CRIVO QUADRÁTICO: UM ESTUDO DA OBTENÇÃO DE UM QUADRADO PERFEITO

Marcelo Figueiredo Terenciani[1]; Adriana Betânia de Paula Molgora[2]

[1]Estudante do Curso de Ciência da Computação da UEMS, Unidade Universitária de Dourados; e-mail: terenciani@yahoo.com.br, Bolsista PIBIC.

[2]Professora do Curso de Ciência da Computação da UEMS, Unidade Universitária de Dourados; e-mail: abmol@terra.com.br

Área Temática: Teoria Computacional dos Números

Resumo. O interesse pela fatoração de números inteiros foi despertado pela necessidade de um entendimento mais aprofundado sobre esse tema. O Crivo Quadrático apesar de ser um método de fatoração de apenas vinte anos é um dos mais importantes na fatoração de números inteiros. O objetivo deste trabalho é realizar um estudo do processo de obtenção de um quadrado perfeito, que é uma das etapas requeridas pelo método em questão. Através da uma pesquisa bibliográfica foram estudados métodos que podem ser utilizados no desenvolvimento dessa etapa do Crivo Quadrático. Com este estudo podemos constatou-se que existem algumas melhorias que podem ser acrescentadas ao Crivo Quadrático resultando em ganho de desempenho ao mesmo.

Palavras chave: Fatoração. Criptografia. Crivo.

1. Introdução.

A Criptografia moderna baseia-se no fato de que a fatoração de números inteiros é um problema muito difícil. Criar grandes números compostos multiplicando primos grandes juntos é muito fácil, mas é muito difícil reconstruir os fatores primos de um número grande. Um exemplo de um sistema que usa este fato é o sistema RSA, famoso e amplamente utilizado hoje. (Asbrink e Brynielsson, 2000).

O Crivo Quadrático *(Quadratic Sieve),* Pomerance (1985), foi desenvolvido por Carl Pomerance em 1981, é um método de fatoração considerado um dos mais eficientes na fatoração de números inteiros. Seu funcionamento é dividido basicamente em duas etapas: determinação de um conjunto de números que sejam fatorados por uma base de fatores e obtenção de números que sejam quadrados perfeitos.

A complexidade do Crivo Quadrático ao fatorar um número *n*, não rigorosamente provada, é dada por $e^{(1+o(1))\sqrt{\log n \log\log n}}$. Portanto, para *n* muito grande o trabalho executado por uma implementação do método cresce exponencialmente, o que torna a fatoração de *n* muito grande impraticável (SOUZA, 2004).

O objetivo desse trabalho é realizar um estudo dos procedimentos envolvidos na segunda etapa do método e disponibilizar conhecimentos, de forma mais simplificada, possibilitando estudos mais avançados em pesquisas posteriores.

2. Materiais e Métodos

O desenvolvimento do trabalho foi centrado na pesquisa bibliográfica, principalmente em:

1. Documentos, e-books, artigos e teses de dissertações disponíveis em sites na internet;
2. Livros particulares e também da Biblioteca Central da UEMS.

3. Resultados

Os conceitos básicos, como o de espaços vetoriais, matriz identidade, independência linear, podem ser encontrados em Lima (2000) e Cláudio e Marins (1994).

3.1 Crivo Quadrático

A fatoração de inteiros através do método Crivo Quadrático tem como base o fato de que se existirem números *x* e *y* que satisfaçam a condição $x^2 \equiv y^2 \pmod{n}$, então se têm que $(x + y) \cdot (x - y) \equiv 0 \pmod{n}$. Logo, $\frac{n}{(x^2 - y^2)} = (x + y) \cdot (x - y)$ e os números $d \equiv mdc\,(x + y, n)$ e $f = (x - y, n)$ poderão ser fatores não triviais de *n*. Ou seja, a idéia básica do método consiste em encontrar congruências da forma $x_i^2 \equiv y_i^2 \pmod{n}$.

De acordo com Crandall e Pomerance (2002), na prática, para encontrar *x* e *y*, em primeiro lugar deve-se encontrar uma base de fatores, que é um conjunto de números primos como, para certo limite *B* e, para cada primo *p*, o número *n* deve ser um resíduo quadrático módulo *p*. Em seguida é determinado um conjunto de números completamente fatorados sobre essa base de fatores $f(r)'s$.

