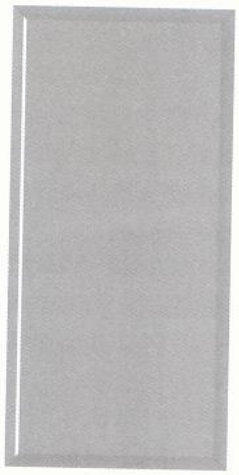
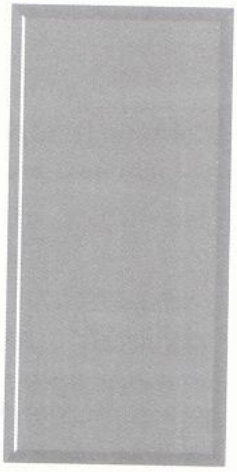


Liege Netto Conrado (Uniso)
Lina Flávia Morete (Uniso)
Mário Biazzi (Uniso)

Os grandes desafios da aritmética: primos em p



Revista de Estudos Universitários | Sorocaba, SP | v. 31 | nº 1 | Jun. 2005 | p. 139-164

RESUMO

Este artigo tem por finalidade descrever alguns testes de primalidade, desenvolvidos ao longo da história da Matemática, e fornecer subsídios matemáticos para que o leitor possa entender a idéia desenvolvida no algoritmo AKS.

Palavras-chave: matemática, história da; números primos; algoritmo.

ABSTRACT

The purpose of this article is to describe some primalidade tests developed throughout the Mathematic's history and to supply mathematical subsidies so that the reader can understand the idea developed in AKS algorithm.

Keywords: Mathematics, history of; prime numbers, algorithm.

"O problema de distinguir números primos de números compostos e de decompor os compostos em seus fatores primos é reconhecido como um dos mais importantes e úteis na Aritmética. Está engajado no trabalho diário e na sabedoria dos modernos geômetras a tal nível que seria supérfluo discutir o problema mais extensamente. Além disso, a dignidade da própria Ciência requer que cada recurso disponível seja explorado para a solução de um problema tão elegante e tão célebre." *Karl Friedrich Gauss*, DisquistionesArithmeticae, *1801*.

1. Introdução

Vamos tratar neste artigo de premissas necessárias para a demonstração do algoritmo, para descobrirmos se um número $N > 1$, qualquer, inteiro, é primo ou composto, além do próprio algoritmo, recentemente descoberto. Os autores dessa proeza são Manindra Agrawal, Neeraj Kayal e Nitin Saxena, do Instituto Indiano de Tecnologia Kanpur. Os algoritmos para determinação de primalidade são importantes na obtenção de números primos muito grandes, usados na confecção de chaves privadas de encriptação. Atualmente dispõe-se de algoritmos probabilísticos que executam em tempo polinomial e acusam se um número é primo, com baixíssimo percentual de erro. O AKS (Agrawal-Kayal-Saxena) é o primeiro algoritmo determinístico a executar esse teste em tempo polinomial. Neste artigo, discutimos as bases matemáticas desse algoritmo. Os primeiros algoritmos criados para testar a primalidade de um número remontam à Grécia antiga. Até 2002, os principais algoritmos desenvolvidos para essa finalidade enquadravam-se em duas grandes classes:

- De tempo não-polinomial e determinísticos: afirmam com 100% de certeza a primalidade de um número, mas o cálculo é realizado em tempo exponencial. Exemplos: Crivo de Eratóstenes, Adleman-Rumely ($(\log\ n)^{O(\log\ \log\ \log\ n)}$).
- De tempo polinomial, mas não-determinísticos: a complexidade do algoritmo é em função de um polinômio — o tempo de cálculo não "explode", quando o número testado é muito grande — mas não dão certeza absoluta quanto à primalidade. Exemplo: Teste de Monte Carlo.

O grande desafio era, portanto, obter um algoritmo de complexidade polinomial e determinístico. Caso esse algoritmo não existisse, o problema

do teste de primalidade seria da classe NP-completo. No entanto, o algoritmo AKS, apresentado no artigo "Primes is in P", é da classe P.

Vamos descrever alguns testes de primalidade desenvolvidos ao longo da história da Matemática. O primeiro algoritmo conhecido é o Crivo de Eratóstenes.

O crivo de Eratóstenes

Desde tempos remotos, os matemáticos são fascinados por problemas que envolvam números primos. Um dos problemas fundamentais dessa área é determinar se um dado número inteiro $N > 1$ é primo. Partindo dos tempos antigos, desde os chineses e os gregos, muito se tem trabalhado nesse tema. O Crivo de Eratóstenes, de 240 a.C., é o mais antigo algoritmo para detectarmos se um número é primo.

O Crivo foi construído numa tabela para qualquer número inteiro; por exemplo, 100 na forma:

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 números sublinhados são primos. Como chegamos a essa conclusão? Começamos pelo 1 que, por definição, não é primo. O primeiro primo positivo é, então, 2. Todos os múltiplos de 2 são necessariamente compostos, por definição. Exclua todos os pares. O próximo primo é 3. Por conseqüência, todos os múltiplos de 3 são compostos. Vamos excluir os múltiplos de 3 e, assim sucessivamente, até que alcancemos um número primo que não tem, na tabela, nenhum múltiplo. Nesse caso aconteceu o fato para $n = 11$. De fato, 22, 33, 44, 55, 66, 77, 88, 99 já estavam excluídos, por serem múltiplos de outros números primos. Com certeza, só restaram números primos, que são os grifados. Qual é, entretanto, o embasamento teórico do

Crivo de Eratóstenes? É o teorema: "Todo número composto a é divisível por um primo tal que $\sqrt{a} \geq p$, sendo p esse primo."

Sendo a um número composto podemos representá-lo na forma: $a = b \cdot c$ Onde $b > 1$ e $c > 1$. Podemos supor $c \geq b$, sem perder a generalidade e, então, $\sqrt{a} \geq b$. Agora, se $b > 1$, existe um divisor primo p, tal que $\sqrt{a} \geq b \geq p$, e que será divisor de b e, logo, de a.

O Crivo foi a primeira prova prática para determinarmos se um número é primo ou composto. Já no século XVII, Fermat provou o conhecido Pequeno Teorema que levou seu nome, no qual afirma que **para qualquer número prio *p***, e qualquer número a , não divisível por ***p***, $a^{p-1} \equiv 1 (\text{mod } p)$. Embora os argumentos desse teorema não sejam seguros, até porque falham espetacularmente para os números de Carmichael, esses resultados têm sido o ponto inicial de diversos e eficientes testes de algoritmos de primalidade (estamos aqui convencionando que o termo primalidade será usado para nomear testes, para sabermos se algum número é ou não primo.). Este é o nosso segundo algoritmo para descobrirmos se um número **p** é primo ou composto.

