Universidade Federal do Rio Grande do Norte
Centro de Ciências Exatas e da Terra
Departamento de Informática e Matemática Aplicada
Curso de Ciências da Computação

ALGUMAS EVIDÊNCIAS COMPUTACIONAIS DA INFINITUDE DOS NÚMEROS PRIMOS PALINDRÔMICOS E GENERALIZAÇÕES DESTES

Aluno: Hugo Tácito Azevedo de Sena
Orientador: Benjamín René Callejas Bedregal

NATAL – RN
2008

HUGO TÁCITO AZEVEDO DE SENA

ALGUMAS EVIDÊNCIAS COMPUTACIONAIS DA INFINITUDE DOS NÚMEROS PRIMOS PALINDRÔMICOS E GENERALIZAÇÕES DESTES

Monografia apresentada à disciplina Relatório de Graduação, ministrada pelo professor Martin Alejandro Musicante para fins de avaliação da disciplina e como requisito para a conclusão do curso de Ciências da Computação do Departamento de Informática e Matemática Aplicada da Universidade Federal do Rio Grande do Norte.

Orientador: Prof. Dr. Benjamín René Callejas Bedregal

Natal – RN
2008

HUGO TÁCITO AZEVEDO DE SENA

ALGUMAS EVIDÊNCIAS COMPUTACIONAIS DA INFINITUDE DOS NÚMEROS PRIMOS PALINDRÔMICOS E GENERALIZAÇÕES DESTES

Monografia apresentada à disciplina Relatório de Graduação, ministrada pelo professor Martin Alejandro Musicante para fins de avaliação da disciplina e como requisito para a conclusão do curso de Ciências da Computação do Departamento de Informática e Matemática Aplicada da Universidade Federal do Rio Grande do Norte.

MONOGRAFIA APROVADA EM 25/06/2008

BANCA EXAMINADORA

_____

Professor: Benjamín René Callejas Bedregal
DIMAp - UFRN

_____

Professor: Márcia Maria de Castro Cruz
Departamento de Matemática - UFRN

_____

Professor: Roque Mendes Prado Trindade
Departamento de Ciências Exatas - UESB

Aos meus pais e amigos

AGRADECIMENTOS

À Deus, fonte de toda a vida, por iluminar meu caminho e me dar forças para seguir sempre em frente. .

Aos meus queridos pais pelas orações, pelos conselhos, empenho, estímulo, força para realizar este trabalho e o grande amor dado a mim em todos os momentos bons e ruins de minha vida.

Ao meu orientador, Benjamín René Callejas Bedregal, pelas orientações, discussões enriquecedoras, dedicação, paciência e apoio durante esta longa jornada.

À minha família, por me guiarem com muito amor nos caminhos corretos da vida.

Aos meus grandes amigos que sempre me incentivaram e me proporcionaram momentos de lazer, imprescindíveis ao bom andamento deste estudo.

À todos os professores, que foram os responsáveis pela minha formação acadêmica, pessoal e profissional.

Enfim, a todos que de alguma maneira contribuíram para a execução desse trabalho, seja pela ajuda constante ou por uma palavra de amizade!

RESUMO

Este trabalho irá abordar um assunto que ainda é pouco explorado na área da Teoria dos números, que são os números primos palindrômicos. O objetivo deste trabalho é evidenciar computacionalmente a infinitude destes através de vários testes. Alguns conceitos da teoria dos números, essenciais para o entendimento do trabalho, e os conceitos do que são palíndromos e números palindrômicos serão explicados aqui. Além disso, explicitaremos também algumas generalizações dos números palindrômicos e um caso particular destes. Os testes de primalidade, que são algoritmos para testar se um número inteiro positivo é primo ou não, também são explicados neste trabalho. Por fim são apresentados os resultados teóricos e computacionais obtidos, bem como considerações finais sobre este trabalho.

Palavras-chave: números primos, números palindrômicos, números primos palindrômicos, testes de primalidade, generalizações.

ABSTRACT

This work will show an subject that is rarely studied on Numbers Theory, which are the palindromic prime numbers, or palprimes. The objective of this work is to show computational evidences about the infinitude of these numbers, through several tests. Some concepts of Numbers Theory needed to understand this work, and definitions about palindrome and palindromic numbers are explained here. Besides, we show some generalizations and a particular case of palindromic numbers. The primality tests - used to test a number for primality - are also explained in this work. Finally the theoric and computational results are presented, as well as final considerations about this work.

Keywords: prime numbers, palindromic numbers, primality tests, generalizations.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Antes de Cristo
2D	2 Dimensões
max	Máximo em relação a um conjunto de números reais
min	Mínimo em relação a um conjunto de números reais
mdc	Máximo divisor comum
mmc	Mínimo múltiplo comum
ln	Logaritmo Neperiano
mod	Módulo da divisão entre dois números
NP	Determinístico Não Polinomial
Co-NP	Complemento de NP
P	Polinomial
AKS	Algoritmo de Teste de Primalidade Determinístico
O	Notação Assimptótica para Complexidade de Pior Caso
$\mid$	Divide
$\nmid$	Não Divide
$\rightarrow$	Implica
$\leq$	Menor ou Igual
$\geq$	Maior ou Igual
$\neq$	Diferença
$=$	Igualdade
$\equiv$	Congruência
$\not\equiv$	Incongruência
$\pm$	Mais ou Menos
$\prod$	Produtório
$\sim$	Aproximadente igual
n!	Número Fatorial
n#	Número Primorial
E_n	Número de Euclides
M_n	Número de Mersenne

F_n	Número de Fermat
$F(n)$	Números de Fibonacci
$\sum$	Somatório
log	Logaritmo
$\sqrt{}$	Raiz Quadrada
$D^{[k]}$	Caractere D repetido k vezes
$\#D^{[k]}$	Número composto apenas pelo Dígito D repetido k vezes
φ	Função que define o comportamento do palíndromo genérico
$\in$	Pertence
$\mathbb{N}$	Conjunto dos números naturais

SUMÁRIO

1 INTRODUÇÃO

Números primos, no entendimento de alguns matemáticos, são números naturais que possuem apenas dois divisores diferentes: um e eles mesmos. Outros matemáticos definem número primo como sendo um número inteiro que possui apenas quatro divisores. Assim, excluímos o número 1, pois ele só pode ser dividido por dois divisores {1 e -1}. Se um número natural é maior que 1 e não é primo, ele é chamado de composto. Os números 0 e 1 não são considerados nem primos nem compostos.

O estudo dos números primos faz parte da Teoria dos Números, a parte da matemática que estuda os números inteiros (embora alguns matemáticos considerem apenas os números naturais), bem como o seu comportamento. Os números primos são alvos de intensas pesquisas, e algumas questões simples e fundamentais têm permanecido sem resposta há séculos, ou então só recentemente obtiveram resposta. Algumas questões são bem conhecidas e famosas como as conjecturas de Cramér e Goldbach. Por isso, os números primos continuam a intrigar os matemáticos por suas características únicas e peculiares.

O problema da distribuição dos números primos é um dos principais objetos de investigação entre os matemáticos: quando observados individualmente, os primos parecem ser distribuídos aleatoriamente, mas quando observados de maneira global, a distribuição parece obedecer a leis bem definidas. Adrien-Marie Legendre e Johann Friedrich Gauss fizeram grandes estudos sobre a densidade dos números primos e chegaram ao Teorema dos Números primos.

Um palíndromo é uma palavra ou número que pode ser lido de trás pra frente do mesmo jeito que de frente pra trás. Um número palindrômico é um

número em que seus dígitos, quando lidos da esquerda pra direita, resulta no mesmo que quando lido da direita pra esquerda, como por exemplo, 43234. Obviamente, números palindrômicos dependem da base na qual são representados, por exemplo, o número onze é palindrômico na base 10, mas não na base 2. Na maior parte do trabalho, usamos a base 10. Quando uma outra base for usada, mencionaremos explicitamente a que base nos referimos. Estes números são estudados por matemáticos em busca de propriedades especiais. Um número palindrômico primo, claramente, é um número que é primo e palindrômico ao mesmo tempo.

Não é fácil provar qualquer fato sobre os números primos. Sua seqüência é razoavelmente suave, mas eles também possuem grande buracos e focos mais densos na seqüência dos números naturais. Quão grandes são esses buracos? Por exemplo, há pelo menos um número primo para uma dada quantidade de dígitos? A resposta é uma afirmativa, mas ela só foi de fato provada na metade do século dezenove, e muitas questões permanecem abertas.

Uma nova onda de desenvolvimento na área da Teoria dos Números surgiu com o advento dos computadores. Como decidir quando um número positivo *n* é primo? É claro que este é um problema finito, mas simples testes de primalidade se tornariam impraticáveis à medida que o número de dígitos cresce. Só acerca de 25 anos atrás, começaram a utilizar idéias que ajudaram a realizar testes de primalidade de maneira mais eficiente. Usando estes métodos, pode-se facilmente determinar se um número de 1000 dígitos é primo ou não.

1.1 MOTIVAÇÃO

Devido a suas propriedades imprevisíveis, os números primos possuem várias questões em aberto e, muitas outras que poderiam ser bastante

importantes para a teoria dos números talvez nunca cheguem a ser formuladas. O que também atrai a atenção de alguns matemáticos, é a maneira como os números primos estão distribuídos, o que acaba gerando muitos desentendimentos e pontos de vista divergentes. Uns dizem que a distribuição é irregular, outros dizem que é regular. A hipótese de Riehman aparece justamente para aumentar ainda mais esses desentendimentos, pois ele diz que todos os números primos são distribuídos o mais regularmente possível, embora nenhuma prova dessa hipótese exista.

Algumas conjecturas associadas a números primos serão apresentadas abaixo:

- Conjectura de Goldbach Forte: diz que todo número inteiro par $n>2$ é a soma de dois primos.

- Conjectura de Goldbach Fraca: diz que todo número inteiro impar $n>5$ é a soma de três primos.

- Conjectura dos primos gêmeos: Existem infinitos primos gêmeos, que são pares de primos cuja diferença entre eles é dois.

- Números primos Euclidianos: não é sabido se os números primos Euclidianos são infinitos ou não.

- O número de primos de Fermat é finito

- O número de primos de Mersenne é infinito

- Conjectura de Brocard: há sempre pelo menos quatro primos entre quadrados consecutivos de primos maior que 2.

- Conjectura de Legendre: há sempre um primo entre n^2 e $(n + 1)^2$ para qualquer inteiro positivo n.

- Toda pirâmide de primos palindrômicos com o passo fixo tem tamanho finito.

1.2 HISTÓRIA DOS NÚMEROS PRIMOS

Os números primos, bem como suas propriedades, começaram a ser estudados pelos antigos matemáticos gregos, embora existam registros de que os antigos egípcios possuíam algum conhecimento sobre os números primos.

Pitágoras de Samos foi um dos precursores desse estudo, que representou um grande avanço na matemática, embora o seu interesse estivesse mais no aspecto místico, chegando a inclusive criar a escola Pitagórica (500 a 300 AC). Ele e seus seguidores possuíam noções de primalidade e se interessavam por números perfeitos e amigáveis. Esta escola dava uma enorme importância ao número ”1”, que era chamado de unidade. Os outros números tinham uma importância reduzida, pois todos eles representavam apenas multiplicidades da unidade e por isso eram chamados de números.

A partir dessas denominações, os pitagóricos começaram a perceber que existiam dois tipos de números:

- Números primos: são números que não podem ser gerados via multiplicação a partir de outros números, como 2,3,5,7,11, etc.

- Números compostos, ou secundários: são números que podem ser gerados a partir de outros números, como o 6 = 2*3, 9 = 3*3,...

Os Elementos de Euclides (cerca de 300AC) possuem importantes teoremas sobre números primos, inclusive uma prova de que os números primos são infinitos, utilizando uma demonstração pelo método da contradição. Euclides demonstra também a Teoria Fundamental da Aritmética que diz que qualquer inteiro só pode ser decomposto como produto de primos de uma única maneira. Euclides também mostrou como construir um número perfeito a partir de um primo Mersenne.

Em 200AC o grego Eratóstenes, criou o Crivo de Eratóstenes, uma maneira simples de calcular primos.

Em seguida, durante séculos, o estudo dos números primos foi abandonado e só foi retomado no século XVII.

Pierre de Fermat surge no início do século XVII provando a conjectura de Albert Girard e cria alguns teoremas que mais tarde seriam usados como base de muitos resultados da Teoria dos Números e de métodos para testes de primalidade que são utilizados até hoje. Fermat correspondeu-se com outros matemáticos do seu tempo, como Marin Mersenne, que junto com Fermat, formularam os Números de Mersenne (número na forma $2^n - 1$).

Provar que um número é primo (para números grandes) não é feito pela divisão trivial. Muitos matemáticos trabalharam em vários teste de primalidade para grandes números, em especial, números de forma específica. Alguns testes de primalidade são: AKS, Fermat, Lucas-Lehmer, Solovay-Stressen, Miller-rabin e curva elíptica. Apesar da existência de vários testes de primalidade, nenhum deles funciona de maneira rápida e eficiente.

Com o advento dos computadores, intensas pesquisas têm sido realizadas em busca de números primos com a maior quantidade de dígitos possível. Até o momento da escrita deste relatório de graduação, o maior

número primo tinha cerca de nove milhões de dígitos e é um Primo de Mersenne.

Por um longo tempo, acreditava-se que os números primos não possuíam nenhuma aplicação fora da matemática. Isso mudou quando em 1970 surgiu o conceito de chave pública criptográfica, que faz uso de números semiprimos (é um número natural que é o produto de dois números primos) e formam a base do algoritmo do sistema de criptografia da RSA.

1.3 HISTÓRIA DOS PALÍNDROMOS

A palavra “palíndromo” tem origem grega, mas foi inventada pelo escritor Ben Johnson no século XVII, embora existam registros de palíndromos desde o ano 79DC.

