UNIVERSIDADE ESTADUAL DO MATO GROSSO DO SUL

Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT

VAGNER CACERES SOARES

NÚMEROS PRIMOS: APLICAÇÕES E PRIMALIDADE

Dourados -MS

2015

VAGNER CACERES SOARES

NÚMEROS PRIMOS: APLICAÇÕES E PRIMALIDADE

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROMAT oferecido pela Universidade Estadual do Mato Grosso do Sul - UEMS, sob orientação do Professor Dr. Alberny Alves Ferreira como exigência para a conclusão do curso.

DOURADOS

2015

VAGNER CACERES SOARES

NÚMEROS PRIMOS: APLICAÇÕES E PRIMALIDADE

Profº. Dr.: Alberny Alves Ferreira -Professor Orientador

Profº. Dr.Cosme Eustáquio Rubio Mercedes

Profª. Dra. Maristela Missio

Prof° Dr. Robert Jesus Rodrigues Reyes

DOURADOS

2015

Agradecimentos

Agradeço primeiramente a Deus por todas as oportunidades e pela vida. Aos meus colegas de classe por toda ajuda, todas as palavras e pelo companheirismo. Aos professores Cosme Eustáquio Rubio Mercedes, Maristela Missio, Aguinaldo Lenine e Alberny Alves Ferreira pelos conhecimentos compartilhados, foram com certeza de grande valia. Que Deus possa recompensa-los por tudo que fizeram por mim e que abençoe sempre o caminho de cada um.

Resumo

Neste trabalho é apresentado primeiramente os conceitos básicos para compreensão dos estudos posteriores. Em seguida, a definição de primos, bem como os tipos de primos que já foram estudados. Após, uma das mais importantes aplicações dos números primos, a criptografia: definições e exemplos. E para finalizar um estudo sobre os testes de primalidade que há tempos tem movido a curiosidade de muitos matemáticos do mundo todo. Destacando seis testes notáveis com suas definições, teoremas e exemplos.

PALAVRAS CHAVES: primos, primalidade, aplicações, criptografia.

Abstract

This paper first presented the basics for understanding of further studies. Then, the definition of prime and prime types that have been studied. After one of the most important applications of prime numbers, encryption: definitions and examples. And to complete a study of the primality tests that has long moved the curiosity of many mathematicians worldwide. Highlighting remarkable six tests with their definitions, theorems and examples.

KEYWORDS: Prime, Primality, applications, encryption.

Sumário

Introdução

Os números primos tem sido fonte de curiosidade e estudo desde a Grécia antiga, e teve suas maiores descobertas no século XIX. Através do Teorema Fundamental da aritmética podemos concluir que os números primos são como tijolos do sistema de numeração, pois todos os outros números podem ser obtidos através do produto entre primos.

Há muitas corridas em torno dos números primos. Um sonho dos especialistas em Teoria dos números é encontrar uma função que fornecesse somente números primos, uma infinidade deles. Assim, $f(n) = n^2 - n + 41$ fornece números primos para $n < 41$, já o polinômio quadrático $f(n) = n^2 - 79n + 1601$ fornece primos para $n < 80$. Temos ainda a conjectura de Fermat (1640), que diz serem primos todos os números da forma $f(n) = 2^{2^n} + 1$ e que foi provada negativamente por W. H. Mills em 1947.

Outra notável corrida, que ocupou muitos matemáticos e programadores, é a de encontrar o maior número primo. Nesta época ainda não havia um teste eficiente para verificar se um número muito grande era primo, por setenta e cinco anos o maior número primo efetivamente testado foi o $2^{127} - 1$ com trinta e nove algarismos obtido em um trabalho do francês Anatole Lucas (1842-1891) em 1876. Em 1952, com a ajuda computacional conseguiu-se mostrar que $180(2^{127} - 1)^2 + 1$ que possuía setenta e nove algarismos. Desde então computadores mostraram que são primos os números da forma $2^n - 1$ para muitos valores de n.

O que para muitos não passava de uma corrida sem objetivo nenhum, se tornou de importância quando em 1970 foram utilizados no comércio os números primos com mais de 100 algarismos, na conhecida hoje como criptografia. Agora a corrida pelos números primos tinha outro sentido.

Por fim, ainda não se conseguia determinar se certo número era primo ou composto. Alguns testes foram desenvolvidos, porém possuíam muitas restrições ou não era viável na verificação para números muito grandes. Até que em 2002 um professor indiano e seus dois alunos desenvolveram um teste que pode fazer isso, através de um algoritmo determinístico em tempo polinomial. [1]

1. Conceitos básicos

Nesta seção serão apresentados os conceitos básicos necessários ao entendimento deste trabalho.

1.1. Divisibilidade

Definição 1.1. Dados $a\ e\ b\ \in \mathbb{Z}, com\ a \neq 0$, dizemos que a divide b quando existir $c \in \mathbb{Z}\ tal\ que\ b = ac$.

Notação 1.1. Se a divide b escrevemos a|b. Se a não divide b escrevemos a∤b.

Exemplo 1.1. O número 2 divide o número 10 porque podemos tomar 5 tal que é verdadeira a igualdade 10 = 2 . 5

Exemplo 1.2. O número 3 não divide 14, pois não existe natural c tal que 14 = 3. c.

Proposição 1.1.
$Se\ a, b\ e\ c\ \in \mathbb{Z}\ com\ a\ \neq 0\ e\ x\ e\ y\ \in \mathbb{Z}\ são\ tais\ que\ a|b\ e\ a\ |c\ então\ a|(xb \pm yc)$.

Demonstração: Se a|b e a|c então existe n_1 e n_2 inteiros tais que $b = an_1$ e $c = an_2$. Assim $xb \pm yc = xan_1 \pm yan_2 = a(xn_1 \pm yn_2)$. Como $xn_1 \pm yn_2$ é inteiro, pois é composto apenas por elementos de $\mathbb{Z}$, logo existe $n_3 = xn_1 \pm yn_2$ tal que $xb \pm yc = an_3$. Portanto a|xb±yc.

Proposição 1.2. (Divisão Euclidiana) Sejam a e b dois números naturais com 0<a<b. Existem dois únicos números naturais q e r tais que b=a.q+r, com r<a.

Demonstração: Suponha b > a e considere, enquanto fizer sentido, os números:

B, b – a, b – 2.a, . . . , b – n.a, . . .

