Universidade Federal do Piauí
Centro de Ciências da Natureza
Pós Graduação em Matemática
Mestrado Profissional em Matemática - PROFMAT

Caracterização dos Números Primos e Aplicações no Ensino Básico

Alvaro Pereira de Carvalho

Orientador
Prof. Ms. João Benício de Melo Neto

Teresina - 2015

Alvaro Pereira de Carvalho

Caracterização dos Números Primos e Aplicações no Ensino Básico

Dissertação submetida à Coordenação Acadêmica Institucional do Programa de Mestrado Profissional em Matemática em Rede Nacional na Universidade Federal do Piauí oferecido em associação com a Sociedade Brasileira de Matemática, como requisito parcial para a obtenção do grau de mestre em Matemática.

Orientador
Prof. Ms. João Benício de Melo Neto

Teresina - 2015

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca Setorial do CCN

C331c Carvalho, Álvaro Pereira de.
Caracterização dos números primos e aplicações no ensino básico. / Álvaro Pereira de Carvalho. – Teresina, 2015.
44f. il.

Dissertação (Mestrado Profissional) – Pós-Graduação em Matemática, Universidade Federal do Piauí, 2015.
Orientador: Prof. Msc. João Benício de Melo Neto

1. Álgebra - Números Primos. 2. Teoria Elementar dos Números. 3. Matemática – Estudo e Ensino. I. Título

CDD 512.72

UNIVERSIDADE FEDERAL DO PIAUÍ
CENTRO DE CIÊNCIAS DA NATUREZA
CENTRO DE EDUCAÇÃO ABERTA E À DISTÂNCIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Dissertação de Mestrado submetida à Coordenação Acadêmica Institucional, na Universidade Federal do Piauí, do Programa de Mestrado Profissional em Matemática em Rede Nacional para a obtenção do grau de **mestre em matemática** intitulada: Caracterização dos Números Primos e Aplicações no Ensino Básico defendida por Alvaro Pereira de Carvalho em 24/02/2015 e aprovada pela banca constituída pelos professores:

Prof. Ms. João Benício de Melo Neto
Orientador

Prof. Dr. Gilvan Lima de Oliveira
Departamento - Universidade Federal do Piauí - UESPI
Examinador Interno

Prof. Dr. Jurandir Lopes de Oliveira
Departamento - Universidade Federal do Piauí - UFPI
Examinador Interno

Prof. Ms. José Arimatéa Rodrigues de Melo Júnior
Departamento - Universidade Estadual do Piauí - UESPI
Examinador Externo

A minha família que sempre esteve ao meu lado em todos os momentos

Agradecimentos

Agradeço a Deus por tudo na minha vida.

Agradeço aos meus pais, Luisa Pereira de Sousa Carvalho e Antonio Alves de Carvalho(*in memorian*), pela educação que me deram.

Agradeço minha família por sempre acreditar e confiar em mim.

Agradeço a minha esposa(Ionne Carvalho) e minha filha(Lara Maria Carvalho) pelo amor incondicional.

Agradeço aos meus amigos, e em especial os da turma PROFMAT 2013 da UFPI, pelo apoio que a mim foi dado.

Agradeço ao meu orientador, Professor João Benício de Melo Neto, pela paciência, pela motivação e por dar sua valiosa e indispensável contribuição para realização do presente trabalho.

Agradeço aos idealizadores do PROFMAT, pela preocupação com a educação do Brasil.

Agradeço a UFPI e em especial aos meus professores do PROFMAT que contribuiram bastante para minha formação.

Agradeço a CAPES pelo apoio intelectual e financeiro.

A Matemática é a rainha das ciências e a teoria dos números é rainha das matemáticas.

Gauss

o verdadeiro, aquele que tem a chave de Davi,
aquele que abre e ninguém fecha,
aquele que fecha e ninguém mais abre

Apocalipse de São João

Resumo

Neste trabalho é feito um estudo sobre os números primos, reproduzindo um breve relato histórico, alguns teoremas, caracterização e resultados importantes a eles relacionados. Também apresentaremos algumas aplicações dos números primos na criptografia e na área de computação. Temos então na área de computação uma importante e valiosa aplicação dos números primos. Primeiramente faremos um breve relato histórico, tratando, desde o surgimento, até o tempo atual e, em seguida, mostraremos a definição, algumas propriedades e apresentaremos teoremas que usaremos para caracterizar os números primos. O estudo sobre estes números mostra algumas fórmulas para gerar números primos, mas, pelo fato dos mesmos não apresentarem certo padrão, torna a identificação deles não ser algo trivial, ou seja, dado um número qualquer ele é primo ou composto? O trabalho apresenta, ainda, algumas curiosidades relacionadas aos números primos e uma atividade para o tema em questão.

Palavras-chave: Números Primos, História, Caracterização, Teoremas, Aplicações.

Abstract

In this work is done a study of prime numbers, playing a brief historical account, some theorems, characterization and important results related to them. Also we will present some applications of prime numbers in cryptography and computing area. We have then in computing an important and valuable application of prime numbers. At first we will take a brief historical account, treating since the appearance, until the current time and then we'll show it the definition, some properties and theorems we present to characterize the prime numbers. The study about these numbers shows some formulas to generate prime numbers, but by the fact of them not present certain default, makes identification of them not be something trivial, i.e. given any number he is prime or composite? The paper presents also some curiosity related to prime numbers and an activity for the issue at hand.

Keywords: Prime Numbers, History, Characterization, Theorems, Aplicacions.

Lista de Figuras

Sumário

As propriedades e as relações entre os números são estudadas na área da matemática denominada Teoria dos Números. O estudo destes conceitos é tratado com maior ênfase nos cursos de graduação, principalmente na graduação em Matemática.

Embora os conceitos, definições e propriedades de divisibilidade, mínimo múltiplo comum, máximo divisor comum e números primos sejam tão pouco explorados na Educação Básica, acredita-se que alguns problemas e algumas situações relacionadas a Teoria dos Números tenham um grande potencial motivador no processo de ensino aprendizagem, pois existem vários problemas contextualizado que favorecem a elaboração de sequências didáticas motivadora afim de promover o desenvolvimento do pensamento conceitual. Conceitos relacionados à Teoria dos Números podem ser poderosas ferramentas na resolução de algumas situações problemas que envolvem números primos.

Os números primos são estudados pelos alunos desde o Ensino Fundamental, porém algumas obras literárias não trata de forma motivadora esse tema. Na Educação Básica, por exemplo, o aluno é apenas indagado se determinado número inteiro é primo ou não, se as raízes de uma dada equação são números primos ou não, além dessas indagações os alunos são levados a repetir exaustivamente várias exercícios sobre fatoração de números naturais, embora muitos pensem que o estudo sobre Teoria dos Números se retém nas primeiras séries da Educação Fundamental, tópicos mais específicos ligados à Teoria dos Números são sugeridos na seção *Conteúdos Propostos para o Ensino de Matemática no Terceiro Ciclo* como segue:

> Conceitos como os de múltiplo e divisor de um número natural ou o conceito de número primo podem ser abordados neste ciclo como uma ampliação do campo multiplicativo, que já vinha sendo construído nos ciclos anteriores, e não como assunto novo, desvinculado dos demais. Além disso, é importante que tal trabalho não se resuma à apresentação de diferentes técnicas ou de dispositivos práticos que permitem ao aluno encontrar, mecanicamente, o mínimo múltiplo comum e máximo divisor comum sem compreender as situações-problema que esses conceitos permitem resolver. (PCN - matemática - 5ª e 8ª séries, p.66)

No entanto aos alunos não são apresentados aplicações práticas, ou seja, os alunos da Educação Básica não são motivados a realizar um estudo mais avançado sobre os números primos.

O presente trabalho tem por objetivo relatar um pequeno contexto histórico dos números primos seguindo a ordém cronológica, caracterizar os números primos por meio de alguns teoremas e apresentar algumas aplicações desses números .

Desde a antiguidade os matemáticos se interessam pelos números primos: Como encontrá-los? Como se distribuem? Anos se passaram, porém algumas dessas perguntas ainda permanecem sem respostas até os dias atuais.

Euclides demonstrou que existem infinitos números primos, por outro lado, algumas afirmações envolvendo números primos resistem ao tempo e ainda não foram demonstradas. Como a forma como os números primos se distribuem, como responder de

maneira prática se um número é primo ou não? Por causa desse grande mistério acerca dos números primos, alguns sistemas de seguranças utilizam números primos para proteger senhas e até mesmo esses números foram utilizados como um poderoso sistema de comunicação entre nações através do uso de criptografia.

Existem alguns problemas relacionados aos números primos que se encontram sem solução, dentre os quais podemos citar:

- A conjectura de Goldbach: Todo número natural par, maior ou igual a quatro, pode ser escrito como a soma de dois números primos;
- Conjectura dos primos Gêmeos: Existem infinitos primos p tal que p + 2 também é primo.
- Dado um número primo qualquer, quantos primos menores que esse existem?

O presente trabalho foi divididos em 4 capítulos:
O primeiro capítulo trás a retrospectiva históricas dos números primos;
O segundo capítulo trata da caracterização dos números primos;
O terceiro capítulo lista algumas aplicações dos números primos
O quarto capítulo mostra algumas curiosidades e mistérios sobre os números primos e uma sugestão de atividade para alunos do Ensino Fundamental e / ou Ensino Médio.