Os palíndromos surgiram como uma forma de brincar com as palavras, por exemplo, os antigos gregos criaram o seguinte palíndromo em muitas de suas fontes batismais: “Nipson anomēmata mē monan opsin”. Isto é traduzido como “lave seus pecados tão bem quanto seus rostos”. Pode-se perceber que isto não é um palíndromo, mas acontece que isto foi escrito usando o alfabeto latino. Quando caracteres gregos são usados isto se torna um palíndromo, pois o “ps” é uma única letra no alfabeto grego, resultando na seguinte cadeia de caracteres gregos: “ΝΙΨΟΝΑΝΟΜΗΜΑΤΑΜΗΜΟΝΑΝΟΨΙΝ”.

Os romanos também admiravam os palíndromos e chegaram a produzir a seguinte sentença: “In girum imus nocte et consumimur igni.” Que significa “nós entramos no círculo depois da escuridão e fomos consumidos pelo fogo” que é dito para descrever o movimento das traças.

O seguinte palíndromo quadrado também é datado da era dos romanos e foi gravado numa pedra fora de Roma, na Itália, e é o mais antigo palíndromo 2D conhecido.

S	A	**T**	O	R
A	R	**E**	P	O
T	**E**	**N**	**E**	**T**
O	P	**E**	R	A
R	O	**T**	A	S

Figura 1.1: Palíndromo 2D

"Sator arepo tenent opera rotas" significa "O semeador Arepo trabalha com a ajuda de uma roda".

Napoleão Bonaparte também falou propositadamente o palíndromo "Able was I ere I saw Elba", ao se referir a ilha de Elba, onde ele foi exilado pelos britânicos.

No conjunto dos números primos palindrômicos, Shareef Bacchus prova por indução que 11 é o único número primo com um número par de dígitos. Qualquer outro palíndromo com um número par de dígitos é divisível por 11, e por isso não pode ser primo. Por exemplo, 987789 é 11 vezes 89799. A lista de curiosidades descobertas por matemáticos e numerologistas é bastante ampla.

O maior primo palindrômico conhecido é $10^{180004} + 248797842 \times 10^{89998} + 1$, encontrado por Harvey Dubner em 2007.

Paulo Ribenboim, um matemático brasileiro, definiu o palíndromo primo triplo, como um número primo palindrômico *p* com *q* dígitos, onde *q* é um palíndromo primo com *r* dígitos, no qual *r* também é um primo palindrômico.

Uma pirâmide de primos palindrômicos é uma seqüência de primos em que cada termo é um palíndromo com o termo anterior como os dígitos

centrais. Então começando com o número primo dois, pode-se chegar a uma pirâmide de primos palindrômicos como os seguintes:

2	2
929	929
39293	39293
7392937	3392933
373929373	733929337

Tabela 1.1: Pirâmide de Primos Palindrômicos

Estas duas pirâmides são as mais altas que podem ser produzidas pelo número 2 e adicionando apenas um dígito de cada lado (passo único).

1.4 IMPORTÂNCIA

Os números primos possuem um papel fundamental na Matemática e na Teoria dos Números, pois eles fazem parte do teorema fundamental dos números, que diz que qualquer número inteiro maior que um e que não seja primo, pode ser escrito como um produto de fatores primos, e isto é a base para várias aplicações na Teoria dos Números. Assim sendo, os números primos são considerados produtos de um único fator (eles mesmos).

A partir do teorema fundamental dos números, pode-se dizer que todo número possui fatoração única se não considerarmos a ordem dos fatores, o que nos leva a concluir que todo número inteiro pode ser reconhecido através de seus fatores. Como os números são representados de maneira única em fatores primos, dois números distintos jamais possuirão a mesma fatoração.

O teorema fundamental dos números é usado em diversas provas de outros teoremas matemáticos, como por exemplo, Euclides enunciou um

teorema que diz que a quantidade de números primos é infinita, e provou isto através de uma contradição envolvendo o teorema fundamental dos números.

Os números primos também têm um papel muito importante na computação, principalmente na área de criptografia. Eles são usados por empresas que precisam transmitir dados com segurança, com a certeza de que eles não serão vistos por nenhuma pessoa que não esteja autorizada para tal. Para manter a salvo este tipo de informação, empresas usam os números primos ou semiprimos para tornar incompreensíveis as informações que precisam ser transmitidas, como se elas tivessem sido escritas em código indecifrável. E esta segurança só é possível graças à criptografia. Quanto maior o número primo (ou semiprimo), mais difícil decifrar a informação, pois é necessário um computador muito potente para trabalhar com tantos dígitos.

Várias organizações como a RSA (Rivest, Shamir, Adleman) têm se dedicado ao estudo dos números primos e suas aplicações na área de criptografia, e chegam inclusive a oferecer prêmios a quem conseguir descobrir um de seus fatores.

Os palíndromos por sua vez também possuem importância devido as suas características únicas, que causam certo interesse na área da Teoria da Computação. Na teoria dos autômatos, um conjunto de palíndromos num dado alfabeto é o típico exemplo de uma linguagem que é livre de contexto, mas não regular. Isto significa que é teoricamente impossível para um computador com uma quantidade finita de memória testar confiantemente todos os palíndromos. (Para objetivos práticos com computadores modernos, esta limitação só se aplicaria as seqüências de caracteres inacreditavelmente longas.). Adicionalmente, o conjunto de palíndromos não pode ser testado fielmente por um autômato de pilha determinístico, e nem podem ser verificados sintaticamente através de gramáticas LR(k), pois lendo um palíndromo da esquerda para a direita, é essencialmente impossível localizar "o meio" até que a palavra inteira tenha sido lida. Porém, a linguagem dos palíndromos pertence

à classe das linguagens lineares determinísticas e, portanto eles podem ser analisados via autômatos lineares determinísticos (Bedregal, 2008).

1.5 OBJETIVOS

Existem algumas conjecturas em torno dos números palindrômicos como a que diz que existem infinitos números palindrômicos primos na base 10. O objetivo deste trabalho é proporcionar algumas evidências computacionais desta conjectura. Para isto desenvolvemos um programa capaz de gerar um número primo palindrômico razoavelmente grande (com mais 1000 casas decimais). Além disso, um tipo particular de números primos palindrômicos - aqueles formados por um só dígito - será estudado. Também será analisada uma generalização do conceito de palíndromos e procuraremos encontrar números primos relativamente grandes para algumas instâncias dessa generalização.

Vale ressaltar que o objetivo deste trabalho não é tentar provar a infinitude dos números primos palindrômicos, mas na realidade, tentar descobrir ou evidenciar, a partir desses resultados computacionais, conjecturas sobre a infinitude de números primos palindrômicos para essas variantes.

1.6 ABORDAGEM DOS CAPÍTULOS

Este trabalho foi organizado de forma que o leitor comece a entender um pouco da teoria dos números, bem como a idéia de números primos e números palindrômicos, de maneira a tornar mais fácil a leitura e o entendimento dos capítulos subseqüentes.

No capítulo 1 foi apresentada a motivação para se realizar um estudo dos números primos palindrômicos, depois foi realizada uma breve explicação sobre o surgimento e curiosidades sobre os números primos e palíndromos.

Logo em seguida foi mostrada a importância do estudo destes números, e também quais são os objetivos deste trabalho.

No capítulo 2 serão apresentados conceitos fundamentais sobre a teoria dos números, e isto inclui desde conceitos básicos como divisibilidade e conceitos sobre os próprios números primos, até a apresentação de tipos especiais de números primos. Além disso, também serão abordados conceitos básicos sobre palíndromos e o funcionamento de alguns testes de primalidade.

O capítulo 3 apresenta alguns resultados teóricos que foram obtidos através da análise de alguns conjuntos de números em busca de possíveis primos, e também mostra como estes números se comportam. Neste capítulo são analisados palíndromos que são compostos por apenas um único dígito e também generalizações sobre os números palindrômicos.

No capítulo 4 será exposto como foram realizados os testes computacionais e também que ferramentas e algoritmos foram utilizados. Além disso, este capítulo aborda as dificuldades e limitações encontradadas para a realização dos testes de primalidade sobre números muito grandes.

No capítulo 5 serão apresentados os resultados computacionais que foram obtidos através da análise de alguns conjuntos relativamente grandes de números.

Finalmente, no capítulo 6 são apresentadas as considerações finais realizadas durante a construção deste trabalho e algumas conjecturas que poderão ser utilizadas para futuros trabalhos na área.

2 CONCEITOS FUNDAMENTAIS

2.1 TEORIA DOS NÚMEROS

A Teoria dos Números é uma área da matemática que estuda os números inteiros e suas propriedades únicas. O seu estudo começou com os filósofos e matemáticos acerca de 2500 anos. Apesar de todo esse tempo, ainda existem muitas questões simples que ainda não possuem resposta, e ainda outras que tiveram algumas respostas encontradas apenas há pouco tempo.

Este relatório de graduação possui como um de seus temas centrais os números primos, portanto, algumas explicações sobre os números primos e sobre a teoria dos números são necessárias. Algumas propriedades básicas dos números inteiros, como noções de divisibilidade, máximo divisor comum e mínimo múltiplo comum, serão discutidas.

2.1.1 Divisibilidade

Um dos conceitos mais básicos do estudo da teoria dos números é o conceito da divisibilidade. Diz-se que *a divide b*, ou *a é um divisor de b*, ou ainda que *b é múltiplo de a*, se existe algum inteiro *m* no qual $b = am$. Na notação utiliza-se $a \mid b$. Se *a* não é um divisor de *b* então se escreve: $a \nmid b$. Se $a \neq 0$, então $a \mid b$ significa que a razão b / a resulta num número um inteiro.

Se $a \nmid b$ e $a > 0$, então ainda é possível dividir *b* por *a* com um resto. O resto *r* da divisão $b \div a$ é um inteiro que satisfaz $0 \leq r < a$. Se o quociente da divisão com resto é *q*, então é obtido [1]:

$$b = aq + r \tag{2.1}$$

A partir disto, algumas observações podem ser realizadas e deram origem a um teorema.

Teorema 2.1: Para todo número inteiro a, b, c, pertencente aos inteiros obtêm-se [2]:

- $a \mid a$, $1 \mid a$ e $a \mid 0$;
- $0 \mid a$ se somente se, $a = 0$;
- Se $a \mid b$ e $a \mid c$ implica que $a \mid (b + c)$;
- Se $a \mid b$ implica que $a \mid -b$;
- Se $a \mid b$ e $b \mid c$ implica que $a \mid c$.

2.1.2 Máximo Divisor Comum

O máximo divisor comum é uma propriedade que existe entre dois números inteiros e diz qual é o maior inteiro que divide os dois. Matematicamente têm-se [3]:

$$mdc(a,b) = \max\{c \to c \mid a \quad e \quad c \mid b\} \tag{2.2}$$

Diz-se que dois números são *primos entre si* quando o máximo divisor comum entre eles é 1.

Note que para qualquer inteiro $a > 0$, o $mdc(a,0) = a$, porque qualquer número inteiro positivo divide *0*, e porque *a* é o maior divisor dele mesmo. Já o valor do $mdc(0,0)$ é indefinido.

2.1.3 Mínimo Múltiplo Comum

O mínimo múltiplo comum é outra propriedade que existe entre dois números inteiros e diz qual é o menor número que é divido pelos dois. Matematicamente tem-se [3]:

$$mmc(a,b) = \min\{c \to a \mid c \quad e \quad b \mid c\} \tag{2.3}$$

Isto se torna indefinido quando $a \leq 0$ ou $b \leq 0$. O mínimo múltiplo comum é análogo ao máximo divisor comum de alguma forma, mas não possui o mesmo tempo de resposta, pois o máximo divisor comum possui algumas propriedades interessantes. Uma delas, é um método de 2300 anos chamado algoritmo de Euclides, que será explorada mais tarde. Uma importante conseqüência deste algoritmo é o seguinte teorema [3]:

Teorema 2.2: Se c|a e c|b então c|mdc(a,b) (2.4)

2.1.4 Primos

Como já definido na introdução, um número inteiro positivo *p* é primo quando ele não é divisível por nenhum outro inteiro a não ser *1* e o próprio *p* (alguns autores também consideram os divisores *–1* e *–p*). Os primos também podem ser definidos como: “inteiros que não podem ser escritos como o produto de dois outros números positivos menores”. Por convenção, o número *1* não é primo, então a seqüência dos números primos irá começar com:

2, 3, 5, 7, 9, 11, 13, 17, 19, 23, 29, etc.

Alguns números podem parecer primos, como o 119 $(= 7 \cdot 17)$ ou 161$(= 7 \cdot 23)$. Estes e outros números, que tem três ou mais divisores, são

chamados de números compostos. Qualquer número inteiro positivo maior que 1 é primo ou composto, mas não ambos.

Os números primos são muito importantes, pois eles são a base para a construção de qualquer número inteiro, ou seja, qualquer número inteiro pode ser escrito como um produto de números primos. Supondo *n* um número inteiro maior que 1 e p_k um número primo qualquer. Matematicamente, tem-se que [3]:

$$n = p_1 \cdots p_m = \prod_{k=1}^{m} p_k \tag{2.5}$$

Por exemplo, $30 = 2 \cdot 3 \cdot 5$; $44 = 2 \cdot 2 \cdot 11$; $637 = 7 \cdot 7 \cdot 13$. Esta fatoração sempre é possível porque se $n > 1$ não é primo, então ele possui um divisor n_1, desta maneira, é possível escrever $n = n_1 \cdot n_2$, e sabe-se que n_1 e n_2 podem ser escritos como produtos de números primos. Os anciões gregos também sabiam e provaram que esta representação é única. O que significa que não existe mais de uma maneira de se escrever um número inteiro positivo como um produto de números primos.

É realmente surpreendente que até hoje não exista uma maneira eficiente de realizar uma fatoração. É claro que poderosos supercomputadores e sistemas de processamento paralelos massivos podem ser usados para encontrar decomposições por força bruta para alguns números muito grandes; o recorde está em torno de 300 dígitos, e a dificuldade cresce exponencialmente à medida que o número de dígitos aumenta. Encontrar a decomposição de um número de 1000 dígitos, por qualquer método conhecido, vai muito além das possibilidades de um computador, num futuro próximo.

