Glaucia Innocencio de Jesus Paulo Paiva

Números primos e testes de primalidade

CAMPINAS
2014

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística
e Computação Científica

GLAUCIA INNOCENCIO DE JESUS PAULO PAIVA

NÚMEROS PRIMOS E TESTES DE PRIMALIDADE

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestra

Orientador: Ricardo Miranda Martins

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELA ALUNA GLAUCIA INNOCENCIO DE JESUS PAULO PAIVA, E ORIENTADA PELO PROF. DR. RICARDO MIRANDA MARTINS.

Assinatura do Orientador

CAMPINAS

2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

P166n

Paiva, Glaucia Innocencio de Jesus Paulo, 1985-
Números primos e testes de primalidade / Glaucia Innocencio de Jesus Paulo Paiva. – Campinas, SP : [s.n.], 2014.

Orientador: Ricardo Miranda Martins.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Números primos. 2. Matemática (Segundo grau) - Estudo e ensino. 3. Congruências e restos. I. Martins, Ricardo Miranda,1983-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

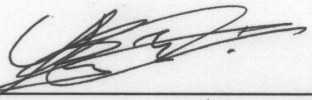
Informações para Biblioteca Digital

Título em outro idioma: Prime numbers and primality test
Palavras-chave em inglês:
Prime numbers
Mathematics - Study and teaching
Congruences and residues
Área de concentração: Matemática em Rede Nacional
Titulação: Mestra
Banca examinadora:
Ricardo Miranda Martins [Orientador]
Pedro José Catuogno
Claudio Aguinaldo Buzzi
Data de defesa: 15-12-2014
Programa de Pós-Graduação: Matemática em Rede Nacional

Dissertação de Mestrado Profissional defendida em 15 de dezembro de 2014 e aprovada Pela Banca Examinadora composta pelos Profs. Drs.

Prof.(a). Dr(a). RICARDO MIRANDA MARTINS

Prof.(a). Dr(a). PEDRO JOSÉ CATUOGNO



Prof.(a). Dr(a). CLAUDIO AGUINALDO BUZZI

Abstract

This dissertation studies integers , their properties and congruences . We cover various topics involving prime numbers , including how to generate them and decide if an integer is prime or composite . Our goal is to describe and study some primality tests such as the Fermat test , Lucas- Lehmer test , Miller- Rabin test and the AKS algorithm. We also propose some didactic sequences to study these topics in an elementary level to basic education .

Keywords: Prime numbers, mathematics - study and teaching, congruences and residues

Resumo

Nesta dissertação estudamos números inteiros, suas propriedades e congruências. Abordamos vários tópicos envolvendo números primos, incluindo como gerá-los e como decidir se um número inteiro é primo ou composto. Nosso objetivo é descrever e estudar alguns testes de primalidade, como o Teste de Fermat, Teste de Lucas-Lehmer, Teste de Miller-Rabin e o algoritmo AKS. Propomos ainda algumas sequências didáticas para estudar estes tópicos em um nível mais elementar, no ensino básico.

Palavras-chave: Números primos, congruência e restos, matemática (2º grau)- estudo e ensino

SUMÁRIO

Dedico ao meu marido, Augusto e aos meus filhos, Matheus e Isabela.

AGRADECIMENTOS

Agradeço a toda minha família que sempre me incentivou a estudar e buscar meus objetivos.

Agradeço em especial minha mãe e meus avós que são meus maiores e melhores exemplos e sempre estiveram do meu lado.

Agradeço também meu padastro, que é um dos maiores incentivadores para que eu estude sempre e sei que vibra com cada conquista minha.

Não poderia deixar de dizer meu muito obrigada por toda a paciência que meus dois filhos, Matheus e Isabela, tiveram com a mamãe em todo esse período.

Agradeço meu orientador pela proposta de tema e auxilio e a Capes pelo auxilio financeiro durante essa jornada.

Agradeço também todos os meus amigos que sempre estiveram ao meu lado mesmo alguns a distância. E por último e com grande importância agradeço meu eterno amor, meu marido que me acompanhou e me ajudou incansavelmente durante esses 3 anos, para que eu consiguisse concluir e conquistar meu título.

INTRODUÇÃO

Criptografia é um tema que sempre esteve presente na história da humanidade. A palavra criptografia vem do grego: Cripto (escondido) e Grafia (escrita). Ela consiste no estudo de técnicas que fazem com que uma informação original seja transformada numa informação ilegível de forma que possa ser conhecida apenas pelo seu destinatário. Apesar do termo criptografia significar em grego mensagem escondida, o envio de mensagens de forma oculta chama-se esteganografia.

A utilização da criptografia é tão antiga quanto a própria escrita. A primeira aparição em documentos da criptografia foi em torno de 1900 a.c., no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição [1]. A partir daí a humanidade tem muitos outros documentos que comprovam o constante uso da criptografia ao longo da história.

Essa utilização se dava principalmente em tempos de guerra, quando um povo precisava transmitir informações que se fossem interceptadas pelo seu rival elas seriam ilegíveis por ele, e então eles utilizavam códigos nos quais o seu adversário não conhecia. Uma antiga e conhecida forma de criptografia foram as Cifras de César, em Roma, Júlio Cesar se utilizava dessas cifras para transmitir informações militares a seus generais. Esse método consistia em trocar as letras por letras três posições a frente no alfabeto. Obviamente para os tempos atuais esse método é fácil de ser decifrado, mas quando utilizado, por volta de $40a.C.$ foi extremamente eficiente e não há documentos que mostrem que alguém tenha conseguido ou sequer tenha tentado decifrar as Cifras de César. Acredita-se que seus rivais achavam que Cesar escrevia em outra língua.

O tempo se passou e mais métodos para encriptar uma informação foram criados, e

cada vez mais decifradores surgiam, até que durante a Segunda Guerra Mundial surgiu a necessidade de métodos mais elaborados para cifrar mensagens. Então começam a surgir algoritmos matemáticos que cifravam e decifravam essas informações. Atualmente com o advento da internet e com a grande quantidade de informações transmitidas, existem vários algoritmos que criptografam uma mensagem. O mais conhecido se chama RSA, tem esse nome devido a seus inventores Ronald Rivest, Adi Shamir e Leonard Adleman, que o criaram em 1978.

O RSA é um algoritmo que se utiliza de dois números primos muito grandes para cifrar uma mensagem. O algoritmo utiliza o produto destes números e caso alguém, que não seja o destinatário, queira decifrar a mensagem deve descobrir quais são os dois números primos utilizados. Para garantir a segurança das informações transmitidas esse números primos tem pelo menos 250 dígitos, tornando o algoritmo inquebrável, pois é extremamente díficil fatorar números inteiros.

A decodificação das mensagens que utilizam o RSA traz à tona um outro tema que, assim como a criptografia, é bem antigo: a fatoração de um número, ou ainda a simples descoberta se um número é primo ou composto. O primeiro algoritmo para este fim foi o Crivo de Erastóstenes, criado mais ou menos no ano de 200a.C.

Ao longo do tempo muitos matemáticos como Fermat, Miller, entre outros, criaram metódos para determinar se um número é ou não primo sem fatorá-lo, mas os únicos que conseguiram um algoritmo em tempo polinomial foram os indianos e cientistas da computação Manindra Agrawal, Neeraj Kayal e Nitin Saxena em 6de Agosto de2002 em um trabalho intitulado "PRIMES is in P".

Os autores receberam o Premio Gödel (é uma premiação dada a cientistas que tenham publicado coisas relevantes na área da ciências da computação) de 2006 por este trabalho. Este algoritmo é conhecido hoje como algoritmo AKS.

A estrutura de capítulos utilizada é a seguinte. No Capítulo 1 falaremos sobre os números inteiros, suas propriedades e congruência. No Capítulo 2 o tema é números primos, números de Mersene e o Crivo de Erastostenes. No Capítulo 3 falaremos sobre alguns testes de primalidade, são eles:Teste de Fermat, Teste de Lucas-Lehmer, Teste de Miller-Rabin e o AKS. No Capítulo 4 e último capítulo colocamos uma sequência didática para ser aplicada em alunos do ensino médio utilizando como tema central testes de primalidade. Em todos os capítulos foram feitos exemplos numéricos para facilitar o entendimento da teoria.