1 Retrospectiva Histórica

Você já se perguntou porque os números primos têm este nome? O nome é uma herança grega e, naturalmente, não se refere a nenhuma relação de parentesco. Os gregos classificavam os números em primeiros ou indecomponíveis e secundários ou compostos. Os números compostos são secundários por serem formados a partir dos primos. Os romanos apenas traduziram literalmente a palavra grega para primeiro, que em latim é primus. É daí que vêm nossos números primos.

Os números primos foram e ainda continua sendo objeto de estudos de grandes matemáticos pela sua importância e mística, eles vem sendo estudados pelos matemáticos desde 500 a.C. . Os matemáticos gregos, os pitagóricos (Sociedade secreta fundada por Pitágoras tinha um código de conduta rígido, acreditavam na transmigração das almas e, portanto, que não se devia matar ou comer um animal porque ele poderia ser a moradia de um amigo morto. Também não se podia comer lentilhas ou alimentos que causassem gases. Os pitagóricos imaginavam que os números ímpares tinham atributos masculinos e os pares eram femininos. O número 1, diziam, é o gerador dos outros números e o número da razão), foram os primeiros a se interessarem pelas propriedades desses números.

No livro Os Elementos publicado por Euclides (foi o homem que deixou escrito a maior obra de Matemática da humanidade "os Elementos ". 13 livros que apresentam a Geometria em sua estrutura formal, que, em número de exemplares editados, só perde da Bíblia. Ressaltamos que a Geometria que estudamos é a Geometria Euclidiana pois se baseia nas ideias de Euclides expressas nestes livros. Falo que ele foi o primeiro homem que criou um sistema axiomático e ressalto que a Geometria que estudamos hoje é idêntica a que ele usava há 2500 anos. Suas histórias são contadas em quase todos tópicos de Geometria) de Alexandria por volta de 300 a.C., existiam alguns relatos muito importante sobre números primos como, por exemplo, a demonstração da infinidade de números primos e a prova do Teorema Fundamental da Aritmética. Euclides também escreveu vários livros dedicados quase na íntegra à Teoria dos Números.

Cerca de 200 a.C. o grego Eratóstenes (nasceu em Cirene, na Grécia, por volta do ano 276 a.C., e estudou na cidade natal, em Alexandria e Atenas. De sua extensa produção intelectual sobressaem a medição do meridiano terrestre e o método prático de determinação dos números primos, conhecido como crivo de Eratóstenes) desenvolveu

um algoritmo para calcular números primos, que ficou conhecido como Crivo de Eratóstenes, que atualmente ainda se mostra o algoritmo mais eficiente para achar todos os números primos não muito grandes.

Depois de alguns séculos sem nenhuma descoberta significante, surge no início do século XVII Pierre de Fermat (conhecido como o "Príncipe dos Amadores", nasceu na França em Beaumont-de-Lomages em Agosto de 1601, não se sabendo o dia exato do seu nascimento. Filho de um rico comerciante de peles, estudou num mosteiro franciscano de Grandselve, recebendo, ali, uma educação privilegiada. Mais tarde foi estudar direito na a cidade de Toulouse onde posteriormente onde, posteriormente, foi juiz do reinado de Luis XIV), ele provou que se p é um número primo, então para todo inteiro a o número p divide a diferença $a^p - a$ conhecido também como pequeno teorema de Fermat. O Pequeno Teorema de Fermat é referência em muitos outros trabalhos na Teoria dos Números e ainda hoje é utilizado em testes de primalidade.

Em uma carta enviada a Mersenne(Padre, matemático, filósofo natural e teólogo francês nascido nas proximidades de *Oizé*, famoso por suas intervenções conciliadoras ou decisórias em atividades e querelas científicas. Nascido de uma família camponesa, frequentou o *College de Mans* após o qual (1604) passou cinco anos no Colégio Jesuíta de *La Fleche*. Estudou teologia em Sorbonne (1609 -1611) e uniu-se à Ordem Religiosa de Minims (1611) uma ordem cuja vida era devotada à oração, estudo e escolaridade), Fermat afirma ter descoberto uma fórmula para achar números primos para todo n natural, $2^{2^n} + 1$. Embora não tivesse conseguido provar este resultado, a fórmula funcionava para $n = 0, 1, 2, 3$ e 4. Os números dessa forma $2^{2^n} + 1$ ficaram conhecidos como números de Fermat. Alguns anos depois o matemático Leonhard Euler (1707 - 1783) mostrou que para $n = 5$ o número $2^{2^5} + 1$ era divisível por 641, ou seja, que esse número não era primo.

Marin Mersenne dedicou-se também ao estudo sobre os números primos. Os números da forma $2^n - 1$ ficaram conhecidos como números de Mersenne , que estão inteiramente ligados aos números perfeitos. Em 1644 Mersenne afirmou, sem uso de métodos demonstrativos, que os números da forma $2^n - 1$ eram primos para $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257 e composto para outros primos menores que 257. Devido aos meios de verificação de testes de primalidades da época Mersenne jamais soube se estava certo. Em 1883, *Pervushin* mostrou que, para $n = 61$, o número $2^{61} - 1$ era primo. Sabe-se também que $2^{89} - 1$ e $2^{107} - 1$ são primos e os números $2^{67} - 1$ e $2^{257} - 1$ são compostos. Usando seu teste Lucas demonstrou que os o número $2^{127} - 1$ era primo e até o ano de 1952 era considerado o maior primo conhecido.

Com o avanço tecnológico, em 1952 deu-se o inicio da era da computação, que veio a dar uma contribuição valiosa e significativa em relação ao estudo dos números primos. Robinson conseguiu, através de computadores, mostrar que os números $2^{607} - 1$,$2^{1279} - 1$, $2^{2203} - 1$ e $2^{2281} - 1$ eram primos. Hoje se conhece que o número $2^{57885161} - 1$ é primo, e que possui no sistema decimal 17425170 de dígitos e foi descoberto em janeiro de 2013.

2 Revisão Teórica

Alguns dos conceitos aqui apresentados, apesar de não serem abordados na Educação Básica, são de extrema importância para os professores que atuam nessa modalidade. Os conceitos e definições que seguem nessa seção são destinados a um estudante com conhecimento básico sobre fatoração de números inteiros e primos, que tenha facilidade no cálculo com fórmulas elementares e que tenha interesse matemático suficiente para apreciar argumentos de demonstrações bastante básico.

Antes de caracterizarmos os números primos, apresentaremos algumas definições, teoremas e alguns resultados que serão muito importantes para o entendimento da caracterização.

2.1 Divisibilidade

Quando falamos em divisibilidade e resto , pensamos logo que esse assunto é trivial, porém esse tema merece um pouco mais de atenção. Dados dois inteiros d e a , dizemos que d divide a ou que d é um divisor de a ou ainda que a é um múltiplo de d e escrevemos

$$d \mid a$$

se existir $q \in \mathbb{Z}$ com $a = q \cdot d$. Caso contrário, escrevemos $d \nmid a$. Vejamos alguns exemplos:

Exemplo 2.1. $4 \mid 12$, pois $12 = 4 \cdot 3$

Exemplo 2.2. $-5 \mid 30$, pois $30 = (-5) \cdot 6$

Exemplo 2.3. $7 \mid -21$, pois $-21 = 7 \cdot (-3)$

Exemplo 2.4. $3 \nmid 11$, pois não existe $q \in \mathbb{Z}$, tal que $11 = 3 \cdot q$

Lema 2.1. *Sejam $a, b, c, d \in \mathbb{Z}$, se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes x e y .*

Demonstração 2.1. *Se $d \mid a$ e $d \mid b$, então podemos escrever $a = d \cdot q_1$ e $b = d \cdot q_2$ com q_1 e $q_2 \in \mathbb{Z}$, logo $ax + by = d(q_1 \cdot x + q_2 \cdot y)$. Como q_1 e $q_2 \in \mathbb{Z}$, temos que $d \mid ax + by$.*

Lema 2.2. *Sejam $a, b, c, d \in \mathbb{Z}$, se $d \mid a$, então $a = 0$ ou $\mid d \mid \leq \mid a \mid$.*

Demonstração 2.2. *Suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = d \cdot q$ com $q \neq 0$, assim $\mid q \mid \geq 1$ e $\mid a \mid = \mid d \mid\mid q \mid \geq \mid d \mid$*

Lema 2.3. *Sejam $a, b, c, d \in \mathbb{Z}$, se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração 2.3. *Se $a \mid b$ e $b \mid c$, então existem q_1 e $q_2 \in \mathbb{Z}$ tais que $b = a \cdot q_1$ e $c = b \cdot q_2$, logo $c = a \cdot q_1 \cdot q_2$ e portanto $a \mid c$.*

2.2 Divisão Euclidiana

Mesmo quando um número inteiro $b \neq 0$ não divide o número inteiro a, Euclides nos seus Elementos,utiliza, sem enunciá-lo explicitamente,o fato de que é sempre possível efetuar a divisão de a por b com resto. Esse resultado não é só um importante instrumento na obra de Euclides, como também é um resultado central da teoria.