Pequeno Teorema de Fermat

Dado um número primo qualquer p, o resto positivo que um número a qualquer, inteiro positivo, deixa, quando dividido por p, deve estar na seqüência: 1, 2, 3, ..., $p-1$. Este é, então, um SISTEMA REDUZIDO DE RESTOS, módulo p. Podemos escrever o SRR (Sistema Reduzido de Restos) que será 1,2,3,... $p-1$, como os números primos com p obtidos do SCR (Sistema Completo de Restos). O Sistema Reduzido de Restos tem as seguintes propriedades: i) são $p-1$ números e ii) esses $p-1$ números são dois a dois primos entre si. Se a não é divisível por p, ou seja, $(p,a) = 1$, então a, $2 \cdot a$, $3 \cdot a$, ..., $a(p-1)$ também constitui um Sistema Completo de Restos, no módulo p. É verdade: são $p-1$ números e se $ai \equiv aj (\text{mod } p)$ com $(a,p) = 1$, então $i \equiv j (\text{mod } p)$. Como esses $p-1$ números são dois a dois incôngruos, então podemos afirmar que $a \equiv i (\text{mod } p)$ para algum i da seqüência.

Sucessivamente:

$$2 \cdot a \equiv j (\text{mod } p)$$
$$3 \cdot a \equiv k (\text{mod } p)$$
$$\ldots$$

...

...

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

Como sabemos, o produto das congruências mantém a congruência verdadeira; logo:

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)(\text{mod } p)$$

ou seja,

$$a^{p-1}[1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)]1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)(\text{mod } p)$$

e como

$$(1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1), p) = 1,$$

então,

$$a^{p-1} \equiv 1(\text{mod } p), \text{ c.q.d.}$$

Números de Carmichael

Um número composto ímpar n é um número de Carmichael se, e somente se, para todo a inteiro, com $(a,n)=1$, então $a^{n-1} \equiv 1(\text{mod } n)$.

Para entender o número de Carmichael, suponha que $n=9$ seja um número de Carmichael.

Então, $a = 1, 2, 4, 5, 6$ e 8 são números positivos menores que nove e primos com 9. Logo, 1^8, 2^8, 4^8, 5^8, 7^8 e 8^8 deveriam ser côngruos a 1 mod9. Ocorre que $1^8 \equiv 1(\text{mod } 9)$ e $8^8 \equiv 1(\text{mod } 9)$ são verdadeiras, porém 2^8, 4^8, 5^8, $7^8 \equiv 1(\text{mod } 9)$ são falsas. Portanto, 9 não é um número de Carmichael. Na realidade, o primeiro número de Carmichael é 561. A sucessão dos números de Carmichael é: 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, ...

Para esses números o Teorema de Fermat não define n como um número primo e, por isso, não podemos utilizar o Pequeno Teorema de Fermat, como um teste de primalidade.

Em 1976, Miller usou essa propriedade para obter um algoritmo que desse a primalidade que, depois, foi modificado por Rabin e ainda alterado por Solovay e Strassen, que usaram os restos quadráticos (seus algoritmos são capazes de ser aleatórios sobre HRE, Hipótese de Riemann Extendida); Critério de Euler e o Símbolo de Legendre. A seguir, apresentaremos um terceiro algoritmo para descobrirmos se um número **p** é primo ou composto.

Restos quadráticos

Um número a é chamado um RESTO QUADRÁTICO de outro número inteiro $m > 1$ se a congruência

$$x^2 \equiv a(\text{mod } m)$$

pode ser satisfeita para algum inteiro x.

Se $x^2 \not\equiv a(\text{mod } m)$ para todo x inteiro, então, a é dito não-resto quadrático de m.

Convencionaremos *aRm*, quando a é um resto quadrático de m, e, *aNm*, quando a é não resto quadrático de m.

Zero é *0Rm* para todo m.

Seja agora p um primo; então, o SRR $(\text{mod } p)$ é 1, 2, 3, ..., $p-1$.

Para $p = 2$ só existe um resto quadrático: 1. O SRR no módulo 2 é 1. $x^2 \equiv 1(\text{mod } 2)$ tem solução para $x = 1$.

Para encontrarmos os restos quadráticos de p, basta tomarmos os quadrados do SRR: 1^2, 2^2, 3^2, ... $(p-1)^2$ e, como sabemos, $(p-i)^2 \equiv i^2(\text{mod } p)$. De fato, $(p-i)^2 \equiv p^2 - 2pi + i^2(\text{mod } p)$, mas $p^2 \equiv 0(\text{mod } p)$ e $2pi \equiv$ $\equiv 0(\text{mod } p)$. Portanto, $(p-i)^2 \equiv i^2(\text{mod } p)$. Logo, podemos reduzir esse sistema para a seguinte seqüência: 1^2, 2^2, ..., $[(p-1)/2]^2$. Aplicando para $p = 7$, temos: SRR 1, 2, 3, 4, 5, 6. Os quadrados do SRR são 1^2, 2^2, 3^2, 4^2, 5^2, 6^2. Como $(7-i)^2 \equiv i^2(\text{mod } 7)$, já que $7^2 - 2 \cdot 7 \cdot i \equiv 0(\text{mod } 7)$; então, $6^2 \equiv 1^2$, $5^2 \equiv 2^2$, $4^2 \equiv 3^2$ e podemos trabalhar apenas com a seqüência 1^2, 2^2, 3^2. Os restos quadráticos, quando $p = 7$, são: *1R7*, *2R7* e *4R7*. Evidentemente *3N7*, *5N7* e *6N7*.

Quaisquer dois elementos da seqüência 1^2, 2^2, 3^2, ... $\left(\frac{p-1}{2}\right)^2$ são incongruentes. De fato, se dois desses números são congruentes no módulo p, então a congruência:
$x'^2 \equiv x^2(\text{mod } p)$ implica que $x'^2 - x^2 \equiv 0(\text{mod } p)$ e $(x'+x)(x'-x) \equiv$ $\equiv 0(\text{mod } p) \cdot x' - x \equiv 0(\text{mod } p)$ e $x' \equiv x(\text{mod } p)$ e, então, $x' = x$ e ambos positivos e menores que $p/2$, ou, então, $x' + x \equiv 0(\text{mod } p)$ e daí $x' \equiv -x(\text{mod } p)$, que é uma congruência impossível, já que $0 < x + x' < p$.