Pela Propriedade da Boa Ordem, o conjunto S formado pelos elementos acima tem um menor elemento (r = b – q . a). Vamos provar que r tem a propriedade requerida, ou seja, r < a. Se a|b, então r = 0 e nada mais temos a provar. Se, por outro lado, a∤b, então r≠a, e, portanto, basta mostrar que não pode ocorrer r > a. De fato, se isto ocorresse, existiria um número natural c < r tal que r = c + a. Consequentemente, sendo r = c + a = b – q . a, teríamos

$$c = b - (q+1).a \in S, \qquad com\ c < r$$

contradição com o fato de r ser o menor elemento de S. Portanto temos que b = a.q + r com r < a, o que prova a existência de q e r. Agora, vamos provar a unicidade. Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Logo, se r = b – a . q e r' = b – a . q', com r < r' < a, teríamos r'- r ≥ a, o que acarretaria r'≥ r + a ≥ a, absurdo. Portanto, r = r'. Daí segue-se que b - a.q = b - a.q' o que implica que a.q=a.q' e, portanto, q=q'.[2]

1.2. Máximo divisor comum

Definição 1.2. Dados dois números inteiros positivos a e b, não simultaneamente nulos, dizemos que o número inteiro positivo d é um divisor comum de a e b se d|a e d|b.

Exemplo 1.3. O número 3 é divisor comum de 12 e 15 pois 3|12 e 3|15.

Definição 1.3. Dizemos que d é o máximo divisor comum de a e b se:

i) d é um divisor comum de a e b.
ii) Se d_1 é um divisor comum de a e b então d_1|d.

Notação 1.2. Se d é o máximo divisor comum de a e b escrevemos d=(a,b).[²]

Exemplo 1.4. Os números 2 e 4 são os divisores comuns de 8 e 12, então o número 4 é o máximo divisor comum pois 2|4, ou seja, (8,12) = 4.

1.3. Mínimo múltiplo comum

Definição 1.4. Um número c é um múltiplo comum de dois inteiros a e b se a|c e b|c.

Exemplo 1.5. O número 20 é múltiplo comum de 4 e 5 pois 4|20 e 5|20.

Definição 1.5.
Sejam a e b dois inteiros tais que $a \neq 0$ *ou* $b \neq 0$. *Dizemos que* $m > 0$ *é o mínimo múltiplo comum de a e b se*:

i) m é um múltiplo comum de a e b.
ii) Se c é um múltiplo comum de a e b então m|c.

Notação 1.3. Se m é o mínimo múltiplo comum de a e b escrevemos m=[a,b].[2]

Exemplo 1.6. Os múltiplos comuns de 4 e 5 são 20, 40, 60, ... como 20|40, 20|60 e dividirá os outros múltiplos pois seguem uma sequência, então 20 é o mínimo múltiplo comum de 4 e 5, ou seja, [4,5]=20.

1.4. Congruências

Definição 1.6. Seja m um número inteiro positivo. Dizemos que dois números inteiros a e b são congruentes módulo m se os restos da sua divisão euclidiana por m são iguais.

Notação 1.4. $Se\ a\ é\ congruente\ a\ b\ módulo\ m\ escrevemos\ a \equiv b\ mod\ m.$

Exemplo 1.7. Temos que $21 \equiv 5\ mod\ 4$ pois 21 deixa resto 1 quando dividido por 4 e 5 também deixa resto 1 quando dividido por 4.

Proposição 1.3. Sejam *a* e *b* dois inteiros quaisquer e seja *m* um inteiro positivo. Diz-se que *a* é congruente a *b* módulo *m* se *m*|*a-b*.

Demonstração: Se $a \equiv bmod\ m$ então a e b deixam mesmo resto quando divididos por m, logo $a = mx + r\ e\ b = my + r$. Fazendo a – b obtemos

$$a - b = mx + r - my - r = mx - my = m(x - y)$$

Portanto m|a-b.[2]

2. Números Primos

Definição 2.1.Um número inteiro p>1 é um número primo se ele for divisível somente por 1 e por si mesmo.

Exemplo 1.7. Os números 2, 3, 5, 7, são os primos menores que 10. Note que o número 2 é o único primo par, os outros primos serão todos ímpares.

Definição 2.2. Um número inteiro positivo maior que 1 é um número composto se ele não é um número primo.[2]

Exemplo 1.8. Os números 4, 6, 8, são os compostos menores que 10. Note que todos eles são divisíveis por 1, por eles mesmos e mais um divisor.

2.1. Fatoração em primos

Teorema 2.1. (Teorema fundamental da aritmética) Qualquer inteiro m>1 é um número primo ou pode ser escrito como um produto de números primos, onde o produto é único exceto pela ordem dos fatores.

Demonstração: $n = 2$ é primo. Vamos mostrar a existência da fatoração por primos por indução: Se n é primo não há o que provar. Se n é composto, $n = ab$, $a, b \in \mathbb{N}$, $a < n$, $b < n$ e, por hipótese de indução, a e b se decompõem como produto de primos, portanto n se decompõe como produto de primos.

Vamos agora mostrar a unicidade, também por indução: Suponha que n admita duas fatorações $n = p_1p_2\ldots p_r$ e $n = q_1q_2\ldots q_s$ como produto de primos. O Corolário acima mostra que, como $p_1 \mid q_1q_2\ldots q_r$, p_1 deve dividir algum q_i e portanto $p_1 = q_i$ (pois são ambos números primos) e, como $n/p_1 = n/q_i < n$ admite uma única fatoração prima, por hipótese de indução, concluímos que a fatoração de n é única.

Teorema 2.2. Se p é um número primo e p|ab onde a e b são inteiros positivos, então p|a ou p|b.

Corolário 2.1. Se um número primo p divide um produto de inteiros $q_1q_2...q_n$ então $p|q_i$ para algum i, $1 \leq i \leq n$.

Corolário 2.2. Se um número primo p divide o produto de primos $q_1q_2...q_n$ então $p=q_i$ para algum i, $1 \leq i \leq n$.

Teorema 2.3. Existem infinitos primos.

Demonstração: Suponha que o conjunto dos números primos seja finito, digamos $\{ p_1, p_2,\ldots, p_n\}$. Nesse caso, o número $N = p_1p_2\ldots p_n + 1$ seria maior que todos os primos, mas não divisível por nenhum deles, pois $p_i \mid (p_1p_2\ldots p_n + 1) \Rightarrow p_i \mid 1$, absurdo. Teríamos então um natural $\mathbf{N} > 2$ que não seria múltiplo de nenhum primo, contradizendo o teorema fundamental da aritmética.

Teorema 2.4. (Pequeno teorema de Fermat) Se p é um números primo se a é um inteiro qualquer então $a^p \equiv a \; mod \; p$.

