Goiânia, 07 a 10 de outubro

Mini Curso

Números Primos: Testes de Primalidade e Aplicações

Maria Aparecida de Faria - Esp. em Mat. do Ens. Básico, IME/UFG

Profa. Dra. Shirlei Serconek - IME/UFG

NÚMEROS PRIMOS:TESTES DE PRIMALIDADE E APLICAÇÕES

FARIA,M.A., SERCONEK,S.

1. Introdução

Durante muitas gerações, tentou-se sem muito êxito, aperfeiçoar o entendimento de Euclides sobre os números primos. G.H. Hardy (1877- 1947), matemático inglês, gostava de dizer que: *" Qualquer tolo pode fazer perguntas sobre os números primos que o mais sábio dos homens não consegue responder."* A corrida em busca de fórmulas geradoras de pelo menos uma lista de números primos envolveu mentes muito brilhantes, grandes matemáticos, que não obtiveram sucesso em suas pesquisas. Ainda hoje, muitos matemáticos buscam entender os mistérios que envolvem os números primos com uma vantagem: contam com auxílio de computadores super modernos nessa difícil missão. Atualmente os números primos deixaram de ser um assunto relevante apenas em Teoria dos Números, devido ao desenvolvimento Criptografia de Chave Pública. Neste artigo, pretendemos mostrar, além de fatos importantes sobre números primos como *O Pequeno Teorema de Fermat* e o *Teorema de Euler*, a Matemática que se utiliza no Criptosistema RSA.

2. Conceitos Básicos

Nesta seção, apresentaremos os conceitos necessários ao entendimento deste trabalho.

2.1. Divisibilidade.

Definição 2.1. *Dados a e $b \in Z$, com $a \neq 0$, dizemos que a divide b, quando existir $c \in Z$ tal que $b = ac$.*

Notação 2.1. *Se a divide b escrevemos $a \mid b$. Se a não divide b escrevemos $a \nmid b$.*

Exemplo 2.2. *Temos que* $2 \mid 4$ *pois* $4 = 2.2$ *e*
$3 \mid 12$ *pois* $12 = 3.4$.

Proposição 2.3. *Se a,b e $c \in Z$ com $a \neq 0$ e x e $y \in Z$ são tais que $a \mid b$ e $a \mid c$ então $a \mid (xb \pm yc)$.*

Demonstração. Se $a \mid b$ e $a \mid c$ então existem f,g $\in Z$ tais que $b = af$ e $c = ag$,logo temos que $xb = xaf$ e $yc = yag$, consequentemente $xb \pm yc = a(xf \pm yg)$ com $xf \pm yg \in Z$. Portanto, $a \mid (xb \pm yc)$. □

Proposição 2.4. *(**Divisão Euclidiana**) Sejam a e b números inteiros com a>0. Existem dois únicos números inteiros q e r tais que b=aq+r, com 0≤r<a.*

Demonstração. Suponha que b>a e considere os números b, b-a, b-2a,..., b-na,... Pelo Axioma da Boa Ordem, o conjunto S formado pelos elementos acima tem um menor elemeto $r = b - aq$. Vamos provar que r<a. Se a|b, então r=0 e nada mais temos a provar. Se a não divide b , então $r \neq a$, 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 $r = c + a = b - aq$, teríamos $c = b - (q + 1)a \in$S, com c<r, contradição com o fato de r ser o menor elemento de S.

Unicidade: 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 $r = b - aq$ e $r' = b - aq'$ com r<r'<a teríamos r'-r ≥a ⇒ r'≥ r+a ≥a. □

2.2. **Máximo Divisor Comum.**

Definição 2.5. *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 $d \mid a$ e $d \mid b$.*

Definição 2.6. *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 $d_1 \mid d$.

Notação 2.2. *Se d é o máximo divisor comum de a e b escrevemos $d = (a, b)$.*

Exemplo 2.7. *Temos que* $4 = (4, 8)$.