CAPÍTULO 1

NÚMEROS INTEIROS

O nascimento do conceito de número surgiu pela necessidade da humanidade de contar. Foram muitos anos para que se estabelecesse o que hoje conhecemos como números naturais:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, ...\}.$$

Muitos anos se passaram e com mais dificuldade de entendimento e aceitação das pessoas foi introduzido o conjunto dos números inteiros:

$$\mathbb{Z} = \{..... - 6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, ...\}.$$

Hoje em dia sabemos e conseguimos pereceber no nosso cotidiano a importância desse conjunto. Veremos então algumas propriedades desses números.

1.1 Propriedades

Os números inteiros possuem duas operações, a soma e a multiplicação. Listaremos agora as propriedades dessas operações:

1. elemento neutro da soma é o 0. Dado $a \in \mathbb{Z}$ temos que $a + 0 = a = 0 + a$, $\forall a \in \mathbb{Z}$;

2. elemento neutro da multiplicação é o 1. Dado $a \in \mathbb{Z}$ temos que $a \cdot 1 = 1 = 1 \cdot a$, $\forall a \in \mathbb{Z}$;

3. elemento oposto da soma: Dado $a \in \mathbb{Z}$ temos que $\exists -a \in \mathbb{Z}$ tal que $a + (-a) = 0 = (-a) + a$;

4. Comutatividade:

   Dados $a, b \in \mathbb{Z}$ temos então que $a + b = b + a$ e $a.b = b.a$;

5. Associatividade:

   Dados $a, b, c \in \mathbb{Z}$ temos então que $(a + b) + c = a + (b + c)$ e $a.(b.c) = a.(b.c)$;

6. distributiva da multiplicação em relação a adição:

   Dados $a, b, c \in \mathbb{Z}$ temos então que $(a + b)c = a.c + b.c$.

1.2 Congruência

A aritimética modular é algo de suma importância para a teoria dos números. Esse conceito foi introduzido por Gauss e se perpetuou.

Dizemos que um número a é congruente a outro número b módulo m, quando a divisão de a por m restar b, e na linguagem matemática escrevemos da seguinte forma:

$$a \equiv b \pmod{m}.$$

Lemos a é congruo b módulo m, com $a, m, b \in \mathbb{Z}$.

Faremos alguns exemplos.

Exemplo 1.2.1. Resolva:$17 \equiv x \pmod 3$

Como $17 = 3 \cdot 5 + 2$, $17 - 2$ é divisível por 3.

Logo $17 \equiv 2 \pmod 3$.

$17 \equiv 2 \pmod 3$ é equivalente escrevermos dessa forma :$17 = 2 + 3y$.

Exemplo 1.2.2. Resolva:$20 \equiv x \pmod 5$.

Como $20 = 5 \cdot 4 + 0$ $20 - 0$ é divisível por 5, logo $20 \equiv 0 \pmod 5$.

$20 \equiv 0 \pmod 5$é equivalente escrevermos dessa forma :$20 = 5y$.

Exemplo 1.2.3. Resolva:$2 \equiv x \pmod 9$.

Neste caso $2 < 9$ então você não consegue fazer a divisão para dar um valor inteiro logo $x = 2$ ou $x = -7$ são respostas equivalentes.

Podemos escrever a equação acima da seguinte forma:$2 = 2 + 9y$ ou $2 = -7 + 9z$.

Vejamos agora algumas propriedades da congruência.

1.3 Propriedades

A congruência satisfaz as propriedades de reflexidade, transitividade e de simetria. Então, dados $a, b, c, n \in \mathbb{Z}$,temos:

- $a \equiv a \pmod{n}$ (reflexiva);
- Se $a \equiv b \pmod{n}$ então $b \equiv a \pmod{n}$ (simétrica);
- Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então $a \equiv c \pmod{n}$ (transitiva).

Uma quarta propriedade é:

$a \equiv b \pmod{n}$ e $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$ e $a \cdot c \equiv b \cdot d \pmod{n}$.

Demonstração:

- Dado que : $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, sabemos então que $a - b$ e $c - d$ são divisiveis por n, então obviamente $a - b + c - d$ é divisivel por n.

  Organizando de forma diferente $a - b + c - d$ temos:$a + c - (b + d)$ como foi dito acima $a - b + c - d$ é divisivel por n , logo

  $$a + c \equiv b + d \pmod{n}.$$

- Dado que : $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, sabemos então que $a - b$ e $c - d$ são divisíveis por n, então obviamente $a - b - (c - d)$
  =
  $a - b - c + d$ é divisível por n.

  Organizando de forma diferente $a - b - c + d$ temos: $a - c - (b - d)$ como foi dito acima $a - b - c + d$ é divisivel por n , logo

  $$a - c \equiv b - d \pmod{n}.$$

- Dado que : $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$,

  $a - b = k.n$, agora vamos multiplicar por c ambos os lados e $c - d = k_1 \cdot n$, vamos multiplicar ambos os lados por b.

Obtemos então as seguintes equações: $ac - bc = c \cdot k \cdot n$ e $bc - dc = c \cdot k_1 \cdot n$.

Agora somando as duas equações teremos:

$ac - bc + bc - dc = c \cdot k \cdot n + c \cdot k_1 \cdot n$

$\Rightarrow$

$ac - dc = c \cdot k \cdot n + c \cdot k_1 \cdot n;$

$ac - dc = n(c \cdot k \cdot + c \cdot k_1 \cdot)$

$\Rightarrow$

$a \cdot\ c \equiv b \cdot d \pmod{\text{n}}$.

1.4 Teorema Chinês dos Restos

Contam que na China, em época de guerra, após os confrontos o general reunia toda sua tropa e contava quantos haviam retornado. Como as tropas eram numerosas ele colocava todos em fila, pedia que fizessem filas de diferentes tamanhos e contabilizava somente o que restava. Com esses números em mãos conseguia obter o número de soldados que havia voltado da guerra. Veremos agora qual o terorema utilizado.

Teorema 1.4.1. Sejam $m_1, m_2, ..., m_r$ inteiros positivos e primos entre si. O sistema de congruências

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

tem solução única $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r \pmod{M}$,
onde $M = m_1 m_2 ... m_r$, $M_k = \frac{M}{m_k}$ e y_k é tal que $M_k y_k \equiv 1 \pmod{m_k}$
ou seja, y_k é o inverso multiplicativo de M_k módulo m_k.

Demonstração
Retirado de [12]
Vamos demonstrar por indução.

- Primeiro vamos provar para 2 equações:

  Dado o sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} (1)$$

Um inteiro x satisfaz o sistema (1) se e somente se existem inteiros y_1 e y_2 tais que

$x = m_1 \cdot y_1 + a_1$ (2)

$x = m_2 \cdot y_2 + a_2$ (3).

Subtraindo as duas equações e reordenando temos:

$m_1 \cdot y_1 - m_2 \cdot y_2 = a_2 - a_1$. (4)

Agora, como $\mathrm{mdc}(\mathrm{m}_1, \mathrm{m}_2) = 1$, sabemos que a equação (4) possui alguma solução $(y_1, y_2) \in \mathbb{Z}^2$.

Fixe uma tal solução e defina $x = x_0$ pela equação (2). Então usando (4) vemos que também vale a equação (3). Portanto este $x = x_0$ é uma solução do sistema (1).

Uma vez encontrada uma solução x_0, vejamos que qualquer $x \equiv x_0 \,(\mathrm{mod}\mathrm{m}_1 \cdot \mathrm{m}_2)$ é solução e de fato:

$x = x_0 + k \cdot m_1 \cdot m_2 \Rightarrow x \equiv x_0 \,(\mathrm{mod}\mathrm{m}_1)$ e $x \equiv x_0 \,(\mathrm{mod}\mathrm{m}_2)$.

