores viessem a acertar perguntas referentes ao nível fundamental e médio . Como por exemplo: "Pra você existe uma fórmula que possa gerar somente números primos?" ou "Pra você, todos números primos são impares?".As respostas erradas dadas a estes tipos de perguntas (anteriores) , surpreenderam, já que de certa forma alguns dos participantes já teriam visto esses contcúdos.

Esse trabalho sem dúvida trouxe um diagnóstico e apontou para o deficit no conhecimento sobre o tema (números primos) de alguns alunos e professores de matemática . Ele (esse trabalho) ainda aponta talvez para uma necessidade em reformular as componentes do curso de matemática, para que o curso possa dar mais ênfase a esse assunto , e fornecer uma melhor formação aos estudantes e futuros professores ou pesquisadores (em matemática) que venham a trabalha com pesquisa em teoria dos números . Talvez alguém venha acreditar que esses conhecimentos sejam poucos relevantes para sua formação acadêmica , com certeza iria logo mudar de ideia quando passasse a aconhecer as aplicações e importância destes números no mundo dos negócios e na segurança de dados . Por outro lado, esse trabalho pode parecer apenas um parêntese, diante de uma infinidade de artigos científicos e teses de mestrados nesse seguimento , mas foi feito de maneira minuciosa e cuidadosa desde as propriedades bem como seu contexto histórico. Com certeza haverá uma grande possibilidade que esse trabalho possar ser futuramente ampliado, tendo em vista ao novo mundo e suas novas descobertas. O mundo caminha para o universo da tecnologia 5 G, sites de pesquisa avançada a exemplo de chatGPT e o surgimento da IA (inteligência virtual) que configurará uma nova geração em que as pesquisas sobre os números primos baseadas em segurança de dados irá crescer na mesma proporção.

Referências

[1] Coutinho, S.C., **Números Inteiros e Criptografia RSA**, Coleção Matemática e Aplicações, 2009.

[2] Hefez, A., **Elementos da Aritmética**, SBM, 2006

[3] Milies, C. P & Coelho, S. P., **Números - Uma Introdução à Matemática** EDUSP, 2001.

[4] Moreira, C. G. T.A., Martinez, F. E. B. & Saldanha, N. C., **Tópicos de Teoria dos Números** Coleção Profmat, SBM 2012.

[5] Santos, J. P. de O., **Introdução à Teoria dos Números**, Coleção Matemática Universitária, 1998.

[6] Ribendoim, P., **Números Primos Velhos Mistérios e Novos Recordes**, Coleção Matemática Universitária, 2012.

[7] **Números Primos: Relação Histórica e Algumas Curiosidades**, Revista IfsCiência, 4 edição do 6 ano.

Anexos

ANEXO A – Teste de Primalidade

TESTE DE PRIMALIDADE

TESTE DE MILLER-RABIN

Seja n um número primo e a um número inteiro escolhido aleatoriamente, tal que

$1 < a > n$. Seja $s = max\ \{ r \in \mathbb{N} : 2^r$ divide $(n\text{-}1) \}$. s é o maior expoente, tal que $2^s \mid (s\text{-}1)$.

Seja d = $(n\text{-}1)/2^n$.Por definição de s, d é, necessariamente ímpar.

TEOREMA

Se n é um número primo e a não tiver um divisor comum com n, então

$a^d \equiv 1\ (mod\ n)$ ou existe um $r \in \{ 0,1,\ldots,s\text{-}1\}$, tal que $a^{2^r d} \equiv 1(mod\ n)$.

Um número a que não satisfaz o teorema acima é denominado de testemunha contra a primalidade de n

TESTE DE FERMAT

O teorema de Fermat, que originou o teste de primalidade de Fermat, oferece um teste simples e eficiente para ignorar números não primos. Qualquer número que falhe ao teste não é primo.

TEOREMA

Se m é primo, então para qualquer a tal que $mdc(a, m) = 1$, temos:

$$a^{m-1} \equiv 1(mod\ m)$$

Se m não é primo, ainda é possível (embora pouco provável) que o supradito se verifique.

Se m é ímpar composto, e a um inteiro tal que $mdc(a, m) = 1$ e $a^{m-1} \equiv 1(mod\ m)$ diz-se que m é *Pseudoprimo*, i.e. um número não primo que passa no teste de Fermat.