2.3. **Mínimo Múltiplo Comum.**

Definição 2.8. *Um número c é um múltiplo comum de dois inteiros a e b se $a \mid c$ e $b \mid c$.*

Definição 2.9. *Sejam a e b dois inteiros tais que a≠0 ou b≠0. Dizemos que m>0 é um 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 $m \mid c$.

Notação 2.3. *Se m é o mínimo múltiplo comum de a e b escrevemos $m = [a, b]$.*

Exemplo 2.10. *Temos que* $6 = [2, 3]$.

2.4. **Congruências.**

Definição 2.11. *Seja m um número inteiro positivo. Dizemos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais.*

Notação 2.4. *Se a é congruente a b módulo m escrevemos* $a \equiv b \ mod \ m$.

Proposição 2.12. *Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo. Diz-se que a é congruente a b módulo m se e somente se* $m \mid a - b$.

Demonstração. Se $a \equiv b \ mod \ m$ então $m \mid a - b$. Por hipótese, $a = mq+r$ e $b = mq_1+r$ onde q e $q_1 \in Z$. Logo $a-b = mq-mq_1 = m(q-q_1)$ onde $q - q_1 \in Z$, portanto, $m \mid a - b$. Se $m \mid a - b$ então $a \equiv b \ mod \ m$. Por hipótese, $m \mid a - b$, isto é, $a - b = mx$ onde $x \in Z$. Desta forma $a = mx + b$. Seja r o resto da divisão de b por m, logo temos que $b = mx_1 + r$ onde $x_1 \in Z$. Substituindo o valor de b na equação $a = mx + b$ temos: $a = mx + mx_1 + r$, logo $a = mx_2 + r$ onde $x_2 \in Z$, e concluimos que a deixa o mesmo resto r quando dividido por m. Portanto, $a \equiv b \ mod \ m$. □

Exemplo 2.13. *Temos que* $21 \equiv 13 \ mod \ 2$ *, pois 21 e 13 deixam o mesmo resto quando divididos por 2.*

3. **Números Primos**

Definição 3.1. *Um número inteiro p>1 é um número primo se ele for divisível somente por 1 e por si mesmo.*

Definição 3.2. *Um número inteiro positivo maior que 1 é um número composto se ele não é um número primo.*

3.1. **Fatoração Prima.**

Teorema 3.3. *Todo inteiro positivo é igual a 1, é um número primo, ou pode ser escrito como um produto de números primos.*

Demonstração. Provaremos o teorema usando o segundo princípio de indução. Para n=1 o teorema é válido.

Vamos supor que ele é válido para todo inteiro positivo n<k. Se k é primo então o teorema é válido para k.

Se k não é primo, então k é divisível por algum inteiro p e k=pq onde nem p, nem q é k ou 1. Como p|k e q|k temos que p e q são menores que k. Logo, pela hipótese de indução p e q podem ser escritos como um produto de números primos. Consequentemente, k=pq pode ser escrito como um produto de números primos. □

Exemplo 3.4. *Temos que 37 é primo e 15=3.5 é um produto de números primos.*

Teorema 3.5. *Se p é um número primo e p|ab, onde a e b são inteiros positivos, então p|a ou p|b.*

Demonstração. Se p|a então a conclusão é válida. Por outro lado, se p não divide a então $(a, p) = 1$. Logo, existem x e y, inteiros positivos tais que $ax + py = 1$. Multiplicando a igualdade anterior por b temos: $abx + pby = b$. Por hipótese p|ab, logo $ab = pk$, para algum k inteiro positivo. Desta forma, $pkx + pby = b \Rightarrow$ p(kx+by)=b. Portanto, p|b. □

Lema 3.6. *Se um número primo p divide um produto de inteiros positivos $q_1q_2...q_n$, então p|q_i, para algum i, 1≤i≤n.*

Demonstração. Vamos mostrar o Lema usando indução sobre n, o número de fatores do produto $q_1q_2...q_n$.

Se $n = 1$, o Lema é válido. Suponhamos que o Lema seja verdadeiro para $n = k$, isto é, se p divide algum produto de k inteiros, então p divide um dos k fatores.