Através do conjunto de números obtidos na etapa anterior, busca-se obter os quadrados perfeito requeridos pelo método Crivo Quadrático, que é o objeto de estudo desse trabalho.

Para a próxima etapa do método é necessário a construção de uma matriz principal (*M*), onde o número de linhas é determinado pelo número de completamente fatorados ($f(r)'s$) e o número de colunas é o número de primos da base de fatores (*p*).

Então para cada $f(r)$ associa-se uma (string) de *p* dígitos binários. Caso o primo correspondente apresente potência par, então o dígito que o representa é 0; se a potência é ímpar o dígito é 1.

O próximo passo é associar uma matriz identidade (*I*) quadrada de acordo com a quantidade $f(r)'s$ à matriz (*M*) formada anteriormente a fim de dizer qual combinação de $f(r)'s$ dará um quadrado perfeito. São realizados os passos da Eliminação Gaussiana nas duas matrizes. A Eliminação Gaussiana é realizada até que seja encontrada uma linha com todos os elementos nulos na matriz principal. A linha correspondente da matriz identidade indicará quais $f(r)'s$ devem ser multiplicados para que se encontre um quadrado perfeito. As colunas da matriz identidade com o dígito 1 indicam quais $f(r)'s$ devem ser multiplicados. Então *x* será o produto dos *r's* correspondentes módulo *n* e *y* serão dado pela raiz do produto dos fatores dos $f(r)'s$ módulo *n*, depois faz o *mdc (x – y, n)* e *mdc(x + y, n).* O resultado destes dois *mdc's* são os fatores de *n.* O maior divisor comum de dois ou mais números é chamado de máximo divisor comum desses números. Usamos à abreviação m.d.c.

Tomando como exemplo o número *8051* com uma base formada pelos primos: {*5, 7, 13, 23, 43, 47, 59, 61, 79, 103*} e os seguintes $f(r)'s$: {*413, 2765, 3185, 4945, 5405, 9373, 12685, 34385, 36049, 60593, 3745*}, e aplicarmos as devidas transformações, ao realizar a Eliminação Gaussiana em a 1º linha a ser zerada é a 8º linha da matriz (*M*). A linha correspondente em identidade (*I*) será: [0 0 1 0 0 0 0 1 0 0 0], ou seja, os $f(r)'s$ serão o 3º e o 8º: 3185 3438. O *x=5734 e y=3320.* Após os cálculos do *mdc* o número *8051* terá os fatores *83* e *97.* A descrição completa desse exemplo e também outros exemplos podem ser encontradas em Sanches (2010).

3.2 Eliminação Gaussiana

Segundo Cláudio e Marins (1994), a Eliminação Gaussiana consiste basicamente em duas etapas, triangulação e retrossubstituição. A triangulação consiste em transformar uma matriz *A* numa matriz triangular superior, mediante permutações e combinações lineares de linhas, ou seja, adição de uma linha com o múltiplo de outra linha, para substituir uma das linhas consideradas, às vezes poderá necessitar de fazer apenas a multiplicação de uma linha por uma

constante, quanto existem elementos nulos na diagonal principal é necessária a troca de linhas. A retrossubstituição consiste no cálculo dos componentes regressivamente.

Por exemplo:

$$\begin{matrix} 6 & 2 & 1 \\ -3 & 1 & 0 \\ 12 & 0 & 3 \end{matrix} \Rightarrow \begin{matrix} 6 & 2 & 1 \\ 0 & 4 & 1 \\ 0 & 2 & 3/2 \end{matrix} \Rightarrow \begin{matrix} 6 & 2 & 1 \\ 0 & 4 & 1 \\ 0 & 0 & -2 \end{matrix}$$

L2 = **2**xL2 + L1 L3 = **-2**xL3 + L2

L3 = **-1/2**xL3 + L1

O último e não menos critico passo do QS é a Eliminação Gaussiana, pois é formada uma matriz muito grande e com quase todas as estradas sendo 0. Não é viável realizar este processo em paralelismo, pois a comunicação que teria de haver entre os processadores seria enorme deixando o método muito lento.