Assim, os restos mínimos positivos dos quadrados 1^2, 2^2, ..., $[(p-1/2)^2]$ são todos incôngruos, cqd.

Então, são exatamente $(p-1)/2$ os restos quadráticos para um número primo p qualquer, que é evidentemente, exatamente o número dos não-restos quadráticos.

Agora, $p=11$:

$1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 16$, $5^2 \equiv 25$, logo 1, 3, 4, 5, 9 são restos quadráticos de 11, e 2, 6, 7, 8, 10 são não-restos quadráticos de 11. Isto porque $1^2 \equiv 1$, $3^2 \equiv 9$, $4^2 \equiv 16 \equiv 5$, $5^2 \equiv 25 \equiv 3$, $9^2 \equiv 81 \equiv 4$, no módulo 11.

Nota-se que $2^2 \equiv 4$, $6^2 \equiv 36 \equiv 3$, $7^2 \equiv 49 \equiv 5$, $8^2 \equiv 64 \equiv 9$, $10^2 \equiv 100 \equiv 1$, no módulo 11, o que confirma a previsão inicial, conforme demonstrado acima.

Critério de Euler

Seja p um primo e a inteiro. Do Pequeno Teorema de Fermat temos que: $a^{p-1} \equiv 1 (\text{mod } p)$

Portanto: $a^{\frac{p-1}{2}} \equiv \pm 1 (\text{mod } p)$

O Critério de Euler nos diz que a será um resto quadrático de acordo com o resultado acima, onde

$$aRp \text{ se } a^{\frac{p-1}{2}} \equiv +1 (\text{mod } p)$$

e

$$aNp \text{ se } a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$$

Demonstração:

aRp

Se existir $x^2 \equiv a (\text{mod } p)$, então $(x^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} (\text{mod } p)$ e então $x^{p-1} \equiv a^{\frac{p-1}{2}} (\text{mod } p)$. Mas, como $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$. Então $x^{p-1} \equiv 1 (\text{mod } p)$ é verdadeira pelo Pequeno Teorema de Fermat.

aNp

Se existir $x^2 \equiv a (\text{mod } p)$, então $(x^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} (\text{mod } p)$ e então como $a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$, $x^{p-1} \equiv -1 (\text{mod } p)$, que é absurdo. Portanto aNp cqd.

Símbolo de Legendre

Legendre introduziu um símbolo útil na Teoria dos Números, para representar o sinal quadrático de números com referência a um módulo primo.

Seja a um inteiro positivo não-divisível por p (primo), o símbolo de Legendre será:

$$\left(\frac{a}{p}\right).$$

Temos, então, que $\left(\frac{a}{p}\right)=1$ se aRp e $\left(\frac{a}{p}\right)=-1$ se aNp.

Uma vez que pelo critério de Euler

$$a^{\frac{p-1}{2}} \equiv 1 \text{ ou } a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

de acordo com aRp ou aNp, o símbolo de Legendre é somente definido pela congruência

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Dessa definição as propriedades seguintes do símbolo de Legendre podem ser derivadas imediatamente.

Propriedades do símbolo de Legendre:

$$(I)\left(\frac{a'}{p}\right)=\left(\frac{a}{p}\right) \text{ se } a' \equiv a \pmod{p}$$

Demonstração:

Se $a' \equiv a \pmod{p}$, então as congruências binomiais quadráticas:

$$x^2 \equiv a' \pmod{p} \text{ e } x^2 \equiv a \pmod{p}$$

têm ambas precisamente 0 ou 2 soluções, isto é, a' e a são não-restos quadráticos de p ou a' e a são restos quadráticos de p, de modo que no primeiro caso:

$$\left(\frac{a'}{p}\right)=\left(\frac{a}{p}\right)=-1$$

e no segundo caso:

$$\left(\frac{a'}{p}\right)=\left(\frac{a}{p}\right)=1$$

portanto, nos dois casos:

$$\left(\frac{a'}{p}\right)=\left(\frac{a}{p}\right), \text{ cqd.}$$

***

$$(II)\left(\frac{aa'}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{a'}{p}\right)$$

Demonstração:

Com efeito, se $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$, temos que

$$\left(\frac{aa'}{p}\right)\equiv (aa')^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\cdot a'^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\cdot\left(\frac{a'}{p}\right)(\text{mod } p)$$

Como o símbolo de Legendre assume somente os valores 1 ou –1, se fosse $\left(\frac{a'a}{p}\right)\neq\left(\frac{a}{p}\right)\cdot\left(\frac{a'}{p}\right)$, teríamos $1\equiv -1(\text{mod } p)$ ou $2\equiv 0(\text{mod } p)$, de modo que $p\,|\,2$, o que é impossível, visto que $p>2$. Portanto:

$$\left(\frac{a'a}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{a'}{p}\right), \text{ cqd.}$$

***

$$(III)\left(\frac{c^2}{p}\right)=1. \text{ Em particular, } \left(\frac{1}{p}\right)=1$$

Demonstração:

$$\left(\frac{c^2}{p}\right)=\left(\frac{c}{p}\right)\cdot\left(\frac{c}{p}\right) \qquad \left(\frac{c}{p}\right)=1, \text{ ou } \left(\frac{c}{p}\right)=-1$$

Se $\left(\frac{c}{p}\right)=1$, temos $\left(\frac{c^2}{p}\right)=\left(\frac{c}{p}\right)\cdot\left(\frac{c}{p}\right)=1.1=1$

Se $\left(\frac{c}{p}\right) = -1$, temos $\left(\frac{c^2}{p}\right) = \left(\frac{c}{p}\right) \cdot \left(\frac{c}{p}\right) = (-1).(-1) = 1$

Logo $\left(\frac{c^2}{p}\right) = 1$, cqd.

A hipótese de Riemann

Definição: A função-zeta de Riemann é:

$$\varsigma(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

sendo s uma variável complexa e a parte real de s maior que 1.

Note que se $R(s) \leq 1$, $\varsigma(s)$ não é convergente.

Sondow obteve uma representação de uma série de potências, usando transformações de séries de Euler.