Demonstração: Se $p \mid a$, então $a^p \equiv a \equiv 0$ (módulo p). Se p não divide a, então mdc (a, p) =1 $\Rightarrow a^{p-1} \equiv 1$ (módulo p) $\Rightarrow a^p \equiv a$ (módulo p).[3]

2.2. Função ϕ de Euler.

Definição 2.3. Se n=1 então ϕ(n)=1, se n>1 então ϕ(n) é o número de inteiros k tais que $1 \leq k < n$ e (k,n)=1.

Teorema 2.5. Sejam r e s números inteiros positivos com r>1, s>1 e (r,s)=1. Então ϕ(r.s)=ϕ(r).ϕ(s).

Teorema 2.6. Se o número n>1, então ϕ(n)=n-1 se e somente se n é primo.

Demonstração: Se $n > 1$ é primo, então cada um dos inteiros positivos menores que n é primo com n e, portanto, $\phi(n) = n - 1$. Se, por outro lado $\phi(n) = n - 1$, com $n > 1$, então n é primo, pois, se n fosse composto, teria pelo menos um divisor d tal que $1 < d < n$, de modo que pelo menos dois dos inteiros 1,2,3,...,n não seriam primos com n, isto é, $\phi(n) = n - 2$. Logo, n é primo.

Teorema 2.7. Se p é primo e k é um inteiro positivo, então:

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$$

Demonstração: De 1 até p^k, temos p^k números naturais. Precisamos excluir desses números os que não são primos com p^k, ou seja, todos os múltiplos de p, que são p, $2p$, ..., $p^{k-1}p$, cujo número é p^{k-1}. Portanto, $\phi(pk) = p^k - p^{k-1}$.

Teorema 2.8. Se $n = {p_1}^{k_1} \dots {p_r}^{k_r}$ é a decomposição de n em fatores primos, então $\phi(n) = {p_1}^{k_1} \dots {p_r}^{k_r} . \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$.

Demonstração: Como os p_r's são números primos temos que,

$$\phi(n) = \phi\left(p_1^{k_1} \dots p_r^{k_r}\right) = \phi\left(p_1^{k_1}\right) \dots \phi\left(p_r^{k_r}\right) = \left(p_1^{k_1} - p_1^{k_1 - 1}\right) \dots \left(p_r^{k_r} - p_r^{k_r - 1}\right) =$$

$$p_1^{k_1} . \left(1 - \frac{1}{p_1}\right) . p_2^{k_2} . (1 - \frac{1}{p_2}) \dots p_r^{k_r} \left(1 - \frac{1}{p_r}\right) = \; p_1^{k_1} \dots p_r^{k_r} . \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Lema 2.1. Seja a e n>1 inteiros, tais que o (a,n)=1. Se a_1, a_2, ..., $a_{\phi(n)}$ são os inteiros positivos menores que n e que são primos com n, então cada um dos inteiros a_1, a_2, ..., $a_{\phi(n)}$ é congruente módulo m a um dos inteiros a_1, a_2, ..., $a_{\phi(n)}$ (não necessariamente nessa ordem).

Teorema 2.9. (Teorema de Euler) Se n é um inteiro positivo e se (a,n)=1 então $a^{\phi(n)} \equiv 1\ mod\ n$.

Demonstração: Para n = 1 o teorema é válido, pois, temos $a^{\phi(1)} \equiv 1 \mathrm{mod}\, \mathrm{n}$. Suponhamos, pois, n > 1. Sejam a_1, a_2... , $a_{\phi(n)}$ *a*os inteiros positivos menores que n e que são primos com n. Como $(a,n) = 1$ então pelo Lema anterior, os inteiros $a.a_1$, $a.a_2$... , $a.a_{\phi(n)}$ são congruentes módulo n, não necessariamente nesta ordem, aos inteiros a_1, a_2... , $a_{\phi(n)}$, isto é,

$$a.a_1 \equiv a_1' mod\ n$$

$$a.a_2 \equiv a_2' mod\ n$$

.....

$$a.a_{\phi(n)} \equiv a_{\phi(n)}' mod\ n$$

Onde $a_1', a_2', \dots, a_{\phi(n)}'$ são os inteiros $a_1, a_2, \dots, a_{\phi(n)}$ numa certa ordem. Multiplicando essas ϕ(n) congruências obtemos:

$a.a_1, a.a_2, \dots, a.a_{\phi(n)} \equiv a_1'.a_2'.\dots.a_{\phi(n)}'\ mod\ n$. Daí temos

$a^{\phi(n)}(a_1.a_2.\dots.a_{\phi(n)}) \equiv a_1'.a_2'.\dots.a_{\phi(n)}' mod\ n$. Como $(a_i, n) = 1$ podemos cancelar o fator comum e portanto $a^{\phi(n)} \equiv 1\ mod\ n$. [4]

3. Aplicações

3.1. Cálculo do M.M.C.

Uma das mais simples e importante aplicação dos números primos é a determinação do mínimo múltiplo comum de um grupo de números naturais. Tal processo é feito através da decomposição simultânea em fatores primos.

Exemplo 3.1. Vamos determinar o mínimo múltiplo comum dos números 12 e 15.

12, 15	2
6, 15	2
3, 15	3
1, 5	5
1, 1	

O mínimo múltiplo comum de 12 e 15 é o produto dos números, 2, 2, 3 e 5, ou seja,
[12,15] = 2.2.3.5 = 60

Exemplo 3.2. Vamos calcular agora o m.m.c dos números 8, 12 e 9.

8, 9, 12	2
4, 9, 6	2
2, 9, 3	2
1, 9, 3	3
1, 3, 1	3
1, 1, 1	

Portanto o mínimo múltiplo comum de 8, 9 e 12 é o produto 2.2.2.3.3= 72.

3.2. Cálculo do m.d.c.

Os números primos também podem ser aplicados para o cálculo do máximo divisor comum. O método da decomposição em fatores primos que nos permite tal cálculo.

Exemplo 3.3. Vamos determinar o m.d.c dos números 12 e 20.

Temos as seguintes decomposições em fatores primos

12 = 2. 2. 3

20= 2. 2. 5

Como o fator dois repete-se nas duas decomposições por duas vezes, então o mdc de 12 e 20 é 2.2=4, ou seja, (12,20) = 4.

3.3. Decomposição do Fatorial

Geralmente no segundo ano do ensino médio há no estudo de Análise Combinatória a dificuldade em calcular o fatorial de um número muito grande, os números primos pode ser uteis durante este processo.

