CRIVO QUADRÁTICO: UM ESTUDO DA OBTENÇÃO DE UM CONJUNTO DE NÚMEROS COMPLETAMENTE FATORADOS SOBRE UMA BASE DE FATORES

Alex Zanella Zaccaron[1]; Adriana Betânia de Paula Molgora[2]

[1]Estudante do Curso de Ciência da Computação da UEMS, Unidade Universitária de Dourados; E-mail: alex_zaccaron@hotmail.com. Bolsista PIBIC/UEMS.

[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 estudo da fatoração de inteiros é extremamente importante por estar diretamente relacionado com a segurança de sistemas criptográficos, como o RSA. O Crivo Quadrático é um dos métodos de fatoração mais importantes da atualidade. Esse trabalho tem como objetivo o estudo de uma das etapas desse método de fatoração que consiste em determinar um conjunto de números que possam ser completamente fatorados sobre uma base de fatores. Esse estudo foi produzido por meio de pesquisas bibliográficas, através das quais apresentou-se um detalhamento da etapa do funcionamento do método especificado.

Palavras-chave: Criptografia. Fatoração. Número Primos.

1. Introdução

O problema de fatoração de números inteiros está entre os mais antigos problemas matemáticos abordados pela humanidade e, até o momento, não foi possível desenvolver um método que fatore qualquer número inteiro dado. Um dos métodos de fatoração de inteiros mais importantes é o do Crivo Quadrático.

Pode-se dizer que a fatoração através do método Crivo Quadrático é desenvolvida em duas etapas principais. A primeira etapa consiste na obtenção de um conjunto de números que possam ser completamente fatorados sobre uma base de fatores. A segunda etapa está relacionada com a determinação de um produto de números obtidos na primeira etapa que seja um quadrado perfeito.

Este projeto tem como objetivo realizar um estudo aprofundado da primeira etapa do método Crivo Quadrático.

2. Materiais e Métodos

Para o alcance do objetivo proposto, o trabalho foi distribuído em 3 fases sendo elas:

1ª Estudo detalhado dos fundamentos matemáticos relacionados com a primeira etapa do processo de fatoração do Crivo Quadrático, através de pesquisa bibliográfica.

2ª Estudo dos algoritmos existentes que possibilitem os cálculos requeridos na primeira etapa do método Crivo Quadrático, por meio de pesquisa bibliográfica.

3ª Documentação dos estudos realizados e resultados obtidos durante a execução do projeto, visando publicação na área de trabalho.

3. Resultados e Discussão

Para um melhor entendimento dos resultados obtidos com esse trabalho, essa seção apresenta alguns conceitos fundamentais buscados em Miles (2006), Ruggiero (1996), Crandall e Pomerance (2005), Coutinho (2000), Antunes (2002).

3.1 Números Primos

Seja um número $p > 1$ pertencente ao conjunto das naturais, p é dito um primo se os seus únicos divisores forem 1 e p. Se p não for primo, é dito composto e pode ser fatorado como um produto $p = r \cdot s$, $r \neq 1$ e $s \neq 1$. Todo número natural $n > 1$ pode ser fatorado como $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m$, onde $p_1, p_2, \ldots, p_m$ são números primos. Exemplo: $90 = 2 \cdot 3 \cdot 3 \cdot 5$. À medida que o número cresce, a probabilidade dele ser um primo diminui. A probabilidade de um inteiro positivo n ser um primo é de aproximadamente $1/\ln(n)$.

3.2 Encontrando os números primos

Um dos mais eficientes meios de achar todos os números primos pequenos, por exemplo, os menores que 10.000.000, é usando o Crivo de Erastótenes. Basta fazer uma lista com todos os inteiros maiores que um e menores ou igual a n e riscar os múltiplos de todos os primos menores ou igual à n. Os números que não estiverem riscados são os números primos.

Para determinar, por exemplo, os primos menores ou iguais a 10:

Inicialmente faz-se a lista dos inteiros de 2 a 10: {1, 2,…, 10}. O número 2 é primo. Vamos mantê-lo e eliminar todos os seus múltiplos. Desta forma, obtemos: {2, 3, 5, 7, 9}. O próximo número "livre" é o 3, outro primo. Vamos mantê-lo e eliminar seus múltiplos: {2, 3, 5, 7}. Como não há mais múltiplos do número 5 e do número 7, obtemos o conjunto final com todos os primos menores ou iguais a 10: {2, 3, 5, 7}.