Essa representação ficou:

$$\varsigma(s) = \frac{1}{1-2^{1-s}} \cdot \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} (-1)^k \binom{1}{k} (k+1)^{-s}$$

Essa forma da função-zeta tem zeros, conhecidos como zeros triviais. Existem, entretanto outros zeros. Daí a **Hipótese de Riemann 1**:

Os zeros não triviais de $\varsigma(s)$ tem parte real igual a $\frac{1}{2}$.

Euler mostrou que a função-zeta pode ser expressa também como o produto sobre o conjunto dos primos.

$$\varsigma(s) = \prod_{p} \frac{1}{(1-p^{-s})}$$

Definição: A integral logarítmica $li(x)$ é definida como:

$$li(x) = \int_2^x \frac{dt}{\log t}$$

Assim:

$$li(x) = \int_2^x \frac{dt}{\log t} = \int_2^x \frac{dt}{\frac{\ln t}{\ln 10}} = \ln 10 \cdot \int_2^x \frac{dt}{\ln t} = \ln 10 \cdot li(\ln x) = \ln 10 \cdot Li(x)$$

Daí

$$li(x) = \ln 10 \cdot Li(x) = \ln 10 \cdot \int_2^x \frac{dt}{\ln t} = \ln 10 \cdot (li(x) - li(2)) \cong \ln 10 \cdot (li(x) - 1{,}04516)$$

Pois Nielsen e Ramanujan descobriram, de forma independente e simultânea, que:

$$li(x) = \gamma + \ln \ln x + \sum_{k=1}^{\infty} \frac{(\ln x)^k}{k! \cdot k}$$

onde γ é a constante de Euler-Mascheroni. $\gamma = 0{,}5772156649$.

Lembrando que $\pi(x)$ é o número de primos menores que x, temos a **Hipótese de Riemann 2**:

$$\pi(x) = li(x) + O(x^{\frac{1}{2}+\varepsilon}),$$

onde $O(n)$ (conhecida como O-Grande) é a notação mais usada para estimar a taxa de crescimento da função.

Definição: $f(n) = O(g(n))$, se existem números positivos c e N tais que $f(n) \leq cg(n)$, $\forall n \geq N$.

Essa definição é lida assim: f é O-Grande de g se há um número positivo c, tal que f não seja maior do que cg para n's suficientemente grandes, isto é, para todos n's maiores que algum número N. A relação entre f e g pode ser expressa, estabelecendo tanto que $g(n)$ é um limite superior no valor de $f(n)$ ou que f cresce no máximo tão rápido quanto g.

Essa definição estabelece somente que precisam existir certos c e N, mas não dá qualquer sugestão de como calcular essas constantes. E, ainda, ela não coloca quaisquer restrições sobre esses valores e dá pouca orientação em situações, quando existem muitos candidatos. De fato, geralmente existem muitos pares de c's e N's que podem ser dados para um mesmo par de funções f e g.

Na *Hipótese de Riemann Extendida 2* temos, então, a relação:

$$\pi(x) - li(x) = O(x^{\frac{1}{2}+\varepsilon})$$

Finalmente, podemos estabelecer mais duas hipóteses eqüidistantes, também sobre números primos.

Precisamos de duas novas funções: as funções ψ e ϑ, funções de Chebyshev.

Definição:

$$\psi(x) = \sum_{p^k \le x} \log p = \log(mmc(1,2,3\ldots,[x\,]))$$

sobre todos os primos p e todos inteiros não-negativos k.

Agora, temos **Hipótese de Riemann 3**:

$$\forall \varepsilon > 0 \qquad \psi(x) = x + O(x^{\frac{1}{2}+\varepsilon})$$

ou

$$\psi(x) - x = O(x^{\frac{1}{2}+\varepsilon})$$

Definição:

$$\vartheta(x) = \sum_{p \le x} \log p$$

e dado o enunciado da **Hipótese de Riemann 4**:

$$\forall \varepsilon > 0 \qquad \vartheta(x) = x + O(x^{\frac{1}{2}+\varepsilon})$$

ou

$$\vartheta(x) - x = O(x^{\frac{1}{2}+\varepsilon})$$

A (HRE) hipótese de Riemann extendida

Vamos, primeiro, definir a função L_p, de uma variável complexa s:

$L_p(s) = \sum_{n=1}^{\infty} \left(\frac{n}{p}\right) \frac{1}{n^s}$, onde $\left(\frac{n}{p}\right)$ é o Símbolo de Legendre, já visto, que foi definido como:

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ se } p|n, \\ 1 \text{ se } n \text{ é resto quadrático mod } p \text{ e } p \text{ não divide } n \\ -1 \text{ se } n \text{ é não resto quadrático mod } p \text{ e } p \text{ não divide } n \end{cases}$$

A HRE é então:

Hipótese de Riemann Extendida 1:

Todos os zeros de $L_p(s)$ com parte real estritamente entre zero e 1 têm a parte real igual a $\frac{1}{2}$.

Hipótese de Riemann Extendida 2:
Para n e a inteiros, primos entre si e $\varepsilon > 0$

$$\pi(x,n,a) = \frac{li(x)}{\phi(n)} + O(x^{\frac{1}{2}+\varepsilon})$$

$\pi(x,n,a)$ é aqui o número de primos menores ou iguais a x e congruentes a a mod n.
$\phi(n)$ é a equação de Euler.

Definição: Chama-se função de Euler a função aritmética ϕ, assim definida para todo inteiro positivo n:
$\phi(n)$ = números de inteiros positivos $\leq n$ e que são primos com n.

Em outros termos, $\phi(n)$ = número de inteiros da seqüência finita:

$$1, 2, 3, \ldots, n-1, n$$

que são primos com n.

Portanto, $\phi(n)$ = número de elementos do conjunto:

$$\{x \in N \mid 1 \leq x \leq n \text{ e } mdc(x,n) = 1\}$$

Em particular, $\phi(1) = 1$, porque o único inteiro positivo ≤ 1 é o próprio 1 e o $mdc(1,1) = 1$.

Para todo inteiro $n \geq 2$, $mdc(n,n) = n \neq 1$, de modo que $\phi(n)$ = número de inteiros positivos $< n$ e que são primos com n. Logo, $\phi(n) < n$ para todo inteiro $n \geq 2$.

Hipótese de Riemann Extendida 3:
Definimos a L-função de Dirichlet como sendo:

$$L(s,x) = \sum_{n \geq 1} \frac{x(n)}{n^s}$$

onde a parte real de $s > 1$.