Definição 3.1: Dado n ∈ ℕ, se n é 0 (zero) ou 1 (um) então o fatorial de n será 1 (um). Caso $n \geq 2$ então o fatorial de n será o produto n. (n-1). (n-2). ... .1. E escrevemos n!.

Exemplo 3.4: Os valores de 5!, 10! e 20! são iguais respectivamente a:

5!=5.4.3.2.1=120

10!=10.9.8.7.6.5.4.3.2.1=3.628.800

20!=20.19.18.17. ... . 3.2.1=2.432.902.008.176.640.000

Definição 3.2: Seja m um natural composto, o valor $E_p(m)$ é o maior expoente da maior potencia de p que divide m. O expoente que aparece na decomposição de m em fatores primos.

Notação 3.1: Vamos utilizar a notação $\left[\frac{n}{p}\right]$ para indicar o quociente da divisão euclidiana de n por p.

Teorema 3.1: (Legendre) Seja n um número natural e p um número primo. Então,

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ ... + \left[\frac{n}{p^m}\right]$$

Onde m é um número natural e p^m é menor que n.

Exemplo 3.5: Vamos fazer a decomposição do 10! usualmente e depois usando o teorema de Legendre.

3.628.800	2
1.814.400	2
907.200	2
453.600	2
226.800	2
113.400	2
56.700	2
28.350	2
14.175	3
4.725	3
1.575	3
525	3
175	5
35	5
7	7
1	

Temos que $10! = 2^8 . 3^4 . 5^2 . 7$

Utilizando o Teorema de Legendre é preciso encontrar $E_p(10!)$ para todo primo p menor ou igual a 10.

$$E_2(10) = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] = 5 + 2 + 1 = 8$$

$$E_3(10) = \left[\frac{10}{3}\right] + \left[\frac{10}{9}\right] = 3 + 1 = 3$$

$$E_5(10) = \left[\frac{10}{5}\right] = 2$$

$$E_7(10) = \left[\frac{10}{7}\right] = 1$$

Logo $10! = 2^8 . 3^4 . 5^2 . 7^1$.

3.4. Criptografia

Atualmente a aplicação mais notável dos números primos é na *Criptografia de Chave Pública*. Um grande avanço foi conseguido na *Criptografia* com o aparecimento dos criptosistemas de *chave pública* em 1976. A ideia é a seguinte: no lugar de uma chave secreta, de posse tanto do emissor quanto do receptor, temos duas chaves. Uma delas é pública, disponível para qualquer pessoa, e uma segunda, privada, de posse apenas de receptor, que serve para decodificar a mensagem. O emissor codifica a mensagem com a chave pública e a transmite. O receptor decodifica a mensagem com a chave privada. Caso alguém intercepte a mensagem, não saberia qual é a chave privada, pois ela não é transmitida a ninguém. Essa ideia se concretizou em 1977, através de Rivest, Shamir e Adleman do Instituto Tecnológico de Massachusetts que criaram o algoritmo *RSA.* Para implementar o mais conhecido dos algoritmos de chave pública o *RSA*, precisamos escolher dois números primos muito grandes *p* e *q*. Para codificar a mensagem usamos $n = p:q$ e para decodificar precisamos conhecer *p* e *q*. A segurança do método vem da dificuldade de fatorar *n* para descobrir *p* e *q*.[5]

3.4.1. Criptosistemas de Chave Pública

Recorde que um Criptosistema de Chave Pública é caracterizado pela existência de uma *chave privada* e uma *chave pública*. Deste modo, para cada usuário U, a chave pública de U está disponível para todos os usuários, e isto inclui a função codificação *EU*. Porém a chave privada de U é conhecida somente por U e consiste da função decodificação *DU*. Além disso, as funções codificação e decodificação são baseadas na noção de uma funçãoo "armadilha" ou trapdoor. Uma função armadilha é uma função f tal que as seguintes propriedades são válidas:

i) *f é* fácil de calcular;
ii) f^{-1} é difícil de calcular;
iii)f^{-1} *é* fácil de calcular quando uma função armadilha torna-se disponível.

Desta forma temos que o Criptosistema de Chave Pública consiste de duas famílias *EU* e *DU* (onde *U é* o conjunto formado por todos os usuários potenciais de funções codificação e decodificação, respectivamente, tais que:

i) Para todo *U*, *DU* (*EU*(*M*) = *M*, onde M é um bloco da mensagem pré-codificada;

ii) Para todo *U*, *EU* está no diretório público, mas *DU* é conhecida somente por *U*;

iii) Para todo *U*, *EU* é a função armadilha ;

iv) Para todo U *EU*(*DU*(*M*) = *M*(assinatura digital).[5]

3.4.2. A matemática do criptosistema RSA

No Criptosistema RSA, dois números primos distintos p e q são escolhidos e mantidos secretos, o produto $N = p.q$ é conhecido. Como N é o produto de dois números primos p e q temos que $\phi(N) = (p - 1).(q - 1)$. Desta forma, cada usuário escolhe inteiros e, d menores que $\phi(N)$ tais que $(e, \phi(N)) = 1$ e $e.d = 1 \bmod (\phi(N))$ onde e é conhecido, mas d é mantido secreto. As funções *codificaçãoao* e *decodificação*, são respectivamente: $E(x) = x^e mod N \; e \; D(x) = x^d mod N, onde \; 1 \leq x < N,$ representa um bloco da mensagem pré-codificada, isto é, uma mensagem onde houve uma mudança de alfabeto. Suponhamos que a mensagem a ser transmitida seja "Viva Hoje". Podemos fazer a seguinte mudança: V=31; I=18; A=10; H=17; O=24; J=19 e E=14. Desta forma obtemos uma pré-codificação em blocos da mensagem a ser transmitida: 31-18-31-10-99-17-24-19-14, onde o 99 é o espaço entre as palavras. Usando o Algoritmo de Euclides podemos determinar o inteiro d tal que $e.d=1 \bmod \phi(N)$. Mostraremos agora que E(D(x))=x e D(E(x))=x, ou seja, as funções E e D são inversa uma da outra, e é por isso que o método funciona. Note que:

$$D\big(E(x)\big) = D(x^e mod N) = x^{e.d} \; mod N$$

$$E\big(D(x)\big) = E(x^d mod N) = x^{e.d} mod N$$

Queremos mostrar que $x^{e.d} \equiv x mod N$. Como N=p.q, onde p e q são primos distintos calculemos $x^{e.d} mod p \; e \; x^{e.d} mod q$ temos que $e.d \equiv 1 mod\big(\phi(N)\big)$.