Definição 2.1. *Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que:*

$$a = b \cdot q + r, \text{ com } 0 \leq r < \mid b \mid$$

Demonstração 2.4. *Considere o conjunto*

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

Existência:

Pela propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - n \cdot b > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - b \cdot q$. Sabemos que $r \geq 0$. Vamos mostrar que $r < \mid b \mid$.Suponhamos por absurdo que $r \geq \mid b \mid$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = \mid b \mid + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Unicidade:

Suponha que $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$, onde $q_1, r_1, q_2, r_2 \in \mathbb{Z}$, $0 \leq r_1 < \mid b \mid$ e $0 \leq r_2 < \mid b \mid$. Assim, temos $- \mid b \mid < -r_1 \leq r_2 - r_1 \leq r_2 < \mid b \mid$. logo, $\mid r_2 - r_1 \mid < \mid b \mid$. Por outro lado, $b(q_1 - q_2) = r_2 - r_1$, o que implica que

$$\mid b \mid\mid q_1 - q_2 \mid = \mid r_2 - r_1 \mid \leq \mid b \mid,$$

o que só é possível se $q_1 = q_2$ e consequentemente, $r_1 = r_2$

Definição 2.2. *Dados dois inteiros a e b , com $a \neq 0$ dizemos que a divide b (denotamos $a \mid b$) se existe c inteiro tal que $b = a \cdot c$.*

2.3 Números Primos

Definição 2.3. *Dizemos que um número inteiro positivo p maior que 1 é primo se, e somente se, p possui exatamente dois divisores positivos distintos o 1 e o próprio p e, se o inteiro p admite outros divisores além de 1 e n o mesmo é chamado de composto.*

Exemplo 2.5. O número 2 é primo, pois os divisores positivos de 2 são 1 e o próprio 2 . E mais, 2 é o único número primo par, pois se existe primo par maior que 2, seria da forma $N = 2 \cdot q(q \geq 1)$. Portanto, 1, 2 e q são divisores de N, o que torna absurdo, pois N é primo.

Segue agora uma ilustração (figura 2.1 [1]) com alguns números primos.

Figura 2.1: Números Primos

Fonte: Brasil Escola

2.4 Teorema Fundamental da aritmética

O Teorema Fundamental da aritmética caracteriza todo número em termos de seus constituintes primos.

Teorema 2.1. *Todo inteiro maior que 1 pode ser representado de maneira única(a menos da ordem) como um produto de fatores primo.*

Demonstração 2.5. *Se n é primo não a nada a ser demonstrado. Suponhamos, que n seja composto. Seja $p_1(p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois caso contrário existiria $p, 1 < p < p_1$ com p/n, contradizendo a escolha de p_1. Logo, $n = p_1 \cdot n_1$.*

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos $n = p_1 \cdot p_2 \cdot n_2$.

Repetindo este procedimento, obtemos uma sequencia decrescente de inteiros positivos $n_1, n_2, \ldots n_r$. Como todos eles são inteiros maiores que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, \ldots p_k$, não são, necessáriamente distintos, n terá, em geral, a forma:

[1] Disponível em < http://www.brasilescola.com/matematica/numeros-primos.htm >

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

Unicidade

Para $n = 2$ a afirmação é verdadeira. Assumimos, então que ela se verifica para todos os inteiros maiores que 1 e menores que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_r$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 \cdot q_2 \cdot \ldots \cdot q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalização podemos supor que $p_1 \mid q_1$. Como ambos são primos, isto implica $p_1 = q_1$. Logo $n/p_1 = p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 \cdot p_2 \cdot \ldots \cdot p_s$ e $q_1 \cdot q_2 \cdot \ldots \cdot q_r$ são iguais.

Proposição 2.1. *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

2.5 Congruencia

Grande parte dos resultados desta seção foi introduzida por Gauss(1777 - 1855) em um trabalho publicado em 1801 (*Disquisitiones Arithmeticae*) quando tinha apenas 24 anos, várias idéias de grande importância, que serviram de base para o desenvolvimento da teoria de números. Até mesmo a notação, lá introduzida, é a que utilizamos hoje.

Definição 2.4. *Sejam a e b números inteiros dizemos que a é congruente a b módulo m ($m > 0$) se $m \mid a - b$. Denotamos por $a \equiv b (mod\ m)$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m.*

Proposição 2.2. *Se a e b são inteiros, temos que $a \equiv b (mod\ m)$ se, e somente se, existir um inteiro k tal que $a = b + k \cdot m$.*

Proposição 2.3. *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1. *$a \equiv a (mod\ m)$*
2. *Se $a \equiv b (mod\ m)$, então $b \equiv a (mod\ m)$*
3. *Se $a \equiv b (mod\ m)$ e Se $b \equiv d (mod\ m)$, então Se $a \equiv d (mod\ m)$*

Teorema 2.2. *Se a, b, c e m são inteiros tais que $a \equiv b (mod\ m)$, então:*

1. *$a + c \equiv b + c (mod\ m)$*

2. $a - c \equiv b - c(mod\ m)$

3. $a \cdot c \equiv b \cdot c(mod\ m)$

Teorema 2.3. *Se a, b, c, d e m são inteiros tais que $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então:*

1. $a + c \equiv b + d(mod\ m)$

2. $a - c \equiv b - d(mod\ m)$

3. $a \cdot c \equiv b \cdot d(mod\ m)$

Teorema 2.4. *Se a, b, c e m são inteiros tais que $a \cdot c \equiv b \cdot c(mod\ m)$, então $a \equiv b(mod\ m/d)$ onde $d = (c, m)$*

Definição 2.5. *Se h e k são dois inteiros com $h \equiv k(mod\ m)$, dizemos que k é um resíduo de h módulo m.*

Definição 2.6. *O conjunto dos inteiros $\{r_1, r_2, \ldots, r_s\}$ é um sitema completo de resíduos módulo m se:*

1. *r_i e r_j forem incongruentes módulo m para $i \neq j$*

2. *para todo inteiro n existe um r_i tal que $n \equiv r_i(mod\ m)$.*

Proposição 2.4. *Se a, b, k e m são inteiros com $k > 0$ e $a \equiv b(mod\ m)$, então $a^k \equiv b^k(mod\ m)$.*

2.6 Congruência Linear

Chamamos de congruência linear em uma variável a uma congruência da forma $ax \equiv b(mod\ m)$, onde x é uma incógnita.

Teorema 2.5. *Sejam a e b inteiros e $d = (a, b)$. Se $d \nmid c$ então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d \mid c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (b/d)k$$
$$y = y_0 - (a/d)k$$

onde k é um inteiro.

Teorema 2.6. *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b(mod\ m)$ não possui nenhuma solução e quando $d \mid b$, possui exatamente d soluções incongruentes módulo m.*

Definição 2.7. *Dizemos que uma solução x_0 de $ax \equiv b(mod\ m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m .*

Proposição 2.5. *Sejam $a, m \in \mathbf{Z}$, com $m > 1$. A congruência $aX \equiv 1(mod\ m)$ possui uma solução se, e somente se, $(a, m) = 1$ (máximo divisor comum de a e m for 1). Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0(mod\ m)$.*

Definição 2.8. *Uma solução $\overline{a}$ de $ax \equiv 1(mod\ m)$ é chamada de um inverso de a módulo m.*

Proposição 2.6. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1(mod\ p)$ ou $a \equiv -1(mod\ p)$.*

2.7 Função de Euler

Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m-1$ que são primos com m . Pondo $\varphi(1) = 1$, isso define uma importante função

$$\varphi : \mathbb{N} \to \mathbb{N}$$

chamada *função fi de Euler.*

2.8 Teorema de Fermat

Teorema 2.7. *Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração 2.6. *Se $p = 2$, o resultado é óbvio já que $a^p - a = a(a-1)$ é par. Suponhamos p ímpar. Nesse caso, claramente basta mostrar o resultado para $a \geq 0$. Vamos provar o resultado por indução sobre a.*

O resultado vale claramente para $a = 0$, pois $p \mid 0$.

Supondo o resultado válido para a iremos prová-lo para $a + 1$. Pela fórmula do Binômio de Newton,

$$(a+1)^p - (a+1) = (a^p - a) + [\tbinom{p}{1}a^{p-1} + \ldots + \tbinom{p}{p-1}a].$$

Dessa igualdade, temos que o segundo membro é divisível por p, concluindo assim nossa demonstração.

3 Caracterização dos números primos

3.1 Teorema de Wilson

Nesta seção, vamos provar um teorema atribuído a John Wilson (1741 - 1793), amigo e estudante do matemático inglês Edward Waring (matemático que anunciou o teorema em 1970), mas que, na realidade, o teorema foi provado, pela primeira vez, por J.L. Lagrange(1736-1813).

O teorema de Wilson é uma das fortes ferramentas utilizadas para caraterização dos números primos.

Teorema 3.1. *(Teorema de Wilson) Se p é um número primo, então*

$$(p-1)! \equiv -1(\mod p).$$

Demonstração 3.1. *Como* $(2-1)! \equiv 1(\mod 2) \equiv -1(\mod 2)$, *logo o resultado é válido para* $p = 2$. *Sabemos que* $ax \equiv 1(mod\ p)$ *possui uma única solução para todo* a *no conjunto {1,2,3, ...,(p -2),(p - 1)} e como, destes elementos, somente 1 e* $p-1$ *são seus próprios inversos módulo p, podemos agrupar os números* $2, 3, 4, \ldots, p-2$ *em* $(p-3)/2$ *pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruências, membro a membro, teremos* $2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot (p-2) \equiv 1(\mod p)$. *Multiplicando-se ambos os lados por* $p-1$ *teremos*

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot (p-2)(p-1) \equiv (p-1)(\mod p)$$

Isto é $(p-1)! \equiv -1(\mod p)$ *uma vez que* $p-1 \equiv -1(\mod p)$.

Vale a recíproca do Teorema de Wilson, como veremos a seguir.

