

ESTUDO DAS ALTERNATIVAS DE IMPLEMENTAÇÃO DO MÉTODO DE FATORAÇÃO DE INTEIROS CRIVO QUADRÁTICO

Daniel de Souza Guilhermitti (Bolsista UEMS), Adriana Betânia de Paula Molgora
Universidade Estadual de Mato Grosso do Sul
Cidade Universitária de Dourados - Caixa postal 351 - CEP: 79804-970
thuruco@hotmail.com abmol@terra.com.br

Resumo. *Criptografia é a ciência que estuda métodos para codificar e decodificar mensagens. O uso desta é imprescindível quando se deseja privacidade e segurança na troca de informações. O problema de fatoração de números inteiros está entre os mais antigos problemas matemáticos e, até o momento, não se conhece nenhum método que realize a fatoração de qualquer número inteiro. Isso tem motivado diversos estudos através dos quais foram desenvolvidos alguns métodos de fatoração. Dentre esses está o método Crivo Quadrático. Este trabalho apresenta uma descrição deste método de fatoração e alguns algoritmos que podem ser utilizados em uma futura implementação.*

Palavras-chave: *Criptografia. Resíduo Quadrático. Crivo.*

Abstract: *Cryptography is the science which studies methods to encode and decode messages. Use of this is essential when you want privacy and security in information exchange. The problem of factorization of integers is among the oldest mathematical problems and, by the time we do not know any method to carry out the factorization of any integer number. This has motivated several studies of which were developed some methods of factorization. Among these is the Quadratic Sieve method that was studied. This paper presents a description of this method of factorization and some algorithms that can be used in a future implementation.*

Keywords: *Cryptography. Quadratic residues. Sieve.*

1. Introdução

Criptografia é a ciência que estuda métodos para codificar e decodificar mensagens. O uso desta é imprescindível quando se deseja privacidade e segurança na troca de informações. Um dos sistemas criptográficos mais utilizados atualmente é o RSA, cuja segurança baseia-se

na dificuldade de fatoração de números grandes.

O problema de fatoração de números inteiros está entre os mais antigos problemas matemáticos abordados pela humanidade e, até o momento não se conhece nenhum método que realize a fatoração de qualquer número inteiro. Isso tem motivado diversos estudos através dos quais foram desenvolvidos alguns métodos de fatoração. Dentre esses está o método Crivo Quadrático (*Quadratic Sieve*), devido a Pomerance [2].

Um estudo prático do método de fatoração Crivo Quadrático depende primeiramente de um estudo teórico dos fundamentos matemáticos envolvidos em seu funcionamento, bem como de um estudo de algoritmos que podem ser aplicados em sua implementação.

Este trabalho tem como objetivo apresentar um estudo teórico de algoritmos que podem ser utilizados em uma implementação do método Crivo Quadrático, disponibilizando conhecimentos sobre esse método de fatoração a fim de possibilitar estudos mais avançados sobre o mesmo.

2. Metodologia

Durante o desenvolvimento desse trabalho, foram realizadas pesquisas bibliográficas em:

- Livros da Biblioteca Central da Universidade;
- Documentos eletrônicos como e-books, artigos e demais textos de domínio público, obtidos principalmente Internet;
- Artigos e projetos finais de curso relacionados com a área de pesquisa;
- Fóruns e listas de discussão da área estudada.

3. Resultados

3.1 Crivo Quadrático

O algoritmo Crivo Quadrático é um moderno método utilizado para fatoração de números inteiros. Atualmente é o segundo método mais rápido conhecido, ficando atrás apenas do poderoso Number Field Sieve (NFS)[1]. Porém, o método Crivo Quadrático é ainda o mais rápido para números inteiros de até 140 dígitos decimais. O tempo de execução desse método de fatoração depende unicamente do tamanho do número inteiro a ser fatorado.

O Crivo Quadrático pode ser usado em conjunto com o método de Dixon [4] para fatoração números grandes. Para o entendimento do método Crivo Quadrático é necessário o entendimento dos aspectos matemáticos envolvidos em seu funcionamento. A seguir, são apresentados alguns desses conceitos matemáticos, bem como os algoritmos que podem ser utilizados em uma implementação desse método de fatoração.