Consequentemente existe um número k tal que $e.d = 1 + k\phi(N) = 1 + k(p-1)(q-1)$ logo $x^{e.d} = x(x^{p-1})^{k(q-1)} mod p$. Para todo x tal que p não divide x e p primo, aplicando o Pequeno Teorema de Fermat temos $x^{p-1} \equiv 1 mod p$. Logo $x^{e.d} \equiv x mod p$ vale para qualquer p. Analogamente $x^{q-1} \equiv 1 mod q$ vale para qualquer q. Observe que

não podemos usar o argumento diretamente para N, pois o faro (N,x)≠1 não significa que $x \equiv 0 mod N, pois\ N$ é $composto$.[5]

Exemplo 3.4. Seja 31-18-31-10-99-17-24-19-14 e os parâmetros p=11 e q=13, daí N=11.13=143. Temos que

$$\phi(\mathrm{N}) = (\mathrm{p}-1)(\mathrm{q}-1) = (11-1)(13-1) = 10.12 = 120$$

Sabemos que $\left(e, \phi(\mathrm{N})\right) = 1$, desta forma vamos considerar e = 7. Podemos assim determinar o valor de d,

$$e.d \equiv 1\ mod\ \phi(\mathrm{N}) \rightarrow 7\mathrm{d} \equiv 1\ \mathrm{mod}\ 120 \rightarrow 120|7\mathrm{d}-1 \rightarrow 7\mathrm{d}-1 = 120\mathrm{k}$$

Assim temos a equação

$$7d - 120k = 1$$

Resolvendo a equação obtemos o menor d positivo como sendo 103. Vamos então decodificar e codificar o valor x = 14. Temos

$$E(x) = x^e mod N = E(14) = 14^7 mod 143 = 53$$
$$D(x) = x^d mod N = D(53) = 53^{103} mod 143 = 14$$

Onde $a\ mod\ n$ é igual ao resto da divisão de a por n.

Assim funciona a criptografia RSA, lógico que supomos um parâmetro 11 e 13, pequenos, os sistemas de segurança usam fatores primos com mais de 100 casas decimais, o que torna o trabalho de descobrir tais fatores, bem difícil.

4. Tipos de Primos

Listamos agora alguns primos que receberam nomes por terem sido fonte de curiosidade e estudo durante muito tempo.

4.1. Primos de Fermat

Em 1640, Fermat mostrou que os números $F_n = 2^{2^n} + 1$ são primos para n=0,1,2,3,4, e conjecturou que todo número desta forma é primo ficando conhecidos como Números Primos de Fermat. Em 1739, cerca de 100 anos mais tarde Euler demonstrou que a conjectura de Fermat era falsa ao provar que $F_5 = 2^{32} + 1$ é divisível por 641. Ainda não se conhece nenhum outro número primo de Fermat além dos cinco primeiros (3,5,17,257,65537). Como também não se sabe se existe uma infinidade de números primos de Fermat ou não.[6]

4.2. Primos de Mersenne

Os números primos de Mersenne tem relação com os números perfeitos. Um número se diz perfeito, se a soma dos seus divisores próprios é igual a si mesmo. Por exemplo, 6 é um número perfeito pois 6=1+2+3, onde 1, 2 e 3 são divisores próprios de 6. O número 28 também é perfeito, assim como o 496 e 8128. Sempre que se descobre um número primo da forma $2^n - 1$ pode se gerar um número perfeito par multiplicando-o por 2^{n-1}. Euclides, no livro IX dos Elementos, demonstrou que qualquer número na forma $2^{n-1}(2^n - 1)$ é par perfeito, se e somente se, $2^n - 1$ for primo. Os números $M_q = 2^q - 1$, q é um número primo, são chamados números de Mersenne. O maior número primo conhecido é um número de Mersenne $2^{32.582.657}$, um gigante com 9.808.358 dígitos, descoberto pelo time de colaboradores formado pelos doutores Curtis Cooper e Steve Boone, do Departamento de Ciência da Computação da Universidade Central de Missouri, no dia 4 de setembro de 2006.

4.3. Números Primos de Sophie e Germain

No início do século XIX o Último Teorema de Fermat era o mais famoso problema da teoria dos números. Muitos matemáticos, inclusive Euler, tinham fracassado ao tentar demonstra-lo gerando um certo desânimo. Todavia, uma descoberta de Marie-Sophie Germain (1776-1831) matemática francesa, fez com que os matemáticos retomassem a busca pela demonstração. O teorema enunciado por Sophie Germain diz que "se p é um número primo de modo que 2p+1 também seja primo, então não existem inteiros x,y e z diferentes de zero e não múltiplos de p, tais que $x^p + y^p = z^p$". Os números p tais que 2p+1 é primo são conhecidos como primos de Sophie Germain. Esse resultado causou um choque no estudo do Último Teorema de Fermat e era superior aos obtidos pelos matemáticos da época. O choque não foi apenas matemático, mas social também pois Sophie Germain teve que adotar um pseudônimo masculino Antonie August Le-Blanc para ser aceita pelos matemáticos. Durante muito tempo Sophie Germain se correspondeu com Gauss usando o pseudônimo masculino. Porém em 1807 ela revelou sua identidade Gauss escreveu-lhe uma carta encantadora. Outro matemático da época que a aprovou foi Adrien-Marie Legendre (1752-1833) que se tornou seu amigo e mentor. Acredita-se que existem infinitos números primos de Sophie Germain.[7]

4.4. Primos Gêmeos

Primos Gêmeos são os números primos tais que dado um número primo p, p+2 também será um número primo. Os números primos gêmeos formam pares, como por exemplo (3,5), (5,7), (11,13), (17,19), (71,73). Os matemáticos acreditam que existem infinitos números primos gêmeos, conjectura ainda não provada. Em1919, o matemático norueguês Viggo Brun (1885-1978) demonstrou um resultado curioso: *a soma dos inversos dos números primos gêmeos é infinita.* O valor dessa soma é conhecido como constante de Brun.