Teorema 3.2. *Se n é um inteiro tal que* $(n-1)! \equiv -1(\mod n)$, *então n é primo.*

Demonstração 3.2. *A prova é por contradição. Vamos supor que* $(n-1)! \equiv -1(\mod n)$, *isto é* $n \mid ((n-1)!+1)$ *e que n não seja primo, ou seja,* $n = rs$, $1 < r < n$ *e* $1 < s < n$. *Nestas condições* $r \mid ((n-1)!$ *e, sendo r um divisor de n,* $r \mid (n-1)!+1$ *e, portanto, deve dividir a diferença* $(n-1)!+1-(n-1)! = 1$, *o que é absurdo, uma vez que* $r > 1$. *Logo, um n satisfazendo* $(n-1)! \equiv -1(\mod n)$ *deve ser primo.*

Note que a proposição acima nos dá um critério de primalidade. Para verificar se um número $n > 4$ é primo, basta calcular $(n-1)! + 1$ e verificar se esse número é divisível por n.

O Teorema de Wilson, apesar de ser um ótimo modelo de caracterização de números primos, não é algo tão útil para números muito grandes como, pois não existe um algoritmo, além da definição, para o cálculo de fatorial de números grandes.

Exemplo 3.1. Mostre através do Teorema de Wilson que o número 31 é primo.

Uma Solução

Temos que mostrar que, para $p = 31$, a igualdade $(31-1)! \equiv -1(\mod 31)$

Observe as congruências:

$$1 \equiv 1(\mod 31)$$
$$2 \cdot 16 = 32 \equiv 1(\mod 31)$$
$$3 \cdot 21 = 63 \equiv 1(\mod 31)$$
$$4 \cdot 8 = 32 \equiv 1(\mod 31)$$
$$5 \cdot 25 = 125 \equiv 1(\mod 31)$$
$$6 \cdot 26 = 156 \equiv 1(\mod 31)$$
$$7 \cdot 9 = 63 \equiv 1(\mod 31)$$
$$10 \cdot 28 = 280 \equiv 1(\mod 31)$$
$$11 \cdot 17 = 187 \equiv 1(\mod 31)$$
$$12 \cdot 13 = 156 \equiv 1(\mod 31)$$
$$14 \cdot 20 = 280 \equiv 1(\mod 31)$$
$$15 \cdot 29 = 435 \equiv 1(\mod 31)$$
$$18 \cdot 19 = 342 \equiv 1(\mod 31)$$
$$22 \cdot 24 = 528 \equiv 1(\mod 31)$$
$$23 \cdot 27 = 621 \equiv 1(\mod 31)$$
$$30 \equiv 30(\mod 31)$$

Multiplicando, membro a membro, teremos:

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot 29 \cdot 30 \equiv 30(\mod 31)$$
$$30! \equiv 30(\mod 31) \Rightarrow 30! \equiv -1(\mod 31)$$
$$(31-1)! \equiv -1(\mod 31)$$

Pelo Teorema de Wilson, segue que 31 é primo.

3.2 Propriedade de Giuga

Aqui só iremos apresentar a Propriedade de Giuga, estudo mais detalhado dessa propriedade pode ser encontrada em [9].

Propriedade 3.1. Se p é um número primo, o pequeno teorema de Fermat mostra que:

$$1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv -1(mod\ p)$$

Em 1950, Giuga perguntou se a recíproca é verdadeira: Se $n > 1$ e se n divide $1^{n-1} + 2^{n-1} + \ldots + (n-1)^{n-1} + 1$, n é número primo?

4 Aplicações dos Números Primos

4.1 Criptografia

A Teoria dos Números, da qual a Aritmética é a parte mais elementar, era considerada uma das áreas mais puras e abstratas da Matemática, desprovida de aplicações práticas. Esse panorama muda completamente a partir do desenvolvimento da Teoria da Informação, que compreende a Criptografia entre outros assuntos, motivada pela evolução e popularização dos computadores e a facilidade de conexão com as grandes redes mundiais.

Tradicionalmente, a criptografia era associada aos segredos militares, de Estado e da diplomacia, para os quais foi desenvolvida ao longo de pelo menos dois milênios, mas foi a utilização maciça dos computadores pelas pessoas comuns, para os mais diversos fins, que mais motivou o desenvolvimento da criptografia moderna.

Nosso foco nessa seção é aplicação de números primos, porém faremos um breve histórico da criptografia.

A palavra criptografia origina-se do grego, onde *kriptos* significa oculto e, portanto, a palavra criptografia significa escrita oculta. Tem-se relatos que de que os persas, gregos e chineses utilizavam vários métodos para ocultar mensagens.

Um dos métodos mais famosos de sitemas criptográfico da antiguidade foi um sistema utilizado na Roma antigo por Júlio César, denominado cifra de César. O sitema consiste em substituir cada letra do alfabeto na mensagem original por uma letra do alfabeto, seguindo um padrão bem determinado. Esse tipo de sistema criptográfico é chamado de cifra por substituição simples, onde letras são substituídas por outras.

A principal fraqueza dos sitemas criptográficos por substituição simples é que um texto é que em um texto de uma determinada língua as letras do alfabeto ocorrem com frequências distintas, além de haver certas regras rígidas de contato entre as letras.

A fragilidade desse método custou literalmente o pescoço à rainha da Escócia Maria Stuart(1542 - 1587) que, juntamente com seu aliados, tramavam o assassinato de sua prima, Elizabeth I da Inglaterra, em que a interceptação das mensagens e a análise de frequência permitiu a quebra do seu sigilo e forneceu provas contra Maria, que foi condenada à morte por decaptação.

Para evitar a quebra de de um código por análise de frequência, há uma outra

vertente de sistemas criptográficos que se baseiam na transposição, ou seja, na formação de anagramas da mensagem original. O problema dessa modalidade de cifragem é que a troca de chaves entre usuários do sistema torna-se difícil se há muitos deles.

A combinação dos dois métodos: substituição de letras e transposição de letras pode dar origem a sistemas criptográficos mais robustos.

Em 1466, em pleno renascimento, o arquiteto italiano Leone Battista Alberti, considerado o pai da criptografia ocidental, propôs uma variante bem mais robusta da cifra de César com o uso de um sitema de substituição polialfabética.

O alemão *Johannes Trithemius* publicou em 1518 um livro intitulado *Poliografia*. Nesse livro *Trithemius* propõe o sistema criptográfico a seguir. Forma-se uma tabela, chamada por ele de tabula recta(Figura 4.1 [1]), com o mesmo número de linhas e de colunas, com, na primeira linha, o alfabeto na ordem normal e, em cada uma das linhas seguintes, uma permutação circular da linha anterior. A cifragem procedia da seguinte forma: a primeira letra da mensagem a ser cifrada é transformada na letra correspondente da terceira linha sucessivamente até esgotar todas as linhas quando se volta para a segunda linha novamente.

Assim, por exemplo, a frase

A BELEZA DOS NÚMEROS PRIMOS

é convertida em:

A CGOIEG KWB XFYRFDI GJIGJO

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

Figura 4.1: tabula recta

Fonte: WIKIPEDIA

Todos esses sitemas criptográficos caracterizam-se pelo uso de chaves simétricas, ou seja, a mesma chave é usada para cifrar e e decifrar uma dada mensagem.

[1] Disponível em: < http://en.wikipedia.org.wiki/Tabula_recta >

A chegada dos telégrafos e finalmente dos computadores revolucionaram a Teoria da Informação. Em 1973, O *National Bureau of Standadrds*, órgão governamental americano, escolheu o sistema criptográfico *Data Encryption Standard* (DES), desenvolvida pela IBM, para ser o sitema oficial americano. Esse sistema, utilizado até 1999, era bastante complexo e funcionava com uma distribuição de chaves simétricas. Hoje em dia são utilizados outros sistemas como o *Advanced Encryption Standard* (AES) ou *Skipjack*, esse último desenvolvido pela *U.S National Security Agency*.

A Teoria dos números, através da noção de congruências, começa a entrar no campo da criptografia quando três norte-americanos, *Whitfield Driffie*,*Martin Hellman* e *Ralph Merkle* desenvolveram um sistema de troca de informações tornando pública algumas informações e secretas outras. Esse método pode ser descrito como segue:

Duas pessoas querem trocar certa informação, elas escolhem em comum um par de números naturais a e m (informações públicas). A primeira escolhe um outro número natural p_1 (secreto). Com ele, calcula o único número $b_1 < m$ tal que $a^{p_1} \equiv b_1(mod\ m)$ e o envia para a segunda pessoa. Por sua vez, a outra pessoa escolhe um número natural p_2 (secreto), e com ele calcula o único número $b_2 < m$ tal que $a^{p_2} \equiv b_2(mod\ m)$, e o envia para a primeira pessoa.

Em seguida, a primeira pessoa calcula $b_2^{p_1}$, obtendo:

$$b_2^{p_1} \equiv (a^{p_2})^{p_1} \equiv a^{p_2 p_1} \equiv c(mod\ m), com\ \mathrm{c} < \mathrm{m}\ .$$

Por sua vez, a segunda pessoa calcula $b_1^{p_2}$, obtendo:

$$b_1^{p_2} \equiv (a^{p_1})^{p_2} \equiv a^{p_1 p_2} \equiv c(mod\ m), com\ \mathrm{c} < \mathrm{m}\ .$$

Sendo c a chave secreta entre as duas pesssoas.

Os números primos ganham relevância no sistema criptográfico em 1978 quando *Ronald Rivest*, *Adi Shamir* e *Leonard Adleman*, do Laboratório de Ciências da Informação do *Massachusetts Institute of Technology* (MIT), tiveram a ideia de implementar o sistema criptográfico com chaves assimétricas, idealizado por *Driffie*.

O princípio basea-se na relativa facilidade em encontrar números primos grandes e ao mesmo tempo na dificuldade prática em fatorar o produto de dois desses números.