Suponhamos que p divide a produto de k+1 inteiros, isto é, p|$q_1q_2...q_kq_{k+1}$, logo p| $(q_1q_2...q_k)q_{k+1}$. Se p|q_{k+1} então o Lema está demonstrado.

Se p não divide q_{k+1} então p|$q_1q_2...q_k$. Mas $q_1q_2...q_k$ é o produto de k inteiros , pela hipótese de indução p|q_i, para algum i, 1≤i≤n. □

Lema 3.7. *Se um número primo p divide o produto de primos $q_1q_2...q_n$, então p=q_i para algum i, 1≤i≤n.*

Demonstração. Temos que p|q_i para algum i,onde 1≤i≤n. Consequentemente p e q_i são ambos primos, logo p=q_i para algum i,1≤i≤n. □

Teorema 3.8. *(**Teorema Fundamental da Aritmética**) Qualquer inteiro positivo 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. Uma vez que m pode ser escrito como um produto de números primos, vamos assumir que $q_1q_2...q_n$ e $p_1p_2...p_s$ são duas maneiras de escrever m como o produto de números primos.

Faremos a demonstração do teorema usando indução sobre n, o número de fatores primos de $q_1q_2...q_n$.

Se $n = 1$ o teorema é verdadeiro. Suponhamos que o teorema seja válido para $q_1q_2...q_k = p_1p_2...p_s$,isto é, se m= $q_1q_2...q_k = p_1p_2...p_s$ então $k = s$ e o produto é único.

Suponha que m=$q_1q_2...q_{k+1}$=$p_1p_2...p_{s'}$.

Temos que q_{k+1} divide $p_1p_2...p_{s'}$ então $q_{k+1} = p_i$ para algum 1≤i≤s'. Dividindo m=$q_1q_2...q_{k+1} = p_1p_2...p_{s'}$ por q_{k+1} temos
$q_1q_2...q_k = p_1p_2...p_{i-1}p_{i+1}...p_{s'}$. Mas $k = s' - 1$ e o produto é único pela hipótese de indução. Consequentemente $k + 1 = s'$. Portanto, a fatoração de m é única. □

Teorema 3.9. *Existem infinitos números primos.*

Demonstração. Suponha que existe somente um número finito de números primos, isto é, p_1,p_2,...,p_k. Considere o inteiro $(p_1p_2...p_k) + 1$. Seja p_r um número primo e suponha que $p_r|((p_1p_2...p_k) + 1)$. Mas $p_r|p_1p_2...p_k$, logo $p_r|1$. (Contradição). Portanto, existem infinitos números primos. □

Teorema 3.10. *(**Pequeno Teorema de Fermat**) Se p é um número primo e se a é um número inteiro qualquer, então* $a^p \equiv a \bmod p$.

Demonstração. Faremos a demonstração por indução sobre a, quando a for positivo. Claramente o resultado vale para $a = 1$, pois $p \mid 0$. Suponhamos que o resultado seja válido para a, provaremos a validade para $a + 1$. Temos, pela fórmula do binômio de Newton, $(a + 1)^p - (a + 1) = a^p - a + \binom{p}{1}a^{p-1} + .. + \binom{p}{p-1}a$. Como $a^p - a$ é divisível por p, pela hipótese de indução, e os números $\binom{p}{i}$, onde $0 < i < p$ são todos divisíveis por p, então $(a + 1)^p - (a + 1)$ é divisível por p. □

3.2. **Função Φ de Euler.**

Definição 3.11. *Se n=1, então Φ(n)=1; se n>1, então Φ(n) é o número de inteiros k tais que 1≤k<n e* $(k, n) = 1$.

Exemplo 3.12. *Φ(5)=4.*

Teorema 3.13. *Sejam r e s números inteiros positivos com* $r > 1$ *e* $s > 1$ *e* $(r, s) = 1$. *Então* $\phi(r.s) = \phi(r).\phi(s)$.

Veja demonstração em [12].