A função $L(s,x)$ tem muitos zeros em $0 < R(s) < 1$.

Então a Hipótese Extendida de Riemann é que todos os zeros naquele intervalo têm a parte real $\frac{1}{2}$.

Essas são as Hipóteses Extendidas de Riemann.

Em 1977, Solovay e Strassem publicaram o algoritmo Monte-Carlo que foi o primeiro algoritmo aleatório para testes de primalidade. Esse algoritmo pode ser não-aleatório com o uso das Hipóteses de Riemann Extendidas.

Solovay-Strassen

O algoritmo é da forma:
Tome um inteiro ímpar $n \geq 3$;
Escolher aleatoriamente a da seqüência $(1,2,3,\ldots, n-1)$;
Se $mdc(a,n) = 1$

Se $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} (\text{mod } n)$;

Então n primo
Se não
n composto

Sugerimos que se faça o teste com: 1º) $n = 15$ e $a = 4$ e 2º) $n = 11$ e $a = 5$, mesmo já sabendo que 15 é composto e 11 é primo.

Teorema: Se n é primo, o teste de Solovay-Strassen nos dá um primo. Se n é composto, nos dá um composto para no mínimo $1/2$ dos a's em $(1,2,3,\ldots, n-1)$. O algoritmo trabalha em tempo polinomial.

Assim, o algoritmo Solovay-Strassen atualmente apresenta um certificado para encontrar números compostos, melhor que de primalidade.

A meta final desta linha de pesquisa é, certamente, obter um algoritmo polinomial determinístico e incondicional para teste de primalidade. Foi alcançado isto, quando foi dado um $\tilde{O}((\log n)^{12})$ tempo algoritmo para testar se um número é primo. Heuristicamente, o algoritmo é muito melhor: sob uma ampla conjetura, acredita na densidade dos primos de Sophie Germain (primos tais que $2p+1$ também é primo), o algoritmo utiliza apenas $\tilde{O}((\log n)^6)$ passos. A exatidão da prova do algoritmo requer somente recursos simples da álgebra, exceto em relação à Teoria do Crivo na densidade dos primos p com $p-1$, tendo um fator primo enorme.

Primos de Sophie Germain

Um primo p é dito primo de Sophie Germain se tanto p quanto $2p+1$ são primos. Os primeiros primos de Sophie Germain são 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131,... Os números primos de Sophie Germain menores que 10^n para n =1, 2, ... são 3, 10, 37, 190, 1171, 7746, 56032, ...

O maior primo de Sophie Germain conhecido é $2540041185 \cdot 2^{11479} - 1$, que tem 34547 dígitos. Não se sabe se existe um número infinito de primos de Sophie Germain.

Os primos p de Sophie Germain na forma $p = 4k - 1$ (que fazem $2p + 1$ um primo) correspondem às relações de *números de Mersenne* compostos M_p.

Um número de Mersenne é um número da forma

$$M_n \equiv 2^n - 1,$$

onde n é um inteiro. Os primeiros números de Mersenne são 1, 3, 7, 15, 31, 63, 127, 255, ...

PRIMOS DE SOPHIE GERMAIN

P	$q = 2p + 1$	p	$q = 2p + 1$
2	5	191	383
3	7	19391	38783
5	11	38183	76367
11	23	1508051	3016103
23	47	...	...
29	59	190909091	381818183
41	83	352909253	705818507
53	107	...	...
83	167	38371917383	76743834767
89	179	...	...
113	227	3947847493	78949694987
131	263	39493939493	78987878987
...	...	...	...

Esses foram alguns algoritmos desenvolvidos para descobrirmos se um número qualquer **p** é primo ou composto. Com essas premissas vamos ver as ferramentas para a demonstração do algoritmo AKS. Qual a idéia básica?

2. Idéia básica e desenvolvimento

Os testes do algoritmo são baseados na seguinte identidade para números primos:

Identidade: Suponha que a e p são primos entre si. Então, p é primo se e somente se

$$(x-a)^p \equiv (x^p - a)(\text{mod } p)$$

Prova:

$$(x-a)^p = \sum_{i=0}^{p} (-1)^i \binom{p}{i} x^{p-i} a^i$$

Condição necessária:
Provemos que, se p é primo, $(x-a)^p \equiv (x^p - a)(\text{mod } p)$.

Antes de qualquer coisa, provemos que $\binom{p}{i}$ é inteiro:

Seja n tal que $n = a + b$;
Então $b = n - a$.

$\binom{n}{a} = \frac{n!}{a!(n-a)!}$ ou $\binom{n}{a} = \frac{(a+b)!}{a!b!}$.

Se $\binom{n}{a}$ for inteiro, $a!b!/(a+b)!$. Por indução finita...

* Para $n = 2$, $a = 1$ e $b = 1$.

$a!b!/(a+b)!$

$1!\cdot 1!/(1+1)!$

$1/2$ (ok)

• Façamos $a + b = n + 1$. A hipótese da indução fica, então:

$(a-1) + b = n \therefore (a-1)!b!/(a+b-1)!$

ou $a + (b-1) = n \therefore a!(b-1)!/(a+b-1)!$

Da hipótese

$(a-1)!b!/(a+b-1)!$, vem

$a \cdot (a-1)!b!/\ a \cdot (a+b-1)!$

$a!b!/\ a(a+b-1)!$

Analogamente, da hipótese,

$a!(b-1)!/(a+b-1)!$, ou

$a!b(b-1)!/\ b(a+b-1)!$
E $a!b!/\ b(a+b-1)!$

Logo,
$a!b!/\ a(a+b-1)!+b(a+b-1)!$
$a!b!/(a+b-1)!(a+b)$
$a!b!/(a+b)!$, cqd.

Provemos também que $\binom{p}{i}$ é múltiplo de p:

De fato, $\binom{p}{i}=\frac{p!}{i!(p-i)!}=\frac{p(p-1)!}{i!(p-i)!}=p\cdot\frac{(p-1)!}{i!(p-i)!}$, e, portanto, é múltiplo de p.

$$(x-a)^p \equiv \sum_{i=0}^{p}(-1)^i\binom{p}{i}x^{p-i}a^i \pmod p$$

$$(x-a)^p \equiv x^p+\sum_{i=1}^{p-1}(-1)^i\binom{p}{i}x^{p-i}a^i-a^p \pmod p$$

Como $\binom{p}{i}$ é inteiro e múltiplo de p, então $\binom{p}{i}=0(\text{mod } p)$ e
$(x-a)^p \equiv x^p-a^p(\text{mod } p)$
Mas, $(a,p)=1$ e $a^p \equiv a(\text{mod } p)$, logo
$(x-a)^p \equiv (x^p-a)(\text{mod } p)$, cqd.