O sistema criptográfico (RSA) funciona da seguinte forma:

Suponhamos que uma pessoa queira cifrar um sistema criptográfico em que qualquer pessoa possa lhe enviar uma mensagem cifrada segundo uma chave pública e que, ele, possa decifrá-lo com a sua chave secreta. Essa pessoa escolhe dois números primos distintos p e q muito grandes e efetua o seu produto $m = p \cdot q$. Note que que é fácil calcular o número m e extremamente difícil fatorar o número m.

Em seguida essa pessoa escolhe um par de números a e b tais que:

$$a \cdot b \equiv 1(mod\ \varphi(m))$$

Note que obrigatoriamente $(a, \varphi(m)) = (b, \varphi(m)) = 1$. A primeira pessoa pode escolher inicialmente a tal que $(a, \varphi(m)) = 1$ e em seguida resolver a congruência $aX \equiv 1(mod\ \varphi(m))$

A primeira pessoa torna públicos os números m e b, que são a chave pública. A chave secreta dela serão os primos p e q, os números $\varphi(m) = (p-1)(q-1)$ e a .

Dado um número $x < m$, a codificação feita pela segunda pessoa que conheça a chave pública da primeira pode cifrar x como segue:

A segunda pessoa acha acha o único $C(x) < m$ tal que:

$$x^b \equiv C(x)\ (mod\ m).$$

A segunda pessoa envia $C(x)$ para a primeira.

A primeira, ao receber $C(x)$, usa a sua chave privada a para achar o número $D(C(x)) < m$ tal que

$$C(x)^a \equiv D(C(x))(mod\ m).$$

Note que somente a primeira pessoa consegue determinar $D(C(x))$, pois só ele detém a chave a. Mas, $D(C(x)) = x$, pois existe $k \in \mathbb{N}$ tal que $a \cdot b = 1 + k \cdot \varphi(m)$ e, temos que:

$$D(C(x)) \equiv C(x)^a \equiv (x^b)^a = x^{a \cdot b} = x^{1+k \cdot \varphi(m)} \equiv x(mod\ m)$$

A geniosidade desse método consiste no uso de números primos grandes e uso de chaves escolhidas com certos critérios.

Para melhor entendimento, iremos exemplificar

Suponha que João usa a senha 102 - 224 para se comunicar com Maria, que por sua vez enviará uma mensagem codificada para João que só ele poderá decodificar essa mensagem (encontrando a senha 102 - 224).

Suponhamos que João queira cifrar um sistema criptográfico em que qualquer pessoa possa lhe enviar uma mensagem cifrada segundo uma chave pública e que, ele, possa decifrá-lo com a sua chave secreta. João escolhe números primos distintos $p = 17$ e $q = 23$ (Colocamos como exemplo números pequenos mais o RSA opera com números primos muito grandes), e efetua o produto entre esses números para encontrar o valor de m , logo $m = 17 \cdot 23 = 391$ e calcula o valor de $\varphi(391)$, da seguinte maneira:

$$\varphi(391) = (17-1) \cdot (23-1) = 352.$$

Em seguida João escolhe, por exemplo, o par de números $a = 235$ e $b = 3$, essa escolha não é feita de maneira aleatória, mas obdece a igualdade:

$$3 \cdot 235 \equiv 1(mod\ \varphi(391)).$$

Note que obrigatoriamente $(3, 352) = (235, 352) = 1$. João pode escolher inicialmente $a = 235$ tal que $(3, 352) = 1$ e em seguida resolver a congruência $235X \equiv 1(mod\ 352)$.

João torna públicos os números $m = 391$ e $b = 3$, que são a chave pública. A chave secreta dele serão os primos $p = 17$ e $q = 23$, os números $\varphi(391) = (17 - 1) \cdot (23 - 1) = 352$ e $a = 235$.

A codificação feita pela segunda pessoa que conheça a chave pública da primeira pode cifrar essas informações como segue:

Maria acha os únicos $C(102)$ e $C(224)$, da seguinte maneira:

$$102^3 \equiv C(102)\ (mod\ 391\ )$$
$$24276 \equiv 34(mod\ 391)$$
$$C(102) = 34$$

$$224^3 \equiv C(224)\ (mod\ 391\ )$$
$$11239424 \equiv 129(mod\ 391)$$
$$C(224) = 129$$

Pronto a senha 102 - 224 é codificada por Maria em 34 - 129.

Maria agora envia o código 34 - 129 para João.

João, ao receber o código 34 - 129 , usa a sua chave privada $a = 235$ para achar os número $D(34)$ e $D(129)$, da seguinte forma:

$$34^{235} \equiv D(34)(mod\ 391)$$
$$34^{235} \equiv 102(mod\ 391)$$
$$D(34) \Rightarrow 102$$

$$129^{235} \equiv D(129)(mod\ 391)$$
$$129^{235} \equiv 224(mod\ 391)$$
$$D(129) \Rightarrow 224$$

João ao receber o código 34 - 129 de alguma pessoa, ao decodificar esse código encotrará o código 102 - 224 e logo saberá que foi Maria que lhe enviou o código.

Pronto! Genial

Note que somente João consegue determinar $D(C(34))$ e $D(C(129))$, pois só ele detém a chave $a = 235$.

4.2 Existem fórmulas que geram primos ?

A partir da observação dos números primos, encontrar fórmula(s) que geram todos os números primos e somente estes, tornou-se um dos principais desafios aos estudiosos da matemática da área da Teoria dos números.

No artigo 329 das *Disquisitiones Arithmeticae*, GAUSS escreveu:

> O problema de distinguir os números primos dos números compostos e de exprimir estes últimos à custa de seus fatores primos deve ser considerado como um dos mais importantes e dos mais úteis em Aritmética . . . . A própria dignidade da ciência requer que todos os meios possíveis sejam explorados para a resolução de um problema tão elegante e tão famoso.[9]

A sequência dos números primos apresenta uma forma bem interessante, encontrar uma fórmula ou polinômio em função de uma única variável, caso exista, que gera os primos, é um grande desafio para os matemáticos desde muito tempo.

Vejamos uma representação geométrica(Figura 4.2 [2]) dos primeiros números primos:

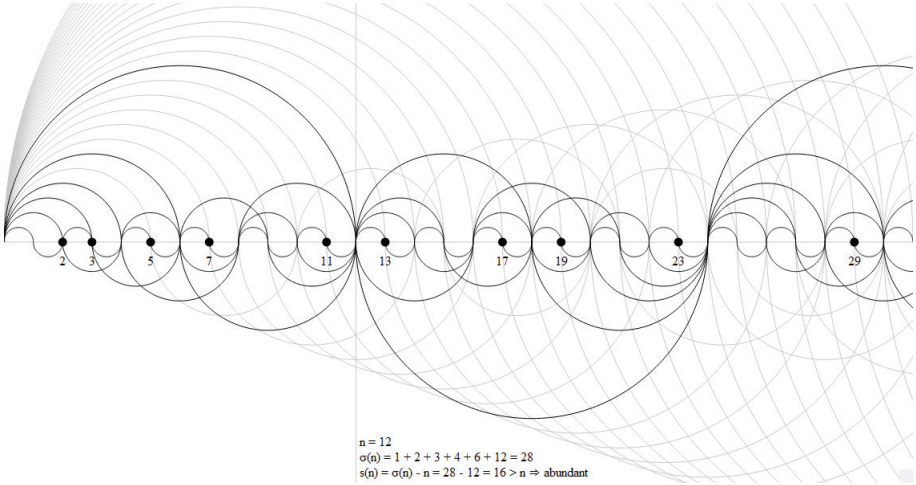

Figura 4.2: El patrón de los Números Primos - Jason Davies

A seguir listaremos algumas fórmulas que geram números primos.

1. (Teorema de Euler) Euler descobriu em 1972 um polinômio tendo uma longa sucessão de valores primos. Para esses poliômios, existem números naturais m e n, com $0 \leq m < n$ (e n - m não muito pequeno), tais que $f(k)$ seja primo, para todo k, com $m \leq k \leq n$.

   Este é o famoso Teorema de Euler

   Teorema 4.1. *Seja* $f(X) = X^2 + X + 41$. *Para* $k = 0, 1, 2, 3, \ldots, 39$, *todos seus valores são números primos, a saber: 41, 43, 47, 53, 61, 71 ,83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 e 1601. Para* $k = 40$ *o valor é* $1681 = 41^2$ *(número composto).*

   Faremos uma observação bem interessante sobre a sequência dos números primos obtidos a partir do polinômio descoberto por Euler.

[2] Disponível em: < https://thequantumfantastic.word-press.com/2012/07/20/prime-number-patterns/ >

Fazendo $a_1 = 41$, $a_2 = 43$, $a_3 = 47$, $a_4 = 53$, $a_5 = 61$, $a_6 = 71$, $a_7 = 83$, $a_8 = 97$, $a_9 = 113$, $a_{10} = 131$, $a_{11} = 151$, $a_{12} = 173$, $a_{13} = 197$, $a_{14} = 223$, $a_{15} = 251$, $a_{16} = 281$, $a_{17} = 313$, $a_{18} = 347$, $a_{19} = 383$, $a_{20} = 421$, $a_{21} = 461$, $a_{22} = 503$, $a_{23} = 547$, $a_{24} = 593$, $a_{25} = 641$, $a_{26} = 691$, $a_{27} = 743$, $a_{28} = 797$, $a_{29} = 853$, $a_{30} = 911$, $a_{31} = 971$, $a_{32} = 1033$, $a_{33} = 1097$, $a_{34} = 1163$, $a_{35} = 1231$, $a_{36} = 1301$, $a_{37} = 1373$, $a_{38} = 1447$, $a_{39} = 1523$, e $a_{40} = 1601$.