Existem vários teoremas dentro da Teoria dos Números e dentre eles alguns serão citados [1]:

Teorema (Teorema Fundamental da Aritmética) 2.3: Qualquer número inteiro positivo pode ser escrito como um produto de números primos, e essa fatoração é única desconsiderando-se a ordem dos fatores.

Teorema 2.4: Existem Infinitos Números Primos.

Teorema 2.5: Para cada número inteiro positivo *k*, existem *k* números consecutivos que são compostos.

Teorema (O Teorema dos Números Primos) 2.6: Seja $\pi(n)$ o número de primos entre 1 e *n*. Então $\pi(n) \sim \frac{n}{\ln n}$.

2.1.5 Fatoração em Primos

Foi visto que, é possível escrever como produto de primos, qualquer número inteiro não primo, maior que "1". Os números primos são considerados produtos de um único fator, e o número 1 é considerado um "produto vazio". Sabendo disto, pode-se provar que o "Teorema Fundamental da Aritmética" (Teorema 1.3) é verdadeiro.

2.1.6 Números Fatoriais

Observando a fatoração de alguns números altamente compostos, os fatoriais, têm-se [3]:

$$n! = 1 \cdot 2 \cdot 3 \cdots n = \prod_{k=1}^{n} k, \text{ para todo inteiro n} \geq 0 \qquad (2.6)$$

De acordo com a convenção de produto vazio, isto define que 0! é 1. Então $n! = n \cdot (n-1)!$ para qualquer inteiro positivo *n*. Isto representa o número de permutações entre *n* objetos distintos. A seguir os 10 primeiros fatoriais:

n	1	2	3	4	5	6	7	8	9	10
n!	1	2	6	24	120	720	5040	40320	362880	3628800

Tabela 2.1: Números Fatoriais

É interessante saber os valores dos seis primeiros fatoriais e o fato de que *10!* é maior que 3.5 milhões. Outro fato interessante, é que o número de dígitos em *n!* ultrapassa *n* quando $n \geq 25$. [3]

2.1.7 Números Primoriais

Na matemática, um número primorial n# é um número natural que é definido como o produto de todos os números primos p_k menores ou iguais a *n*, com $n \geq 2$. Este nome é atribuído a Harvey Dubner e é a combinação da palavra “primo” e “fatorial”. Matematicamente, têm-se:

$$n\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n = \prod_{k=1}^{p_n} p_k \tag{2.7}$$

Exemplos:

$2\# = 2$
$3\# = 2 \cdot 3 = 6$
$4\# = 2 \cdot 3 = 6$
$5\# = 2 \cdot 3 \cdot 5 = 30$
$6\# = 2 \cdot 3 \cdot 5 = 30$
$7\# = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

Os primeiros 10 primos primoriais são:

n	1	2	3	4	5	6	7	8	9	10
n#	1	2	6	6	30	30	210	210	210	210

Tabela 2.2: Números Primoriais

2.1.8 Congruências

Carl Friedrich Gauss introduziu o conceito de congruência para denotar que um número inteiro *a* e um número inteiro *b* possuem o mesmo resto quando dividido por um número inteiro *m*, por perceber que as propriedades desta relação possuem certa similaridade com a igualdade.

Se *a* e *b* possuem o mesmo resto quando divididos por *m* (no qual *a*, *b* e *m* são inteiros com *m > 0*), então pode-se escrever [1]:

$$a \equiv b (\mathrm{mod}\, m) \tag{2.8}$$

(leia-se *a* é côngruo a *b* módulo *m*). Uma maneira equivalente é dizer que *m* é divisor de *b – a*. O número *m* é chamado módulo da relação de congruência.

Por exemplo, $5 \equiv 9 (\mathrm{mod}\, 4)$, já que 5 mod 4 = 1 = 9 mod 4.

Esta notação sugere que esta relação possui analogias a igualdade. E realmente, muitas propriedades da igualdade são válidas para a congruência, embora, é claro, mantendo o módulo fixo. As propriedades a seguir estão presentes tanto na igualdade como na congruência. Para todo número inteiro *a*, *b*, *c*, tem-se:

- reflexividade: $a \equiv a (\mathrm{mod}\, m)$;
- simetria: $a \equiv b (\mathrm{mod}\, m) \Rightarrow b \equiv a (\mathrm{mod}\, m)$;
- transitividade $a \equiv b (\mathrm{mod}\, m), b \equiv c (\mathrm{mod}\, m) \Rightarrow a \equiv c (\mathrm{mod}\, m)$;

É possível também computar congruências tais como simples equações. Supondo que existem duas congruências com o mesmo módulo:

$$a \equiv b (\mathrm{mod}\, m) \text{ e } c \equiv d (\mathrm{mod}\, m) \tag{2.9}$$

então é possível somar, subtrair e multiplicar essas congruências, tendo:

$$a + c \equiv b + d (\mathrm{mod}\, m), \quad a - c \equiv b - d (\mathrm{mod}\, m), \quad a \cdot c \equiv b \cdot d (\mathrm{mod}\, m) \tag{2.10}$$

Além disso, a multiplicação possui um caso especial que permite multiplicar ambos os termos da congruência por um mesmo número, ou seja, se $a \equiv b (\mathrm{mod}\, m) \rightarrow ak \equiv bk (\mathrm{mod}\, m)$ para qualquer inteiro k.

2.1.9 Pequeno Teorema de Fermat

Números primos têm sua importância devido ao fato de que a partir de sua composição é possível formar qualquer outro número inteiro, mas apesar disso, os números primos também possuem outras incríveis propriedades. Uma delas foi encontrada por Pierre de Fermat e, por isso, possui o mesmo nome do autor.

Teorema (Pequeno Teorema de Fermat) 2.7: se p é um primo e a é um inteiro, então $p \mid a^p - a$.(2.11)[1].

Outra forma equivalente para este teorema é: se p é um primo e a é um inteiro, então $p \mid a^{p-1} - 1$.

Muitos algoritmos de testes de primalidade se basearam neste teorema para aumentar a eficiência.

2.1.10 Algoritmo de Euclides

Muito já foi abordado sobre as noções e resultados a respeito dos números inteiros. Um aspecto que será explorado agora é como realizar testes computacionais baseados nestes resultados.

Para muitos resultados na teoria dos números, é necessário um algoritmo que calcule o máximo divisor comum entre dois números da maneira mais eficiente possível.

O máximo divisor comum entre dois números inteiros positivos pode ser facilmente encontrado usando a fatoração de números primos. Procuramos os fatores primos em comum, escolhemos aqueles de menor expoente e em seguida os multiplicamos. Apesar de fácil, este método é bastante ineficiente para grandes números inteiros. O algoritmo para calcular o *mdc* discutido aqui, é bastante eficiente e não precisa realizar a fatoração de seus membros. Este algoritmo, ainda hoje, é bastante importante para a muitos dos algoritmos que realizam computação com inteiros.

O algoritmo de Euclides é baseado em 2 fatos simples, que são se $a \mid b \rightarrow mdc(a,b) = a$ e $mdc(a,b) = mdc(a,b-a)$. (2.12)

Suponha que dados dois inteiros positivos *a* e *b*, deseja-se saber o máximo divisor comum entre eles. Então [1]:

1. Se *a* > *b*, troca-se *a* por *b*.
2. Se *a* > *0*, divida *b* por *a*, para pegar o resto *r*. Substitua *b* por *r* e volte para o passo 1.
3. Se a = 0, então retorne *b* e finalize.

Quando se aplica o algoritmo, principalmente de forma manual, não existe uma boa razão para mudar *a* por *b* se *a* < *b,* pode-se ao invés disto,

simplesmente dividir o maior número pelo menor e substituir o maior pelo resto, enquanto este não for igual a 0. Por exemplo:

mdc(200,14) = mdc(4,14) = mdc(4,2) = 2
mdc(99, 100) = mdc(99,1) = 1
mdc(89,55) = mdc(34,55) = mdc(34,21) = mdc(13,21) = mdc(13,8) = mdc(5,8) = mdc(5,3) = mdc(2,3) = mdc(2,1) = 1

Como se trata de um algoritmo, é necessário levar em consideração o fato dele terminar ou não. Neste caso, o algoritmo de Euclides é finito pelo fato de que os termos do mdc nunca aumentam, na verdade eles sempre diminuem, de acordo com o passo 2 do algoritmo, além disso o resto nunca é negativo, desta forma o procedimento nunca executa infinitamente.

O segundo passo é verificar também se o algoritmo realiza realmente o cálculo do máximo divisor comum. No passo 1 e no passo 3, trivialmente o algoritmo não altera o máximo divisor comum. Já no passo 2, o número retornado é realmente o máximo divisor comum dos dois termos, de acordo com: se $a \mid b \rightarrow mdc(a,b) = a$.

Uma terceira observação mais sutil, é verificar se o algoritmo é eficiente e rápido. Desde que um ou outro número diminui a cada iteração quando os passos 1 e 2 são executados, podemos afirmar que o algoritmo irá parar em menos de $a + b$ iterações. Desconsiderando-se o pior caso, que é a aproximação mais pessimista, a maioria dos exemplos mostra que o algoritmo termina muito rápido.

Os exemplos também sugerem que esta é uma questão bastante delicada, já que o algoritmo de Euclides pode ter vários tempos de execução diferentes, de acordo com os números testados em questão.

2.1.11 Tipos Especiais de Números Primos

Devido a sua natureza misteriosa, os números primos são extensivamente estudados pelos matemáticos. Alguns destes matemáticos, batizaram alguns dos principais tipos de números primos que serão abordados nesta seção.

2.1.11.1 Número Primo Primorial

Um número primo *p* é chamado de primorial quando este está na forma [8]:

$$p = n\# \pm 1 \tag{2.13}$$

para algum número *n*. Os primeiros primos primoriais são:

3, 5, 7, 29, 31, 211, 2309, 2311, 30029, 200560490131, 304250263527209, etc.

Até o momento da escrita deste documento, o maior primo primorial conhecido é o 392113# + 1 com 169966 dígitos, encontrado em 2001 por Daniel Heuer[5].

Os números de Euclides são um subconjunto dos números primos primoriais [8]:

$$E_n = n\# + 1 \tag{2.14}$$

Os primeiros primos de Euclides são:

3, 7, 31, 211, 2311, 30031, 510511, etc.

Não se sabe se existem infinitos números de Euclides.

$E_6 = 13\# + 1 = 30031 = 59 \cdot 509$ é o primeiro número de Euclides composto, demonstrando que nem todos os números de Euclides são primos.

Note que para todo $n \geq 3$, o último digito de E_n é 1, logo $E_n - 1$ é sempre divisível por 2 e 5.

2.1.11.2 Número Primo Fatorial

Um número primo *p* é chamado de fatorial se ele está na forma:

$$p = n! \pm 1 \tag{2.15}$$

para algum número *n*. Os primeiros primos fatoriais são:

n	1	2	3	3	4	6	7	11	12	14
p	2	3	5	7	23	719	5039	39916801	479001599	87178291199

Tabela 2.3: Números Primos Fatoriais

O maior número primo fatorial conhecido durante a escrita deste documento é 34790! – 1, encontrado por Marchal, Carmody e Kuosa em 2002.[6] Não existem provas da infinitude dos números primos fatoriais e primoriais.

2.1.11.3 Primos de Mersenne

Na teoria dos números, um número primo é um número primo de Mersenne se ele pode ser escrito na forma [7]:

$$M_n = 2^n - 1 \tag{2.16}$$

Até agosto de 2007, apenas 44 primos de Mersenne eram conhecidos. O maior número primo conhecido atualmente é um número de Mersenne ($2^{32.582.657} - 1$).

Não se sabe se existe o maior número primo de Mersenne, o que significaria que o conjunto de números primos de Mersenne seria finito, embora algumas conjecturas afirmem o contrário.

Um teorema básico sobre os números primos de Mersenne é que se M_n é um número primo, então o expoente *n* também deve ser um número primo. Embora isto seja verdade, existem casos em que M_n não é primo mesmo com o expoente *n* sendo primo. Por exemplo, o $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$, não é primo, mesmo o 11 sendo primo.

Os primos de Mersenne foram observados primeiramente por Euclides, mas apenas no século XVII, o estudante francês Marin Mersenne compilou uma lista dos primos de Mersenne com expoentes até 257. Mersenne não indicou como ele criou a lista, e uma verificação rigorosa só foi completada mais de dois séculos depois. Foi constatado que apenas alguns elementos da lista estavam errados.

Portanto, os primeiros primos de Mersenne são:

n	2	3	5	7	13	17	19	31	61
M_n	3	7	31	127	8191	131071	524287	2147483647	2305843009213693951

Tabela 2.4: Números Primos de Mersenne

2.1.11.4 Primos de Fermat

Os números de Fermat são números da forma [7]:

$$F_n = 2^{2^n} + 1 \tag{2.17}$$

no qual n é um inteiro não negativo. Os números primos de Fermat são números de Fermat que também são primos. Os únicos números primos de Fermat conhecidos são [8]:

3, 5, 17, 257, 65537

Assim, não se sabe se existe algum primo de Fermat F_n para $n > 4$. Na verdade pouco se sabe sobre números de Fermat com um *n* muito grande. Não se sabe se existem infinito números primos de Fermat, ou se todo número de Fermat é composto para todo $n > 4$.

Até o ano de 2007, apenas os 12 primeiros números de Fermat tinham sido completamente fatorados. É também conhecido que os números de Fermat são compostos no intervalo $5 \le n \le 32$. O maior número de Fermat conhecido como composto é $F_{2478782}$.

Por causa do tamanho dos números de Fermat, é difícil fatorar ou provar a primalidade deles. Portanto, alguns testes de primalidade mais otimizados, como o teste de Pepin[8], devem ser utilizados para obter uma resposta em menor tempo.

2.1.11.5 Primo de Smarandache-Wellin

O número de Smarandache-Wellin é um inteiro formado pela concatenação dos *n* primeiros números primos. Os primeiros números de Smarandache-Wellin são [9]:

2, 23, 235, 2357, 235711, etc.