5.Teste de primalidade

Os números primos são de fundamental importância na matemática em geral, e na teoria dos números em particular. Então é de grande importância estudar as diferentes propriedades dos números primos. De especial interesse são aquelas propriedades que permitem determinar de forma eficiente se um número é primo. Tais testes são também eficientes e utilizados na seguinte prática: uma série de protocolos de criptografia precisa de grandes números primos. Usando P para denotar o conjunto dos números primos. A definição de números primos já nos dá uma forma de determinar se um número n pertence a P: tentar dividir n por cada número $m \leq \sqrt{n}$ - Se algum m dividir n então é composto, caso contrário é primo. Este teste é conhecido desde a Grécia Antiga – isto é uma particularidade do Crivo de Eratóstenes (240 A.C.) que determina todos os primos menores que n. O teste, contudo, é ineficiente: usamos $\sqrt{n}$ passos para determinar se n é primo. Um teste eficiente deve necessitar apenas de um número polinomial de passos (uma entrada de tamanho log n). A propriedade que quase nos dá um eficiente teste é o Pequeno Teorema de Fermat: Para um número primo p, e um número a não divisível por p, $a^{p-1} \equiv 1(mod\ p)$. Temos um a e n que podem ser checados eficientemente se $a^{n-1} \equiv 1(mod\ n)$ usando repetidamente até a $(n-1)^{th}$ potencia de a. Por outro lado esse não é um teste correto, de que muitas composições n satisfaçam isto para alguns a's. Não é fácil provar se um determinado número inteiro é primo ou não, mas existem algoritmos muito eficientes que provam a primalidade de um inteiro positivo. Tais algoritmos são chamados Testes de Primalidade. Os testes de primalidade podem ser: *determinísticos* ou *probabilísticos.* Os testes de primalidade determinísticos determinam com certeza se um número inteiro dado é primo ou composto. No entanto, é prático apenas para inteiros pequenos ou inteiros que sejam divisíveis por um primo pequeno. Os testes de primalidade probabilísticos são testes que podem provar que um número é composto, mas podem indicar, apenas com certa probabilidade que um número inteiro é primo. Os testes probabilísticos ainda são muito utilizados por serem mais rápidos, mais eficientes (são executados em tempo polinomial) que os testes determinísticos. Vejamos agora alguns desses testes.[8]

5.1. O Crivo de Eratóstenes

É o método determinístico mais antigo conhecido para encontrar todos os primos até um certo inteiro N específico. A palavra Crivo quer dizer peneira. O algoritmo atua, de fato, como uma peneira separando os múltiplos dos primos em sucessão, deixando passar apenas os que não são divisíveis por estes primos. O método consiste em escrever todos os inteiros de 1 a N. Como 1 não é primo, pode ser riscado imediatamente. O algoritmo prossegue, sequencialmente em passos. Em cada etapa, encontramos o primeiro número que não foi riscado, marcamos ele como primo e riscamos todos os seus múltiplos. Enquanto o último número a ser avaliado não excede a raiz quadrada de N, repetimos os passos citados.

Exemplo 5.1. Construir a tabela com todos os primos menores que 100 utilizando o Crivo de Eratóstenes.

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

Os primos p tais que $p \leq \sqrt{100} = 10$ são 2, 3, 5 e 7. Vamos eliminar todos os inteiros compostos que são multiplos de 2, 3, 5 e 7. Os inteiros positivos não riscados 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 todos números primos menores que 100.[4]

5.2. Divisão por tentativas

Proposição 5.1. Todo número inteiro maior que 1 tem um divisor primo.

Demonstração: O número inteiro a tem um divisor que é maior que 1, ou seja, a. Entre todos os divisores de a que forem maiores que 1, seja p o menor de todos. Então p tem que ser primo, caso contrário, p teria um divisor b com $1 < b < p < a$. Contradição.

Proposição 5.2. Se n é um inteiro positivo composto então n possui um divisor primo p que é menor ou igual a $\sqrt{n}$.

Demonstração: Como n é composto podemos escrever $n = a.b$, onde a e b são inteiros positivos: $a > 1\ e\ b > 1$. Temos que $a \leq \sqrt{n}\ ou\ b \leq \sqrt{n}$, do contrário $n = a.b > \sqrt{n}\sqrt{n} = n$. Suponha que $a \leq \sqrt{n}$. Pela proposição 5.1, a tem um divisor primo p. Como $p \leq a \leq \sqrt{n}$ temos que p também é divisor de n. Portanto, n possui um divisor primo p tal que $p \leq \sqrt{n}$.

A proposição 5.2 sugere um algoritmo determinístico para testar se n é um número primo. O algoritmo verifica para todo número primo p que for menor ou igual a $\sqrt{n}$, se ele é um divisor de n. Se for encontrando um divisor primo de n, então n é composto. Do contrário, n é primo. Esse procedimento é chamado Divisão por tentativas. Na prática este teste é utilizado para testar a primalidade de números inteiros pequenos.

Exemplo 5.2. Vamos verificar se o número 43 é primo ou não. Temos que o inteiro mais próximo da raiz quadrada de 43 é o 6. Logo devemos testar se um dos números primos $p \leq 6$ será divisor de 43. Os números primos p menores que 6 são 2, 3, e 5. Nenhum deles é divisor de 43. Portanto 43 é um número primo.[4]

5.3. Teste de Fermat

O Pequeno Teorema de Fermat dá origem a um teste de primalidade probabilístico chamado teste de Fermat. O teste consiste em: Dados $a > 1$, escolha $p > 1$ e calculemos $a^{p-1} mod p$. Se o resultado não for 1modp, então p é um número composto. Se o resultado encontrado for 1 mod p, então p pode ser um número primo e recebe o nome de *primo provável na base a* ou *pseudoprimo* na base *a*.

Exemplo 5.3. O número 341 é pseudoprimo para a base 2, pois $2^{340} \equiv 1 mod 341$.
A existência de pseudoprimos atesta que o Teste de Fermat não é determinístico. Podemos aumentar a eficácia do Teste de Fermat, aplicando-o repetidamente e utilizando várias bases. O número 341, por exemplo, não passa no teste para a base 3, pois $3^{340} \equiv 56 mod 341$. Portanto, 3 é testemunha de que 341 é composto.[3]

5.4. Números de Carmichael

Existem inteiros compostos que não se consegue provar que são compostos pelo Teste de Fermat com qualquer base, isto é, há inteiros que enganam o Teste de Fermat para todas as bases.

Tabela 5.1 O menor pseudoprimo

Inteiro a	Menor pseudoprimo para a base a
2	341 = 11.13
3	91= 7.13
4	15= 3.5
5	4= 2.2
6	35= 5.7
7	25= 5.5
8	9= 3.3
9	28= 4.7
10	33 = 3.11

Portanto, números de Carmichael são pseudoprimos de Fermat para todas as bases.

Exemplo 5.4. O número 561 é um número de Carmichael. Não é fácil provar esta afirmação usando a definição, pois precisaríamos verificar que $a^{561} \equiv a \bmod 561$ para a = 2; 3; ... ; 559 o que dá um total de 558 bases a serem testadas, algumas não tão pequenas. Em 1899, uma caracterização para os números de Carmichael foi dada no Teorema de Korselt.

