O Algoritmo de Fatoração GNFS

Pedro Carlos da Silva Lara* **Fábio Borges de Oliveira**
Coordenação de Sistemas e Redes, CSR, LNCC,
25651–075, Petrópolis, RJ
E-mail: {pcslara,borges}@lncc.br

RESUMO

Em 1988, J. Pollard [3] introduziu um método para fatorar inteiros da forma x^3+k, o NFS (*Number Field Sieve*). Este método foi estendido para atuar em números da forma r^e+s com r e $|s|$ naturais relativamente pequenos. Este algoritmo é conhecido como SNFS (*Special Number Field Sieve*) [2]. O GNFS (*General Number Field Sieve*) [1] ficou sendo a modificação do NFS para trabalhar em qualquer inteiro, não tendo nenhuma restrição. Este resumo apresenta um estudo teórico do GNFS onde foram feitas implementações para o entendimento do funcionamento matemático do algoritmo. O GNFS usa o método de Dixon para fatorar, ou seja, busca inteiros x, y tais que, $x \not\equiv \pm y \pmod n$ e $x^2 \equiv y^2 \pmod n$, onde n é o inteiro ímpar que se deseja fatorar. Então $n|(x+y)(x-y)$ logo temos um probabilidade de $\frac{1}{2}$ que $\mathrm{mdc}(n, x-y)$ e $\mathrm{mdc}(n, x+y)$ seja um fator não trivial de n. Para tanto primeiro procuramos por um polinômio mônico com coeficientes coprimos entre si: $f \in \mathbb{Z}[x]$ e um inteiro m tais que $f(m) \equiv 0 \pmod n$. Considere também a raiz $\theta \in \mathbb{C}$ ($\mathbb{C}$ denotará o corpo dos números complexos) de f. A obtenção de θ nos permite construir um anel $\mathbb{Z}[\theta]$ cujos elementos são da forma $\mathbb{Z}[\theta] = \{\delta : \delta = a_{d-1}\theta^{d-1} + a_{d-2}\theta^{d-2} + \ldots + a_0\}$, com $a_j \in \mathbb{Z}$ e d o grau de f. Neste momento iremos definir um homomorfismo $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}_n$ satisfazendo $\phi(\theta) \equiv m \pmod n$. Em outras palavras, $\phi : \sum a_j\theta_i^j \to \sum a_j m^j$. Finalmente, considere um conjunto não vazio $S \subset \{(a,b) \in \mathbb{Z}^2 : \mathrm{mdc}(a,b) = 1\}$. Com estas preliminares podemos definir a principal idéia do algoritmo GNFS: procurar por dois quadrados $\beta^2 \in \mathbb{Z}[\theta]$ e $y^2 \in \mathbb{Z}$ tais que

$$x^2 = (\phi(\beta))^2 \equiv \phi(\beta^2) \equiv \phi(\textstyle\prod_{(a,b)\in S}(a-b\theta)) \equiv$$
$$\equiv \prod_{(a,b)\in S}(a-bm) = y^2 \pmod n.$$

Se considerarmos $x = \phi(\beta)$ e $y = \sqrt{\prod_{(a,b)\in S}(a-bm)}$, encontramos os inteiros que precisávamos. Em suma, este algoritmo é eficiente se encontrarmos, em um tempo razoável, o conjunto S de pares de inteiros (a,b), tais que

$$\prod_{(a,b)\in S}(a-b\theta) \text{ é um quadrado em } \mathbb{Z}[\theta],$$

$$\prod_{(a,b)\in S}(a-bm) \text{ é um quadrado em } \mathbb{Z}.$$

O GNFS é considerado um dos melhores existentes na atualidade para encontrar fatores grandes (mais de 30 dígitos decimais). Possui tempo de execução $O(\exp(c + o(1))\sqrt[3]{(\ln n)(\ln\ln n)^2})$, onde c é uma constante e n é o inteiro ímpar que se pretende fatorar.

Referências

[1] J. P. Buhler, H. W. Lenstra, and C. Pomerance, *Factoring integers with the number field sieve*, 1992.

[2] Arjen K. Lenstra, Hendrik W. Lenstra Jr., Mark S. Manasse, and J. M. Pollard, *The number field sieve*, ACM Symposium on Theory of Computing, 1990, pp. 564–572.

[3] J. M. Pollard, *Factoring with cubic integers*, manuscript, 1988, pp. 4–10.

*Bolsista de iniciação científica PIBIC/CNPq