3.2 Resíduo Quadrático

Seja o conjunto Zp^* , onde p é um número primo maior que 2 e $a \in Zp^*$. Dizemos que a é um resíduo quadrático módulo p se:

$$b^2 \equiv a \pmod{p} \text{ para algum } b \in Zp^*$$

Exemplo:

Tomamos como exemplo o conjunto Z_{11}^* e os quadrados dos cinco primeiros elementos do conjunto, a seguir:

$$1^2 \equiv 1 \pmod{11}$$

$$2^2 \equiv 4 \pmod{11}$$

$$3^2 \equiv 9 \pmod{11}$$

$$4^2 \equiv 16 \equiv 5 \pmod{11}$$

$$5^2 \equiv 25 \equiv 3 \pmod{11}$$

Lema 1.1: Dado um número primo $p > 2$, exatamente metade dos elementos de Zp^* são resíduos quadráticos.

3.3 Símbolo de Legendre:

Adrien-Marie Legendre (1752-1833) introduziu um símbolo para exprimir o carácter quadrático de um inteiro com respeito a um primo [3].

Definição: Seja p um inteiro primo ímpar. Para um inteiro a , definimos o símbolo de Legendre por:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p|a, \\ 1 & \text{se } a \text{ é um quadrático modulo } p, \\ -1 & \text{se } a \text{ não é um residuo quadrático modulo } p. \end{cases}$$

O símbolo de Legendre pode ser calculado utilizando o critério de Euler, enunciado a seguir.

(Critério de Euler) Seja p um primo. Então

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

Em particular, para um primo ímpar p temos que -1 é resíduo quadrático módulo p se, e somente se, $p \equiv 1 \pmod{4}$.

Do critério de Euler, também segue que o símbolo de Legendre é multiplicativo:

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

3.4 Método de Euclides

Sejam $a, b \in \mathbb{Z}_p$ com $a, b \neq 0$. O máximo divisor comum de a e b , denotado por $\text{mdc}(a, b)$ é o maior inteiro c que divide ambos a e b .

O cálculo do mdc pode ser realizado através dos seguintes passos:

- 1) Divide-se a por b encontrando o resto r_1 ;
- 2) Se $r_1 \neq 0$, divide-se b por r_1 encontrando o resto r_2 ;
- 3) Se $r_2 \neq 0$, divide-se r_1 por r_2 encontrando o resto r_3 . E assim por diante. Esse processo é repetido até que se encontre o último resto igual a zero, e então o $\text{mdc}(a, b)$ será o último resto diferente de zero.

Exemplo:

Sejam $a=858$ e $b=253$. Utilizando o algoritmo euclidiano, o mdc entre a e b é obtido calculando-se:

$$858=3 \times 253+99$$

$$253=2 \times 99+55$$

$$99=1 \times 55+44$$

$$55=1 \times 44+11$$

$$44=4 \times 11$$

Portanto o $\text{mdc}(858, 253)=11$.

3.5 Eliminação Gaussiana

Em álgebra linear, a eliminação gaussiana é um algoritmo que visa transformar uma matriz arbitrária numa matriz triangular equivalente através de operações elementares (trocas de linhas e adições de múltiplos de certas linhas a outras linhas).

A eliminação gaussiana consiste em realizar $n-1$ eliminações (onde n é o número de linhas da matriz), usando do procedimento abaixo:

$$l_i = l_i - \left(\frac{a_{ik}}{a_{kk}}\right) l_k$$

$$i = k + 1, k + 2, \dots, n$$

$$k = 1, 2, \dots, n - 1$$

Exemplo:

Seja A a matriz dada por $\begin{bmatrix} 2 & 3 & -1 \\ 4 & 4 & -3 \\ 2 & -3 & 1 \end{bmatrix}$. Realizando-se o cálculo de $l_i = l_i - \left(\frac{a_{ik}}{a_{kk}}\right) l_k$ nas

linhas 2 e 3 obtém-se $\begin{bmatrix} 2 & 3 & -1 \\ 0 & -2 & -1 \\ 2 & -6 & 2 \end{bmatrix}$. Realizando-se novamente o cálculo de $l_i = l_i - \left(\frac{a_{ik}}{a_{kk}}\right) l_k$

na linha 3, obtém-se $\begin{bmatrix} 2 & 3 & -1 \\ 0 & -2 & -1 \\ 0 & 0 & 5 \end{bmatrix}$, que é uma matriz triangular equivalente à matriz A.

3.6 Funcionamento do método Crivo Quadrático

Nessa seção vamos descrever o funcionamento do método Crivo Quadrático explicando como encontrar um divisor próprio de um inteiro composto n . De modo geral, podemos aplicar este algoritmo recursivamente para fatorar completamente um inteiro n .

