

ESTUDO DO MÉTODO DE FATORAÇÃO DE INTEIROS NFS

Jéssica Nazareth da Silva¹; Adriana Betânia de Paula Molgora²

¹Estudante do Curso de Matemática da UEMS, Unidade Universitária de Dourados; E-mail:

jessica-nazareth@hotmail.com

²Professora do Curso de Matemática da UEMS, Unidade Universitária de Dourados; E-mail:

adrianamolgora@gmail.com

Área Temática: Teoria Computacional dos Números

Resumo

O problema de fatoração de inteiros tem motivado diversos estudos devido a sua aplicação em sistemas criptográficos como o RSA (*Rivest Shamir Adleman*). O NFS (*Number Field Sieve*) é um dos métodos de fatoração de inteiros mais importantes da atualidade, utilizado na fatoração de números com mais de cem dígitos decimais. No entanto, o entendimento do funcionamento desse método exige muito estudo devido à complexidade dos conceitos matemáticos envolvidos em seu processo de fatoração. Nesse sentido, esse trabalho tem como objetivo apresentar um estudo teórico do método NFS, realizado através de pesquisas bibliográficas sobre o mesmo.

Palavras-chave: RSA. Números primos. Congruências.

1. Introdução

A fatoração de inteiros é um problema matemático antigo que tem sido muito estudado por ter aplicação direta em sistemas criptográficos de chave pública como o RSA. Isso justifica-se pelo fato de que se for desenvolvido um método que fatore qualquer inteiro dado, a segurança desses sistemas criptográficos estará comprometida [4]. Nesse sentido, estudos sobre métodos de fatoração são imprescindíveis.

O NFS figura como o método mais utilizado na fatoração de números inteiros com mais de 100 dígitos decimais [2]. O entendimento do funcionamento desse método exige um estudo aprofundado e detalhado de diversos conceitos matemáticos. Nesse sentido, esse trabalho tem como objetivo apresentar um estudo teórico do método NFS de fatoração de inteiros, visando disponibilizar conhecimentos sobre o funcionamento desse método de fatoração e possibilitar estudos mais avançados em pesquisas posteriores.

2. Materiais e Métodos

Para alcançar o objetivo proposto o trabalho foi distribuído em quatro etapas compreendendo:

- Estudo da fundamentação matemática aplicada ao método NFS;
- Estudo dos passos do processo de fatoração realizado por meio do método NFS;
- Estudo das pesquisas mais recentes relacionadas com o método NFS;
- Documentação do processo de fatoração pelo método NFS, de forma a facilitar o entendimento do mesmo.

Esse estudo foi realizado através de pesquisa bibliográfica.

3. Resultados e Discussão

A idéia fundamental do método NFS, foi desenvolvida por John Pollard em 1988 [3]. Nesta seção será apresentado o processo de fatoração realizado por esse método de fatoração. Mais informações podem ser obtidas em [1, 2, 3, 4, 5].

O processo de fatoração através do método NFS tem como base o fato de que se existirem números x e y tais que $x^2 \equiv y^2 \pmod{n}$, então $(x+y)(x-y) \equiv 0 \pmod{n}$. Ou seja, os números $a = \text{mdc}(x+y, n)$ e $b = \text{mdc}(x-y, n)$ são fatores de n . Nesse sentido, a fatoração de um inteiro n através do método NFS é realizada supondo-se que é possível encontrar um $\beta^2 \in \mathbb{Z}[\theta]$ que é um quadrado perfeito e $y^2 \in \mathbb{Z}$ que é um quadrado perfeito. Então pode se produzir uma congruência de diferença de quadrados para ser utilizada na fatoração de n . Essa idéia tem como base o teorema a seguir:

Teorema: Dado um polinômio $f(x)$ com coeficientes inteiros, uma raiz $\theta \in \mathbb{C}$, e um $m \in \mathbb{Z} \setminus n\mathbb{Z}$ tal que $f(m) \equiv 0 \pmod{n}$, existe uma única função $\phi: \mathbb{Z}[\theta] \rightarrow \mathbb{Z}/n\mathbb{Z}$ satisfazendo

- 1) $\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in \mathbb{Z}[\theta]$
- 2) $\phi(a+b) = \phi(a) + \phi(b) \quad \forall a, b \in \mathbb{Z}[\theta]$
- 3) $\phi(1) \equiv 1 \pmod{n}$
- 4) $\phi(\theta) \equiv m \pmod{n}$

(As condições acima também implicam que $\phi(za) = z\phi(a) \quad \forall a \in \mathbb{Z}[\theta], z \in \mathbb{Z}$).