3.3 Congruências

Tomando a, b e c números inteiros e $c > 0$, a é côngruo a b, módulo c, se $c|(a-b)$.

Notação: $a \equiv b(mod\ c)$

Exemplo: $3 \equiv 21(mod\ 6)$; $6|(3-21)$; $6|-18$, portanto 3 é côngruo a 21, modulo 6.

3.4 Resíduo Quadrático

Um inteiro a é dito resíduo quadrático módulo m se a congruência: $x^2 \equiv a(mod\ m)$tiver solução, caso contrário, dizemos que a é um resíduo não quadrático modulo m.

Exemplo: $4^2 \equiv 2(mod\ 7)$; $7|(16-2)$, então 2 é um resíduo quadrático módulo 7.

3.5 Símbolo de Legendre

Seja p um primo ímpar e x um inteiro não divisível por p, o Símbolo de Legendre é definido como:

$$\left(\frac{x}{p}\right)\begin{cases} 1, \text{se } x \text{ é um resíduo quadrático de } p. \\ -1, \text{se } x \text{ não é um resíduo quadrático de } p. \end{cases}$$

Exemplo: $\left(\frac{2}{7}\right) = \left(\frac{3}{7}\right) = 1$, pois $x^2 \equiv 2(mod\ 7)$ e $x^2 \equiv 3(mod\ 7)$ têm solução.

3.6 Crivo Quadrático: Primeira Etapa

De acordo com Crandall e Pomerance (2005), 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 $x^2 \equiv y^2(mod\ n)$, então tem-se que $(x+y)\cdot(x-y) \equiv 0(mod\ n)$. Logo, $\frac{n}{(x^2-y^2)} = (x+y)\cdot(x-y)$ e os números $d = mdc(x+y, n)$ e $f = mdc(x-y, n)$ poderão ser fatores não triviais de n. Ou seja, a idéia básica do método consiste em encontrar congruências da forma $x_i^2 \equiv y_i(mod\ n)$, onde $\prod y_i = y^2$ é um quadrado perfeito. Se $x = \prod x_i$, então $x^2 \equiv y^2(mod\ n)$. Na prática, para encontrar x e y, a primeira etapa do método consiste em encontrar uma base de fatores, que é um conjunto de números primos, e, em seguida determinar um conjunto de números completamente fatorados sobre uma base de fatores.

3.6.1 Determinando a Base de fatores

A base de fatores, segundo Pomerance (1985), é formada por numero primos tais que $p_i \leq B$, onde B é o limite dado, e para cada primo p, o número n deve ser resíduo quadrático módulo p. Ou seja, serão considerados os números primos menores que B tais que:

$$n^{(p-1)/2}(mod\ p) = 1 \quad \leftrightarrow \quad \left(\frac{n}{p}\right) = 1 \text{ (Símbolo de Legendre)}$$

Exemplo: Seja n = 10186 o número a ser fatorado, e 3 o primo a ser verificado se pertence a base de fatores:

$10186^1(mod\ 3) = 1$, portanto 3 é incluído na base de fatores. Caso contrário, 3 seria descartado e o próximo primo seria examinado, assim sucessivamente, até $p_i \leq B$.

De acordo com Crandall e Pomerance (2005), o valor para o limite B é calculado a partir de experimentação, não há uma fórmula exata. Se dois valores de B tiverem resultados similares,

obviamente é vantajoso escolher o menor. A seguinte fórmula $B = \left(e^{\sqrt{\ln(n)\cdot\ln(\ln(n))}}\right)^{1/2}$ pode encontrar o valor aproximado de *B*.

Segundo Landquist (2001), a fórmula $B = \left(e^{\sqrt{\ln(n)\cdot\ln(\ln(n))}}\right)^{\sqrt{2}/4}$ também pode encontrar o valor aproximado de *B*.