Condição suficiente:
Provemos que se $(x-a)^p \equiv (x^p-a)(\text{mod } p)$, então p é primo:

Suponha p composto. Seja q um primo, tal que $p=q^kN$ e, portanto $q^k/\ p$. Então q^k não divide $\binom{p}{q}$ e $(q^k,a^{p-q})=1$.

De fato,

$$\binom{p}{q}=\frac{p!}{q!(p-q)!}=\frac{(q^kN)!}{q!(p-q)!}=\frac{q^kN\cdot(q^kN-1)\cdot\ldots\cdot(p-q+1)}{q\cdot(q-1)\cdot\ldots\cdot3\cdot2\cdot1}$$

$$= \frac{q^k}{q} \cdot \frac{N \cdot (q^k N - 1) \cdot \ldots \cdot (p - q + 1)}{(q-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1} = q^{k-1} \frac{N \cdot (q^k N - 1) \cdot \ldots \cdot (p - q + 1)}{(q-1) \cdot \ldots \cdot 3 \cdot 2 \cdot 1}.$$

E daí, $q^{k-1} / \binom{p}{q}$ e q^k não divide $\binom{p}{q}$.

O coeficiente de x^p é $\binom{p}{q} a^{p-q} \not\equiv 0 (\text{mod } p)$ e, portanto, $(x-a)^p \not\equiv (x^p - a)(\text{mod } p)$, mas $(x-a)^p \equiv (x^p - a)(\text{mod } p)$ — ABSURDO. Logo, p é primo, cqd.

Assim, dado um p como entrada, podemos tomar um polinômio $P(x) = x - a$ e verificar se a congruência acima demonstrada é satisfeita ou não. Isso requer tempo, pois precisamos avaliar p coeficientes, na pior hipótese. Então, para que isso se torne possível, avaliaram-se ambos os lados da congruência módulo um polinômio da forma $x^r - 1$. Uma das iterações do algoritmo consiste em verificar as congruências:

$$(x-a)^p \equiv (x^p - a)(\text{mod } x^r - 1, p)$$

O algoritmo primeiro escolhe um r adequado. Este r é adequado, se é um primo $= O(\log^6 p)$ e se $r-1$ contém um fator primo de tamanho pelo menos $r^{\frac{1}{2}+\delta}$ para alguma constante $\delta > 0$. Portanto, o algoritmo verifica a congruência para um pequeno número de $a's$.

Seja, por exemplo, $p = 7$, $a = 2$ e $r = 3$:

Os polinômios da forma $x^p - a$ e $x^r - 1$ ficariam $x^7 - 2$ e $x^3 - 1$, respectivamente.

Precisamos demonstrar que $(x-2)^7 \equiv x^7 - 2(\text{mod } 7)$.

Para tal vamos recorrer ao módulo polinômio $x^3 - 1$.

Temos que:

$(x-2)^7 = x^7 - 14x^6 + 84x^5 - 280x^4 + 560x^3 - 672x^2 + 448x - 128$

Ao dividirmos $(x-2)^7$ por $x^3 - 1$, temos por resto da divisão o polinômio $-588x^2 + 169x + 418$.

Daí, como já sabemos, $(x-2)^7 \equiv (-588x^2 + 169x + 418)(\text{mod } x^3 - 1)$.

Agora, $x^7 - 2$, quando dividido por $x^3 - 1$ deixa resto $x - 2$ e, portanto, $x^7 - 2 \equiv x - 2 (\mathrm{mod}\, x^3 - 1)$.

No módulo 7 temos que $-588x^2 + 169x + 418 \equiv x + 5 (\mathrm{mod}\, 7)$, pois

$-588 \equiv 0 (\mathrm{mod}\, 7)$;

$169 \equiv 1 (\mathrm{mod}\, 7)$;

$418 \equiv 5 (\mathrm{mod}\, 7)$.

e então,

$-588x^2 \equiv 0 (\mathrm{mod}\, 7)$;

$169x \equiv x (\mathrm{mod}\, 7)$;

$418 \equiv 5 (\mathrm{mod}\, 7)$.

Portanto, $-588x^2 + 169x + 418 \equiv x + 5 (\mathrm{mod}\, 7)$.

Mas $x + 5 \equiv x - 2 (\mathrm{mod}\, 7)$.

Como $(x^7 - 2) \equiv (x - 2) (\mathrm{mod}\, x^3 - 1)$ e $(x - 2)^7 \equiv (-588x^2 + 169x + 418)$ $(\mathrm{mod}\, x^3 - 1)$, podemos trabalhar com $x^7 - 2 \equiv x + 5 \equiv (x - 2)^7 (\mathrm{mod}\, 7)$.

O que nos conduz à tese do exemplo.

Com esses artifícios chegamos, de maneira muito mais rápida, à conclusão de que $x^7 - 2 \equiv (x - 2)^7 (\mathrm{mod}\, 7)$

3. Notação e Preliminares

Lema 3.1. Seja p e r números primos, $p \neq r$.

1. O grupo multiplicativo de qualquer campo F_{p^t} para $t \geq o$, denotado por $F^*_{p^t}$, é cíclico.

Definição 1: Seja G um conjunto não-vazio e $(x, y) \to x * y$, uma lei de composição interna em G. G é grupo se e somente se obedece às seguintes propriedades:

a) Associativa: $a*(b*c) = (a*b)*c$, $\forall a, b, c \in G$;

b) Elemento Neutro: $\exists e \in G \mid a*e = e*a = a$, $\forall a \in G$;

c) Elemento Inverso: $\forall a \in G$, $\exists a' \in G \mid a*a' = a'*a = e$;

Se a lei de composição for uma "multiplicação", temos um *Grupo Multiplicativo.*

Para F_{p^t}:

a) Associativa: $p^t \cdot (p^u \cdot p^v) = (p^t \cdot p^u) \cdot p^v$, $\forall p^t, p^u, p^v \in F_{p^t}$;

b) Elemento Neutro: $\exists e \in G \mid p^t \cdot e = e \cdot p^t = p^t, \forall p^t \in F_{p^t}$, onde $e = p^0$;

c) Elemento Inverso: $\forall p^t \in F_{p^t}$, $\exists p^{t\prime} \in G \mid p^t \cdot p^{t\prime} = p^{t\prime} \cdot p^t = e$, onde $p^{t\prime} = p^{-t}$;

E, portanto, F_{p^t} é grupo multiplicativo.