Quando um número de Smarandache-Wellin é também um número primo, ele é chamado de primo de Smarandache-Wellin. Os índices dos primeiros primos de Smarandache-Wellin na base decimal são:

1, 2, 4, 128, 174, 342, 435.

2.1.11.6 Primos Truncáveis

Um primo truncável, é um número que não contém nenhum zero e se um dígito de uma das pontas for retirado sucessivamente o número resultante também deve ser primo, por exemplo, 1223 é um primo truncável à esquerda, pois, 223, 23, e 3 são todos primos, outro exemplo seria 3739, que é um primo truncável a direita, pois, 373, 37 e 3 são todos primos.

Existem 4260 primos truncáveis a esquerda na base decimal. Os primeiros são:

2, 3, 5, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 113, 137, 167, 173, etc.

O maior primo truncável a esquerda tem 24 dígitos: 357686312646216567629137.

Existem 83 primos truncáveis a direita. Os primeiros são:

2, 3, 5, 7, 23, 29, 31, 37, 53, 59, 71, 73, 79, 233, 239, 293, 311, 313, 317, etc.

O maior primo truncável a direita tem 8 dígitos: 73939133. Todos os primos acima de 5 terminam com o dígito 1, 3, 7 ou 9, então os primos truncáveis a direita só podem conter estes dígitos na sua ponta direita.

Existem também os primos truncáveis de dois lados, no qual um dígito pode ser retirado tanto da esquerda quanto da direita e o resultado continua sendo primo. A lista completa com esses números será mostrada a seguir:

2, 3, 5, 7, 23, 37, 53, 73, 313, 317, 373, 797, 3137, 3797, 739397

2.1.11.7 Primos de Fibonacci

Os números de Fibonacci são uma seqüência de números que obedecem a seguinte função recorrente [11]:

$$F(n) = \begin{cases} 0, \text{ se n = 0;} \\ 1, \text{ se n = 1;} \\ F(n-1) + F(n-2), \text{ se n > 1.} \end{cases} \qquad (2.18)$$

Assim, depois dos dois primeiros valores, cada número é a soma dos dois números anteriores. Os primeiro números de Fibonacci são:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F(n)	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

Tabela 2.5: Números de Fibonacci

Um número primo de Fibonacci é um número primo que faz parte da seqüência de Fibonacci. Os primeiros 10 números primos de Fibonacci são:

2, 3, 5, 13, 89, 233, 1597, 28657, 514229, 433494437.

2.2 PALÍNDROMOS

Um palíndromo é uma palavra, frase, ou qualquer outra seqüência de unidades (como uma cadeia de DNA) que tem a propriedade de ser lida de ambas as direções da mesma forma. Nos palíndromos, geralmente são desconsiderados os sinais ortográficos, bem como o espaço entre as palavras. Provavelmente, o palíndromo mais famoso na língua portuguesa é “Socorram-me, subi no ônibus em Marrocos" de autoria anônima. Porém, este palíndromo só pode ser lido corretamente quando os espaços são desconsiderados. A palavra **a** e **e** são as palavras mais simples e por isso os palíndromos menos interessantes, a palavra anilina e o nome Natan são mais interessantes e ilustrativos. A palavra "palíndromo" vem das palavras gregas palin ("trás") e dromos ("corrida").

Rômulo Marinho, um político brasileiro e veterano palindromista, propôs uma classificação dos palíndromos em 3 classes [12]:

- Expliciti - exibe uma mensagem clara, fácil e direta, como "Socorram-me, subi no ônibus em Marrocos”.

- Interpretabiles – é coerente, o leitor precisa exercer esforço intelectual para entender, como "A Rita, sobre vovô, verbos atira."

- Insensati – o único objetivo é formar o palíndromo, sem se preocupar com o sentido, como "Olé! Maracujá, caju, caramelo."

As frases formando um palíndromo também são chamadas de anacíclicas, do grego anakúklein, significando que volta em sentido inverso, que refaz inversamente o ciclo.

Escrever literatura em palíndromos é um exemplo de escrita constrangida - uma técnica literária no qual o escritor não possui total liberdade para criar a sua obra - a escrita precisa seguir algum padrão.

Existem vários tipos de palíndromos, dentre eles alguns serão citados a seguir:

2.2.1 Caractéres

O tipo de palíndromo mais comum são os lidos caractér-a-caractér: os caracteres podem ser lidos de ambas as direções. Palíndromos podem consistir de uma única palavra (asa, osso, reter), ou uma frase ou sentença (“A base do teto desaba”, "E até o Papa poeta é.”) [12]. Espaços, pontuação e acentos são normalmente ignorados.

Algumas pessoas também têm seus nomes como palíndromos, como por exemplo, Natan e Renner.

2.2.2 Palavras

Alguns palíndromos usam palavras como unidades ao invés de letras. Exemplos são “Avesso do Avesso”, “Primeiro-Ministro regrou: ministro primeiro!”. O palíndromo “Seres matam seres” é composto apenas por palavras que também são palíndromos, e por isso é palíndromo caracter-a-caracter e palavra-a-palavra.

2.2.3 Linhas

Existem também outros palíndromos que usam linhas como unidades. O poema Doppelganger, escrito por James A. Lindon, é um exemplo, e será exibido abaixo:

Entering the lonely house with my wife
I saw him for the first time
Peering furtively from behind a bush --
Blackness that moved,
A shape amid the shadows,
A momentary glimpse of gleaming eyes
Revealed in the ragged moon.
A closer look (he seemed to turn) might have
Put him to flight forever --
I dared not
(For reasons that I failed to understand),
Though I knew I should act at once.

I puzzled over it, hiding alone,
Watching the woman as she neared the gate.
He came, and I saw him crouching
Night after night.
Night after night
He came, and I saw him crouching,
Watching the woman as she neared the gate.

I puzzled over it, hiding alone --
Though I knew I should act at once,
For reasons that I failed to understand
I dared not
Put him to flight forever.

A closer look (he seemed to turn) might have
Revealed in the ragged moon.
A momentary glimpse of gleaming eyes
A shape amid the shadows,
Blackness that moved.
Peering furtively from behind a bush,
I saw him for the first time,
Entering the lonely house with my wife. [15]

2.2.4 Lista de Números Palindrômicos

Os números palindrômicos são números, com representação decimal geralmente assumida, que quando é lido de direita para esquerda resulta no mesmo número lido da esquerda para direita, por exemplo, 58685. Os primeiros 30 números palindrômicos na base decimal são:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 22, 33, 44, 55, 66, 77, 88, 99, 101, 111, 121, 131, 141, 151, 161, 171, 181, 191, 202.

Como exemplo pode-se citar:

- Um primo palindrômico é um número que é palindrômico e primo ao mesmo tempo. Os primeiros 20 números primos palindrômicos são: 2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929.

- Um número quadrático palindrômico é um número que é quadrático e palíndromo ao mesmo tempo. Os primeiros 10 números primos quadráticos palindrômicos são[17]: 0, 1, 4, 9, 121, 484, 676, 10201, 12321, 14641.

Sabe-se que em qualquer que seja a base, existe um número infinito de números palindrômicos, desde que em cada base seja possível escrever uma quantidade infinita de números.

A palavra **capicúa**, “cap” que significa cabeça e “cúa” que significa cauda[17], de origem catalã, explica os números palindrômicos (matemática) ou palíndromo, para palavras, frase e outros.

2.2.5 Definição Formal

Embora a maioria dos números palindrômicos conhecidos sejam aqueles no sistema decimal, o conceito dos palíndromos pode ser aplicado aos números naturais em qualquer sistema numérico. Considere um número *n > 0* na base $b \geq 2$, no qual ele é escrito na notação padrão com *k + 1* dígitos a_i, assim [17]:

$$n = \sum_{i=0}^{k} a_i b^i$$

com $0 \leq a_i < b$ para todo *i* e $a_k \neq 0$. Então n é um número palindrômico, se e somente se, $a_i = a_{k-i}$ para todo *i*. Zero é escrito 0 em qualquer base e por definição também é um número palindrômico.

Uma definição alternativa, mas equivalente é mostrada a seguir. Em uma base arbitrária, mas fixa *b,* um número *n* é palindrômico se e somente se:

- *n* consiste de um único dígito, ou
- *n* consiste de dois dígitos iguais, ou
- *n* consiste de três ou mais dígitos, onde o primeiro e o último dígito são iguais e o número obtido retirando-se o primeiro e o último dígito continua sendo um palíndromo.

Números não palindrômicos podem gerar um número palindrômico através de uma série de operações. Primeiro, o número não palindrômico é revertido e o resultado é adicionado ao número original. Se o resultado não for um palíndromo o processo se repete até que um palíndromo seja encontrado. Por exemplo, 56 + 65 = 121, 125 + 521 = 646.

Mas não é garantido que todos os números não palindrômicos irão gerar um palíndromo desta maneira. Embora isto não seja provado, muitos números não conseguem gerar um palíndromo desta maneira. Por exemplo, o número 196 não consegue gerar um palíndromo mesmo depois de 700.000.000 de iterações. Qualquer número que nunca gerar um palíndromo desta maneira é chamado de números de Lychrel[18].

2.2.6 Data e Hora

Datas palindrômicas despertam interesses em matemáticos amadores e numerólogos, e algumas vezes geram comentários na mídia. Se uma data é palindrômica ou não, depende da forma como ela é escrita. Por exemplo, na forma dd/mm/aaaa, o último palíndromo foi no dia 20 de fevereiro de 2002 (20/02/2002) e o próximo será em 01 de fevereiro de 2010 (01/02/2010). Alguns ainda consideram a hora, no formato hh:mm dd/mm/aaaa, então às 20 horas e 02 minutos do dia 21 de dezembro de 2002 (20:02 21/12/2002) foi a última data palindrômica.

2.2.7 Música e Acústica

Algumas letras de músicas possuem palíndromos na sua composição, outras ainda possuem palíndromos em sua melodia.

A sinfonia número 47 de Joseph Haydn foi apelidada de "*Palindrome*"**.** O terceiro movimento, o minueto e o trio é um palíndromo musical. Algumas partes avançam duas vezes, depois retrocedem duas vezes e em seguida voltam ao mesmo lugar.

Um palíndromo no qual a fonética de uma frase é a mesma quando tocada de trás pra frente foi descoberta por John Oswald em 1974 enquanto ele trabalhava manipulando fitas cassete.

2.2.8 Programas de Computador

Brian Westley escreveu um programa na linguagem de programação C em 1987 para o Concurso Internacional de código C Ofuscado que é um palíndromo linha a linha.[19] O código será exibido a seguir:

```
char rahc
[ ]
=
"\n/"
,
redivider
[ ]
=
"Able was I ere I saw elbA"
,
*
deliver,reviled
=
1+1
,
niam ; main
```

```
( )
{/*\}
\*/
int tni
=
0x0
,
rahctup,putchar
( )
,LACEDx0 = 0xDECAL,
rof ; for
(;(int) (tni);)
(int) (tni)
= reviled ; deliver =
redivider
;
for ((int)(tni)++,++reviled;reviled* *deliver;deliver++,++(int)(tni)) rof
=
(int) -1- (tni)
;reviled--;--deliver;
(tni)  =  (int)
- 0xDECAL + LACEDx0 -
rof ; for
(reviled--,(int)--(tni);(int) (tni);(int)--(tni),--deliver)
rahctup = putchar
(reviled* *deliver)
;
rahctup * putchar
((char) * (rahc))
;
/*\
{\*/}
```

2.2.9 Estruturas Biológicas

Na maioria dos genomas ou conjuntos de instruções genéticas, vários palíndromos são encontrados. Entretanto, o significado de palíndromo no contexto da genética é um pouco diferente da definição usada para palavras e sentenças. Desde que o DNA é formado por dois pares de nucleotídeos, e estes sempre formam pares da mesma maneira ((A)denina com (T)iamina e (C)itosina com (G)uanina), uma seqüência de DNA é dita palíndromo se ela for igual a sua leitura complementar lida de trás pra frente. Por exemplo, a seqüência ACCTAGGT é palindrômica porque o seu complemento é TGGATCCA, que é igual a seqüência original reversa.

2.2.10 Semi-Palíndromos

Semi-palíndromos é uma palavra ou frase que remete a uma outra palavra ou frase diferente quando lida de trás pra frente. Estas palavras, geralmente são muito usadas na construção de palíndromos, pois juntas elas formam um palíndromo, e também podem ser adicionadas aos extremos de outros palíndromos para serem prolongados. Exemplo: missa/assim.

Um emirp é um primo que se torna um primo diferente quando os dígitos decimais são lidos de trás pra frente.

2.2.11 Exemplos

2.2.11.1 Palavras

Existem algumas palavras que são naturalmente palíndromos, no português tem-se:

- aba, acaiaca, Ada, ala, ama, amarram-a, Ana, anilina, ara, arara, asa, assa, ata, esse, iriri, mamam, matam, mapam, melem, metem, mexem, mirim, mutum, mussum, Natan, oco, omo, osso, oto, ovo, racificar, radar, ralar, ramar, rapar, rasar, ratar, reler, Renner, reter, rever, reviver, rir, rotor, sacas, salas, seres, siris, saras, socos, sapas, solos, soros, seles, somavamos, somos, sugus, supus.

Existem também várias palavras semi-palindromos, por exemplo:

- avaro/orava. auge/egua. Edna/ande. apartas/satrapa. Raul/luar. amar/rama. roma/amor. ator/rota. servil/livres. Messias/saissem. missa/assim. atlas/salta. Ari/ira. Eva/ave. Avó/ova. Sapos/Sopas. sacos/socas. será/ares.

2.2.11.2 Frases

Diz-se que uma frase é um palíndromo com simetria total, quando se considera os espaços entre as palavras. Alguns exemplos são citados a seguir:

- “Ame a ema.”
- “Assim a aluna anula a missa.”
- “Morram após a sopa marrom.”
- “Eva, asse essa ave.”

Um palíndromo de simetria parcial não considera os espaços entre as palavras. Por exemplo:

- “A base do teto desaba.” [14]
- "Anotaram a data da maratona."
- “Acata o danado... e o danado ataca!”
- “A miss é péssima!”