3.6.2 Determinando os *f(xᵢ)'s*

Depois de encontrada a base de fatores, Crandall e Pomerance (2005), afirmam que, deve-se agora determinar os $f(x_i)$'s que sejam completamente fatorados pela base de fatores por meio da expressão: $f(x_i) = x_i^2 - n$, onde *n* é o número a ser fatorado e x_i são números próximos de $\lfloor\sqrt{n}\rfloor$. É aconselhável que o número -1 esteja contido na base de fatores, mesmo não sendo um número primo, para o caso de algum $f(x_i) < 0$. O intervalo ideal é determinado por meio de experimentação, tal como o tamanho da base e fatores. A fórmula $M = B^2 = e^{\sqrt{\ln(n)\cdot\ln(\ln(n))}}$ pode determinar o valor aproximado de *M*.

Onde 2M = quantidade de x_i's.

De acordo com Landquist (2001), a fórmula $M = \left(e^{\sqrt{\ln(n)\cdot\ln(\ln(n))}}\right)^{3\sqrt{2}/4}$ também pode encontrar o valor aproximado de *M*.

Exemplo: Dado *n* = 9487 $\lfloor\sqrt{n}\rfloor = 97$

Suponha que tomamos *M* = 23, ou seja, $80 < x_i < 105$, portanto são: 81, 82,…, 104.

Ao obter os x_i's, são determinados os $f(x_i)$'s completamente fatorados pela base de fatores. Para $x_i = 81$: $f(81) = 81^2 - 9487 = -2926 = (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$.

Se $p_1, p_2, \ldots, p_n$ estão contidos na base de fatores, então $f(81)$ pode ser utilizado como $f(x_i)$. Repetindo o processo até, no caso, $f(104)$.

3.7 Crivo Quadrático com Múltiplos Polinômios – MPQS

Segundo Crandall e Pomerance (2005), no método básico Crivo Quadrático busca-se valores x_i's como inteiros próximos à n, procurando por valores $x^2 - n$ que são completamente fatorados pela base de fatores. A razão pela qual toma-se *x* próximo à n é reduzir o tamanho de $x^2 - n$, uma vez que, números menores são mais fáceis de serem fatorados. O método MPQS (Crivo Quadrático com Múltiplos Polinômios) é uma variação do método do Crivo Quadrático que utiliza uma família de polinômios ao invés de somente o polinômio $x^2 - n$. Considere *a*, *b* e *c* valores inteiros com $b^2 - ac = n$ e o polinômio $f(x) = ax^2 + 2bx + c$. Então:

$$af(x) = a^2x^2 + 2abx + ac = (ax + b)^2 - n,$$

de modo que: $(ax + b)^2 \equiv af(x)(mod\ n)$.

Para determinar o conjunto de números completamente fatorados pela base de fatores, Crandall e Pomerance (2005), afirmam que, toma-se o coeficiente *b*, satisfazendo a condição $|b| < a/2$. O maior valor de $f(x)$ no intervalo $[-M, M]$ é de aproximadamente $(a^2 \cdot M^2 - n)\ /a$, portanto $a \approx \sqrt{2n/M}$. Se *a* satisfaz tal aproximação, o valor absoluto de $f(x)$ no intervalo $[-M, M]$ é limitado por $M\sqrt{n}/\sqrt{2}$. Comparando com o polinômio original, $x^2 - n$, usado no método básico crivo quadrático, no intervalo $[\sqrt{n} - M, \sqrt{n} + M]$ os valores tem limite de aproximadamente $2M\sqrt{n}$. O valor de *c* pode ser definido como $c = (b^{2-n})/a$. Pode-se escolher $M = B = L(n)^{1/2}$ quando usa-se múltiplos polinômios, e $M = B^2 = L(n)$ (seção 3.6.2) quando usa-se somente um polinômio onde $L(n) = e^{\sqrt{\ln(n) \cdot \ln(\ln(n))}}$.

Para poder escolher os valores de *b* e *c*, precisamos encontrar um valor para *a*. Uma maneira eficiente seria tomando primos $p \approx (2n)^{1/4}/M^{1/2}$, com $\left(\frac{n}{p}\right) = 1$ e escolhendo $a = p^2$.