Definição 2: Um grupo multiplicativo é cíclico se:

$$\exists a \in G \mid G = \{a^m / m \in Z\}$$

$G = [a]$ e a é gerador de G.

Obs.: O mesmo grupo multiplicativo pode conter mais que um gerador.

De fato, o gerador de $F^*_{p^t}$ será p, pois p^t com $t > 0$ gera $F^*_{p^t}$:

2. Seja f(x) um polinômio com coeficientes inteiros. Então $f(x)^p \equiv f(x^p) (\mathrm{mod}\, p)$.

$$f(x) = a_0 + a_1 x + \ldots + a_d x^d$$
$$f(x)^p = (a_0 + a_1 x + \ldots + a_d x^d)^p$$
$$f(x^p) = a_0 + a_1 x^p + \ldots + a_d (x^p)^d$$

O coeficiente de x^i em $f(x)^p$ é $\sum_{\substack{i_0+\ldots+i_d=p \\ i_1+2i_2+\ldots+di_d=i}} a_o^{i_0} \cdot \ldots \cdot a_d^{i_d} \frac{p!}{i_0! \ldots i_d!}$.

Essa soma é divisível por p, a menos que um dos i_j's seja p. Neste último caso o coeficiente de x_i será a_j^p e $a_j^p x_i \equiv a_j x_i (\mathrm{mod}\, p)$.

$$x^p \equiv x (\mathrm{mod}\, p)$$
$$(x^p)^2 \equiv x^2 (\mathrm{mod}\, p)$$
$$\vdots$$
$$(x^p)^d \equiv x^d (\mathrm{mod}\, p)$$

Assim,

$$f(x^p) \equiv a_0 + a_1 x^p + \ldots + a_d (x^p)^d (\mathrm{mod}\, p)$$
$$f(x^p) \equiv a_0 + a_1 x + \ldots + a_d x^d \equiv f(x) (\mathrm{mod}\, p)$$
$$f(x^p) \equiv (a_0 + a_1 x^p + \ldots + a_d (x^p)^d)^p (\mathrm{mod}\, p)$$

$$f(x^p) \equiv a_0 + a_1x + \ldots + a_dx^d \equiv f(x) \pmod{p}$$

Logo, $f(x^p) \equiv f(x)^p \pmod{p}$

Observe o exemplo:

Seja $f(x) \equiv a_0 + a_1x + a_2x^2$

$f(x^3) \equiv a_0 + a_1x^3 + a_2x^6$

$f(x)^3 \equiv (a_0 + a_1x + a_2x^2)^3 =$

$= (a_0 + a_1x)^3 + 3(a_0 + a_1x)^2 a_2x^2 + 3(a_0 + a_1x)a_2^2x^4 + a_2^3x^6 =$

$= a_0^3 + 3a_0^2a_1x + 3a_0a_1^2x^2 + a_1^3x^3 + 3(a_0^2 + 2a_0a_1x + a_1^2x^2)a_2x^2 +$

$+3a_0a_2^2x^4 + 3a_1a_2^2x^5 + a_2^3x^6 =$

$= a_0^3 + 3a_0^2a_1x + 3a_0a_1^2x^2 + a_1^3x^3 + 3a_0^2a_2x^2 + 6a_0a_1a_2x^3 + 3a_1^2a_2x^4 +$

$+3a_0a_2^2x^4 + 3a_1a_2^2x^5 + a_2^3x^6 =$

$= a_0^3 + 3a_0^2a_1x + 3a_0(a_1^2 + a_0a_2)x^2 + (a_1^3 + 6a_0a_1a_2)x^3 +$

$+3(a_1^2a_2 + a_0a_2^2)x^4 + 3a_1a_2^2x^5 + a_2^3x^6 =$

Mas,

$a_0^3 \equiv a_0 \pmod{3}$

$3a_0^2a_1x \equiv 0 \pmod{3}$

$3a_0(a_1^2 + a_0a_2) \equiv 0 \pmod{3}$

$(a_1^3 + 6a_0a_1a_2) \equiv a_1 + 0 \pmod{3}$

$3(a_1^2a_2 + a_0a_2^2) \equiv 0 \pmod{3}$

$3a_1a_2^2 \equiv 0 \pmod{3}$

$a_2^3 \equiv a_2 \pmod{3}$

Logo, $f(x)^3 \equiv a_0 + a_1x^3 + a_2x^6 \therefore f(x)^3 \equiv f(x^3) \pmod{3}$

3. Seja $h(x)$ um fator de $x^r - 1$. Seja $m \equiv m_r \pmod{r}$. Então $x^m \equiv x^{m_r} \pmod{h(x)}$. $m \equiv m_r \pmod{r} \therefore m = kr + m_r$

$$x^r \equiv 1 \pmod{x^r - 1}$$

$$x^{kr} \equiv 1 \pmod{x^r - 1}$$

$$x^{kr+m_r} \equiv x^{m_r} \pmod{x^r - 1}$$

$$x^m \equiv x^{m_r} (\text{mod}\, x^r - 1)$$

Mas, $h(x) / x^r - 1$ e $x^r - 1 / x^m - x^{m_r}$

$$\therefore x^m \equiv x^{m_r} (\text{mod}\, h(x))$$

4. Seja $o_r(p)$ a ordem de p no módulo r. Então, temos em $F_p, \dfrac{x^r - 1}{x - 1}$ que é um polinômio que pode ser escrito como produto de polinômios irredutíveis que tem grau igual a $o_r(p)$.

Vamos admitir que $O_r(p) = d$. Suponha ainda que $O_r(x) = \dfrac{x^r - 1}{x - 1}$ é um polinômio que tem um fator irredutível $h(x)$ em F_p sendo que o grau de $h(x) = k$.

Para provar a tese 4 do lema, basta provar que $O_r(p) =$ grau de $h(x)$, ou seja $d = k$.

Pelo fato 2 do lema, temos que

$g(x)^p = g(x^p)$, onde $g(x)$ é um gerador do grupo cíclico F_p

ou ainda $g(x)^{pd} = (g(x^p))^d$ e pelo fato 3 do lema temos

$g(x)^{pd} = g(x)$ e, finalmente,

$g(x)^{pd-1} = 1$.

