# Um estudo do método de fatoração de inteiros Crivo Quadrático

**Aline de Paula Sanches**
Universidade Estadual de Mato Grosso do Sul, Ciência da Computação
79804-970, Dourados, MS
E-mail: Aline_paula_sanches@hotmail.com

**Adriana Betânia de Paula Molgora**
Universidade Estadual de Mato Grosso do Sul, Ciência da Computação
79804-970, Dourados, MS
E-mail: abmol@terra.com.br

## RESUMO

O problema de fatoração de números inteiros tem ocupado lugar de destaque na Teoria dos Números. Tal interesse deve-se ao fato de que um método eficiente de fatoração pode comprometer a segurança de sistemas criptográficos de chave pública, como o RSA. Um dos métodos de fatoração mais importantes já desenvolvidos é o Crivo Quadrático [2]. O entendimento do método Crivo Quadrático depende de um estudo dos diversos conceitos matemáticos envolvidos em seu funcionamento. Esse trabalho tem como objetivo apresentar uma descrição concisa desse método de fatoração, como segue.

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 $x^2 \equiv y^2 (\mathrm{mod}\, n)$, então tem-se que $(x+y)\cdot(x-y) \equiv 0(\mathrm{mod}\, n)$. Logo, $n \mid (x^2 - y^2) = (x+y)\cdot(x-y)$ 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 $x_i^{\,2} \equiv y_i (\mathrm{mod}\, n)$, onde $\prod y_i = y^2$ é um quadrado perfeito. Se $x = \prod x_i$, então $x^2 \equiv y^2 (\mathrm{mod}\, n)$.

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, por exemplo, o conjunto $\{-1, 2, p_2, ..., p_k\}$, tal que $p_i \le B$, para um certo limite $B$ e, para cada primo $p$, o número $n$ deve ser um resíduo quadrático módulo $p$. A seguir, são calculados números $f(x_i)$'s dados por $f(x_i) = x_i^{\,2} - n$ para $x_i$ próximo de $\sqrt{n}$. Usando o Crivo de Eratóstenes [1], devem-se determinar $x_i$'s suficientes para os quais $f(x_i)$ pode ser completamente fatorado pela base de fatores. A quantidade desses $f(x_i)$'s deve ser maior do que o número de primos menores do que $B$. Armazenando os $f(x_i)$'s, em um vetor na base binária, utiliza-se a adição de vetores para descobrir uma combinação linear que produz um vetor nulo que corresponderá a um quadrado perfeito. Então $x$ será dado pelo produto dos $x_i$'s correspondentes módulo $n$ e $y$ será dado pela raiz do produto dos fatores dos $f(x_i)$'s correspondentes. Em seguida é calculado $d = mdc(x+y, n)$. Se $d$ é fator não trivial de $n$, então um fator foi encontrado e, para determinar o segundo fator basta calcular a divisão de $n$ por $d$.

Para um melhor entendimento do funcionamento do método Crivo Quadrático, tome como exemplo o número $n$ = 9487. É evidente que para a obtenção da base de fatores deve-se estabelecer em primeiro lugar o limite $B$. Existem diferentes abordagens para a resolução desse

problema, no entanto, essa escolha consiste mais em arte do que em ciência pois, em geral, o esse valor é obtido de forma empírica [1], baseada em experimentação. Nesse exemplo, considere $B = 30$. Então verifica-se para cada primo $p$ menor do que 30, se $n$ é resíduo quadrático modulo $p$. Esse verificação pode ser realizada através do teste de Euler [1], calculando-se $n^{(p-1)/2} \bmod p$. Se o resultado for 1, tem-se que $n$ é resíduo quadrático modulo $p$. Caso contrário, o número primo deve ser descartado.Assim, a base de fatores será dada por {-1, 2, 3,7,11,13,17,19,29}.

Depois de obtida a base de fatores, são calculados os $f(x_i)$'s completamente fatorados pela base de fatores para $x_i$ próximo de $\sqrt{9487}$. Por exemplo, considerando $x_i = 98$, tem-se $f(98) = 98^2 - 9487 = 117 = 3^2 \times 13$, isto é, 117 é completamente fatorado pela base de fatores. Em seguida, para cada $f(x_i)$ encontrado é associado um vetor de 9 dígitos binários, cada coluna correspondendo a um dos primos da base. Se o número for negativo o primeiro dígito será 1, caso contrário será 0. Se o primo correspondente tem potência par, então o dígito será 0, caso contrário será 1. A seguir são apresentados exemplos de $x_i$'s, $f(x_i)$'s e seus dígitos binários correspondentes.

| $x_i$ | $f(x_i)$ | -1 | 2 | 3 | 7 | 11 | 13 | 17 | 19 | 29 |
|---|---|---|---|---|---|---|---|---|---|---|
| 81 | -2926 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 84 | -2431 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 85 | -2262 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 89 | -1566 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 95 | -462 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 97 | -78 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 98 | 117 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 100 | 513 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 101 | 714 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 103 | 1122 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |

Calculando v(81)+v(95)+v(100) obtém-se o vetor <0,0,0,0,0,0,0,0,0>, que corresponde ao quadrado perfeito $(81 \times 95 \times 100)^2 = (2 \times 3^2 \times 7 \times 11 \times 19)^2 \bmod 9487$. Então $x = 81 \times 95 \times 100 (\bmod 9487) \equiv 1053$ e $y = 2 \times 3^2 \times 7 \times 11 \times 19 (\bmod 9487) = 7360$. Calculando $d = mdc(1053 + 7360, 9487) = 179$, obtém-se um fator não trivial de $n$. O segundo fator é dado por $9487 \div 179 = 53$.

É notável que o entendimento completo do método Crivo Quadrático não é uma tarefa trivial. É necessário um estudo mais detalhado sobre alguns conceitos matemáticos como, por exemplo, o conceito resíduo quadrático e a obtenção do limite $B$ utilizado na base de fatores. Para uma melhor compreensão desse método, informações adicionais podem ser encontradas em [1, 2].

**Palavras-chave**: *Fatoração de inteiros, Crivo Quadrático.*

**Referências**

[1] R. Crandall e C. Pomerance, "Prime Numbers – A Computational Perspective", Springer-Verlag, New York, 2002.

[2] C. Pomerance, The Quadratic Sieve Factoring Algorithm, em EUROCRYPT 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, Springer-Verlag, New York, 1985.