3.3. **Cálculo de** $\Phi(n)$**.**

Teorema 3.14. *Se o inteiro* $n > 1$, *então* $\phi(n) = n - 1$ *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 3.15. *Se p é primo e se 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, $\phi(p^k) = p^k - p^{k-1}$. □

Conhecendo os resultados anteriores sobre a função Φ de Euler, podemos obter a expressão $\phi(n)$ para qualquer n pertencente aos inteiros positivos.

Teorema 3.16. *Se $n = p_1^{k_1}....p_r^{k_r}$ é a decomposição de n em fatores primos, então $\phi(n) = p_1^{k_1}....p_r^{k_r}.(1 - \frac{1}{p_1})...(1 - \frac{1}{p_r})$.*

Demonstração. Como os $p_{r's}$ são números primos temos que $\phi(n) = \phi(p_1^{k_1}....p_r^{k_r}) = \phi(p_1^{k_1})....\phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1})...(p_r^{k_r} - p_r^{k_r-1}) = p_1^{k_1}.(1 - \frac{1}{p_1}).p_2^{k_2}.(1 - \frac{1}{p_2})...p^{k_r}.(1 - \frac{1}{p_r}) = p_1^{k_1}....p_r^{k_r}.(1 - \frac{1}{p_1})...(1 - \frac{1}{p_r})$.

□

Lema 3.17. *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: $a.a_1, a.a_2, ..., a.a_{\phi(n)}$ é congruente módulo n a um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ (não necessariamente nesta ordem).*

Veja demonstração em [12].

Teorema 3.18. *(***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 $a^{\phi(1)} \equiv 1\ mod\ n$. Suponhamos, pois, $n > 1$. Sejam $a_1, a_2, ..., a_{\phi(n)}$ 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,

$$\begin{gathered} a.a_1 \equiv a'_1\ mod\ n \\ a.a_2 \equiv a'_2\ mod\ n \\ ..... \\ a.a_{\phi(n)} \equiv a'_{\phi(n)}\ mod\ n \end{gathered}$$

onde $a'_1, a'_2, ..., a'_{\phi(n)}$ são os inteiros $a_1, a_2, ..., a_{\phi(n)}$ numa certa ordem. Multiplicando essas $\phi(n)$ congruências obtemos:

$a.a_1, a.a_2, ..., a.a_{\phi(n)} \equiv a'_1.a'_2.....a'_{\phi(n)}\ mod\ n$. Daí, temos

$a^{\phi(n)}.(a_1.a_2.....a_{\phi(n)}) \equiv a'_1.a'_2.....a'_{\phi(n)}\ mod\ n$. Como $(a_i, n) = 1$ podemos cancelar o fator comum e portanto, $a^{\phi(n)} \equiv 1\ mod\ n$.

□

Observe que, se p é um número primo, então $\phi(p) = p - 1$, e se $(a, p) = 1$ temos que $a^{\phi(p)} \equiv 1\ mod\ p$, logo $a^{(p-1)} \equiv 1\ mod\ p$ que é o pequeno teorema de Fermat. Desta forma, o teorema de Euler é uma generalização do pequeno teorema Fermat.

4. **A Busca pelos Números Primos**

O Renascimento da Aritmética se deu, com o jurista francês Pierre de Fermat (1601-1665). Os resultados de Fermat foram divulgados, principalmente, por Marin Mersenne (1588-1648) outro curioso que se dedicou ao estudo dos números primos.

Leonhard Euler (1707-1783), a *"Águia Matemática"*, foi sem dúvida um dos maiores e mais férteis matemáticos de todos os tempos. A paixão de Euler pela teoria dos números foi motivada pela correspondência com Christian Goldbach, um matemático amador alemão que vivia em Moscou. Foi a Euler que Goldbach fez sua famosa conjectura de que *" todo número par maior ou igual a 4 pode ser escrito como a soma de dois números primos".*

Euler mostrou que o polinômio $p(n) = n^2 + n + 41$ gera números primos para $0 \leq n < 40$.