Teorema 5.1. (Teorema de Korselt) Um inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as duas condições seguintes: $p^2 \nmid n$ e $p-1 \mid n-1$.

Não demonstraremos aqui o Teorema de Korselt, a prova exige conhecimento sobre corpos finitos. Utilizando o Teorema de Korselt podemos mostrar que 561 é um número de Carmichael facilmente.

Exemplo 5.5. Temos que 561 = 3.11.17. Ainda, 3^2 não divide 561, 11^2 e 17^2 também não dividem 561. Por outro lado 2, 10 e 16 dividem 560. Portanto 561 é um número de Carmichael e é o menor deles. Em 1994 os matemáticos Willian Alford, Andrew Granville e Carl Pomerance provaram que há infinitos números de Carmichael.[3]

5.5. Teste de Miller-Rabin

O teste de primalidade de Miller – Rabin é um teste probabilístico criado em 1976 por G. L. Miller e modificado por M. O. Rabin. Este teste é uma pequena modificação do teste de Fermat, sendo mais eficiente, ainda que haja uma pequena chance de erro. Seja n um inteiro positivo ímpar cuja primalidade desejamos testar. O inteiro n-1 é par. Seja s a maior potência de 2 que divide n-1, isto é, $n-1 = 2^s.d$ onde d é ímpar. Seja $1 < b < n-1$ um inteiro que será a base para o teste. Considere as potências de b: $b^d, b^{2d}, b^{2^2d}, \dots, b^{2^{s-1}d}, b^{2^s d}$. Se n for um número primo, então.

$$b^{2^s d} = b^{n-1} \equiv 1 mod n$$

Talvez alguma potência anterior a essa seja congruente a 1 mod n.Seja k o menor expoente tal que $b^{2^k d} \equiv 1\ mod\ n$, isto é, $n | b^{2^s d} - 1$.

Se k = 0 então $b^{2^0 d} \equiv 1\ mod\ n$ daí $b^d \equiv 1\ mod\ n$. Se k > 0, então podemos fatorar $b^{2^k d} - 1$ como $(b^{2^{k-1}d} - 1)(b^{2^{k-1}d} + 1)$. Como n é primo e divide $b^{2^k d} - 1$, então divide um dos dois fatores, mas, n não pode dividir $b^{2^{k-1}d} - 1$ pela escolha de k como o menor inteiro tal que n divide $b^{2^k d} - 1$. Portanto, n divide $b^{2^k d} + 1$, isto é,

$$b^{2^{k-1}d} \equiv -1\ mod\ n$$

Concluímos que: Se n é primo, então para toda base $1 < b < n - 1$ escrevendo as potências $b^d, b^{2d}, b^{2^2 d}, \ldots, b^{2^{s-1} d}, b^{2^s d}$ ou a primeira é congruente a 1 mod n ou alguma delas é congruente a -1 mod n. Se nada disso acontecer, então o inteiro n é composto e dizemos que b é uma testemunha de que n é composto. Se um inteiro positivo composto satisfaz alguma das condições acima para a base b, então n é pseudoprimo forte para a base b.

Exemplo 5.6. Tomando $n = 341$ temos que $n - 1 = 340 = 2^2.85, 0 \leq s < 2$. Sendo b=2 precisamos calcular duas potências

$$2^{2^0.85} = 2^{85} \equiv 32 \; mod \; 341$$

$$2^{2^1.85} = 2^{170} = (2^{85})^2 \equiv 32^2 \equiv 1 \; mod \; 341$$

Como a primeira potência não é congruente a 1 mod 341 e a segunda não é congruente a -1 mod 341, então 2 é a testemunha de que 341é composto.

Exemplo 5.7. Tomando $n = 25$ temos que $n - 1 = 24 = 2^3.3, \; 0 \leq s < 3$. Sendo b=7 precisamos calcular duas potências

$$7^{2^0.3} = 7^3 \equiv 18 \; mod \; 25$$

$$7^{2^1.3} = 7^6 \equiv 24 \equiv -1 \; mod \; 25$$

$$7^{2^2.3} = 7^{12} \equiv 1 \; mod \; 25$$

Como $7^6 \equiv 24 \equiv -1 \; mod \; 25$ segue que 25é um pseudoprimo forte para a base 7, embora saibamos que 25 é composto.[4]

5.6. Teste de Primalidade AKS

Este teste é baseado na seguinte identidade para números primos a qual é uma generalização do pequeno teorema de Fermat.

Lema 5.1$Seja \; a \in \mathbb{Z}, n \in \mathbb{N}, n \geq 2, e \; (a, n) = 1. Então \; n$ é $primo \; se \; e \; somente \; se$

$$(x + a)^n \equiv \; x^n + a \; (mod \; n). \quad (1)$$

Demonstração:

A identidade acima sugere um teste simples para primalidade: dada uma entrada n, escolha um a e teste se a congruência (1) está satisfeita. No entanto, isso leva tempo (n) porque precisamos avaliar n coeficientes, na pior das hipóteses. Uma maneira simples de reduzir o número de coeficientes é avaliar ambos os lados de (1) um modulo polinomial da forma X_r - 1 para um pequeno r adequadamente escolhido. Em outras palavras, se o teste seguinte equação é satisfeita:

$$(x + a)^n \equiv x^n + a \ (mod\ x^r - 1, n). \quad (2)$$

Do Lema 2.1 é imediato que todos os primos n satisfazem a equação (2) para todos os valores de a e r. O problema agora é que alguns compostos n podem também satisfazer a equação para alguns valores de a e r. No entanto, nós podemos restaurar a caracterização: nós mostramos que para um número r escolhido apropriadamente, se a equação (2) é satisfeita para vários a então n é uma potencia privilegiada. O número de um a e r adequado são tanto limitado por um polinômio em log n e, portanto, temos um algoritmo determinístico de tempo polinomial para testes de primalidade.