Existem diferentes algoritmos para realizar a resolução de sistemas lineares, entre eles está o Algoritmo de Lanczos, descrito em Buchmann e Muller (2005), consiste em encontrar uma matriz inversível $W = [w_1,..., w_n]$ tal que $W^t \cdot A \cdot W = D$, onde D é uma matriz diagonal (matriz composta somente pela diagonal principal). Em seguida uma solução y do sistema linear $D \cdot y = W^t \cdot b$ é uma solução. Uma vez que D é uma matriz diagonal, uma solução de $D \cdot y = W^t \cdot b$ pode ser calculada muito fácilmente. Portanto nós reduzimos a solução de para a determinação da matriz W. O Algoritmo de Lanczos usa a independência linear dos vetores coluna para encontrar a matriz W.

Seja $S = \{v_1, v_2,..., v_r\}$ conjunto não vazio de vetores do espaço vetorial E.

(i) Diz-se que S é linearmente independente se satisfaz a condição: Para quaisquer $k_1, k_2,..., k_r \in K$,

$$k_1v_1 + k_2v_2 +... + k_rv_r = 0 \Rightarrow k_1 = k_2 = ... = k_n = 0.$$

(ii) Diz-se que S é linearmente dependente, caso contrário.

3.3 Discussão

Com esse estudo vimos que a fatoração de números inteiros grandes é bem complexa, necessitando de um estudo aprofundado dos aspectos matemáticos envolvidos em seu contexto.

Esse trabalho mostrou-nos o quão importante é o QS e que a documentação dos conhecimentos adquiridos é muito importante, principalmente para estudos futuros.

4. Conclusão

Apesar de ser um método relativamente novo, o Crivo Quadrático muito importante, necessitando de estudos e aperfeiçoamento. Nesse sentido esse trabalho apresentou um estudo detalhado de uma das etapas do método em questão, que consiste na obtenção de um quadrado perfeito.

Para trabalhos futuros sugere-se a implementação desse estudo, para resultados práticos.

5. Agradecimentos

Agradecemos à Universidade Estadual de Mato Grosso do Sul pela concessão da bolsa de auxilio financeiro que nos possibilitou uma maior dedicação às atividades desenvolvidas em torno da pesquisa e também a todos acadêmicos, professores e técnicos, que contribuíram para a realização dessa pesquisa.

6. Referências

6.1 Livros

CLÁUDIO M. D; MARINS J. M. **Cálculo Numérico Computacional;** São Paulo: Atlas; 2ª Edição; 1994.

CRANDALL, R.; Pomerance, C. **Prime Numbers- A Computational Perspective**; New York: Springer-Verlag: 1ª Edição; 2002. p. 227-242.

LIMA, Elon Lages. **Álgebra Linear**; Instituto de Matemática Pura e Aplicada, Rio de Janeiro: CNPQ; 4ª Ed; 2000.

POMERANCE, C. **The Quadratic Sieve Factoring Algorithm**; New York: Springer-Verlag, Ed. T. Beth, N. Cot, and I. Ingemarsson; 1985. p. 13.

6.2 Teses

SOUZA, B. A. de. **Teoria dos Números e o RSA**. Dissertação de Mestrado, Universidade Estadual de Campinas; 2004**.** Disponível em: <http://www.ime.unicamp.br/~mdc/teses/plinio/bianca.pdf> (último acesso em 03/06/2011).

6.3 Sites

ASBRINK, O., BRYNIELSSON, J. **Factoring large integers using parallel Quadratic Sieve**; 2000. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/versions?doi=10.1.1.96.3685& version=0> (último acesso em 15/07/2011).

BUCHMANN, J. MULLER, V. **Algorithms for Fatoring Integers**; Technische Hochschule Darmstadt Institut für theoretische Informatik; 2005. <http://www.cdc.informatik.tudarmstadt.de/ ~buchmann/Lecture%20Notes/Algorithms%20for%20factoring%20integers.pdf> (ultimo acesso em 25/07/2011).

LANDQUIST, E. **The Quadratic Sieve Factoring Algorithm**; 2001. Disponível em: <http://www.cs.virginia.edu/crab/QFS_Simple.pdf> (último acesso em 15/07/2011).

SANCHES, A. de P. MOLGORA, A. B. de P. **Implementação do Método de Fatoração de Inteiros Crivo Quadrático**; Universidade Estadual de Mato Grosso do Sul. 2010. Disponível em: <https://www.periodicos.uems.br/index.php/enic/article/view/2089/749> (último acesso em 09/07/2011).