Carl Friedrich Gauss (1777-1855), o Príncipe dos Matemáticos, vendo que após séculos de pesquisa ainda não havia sido possível descobrir uma fórmula que gerasse números primos pensava em adotar uma estratégia diferente.

O grande avanço de Gauss, na busca pelos números primos, foi tentar descobrir como se distribuiam os números primos entre os 100 primeiros números inteiros, entre os primeiros 1000 e assim por diante.

Bernhard Riemann (1826-1866) também se dedicou à busca pelos números primos apesar da teoria dos números não ser sua área de interesse.

Riemann teve a idéia de definir a função zeta para todos os números complexos s, tendo parte real maior que 1,

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

A Função Zeta de Riemann deu origem à Hípótese de Riemann. Uma hipótese matemática publicada em 1859 por Bernhard Riemann que declara que os *os zeros não triviais da Função Zeta de Riemann pertencem todos à " linha crítica".*

A Hipótese de Riemann é de tal importância que tem intrigado os matemáticos há mais de 150 anos e é hoje um dos poucos problemas apresentados por David Hilbert (1862-1943), em 1900, no Congresso Internacional de Matemática em Paris, não resolvidos.

A busca pelos números primos continua. 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 cripto-sistemas de *chave pública* em 1976. A idéia 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 saberá qual é a chave privada, pois ela não é transmitida a ninguém. Essa idéia 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. **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 E_U. Porém a chave privada de U é conhecida somente por U e consiste da função decodificação D_U. Além disso, as funções codificação e decodificação são baseadas na noção de uma "função 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 E_U e D_U (onde U é o conjunto formado por todos os usuários potenciais) de funções codificação e decodificação, respectivamente, tais que:

i) Para todo U, $D_U(E_U(M) = M$, onde M é um bloco da mensagem pré-codificada;

ii) Para todo U, E_U está no diretório público, mas D_U é conhecida somente por U;

iii) Para todo U, E_U é a função armadilha ;

iv) Para todo U $E_U(D_U(M) = M$(assinatura digital).

5.1. ***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 $e.d = 1 \mod (\phi(N))$ onde e é conhecido, mas d é mantido secreto. As funções *codificação* 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 99 é o espaço entre as duas palavras.

Usando o Algoritmo Euclideano podemos determinar o inteiro d tal que $e.d = 1 \mod (\phi(N))$. Mostraremos agora que $E(D(x)) = x$ e $D(E(x)) = x$, ou seja, as funções E e D são a inversa uma da outra e é por isso que o método funciona. Note que $D(E(x)) = D(x^e mod N) = x^{e.d} mod\ N$ e $E(D(x)) = E(x^d mod\ N) = x^{e.d} mod\ N$. 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, $e.d \equiv 1\ mod\ (\phi(N)$. Consequentemente existe um inteiro 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, $x^{e.d} \equiv x\ mod\ p$. Se p divide x então $x \equiv 0\ mod\ p$. Assim $x^{e.d} \equiv x\ mod\ p$ vale para qualquer p. Analogamente $x^{e.d} \equiv x\ mod\ q$ vale para qualquer q. Observe que não podemos usar um argumento diretamente para N , pois o fato $(N, x) \neq 1$ não significa que $x \equiv 0\ mod\ N$, pois N é composto.

Exemplo 5.1. *Seja 31-18-31-10-99-17-24-19-14 a mensagem pré-codificada em blocos vista anteriormente. Queremos codificar o bloco* $x = 14$. *Vamos determinar os parâmetros para fazermos a codificação. Sejam* $p = 11$ *e* $q = 13$, *daí* $N = 11.13 = 143$. *Temos que* $\phi(N) = (p-1).(q-1) = (11-1).(13-1) = 10.12 = 120$. *Sabemos que* $(e, \phi(N)) = 1$, *desta forma vamos considerar* $e = 7$. *Considerando* $e = 7$ *podemos determinar o valor de d. Sabemos que* $e.d \equiv 1\ mod\ (\phi(N)) \Rightarrow 7.d \equiv 1\ mod\ 120 \Rightarrow 120 \mid 7.d - 1 \Rightarrow 7.d - 1 = 120.k \Rightarrow 7.d - 120.k = 1$.