- “A mala nada na lama.” [20]

2.2.11.3 Poemas

Palíndromo do amor total [14]

Ávido?
Amá-la na taba, no toco da casa,
Ama?
no muro, no paço, na poça,
na maca, na livre sala,
servi-la na cama,
na copa, no capô, no rumo,
na saca do coto, na bata, na lama...
Ó diva!

Haikai (Beto Furquim)

Aroma.
Me supus em
amora.

2.3 TESTES DE PRIMALIDADE

Os testes de primalidade são algoritmos que basicamente recebem como entrada um número e verificam se esse número é primo ou não. Eles possuem uma grande importância na teoria dos números e também possui muitas aplicações associadas à criptografia, pois é essencial que estes algoritmos realizem testes de maneira muito eficiente para números bastante

grandes, ou o processo de criptografia seria muito demorado e, portanto inviável.

Existem também algoritmos de fatoração de números inteiros, que recebem como entrada um número e, cuja resulta em pelo menos um dos fatores deste número. Os testes de primalidade são computacionalmente mais fáceis quando comparados a algoritmos de fatoração.

A teoria da complexidade algorítmica é um ramo da matemática que estuda e classifica problemas de acordo com o grau de dificuldade em ser resolvido. Existem várias classes de problemas, os principais são [26]:

- **NP**, no qual “NP” significa que problema não é determinístico em tempo Polinomial, ou seja, ele permite uma solução não determinística, e o número de passos para que o algoritmo encontre a resposta é limitado por uma potência da ordem do tamanho do problema.

- **Co-NP**, significa um complemento da classe *NP*, ou seja, quando um problema não está na classe *NP*, então ele está na classe *Co-NP*.

- **P**, no qual o “P” significa problema de “tempo Polinomial”. Isto quer dizer que o número de passos para que o algoritmo encontre a resposta é limitado por uma potência da ordem do tamanho do problema. Esta classe de problemas está localizada entre as classes *NP* e *Co-NP*.

Até 2002, todos os testes de primalidade estavam entre as classes *NP* e *Co-NP*, ou seja, podiam até ser algoritmos eficientes, mas não executavam em tempo polinomial para determinadas entradas. Então surgiu o teste de primalidade AKS, que provou que os testes de primalidade também são da classe *P*, enquanto que os testes de fatoração ainda podem ou não fazer parte desta classe.

Existem vários tipos de testes de primalidade, que variam de algoritmos bastante simples até algoritmos com heurísticas bastante elaboradas, embora todos sejam baseados em características próprias dos números primos. Além disso os testes de primalidade podem ser classificados em vários critérios, dentre eles:

Tipo de número	Testes para números de forma particular
	Testes para números genéricos
Justificativa	Testes justificados completamente por teoremas
	Testes cuja justificativa é baseada em conjecturas
Certeza	Testes Determinísticos
	Testes Probabilísticos (ou de Monte Carlo)

Tabela 2.6: Classificação dos Testes de Primalidade

Alguns destes algoritmos serão abordados logo em seguida, e suas principais características serão descritas.

2.3.1 Testes Determinísticos

Os testes determinísticos são testes de primalidade que garantem que o resultado produzido sempre estará correto e, considerando-se uma entrada em particular, ele sempre irá produzir a mesma saída e sempre irá passar pela mesma seqüência de estados.

Os testes de primalidade determinísticos geralmente cobram um preço caro por sempre produzirem a resposta correta. Nenhum deles é mais rápido que alguns testes probabilísticos. Os primeiros algoritmos de testes de primalidade, como o crivo de Eratóstenes e o método da força bruta, eram determinísticos porém bastante lentos e ineficientes.

O teste ciclotômico foi o primeiro teste de primalidade determinístico que foi significativamente mais rápido que os testes de força bruta e o crivo de Eratóstenes. Embora este teste seja determinístico e não se baseie em nenhuma hipótese, a sua complexidade de tempo de execução é não-polinomial. Seu tempo de execução foi provado como $O((\log n)^{c \log\log\log n})$, no qual n é o número a ser testado, e c uma constante independente de n [36].

O teste da curva elíptica roda em tempo polinomial $O((\log n)^6)$, porém se fundamenta em uma conjectura (embora amplamente acreditada como verdadeira) sobre a teoria dos números analítica. Este algoritmo é um dos mais utilizados para testes determinísticos na prática.

A implementação dos algoritmos do teste ciclotômico e do teste da curva elíptica são bastante complexos e muito susceptíveis a erros e, portanto é preferível não utilizá-los.

O teste de primalidade de Miller-Rabin pode se tornar uma versão determinística com algumas adaptações ao se adotar a hipótese de Riemann como verdadeira. Na prática este algoritmo é geralmente mais lento que os testes ciclotômico e da curva elíptica.

Apenas em 2002 surge o teste de primalidade AKS, que é um algoritmo que roda em tempo polinomial, é determinístico e não depende de nenhuma hipótese. A origem do nome deste teste vem de seus criadores: Manindra Agrawal, Neeraj Kayal e Nitin Saxena. Eles provaram que o algoritmo funcionaria em tempo polinomial de $\tilde{O}((\log n)^{12})$, embora na prática este algoritmo seja ainda muito mais lento que testes probabilísticos.

2.3.1.1 Crivo de Eratóstenes

O crivo de Eratóstenes foi criado pelo antigo matemático grego Eratóstenes que deu origem ao seu nome. É um algoritmo simples e permite encontrar todos os primos possíveis até um determinado inteiro positivo. Ele surgiu antes do Crivo de Atkins que é mais rápido, porém mais complexo. Como se trata de um teste de primalidade, então ele é baseado numa característica simples de todo número primo.

Supondo *n* o número que se deseja verificar a primalidade, o algoritmo funciona da seguinte forma [35]:

1. Verifica-se o maior valor a ser testado. Este valor corresponde a raiz quadrada de *n*, arredondado pra baixo.
2. Cria-se uma lista com os valores inteiros de 2 até *n*.
3. Encontra-se o primeiro elemento da lista, o número primo 2.
4. Removem-se da lista todos os múltiplos de 2 encontrados.
5. O próximo número da lista é primo.
6. Todos os números múltiplos desse número devem ser removidos da lista.
7. Os passos 5 e 6 são repetidos até que o próximo item da lista seja o maior valor a ser testado ($\sqrt{n}$). Se o número *n* ainda estiver na lista ele é primo, caso contrário composto.

Este algoritmo é eficiente e muito lento, já que requer uma grande quantidade de passos para que o problema seja resolvido, embora possua algumas características desejáveis:

- Funcionar para qualquer número
- Ser justificado pela própria definição de números primos
- Ser determinístico

Este algoritmo é inviável para teste de números muito grandes.

2.3.1.2 Método da Força Bruta

Este teste de primalidade é um dos mais simples de todos. Considerando-se um dado número *n*, o algoritmo verifica se existe algum inteiro *q* no intervalo de 2 até *n-1*, que divide *n*. Se *n* for divisível por qualquer *q*, então *n* é um número composto, senão, é primo.

Mas este método pode ser melhorado um pouco mais. Por exemplo, o número *n* só precisa ser testado de 2 até $\sqrt{n}$, pois se *n* for composto ele pode ser fatorado em dois valores, e pelo menos um deles deve ser menor ou igual a $\sqrt{n}$. Pode-se também melhorar a eficiência, se pularmos todo *m* par exceto o número 2, já que se algum *m* par dividisse *n*, então 2 também dividiria.

Uma maneira de acelerar este teste de primalidade ainda mais (inclusive todos os outros testes que serão mencionados a seguir), é pré-calcular e colocar numa lista todos os números primos até um certo valor, por exemplo, todos os primos até 500. Então antes de realizar um teste de primalidade sobre um número *n* com qualquer método, primeiro deve-se verificar se o número *n* é divisível por qualquer número da lista.

Assim como o método do Crivo de Eratóstenes, este teste é determinístico, funciona pra qualquer número e também é justificado pela própria definição de números primos. Apesar disto, também é bastante lento, já que é necessária a repetição dos passos muitas vezes para se obter o resultado. Portanto o uso deste algoritmo para calcular a primalidade de números grandes não é incentivado.

2.3.1.3 Teste de Primalidade AKS

O teste de Primalidade AKS é um algoritmo de teste de primalidade determinístico, criado por cientistas da computação do Instituto Indiano de Tecnologia de Kanpur, Manindra Agrawal, Neeraj Kayal, e Nitin Saxena em Agosto de 2002 no artigo entitulado PRIMES is in P. Os autores receberam muitos prêmios incluíndo o Prêmio Gödel e Fulkerson em 2006 por este trabalho [38].

Este teste de primalidade, verifica se um número qualquer é primo ou composto em tempo polinomial $O((\log n)^{12})$, além de ser justificado matematicamente, daí a importância deste trabalho. Em 2005, Carl Pomerance e H. W. Lenstra Jr demonstraram uma variante deste algoritmo que roda em $O(\log^6 n)$ passos, no qual n é o número a ser testado, representando uma significativa melhora em relação ao algoritmo original.

O teste é baseado numa generalização do Pequeno Teorema de Fermat. Considerando a um inteiro, e n um número inteiro positivo maior ou igual a 2, no qual a e n são primos entre si, então n é primo se e somente se [23]:

$$(X + a)^n = X^n + a \,(\mathrm{mod}\, n) \tag{2.19}$$

Para uma entrada $n > 1$. O algoritmo será mostrado a seguir:

1. Se ($n = a^b$ para qualquer a inteiro positivo e $b > 1$), então retorne COMPOSTO.
2. Encontre o menor r no qual $o_r(n) > \log^2 n$.
3. Se $1 < (a,n) < n$ para algum $a < r$, então retorne COMPOSTO.
4. Se $n \leq r$, então retorne PRIMO.

5. Para a = 1 até $\left\lfloor \sqrt{\phi(r)} \log n \right\rfloor$ faça: se $((X+a)^n \neq X^n + a \,(\mathrm{mod}\, X^r - 1, n))$ então retorne COMPOSTO.
6. Retorne PRIMO.

2.3.1.4 Teste de Primalidade de Lucas-Lehmer

O teste de primalidade de Lucas-Lehmer que foi criado por Edouard Lucas e Derrick Henry Lehmer é determinístico e justificado a partir de teoremas. Dado um número n, este algoritmo requer que os fatores do número n-1 sejam conhecidos. Sendo assim, ele não se torna muito útil para verificar a primalidade de números de propósito geral. Seu uso é mais adequado para números especiais como os de Mersenne.

O algoritmo de Lucas-Lehmer funciona da seguinte maneira:

- Se para qualquer *a* entre os fatores primos de *n – 1,* e para todo *q* fator de *n – 1*, as condições $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ *e* $a^{\frac{n-1}{q}} \bmod n \neq 1$ forem verdadeiras, então *n* é primo, senão é composto.

2.3.2 Testes Probabilísticos

Os testes de primalidade mais populares são os testes probabilísticos. Estes testes são baseados em números escolhidos de forma aleatória (*a*) num dado espaço amostral, sem nenhuma relação com o número a ser testado (*n*). A maioria deles nunca retorna um número primo como composto, mas pode retornar um número composto como primo. A chance de erro pode ser reduzida ao se repetir o teste várias vezes, sempre alterando o valor de *a* aleatoriamente.

Considerando-se dois testes comumente utilizados, para qualquer número composto *n*, ele tem metade da chance de detectar que n é composto. Ao se repetir o teste *k* vezes, a chance de erro cai para 2^{-k}, que pode ser cada vez menor ao se aumentar ainda mais o valor de k.

A estrutura básica dos testes de primalidade probabilísticos é a seguinte [36]:

- Escolhe-se um número aleatório *a*.
- Realiza-se uma comparação de igualdade entre *a* e um dado número *n*. Se a igualdade não for verdadeira, então *n* será um número composto e *a* será conhecido como *testemunha* da composição e o teste acaba.
- Este procedimento se repete desde o primeiro passo até que algum grau de certeza seja alcançado.

Se depois de algumas interações, *n* não foi considerado um número composto, então ele pode ser declarado primo provável.

O teste probabilístico mais simples é o teste de primalidade de Fermat. É apenas um teste Heurístico. Alguns números compostos, como os números de Carmichael, serão declarados como primos prováveis, não importando qual seja a testemunha escolhida [36].

Os testes de primalidade de Miller-Rabin e o teste de Solovay-Strassen são mais complexos e conseguem detectar todos os números compostos, e devido a sua alta velocidade na resposta, eles são os mais usados geralmente. O teste de Frobenius apresenta uma confiabilidade maior, mas não é muito usado, pois ele é cerca de três vezes mais demorado que os dois anteriores.

2.3.2.1 Teste de Primalidade de Fermat

Como já foi abordado anteriormente, o pequeno teorema de Fermat afirma que se p é primo e $1 \leq a \leq p$, então $p \mid a^{p-1} - 1$, ou ainda, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

O teste de primalidade de Fermat consiste em simplesmente se escolher alguns valores aleatórios para *a* no intervalo considerado e verificar se esta congruência permanece verdadeira para todos os valores de *a*. Se esta congruência permanecer verdadeira então p é um primo provável. Se alguma destas congruências falharem para algum valor de *a,* então certamente *p* é composto.

Como se trata de um algoritmo probabilístico, o resultado obtido algumas vezes pode ser inesperado. Existem números que independente do valor de a, irão sempre retornar primos, apesar dos números serem compostos. Este tipo de número é chamado de número de Carmichael, e embora sejam raros, eles são suficientes para que o teste de primalidade de Fermat não seja tão utilizado quanto os testes de Miller-Rabin e Solovay-Strassen.

2.3.2.2 Teste de Primalidade Probabilidade de Miller-Rabin

Este teste de primalidade na realidade pode se comportar de duas maneiras, uma versão determinística baseada na hipótese de Riemman (que ainda não foi provada), e outra versão incondicional e probabilística. Para o escopo deste trabalho apenas a versão probabilística será abordada.

Assim como o teste de Fermat, o teste de Miller-Rabin é baseado em uma congruência, que será verdadeira para números primos ou falsa quando o número não for primo.