A sequência (S_n), com $n \in \mathbb{N}$, formada pela diferênça entre os termos consecutivos será:

$$S_n = \{a_2 - a_1, a_3 - a_2, a_4 - a_3, \ldots, a_{40} - a_{39}\}.$$

$$S_n = \{2, 4, 6, \ldots, 78\}.$$

Notamos que a sequência S_n é uma progressão aritmética de primeiro termo 2, de razão 2 e último termo sendo 78, ou seja, cada termo da sequência S_n é do tipo $2n + 39$. A sequência dos números primos, obtidos a partir do polinômio descoberto por Euler, formam uma progressão aritmética de segunda ordem.

Teorema 4.2. *(Caracterização das Funções Quadráticas) A fim de que a função contínua $f : \mathbb{R} \to \mathbb{R}$ seja quadrática é necessãrio e suficiente que toda progressão aritmética não-constante seja transformada por f numa progressão aritmética de segunda ordem não-degenerada.*

Não faremos aqui a demonstração desse teorema, mas ela pode ser encontrada em [5].

Esse teorema mostra que existe uma função quadrática para a sequência dos números primos obtidos a partir do polinômio descoberto por Euler.

Vimos, no início dessa seção, que para $k = 40$ o valor é $1681 = 41^2$ (número composto), note que a diferença 1681 - 1601 = 80 não pertence a sequência S_n, pois teríamos:

$$2n + 39 = 80$$

$$n = \frac{41}{2} \text{ (contradizendo o fato de } n \text{ ser um número natural).}$$

2. O polinômio quadrático $f(X) = 36X^2 - 810X + 2753$, descoberto por *R. Ruby*, em 1990, é presentemente o que fornece a mais longa sucessão $| f(k) |$ (para $k = 0, 1, 2, 3, \ldots, 44$) de valores absolutos primos iniciais.

3. Os polinômio $103X^2 - 3945X + 34381$ de *R. Ruby* e $47X^2 - 1701X + 10181$ de *G. Fung* dão, cada um deles 43 valores absolutos primos iniciais.

4. Fórmulas Polinomiais

- $F_n = n^2 + n + 41$, $0 \leq n \leq 39$
- $F_n = 2n^2 + 29$, $0 \leq n \leq 28$
- $F_n = 3n^2 + 3n + 23$, $0 \leq n \leq 21$

5. Para polinômios de grau superior, *DRESS* e *LANDREAU* acharam em 2003 os dois polinômos seguintes:

   $f(X) = 66x^3 + 83X^2 - 13735X + 30139$ com 46 primos $\mid f(k) \mid$ para k de - 26 a 19,

   $f(X) = 16x^4 + 28x^3 + 1685X^2 - 23807X + 110647$ com 46 primos $\mid f(k) \mid$ para k de - 2 a 22,

   O que essas funções ou expressões polinomiais possuem em comum é o fato de k pertencer a um intervalo limitado, ou seja, para alguns valores encontraremos números compostos.

   Mais a pergunta é

Existe(m) ou não fórmula(s) fechadas para encontrar ou gerar números primos?

Teorema 4.3. *Sejam x e $y \in \mathbb{N}$, com $y \neq 0$ e $a = x(y+1) - (y!+1)$.*

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

Composta de duas variáveis e a um número que depende das mesmas.

Demonstração 4.1. *Mostraremos que , dada a função $f(x,y) = \frac{y-1}{2}[\mid a^2 - 1 \mid -(a^2-1)] + 2$ é um número primo e que dado um primo p existem x e $y \in \mathbb{N}$, tal que $f(x,y) = p$, isto é, precisaremos mostrar que:*

a)$f(x,y)$ é sempre um número primo.

- *O número a é um número inteiro e, portanto, a^2 é inteiro. Há dois casos:*

$$a^2 \geq 1 \text{ ou } a^2 = 0$$

- *Se $a^2 \geq 1$, $\mid a^2 - 1 \mid = a^2 - 1$ e $f(x,y) = 0 + 2 = 2$(número primo).*

- *Se $a^2 = 0$,*

  $a^2 = 0 \Rightarrow f(x,y) = \frac{y-1}{2}[\mid 0 - 1 \mid -(0-1)] + 2 = \frac{y-1}{2} \cdot 2 + 2 = y + 1$ e, de $a^2 = 0 \Rightarrow a = 0$, temos que: $x(y+1) - (y!+1) = 0 \Rightarrow x(y+1) = (y!+1)$

  Pelo Teorema de Wilson (visto no capítulo 3) temos que se p é primo se, e somente se, p divide $(p-1)! + 1$, fazendo $p - 1 = y \Rightarrow p = y + 1$, daí $f(x,y)$ é um número primo sempre que $y + 1$ for primo.

b) $f(x, y)$ fornece todos os números primos.

- *Seja p um número primo. Pelo Teorema de Wilson, temos que p divide o número $(p-1)!+1$, ou seja, o número $\dfrac{(p-1)!+1}{p}$ é um número natural e podemos calcular $f(\dfrac{(p-1)!+1}{p}, p-1)$.*
- *O valor de a é:*
  $a = \dfrac{(p-1)!+1}{p} \times p - [(p-1)!+1]$.
  $a = (p-1)! + 1 - (p-1)! - 1$
  $a = 0$
  Segue-se que:
  $f(\dfrac{(p-1)!+1}{p}, p-1) = p - 1 + 1 = p$.

Vejamos os seguintes exemplos:

Exemplo 4.1. Encontre o valor de $f(x, y)$, se $x = 1$ e $y = 1$.

- Encontraremos inicialmente o valor do número inteiro a.

$$a = x(y+1) - (y! + 1)$$
$$a = 1(1+1) - (1! + 1)$$
$$a = 1(2) - (2)$$
$$a = 0$$

- Fazendo $x = 1$, $y = 1$ e $a = 0$ e aplicando na fórmula, esses valores, teremos:

$$f(1,1) = \frac{1-1}{2}[|\ 0^2 - 1\ | - (0^2 - 1)] + 2$$
$$f(1,1) = \frac{0}{2}[2] + 2$$
$$f(1,1) = 0 + 2$$
$$f(1,1) = 2$$
$$f(1,1) = 2;$$

Exemplo 4.2. Encontre o valor de $f(x, y)$, se $x = 1$ e $y = 2$.

- Encontraremos inicialmente o valor do número inteiro a.

$$a = x(y+1) - (y!+1)$$
$$a = 1(2+1) - (2!+1)$$
$$a = 1(3) - (3)$$
$$a = 0$$

- Fazendo $x = 1$, $y = 2$ e $a = 0$ e aplicando na fórmula, esses valores, teremos:

$$f(1,2) = \frac{2-1}{2}[|\ 0^2 - 1\ |\ -(0^2 - 1)] + 2$$
$$f(1,2) = \frac{1}{2}[2] + 2$$
$$f(1,2) = 1 + 2$$
$$f(1,2) = 3$$

Exemplo 4.3. Encontre o valor de $f(x,y)$, se $x = 1$ e $y = 3$.

- Encontraremos inicialmente o valor do número inteiro a.

$$a = x(y+1) - (y!+1)$$
$$a = 1(3+1) - (3!+1)$$
$$a = 1(4) - (7)$$
$$a = -3$$

- Fazendo $x = 1$, $y = 3$ e $a = -3$ e aplicando na fórmula, esses valores, teremos:

$$f(1,3) = \frac{3-1}{2}[|\ (-3)^2 - 1\ |\ -((-3)^2 - 1)] + 2$$
$$f(1,3) = \frac{2}{2}[0] + 2$$
$$f(1,3) = 0 + 2$$
$$f(1,3) = 2$$

Exemplo 4.4. Encontre o número primo 7, usando a fórmula $f(x,y) = \frac{y-1}{2}[|\ a^2 - 1\ | -(a^2 - 1)] + 2$.

Solução

Encontrando os naturais x e y tais que:

- $x = \frac{(p-1)!+1}{p}$

$$x = \frac{(7-1)!+1}{7}$$

$$x = \frac{(6)! + 1}{7}$$
$$x = \frac{720 + 1}{7}$$
$$x = \frac{721}{7}$$
$$x = 103$$

- $y = p - 1$

$$y = 7 - 1$$
$$y = 6$$

Calculando o valor de $f(103, 6)$ pela fórmula, teremos:

- Encontrando o valor do número inteiro a, segue:

$$a = 103(6 + 1) - (6! + 1)$$
$$a = 103(7) - (720 + 1)$$
$$a = 721 - 721$$
$$a = 0$$

- Fazendo $x = 103$, $y = 6$ e $a = 0$ e aplicando na fórmula, esses valores, teremos:

$$f(103, 6) = \frac{6 - 1}{2}[\mid 0^2 - 1 \mid -((0^2 - 1)] + 2$$
$$f(103, 6) = \frac{5}{2}[2] + 2$$
$$f(103, 6) = 5 + 2$$
$$f(1, 3) = 7$$

Não se trata de uma fórmula prática, entretanto ela tem uma forte relação com o número 2. Além disso, mesmo para produzir primos pequenos, começamos a ter dificuldades.

O que acabamos de mostrar é que existe fórmula para gerar números primos, e vale salientar que essa não é a única, existem outras fórmulas que geram números primos com mais de uma variável.