Aplicando o Algoritmo Euclideano para e e $\phi(N)$ *obtemos:* $120 = 17.7 + 1 \Rightarrow 1 = 120 + (-17).7$, *logo o inverso de 7 módulo 120 é -17, mas precisamos que d seja positivo. Portanto,* $d = 120 - 17 = 103$ *que é o menor inteiro positivo congruente a -17 módulo 120.*

Assim o bloco $x = 14$ *é codificado como* $E(14) = 14^7\ mod\ 143$, *isto é,* $E(14)$= *o resto da divisão de* 14^7 *por* 143. *Fazendo os cálculos encontramos que* $14^7 \equiv 53\ mod\ 143 \Rightarrow E(14) = 53$. *Para decodificarmos* $E(14) = 53$ *vamos usar a função decodificação D, ou seja,* $D(E(14)) = E(14)^d\ mod\ N = 53^{103}\ mod\ 143$, *isto é,* $D(E(14))$ = *o resto da divisão de* 53^{103} *por 143. Fazendo os cálculos encontramos* $53^{103} \equiv 14\ mod\ 143$. *Portanto,* $D(53) = 14$.

Como vimos anteriormente, a segurança do RSA está na dificuldade de se fatorar N. Se a escolha dos parâmetros p e q não for feita com cuidado, pode ser fácil quebrar o sistema RSA.

6. **Tipos de Números Primos**

Existem números primos que possuem nomes especiais. A maioria deles leva o nome de seus descobridores e seguem um modelo para obtê-los.

6.1. **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 assim 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.

6.2. **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 os divisores próprios de 6. O número 28 também é perfeito, assim como 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 da forma* 2^{n-1}*(*2^n*-1) é par perfeito, se e somente se,* 2^n*-1 for primo.*

A existência de um número perfeito ímpar é um dos mais antigos problemas matemáticos ainda sem solução. Conjectura-se com fortes indícios experimentais que não existe nenhum.

Os números M_q=2^q-1 , q número primo, são chamados *números de Mersenne*. O maior número primo conhecido é um Número de Mersenne $2^{32.582.657} - 1$, um gigante com 9.808.358 de 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.

6.3. **Números Primos de Sophie 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 demonstrá-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 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 Antoine August Le- Blanc para ser aceita pelos matemáticos. Durante muito tempo Sophie Germain se correspondeu com Gauss usando o pseudôni-mo masculino. Porém, em 1807 ela revelou sua identidade e 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.

6.4. **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. Em 1919, 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.

7. **Testes de Primalidade**

Números Primos são de fundamental importância em matemática em geral, e em teoria dos números em particular. Desta forma, há um grande interesse em estudar diferentes propriedades dos números primos. Especialmente aquelas que permitem determinar eficientemente se um dado número é primo. Um problema clássico em matemática é: dado um número n, como conhecer se ele é primo ou composto?

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. Neste trabalho serão apresentados testes de primalidade *determinísticos e probabilísticos.*

7.1. **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 escre-ver todos os inteiros de 1 a N. Como 1 não é primo, pode ser riscado imediatamente. O algorítmo 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 7.1. *Construir a tabela de todos os primos menores que 100.*

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 múltiplos 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.*

7.2. **Divisão por Tentativas.**

Proposição 7.2. *Todo número inteiro* α *maior que 1 tem um divisor primo.*

Demonstração. O número inteiro α tem um divisor que é maior que 1, ou seja, α. Entre todos os divisores de α 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 $1 < b < p \leq \alpha$. (Contradição).

□

Proposição 7.3. *Se n é um inteiro positivo composto, então n possui um divisor primo p que é menor que ou igual a* $\sqrt{n}$.