Para uma entrada $n > 1$ ímpar, com índice de certeza k. O algoritmo funciona da seguinte maneira [38]:

- Decomponha o n - 1, que é par, numa potência de 2. O número deverá ficar da forma: $2^s \cdot d$

- Repita k vezes:
  - Escolha um número aleatório a, no qual $1 \leq a \leq n-1$.
  - Se $a^d \not\equiv 1 \pmod{n}$ e $a^{2^r d} \not\equiv -1 \pmod{n}$, para todo r, no qual $1 \leq r \leq s-1$, então retorne composto.
- Retorne primo provável.

Como se trata de um teste probabilístico, ele pode retornar resultados não muito confiáveis. Como ¾ dos números de valores de a servem como testemunhas de composição de n, então o algoritmo tem 75% de chance de acertar o resultado na primeira iteração. A medida que vai aumentando o número de iterações para um mesmo número a chance de acertar aumenta. Vale ressaltar que o teste de primalidade de Miller-Rabin funciona para qualquer tipo de número e esta versão probabilística não é condicionada a nenhuma hipótese.

3 RESULTADOS TEÓRICOS

Baseando-se na análise do comportamento dos números primos palindrômicos e suas generalizações, alguns resultados teóricos foram obtidos, acarretando numa diminuição no tempo computacional para calcular a primalidade destes números, já que alguns destes números poderiam ser descartados sem a necessidade de se calcular a primalidade, que é um processo bastante demorado para números muito grandes. Nesta seção, será explicado como os resultados foram obtidos e as idéias que foram utilizadas para aperfeiçoar os testes computacionais. Além disto, serão abordadas algumas generalizações e uma restrição dos números primos palindrômicos.

3.1 NÚMEROS PRIMOS PALINDRÔMICOS COMPOSTOS POR UM ÚNICO DÍGITO

Existe um tipo especial de número palindrômico que é formado por apenas um único dígito. Considerando D o conjunto dos dígitos, ou seja, $D = \{0,1,2,\cdots,9\}$ e k o número de dígitos que formam o palíndromo, têm-se:

$$D^{[k]} = \underbrace{D \cdots D}_{k}$$

Considerando isto como uma cadeia de caracteres, então:

$$D^{[1]} = D$$
$$D^{[k+1]} = D^{[k]}D$$

Se o palíndromo for considerado um número, então matematicamente:

$$\#D^{[1]} = D$$
$$\#D^{[k+1]} = \#D^{[k]} \cdot 10 + D$$

Por exemplo, considerando D = 2, os primeiros 4 palíndromos são:

$$2^{[1]} = 2$$
$$2^{[2]} = 2^{[1]}2 = 22$$
$$2^{[3]} = 2^{[2]}2 = 222$$
$$2^{[4]} = 2^{[3]}2 = 2222$$
ou
$$\#2^{[1]} = 2$$
$$\#2^{[2]} = \#2^{[1+1]} = \#2^{[1]} \cdot 10 + 2 = 2 \cdot 10 + 2 = 22$$
$$\#2^{[3]} = \#2^{[2+1]} = \#2^{[2]} \cdot 10 + 2 = 22 \cdot 10 + 2 = 222$$
$$\#2^{[4]} = \#2^{[3+1]} = \#2^{[3]} \cdot 10 + 2 = 222 \cdot 10 + 2 = 2222$$

Para que se obtenha um número primo palindrômico de um único dígito, esse dígito só pode ser o “1”, pois caso contrário, o palíndromo seria divisível pelo próprio dígito, e portanto, não poderia ser primo. Por exemplo:

$$3333 = 3 \cdot 1111$$
$$55555 = 5 \cdot 11111$$
$$777777 = 7 \cdot 111111$$
$$9999999 = 9 \cdot 1111111$$

Assim, os únicos primos palindrômicos de um único dígito, são os formados pelo dígito 1.

Outra observação feita através da análise de resultados obtidos computacionalmente sobre os números primos palindrômicos de um único dígito, é que a quantidade de dígitos deve ser um número primo. E isto deu origem ao seguinte teorema:

Teorema 3.1: Se $\#1^{[k]}$ é primo então *k* é primo

Prova: Esta prova será realizada utilizando o princípio da contraposição, então para isso, precisa-se provar que se *k* não é primo, então $\#1^{[k]}$ não pode ser primo.

Através da equação abaixo, está provado que independente de seu valor, se *k* não é primo então $\#1^{[k]}$ não pode ser primo.

$$\begin{aligned} &k = M \cdot N \\ &\#1^{[k]} = \#1^{[M \cdot N]} = \#1^{[M]} \cdot (\#(10^{[M-1]})^{[N-1]} \cdot 10 + 1) \end{aligned} \tag{3.1}$$

Para exemplificar então suponha que *k* não seja primo, dessa forma existem duas possibilidades:

Caso *k* seja par então ele é divisível por 2 e portanto pode-se assumir que *M=2*, assim sendo:

$$\begin{aligned} &k = 2 \cdot N \\ &\#1^{[k]} = \#1^{[2 \cdot N]} = \#1^{[2]} \cdot (\#(10^{[2-1]})^{[N-1]} \cdot 10 + 1) \end{aligned}$$

Por exemplo:

$$\#1^{[10]} = \#1^{[2]} \cdot (\#(10^{[2-1]})^{[5-1]} \cdot 10 + 1) = 11 \cdot 101010101 = 1111111111$$

Portanto, para k sendo par, então $\#1^{[k]}$ não pode ser primo.

Caso k seja ímpar e não primo, então $k = M \cdot N$ para algum número ímpar *M>2* e algum número ímpar *N>2* e a partir disso tem-se como exemplo:

$$\#1^{[21]} = \#1^{[3\cdot 7]} = \#1^{[3]}.(\#(10^{[3-1]})^{[7-1]} \cdot 10 + 1)$$
$$= 111 \cdot (\#(100)^{[6]} \cdot 10 + 1) = 111 \cdot (100100100100100100 \cdot 10 + 1)$$
$$= 111 \cdot 1001001001001001001 = 11111111111111111111$$

Portanto, para k sendo ímpar e não primo, $\#1^{[k]}$ não pode ser primo.

Assim está provado por contraposição, que se $\#1^{[k]}$ for primo então k será necessariamente um primo.

Os números construídos apenas utilizando o dígito “1”, chamados de **repunits** (que significa **rep**eated **units**), já foram estudados previamente por outros matemáticos. Um desses estudos resultou em um teorema que diz que, caso um **repunit** seja primo, então é necessário que a quantidade de dígitos desse **repunit** seja um primo. Apesar disto, esta nova prova introduzida neste trabalho possui sua importância devido a sua simplicidade em relação as outras.

3.2 NÚMEROS PRIMOS PALINDRÔMICOS GENÉRICOS

Considere uma função $\varphi : D \to D$ bijetiva, no qual $D = \{0,1,\cdots,9\}$, e também as variáveis *a, b, c, d, e, f, g, h, i, j*, como qualquer elemento do conjunto *D* (que não se repetem), dessa maneira, têm-se:

$$\varphi(a) = j, \varphi(b) = i, \varphi(c) = h, \varphi(d) = g, \varphi(e) = f,$$
$$\varphi(f) = e, \varphi(g) = d, \varphi(h) = c, \varphi(i) = b, \varphi(j) = a$$

Uma seqüência de dígitos $d_0 d_1 \ldots d_n$ é um palíndromo modulo φ, se $n \geq 0$ e $d_i = \varphi(d_{n-i})$, $\forall i \in \left\{0,\ldots,\left\lfloor \frac{n-1}{2} \right\rfloor, \left\lceil \frac{n+1}{2} \right\rceil,\ldots,n\right\}$.

Por exemplo, para:

n	0	1	2	3	4	5	6	7	8	9
φ(n)	9	8	3	2	7	6	5	4	1	0

Tabela 3.1: Função inversa

Tem-se que: 1, 23, 47, 566, 1818, 1188, 90365290 são exemplos de palíndromos módulo φ.

Embora possa parecer estranho, os números 11, 22, 44, 565, 1881, 90355309 não são palíndromos módulo φ, para este exemplo.

Note que a função identidade em D, permite a criação de números palindrômicos que são conhecidos normalmente, ou seja, para:

n	0	1	2	3	4	5	6	7	8	9
φ(n)	0	1	2	3	4	5	6	7	8	9

Tabela 3.2: Função identidade.

Alguns palíndromos que podem ser formados a partir dessa função são:

2, 11, 33, 747, 9889, 56211265 e eles são exemplos de palíndromos que são conhecidos geralmente.

Os números palindrômicos normalmente discutidos são, portanto, apenas um dos casos desta generalização. Assim, para se gerar um novo tipo de número primo palindrômico, basta alterar o comportamento da função φ.

A quantidade de funções bijetivas φ que podem ser utilizadas é igual a $\binom{10}{5}5! + \binom{10}{2}\binom{8}{4}4! + \binom{10}{4}\binom{6}{3}3! + \binom{10}{6}\binom{4}{2}2! + \binom{10}{8}\binom{2}{1}1! + 1 = 133651.$

Desta maneira se torna inviável testar todos os comportamentos desta função, então apenas alguns destes serão testados.

As funções que foram utilizadas neste trabalho foram:

n	0	1	2	3	4	5	6	7	8	9
$\varphi_1(n)$	0	1	2	3	4	5	6	7	8	9

Tabela 3.3: Função $\varphi_1(n)$.

n	0	1	2	3	4	5	6	7	8	9
$\varphi_2(n)$	9	8	7	6	5	4	3	2	1	0

Tabela 3.4: Função $\varphi_2(n)$.

n	0	1	2	3	4	5	6	7	8	9
$\varphi_3(n)$	1	0	3	2	5	4	7	6	9	8

Tabela 3.5: Função $\varphi_3(n)$.

n	0	1	2	3	4	5	6	7	8	9
$\varphi_3(n)$	3	4	8	0	1	9	7	6	2	5

Tabela 3.6: Função $\varphi_4(n)$.

Para algumas variações da função φ não foi obtido nenhum resultado teórico relevante, como as funções φ_3 e φ_4. No entanto, algumas observações sobre estas funções serão apresentadas nos resultados computacionais.

A seguir serão realizadas observações acerca de cada uma das funções:

3.2.1 *Função φ_1*

Como esta função se trata da função identidade, então os palíndromos gerados por ela são os palíndromos normais e, portanto, os teoremas e conjecturas dos primos palindrômico normais se aplicam aqui.

Por exemplo, os números primos palindrômicos gerados utilizando esta função têm sempre uma quantidade ímpar de dígitos. A única exceção é o número 11.

O principal motivo da utilização desta função é realizar uma análise comparativa da densidade destes números em relação às outras funções, além de tentar descobrir um número primo palindrômico bastante grande que possa evidenciar a infinitude dos números primos palindrômicos.

3.2.2 Função φ_2

Assim como a função anterior, esta função só gera primos se a quantidade de dígitos for ímpar. Isso acontece porque se a quantidade de números fosse par, ele sempre seria divisível por 9, já que a soma dos seus dígitos seria um múltiplo de 9.

Por exemplo, dado o palíndromo módulo φ_2 679023 ao se somar seus dígitos são obtidos: $6+3=9, 7+2=9, 9+0=9$ resultando em 27 no total, assim este número deve ser divisível por 9. E realmente $679023 = 9 \cdot 75447$.

Além disto, quando a quantidade de dígitos é impar, o número só poderá ser primo se o número que fica no centro do palíndromo for diferente de 0, 3, 6, 9, pois caso contrário ele seria divisível por 3.

Tomando o exemplo anterior e inserindo o dígito 6 no meio, tem-se o palíndromo de módulo φ_2 6796023, mas realizando a soma de seus dígitos é obtido $27+6=33$ que é múltiplo de 3. Logo, o número 6796023 é composto.

4 TESTES COMPUTACIONAIS

Os testes computacionais foram realizados utilizando a linguagem de programação Java e o Ambiente de Desenvolvimento Integrado (IDE) Eclipse, desde a fase de desenvolvimento dos algoritmos geradores dos números palindrômicos, até os testes de primalidade e os algoritmos para a análise dos dados obtidos.

A ferramenta Eclipse foi utilizada porque ela permite um rápido desenvolvimento dos algoritmos com algumas facilidades para o usuário, como por exemplo, a função auto-completar. Ela possui um depurador bastante poderoso, o que auxilia bastante no processo de detecção de possíveis erros nos algoritmos. A linguagem *Java* foi utilizada por possuir nativamente suporte a números muito grandes através da abstração *BigInteger*.

Estes testes foram todos completamente realizados no LABLIC (Laboratório de Inteligência e Lógica Computacional) do DIMAp (Departamento de Informática e Matemática Aplicada). O Sistema Operacional utilizado foi o *Linux Ubuntu* e a máquina utilizada possuía um processador *Core 2 Duo* da *Intel* e 1 Gigabyte de Memória de Acesso Aleatório (RAM).

Devido às limitações de *Hardware* e tempo, seria impraticável tentar encontrar o maior número primo, portanto apenas algumas observações puderam ser efetuadas. Para se ter uma vaga idéia, para se encontrar o maior número primo em 2006, foram utilizadas 70000 máquinas ligadas em *Cluster* funcionando durante nove meses. Se fosse utilizada uma única máquina, um resultado só seria obtido em 4 mil anos! [39]

Durante a primeira fase de testes, os algoritmos produzidos eram responsáveis por gerar uma enorme lista com os possíveis números a serem

testados, bem como a manipulação desta lista. Os algoritmos deveriam ser capazes de realizar as operações de exibir na tela, bem como começar os testes de primalidade a partir de um dado número dentro daquela lista. Os resultados obtidos foram salvos em arquivos texto a partir de um simples redirecionamento do *buffer* de saída da tela para o arquivo escolhido.

Escolher o teste de primalidade que seria utilizado foi uma tarefa bastante complicada, pois a princípio a idéia seria utilizar o algoritmo determinístico e polinomial AKS. Apesar das características desejáveis deste algoritmo, na prática ele é de difícil implementação e muito lento em relação aos algoritmos probabilísticos. Em seguida a segunda opção foi implementar e utilizar o teste de primalidade de Miller-Rabin probabilístico pois este algoritmo não se baseia em nenhuma hipótese, o que não é o caso da versão determinística, que se baseia na hipótese de Riemann, que ainda não foi provada.