4.3 Construção de Polígonos Regulares

Nos tempos modernos, o termo construção em geometria plana se tornou praticamente sinônimo de construção com régua e compasso.

Durante o século dezenove várias outras construções equivalentes à construção com régua e compasso foram descobertas, por exemplo, construções com régua e dois círculos fixos que se intersectam.

A caractrerização das construções possíveis e impossíveis deu origem a considerações de interesses matemáticos maior. Citaremos somente um resultado, devido essencialmente ao grande matemático alemão *C.F Gauss*(1777 - 1855). O teorema está relacionado com o problema de saber que polígonos regulares são construtíveis e afirma que:

Teorema 4.4. *Um polígono regular de n lados pode ser construído com régua e compasso se, e somente se, ou $n = 2^\alpha$ ou*

$$n = 2^\alpha \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r$$

onde $p_1, p_2, \ldots, p_r$ são números distintos da forma

$$p = 2^{2^\beta} + 1$$

com α e β são inteiros ≥ 0.

Alguns comentários sobre este teorema são apropriados. Sua demosntração é por demais complexa para ser apresentada aqui; é suficiente dizer que *Gauss* percebeu a conexão entre o problema geométrico de dividir um círculo em n partes iguais e o problema algébrico de resolver a equação

$$x^n = 1.$$

Com efeito, as n raízes desta equação, quando marcadas no plano complexo, formam os vértices de um polígono regular de n lados inscritos no círculo unitário.

Mas vejamos o que diz o teorema. O fator 2^α é fácil de compreender, pois se pudermos construir um certo polígono regular, podemos construir imediatamente um com duas vezes este número de lados, dividindo simplesmente ao meio todos os arcos do círculo circunscrito.

5 Curiosidades e Mistérios sobre os Números Primos e sugestão de atividade

5.1 Curiosidades e Mistérios

1. Cigarras usam números primos

   O ataque das cigarras como tem sido chamada a emergência sincronizada de algumas espécies do inseto, num ciclo exato de 17 anos pode ser resultado não do acaso, mas sim de uma forte pressão seletiva. É o que sugere um estudo de pesquisadores brasileiros, que aponta uma solução para o mistério que tem encantado os americanos nas últimas semanas.

   A pesquisa faz uso das possibilidades de simular em computador o processo de evolução por seleção natural, área de estudo chamada genericamente de "vida digital". A ideia é criar uma espécie de videogame em que criaturas são simuladas por programas. Elas se reproduzem e sobrevivem como coisas vivas, de acordo com a maior ou menor adaptação.

   No caso das cigarras, os pesquisadores conceberam um modelo que mostrasse como poderia emergir o estranho padrão desses insetos. Muitas espécies de cigarra têm períodos diferentes de amadurecimento, com ciclos vitais de duração variada, enquanto as larvas ficam sob a terra. Mas sete espécies do gênero Magicicada têm uma característica adicional: elas são sincronizadas, ou seja, saem do chão todas ao mesmo tempo, para cerca de duas semanas de canto ensurdecedor, acasalamento e postura de ovos.

   Para esses grupos sincronizados, é curioso notar que os ciclos normalmente acontecem em 13 ou 17 anos. São números primos, ou seja, divisíveis apenas por si mesmos e por um.

   É difícil acreditar que a natureza tenha escolhido aleatoriamente esses números para as cigarras.

2. Conjectura de Goldbach

   Goldbach entrou para a história da Matemática com mais uma de suas perguntas. Em uma carta escrita em 7 de junho de 1724, pergunta a Euler se seria possível escrever qualquer número inteiro maior do que dois como a soma de três primos. Goldbach considerava o número 1 como primo, coisa que não fazemos mais. Euler representou a pergunta da seguinte forma: seria possível escrever qualquer número inteiro par maior que 2 como a soma de dois números primos? Por exemplo: $12 = 7 + 5$; $14 = 11 + 3$ e $1248 = 337 + 911$. Essa questão continua, até a apresentação desse trabalho, desafiando os praticantes de teoria dos números até esse momento!

3. Recordes

   - O maior número de FERMAT primo conhecido é $F_4 = 65637$
   - Até hoje são conhecidos 47 números de MERSENNE m_q que são primos. O maior deles com $q = 43112609$, tem 12978189 algarismos. Foi descoberto em 2008 por E.SMITH, G.F WOLTMAN, . KUROWSKI e GIMPS.
   - Os primos de *Sophie Germain*: p é um primo de SOPHIE GERMAIN se $2p + 1$ é também número primo.

     Sophie Germain demonstrou o seguinte Teorema:

     Se p é um número primo de SOPHIE GERMAIN, então não existem inteiros x, y e z, diferentes de zero e não múltiplos de p, tais que $x^p + y^p = z^p$.

     O maior número de SOPHIE GERMAIN conhecido é $183027 \times 2^{265540} - 1$ descoberto por T.WU e J. PENNÉ em 2010.

5.2 Sugestão de Atividade

Esta seção é destinada a uma proposta de atividade sobre números primos voltada para estudantes de matemática do Ensino Fundamental e/ou Ensino Médio, alguns dos problemas a seguir foram selecionados de agumas referências sobre olimpíadas de Matemática. As soluções dos problemas aqui propostos seguem nos anexos.

1. (QUESTÃO 47 NÍVEL 2 - BQ 2011)

   Primos Não!

   (a) Prove que o número 3999991 não é primo.

   (b) Prove que o número 1000343 não é primo

2. (QUESTÃO 03 NÍVEL 1 - BQ 2009)

   O caminho da Joaninha - Dona Joaninha quer atravessar um pátio com azulejos quadrados numerados como mostra a figura [1]. Ela vai partir do ponto P e quer chegar ao ponto C andando somente sobre os lados dos azulejos. Dona Joaninha não quer ter números primos à sua direita ao longo de todo o percurso. Qual é o menor percurso que ela pode fazer?

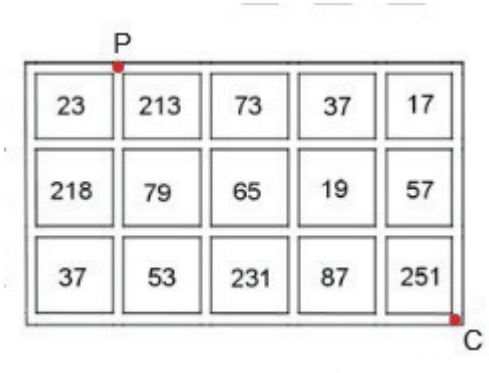

Figura 5.1: O caminho da Joaninha

Fonte: BANCO DE QUESTÕES(BQ) - OBMEP

3. (XXVI OBM - PROBLEMAS NÍVEL 1 PARTE A)

   A soma de dois números primos a e b é 34 e a soma dos primos a e c é 33. Quanto vale a + b + c?

4. Sequência de Fibonacci - O nome sequência de Fibonacci, foi dado pelo matemático francês Edouard Lucas no século XIX. Porém, a sequência surgiu de um problema que estava proposto na obra "Liber Abaci"de Leonardo de Pisa (1180 - 1250), conhecido como Fibonacci. O problema era o seguinte: "Um homem põe um casal de coelhos dentro de um cercado. Quantos pares de coelhos serão produzidos em um ano, se a natureza desses coelhos é tal que a cada mês um casal gera um novo casal, que se torna fértil a partir do segundo mês?"Depois de séculos de trabalho, é possível hoje citar uma quantidade enorme de propriedades da sequência do número de coelhos existentes após n meses. Definição

   A sequência de Fibonacci é definida da seguinte maneira: $f_1 = f_2 = 1$ e $f_n = f_{n-1} + f_{n-2}$, $\forall\, n > 2$. Encontre os 7 primeiros números primos que pertencem a Sequência de Fibonacci.

5. (XXVII OBM - PRIMEIRA FASE - NÍVEL 1)

[1] Disponível em < http://www.obmep.org.br/bq/bq2009.pdf >

O número 10 pode ser escrito de duas formas como soma de dois números primos: $10 = 5 + 5$ e $10 = 7 + 3$. De quantas maneiras podemos expressar o número 25 como uma soma de dois números primos?

6. (QUESTÃO 02 - REVISTA DA OLIMPÍADA - OLIMPÍADA DE MATEMÁTICA DO ESTADO DE GOIÁS - Nº4 Abril/2003)

   Durante uma aula, perguntado sobre o dia de seu aniversário, o professor de Matemática disse:

   O dia em que nasci é um número primo maior do que o quadrado e menor que o cubo do mês em que nasci. A soma do dia com o mês também dá um número primo, mas a diferença não.

   Em que dia ele faz aniversário?

7. Mostre usando o Teorema de Wilson que o número 13 é primo.

6 Considerações Finais

O presente trabalho apresentou um pequeno relato histórico sobre os números primos, caracterização e algumas aplicações dos mesmos, mostrou-se que os números primos possuem uma grande importância, principalmente no sistema de informações. Apresentou também uma série de situações - problemas selecionados de tal forma que o leitor sinta-se motivado a respondê-los.

A expectativa é que esse material possa servir como referência ou apoio na construção de uma sequência didática inovadora no sentido de buscar uma motivação dos alunos da Educação Básica e / ou Superior . Podemos, então, destacar a importância desse trabalho pelo fato do mesmo apresentar uma relação com outras áreas do conhecimento.

Por não conhecer até hoje uma expressão, que depende apenas de uma variável inteira, e por saber que não existe fórmula polinomial de coeficientes inteiros que gere todos os primos e somente estes(demonstrado em [9]), chegamos à conclusão que a fórmula apresentada nesse trabalho é de grande valia para quem a não conhece.