Por outro lado, veremos que todas as soluções são dessa forma. Suponha x solução do sistema. Como x_1 também é solução, temos que $y = x - x_0$ satisfaz:

$$\begin{cases} y \equiv a_1 - a_1 \equiv 0 \pmod{m_1} \\ y \equiv a_2 - a_2 \equiv 0 \pmod{m_2} \end{cases}$$

Pelas equações acima temos que m_1 divide y, isto é, existe l tal que $y = l \cdot m_1$ e m_2 divide $y = l \cdot m_1$. Como m_1 e m_2 são primos entre si, m_2 divide l, isto é, existe k tal que $l = k \cdot m_2$. Portanto $y = k \cdot m_1 \cdot m_2 \equiv 0 (\mathrm{mod}\mathrm{m}_1 \cdot \mathrm{m}_2)$, ou seja, $x \equiv x_0 (\mathrm{mod}\mathrm{m}_1 \cdot \mathrm{m}_2)$,como queríamos provar.

- Já vimos que o teorema vale para 2 equações. Agora fixe $k \geq 2$ e suponha que o teorema vale para $k - 1$ equações. Dados $m_1, \cdots, m_k$ dois a dois primos entre si, e $a_1, \cdots, a_k$ quaisquer, considere o sistema formado apenas pelas $k - 1$ primeiras equações. Pela hipótese de indução, existe um b tal que este subsistema é equivalente a uma única equação, a saber,

$$x \equiv b \,(\mathrm{modM}), \text{ onde } M = m_1 \cdots m_{k-1}.$$

Portanto o sistema inteiro é equivalente a um sistema com duas equações:

$$\begin{cases} x \equiv b \pmod{M} \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Notando que M e m_k são primos entre si, e usando que o teorema vale para duas equações, temos que existe solução x_0. Além disso, x é solução se e somente se $x \equiv x_0 \pmod{M \cdot m_k}$ e $M \cdot m_k = m_1 \cdots m_{k_1} \cdot m_k$, como queríamos demonstrar.

Exemplo 1.4.2. (Exemplo retirado de [1])

Há mais de mil anos, um general chinês desejava saber exatamente quantos soldados tinha em seu exército. Estimou que este número estava entre 500 e 1000. Para determiná-lo precisamente, utilizou o método descrito a seguir. Ordenou que seus soldados entrassem em uma formação com colunas de 9 soldados e contou o número de soldados que não puderam ser arranjados em uma destas colunas. Foram 3. Repetiu o procedimento com colunas de tamanho 10 e 11 e descobriu que sobraram respectivamente 4 e 10 soldados. Para chegar ao tamanho do seu exército, o general resolveu o problema matemático detalhado no próximo parágrafo. Este fato é verídico exceto pelos números envolvidos.

Este é um problema explícito de congruência. Denotaremos por x o número total soldados, então:

$$\begin{cases} x \equiv 3 \pmod{9} \\ x \equiv 4 \pmod{10} \\ x \equiv 10 \pmod{11} \end{cases}$$

Então $9.q_1 + 3 = x$,

- substituindo na segunda equação do sistema temos $9.q_1 \equiv 1 \pmod{10} \Rightarrow q_1 \equiv 9$ $pmod10$.
- Substituindo agora na terceira equação temos $9.q_1 \equiv 7 \pmod{11} \Rightarrow q_1 \equiv 8 \pmod{11}$.

Temos então um novo sistema modular:

$$\begin{cases} q_1 \equiv 9 \pmod{10} \\ q_1 \equiv 8 \pmod{11} \end{cases}$$

E a partir dele novas equações:

$$\begin{cases} 10.q_2 + 9 = q_1 \\ 11q_2 + 8 = q_1 \end{cases}$$

E então conluimos que $q_2 = 1$ e $q_1 = 19$

Exemplo 1.4.3. Considere-se a equação:

$$327x \equiv 171 \pmod{520}$$

Vamos calcular o $\text{mdc}(327, 520) = 1$ podemos deduzir que existe uma única solução, utilizaremos então o metódo explicado acima.

Fatoramos o $520 = 5.8.13$, e passamos ao sistema

$$\begin{cases} 327x \equiv 171 \pmod{5} \\ 327x \equiv 171 \pmod{8} \\ 327x \equiv 171 \pmod{13} \end{cases} \Leftrightarrow \begin{cases} 2x \equiv 1 \pmod{5} \\ 7x \equiv 3 \pmod{8} \\ 2x \equiv 4 \pmod{13} \end{cases}$$

Queremos que o x fique multiplicado por 1, então vamos multiplicar a primeira equação do sistema por 8, a segunda e a terceira por 7.

$$\begin{cases} 16x \equiv 8 \pmod{5} \\ 49x \equiv 21 \pmod{8} \\ 14x \equiv 28 \pmod{13} \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{8} \\ x \equiv 2 \pmod{13} \end{cases}$$

Agora podemos resolver os sistema.

Vamos começar trabalhando com as duas primeiras equações de congruência,temos que:
$x = 3 + 5y \Rightarrow 3 + 5y \equiv 5 \pmod{8} \Rightarrow y \equiv 2 \pmod{8} \Rightarrow y = 8k + 2$

Logo: $x = 3 + 5(8k + 2) \Rightarrow x = 40k + 13$

Agora vamos utilizar o resultado acima e a equação 3:
$40k + 13 \equiv 2 \pmod{13} \Rightarrow k \equiv 2 \pmod{13} \Rightarrow k = 2 + 13w$

Logo: $x = 40(2 + 13w) + 13 \Rightarrow x = 93 + 520w$ com $w \in \mathbb{Z}$

CAPÍTULO 2

NÚMEROS PRIMOS

Definição 2.0.4. Um número $n \in \mathbb{N}$ é chamado de primo se $n > 1$ é divisível apenas por ele mesmo e por 1.

Exemplo 2.0.5. Alguns exemplos de números primos são: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$.....

Alguns autores utilizam outra definição para os primos:

Definição 2.0.6. Dado $n \in \mathbb{Z}$, $n \neq \pm 1$ e $n \neq 0$, então dizemos que n é primo se n só é divisível por ± 1, $\pm p$.

As duas são igualmente válidas mas neste trabalho usaremos apenas a primeira definição.

Os números primos tem esse nome por serem os números primários geradores de todos os outros. Essa nomenclatura foi utilizada por Fibonacci, e consagrada no mundo matemático, e hoje é conhecido no mundo todo [5].

Esses números começaram a ser estudados ainda na Grécia em $400a.C.$ pelos Pitagóricos, que tinham interesse em estudá-los pois viam uma ligação com a numerologia, algo místico, e foi mais aprofundada na obra de Euclides, "Os elementos", onde ele definiu o que seriam primos, e demonstrou por contradição que existem infinitos primos. Nessa mesma obra ele define e demonstra *O Teorema Fundamental da Aritimética* que enunciamos abaixo:

Teorema 2.0.7. Todo número inteiro maior do que 1 ou é primo ou pode ser escrito como um produto de números primos e de maneira única.

Demonstração: Vamos primeiro demonstrar que um número natural n se escreve como um produto de primos e depois provamos a unicidade:

Por indução finita:

- Para $n = 2$ e sabemos que 2 é primo logo está provado!
- Agora supondo que para um $n \in \mathbb{N}$ qualquer então temos $n = p_1.p_2.p_3.....p_j$ e aceitamos como válido!
- Vamos mostrar então que para um $m > n$ com $m \in \mathbb{N}$, também vale, então temos que: $m = n.k$, com $k \in \mathbb{N}$ como $n = p_1.p_2.p_3.....p_j$ temos três possibilidades para k:
  1. se k for primo e $k \neq p_1, p_2, p_3, ..., p_j$ então $m = q_1.q_2.q_3.....q_j.k$ OK!
  2. se k é primo e $k = p_1, p_2, p_3, ..., p_j$ idem anterior!
  3. k não é primo , logo também é decomposto em números primos $k = q_1.q_2.q_3.....q_i$ Então $m = p_1.p_2.p_3.....p_j.q_1.q_2.q_3.....q_i$.

Agora precisamos provar a unicidade da decomposição.

Vamos provar por contradição , então vamos supor que dado um $a \in \mathbb{N}$ ele pode ser decomposto de duas formas diferentes:

$a = p_1.p_2.p_3.....p_j$ e $a = q_1.q_2.q_3.....q_i$

com $p_1, p_2, p_3, ..., p_j, q_1, q_2, q_3, ..., q_i$ primos .