5.6.1. O algoritmo original

$$1. Se\ (n = a^b\ com\ b > 1) então\ n \text{ é } composto.$$

$$2. r = 2.$$

$$3. Enquanto\ (r < n)\ faça,$$

$$4. Se\ (n, r) \neq 1 então\ n \text{ é } composto.$$

$$5. Se\ r \text{ é } primo\ maior\ que\ 2\ então\ faça,$$

$$6. Encontrar\ q, tal\ que\ q\ seja\ o\ maior fator\ primo\ de\ r - 1$$

$$7. Se\ q > 4\sqrt{r}\log_2 n\ \ e\ n^k \not\equiv 1\ mod\ n.$$

$$8. Parar\ teste.$$

$$9. r = r + 1$$

10. $fim.$

11. $Para\ a = 1\ até\ 2\sqrt{r}\ \log n\ \ faça,$

12. $Se\ (x-a)^n \not\equiv (x^n - a)(mod\ n, x^r - 1) então\ n$ é $composto.$

13. $Fim.$

14. n é $primo.$

Até a 10ª linha do teste temos um filtro para os valores de r. Da 11ª linha em diante temos a primalidade do número. A 12ª linha usa a aplicação do Pequeno Teorema de Fermat.

Em outras palavras, o presente teste escolhe um r primo para obter q, o maior fator primo de r-1, tal que este r delimita um intervalo onde certamente haverá um fator primo de n se este for composto. Em seguida testa-se a conguência para $a \in [1, 2\sqrt{r}\log n]$ uma quantidade de vezes em tempo polinomial.

O teste de primalidade AKS faz uso da relação de equivalência (2) a qual pode ser verificada em tempo polinomial. Contudo, enquanto todos os primos satisfazem esta equivalência, alguns números compostos também o fazem. O algoritmo para o teste de primalidade de algum inteiro n consiste em duas partes. O primeiro passo gira em torno de encontrar um número primo conveniente $r = k.q + 1$, tal que:

I)$P(r-1) = q\ onde\ P(x)$é $o\ maior\ fator\ primo\ de\ x.$

II) $q \geq 4\sqrt{r}\log_2 n$

III)$n^k \not\equiv 1\ mod\ r$

Durante este passo é importante verificar se n não é divisível por nenhum primo $p \leq r$. Se ele é divisível então o teste será finalizado pois n seria um número composto.

No segundo passo, um número de testes são realizados para verificar a veracidade da equivalência de dois polinômios no campo $(x-a)^n \not\equiv (x^n - a)(mod\ n, x^r - 1)$. Para todos os inteiros positivos com $a \leq 2\sqrt{r}\log_2 n$ então n é garantidamente primo. Em todos os outros casos ele é composto.

Desde que o teste de primalidade AKS foi desenvolvido (2002) houveram muitos aperfeiçoamentos. Novas variantes foram mostradas por Lenstra (2002), Weisstein (2010), Berrizbeitia (2010), as quais melhoraram a velocidade para determinar o sub-conjunto ao qual pertence o r conveniente.

Em março de 2003 os matemáticos indianos publicaram uma revisão do texto original, o qual continha as mudanças feitas por Hendrik Lenstra Jr. (2002). O algoritmo melhorado ficou assim:

$$Entrada: inteiro\ n > 1$$

$$1 - Se\ (n = a^b\ para\ a \in N\ e\ b > 1), escreva\ COMPOSTO.$$

$$2 - Encontre\ o\ menor\ r\ tal\ que\ o_r(n) > log_2 n.$$

$$3 - Se\ 1 < (a, n) < n\ para\ algum\ a \leq r, escreva\ COMPOSTO.$$

$$4 - Se\ n \leq r, escreva\ PRIMO.$$

$$5 - Para\ a = 1\ até\ \sqrt{\emptyset(r)}\log n\ \ faça,$$

$$Se\ \ (x + a)^n \not\equiv\ x^n + a\ (mod\ x^r - 1, n), escrever\ COMPOSTO.$$

$$6 - Escreva\ PRIMO.$$

A ideia é a mesma do teste original, porém a busca pelo r conveniente foi aprimorada e agilizada. O teste segue os seguintes passos:

1: Verificar se n é potencia perfeita de algum número natural; Se for então n é composto.

2: Encontrar r conveniente;

3: Calcular (a,n), para $a \leq r$, se (a,n) for maior que 1 então n é composto.

4: Se n for menor ou igual a r, n é primo.

5: Verificar a congruência $(x + a)^n \equiv\ x^n + a\ (mod\ x^r - 1, n)$ para todo a que pertença ao intervalo dado. Se não existir a congruência então n é composto.

6: Caso contrário, n é primo.

No teste de primalidade Miller-Rabin, o resultado depende da base que escolhemos. Isso torna inviável para um n muito grande. Então o presente teste constrói um subconjunto de bases que podem dar o resultado correto.[9]

Conclusão

Podemos perceber que os números primos, desde a Grécia Antiga tem sido fonte de curiosidade para os amantes da Teoria dos números. Mas só é possível verificar sua importância quando em 1970 começa a ser utilizado na Criptografia para segurança nas transações financeiras.

Os testes de primalidade ainda não tem um objetivo específico fora o da curiosidade em descobrir mais sobre os primos. Agora o estudo em torno dos números primos continua, a busca é encontrar uma forma de determinar quem são os fatores primos de um número composto muito grande.

Isso seria um grande problema para as transações financeiras que utilizam a Criptografia para esconder usas senhas, pois, com isso seria possível quebrar qualquer sistema nos computadores.

Mas pelo que parece ainda não estamos longe disso, pois como vimos a última descoberta foi a de Manindra e seus alunos com o teste de primalidade em tempo polinomial em AKS.

Tomara que essa descoberta demore um pouco mais para que se possa usufruir da tecnologia que os números primos nos proporcionam através da Criptografia.

Referências Bibliográficas

[1] EVES, H. Introdução à história da Matemática. Howard Eves; tradução: Hygino H. Domingues. Campinas, São Paulo, 2004.

[2] HEFEZ, A. e VILELA, M.L.T., *Elementos de Aritmética* , SBM, Rio de Janeiro, 2006.

[3] ROSEN, K. Elementary number theory and its applications, Library of Congress Cataloging in Publication Data, Canadá, 1986.

[4] KRANAKIS, E. *Primality and Cryptography*, Teubner, Chichester, New York, Brisbane, Toronto, Singapore: Wiley, 1986.

[5] COUTINHO, S.C., *Números Inteiros e Criptografia RSA*, IMPA/SBM, Série de Computação e Matemática, Rio de Janeiro, 1997.

[6] PANTOJA, Pedro. Números de Fermat. Lisboa, Portugal.

[7] PAZ, German. Números Primos de Sophie e Germain, demonstración de su infinitud. Santa Fé, Argentina. 2000.

[8] AGRAWAL, M.,KAYAL, N. e SAXENA, N., *Primes is in P,* Annals of Mathematics, 160 (2004),

[9] BATISTA, C.J., Algoritmo AKS para verificar a primalidade em tempo polinomial, Lavras, Minas Gerais, 2010.