Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 12, n. 1, 2026.

Trabalho apresentado no XLIV CNMAC, Fundação Getulio Vargas - Rio de Janeiro - RJ, 2025.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Análise Assintótica de Abordagens Propostas para a Resolução de Sistemas de Congruências Lineares

Ana Carla Q. Rosa[1], Fernando C. G. Manso[2], Wellington J. Corrêa[3]
Universidade Tecnológica Federal do Paraná (UTFPR), Campo Mourão, PR

A Teoria dos Números é um ramo da Matemática que estuda as propriedades e relações entre os números inteiros [2], com aplicações significativas em Ciência da Computação, como a cifração e decifração de blocos do algoritmo criptográfico RSA. Nesse contexto, as congruências lineares desempenham um papel crucial, especialmente na resolução de sistemas de equações modulares. O Teorema Chinês do Resto (TCR) é uma ferramenta para a resolução de tais sistemas, mas sua eficiência computacional varia conforme a implementação.

A análise assintótica provê ferramentas e técnicas matemáticas para analisar o desempenho de algoritmos [1]. Desse modo, pode-se determinar se uma implementação computacional oferece uma solução correta em tempo viável de execução conforme o crescimento do tamanho da entrada. Este trabalho propõe uma análise assintótica de diferentes abordagens para a resolução de sistemas de congruências lineares, com foco na otimização do tempo de execução.

Uma congruência linear é uma equação da forma $ax \equiv b \pmod{m}$, onde x é a incógnita. Para resolver sistemas de congruências lineares, o TCR é amplamente utilizado. De acordo com esse teorema, se os módulos $m_1, m_2, \ldots, m_n$ são coprimos, o sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}, \tag{1}$$

tem uma solução única módulo $M = m_1 \cdot m_2 \cdot \cdots \cdot m_n$. O Algoritmo Estendido de Euclides, que expressa o Máximo Divisor Comum (MDC) entre dois números inteiros como uma combinação linear desses mesmos números, por meio da Relação de Bézout, permite o cálculo dos inversos modulares no TCR, necessários para a resolução das congruências modulares.

Em [4], propomos uma abordagem para o Algoritmo Estendido de Euclides. O custo assintótico dessa implementação é $O(\log(\min(a, b)))$, o mesmo da versão tradicional, como apresentado em [1], mas com uma estrutura que facilita a integração com o TCR.

O TCR clássico exige que os módulos sejam coprimos e possui um custo assintótico de $\Theta(n^2)$, onde n é o número de equações do sistema. No entanto, em muitos casos, os módulos não são coprimos, o que limita a aplicabilidade do TCR tradicional. Em [3], apresentamos uma implementação que elimina a necessidade de verificação de módulos coprimos, reduzindo o custo assintótico para $O(n \cdot \log(\min(a, b)))$.

Em síntese, a abordagem proposta utiliza uma conjectura que verifica se o MDC dos módulos divide a diferença entre os resíduos das congruências. Se essa condição for satisfeita, o sistema tem solução, e o algoritmo retorna uma solução válida. Para exemplificar, considere o sistema

[1] anacarlaquallio@gmail.com
[2] fmanso@utfpr.edu.br
[3] wcorrea@professores.utfpr.edu.br

$$\begin{cases} mx & \equiv a \pmod{b} \\ nx & \equiv c \pmod{d} \end{cases}. \tag{2}$$

De acordo com a implementação proposta, caso m seja diferente de 1, é preciso encontrar o inverso multiplicativo de m em relação a b, ou seja, $m^{-1} \pmod{b}$. O mesmo vale para n, no caso $n^{-1} \pmod{d}$. Em seguida, deve-se multiplicar as equações pelos seus respectivos inversos, de forma que se tenha $1x$. Assim, pode-se utilizar a equação:

$$x = \left[(b^{-1} \pmod{d}) \cdot b \cdot (c-a) + a\right] \pm b \cdot d \cdot j \cdot \gamma, \text{ em que } j = \text{mdc}(b,d). \tag{3}$$

No caso em que $j = 1$, o algoritmo funciona da mesma forma que o TCR tradicional. Para um sistema com módulos não coprimos, o método sugerido retorna solução se e somente se o MDC entre b e d divide $(c-a)$.

Diante desse cenário, a análise assintótica dos algoritmos propostos revela que o Algoritmo Estendido de Euclides, tanto na versão tradicional quanto na modificada, possui custo $O(\log(\min(a,b)))$, dominado pelo cálculo do MDC. Já a implementação clássica do TCR tem custo $\Theta(n^2)$, devido à necessidade de verificar a coprimalidade dos módulos e calcular inversos modulares para cada equação. A nova implementação reduz o custo para $O(n \cdot \log(\min(a,b)))$, eliminando a verificação de coprimalidade e simplificando o cálculo dos inversos modulares.

Os resultados demonstram que a abordagem proposta é mais eficiente que o TCR clássico, especialmente para sistemas com um grande número de equações. A conjectura introduzida permite que o algoritmo lide com módulos não coprimos, ampliando sua aplicabilidade. Além disso, a combinação do Algoritmo Estendido de Euclides modificado com o TCR proposto oferece uma solução mais eficiente para a resolução de sistemas de congruências lineares, com aplicações potenciais em criptografia, processamento de sinais e outras áreas da computação. A implementação desses algoritmos está disponível em um repositório do GitHub[4].

Agradecimentos

Agradecemos à Fundação Araucária pelo fomento financeiro (Edital UTFPR-PROPPG n.º 02/2023 — PIBIC).

Referências

[1] T. H. Cormen, C. E. Leiserson, R. L. Rivest e C. Stein. **Introduction To Algorithms**. 2a. ed. MIT Press, 2001. ISBN: 0262032937.

[2] G. H. Hardy, E. M. Wright, D. R. Heath-Brown e J. Silverman. **An Introduction to the Theory of Numbers**. 6a. ed. USA: OUP Oxford, 2008. ISBN: 9780199219865.

[3] A. C. Q. Rosa, F. C. G. Manso e W. J. Corrêa. "Uma abordagem matemática para a otimização do custo computacional do Teorema Chinês do Resto". Em: **Anais da XI Bienal da Matemática**. UFSCar, São Carlos, SP, 2024.

[4] A. C. Q. Rosa, F. C. G. Manso e W. J. Corrêa. "Uma nova perspectiva para o Algoritmo de Euclides: Uma abordagem computacional para o cálculo dos coeficientes da Relação de Bézout". Em: **Anais do XIII Seminário de Extensão e Inovação e XXVIII Seminário de Iniciação Científica e Tecnológica da UTFPR**. UTFPR, Ponta Grossa, PR, 2023.

[4] Disponível em: `https://github.com/anacarlaquallio/IC`. Acesso em 09 mar. 2024.