Então $p_1.p_2.....p_j = q_1.q_2.....q_i$,

sendo assim $p_1 \mid q_1.q_2.....q_i \Rightarrow p_1 = q_r$, para algum $r \Rightarrow p_1 \geq q_1$.

Da mesma forma $q_1 \mid p_1.p_2.p_3....p_j \Rightarrow q_1 = p_s$, para algum $s \Rightarrow q_1 \geq p_1$.

Logo $p_1 = q_1$.

Com o mesmo raciocínio concluimos que :$p_2 = q_2$, $p_3 = q_3$,...,$p_j = p_i$.

2.1 Co-primos

Existem também os conhecidos co-primos ou primos entre si:

Definição 2.1.1. Dados $a \in \mathbb{N}$ e $b \in \mathbb{N}$ e $mdc(a, b) = 1$ então dizemos que a e b são co-primos ou primos entre si.

CRIVO DE ERASTÓSTENES

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Exemplo 2.1.2. Os números 49 e 24 são primos entre si, pois $\text{mdc}(49, 24) = 1$. Ou seja, eles não tem nenhum fator primo em comum.

Exemplo 2.1.3. Os números 81 e 12 não são primos entre si já que o $\text{mdc}(81, 12) = 3$.

Durante toda a história, surgiram matemáticos interessados em demonstrar ou encontrar uma regularidade entre os números primos. Eratóstenes encontrou um metodo prático para encontrar os números primos.

2.2 Crivo de Erastóstenes

Erastóstenes foi uma filósofo que viveu 200 anos antes de Cristo, e teve seus maiores trabalhos no campo da geografia, mas teve também contribuições para a matemática. Criou o chamado Crivo de Erastóstenes.

O Crivo é uma tabela onde você coloca os números naturais até onde desejar, e depois vai "crivando"(ou cortando) os números múltiplos, e os que sobrarem sem o corte são os primos, como no exemplo abaixo:

Exemplo 2.2.1. Vamos encontrar os números primos até 100:

- Corta-se o número 1, pois por definição ele não é primo,
- 2 não corta, e a partir daí cortam todos os múltiplos de 2,

CRIVO DE ERASTÓSTENES

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
51	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	~~59~~	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

- Vamos para o próximo número que não foi riscado é o 3, e não cortamos, e a partir daí cortam todos os múltiplos de 3,
- e vamos cortando todos os múltiplos dos anteriores até que sobrarão somente os primos.

E o crivo fica da seguinte forma:
Concluimos que os primos até 100 são:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$

Para a época o metódo utilizado por Erastóstenes, foi de extrema importância, mas obviamente esse algoritmo para números primos muito grandes é inviável, então vieram outros matemáticos que tentaram descobrir formas mais rápidas de se ter o resultado.

Na corrida para descobrir alguma regra ou característica comum entre os primos, surgiram outros grupos de números que seguiam alguma regularidade. Um dos conjuntos mais importantes formado por números primos é o conhecido como números de Mersenne.

2.3 Números de Mersenne

Esse conjunto de números tem esse nome pois seu descobridor foi Mersenne um padre, teólogo e matemático que no século XVII mantinha contato com Pierre de Fermat.

Fermat que também era matemático e teve estudos importantissimos na área da aritimética, estava estudando sobre os números primos, e então mandou uma carta com uma

fórmula para Mersenne. Essa fórmula nos dá o que hoje conhecemos como números de Fermat, $2^{2p}+1$, e Mersenne resolveu então inspirado na fórmula de Fermat, descobrir para quais valores de p uma outra fórmula, $2^p - 1$, seria um número primo. Ele percebeu então que se:

- p fosse composto então $2^p - 1$ também seria,
- p fosse primo então $2^p - 1$ poderia ser primo ou composto.

Ele enumerou então alguns valores pra p que ele acreditava serem todos primos, e que resultariam em $2^p - 1$ também primo, os números são:

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

E isso perdurou por anos, até que outros matemáticos conseguiram encontrar outros valores de p primos que faziam com que sua fórmula resultaria em um número primo e também perceberam que para os primos 67 e 257 a fórmula resultava um número composto.

Fazendo os calculos para os valores de p que resultam em um primo, veremos quais valores Mersenne encontrou:

- Para $p = 2 \Rightarrow 2^2 - 1 = 3$
- Para $p = 3 \Rightarrow 2^3 - 1 = 7$
- Para $p = 5 \Rightarrow 2^5 - 1 = 31$
- Para $p = 7 \Rightarrow 2^7 - 1 = 127$
- Para $p = 13 \Rightarrow 2^{13} - 1 = 8.191$
- Para $p = 17 \Rightarrow 2^{17} - 1 = 131.071$
- Para $p = 19 \Rightarrow 2^{19} - 1 = 524.287$
- Para $p = 31 \Rightarrow 2^{31} - 1 = 2.147.483.647$
- Para $p = 127 \Rightarrow 2^{127} - 1 = 1.701.411.83.460.469.231.731.687.303.715.884.105.727$

Enunciaremos então a seguinte preposição:

Proposição 2.3.1. (Primos de Mersenne) Dado $M_n = 2^n - 1$ primo, então n é primo.

Demonstração: Vamos provar por absurdo , supondo que n não seja primo, então $n = p.q$ Logo:

$M_n = 2^{pq} - 1$

$M_n = (2^p - 1).(2^{p(s-1)} + 2^{p(s-2)} + 2^{p(s-3)} + +2^{p(s-4)} + ... + 2^{p(s-(s-1))} + 2^{p(s-s)})$

$M_n = (2^p - 1).(2^{p(s-1)} + 2^{p(s-2)} + 2^{p(s-3)} + +2^{p(s-4)} + ... + 2^p + 1)$

Como $p|n$ então $M_p|M_n$, Logo M_n não é primo ABSURDO!

Exemplo 2.3.2. Para $n = 2$ qual o valor de M_n?

$M_2 = 2^2 - 1 \rightarrow M_2 = 3$

M_2 é primo $\Rightarrow n = 2$ é primo.

Exemplo 2.3.3. Para $n = 9$ $M_9 = 2^9 - 1 \rightarrow M_9 = 511$

$511 = 7.73$ logo é composto

$n = 9$ é composto $\Rightarrow M_9$ é composto

Exemplo 2.3.4. Para $n = 11$ $M_{11} = 2^{11} - 1 \rightarrow M_{11} = 2047$

$2047 = 23.89$ logo é composto

Com este exemplo percebemos que a recíproca da preposição não é verdadeira, pois se temos um n primo, podemos encontrar um M_n composto

Anos se passaram e muito outros matemáticos continuaram na busca pelos primos de Mersenne, veremos na tabela abaixo os 48 primos de Mersenne conhecidos:

(∗) *A tabela acima não é discretamente exaustiva em todo o intervalo apresentado. Até agora (Out.*$19, 2014$*), do que a tabela contém, sabe-se (por critérios algorítmicos de busca exaustiva) que todos os primeiros mersennes primos de* M_2 *a* $M_{13.466.917}$ *já foram identificados e são ali listados. Entretanto, entre os Mersennes primos* $M_{25.964.951}$ *e* $M_{57.884.161}$ *(respectivamente,* 42ž *e* 48ž*, este o mais recente descoberto), não se tem registro oficial de outros Mersennes primos o que não significa poder afirmar-se inequivocamente não os haja: os intervalos são cada vez maiores e as buscas são cada vez mais trabalhosas. Como exemplo histórico, cite-se que o* 29ž *Mersenne primo foi descoberto somente após os* 30ž *e* 31ž*. É digno de nota que após o* $M_{46ž}$*, em apenas quatorze dias descobriu-se um Mersenne primo menor* $M_{45ž}$*, conforme acima citado. FONTE:[8]*

Muito antes de Mersenne, Euclides em meados de 300 a.C., descobriu um conjunto de números com uma carcaterística bem interessante que veremos a seguir, esses números ele deu o nome de números perfeitos. Veremos a definição:

Ordem	p	Dígitos	Anos	Referências ao descobridor
1	2	1	antiguidade	
2	3	1	antiguidade	
3	5	2	antiguidade	
4	7	3	antiguidade	
5	13	4	1461	Reguis (1536), Cataldi (1603)
6	17	6	1588	Cataldi (1603)
7	19	6	1588	Cataldi (1603)
8	31	10	1750	Euler (1772)
9	61	19	1883	Pervouchine (1883), Seelhoff (1886)
10	89	27	1911	Powers (1911)
11	107	33	1913	Powers (1914)
12	127	39	1876	Lucas (1876)
13	521	157	Jan. 30, 1952	Robinson
14	607	183	Jan. 30, 1952	Robinson
15	1.279	386	Jan. 30, 1952	Robinson
16	2.203	664	Jan. 30, 1952	Robinson
17	2.281	687	Jan. 30, 1952	Robinson
18	3.217	969	Set. 8, 1957	Riesel
19	4.253	1281	Nov. 3, 1961	Hurwitz
20	4.423	1332	Nov. 3, 1961	Hurwitz
21	9.689	2917	Mai 11, 1963	Gillies (1964)
22	9.941	2993	Mai 16, 1963	Gillies (1964)
23	11.213	3376	Jun. 2, 1963	Gillies (1964)
24	19.937	6002	Mar. 4, 1971	Tuckerman (1971)
25	21.701	6533	Out. 30, 1978	Noll and Nickel (1980)
26	23.209	6987	Fev. 9, 1979	Noll (Noll Nickel 1980)
27	44.497	13395	Abr. 8, 1979	Nelson Slowinski (Slowinski 1978-79)
28	86.243	25962	Set. 25, 1982	Slowinski
29	110.503	33265	Jan. 28, 1988	Colquitt e Welsh (1991)
30	132.049	39751	Set. 20, 1983	Slowinski

Ordem	p	Dígitos	Anos	Referências ao descobridor
31	216.091	65050	Set. 6, 1985	Slowinski
32	756.839	227832	Fev. 19, 1992	Slowinski e Gage
33	859.433	258716	Jan. 10, 1994	Slowinski e Gage
34	1.257.787	378632	Set. 3, 1996	Slowinski e Gage
35	1.398.269	420921	Nov. 12, 1996	Joel Armengaud/GIMPS
36	2.976.221	895832	Ago. 24, 1997	Gordon Spence/GIMPS (Devlin 1997)
37	3.021.377	909526	Jan. 27, 1998	Roland Clarkson/GIMPS
38	6.972.593	2098960	Jun. 1, 1999	Nayan Hajratwala/GIMPS
39	13.466.917	4053946	Nov. 14, 2001	Michael Cameron/GIMPS (Whitehouse 2001)
40	20.996.011	6320430	Nov. 17, 2003	Michael Shafer/GIMPS (Weisstein 2003)
41	24.036.583	7235733	Mai 15, 2004	Josh Findley/GIMPS (Weisstein 2004)
42*	25.964.951	7816230	Fev. 18, 2005	Martin Nowak/GIMPS (Weisstein 2005)
43*	30.402.457	9152052	Dez 15, 2005	Dr. Curtis Cooper e Dr. Steven Boone
44*	32.582.657	9808358	Set. 4, 2006	Dr. Curtis Cooper e Dr. Steven Boone
45*	37.156.667	11.185.272	Set. 6, 2008	GIMPS / Hans-Michael Elvenich
46*	42.643.801	12.837.064	Abril.12, 2009	GIMPS / Odd M. Strindmo
47*	43.112.609	12.978.189	Ago. 23 , 2008	GIMPS / Edson Smith
48*	57.885.161	17.425.171	Jan. 25 , 2013	GIMPS / Curtis Cooper

Definição 2.3.5. (Números perfeitos): Seja $n > 1$ um número natural e considere $S(n)$ a soma dos divisores positivos(d) de n, tal que $d < n$. Chamaremos n de um número perfeito, se $S(n) = n$.

Vamos aos exemplos.

Exemplo 2.3.6. Vamos verificar se o número 6 é perfeito.

$6 = 3 \cdot 2 \cdot 1$, sendo assim os divisores de 6 são $3, 2, 1$ $S(6) = 3 + 2 + 1 = 6$, logo 6 é um número perfeito

Exemplo 2.3.7. Vamos verificar se o número 15 é perfeito.

$15 = 5 \cdot 3 \cdot 1$, sendo assim os divisores de 15 são $5, 3, 1$ $S(15) = 5 + 3 + 1 = 9$, logo 15 não é um número perfeito.

Teorema 2.3.8. (Fórmula de Euclides) Dado $k \in \mathbb{N}$, se $2^k - 1$ for primo, então

$n = 2^{k-1}(2^k - 1)$ é um número perfeito.

Demonstração: Suponha $2^k - 1 = p$ e p primo. Se pegarmos o número $2^{k-1} \cdot p$ e sabemos então que a soma dos divisores de $n = 2^{k-1} \cdot p$ menores que ele é :

$S(n) = S(2^{k-1} \cdot p) = (1 + 2 + 2^2 + ... + 2^{k-1}) + (p + 2p + 2^2p + ... + 2^{k-2}p)$
$S(n) = \frac{1.(2^k-1)}{2-1} + p\left[\frac{1.(2^{k-1}-1)}{2-1}\right] = 2^k - 1 + p(2^{k-1} - 1)$
$S(n) = p + p(2^{k-1} - 1) = p(1 + 2^{k-1} - 1) = p(2^{k-1}) = n$

Exemplo 2.3.9. Dado $k = 2 \Rightarrow n = 2^{k-1}(2^k - 1) = 2^1 \cdot (2^2 - 1) \Rightarrow n = 6$.

Como $2^2 - 1 = 3$ que é um número primo então, 6 é perfeito, como já haviamos verificado.

Exemplo 2.3.10. Dado $k = 7 \Rightarrow n = 2^{k-1}(2^k - 1) = 2^6 \cdot (2^7 - 1)n = 8.128$.

Como $2^7 - 1 = 127$ que é um número primo então, 8128 é perfeito.

$S(n) = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064 = 8.128 = n$

Exemplo 2.3.11. Dado $k = 11 \Rightarrow n = 2^{k-1}(2^k - 1) = 2^{10} \cdot (2^{11} - 1)$. Como $2^{11} - 1 = 2.047 = 23 \cdot 89$ não é primo. Logo n não é perfeito.

CAPÍTULO 3

TESTE DE PRIMALIDADE

Sabemos que existem mais de 100 diferentes testes de primalidade, existem alguns que diferem totalmente , e existem testes que são apenas melhorias de algoritmos já utilizados. Faremos aqui uma descrição dos testes mais relevantes para esse trabalho.

3.1 Teste de Fermat

Pierre de Fermat foi um dos maiores matemáticos do século XVII. Não teve nenhuma publicação em vida, mas deixou grandes contribuições para a evolução da matemática, sendo uma delas conhecida como Pequeno Teorema de Fermat. Esse teorema diz o seguinte:

Teorema 3.1.1. (Pequeno Teorema de Fermat) Se p é um número primo, então para qualquer inteiro a, temos que:

$$a^p \equiv a \pmod{\text{p}}.$$

Demonstração: Vamos fazer a demonstração por indução finita em a:

1. Vamos verificar que para $a = 1$ e p um primo qualquer vale,

   então: $1^p \equiv 1 \pmod{\text{p}}$ OK!

2. Vamos supor verdade para um $a = n$ com $n \in \mathbb{N} \Rightarrow n^p \equiv n \pmod{p}$

3. Vamos provar que vale para $a = n + 1$,então queremos mostrar que:

$$(n+1)^p \equiv (n+1) \pmod{\text{p}}.$$

Para isso utilazaremos do seguinte Lema:

Lema 3.1.2. Seja p primo e a e b inteiros. Então:

$$(a+b)^p \equiv (a^p + b^p) \pmod{\text{p}}$$

Demonstração do Lema acima se dá pelo desenvolvimento de $(a+b)^p$ por Binômio de Newton.

Agora, utilizando do Lema acima temos que:

$$(n+1)^p \equiv (n^p + 1^p) \pmod{p} \Rightarrow (n+1)^p \equiv n^p + 1 \pmod{p}.$$

Mas sabemos pela hipótese de indução que: $n^p \equiv n \pmod{\text{p}}$.