Para fatorar n , o método procura dois inteiros x e y tais que

$$x^2 \equiv y^2 \pmod{n} \text{ e } x \text{ não é } \equiv \pm y \pmod{n}.$$

Isto implica que n é um divisor de $x^2 - y^2 = (x + y)(x - y)$ mas não é divisor de $(x - y)$ nem de $(x + y)$. Logo, $g = (x - y, n)$ é um divisor próprio de n , que pode ser facilmente calculado através do algoritmo de *Euclides*.

Exemplo:

Sejam $n = 7429, x = 227, y = 210$.

Então: $x^2 - y^2 = n, x - y = 17$ e $x + y = 437$.

Portanto, $g = (x - y, n) = 17$ é um divisor próprio de n

A idéia de procurar inteiros x e y também é usada por outros algoritmos tais como “Number Field Sieve”. Mas os algoritmos diferem no modo de descobrir os inteiros x e y .

O método *Crivo Quadrático* encontra os inteiros x e y da seguinte maneira:

Seja $m = \lfloor \sqrt{n} \rfloor$ e $f(X) = (X + m)^2 - n$. Primeiro calculamos $f(X_i)$ e escolhemos somente os números X_i para os quais $f(X_i)$ só tem fatores primos pequenos. Dentre a família de congruências $(X_i + m)^2 \equiv f(X_i) \pmod{n}$,

Escolheremos um subconjunto $\{X_i\}_{i=1\dots n}$ para o qual o produto dos $f(X_i)$ é um quadrado perfeito, ou seja, os expoentes dos fatores primos de $\prod f(X_i)$ são pares.

Exemplo:

Se $n = 7429$, então $m = \lfloor \sqrt{n} \rfloor = 86$ e $f(X) = (X + 86)^2 - 7429$.

Temos:

$$f(-3) = 83^2 - 7429 = -540 = -1 \cdot 2^2 \cdot 3^2 \cdot 5$$

$$f(1) = 87^2 - 7429 = 140 = 2^2 \cdot 5 \cdot 7$$

Isto implica que

$$83^2 \equiv -1 \cdot 2^2 \cdot 3^2 \cdot 5 \pmod{7429}$$

$$87^2 \equiv 3^2 \cdot 5 \cdot 7 \pmod{7429}$$

$$88^2 \equiv 3^2 \cdot 5 \cdot 7 \pmod{7429}.$$

Se multiplicarmos as duas últimas congruências, obtemos:

$$(87.88)^2 \equiv (2.3.5.7)^2 \pmod{n}.$$

Encontramos os inteiros $x = 227 \equiv 87.88 \pmod{n}$ e $y = 210 \equiv 2.3.5.7 \pmod{n}$.

Nesse exemplo foi fácil encontrar as congruências a multiplicar, No entanto se n é demasiadamente grande, é preciso considerar mais fatores primos e mais congruências. Como é que podemos selecionar tais congruências apropriadas?

O processo é uma aplicação da Álgebra Linear. Primeiro escolhemos um inteiro positivo L .

Devemos procurar somente os inteiros X tais que $f(X)$ só tem fatores primos que pertencem a base de fatores

$$F(L) = \{p \mid p \leq L \text{ e } p \text{ primo}\} \cup \{-1\}.$$

A seguir, apresentaremos alguns parâmetros que podem ser utilizados para a base de fatores:

Na tabela temos a base de fatores a considerar:

Dígitos decimais de n	50	60	70	80	90	100	110	120
Base de fatores (x100)	3	4	7	15	30	51	120	245

Tamanho da base de fatores e do intervalo de crivação

Depois de encontrar tantos elementos X quanto o número de elementos da base de fatores, resolvemos o sistema linear correspondente em Z_2 . Este sistema é resolvido, por exemplo, utilizando a eliminação de *Gauss*.