Demonstração. Se n é um inteiro positivo composto então n possui um divisor primo p tal que p$\leq\sqrt{n}$. Como n é composto podemos escrever n=ab, 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=ab>$\sqrt{n}\sqrt{n}$=n. Suponha que a$\leq\sqrt{n}$. Pela proposição 7.2 *a* tem um divisor primo p. Como p$\leq$a$\leq\sqrt{n}$ $\Rightarrow$ p também é divisor de n. Portanto, n possui um divisor primo p tal que p$\leq\sqrt{n}$. □

A proposição anterior 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 encontrado 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 7.4. *43 é um número primo?*

Temos que a raiz quadrada inteira mais próxima de 43 é 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.

7.3. **Teste de Fermat.** O Pequeno Teorema de Fermat dá origem a um teste de primalidade probabilístico chamado Teste de Fermat. O Teste consiste em:

Dado a>1, escolha p>1 e calculemos a^{p-1} *mod p*. Se o resultado não for 1 mod p, então n 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 7.5. *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. A Tabela 1 apresenta o menor pseudoprimo para as bases entre 2 e 10.

7.4. **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.

Definição 7.6. *Um número composto ímpar n>0 é um número de Carmichael se* $a^n\equiv$ *a mod n para todo 1<a<n-1.*

TABELA 1. Menor Pseudoprimo

Inteiro a	Menor pseudoprimo para a base a
2	341=11.13
3	91=7.13
4	15=3.5
5	124=2^2
6	35=5.7
7	25=5^2
8	9=3^2
9	28=2^2.7
10	33=3.11

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

Exemplo 7.7. *O número 561 é um número de Carmichael. Não é fácil provar esta afirmação usando a definição, pois precisaríamos verificar que* $a^{561} \equiv a \ mod\ 561$ *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 7.8. *(**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 *não divide n e p-1 divide n-1.*

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

Exemplo 7.9. *Temos que 561= 3.11.17.*
$3^2 \nmid 561$, $11^2 \nmid 561$, $17^2 \nmid 561$. *Temos que* $3-1 = 2$ *e* $2 \mid 560$,$11-1 = 10$ *e* $10 \mid 560$ *e* $17-1 = 16$ *e* $16 \mid 560$.

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.

7.5. **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 seguintes potências de b: b^d, b^{2d}, b^{2^2d},..., $b^{2^{s-1}d}$, b^{2^sd}. Se n for um número primo, então
$b^{2^sd} = b^{n-1} \equiv 1$ mod n.

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

Se k=0 então $b^{2^0d} \equiv 1$ mod n daí $b^d \equiv 1$ mod n.

Se $k > 0$, então podemos fatorar b^{2^kd}-1 como $(b^{2^{k-1}d}-1).(b^{2^{k-1}d}+1)$. Como n é primo e divide b^{2^kd}-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^kd}-1. Portanto, n divide $b^{2^{k-1}d}+1$, isto é, $b^{2^{k-1}d} \equiv$ -1 mod n.

Concluimos, pela análise anterior que: se n é primo, então para toda base b 1<b<n-1 escrevendo as d potências b^d, b^{2d}, b^{2^2d},..., $b^{2^{s-1}d}$, b^{2^sd}, ou a primeira é congruente a 1 mod n ou alguma delas será 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 n satisfaz alguma das condições acima para a base b, então n é *pseudoprimo forte* para a base b.

Exemplo 7.10. *Se n=341 temos que n-1=340=$2^2$85, onde d=85 e 0≤s<2. Sendo b = 2 precisamos calcular duas potências:*
$2^{2^0 85} = 2^{85} \equiv$ *32 mod 341*
$2^{2^1 85} = 2^{170} = 2^{85} \equiv 32^2 \equiv$ *1 mod 341.*

Como nem a primeira potência é congruente a 1 mod 341, nem alguma delas é congruente a -1 mod 341, então 2 é testemunha de que 341 é composto.