Então utilizando as propriedades de congruência temos:

$n^p \equiv n \pmod{p}$ e $1 \equiv 1 \pmod{p} \Rightarrow n^p + 1 \equiv (n+1) \pmod{p}$

$$(n+1)^p \equiv n + 1 \pmod{\text{p}}.$$

Como queríamos provar!

Exemplo 3.1.3. Agora vamos testar para um $p = 5$ e $a = 2$.
$2^5 \equiv 32 \equiv 2 \pmod{5}$.

Exemplo 3.1.4. Agora vamos testar para um $p = 5$ e $a = 4$.
$4^5 = 1024 \equiv 4 \pmod{5}$.

Facilmente encontramos um contra exemplo para a recíproca do Teorema, ou seja, se quisermos saber se um número é primo se utilizando do Pequeno Teorema de Fermat temos grande chances de chegarmos a conclusão equivocada. Veremos no exemplo a seguir.

Exemplo 3.1.5. Dado $p = 341$ e $a = 2$, através do Pequeno Teorema de Fermat, vamos tentar concluir se 341 é ou não primo. Sabemos que :

$$2^{10} = 1024 \equiv 1 \pmod{341}.$$

Elevando os dois lados a 10, temos que:

$$2^{10 \cdot 10} \equiv 1^{10} \pmod{341} \Rightarrow 2^{100} \equiv 1 \pmod{341}.$$

Elevando os dois lados ao cubo, temos que:

$$2^{300} \equiv 1^3 \pmod{341}.$$

Multiplicando por 2^{10} temos que:

$$2^{300}.2^{10} \equiv 1 \pmod{341}.$$

Repetindo a multiplicação por mais 3 vezes:

$$2^{300}.2^{40} \equiv 1 \pmod{341}.$$

Agora para finalizar multiplicamos por 2 e teremos :

$$2^{340}.2 \equiv 1.2 \pmod{341},$$
$$2^{341} \equiv 2 \pmod{341}.$$

Sendo assim poderíamos concluir que 341 é primo! O que é mentira, já que $341 = 11.31$.

Com este exemplo vimos que a recíproca não é verdadeira, testamos somente com $a = 2$, e concluimos que 341 é primo.

O Teste de Fermat para saber se um número natural é ou não primo, se utiliza justamente do teorema descrito acima. A máquina utilizada testa o valor dado com vários valores de a naturais e diferentes até que se para todos os valores testados o Pequeno Teorema de Fermat se confirma ela retornará que o valor é primo e caso contrário ela retorna que o número é composto.

Esse é um teste probabilístico já que não é possível testar para todos os números naturais. Sendo assim, para números muito grandes você pode ter o resultado errado caso a máquina teste aquele valor só para números onde o Teorema funcionará e retorne que ele é primo , quando na verdade se tivesse feito o teste com outro valor teria constatado que ele era composto. Mas se tivessemos feito outros testes para o nosso último exemplo talvez tivessemos feito com números que confirmassem o Pequeno Teorema de Fermat e assim retornaria que o valor era primo , o que vimos que não é verdade.Logo este é um teste que não dá 100% de certeza.

Quanto mais valores testarmos mais chances temos de acertar, mas nunca teremos certeza, principalmente para valores muito grandes.

3.2 Teste de Lucas-Lehmer

Este é um teste que foi criado por Lucas em 1876. Após meio século, em 1936, Lehmer fez algumas contribuições para o teorema. O teste se utiliza dos números de Mersenne, ele testa o valor dado através de uma recorrência e retorna verdadeiro quando é primo.

No algoritmo utiliza-se as seguintes equações:

$$S_0 = 4, S_n \equiv (S_{n-1}^2 - 2) \pmod{M_p}, \text{com} M_p = 2^p - 1. \text{Se } S_{n-2} \equiv 0 \pmod{M_p} \Rightarrow M_p \text{ é primo.} \tag{3.1}$$

A demonstração deste algoritimo foi feita por Lucas e não é trivial ele foi melhorado por Lehmer mas ainda assim não cabe fazê-la neste trabalho. Pode-se encontrar essa demonstração em [2].

Faremos alguns exemplos para entendermos como funciona esse teste.

Exemplo 3.2.1. Vamos testar para: $n = 3 \Rightarrow M_3 = 2^3 ? 1 = 7$.

temos que : $S_0 = 4$,

$S_1 \equiv 14 \pmod{7}$, $S_1 \equiv 0 \pmod{7}$.

Logo 7 é primo.

Exemplo 3.2.2. Vamos testar agora para o número 7.

Primeiro calculamos $M_7 = 2^7 - 1 \Rightarrow M_7 = 127$

Dado $S_0 = 4$, vamos calcular S_1, S_2, S_3, S_4, S_5

$S_1 \equiv 14 \pmod{127}$,

$S_2 \equiv 67 \pmod{127}$,

$S_3 \equiv 42 \pmod{127}$,

$S_4 \equiv 111 \pmod{127}$,

$S_5 \equiv 0 \pmod{127}$,

Conluimos então que 127 é primo.

3.3 Teste de Miller-Rabin

Este teste foi criado por Gary Miller e Michael Rabin, dois profissionais da área da informática que estudam criptografia e através também do pequeno Teorema de Fermat

criaram um teste probabilistico com alto grau de acerto.

Teorema de base para o teste:

Teorema 3.3.1. Sejam p um número primo e $x > 1$ tal que $x^2 \equiv 1 \pmod{p}$. Então $x \equiv 1 \pmod{p}$ ou $x \equiv p-1 \pmod{p}$

Demonstração

$x^2 \equiv 1 \pmod{p} \Rightarrow x^2 - 1 \equiv 0 \pmod{p} \Rightarrow$

$(x+1)(x-1) \equiv 0 \pmod{p} \Rightarrow x \equiv -1 \pmod{p}$ ou $x \equiv 1 \pmod{p} \Rightarrow$

$x \equiv (p-1) \pmod{\text{p}}$ ou $x \equiv 1 \pmod{\text{p}} \Rightarrow$

C.Q.D

O teste de Miller testa só números impares pelo motivo óbvio que o único primo par é o 2, ele funciona de seguinte forma:

1. Dado um n inteiro, ele divide $n-1$ por 2 diversas vezes até encontrar um valor k ímpar. E então $n - 1 = 2^q.k$

2. É escolhido um a natural e $a < n$, e então se faz o 1º teste:

$$a^k \equiv 1 \pmod{\text{n}}.$$

3. E depois uma sequência de testes com o mesmo valor de a, mas com i variando

$$a^{2^i.q} \equiv -1 \pmod{\text{n}}$$

   Com $0 < i < q - 1$

4. Caso em algum momento dos testes a igualdade seja verdadeira a máquina retorna que o n é primo caso contrário ela retorna que o n é composto.

Vamos fazer alguns exemplos se utilizando do teste mostrado nessa seção.

Exemplo 3.3.2. Neste exemplo, vamos utilizar o teste de Miller para descobrir se $n = 15$ é primo ou composto.

Então seguiremos os passos acima:

1. Então pegaremos $n-1=15-1=14$ e dividiremos por 2 até que o resultado dê um número ímpar $14=2^1.7$. Então $k=7$ e $q=1$.

   E usaremos $a=2$.

2. Agora vamos substituir na primeira fórmula: $2^7 \equiv 128 \equiv 8 \pmod{15}$ Como $8 \neq 1$ então vamos para a segunda parte

3. Agora subtituiremos na segunda fórmula,

   $2^1 \equiv 2 \pmod{5}$,

   $2^2 \equiv 4 \pmod{15}$,

   $2^4 \equiv 1 \pmod{15}$,

   Sendo assim provamos que 15 é composto.

Exemplo 3.3.3. Vamos testar agora para $n=561$.

1. Então $n-1=561-1=560$ e $560=2^4.35$ então $k=35$ e $q=4$.

2. Escolhendo $a=2$ temos que utilizar : $a^k \equiv 1 \pmod{\text{n}}$.

   Então:$2^{35} \equiv 263 \pmod{561}$.