Exemplo 3:

Vamos exemplificar o método geral de seleção de congruências para o exemplo 2. Podemos escolher de entre três congruências. O processo de seleção é controlado pelos coeficientes $\lambda_i \in \{0,1\}, 1 \leq i \leq 3$. A congruência i é escolhida somente se $\lambda_i = 1$. O produto das congruências escolhidas pode ser expresso como:

$$(-1 \cdot 2^2 \cdot 3^3 \cdot 5)^{\lambda_1} \cdot (2^2 \cdot 5 \cdot 7)^{\lambda_2} \cdot (3^2 \cdot 5 \cdot 7)^{\lambda_3}$$

$$= (-1)^{\lambda_1} \cdot 2^{2\lambda_1+2\lambda_2} \cdot 3^{3\lambda_1+2\lambda_3} \cdot 5^{\lambda_1+\lambda_2+\lambda_3} \cdot 7^{\lambda_2+\lambda_3}.$$

Queremos que este número seja um quadrado, ou seja, que os expoentes de todos os elementos da base de fatores sejam pares. Logo, basta resolver o seguinte sistema:

$$\begin{cases} \lambda_1 & \equiv 0 \pmod{2} \\ 2\lambda_1 + 2\lambda_2 & \equiv 0 \pmod{2} \\ 3\lambda_1 + 2\lambda_3 & \equiv 0 \pmod{2} \\ \lambda_1 + \lambda_2 + \lambda_3 & \equiv 0 \pmod{2} \\ \lambda_2 + \lambda_3 & \equiv 0 \pmod{2} \end{cases}$$

Como o sistema tem solução $\lambda_1 = 0$, $\lambda_2 = 1$. Escolheremos a segunda e terceira congruências.

Para concluir a descrição de método, falta mostrar como encontrar objetos X_i tal que $f(X_i)$ só tem fatores primos que pertencem à base de fatores $F(L)$, para um inteiro L fixo.

Uma possibilidade é calcular $f(X)$ para $X = 0, \pm 1, \pm 2, \pm 3 \dots$, e testar se cada $f(X)$ só tem fatores primos que pertencem à base de fatores. Para cada $f(X)$ temos efetuar divisões por todos os elementos da base de fatores.

A complexidade desse método de fatoração é da ordem de $\exp(\sqrt{\ln n \ln n})$ Ou seja, o tempo de execução desse método depende do tamanho do número a ser fatorado.

A seguir é apresentado um exemplo de fatoração pelo método Crivo Quadrático.

Exemplo: Seja $n= 87463$ o número a ser fatorado.

É necessário seguir alguns passos para a fatoração de n :

1-Encontrar uma base de fatores;

2-Executar o crivo de Eratóstenes para encontrar números que podem ser fatorados sobre a base de fatores criadas com o passo 1;

3-Usar eliminação gaussiana para encontrar um produto de números determinados no passo 2 que é um quadrado perfeito.

Para encontrar uma base de fatores, considerar os seguintes valores de $\left(\frac{n}{p}\right)$:

p	2	3	5	7	13	17	19	23	29	31	37
$\left(\frac{n}{p}\right)$:	1	1	-1	-1	-1	1	1	1	-1	1	-1

Assim determina-se o a base de fatores = (2,3,13,17,19,29)

As soluções para $x^2 \equiv (\text{mod } p)$ são:

p	2	3	13	17	19	29
x	1	1,2	5,8	7,10	5,14	12,17

Agora iniciaremos a peneiração utilizando números próximos de $\lfloor \sqrt{n} \rfloor = 295$;

Os valores de x para os quais $F = x^2 - n$ divide completamente são:

x	-1	2	3	13	17	19	29
265	1	1	1	0	1	0	0
278	0	0	0	0	1	0	0
269	0	1	1	0	1	1	0
307	0	1	0	1	0	0	1
316	0	0	0	0	1	0	0

Disposmos os números em uma matriz transposta e resolvemos $av = 0$;

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \cdot v = 0;$$

Através dessa matriz será realizada uma eliminação gaussiana a fim de se encontrar uma combinação de F^7 s que é um quadrado perfeito.

Uma solução seria:

$$V = (1,1,1,0,1,0)$$

Assim toma-se o 1^a, 2^a, 3^a e 4^a valores de x e obtém-se:

$$X = 265.278.296.307 = 6694540240 \equiv 34757 \pmod{n}$$

$$Y = \sqrt{((265^2 - n) \times (278^2 - n) \times (296^2 - n) \times (307^2 - n))} = 2.9^2 \cdot 13.17.29 = 13497354 \equiv 28052 \pmod{n}$$

Com isso:

$$MDC(x - y, n) = 149;$$

$$MDC(x + y, n) = 587$$

Que resulta na fatoração de n , ($149 * 587 = 8746$)

Algoritmo Crivo Quadrático (pseudocódigo):