Pode-se aplicar este teorema para obter uma diferença de quadrados congruentes supondo que existe um conjunto finito U de pares inteiros (a, b) tal que

$$\prod_{(a,b) \in U} (a+b\theta) = \beta^2 \text{ e } \prod_{(a,b) \in U} (a+bm) = y^2, \text{ para } \beta \in \mathbb{Z}[\theta] \text{ e } y \in \mathbb{Z}. \text{ Seja } x = \phi(\beta). \text{ Então, usando}$$

congruências modulo n , tem-se que $x^2 \equiv \phi(\beta) \phi(\beta) \equiv \phi(\beta^2) \equiv \phi\left(\prod_{(a,b) \in U} (a + b\theta)\right)$
 $\equiv \prod_{(a,b) \in U} (\phi(a + b\theta)) \equiv \prod_{(a,b) \in U} (a + bm) \equiv y^2$. Portanto, uma relação $x^2 \equiv y^2 \pmod{n}$ foi criada.

Para um melhor entendimento do método NFS, será apresentado um exemplo numérico do processo de fatoração realizado por esse método, obtido em [2]. Considere o número composto $n = 45113$. Em primeiro lugar, deve-se encontrar um polinômio $f: \mathbb{R} \rightarrow \mathbb{R}$ com coeficientes inteiros, e um $m \in \mathbb{N}$ que satisfaça $f(m) \equiv 0 \pmod{n}$. Por exemplo, para $m = 31$ e considerando $n = am^d + am^{(d-1)} + \dots + a$ tem-se $45113 = 31^3 + 15 \cdot 31^2 + 29 \cdot 31 + 8$. Ou seja, o polinômio será dado por $f(x) = x^3 + 15x^2 + 29x + 8$, pois, $f(31) = 45113 \equiv 0 \pmod{n}$.

Em segundo lugar obtém-se uma base de fatores racionais. Por exemplo, considerando os números primos inferiores a 30, tem-se $R = (2, 3, 5, 7, 11, 13, 17, 19, 23, 29)$.

Depois de obtida essa base, constrói-se uma base A representada por pares (r, p) onde p é um primo e r satisfaz $f(r) \equiv 0 \pmod{p}$. Aleatoriamente é escolhido um p inferior a 90 tal que para $\forall_i, f(r_i) \equiv 0 \pmod{p}$. Para cada r_i é adicionada uma entrada (r_i, p) para A . Esse processo é repetido para todos os p no conjunto dos números primos inferiores a 90. Por exemplo, para $p = 2$ e $r = 0$ tem-se $f(r) = r^3 + 15r^2 + 29r + 8 \Rightarrow f(r) = 0^3 + 15 \cdot 0^2 + 29 \cdot 0 + 8 \Rightarrow f(r) = 8 \Rightarrow 8 \pmod{2} \equiv 0$. Como $f(r) \equiv 0 \pmod{p}$ obtemos assim o par $(0, 2)$. Realizando esses cálculos para os demais pares, obtém-se:

$A = \{(0,2), (6,7), (13,17), (11,23), (26,29), (18,31), (19,41), (13,43), (1,53), (46,61), (2,67), (6,67), (44,67), (50,73), (23,79), (47,79), (73,79), (28,89), (62,89), (73,89)\}$

Depois de obtida a base A , é necessário obter uma base Q de pares (s, q) , escolhendo primos que não estejam na base A . Para cada q deve-se encontrar s que satisfaça $f(s) \equiv 0 \pmod{q}$. Por exemplo, para $q = 97$ e $s = 28$ tem-se $f(s) = f(28) = 28^3 + 15 \cdot 28^2 + 29 \cdot 28 + 8 = 34532 \pmod{97} \equiv 0$. Assim obtém-se o par $(28, 97)$. O mesmo procedimento é realizado na obtenção dos demais pares. Dessa forma, tem-se $Q = \{(28,97), (87, 101), (47, 103), (4, 107), (8, 107), (80, 107)\}$

O próximo passo é encontrar pares (a, b) , que satisfaçam $a + bm$ e $a + b\theta$. Nesse caso, tem-se 38 pares que satisfazem essas condições: $(-73,1) (-13,1) (-6,1) (-2,1) (-1,1) (1,1) (2,1) (3,1) (13,1) (15,1) (23,1) (61,1) (1,2) (3,2) (33,2) (2,3) (5,3) (19,4) (14,5) (37,5) (313,5) (11,7) (15,7) (-7,9) (119,11) (-247,12) (175,13) (5,17) (-1,19) (35,19) (17,25) (49,26) (375,29) (9,32) (1,33) (78,37) (5,41) (9,41)$. Esses pares devem então ser representados em uma matriz de 0's

e 1's, como segue. Calcular $a+bm$ para cada par (a,b) . Se o resultado for positivo a entrada é igual a 0, se for negativo entrada 1. Para o par $(119,11)$ e $m = 31$, tem-se $(a+bm) = 119+11 \cdot 31 = 460$. Como o resultado é positivo a entrada recebe 0. Depois de calculado $a+bm$ fatora-se o valor encontrado. Os fatores serão divisíveis pelos números da base R . Usando então os expoentes destes fatores tem-se, para o par $(119,11)$ que $(a+bm) = 460 = 2^2 \cdot 5 \cdot 23$. Ou seja, a representação será dada por:

0 0010000010

O passo seguinte será verificar se um elemento particular de A divide $a + b\theta$. Para essa verificação é utilizado o polinômio $(-b)^d f(-a/b)$, onde d é o grau do polinômio. Ou seja, $a + b\theta = (-b)^d f(-a/b) = a^3 - 15a^2b + 29ab^2 - 8b^3$. Para o par $(119,11)$, tem-se $(a + b\theta) = (-11)^3 f(-119/11) = (119)^3 - 15 \cdot (119)^2 \cdot 11 + 29 \cdot 119 \cdot (11)^2 - 8 \cdot (11)^3 = -244 483 = -1 \cdot 41 \cdot 67 \cdot 89$. Logo, os pares que satisfazem essa condição são:

$(19,41), (2,67), (6,67), (44,67), (28,89), (62,89), (73,89)$

Em seguida, para cada um desses pares é calculada a congruência $a \equiv -br \pmod{p}$. Para o par que satisfaz a congruência dada atribui-se 1. Para os demais pares de A atribui-se 0. Ou seja, para o par $(119,11)$ tem-se:

00000010000010000010

O próximo passo é calcular o símbolo de Legendre $\left(\frac{a+bs}{q} = 1\right)$, para os pares do conjunto Q . Cada entrada será definida como 0 se o resultado for igual a 1. Caso contrário, a entrada será 1. Assim, para o par $(a, b) = (119,11)$ e para os pares do conjunto Q tem se:

110000

Em seguida, é montada uma matriz X , cujas linhas são determinadas pelos pares (a,b) , através do processo já descrito. Ou seja, a linha de X referente ao par $(119,11)$ será dada por:

[0 0010000010 00000010000010000010 110000]

Nesse caso, a matriz X terá 38 linhas e 37 colunas. Aplicando-se o processo de eliminação gaussiana [5] em X e, ao mesmo tempo na matriz identidade $I_{38 \times 38}$, será possível obter uma ou mais linhas nulas em X . A linha correspondente em I , poderá assim, possibilitar a obtenção de uma diferença de quadrados. Nesse exemplo, uma das soluções será:

[0,0,0,1,0,1,0,0,1,1,1,0,0,1,1,0,1,1,1,0,0,0,1,0,1,0,1,0,1,0,0,0,0,0,0]

Utilizando os pares $(-2,1), (1,1), (13,1), (15,1), (23,1), (3,2), (33,2), (5,3), (19,4), (14,5), (15,7), (119,11), (175,13), (-1,19), (49,26)$ correspondentes aos 1's que aparecem na solução

encontrada, obtém-se $\prod_{(a,b) \in V} (a + bm) = 45999712751795195582606376960000$ e

$$\prod_{(a,b) \in V} (a + b\theta) = 58251363820606365 \theta^2 + 149816899035790332 \theta +$$

$$75158930297695972. \text{ Ou seja, } 2553045317222400^2 = \prod_{(a,b) \in V} (a + bm) \text{ e}$$

$$\left(108141021 \cdot \theta^2 + 235698019 \cdot \theta + 62585630\right)^2 = \prod_{(a,b) \in V} (a + b\theta) \text{ e}$$

$$\phi \left(108141021 \cdot \theta^2 + 235698019 \cdot \theta + 62585630\right) = 111292745400$$

$$\text{Logo, } 111292745400^2 \equiv 2553045317222400^2 \pmod{n} \text{ e}$$

$$\text{mdc}(45113, 111292745400 + 2553045317222400) = 197$$

$$\text{mdc}(45113, 111292745400 - 2553045317222400) = 229$$

Portanto, $n = 45113 = 197 \cdot 229$, e a fatoração foi concluída.

É notável, que o processo de fatoração de números inteiros através do método NFS é bastante complexo, necessitando de estudos aprofundados dos aspectos matemáticos envolvidos em seu contexto.

Através desse estudo, foi possível obter conhecimento e experiência sobre o funcionamento do método NFS e divulgar conhecimentos que possam servir como base para facilitar estudos mais avançados sobre o mesmo.

4. Agradecimentos

Os autores agradecem pelo apoio financeiro (bolsa) concedido pela Universidade Estadual de Mato Grosso do Sul e também por todos que diretamente ou indiretamente, contribuíram para a realização desse trabalho.

5. Bibliografia

- [1] ANTUNES, Cristiane M. Métodos de Fatoração de Números Inteiros. 2002. 75p. Dissertação de Mestrado-Universidade Federal do Rio Grande do Sul.
- [2] CASE, Michael. A Beginner's Guide To The General Number Field Sieve, 2003. Disponível em: <<http://www.islab.oregonstate.edu/koc/ece575/03Project/Case/paper.pdf>> Acesso em: 15 de setembro de 2009.
- [3] POMERANCE, Carl. The Number Field Sieve, 1994. Disponível em <<http://www.math.dartmouth.edu/~carlp/PDF/paper99.pdf>> Acesso em: 10 de setembro de 2009.
- [4] COUTINHO, S. Números inteiros e Criptografia RSA. IMPA-SBM, 2000.
- [5] RUGGIERO, Márcia A. Gomes; LOPES, Vera Lúcia da Rocha. Cálculo Numérico: aspectos teóricos e computacionais. 2. ed. São Paulo: MAKRON Books, 1996.