Neste trabalho apresentamos uma atividade, relacionada ao tema, tendo como referência Olimpíadas de Matemática, pois acreditamos que as Olimpíadas de Matemática podem ser um diferencial na vida escolar de um jovem e de uma criança e que pode abrir portas para o conhecimento despertando o interesse dos mesmos pela matemática.

Busca-se nesse trabalho despertar o interesse dos alunos, ou seja , motiva-los a buscar o conhecimento a partir de uma nova abordagem baseada na história e nas aplicações dos números primos.

Este trabalho apresenta, também, uma série de curiosidades e mistérios sobre os números primos despertanto ainda mais o interesse pelo tema abordado.

Posteriormente, pretende-se que o resultado deste estudo seja socializado através de oficinas e /ou formação continuada junto aos professores de matemática da Educação Básica, de modo a proporcionar a estes um aprofundamento sobre o tema abordado.

Referências

[1] BRASIL, Ministério da Educação. Secretaria de Educação Fundamental. - *Parâmetros Curriculares Nacionais* .(5ª a 8ª séries). Brasília: MEC, 1998.

[2] COUTINHO, S. C - *Criptografia* . Rio de Janeiro . 2008.

[3] FOLHA ON LINE. - *São Paulo. Diário. Disponível em: <http://www1.folha.uol.com.br/folha/ciencia/ult306u11973.shtml>.* Acesso em: 09 de jan. 2015

[4] HEFEZ, Abramo - *Aritmética*. Rio de Janeiro: SBM, 2013.

[5] LIMA, Elon Lages; CARVALHO, Paulo Cezar Pinto; WAGNER, Eduard; MORGADO, Augusto César. - *A Matemática do Ensino Médio*.Volume 1. Rio de Janeiro: SBM,9ª Ed., 2000.

[6] MARTINEZ, F.B.; [ET AL - *Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro: IMPA, 2013.

[7] MOREIRA, Carlos Gustavo T. de A; MARTÍNEZ, Fabio E. Brochero; SALDANHA, Nicolau C. - *Tópicos de Teoria dos Números*. Rio de Janeiro: SBM, 2012.

[8] *OLIMPÍADA BRASILEIRA DE MATEMÁTICA - OBM*, < http://www.obm.org.br. Acesso em: 27 de dez. 2014.

[9] RIBENBOIM, Paulo - *Números Primos: Velhos Mistérios e Novos Recordes*. 1ª ed. Rio de Janeiro:IMPA, 2014(Coleção Matemática Universitária).

[10] SANTOS, José Plíno de Oliveira - *Introdução à Teoria dos Números*. 3ª ed. Rio de Janeiro:IMPA, 2012.

[11] SINGH, Simon - *O ÚLTIMO TEOREMA DE FERMAT*. Rio de Janeiro . São Paulo : Record, 2008.

[12] SOCIEDADE BRASILEIRA DE MATEMÁTICA (SBM) - *Olimpíada Brasileira de Matemáticas das Escolas Públicas (OBMEP)*. Banco de questões 2009.

[13] SOCIEDADE BRASILEIRA DE MATEMÁTICA (SBM) - *Olimpíada Brasileira de Matemáticas das Escolas Públicas (OBMEP)*. Banco de questões 2011.

[14] WATANABE, Renate G. - *UMA FÓRMULA PARA NÚMEROS PRIMOS*. RPM 37 - 1998, PP.19 - 21.

A Título do Primeiro Apêndice

A.1 Soluções dos problemas propostos no capítulo 5

Sabemos que existem várias maneiras de analisar problemas. Aqui apresentaremos uma solução para cada problema, tendo em vista a possibilidade de outras soluções.

1. Problema

   Solução

   (a) Observe que:

   $$\begin{aligned}3999991 &= 4000000 - 9\\ &= 4 \cdot 10^6 - 3^2\\ &= (2 \cdot 10^3)^2 - 3^2\\ &= (2 \cdot 10^3 - 3) \cdot (2 \cdot 10^3 + 3)\\ &= 1997 \cdot 2003\end{aligned}$$

   e portanto não é um número primo.

   (b)Observe que:

   $$\begin{aligned}1000343 &= 10^6 + 7^3\\ &= (10^2)^3 + 7^3\\ &= (10^2) + 7) \cdot ((10^2)^2 - 10^2 \cdot 7 + 7^2)\\ &= 107 \cdot 9349\end{aligned}$$

   e portanto não é um número primo.

2. Problema

   Solução

   Os números primos que aparecem na tabela são 23, 73, 37, 17, 79, 19, 37, 53 e 251, logo, o caminho a ser percorrido pela Joaninha está descrito na figura A.1[1].

[1]Disponível em < http://www.obmep.org.br/bq/bq2009.pdf >

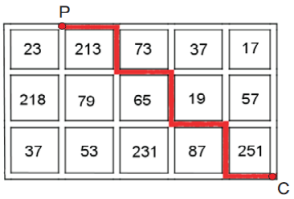

Figura A.1: O caminho da Joaninha - Solução

3. Problema

Solução

$$a + b = 34$$
$$a + c = 33$$

Logo:

$$b - c = 1$$

Como b e c são primos, concluímos que $b = 3$ e $c = 2$.

Dessa forma,

$$a + 3 = 34 \Rightarrow a = 31,$$

de onde vem:

$$a + b + c = 31 + 2 + 3 = 36$$

4. Problema

Solução

A solução desse problema consiste em listar os números da Sequência de Fibonacci, através da definição.

A sequência de Fibonacci é definida da seguinte maneira: $f_1 = f_2 = 1$ e $f_n = f_{n-1} + f_{n-2}, \forall\ n > 2$.

Usando a definição podemos listar os primeiros números da sequência, como segue:

$$(1,\ 1,\ 1\ +1,\ 1\ +\ (\ 1\ +\ 1\ ),\ ...\ )$$
$$(1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,\ 233,\ 377,\ 610,\ 987,\ 1597,\ 2584.\ \ldots)$$

Porém o problema consiste em encontrar os 7 primeiros números da sequência de Fibonacci que são primos, que listaremos a seguir.

$$2,\ 3,\ 5,\ 13,\ 89,\ 233 \text{ e } 1597.$$

5. Problema

Solução

Responder esse problema consiste em encontrar dois números primos que a soma seja 25.

Podemos escrever 25 como:

$$1 + 24 = 25 \text{ (Ambos não primos)}$$
$$2 + 23 = 25 \text{ (Ambos primos)}$$
$$3 + 22 = 25 \text{ (22 número composto)}$$
$$4 + 21 = 25 \text{ (Ambos não primos)}$$
$$5 + 20 = 25 \text{ (20 número composto)}$$
$$6 + 19 = 25 \text{ (6 número composto)}$$
$$7 + 18 = 25 \text{ (18 número composto)}$$
$$8 + 17 = 25 \text{ (8 número composto)}$$
$$9 + 16 = 25 \text{ (Ambos compostos)}$$
$$10 + 15 = 25\text{(Ambos compostos)}$$
$$11 + 14 = 25\text{(14 número composto)}$$
$$12 + 13 = 25\text{(12 número composto)}$$

Daí em diante a sequência volta a se repetir, sendo trocada apenas a ordem das parcelas em cada soma.

Portanto 25 é escrito de uma única maneira como soma de dois números primos.

6. Problema

Solução

As condições enunciadas para achar o dia (d) e o mês (m) são:

(1) d é um número primo.

(2) $d > m^2$

(3) $d < m^3$.

(4) $(d + m)$ é um número primo.

(5) $(d - m)$ não é número primo.

Para satisfazer ás condições (1), (2) e (3), os dias possíveis são:

- Fevereiro - $2^2 <$ dia primo $< 2^3$, dias e meses possíveis: 5/2 e 7/2
- Março - $3^2 <$ dia primo $< 3^3$, dias e meses possíveis: 11/3, 13/3, 17/3, 19/3 e 23/3.
- Abril - $4^2 <$ dia primo $< 4^3$, dias e meses possíveis: 17/4, 19/4, 23/4 e 29/4.
- Maio - $5^2 <$ dia primo $< 5^3$, dias e meses possíveis: 29/5 e 31/5.

Janeiro fica eliminado pela condição (3) e os demais meses pela condição (2). A condição (4) elimina: 7/2, todos os dias de março, 17/4, 23/4, 29/4 e os dias de maio. Ficamos com apenas duas datas: 5/2 e 19/4. A condição (5) elimina 5/2.

Logo, o aniversário do professor é no dia 19 de abril.

7. Problema

Uma Solução

Responderemos esse problemas de maneira análoga ao exemplo da página 20.

Temos que mostrar que, para $p = 13$, a igualdade $(13-1)! \equiv -1(\mod 13)$

Observe as congruências:

$$1 \equiv 1(\mod 13)$$
$$2 \cdot 7 = 14 \equiv 1(\mod 13)$$
$$3 \cdot 9 = 27 \equiv 1(\mod 13)$$
$$4 \cdot 10 = 40 \equiv 1(\mod 13)$$
$$5 \cdot 8 = 40 \equiv 1(\mod 13)$$
$$6 \cdot 11 = 66 \equiv 1(\mod 13)$$
$$12 \equiv 12(\mod 13)$$

Multiplicando, membro a membro, teremos:

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot 11 \cdot 12 \equiv 12(\mod 13)$$
$$12! \equiv 12(\mod 13) \Rightarrow 12! \equiv -1(\mod 31)$$
$$(13-1)! \equiv -1(\mod 13)$$

Pelo Teorema de Wilson, segue que 13 é primo.