O teste de Miller-Rabin foi o algoritmo escolhido para a realização dos testes computacionais de primalidade deste trabalho, pois ele é bastante veloz comparado aos determinísticos, sua lógica é simples de implementar e para diminuir a chance de erro basta testar a mesma instância várias vezes apenas alterando a testemunha. Juntamente com este teste, a abstração *BigInteger* da linguagem *Java*, fornece um método que também verifica probabilisticamente se um número é primo. Esta versão do teste da API do Java, é uma outra implementação do Miller-Rabin e do Lucas-Lehmer. Ele foi utilizado juntamente com a nossa implementação do Miller-Rabin para alguns casos de teste. Aumentamos a precisão do nosso teste utilizando os dois testes em conjunto.

Para o caso de teste dos números primos compostos de um único dígito, foi verificada a primalidade de pouco menos de 1400 números, dos quais os últimos números desta seqüência têm mais de 11000 dígitos. Este teste de primalidade para números compostos de um único dígito durou cerca de 9 dias. Como ocorre um aumento de pelo menos dois dígitos nos números em cada

iteração, o tempo de execução de cada passo aumenta exponencialmente e também o custo computacional.

Neste trabalho foram gerados cerca de 2 bilhões de números palindrômicos diferentes por função, sendo suficiente para uma análise da densidade destes números.

5 RESULTADOS COMPUTACIONAIS

Os resultados que foram obtidos através de testes computacionais bem como a análise estatística destes resultados serão apresentados nesta seção.

5.1 RESULTADOS COMPUTACIONAIS PARA NÚMEROS PALINDRÔMICOS COMPOSTOS POR UM ÚNICO DÍGITO:

A tabela a seguir possui algumas estatísticas computacionais a respeito dos números compostos por um único dígito.

Quantidade números de um único dígito testados.	1387
Quantidade de dígitos do maior número explorado.	11503
Quantidade de dígitos do maior número primo encontrado.	1031
Quantidade de números primos encontrados.	5
Porcentagem de números primos.	0,36%
Quantidade de números com a quantidade de dígitos igual a um número primo.	5

Tabela 5.1: Resultados Computacionais para Palíndromos Compostos por um Único Dígito.

Todos os números testados possuíam uma quantidade prima de dígitos, pois esta é uma condição necessária para o número $\#1^{[p]}$ ser primo, como foi provado no Teorema 3.1. A partir daí, foram realizados testes de primalidade para os primeiros 1387 números com quantidade prima de dígitos.

Como já foi observado nos resultados teóricos, o único dígito que dá origem a números primos compostos por um único dígito é o número 1. Portanto todo o primo composto por um único dígito termina com o número 1.

A tendência é que a densidade destes números primos se torne cada vez menor conforme o espaço amostral vai aumentando.

5.2 RESULTADOS COMPUTACIONAIS PARA NÚMEROS PALINDRÔMICOS GENÉRICOS:

5.2.1 Função φ_1

As tabelas que serão apresentadas a seguir possuem alguns resultados computacionais com relação aos números palindrômicos módulo φ_1.

Para números palindrômicos módulo φ_1 com uma quantidade de dígitos ímpar os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	30483564
Quantidade de números compostos palindrômicos obtidos	969516436
Maior número primo obtido	99999999299999999
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	7785054
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	7623865
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	7541074
Quantidade de números primos palindrômicos que terminam com o dígito ‘9’	7533569

Tabela 5.2: Resultados Computacionais para Palíndromos módulo φ_1 com uma quantidade de dígitos ímpar.

Para números palindrômicos módulo φ_1 com uma quantidade de dígitos par os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	1
Quantidade de números compostos palindrômicos obtidos	999999999
Maior número primo obtido	11
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	1
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘9’	0

Tabela 5.3: Resultados Computacionais para Palíndromos módulo φ_1 com uma quantidade de dígitos par.

Finalmente os resultados computacionais para palíndromos módulo φ_1 são apresentados na tabela abaixo.

Total de números testados	2000000000
Maior número primo obtido	99999999299999999
Total de números primos palindrômicos que terminam com o dígito ‘1’	7785055
Total de números primos palindrômicos que terminam com o dígito ‘3’	7623865
Total de números primos palindrômicos que terminam com o dígito ‘7’	7541074
Total de números primos palindrômicos que terminam com o dígito ‘9’	7533569

Total de números primos palindrômicos obtidos	30483565
Total de números compostos palindrômicos obtidos	1969516435
Percentual total de números primos:	1.547769%

Tabela 5.4: Resultados Computacionais para Palíndromos módulo φ_1.

Considerando a densidade dos números primos palindrômicos de módulo φ_1 para um intervalo de um até 10^{18} , tem-se:

De 1 até 10^{17}	30483565
De $10^{17}+1$ até $2\cdot10^{17}$	0
De $2\cdot10^{17}+1$ até $3\cdot10^{17}$	0
De $3\cdot10^{17}+1$ até $4\cdot10^{17}$	0
De $4\cdot10^{17}+1$ até $5\cdot10^{17}$	0
De $5\cdot10^{17}+1$ até $6\cdot10^{17}$	0
De $6\cdot10^{17}+1$ até $7\cdot10^{17}$	0
De $7\cdot10^{17}+1$ até $8\cdot10^{17}$	0
De $8\cdot10^{17}+1$ até $9\cdot10^{17}$	0
De $9\cdot10^{17}+1$ até 10^{18}	0

Tabela 5.5: Densidade dos números primos para Palíndromos módulo φ_1.

Os testes de primalidade foram realizados sobre os 2000000000 primeiros números palindrômicos módulo φ_1.

Como podem ser observados nos resultados computacionais, os números primos palindrômicos nunca possuem uma quantidade de dígitos par com exceção do palíndromo 11 e isto foi provado por Shareef Bacchus utilizando o método da indução[32].

Outro fator a ser observado é que a distribuição dos números primos levando em consideração o último dígito é bem equilibrada.

Pelo fato de palíndromos módulo φ_1 nunca possuírem uma quantidade par de dígitos, então a densidade de números primos para esta função não será homogênea, na realidade os números primos menores que 10^{18} se concentram exclusivamente no intervalo entre 1 e 10^{17} .

5.2.2 Função φ_2

As tabelas que serão apresentadas a seguir possuem alguns resultados computacionais com relação aos números palindrômicos módulo φ_2.

Para números palindrômicos módulo φ_2 com uma quantidade de dígitos ímpar os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	21819243
Quantidade de números compostos palindrômicos obtidos	978180757
Maior número primo obtido	89999997820000001
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	7142532
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	7220591
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	7456118
Quantidade de números primos palindrômicos que terminam com o dígito ‘9’	0

Tabela 5.6: Resultados Computacionais para Palíndromos módulo φ_2 com uma quantidade de dígitos ímpar.

Para números palindrômicos módulo φ_2 com uma quantidade de dígitos par os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	0
Quantidade de números compostos palindrômicos obtidos	1000000000
Maior número primo obtido	Nenhum
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘9’	0

Tabela 5.7: Resultados Computacionais para Palíndromos módulo φ_2 com uma quantidade de dígitos par.

Finalmente os resultados computacionais para palíndromos módulo φ_2 são apresentados na tabela abaixo.

Total de números testados	2000000000
Maior número primo obtido	89999997820000001
Total de números primos palindrômicos que terminam com o dígito ‘1’	7142532
Total de números primos palindrômicos que terminam com o dígito ‘3’	7220591
Total de números primos palindrômicos que terminam com o dígito ‘7’	7456118
Total de números primos palindrômicos que terminam com o dígito ‘9’	0

Total de números primos palindrômicos obtidos	21819243
Total de números compostos palindrômicos obtidos	1978180757
Percentual total de números primos:	1.1029954%

Tabela 5.8: Resultados Computacionais para Palíndromos módulo φ_2.

Considerando a densidade dos números primos palindrômicos de módulo φ_2 para um intervalo de um até 10^{18} , tem-se:

De 1 até 10^{17}	30483565
De $10^{17}+1$ até $2\cdot10^{17}$	0
De $2\cdot10^{17}+1$ até $3\cdot10^{17}$	0
De $3\cdot10^{17}+1$ até $4\cdot10^{17}$	0
De $4\cdot10^{17}+1$ até $5\cdot10^{17}$	0
De $5\cdot10^{17}+1$ até $6\cdot10^{17}$	0
De $6\cdot10^{17}+1$ até $7\cdot10^{17}$	0
De $7\cdot10^{17}+1$ até $8\cdot10^{17}$	0
De $8\cdot10^{17}+1$ até $9\cdot10^{17}$	0
De $9\cdot10^{17}+1$ até 10^{18}	0

Tabela 5.9: Densidade dos números primos para Palíndromos módulo φ_2.

Os testes de primalidade foram realizados sobre os 2000000000 primeiros números palindrômicos módulo φ_2.

Como podem ser observados nos resultados computacionais, os números primos palindrômicos nunca possuem uma quantidade de dígitos par, este fato já foi previamente explicado na seção 3.2.2.

Além disto, como não existe nenhum número que comece com ‘0’, então também não existe nenhum número primo palindrômico que termine em ‘9’, devido as características da função φ_2.

Outro fator a ser observado é que a distribuição dos números primos levando em consideração o último dígito e excetuando os que terminam em “9”, é bem equilibrada.

Como os palíndromos módulo φ_2 nunca possuem uma quantidade par de dígitos, então a densidade de números primos para esta função não será homogênea e assim como a função φ_1, os números primos menores que 10^{18} se concentram apenas no intervalo entre 1 e 10^{17} .

5.2.3 Função φ_3

As tabelas que serão apresentadas a seguir possuem alguns resultados computacionais com relação aos números palindrômicos módulo φ_3.

Para números palindrômicos módulo φ_3 com uma quantidade de dígitos ímpar os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	22185953
Quantidade de números compostos palindrômicos obtidos	977814047
Maior número primo obtido	89999996578888889
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	7533748
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	7343875
Quantidade de números primos palindrômicos que	7308328

terminam com o dígito ‘9’	

Tabela 5.10: Resultados Computacionais para Palíndromos módulo φ_3 com uma quantidade de dígitos ímpar.

Para números palindrômicos módulo φ_3 com uma quantidade de dígitos par os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	22186717
Quantidade de números compostos palindrômicos obtidos	977813283
Maior número primo obtido	899999970168888889
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	7488721
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	7345867
Quantidade de números primos palindrômicos que terminam com o dígito ‘9’	7352126

Tabela 5.11: Resultados Computacionais para Palíndromos módulo φ_3 com uma quantidade de dígitos par.

Finalmente os resultados computacionais para palíndromos módulo φ_3 são apresentados na tabela abaixo.

Total de números testados	2000000000
Maior número primo obtido	899999970168888889
Total de números primos palindrômicos que terminam com o dígito ‘1’	0
Total de números primos palindrômicos que terminam com o dígito ‘3’	15022469

Total de números primos palindrômicos que terminam com o dígito ‘7’	14689742
Total de números primos palindrômicos que terminam com o dígito ‘9’	14660454
Total de números primos palindrômicos obtidos	44372670
Total de números compostos palindrômicos obtidos	1955627330
Percentual total de números primos:	2.2689738%

Tabela 5.12: Resultados Computacionais para Palíndromos módulo φ_3.

Considerando a densidade dos números primos palindrômicos de módulo φ_3 para um intervalo de um até 10^{18} , tem-se:

De 1 até 10^{17}	24125032
De $10^{17}+1$ até $2\cdot10^{17}$	0
De $2\cdot10^{17}+1$ até $3\cdot10^{17}$	6832415
De $3\cdot10^{17}+1$ até $4\cdot10^{17}$	0
De $4\cdot10^{17}+1$ até $5\cdot10^{17}$	0
De $5\cdot10^{17}+1$ até $6\cdot10^{17}$	0
De $6\cdot10^{17}+1$ até $7\cdot10^{17}$	6702569
De $7\cdot10^{17}+1$ até $8\cdot10^{17}$	0
De $8\cdot10^{17}+1$ até $9\cdot10^{17}$	6712654
De $9\cdot10^{17}+1$ até 10^{18}	0

Tabela 5.13: Densidade dos números primos para Palíndromos módulo φ_3.

Os testes de primalidade foram realizados sobre os 2000000000 primeiros números palindrômicos módulo φ_3.

De acordo com os resultados computacionais explicitados nas tabelas anteriores, os números primos palindrômicos gerados a partir da função φ_3 são independentes da quantidade de dígitos. Isto causa um aumento na quantidade

total de números primos produzidos, resultando num percentual de números primos maior que as duas funções previamente apresentadas.

Além disto, como não existe nenhum número que comece com ‘0’, então também não existe nenhum número primo palindrômico módulo φ_3 que termine em ‘1’, devido as características da função φ_3.

Outro fator a ser observado é que a distribuição dos números primos levando em consideração o último dígito e excetuando os que terminam em “1”, é bem equilibrada.

Como os número primos, com exceção do número 5, só podem terminar com os dígitos 1, 3, 7 e 9, os palíndromos módulo φ_3 só poderão ser primos caso estes se iniciem com os dígitos 2, 6 e 8. Portanto apenas os intervalos que possuem números que começam com esses dígitos, podem produzir números primos módulo φ_3. E de fato os intervalos de 1 até 10^{17}, $2\cdot10^{17}+1$ até $3\cdot10^{17}$, $6\cdot10^{17}+1$ até $7\cdot10^{17}$ e $8\cdot10^{17}+1$ até $9\cdot10^{17}$ são os únicos que produzem números primos, para palíndromos menores que 10^{18}.

5.2.4 Função φ_4

As tabelas que serão apresentadas a seguir possuem alguns resultados computacionais com relação aos números palindrômicos módulo φ_4.