3. E agora vamos utilizar a fórmula $a^{2^i.q} \equiv -1 \pmod{\text{n}}$, com $0<i<q-1$

   $2^{2^1.35} \equiv 166 \pmod{561}$,

   $2^{2^2.35} \equiv 67 \pmod{561}$,

   $2^{2^3.35} \equiv 1 \pmod{561}$, sendo assim 561 é composto.

Exemplo 3.3.4. Vamos testar para o $n=7$, sabemos que ele tem que retornar que o valor é um possível primo.

1. Então $n-1=7-1=6$ e $6=2^1.3$ então $k=3$ e $q=1$

2. Escolhendo $a=2$ temos que utilizar : $a^k \equiv 1 \pmod{\text{n}}$

   Então:$2^3 \equiv 1 \pmod{7}$

Exemplo 3.3.5. Vamos testar para o $n=1.373.653$.

1. Então $n - 1 = 1.373.653 - 1 = 1.373.652$ e $1.373.652 = 2^2 \cdot 343.413$ então $k = 343.413$ e $q = 2$.

2. Escolhendo $a = 2$ temos que utilizar : $a^k \equiv 1 \pmod{\text{n}}$.

   Então:$2^{343.413} \equiv 890.592 \pmod{1.373.653}$.

3. E agora vamos utilizar a fórmula $a^{2^i \cdot q} \equiv -1 \pmod{\text{n}}$, com $0 < i < q - 1$.

   $2^{2^1 \cdot 343.413} \equiv 1.373.652 \pmod{1.373.653}$,

   $2^{2^1 \cdot 343.413} \equiv -1 \pmod{1.373.653}$,

   Sendo assim concluimos que 1.373.653 é primo. O que não é verdade pois $1.373.653 = 829 \cdot 1657$.

   Então dizemos que 1.373.653 é um pseudo-primo para $a = 2$.

Apesar do teste de Miller ser um teste probabílistico, é conhecido que se for testado com alguns valores de a conseguimos torna-lo um teste determinístico, como veremos na abaixo:

- se $n < 2.047$, é suficiente testar para $a = 2$;
- se $n < 1373653$, é suficiente testar para $a = 2$ e 3;
- se $n < 9080191$, é suficiente testar para $a = 31$ e 73;
- se $n < 25326001$, é suficiente testar para $a = 2, 3$, e 5;
- se $n < 4759123141$, é suficiente testar para $a = 2, 7$, e 61;
- se $n < 1.122.004.669.633$, é suficiente testar para $a = 2, 13, 23$, e 1.662.803;
- se $n < 2.152.302.898.747$, é suficiente testar para $a = 2, 3, 5, 7$, e 11;
- se $n < 3.474.749.660.383$, é suficiente testar para $a = 2, 3, 5, 7, 11$, e 13;
- se $n < 341.550.071.728.321$, é suficiente testar para $a = 2, 3, 5, 7, 11, 13$, e 17;
- se $n < 3.825.123.056.546.413.051$, é suficiente testar para $a = 2, 3, 5, 7, 11, 13, 17, 19$, e 23.

Fonte: Referência [12]

Se um número composto n tem resultado inconclusivo para o teste de Miller com respeito a uma base b, dizemos que n é um pseudoprimo forte para a base b. Existem mais de 1200 pseudoprimos fortes entre 1 e 10^9.Segue alguns deles: 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401, 172081, 188461, 252601, 278545, 294409, 314821, 334153, 340561, 399001, 410041, 449065, 488881, 512461.

3.4 AKS

Todos os testes citados anteriormente tiveram sua importância na época em que foram descobertos, mas nenhum deles supri a necessidade que temos na atualidade devido a tecnologia que estamos inseridos. A busca por um teste que diga se um número muito grande é primo ou não continuou, até que surgiu o algoritimo AKS, que veremos a seguir.

Este teste foi criado por 3 indianos conhecidos como : Manindra Agrawal, Neeraj Kayal e Nitin Saxena o que originou o nome ao teste AKS. Em 2002, então Agrawal , professor doutor em Ciências da Computação e seus alunos Kayal e Saxena, recém formados do curso de Ciências da Computação, que tinham seu trabalho de conclusão de curso intitulado *Towards a deterministic polynomial-time Primality Test*, estavam então a procura de um Teste de primalidade que faria isso em um tempo polinomial, ou seja, diria se um número era primo ou não mais rápido do que todos os testes já vistos até então.

Este é um teste que tem como seu principal diferencial o tempo de resposta, e faz com que as pessoas imaginem que seu algoritimo se utilize de uma matemática avançada o que não é verdade. Ele teve uma repercução muito grande e prova disso foi que assim do seu lançamento, no dia seguinte já haviam várias sugestões de simplificações dadas pelos mais diversos estudiosos da área, que já perceberam a importância daquele artigo.

O algoritimo tem como base a seguinte equação de congruência:

$$(x-a)^p \equiv (x^p - a) \pmod{p} \Leftrightarrow p \text{ é primo.}$$

Sendo $a \in Z$ e $p > 1$, desenvolvimento dessa equação se dá pela expansão binomial de:

$$\sum_{p=0}^{n} (x-a)^p \ .$$

Visto que desenvolver essa equação e mostrar que um número grande p é primo levaria muito tempo, então houve uma melhoria desse algoritimo. Ao invés de (mod p) se utiliza mod $(x^r - 1, p)$ onde r é um número primo pequeno. O algoritimo AKS utiliza também congruência de polinômios nesse trabalho não foi feito uma explanação sobre esse assunto, mas na bibliografia [13] você encontra uma introdução sobre o tema.

Vamos fazer exemplos numéricos, para ficar mais claro.

Exemplo 3.4.1. Vamos fazer a verificação se 7 é um número primo através do teste AKS. Seja $p = 7$ e vamos tomar $a = 2$ e $r = 3$.

Substituindo os valores na equação, abaixo:

$$(x-a)^p \equiv (x^p - a) \mod (x^r - 1, p),\ (x-2)^7 \equiv (x^7 - 2) \mod (x^3 - 1, 7).$$

1. Precisamos verificar qual o resto da divisão de $x^7 - 2$ por $x^3 - 1$.

   Fazendo os calculos temos que o resto é $x - 2$.

   Faremos então, $(x - 2)$ dividido por 7 e o resto da divisão é **5+x**.

2. Agora vamos verificar se $(x-2)^7 \mod(x^3 - 1, 7)$ também tem como resto $5 + x$.

   Então utilizando a expansão binômial,temos: $(x-2)^7 = -128+448x-672x^2+560x^3-280x^4+84x^5-14x^6+x^7$.

   E agora se utilizando do resultado da expansão, dividiremos por $x^3 - 1$ e o resto dessa divisão é $418 + 169x - 588x^2$.

   Vamos dividir então $418 + 169x - 588x^2$ por 7 e o resto dessa divisão é igual a **5+x**.

Logo 7 é primo.

Exemplo 3.4.2. Faremos agora para $p = 4$, $a = 2$ e $r = 3$.

1. Vamos fazer a divisão de $x^4 - 2$ por $x^3 - 1$, o resto da divisão é igual a **x-2**.
   Agora dividindo $x - 2$ por 4 , o resto da divisão é **2+x**.

2. Usando a expansão binomial de $(x - 2)^4$ temos $x^4 - 8x^3 + 24x^2 - 32x + 16$ e agora vamos dividir o resultado por $x^3 - 1$ e obtemos o resto igual a **-3x**.
   Como $\mathbf{x - 2 \neq -3x}$.

Portanto 4 é composto.

CAPÍTULO 4

SEQUÊNCIA DIDÁTICA

4.1 Introdução

A matemática não costuma ser a matéria mais fascinante para a maioria dos alunos, por diversos motivos. Um deles é a falta de significado que existe nos conteúdos dos livros e apostilas usadas nas escolas. Alguns conteúdos conseguimos com facilidade encontrar uma aplicabilidade e uma resposta para aquela velha pergunta: “Professor, para o que eu vou usar isso na minha vida?”.

Esse trabalho vem para contribuir, para dar significado a alguns conteúdos ensinados no ensino médio, por mais que alguns conteúdos não tenha aplicação direta no cotidiano daqueles alunos, precisamos mostrar aos alunos que indiretamente ele está usando algo que é uma consequência do que ele aprendeu.