[Início]

$$B = \lceil \ln^{1/2} \rceil;$$

$$\text{Marque } p_1 = 2 \text{ e } a_1 = 1;$$

Ache os primos impares $p \leq B$ onde $\left(\frac{n}{p}\right) = 1$ e marque em $p_2 \dots p_k$;

Para $(2 \leq i \leq K)$ ache raizes $\pm a_i$ com $a_i^2 \equiv n \pmod{p_i}$

Encontrando a raiz

Encontre um inteiro aleatório $t \in [0, p - 1]$ tal que $\left(\frac{t^2 - a}{p}\right) = -1$;

Encontre a raiz quadrada entre $F_{p^2} = F_p(\sqrt{t^2 - a})$

$$x = (t + \sqrt{t^2 - a})^{(p+1)/2};$$

retorne x ;

[Peneirando]

Peneire a sequencia $(x^2 - n), x$

$= [\sqrt{n}], [\sqrt{n}] + 1 \dots$ para valores de B até K

$+ 1$, tais variaveis serão coletadas em um conjunto S ;

[Algebra linear]

Para $((x^2, x^2 - n) \in S \{$

Estabeleça a fatoraçoão do primo $x^2 - n = \prod_{i=1}^k p_i^{e_i}$;

$\vec{v}(x^2 - n) = (e_1, e_2, \dots, e_k); \}$ Vetor expoente

A forma de $(K + 1)$

da matrix com linhas sendo vetores variaveis reduzido a $(\text{mod } 2)$;

Use os algoritmos existentes de algebra linear para achar um

subconjunto não trivial das filas da matrix que some com

$$0 - \text{vetor(mod } 2) \text{ supondo } \vec{v}(x_1) + \vec{v}(x_2) + \dots + \vec{v}(x_k) = \vec{0};$$

$$x = x_1 x_2 \dots x_k \pmod{n}; y = \sqrt{(x_1^2 - n)(x_2^2 - n) \dots (x_k^2 - n)};$$

Deduzimos esta raiz diretamente da fatoração do primo encontrado no quadrado perfeito $(x_1^2 - n)(x_2^2 - n) \dots (x_k^2 - n)$;

$$d = \text{gcd}(x - y, n);$$

retorne d;

[Fim algoritmo].

3.7 Aspectos computacionais

Das várias linguagens de programação existentes para a implementação de algoritmos, a linguagem C/C++ tem se mostrado muito eficiente e pode ser utilizada na implementação do método Crivo Quadrático.

Para a realização de cálculos com números acima de 100 dígitos decimais é necessário a utilização de uma biblioteca matemática, como por exemplo a biblioteca GMP[6], escrita em C.

Essa biblioteca é direcionada principalmente para aplicações criptográficas, sistemas algébricos e pesquisas em álgebra computacional.

4-Discussão:

A realização dessa pesquisa foi muito relevante para a aquisição de novos conhecimentos na área de fatoração de inteiros.

Esses conhecimentos, disponibilizados através desse trabalho, poderão servir como base para um estudo prático do método Crivo Quadrático, a partir da realização de uma implementação desse método de fatoração.

Agradecimentos

Os autores agradecem à Universidade Estadual de Mato Grosso do Sul pelo apoio financeiro concedido. Os agradecimentos se estendem a todos familiares e amigos que, direta ou indiretamente, contribuíram para a realização desse trabalho.

Referências

[5] CRANDALL R. e C. Pomerance, **Prime Numbers** – A computational perspective, Springer-Verlag, 2002.

[6] GMP: **The GNU Multiple Precision Arithmetic Library**. Disponível em: <http://gmplib.org> <<Acessado em: 15/08/09.

[1] LENSTRA A. K. e W. H. Lenstra, M. S. Manasse e J. M. Pollard, **The Number Field Sieve**, Abstratic em “Proc.22nd Ann. ACM Syrup. On Theory of Computing (STOC)”, 1990.

[2] POMERANCE C., **The Quadratic Sieve Factoring Algorithm**, em “EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques” Springer-Verlag, New York, 1985.

[4] **QUADRATIC SIEVE**. http://en.wikipedia.org/wiki/Quadratic_sieve << Acessado em: 15 de abril de 2009.

[3]**Reciprocidade Quadrática**. Disponível: http://erdos.ime.usp.br/index.php/Reciprocidade_Quadr%C3%A1tica. << Acessado em: 25 de março de 2009.