Para números palindrômicos módulo φ_4 com uma quantidade de dígitos ímpar os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	21962473
Quantidade de números compostos palindrômicos	978037527

obtidos	
Maior número primo obtido	69999997665555557
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	7363172
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	1
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	7284642
Quantidade de números primos palindrômicos que terminam com o dígito ‘9’	7314656

Tabela 5.14: Resultados Computacionais para Palíndromos módulo φ_4 com uma quantidade de dígitos ímpar.

Para números palindrômicos módulo φ_4 com uma quantidade de dígitos par os seguintes resultados computacionais foram obtidos.

Quantidade de números palindrômicos testados	1000000000
Quantidade de números primos palindrômicos obtidos	20729597
Quantidade de números compostos palindrômicos obtidos	979270403
Maior número primo obtido	699999997655555557
Quantidade de números primos palindrômicos que terminam com o dígito ‘1’	6935362
Quantidade de números primos palindrômicos que terminam com o dígito ‘3’	0
Quantidade de números primos palindrômicos que terminam com o dígito ‘7’	6882202
Quantidade de números primos palindrômicos que terminam com o dígito ‘9’	6912029

Tabela 5.15: Resultados Computacionais para Palíndromos módulo φ_4 com uma quantidade de dígitos par.

Finalmente os resultados computacionais para palíndromos módulo φ_4 são apresentados na tabela abaixo.

Total de números testados	2000000000
Maior número primo obtido	699999997655555557
Total de números primos palindrômicos que terminam com o dígito '1'	14298534
Total de números primos palindrômicos que terminam com o dígito '3'	1
Total de números primos palindrômicos que terminam com o dígito '7'	14166844
Total de números primos palindrômicos que terminam com o dígito '9'	14226685
Total de números primos palindrômicos obtidos	42692070
Total de números compostos palindrômicos obtidos	1957307930
Percentual total de números primos:	2.1811628%

Tabela 5.16: Resultados Computacionais para Palíndromos módulo φ_4.

Considerando a densidade dos números primos palindrômicos de módulo φ_4 para um intervalo de um até 10^{18}, tem-se:

De 1 até 10^{17}	24298930
De $10^{17}+1$ até $2\cdot10^{17}$	0
De $2\cdot10^{17}+1$ até $3\cdot10^{17}$	0
De $3\cdot10^{17}+1$ até $4\cdot10^{17}$	0
De $4\cdot10^{17}+1$ até $5\cdot10^{17}$	6154015
De $5\cdot10^{17}+1$ até $6\cdot10^{17}$	6132006
De $6\cdot10^{17}+1$ até $7\cdot10^{17}$	6107119
De $7\cdot10^{17}+1$ até $8\cdot10^{17}$	0
De $8\cdot10^{17}+1$ até $9\cdot10^{17}$	0

De $9 \cdot 10^{17} + 1$ até 10^{18}	0

Tabela 5.17: Densidade dos números primos para Palíndromos módulo φ_4.

Os testes de primalidade foram realizados sobre os 2000000000 primeiros números palindrômicos módulo φ_4.

De acordo com os resultados computacionais explicitados nas tabelas anteriores, os números primos palindrômicos gerados a partir da função φ_4 são independentes da quantidade de dígitos. Isto causa um aumento na quantidade total de números primos produzidos, resultando num percentual de números primos maior que as duas funções previamente apresentadas.

Além disto, como não existe nenhum número que comece com '0', então devido as características da função φ_4, existe apenas um número primo palindrômico módulo φ_4 que termine em '3', que é o próprio.

Outro fator a ser observado é que a distribuição dos números primos levando em consideração o último dígito e excetuando os que terminam em "3", é bem equilibrada.

Como os número primos, com exceção do número 5, só podem terminar com os dígitos 1, 3, 7 e 9, os palíndromos módulo φ_4 só poderão ser primos caso estes se iniciem com os dígitos 4, 6 e 5. Portanto apenas os intervalos que possuem números que começam com esses dígitos, podem produzir números primos. E de fato os intervalos de 1 até 10^{17}, $4 \cdot 10^{17} + 1$ até $5 \cdot 10^{17}$, $5 \cdot 10^{17} + 1$ até $6 \cdot 10^{17}$ e $6 \cdot 10^{17} + 1$ até $7 \cdot 10^{17}$ são os únicos que produzem números primos módulo φ_4, para palíndromos menores que 10^{18}.

6 CONSIDERAÇÕES FINAIS

O objetivo deste trabalho foi tentar evidenciar computacionalmente a infinitude dos números primos palindrômicos, além de realizar algumas generalizações sobre eles. Além disto, este trabalho proporcionou uma visão abrangente sobre assuntos correlacionados aos objetivos, para que se tornasse bastante claro ao leitor quais foram as bases para a construção deste trabalho.

A partir dos resultados computacionais obtidos na seção anterior, é possível conjecturar que:

Conjectura 1: Para qualquer que seja a função φ, a quantidade de números primos palindrômicos módulo φ é sempre infinita.

Caso esta conjectura seja comprovada, pode-se afirmar com certeza que os números primos palindrômicos normais são realmente infinitos, já que eles são apenas um caso particular dos números palindrômicos módulo φ.

Um fato que pode ser provado facilmente é que para qualquer função φ, se todo $\varphi(i)+i$ for divisível por "3", então não existirá nenhum palíndromo primo módulo φ com uma quantidade par de dígitos.

Uma generalização também pode ser realizada sobre os números primos escritos a partir de um único dígito. Para se obter esta generalização, considera-se n o número de repetições de uma seqüência s, no qual $s \in \mathbb{N}$ e $n \in \mathbb{N}$, então é possível observar, que se $s^{[n]}$ é primo, então $s=1$ ou $n=1$. Isto é claramente verdadeiro, pois caso contrário, a seqüência $s^{[n]}$ seria divisível pelo próprio s.

Apesar de amplamente estudado por muitos matemáticos, os números primos palindrômicos ainda possuem uma grande quantidade de questões sem resposta, e isto associado as suas propriedades especiais, é um grande incentivo para o estudo destes maravilhosos números.

Assim, uma continuação dos testes computacionais anteriores para uma quantidade ainda maior de números e dígitos, poderia ser realizada futuramente, com o objetivo de evidenciar cada vez mais a infinitude dos números primos palindrômicos.

REFERÊNCIAS

[1] LOVÁSZ, László; PELIKÁN, József; VESZTERGOMBI, Katalin. ***Discrete Mathematics:*** Elementary and Beyond. Springer-Verlag, 2003.

[2] SHOUP, Victor; ***A Computational Introduction to Number Theory and Algebra***. Cambridge University Press, 2005.

[3] GRAHAM, Ronald L., KNUTH, Donald E., PATASHNIK, Oren. ***Concrete mathematics:*** a foundation for computer science. Addison-Wesley, 1989.

[4] ***Primorial Prime – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Primorial_prime. Acesso em: 22 de maio de 2008.

[5] ***Euclid Number – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Euclid_number. Acesso em: 22 de maio de 2008.

[6] ***Prime Number – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Prime_number. Acesso em: 22 de maio de 2008.

[7] SHOKRANIAN, Salahoddin. ***Criptografia para Iniciantes***. Brasília: Editora Universidade de Brasília, 2005. 94p.

[8] RIBENBOIM, Paulo. ***Números Primos:*** *Mistérios e Recordes*. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2001. 292p.

[9] ***Smarandache-Wellin Number – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Smarandache-Wellin_prime. Acesso em: 22 de maio de 2008.

[10] ***Truncable Prime – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Truncatable_prime. Acesso em: 22 de maio de 2008.

[11] ***Fibonacci Number – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Fibonacci_number. Acesso em: 22 de maio de 2008.

[12] ***Palíndromo – Wikipédia, a enciclopédia livre***. Disponível em: http://pt.wikipedia.org/wiki/Pal%C3%ADndromo. Acesso: 22 de maio de 2008.

[13] ***Palindrome – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Palindrome. Acesso em: 22 de maio de 2008.

[14] ***Rômulo Marinho – Wikipédia, a enciclopédia livre***. Disponível em: http://pt.wikipedia.org/wiki/R%C3%B4mulo_Marinho. Acesso em: 22 de maio de 2008.

[15] ***Hunting The Muse: Palindrome Poem***. Disponível em: http://www.museworld.com/archives/001265.html. Acesso em: 22 de maio de 2008.

[16] ***Capicua – Wikipédia, a enciclopédia livre***. Disponível em: http://pt.wikipedia.org/wiki/Capicua. Acesso em: 22 de maio de 2008.

[17] ***Palindromic Number – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Palindromic_number. Acesso em: 22 de maio de 2008.

[18] ***Lychrel Number – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Lychrel_number. Acesso em: 22 de maio de 2008.

[19] WESTLEY, Brian. ***International Obfuscated C Code Contest***. Disponível em: http://www0.us.ioccc.org/1987/westley.c. Acesso em: 22 de maio de 2008.

[20] ***Millôr Fernandes – Wikipédia, a enciclopédia livre***. Disponível em: http://pt.wikipedia.org/wiki/Mill%C3%B4r_Fernandes. Acesso em: 22 de maio de 2008.

[21] DIRICHLET, Peter Gustav Lejeune. ***Lectures on number theory***. Tradução por: John StillWell. American Mathematical Society, 276p. (History of mathematics; v. 16 ; Suplementos por R. Dedekin).

[22] AGRAWAL, Manindra; BISWAS, Somenath. ***Primality and Identity Testing via Chinese Remaindering***. 21 de Fevereiro de 2003.

[23] AGRAWAL, Manindra; KAYAL, Neeraj; SAXENA, Nitin. ***Prime is in P***. Annals of Mathematics, 160 (2004) 781-793. 24 de Janeiro de 2003.

[25] ***Co-NP – Wikipedia, the free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Co-NP. Acesso em 29 de maio de 2008.

[26] WEISSTEIN, Eric W. ***MathWorld News:*** *Primality Testing is easy*. Disponível em: http://mathworld.wolfram.com/news/2002-08-07/primetest/. Acesso em 29 de maio de 2008.

[27] WEISSTEIN, Eric W. ***MathWorld News:*** *Palindromic Prime*. Disponível em: http://mathworld.wolfram.com/PalindromicPrime.html. Acesso em: 9 de junho de 2008.

[28] HONAKER, G. L; CALDWELL, Chris K. ***Supplement to "Palindromic Prime Pyramids"***. Disponível em:

http://www.utm.edu/staff/caldwell/supplements/. Acesso em: 9 de junho de 2008.

[29] CALDWELL, Chris. ***The Prime Glossary:*** *palindromic prime*. Disponível em: http://primes.utm.edu/glossary/page.php?sort=PalindromicPrime. Acesso em: 9 de junho de 2008.

[30] SILVEIRA, J. F. Porto da. ***Cálculo de Números primos:*** *colocações iniciais*. Disponível em: http://www.mat.ufrgs.br/~portosil/pqprimo.html. Acesso em: 9 de junho de 2008.

[31] OLIVEIRA, Sara; VENTURA, Helena; PAIS, Alexandre. ***História dos números primos***. Disponível em: http://www.educ.fc.ul.pt/icm/icm98/icm12/Historia.htm. Acesso em: 9 de junho de 2008.

[32] SHAREEF, Bacchus. ***Those Amazing Palindromes***. Disponível em: http://jwilson.coe.uga.edu/emt669/Student.Folders/Bacchus.Mohamed/pal/pal.html. Acesso em: 9 de junho de 2008.

[33] PETERSON, Ivars. ***Primes, Palindromes and Pyramids***. Disponível em:http://www.sciencenews.org/view/generic/id/6506/title/Primes%2C_Palindromes%2C_and_Pyramids. Acesso em: 9 de junho de 2008.

[34] BEDREGAL, Benjamin Callejas. ***Nondeterministic Linear Automata***. Journal of Automata, Language and Combinatorics. Submitted.

[35] ***Crivo de Eratóstenes – Wikipédia, A enciclopédia livre***. Disponível em: http://pt.wikipedia.org/wiki/Crivo_de_Erat%C3%B3stenes. Acesso em: 30 de maio de 2008.

[36] ***Primality Test – Wikipedia, The free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Primality_test. Acesso em: 30 de maio de 2008.

[37] ***AKS primality test – Wikipedia, The free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/AKS_primality_test. Acesso em: 31 de maio de 2008.

[38] ***Miller-Rabin primality test – Wikipedia, The free encyclopedia***. Disponível em: http://en.wikipedia.org/wiki/Miller-Rabin_primality_test. Acesso em: 01 de junho de 2008.

[39] ***44th Mersenne Prime Discovered***. Disponível em: http://www.mersenne.org/32582657.htm. ORLANDO, Florida. 11 de Setembro de 2006. Acesso em: 04 de junho de 2008.

ANEXOS

Os 187 números a seguir representam os números palindrômicos compostos apenas pelo dígito “1” e foram gerados a partir do teorema 3.1, para que seja possível encontrar algum primo. O número representa a quantidade de vezes que o número 1 foi repetido, ou seja, o número representa o valor de k para a seqüência $\#1^{[k]}$, e ele pode ser seguido pelos caracteres “é primo” para indicar que o $\#1^{[k]}$ é primo. Embora tenham sido gerados 1387 números, apenas 187 são apresentados, já que nenhum k > 1031 dentro deste intervalo é primo.

2 é primo.	293	677
3	307	683
5	311	691
7	313	701
11	317 é primo	709
13	331	719
17	337	727
19 é primo	347	733
23 é primo	349	739
29	353	743
31	359	751
37	367	757
41	373	761
43	379	769
47	383	773
53	389	787
59	397	797
61	401	809
67	409	811
71	419	821

73	421	823
79	431	827
83	433	829
89	439	839
97	443	853
101	449	857
103	457	859
107	461	863
109	463	877
113	467	881
127	479	883
131	487	887
137	491	907
139	499	911
149	503	919
151	509	929
157	521	937
163	523	941
167	541	947
173	547	953
179	557	967
181	563	971
191	569	977
193	571	983
197	577	991
199	587	997
211	593	1009
223	599	1013
227	601	1019
229	607	1021
233	613	1031 é primo
239	617	1033

241	619	1039
251	631	1049
257	641	1051
263	643	1061
269	647	1063
271	653	1069
277	659	1087
281	661	1091
283	673	1093