Exemplo 7.11. *Se n=25 temos que n-1=24=$2^3$3 onde d=3 e 0≤s<3. Calculando as potências para b = 7 obtemos:*
$7^{2^0 3} = 7^3 \equiv$ *18 mod 25,* $7^{2^1 3} = 7^6 \equiv$*24 mod 25*
e $7^{2^2 3} = 7^{12} \equiv$ *1 mod 25.*
Vemos que 7^3 *não é congruente 1 mod 25, mas temos que* $7^6 \equiv$ *24 mod 25 e*
24≡ -1 mod 25. Portanto, 25 é um pseudoprimo forte *para base 7, embora saibamos que 25 é composto.*

7.6. **Teste de Primalidade *AKS*.**

Definição 7.12. *Um algorítmo é chamado de tempo polinomial se existirum polinômio f(X), tal que para todo N o tempo necessário para executá-lo, quando o dado inicial é o número N, é limitado por f(N).*

Em 2002, o Professor Manindra Agrawal e dois de seus alunos de graduação, Neeraj Kayal e Nitin Saxena, descobriram um algorítmo determinístico de tempo polinomial para testar se um número é primo ou composto. Esta equipe de jovens pesquisadores do Instituto Indiano de Tecnologia de Kampur, resolveu um problema em Teoria dos Números e Ciência da Computação que desafiou as melhores mentes por décadas. O AKS é o primeiro algoritmo determinístico a executar um teste de primalidade em tempo polinomial. O algoritmo AKS é baseado na identidade $(X-a)^n \equiv (X^n - a)\ mod\ n$ a qual é verdadeira somente se n é primo. Esta identidade é uma generalização do Teorema de Fermat estendido para polinômios e pode ser provada usando o Teorema Binomial [4] , juntamente com o fato de que $\binom{n}{k} \equiv 0\ mod\ n$ para todo $0 < k < n$ se n é primo.

O AKS faz uso da equivalência $(X^n - a) \equiv\ X^n + a(mod\ X^r - 1, n)$ a qual pode ser verificada em tempo polinomial. Enquanto todos os primos satisfazem esta equivalência alguns números compostos também a satisfazem. Para corrigir este problema mostra-se que para escolhas apropriadas de r, a equação é satisfeita para vários $a's$ e logo n deverá ser uma potência de um primo. O número de $a's$ e r apropriados são ambos limitados por um polinômio em logn e desta forma, conseguiu-se um *algoritmo determinístico em tempo polinomial*.

Após dois anos da divulgação do artigo *Primes is in P*, onde os pesquisadores indianos detalham o algoritmo, já existem versões otimizadas e generalizadas.

8. **Conclusão**

Neste mini-curso apresentamos e desenvolvemos alguns fudamentos matemáticos dos Criptosistemas de Chave Pública, além de mostrar que os resultados mais interessantes e curiosos sobre números primos foram obtidos com a utilização do computador, e que o Pequeno Teorema de Fermat é fundamental na criação de testes de primalidade mais modernos.

Referências

[1] ANDERSON, M.A. e BELL, J.M., *Number Theory with Applications,* PRENTICE HALL, New Jersey, 1997.

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

[3] COUTINHO, S.C., *Primalidade em Tempo Polinomial,* SBM, Coleção Iniciação Científica, Rio de Janeiro, 2004.

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

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

[6] *Divisibilidade e Números Inteiros,* OBMEP 2005.

[7] ARNAULT, F. , *Rabin-Miller Primality Test: Composite Numbers Which Pass It,* American Mathematical Society, 1995.

[8] AGRAWAL, M.,KAYAL, N. e SAXENA, N., *Primes is in P,* Annals of Mathe matics, 160 (2004), 781-793.

[9] RIBENBOIM ,P., *Números Primos: mistérios e recordes ,* IMPA, Coleção Matemática Universitária, Rio de Janeiro, 2001.

[10] SAUTOY, M., *A Música dos Números Primos,* Editora ZAHAR, Rio de Janeiro, 2003.

[11] SHKLARSKY, D.O., CHENTZOV, N.N. e YAGLOM, I.M.,*THE USSR OLYMPIAD PROBLEM BOOK,* DOVER PUBLICATION, INC, New York, 1994.

[12] ALENCAR FILHO.E., *Teoria Elementar dos Números*, Editora Nobel, São Paulo, 1985.