Depois de todos os conceitos vistos acima vamos aplicar alguns deles direta outros indiretamente nesta sequência didática, que visa também passar um pouco de conhecimento além do curriculo regular do ensino básico.

4.2 Objetivo

Nosso objetivo é através dos testes de primalidade trazer a tona a aplicabilidade dos números primos. Esse é um assunto que acompanha toda a trajetória matemática do nosso

aluno no ensino básico e muitos deles não veem uma aplicação real para o tema.

Vimos nesse trabalho alguns testes de primalidade e escolhemos apresentar para os alunos o Crivo de Eratóstenes e o Teste Miller. O motivo da escolha do Crivo de Eratóstenes é mostrar para os alunos porque tantos outros testes surgiram mesmo já existindo há tantos anos esse método. A escolha do teste de Miller foi feita devido a maior facilidade de entendimento dos alunos na faixa etária que se encontram.

4.3 Metodologia

- O professor deve dar uma introdução histórica da importância dos números primos. Essa introdução pode ser retirada desse trabalho no Capítulo 3 que fala sobre os números primos. Nesse momento o aluno precisa também já ter aprendido o que são números primos e também o que significa fatorar um número.

- Para contextualizar e fazer a aula se tornar mais interessante pode-se contar um pouquinho sobre criptografia. Na introdução desse trabalho você encontra um breve histórico da criptografia.

- Caso a escola tenha o recurso da sala de informática é interessante fazer com que os alunos pesquisem sobre o assunto para que não fique apenas uma aula expositiva e eles consigam discutir sobre o tema.

- Iniciar o assunto mostrando a forma mais simples de se encontrar um número primo, que é pelo Crivo de Eratóstenes, contar um pouquinho sobre o Crivo de Eratóstenes e como ele fazia para encontrar um número primo.

4.4 Atividade 1

Primeiramente, os alunos devem descobrir se um número é primo ou não da forma usual, ou seja, pelo algoritmo da divisão. Assim, dado um número pequeno (não muito maior que 100), os alunos devem efetuar divisões por vários números inteiros até descobrir sua fatoração. Desta forma, descobrirão se ele é ou não primo.

A seguir, os alunos podem se dividir em grupos de mais ou menos 4 alunos e cada grupo recebe um outro número (ou o mesmo do início) para descobrir através do crivo se é ou não

primo. É esperado que esta atividade termine antes da primeira. Se o número for riscado, ele não é primo. Se não for riscado, ele é primo.

Finalmente, deve-se propor aos alunos que encontrem todos os números primos que estão compreendidos entre 0 e 100.

Após esses cálculos mostre para os alunos o quanto demoraria se tivesse que encontrar um número primo muito grande e conclua então que é por isso que existem várias outras formas (algoritmos) de decidir sobre primalidade. Existem algumas mais eficientes outras menos.

Falar sobre os seguintes testes de primalidade:

1. Teste de Fermat
2. Teste de Lucas-lehmer
3. Teste de Miller
4. Algoritmo AKS

Todos eles têm os nomes dos seus descobridores o último é o mais atual e é o que apresenta a resposta se um número é ou não primo com mais rapidez. Devido à complexidade dos cálculos, sugiro que seja utilizado o Teste de Miller na aula seguinte, para ilustrar o poder do algoritmo.

4.5 Atividade 2

Agora faremos uma explanação sobre como o teste de Miller encontra um número primo com porcentagem mínima de erro.

Após apresentar uma sequência de passos de como o teste encontra se um número é primo ou não, faça com um valor o passo a passo com os alunos. Não creio que seria interessante para os alunos a demonstração, pois se torna cansativa. No entanto, isto fica a critério do professor que irá realizar a atividade, pois às vezes o nível de conhecimento matemático da turma permite que a prova seja feita.

Fazer então um passo a passo de preferência já com um exemplo númerico para ficar mais claro. Segue o passo a passo do Teste de Miller.

1. Dado um número n calcule $n - 1$.

2. Divida o número $n-1$ por 2 por várias vezes até encontrar um número ímpar.

3. Você obteve então um número $n-1=2^q k$. Agora escolha um valor que chamaremos de a e deve ser menor que $n-1$.

4. Agora calcule a^k. Este resultado você deve dividir por n e, caso o resto seja 1, n é um possível número primo.

5. Agora faça: $a^{2^i k}$ com $0 < i < q-1$ e divida por n. Se em algum momento o resto for $n-1$ então esse número é um possível primo.

Dê então valores para que os alunos possam encontrar possíveis primos utilizando o Teste de Miller.

É bom enfatizar que o Teste de Miller é probabilístico, ou seja, ele pode falhar. Dar um exemplo quando o teste falha (por exemplo são pseudo-primos para $a=2$ os seguintes valores:$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841.29341, 41041, 46657, 52633.62745, 63973$ e o 75361).

Após a atividade seria interessante levantar com os alunos o que eles acharam e se conseguiram perceber o quanto a matemática está inserida nas mais variadas situações.

Observamos que na referencia [8] existe um simulador do Teste de Miller, que faz todos os cálculos acima.

4.6 Atividade 3

Esta atividade é um jogo, que pode ser executado em gincanas ou mesmo durante a aula. A proposta é que o docente escolha vários números (primos, compostos e pseudoprimos para o teste de Miller) e escreva em pedaços de papel.

Com a turma dividida em grupos, a ideia é pegar cada número e decidir se é primo ou composto, utilizando algum método (fatoração, crivo de Eratóstenes ou teste de Miller).

Após algum tempo, paramos a disputa e somamos os números que cada grupo conseguiu definir a primalidade. Ganha a disputa o grupo cuja soma dos números for maior.

Desta forma, existem duas opções para os grupos: escolher poucos números grandes para testar, ou muitos números pequenos.

4.7 Conclusão

Como foi citado no início dessa sequência didática, o grande intuito é mostrar para os nossos alunos como a matemática está presente no seu cotidiano, mesmo que as vezes indiretamente.

Mostrar a aplicação de um teste de primalidade para os alunos, tem como intuito mostrar a eles que a matemática está aplicada a tecnologia que eles estão inseridos e utilizam diariamente.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] História da criptografia. Disponível em:

http://prof-ricardovianna.blogspot.com.br/2011/05/criptografia-parte-i-historia-da.html

(acesso em 01/08/2014)

[2] COUTINHO S. C., Números Inteiros e Criptografia RSA. Coleção Matemática e Aplicações, IMPA, 2013.

[3] História do Prêmio Godel. Disponível em:

http://www.matematika.it/public/premi/Premio%20GODEL.pdf

(acesso em 01/09/2014)

[4] Lemos Manoel, Criptografia, Números Primos e Algoritmos.Disponível em:

http://www.impa.br/opencms/pt/biblioteca/pm/PM_04.pdf

(acesso em 20/07/2014)

[5] Universidade de Lisboa, Página dos Números Primos. Disponível em:

http://www.educ.fc.ul.pt/icm/icm98/icm12/Historia.htm

(acesso em 20/07/2014)

[6] Santos José Plinio O., Introdução à teoria dos números.Coleção Matemática Universitária, IMPA, 2009.

[7] Martinez, Fabio Brochero; et al , Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro,IMPA , 2011

[8] Simulador do Teste de Miller: http://gandraxa.com/miller_rabin_primality_test.xml (acesso em 15/10/2014)

[9] Números primos de Mersenne. Disponível em:

http://www.profcardy.com/artigos/mersenne.php

(acesso em :15/10/2014)

[10] Tabela com números de Primos de Mersenne: http://www.mersenne.org/primes/

[11] Deterministic variants of the test Disponível em :

http://en.wikipedia.org/wiki/Miller%E2%80%93Rabin_primality_test (acesso em 15/10/2014)

[12] Teorema Chinês do Restos. Disponível em:

http://www.mat.puc-rio.br/ jairo/MAT1310/ (acesso em 25/01/2015)

[13] Congruência de polinômios.

http://www.rumoaoita.com/site/attachments/065_filipe_aulas_congruencia.pdf

(acesso 25/01/2015).