3.7.1 Crivo Quadrático: Self Initialization – SIQS

Quando são fatorados números grandes pelo método MPQS, de acordo com Crandall e Pomerance (2005), a troca de polinômios acaba tendo um alto custo e faz com que o método perca eficiência. Uma maneira mais eficiente de realizar essa troca é apresentada a seguir.

Para os valores de *a*, *b*, *c* e cada primo *p* que está contido na base de fatores com $\left(\frac{n}{p}\right) = 1$, é necessário resolver a congruência: $ax^2 + 2bx + c \equiv 0(mod\ p)$.

Tal congruência possui duas soluções $r(p)$ e $s(p)$:

$r(p) = (-b + t(p)a^{-1} mod\ p)$ e $s(p) = (-b - t(p)a^{-1} mod\ p)$ onde: $t(p) \equiv n(mod\ p)$.

O mesmo resíduo *t*(*p*) é utilizado para cada $r(p)$ e $s(p)$ calculado, dessa maneira, o principal gasto para calcular $r(p)$ e $s(p)$ é encontrando $a^{-1} mod\ p$ para cada primo p e as duas multiplicações $mod\ p$. O mesmo valor de a é utilizado nos vários polinômios, amortizando o gasto do cálculo de $r(p)$ e $s(p)$. Essa é a principal idéia do SIQS.

Crandall e Pomerance (2005) salientam que, para cada valor de *a*, é escolhido *b*, tal que $b^2 \equiv n(mod\ a)$ com $0 < b < a/2$, e $c = (b^2 - n)/a$. Assim, tem-se um polinômio $ax^2 + 2bx + c$. Para cada valor de *a*, (assumindo *a* primo), tem-se 2^{k-1} escolhas para *b*, onde *k* é a quantidade de fatores primos $p|a$ com $\left(\frac{n}{p}\right) = 1$. Dessa maneira, se $a = p^2$, usado no MPQS,

temos somente um valor para b, então, tomamos o valor de a como: $a = p_1, p_2, \dots, p_n$, onde os p's são primos distintos pertencentes à base e fatores, obtendo vários valores para b.

4. Resultados e Discussão

O desenvolvimento do trabalho transcorreu como o previsto. Foram realizados diversos estudos, contribuindo para a aquisição de conhecimentos sobre o método especificado.

Alguns exemplos numéricos sobre o método não foram apresentados devido à complexidade dos cálculos que demandam implementações sobre a etapa do método estudado, o que não fazia parte do objetivo principal desse trabalho.

5. Agradecimentos

À Universidade Estadual de Mato Grosso do Sul pela concessão da bolsa .

À professora Adriana Betânia de Paula Molgora pela paciência na orientação e incentivo.

6. Conclusão

A fatoração é um problema matemático muito importante na atualidade por estar diretamente relacionado com a segurança de sistemas criptografados, como o RSA.

Esse trabalho apresentou um estudo teórico da primeira etapa do método Crivo Quadrático. Para trabalhos futuros sugere-se a implementação desse estudo realizado a fim de se estudar os resultados práticos do mesmo.

REFERÊNCIAS

ANTUNES, Cristiane. Métodos de Fatoração de Números Inteiros. 2002. 75 f. Dissertação (Mestrado em Matemática Aplicada) – Instituto de Matemática, Universidade Federal do Rio Grande do Sul, Porto Alegre. 2002.

COUTINHO, S.C. Números Inteiros e Criptografia RSA. IMPA-SBM, 2000.

CRANDALL, R.; POMENRANCE, C. Prime Numbers: A Computational Perspective, 2nd ed. New York: Springer-Verlag, 2005.

LANDQUIST, Eric. The Quadratic Sieve Factoring Algorithm. 2001.

MILIES, César Polcino; COELHO, Sônia Pitta. Números: Uma Introdução a Matemática. São Paulo: Editora da Universidade de São Paulo, 2006.

POMERANCE, Carl. The quadratic sieve factoring algorithm. Berlin: Springer-Verlag, 1985.

RUGGIERO, Márcia A. Gomes; LOPES, Vera Lúcia da Rocha. Cálculo Numérico: Aspectos Teóricos e Computacionais. 2. ed. São Paulo: MAKRON Books, 1996.