Já que $(p^k - 1)$ é a ordem de $g(x)$, temos que $(p^k - 1) | (p^d - 1)$ e isto implica que $k | d$, pois na divisão de $(p^d - 1)$ por $(p^k - 1)$ obtemos por resto $p^{d-nk} - 1$ com n natural e daí $d - nk = 0$ e $k | d$.

Também temos que $r | (p^k - 1)$, isto é, $p^k \equiv 1 (\text{mod}\, r)$. Concluímos, então, que $d | k$.

Se $k | d$ e $d | k$, então $d = k$, conforme queríamos demonstrar.

Lema 3.2. Seja $P(n)$ o maior divisor primo de n. Então, existem constantes $c > 0$ e n' tais que, para todo $x \geq n'$

$$|\{p \mid p \text{ é primo, } p \leq x \text{ e } P(p-1) > x^{2/3}\}| \geq c \frac{x}{\log x}.$$

Exemplo:

$n = 12, \quad P(12) = 3$

$p = 17, \quad P(16) = 2$

$p = 23, \quad P(22) = 11$

Lema 3.3. Seja $\pi(n)$ o número de primos $\leq n$. Então, para $n \geq 1$:

$$\frac{n}{6\log n} \leq \pi(n) \leq \frac{8n}{\log n}.$$

Para $n = 10, \quad \pi(n) = 4$

Daí teremos: $$\frac{10}{6\log 10} = \frac{5}{3} \leq 4 \leq \frac{80}{\log 10} = 80.$$

4. O Algoritmo

1. se (n é da forma a^b, $b > 1$) saída COMPOSTO;
2. $r = 2$;
3. enquanto $(r < n)$ {
4. se (mdc $(n, r) \neq 1$) saída COMPOSTO;
5. se (r é primo)
6. torne q o maior fator primo de $r - 1$;
7. se $(q \geq 4\sqrt{r}.\log n)$ e $(n^{\frac{r-1}{q}} \not\equiv 1 (\mathrm{mod}\, r))$
8. interrompe;
9. $r \leftarrow r + 1$ (acumula $r + 1$ em r)
10. }
11. para $a = 1$ até $2\sqrt{r}\log n$
12. se $((x - a)^n \not\equiv (x^n - a)(\mathrm{mod}\, x^n - 1, n))$ saída COMPOSTO;
13. saída PRIMO.

O algoritmo responde primo se e somente se *n* é primo.

Para a demonstração dessa frase alguns lemas foram demonstrados:

LEMA 1 — Existem as constantes positivas c_1 e c_2 para as quais existe um primo r no intervalo $[c_1(\log n)^6, c_2(\log n)^6]$ tal que $r - 1$ tem um fator primo $q \geq 4\sqrt{r}\log n$ e $q \mid o_r(n)$.

LEMA 2 — Se n é primo, o algoritmo responde **primo**.

LEMA 3 — No campo $F_p[x]/(h(x))$ o grupo gerado pelos l binomiais $(x-a)$, $1 \le a \le l$

$$G = \{\prod_{1 \le a \le l} (x-a)^{\alpha a} \mid \alpha a \ge 0, \forall 1 \le a \le l\}$$

é cíclico e de tamanho $> \left(\frac{d}{l}\right)^l > (d/l)^l$.

LEMA 4 — O conjunto $I_{g(x)}$ é fechado em relação à multiplicação.

LEMA 5 — Seja a ordem de $g(x)$ em $F_p[x]/(h(x))$, O_g. Seja m_1, $m_2 \in I_{g(x)}$. Então, $m_1 \equiv m_2 (\mathrm{mod}\, r)$ implica que $m_1 \equiv m_2 (\mathrm{mod}\, o_g)$.

LEMA 6 — Se n é composto, o algoritmo responde **composto**.

O nosso objetivo, neste artigo, ficou restrito a fornecer subsídios matemáticos para que o leitor possa entender a idéia desenvolvida nos treze passos do algoritmo AKS. Esperamos ter alcançado esse objetivo.

REFERÊNCIAS

AGRAWAL, M.; KAYAL, N.; SAXENA, N. *Primes is in P.* Departament of Computer Science & Engineering. Indian Institute of Technology Kanpur. Kanpur-208016, India. 6 ago 2002. Disponível em <http://www.cse.iitk.ac.in/primality.pdf>.

ALENCAR FILHO, E. de. *Teoria das congruências.* São Paulo: Nobel, 1986.

BOREVICH, Z. I.; SHAFAREVICH, I. R. *Number theory.* New York: Academic Press, 1964.

BRAGA, B. da R. *Algoritmo AKS. Primalidade de um número em tempo polinomial* Disponível em <http://www.lockabit.coppe.ufrj.br/downloads/academicos/aks.pdf>. Acesso em 11 set. 2002.

DOMINGUES, H. H.; IEZZI, G. *Álgebra moderna.* 3. ed. São Paulo: Atual, 1995.

DROZDEK, A. *Estrutura de dados e algoritmos em C++.* São Paulo: Pioneira Thomson Learning, 2002.

LOGARITHMIC Integral. Disponível em <http://mathworld.wolfram.com/LogarithmicIntegral.html>.

LE VEQUE, W. J. *Teoría elemental de los números*. México: Herrero Hermanos, 1968.

MODULAR Arithmetic from Fermat and Euler to Carmichael and beyond... Disponível em <http://home.att.net/~numericana/answer/modular.htm#lambda>

ORE, O. *Number theory and its history*. New York: Dover, 1976.

QUADRATIC Residue. Disponível em <http://mathworld.wolfram.com/QuadraticResidue.html>

SIERPINSKI, W. *Elementary theory of numbers*. Warszawa: Panstwowe, 1964.

SOPHIE Germain Prime. Disponível em <http://mathworld.wolfram.com/SophieGermainPrime.html>.

USPENSKY, J. V.; HEASLET, M. A. *Elementary number theory*. New York and London: Mc Graw Hill, 1939.

VINOGRÁDOV, I. *Fundamentos de la teoría de los números*. Moscou: Mir, 1971.

WOJCIECHOWSKI, J. *The Extended Riemann Hypotesis and its application to computation*. Disponível em http://wonka.hampshire.edu/~jason/math/comp2/final_paper.pdf. Acesso em22 jan 2003.

Endereço dos autores:

Rodovia Raposo Tavares, km 92,5
CEP 18023-000
Sorocaba, SP