UFSCar
UTFPR UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ CAMPUS CAMPO MOURÃO
XI Bienal de Matemática 2024
Universidade Federal de São Carlos - UFSCar
29 de julho a 02 de agosto de 2024

Uma abordagem matemática para a otimização do custo computacional do Teorema Chinês do Resto

Rosa, Ana Carla Quallio[1]; Manso, Fernando Cézar Gonçalves[2] e Corrêa, Wellington José[3]

Resumo: *Este trabalho tem como objetivo apresentar uma abordagem matemática para otimizar o custo computacional do Teorema Chinês do Resto. Enquanto o algoritmo tradicional considera apenas módulos coprimos, resultando em um custo de $\Theta(n^2)$, o método proposto, que contempla uma conjectura para módulos não coprimos, possui um custo de $O(n \cdot \log(\min(a,b)))$. Essa abordagem representa uma significativa melhoria de eficiência no contexto da Ciência da Computação.*

Palavras-chave: *Algoritmo, Custo Computacional, Teorema Chinês do Resto.*

1. Introdução

A Teoria dos Números é um ramo da Matemática que visa, primordialmente, entender as propriedades e relações entre os números. Na área de Teoria Elementar, há o estudo de congruências lineares (HARDY *et. al.*, 2008). O termo *congruência* significa "de mesma medida", desse modo, dizemos que dois números são *congruentes módulo m* quando deixam o mesmo resto na divisão por m.

Na computação, a congruência tem diversas aplicações, como a cifração e decifração de blocos do algoritmo criptográfico RSA. Para a resolução de um sistema de congruências, utiliza-se o Teorema Chinês do Resto. Em muitos contextos, torna-se necessário o uso de algoritmos computacionais para encontrar uma solução mais rapidamente. A análise assintótica, diante desse cenário, provê ferramentas para determinar o custo de implementações computacionais (CORMEN *et. al.*, 2001), possibilitando otimizações no tempo de execução.

O Teorema Chinês do Resto tradicional possui um custo assintótico de $\Theta(n^2)$. Este trabalho propõe um algoritmo mais eficiente com custo de $O(n \cdot \log(\min(a,b)))$. Essa otimização é alcançada ao considerar a possibilidade dos módulos não serem coprimos, por meio da introdução de uma conjectura.

2. O Teorema Chinês do Resto

O Teorema Chinês do Resto tradicional é um método que resolve sistemas de congruências lineares dois a dois da forma:

$$\begin{aligned} x &\equiv A_1 \pmod{m_1} \\ &\vdots \\ x &\equiv A_n \pmod{m_n} \end{aligned}$$

Em que $m_1, m_2, \ldots, m_n$ são coprimos. A Figura 2 ilustra uma possível forma de determinar uma solução para um sistema de equações por meio do Teorema Chinês do Resto.

A	M	$\overline{M}$	$\overline{M^{-1}}$	$\mathrm{A} \cdot \mathrm{M} \cdot \overline{M^{-1}}$
A_1	M_1	$\overline{M_1}$	$\overline{M_1^{-1}}$	$\mathrm{A}_1 \cdot \mathrm{M}_1 \cdot \overline{M_1^{-1}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
A_n	M_n	$\overline{M_n}$	$\overline{M_n^{-1}}$	$\mathrm{A}_n \cdot \mathrm{M}_n \cdot \overline{M_n^{-1}}$

Fig. 2: Possibilidade de aplicação do Teorema Chinês do Resto

No qual M é o produto de $m_1, m_2, \ldots, m_n$ excluindo a linha correspondente; $\overline{M}$ é a classe de equivalência de M em relação ao módulo da linha atual e $\overline{M^{-1}}$ é o inverso de $\overline{M}$. No algoritmo proposto, também são resolvidas equações de dois a dois. Para exemplificar, considere o sistema:

$$\begin{aligned} mx &\equiv a \pmod{b} \\ nx &\equiv c \pmod{d} \end{aligned}$$

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:

$$x = \left[b^{-1} \pmod{d} \cdot b \cdot (c-a) + a\right] \pm b \cdot d \cdot j \cdot \gamma$$

Em que $j = \mathrm{mdc}(b,d)$. No caso em que $j = 1$, o algoritmo funciona da mesma forma que o Teorema Chinês do Resto. Para um sistema com módulos não coprimos, o método sugerido retorna solução se e somente se o Máximo Divisor Comum entre b e d divide $(c-a)$.

Para a demonstração, assuma que $\mathrm{mdc}(b,d)$ divide $c-a$. Isso significa que $c \equiv a \pmod{(\mathrm{mdc}(b,d))}$. Caso o sistema tenha solução, é possível afirmar, pela definição de congruência, que:

1) $x - a = bk$;
2) $x - c = dk'$;
3) $a + bk = c + dk' \iff a - c = dk' - bk$.

Dessa igualdade conclui-se que $\mathrm{mdc}(d,b)$ divide $a-c$, e portanto $c-a$, uma vez que divide $dk' - bk$. Isso conclui a prova. Outro ponto a ser detalhado é que, ao aplicar o algoritmo, obtém-se um conjunto de possibilidades que satisfazem o sistema de congruências lineares, em função de γ. A fim de tornar mais claro, considere como exemplo o seguinte sistema:

$$\begin{aligned} x &\equiv 5 \pmod{6} \\ x &\equiv 19 \pmod{20} \end{aligned}$$

Note que $\mathrm{mdc}(6,20) = 2$, porém o sistema possui solução. Para a resolução, considere $j = \mathrm{mdc}(b,d)$ e divida os números b e d por j, reescrevendo o sistema para:

$$\begin{aligned} x &\equiv 5 \pmod{3} \\ x &\equiv 19 \pmod{10} \end{aligned}$$

Resolvendo o sistema, então tem-se:

$$\begin{aligned} x &= \left[3^{-1} \pmod{10} \cdot 3 \cdot (19-5) + 5\right] \pm 3 \cdot 10 \cdot 2 \cdot \gamma \\ x &= [7 \cdot 3 \cdot 14 + 5] \pm 60\gamma \\ x &= 299 \pm 60\gamma \\ x &= 59 \pm 60\gamma \end{aligned}$$

Portanto, a solução que satisfaz o conjunto de equações é $x \equiv 59 \pmod{60}$.

3. Custo computacional

O estudo assintótico, de acordo com Cormen *et. al.* (2001), descreve o tempo de execução de um algoritmo em função do tamanho de entrada n, expresso em três notações principais:

- Notação O: indica um limite assintótico superior. Pela definição, $O(g(n)) = \{f(n)$: existem constantes positivas c e n_0 tais que $0 \leq f(n) \leq c \cdot g(n)$ para todo $n \geq n_0\}$.
- Notação Ω: indica um limite assintótico inferior. Pela definição, $\Omega(g(n)) = \{f(n)$: existem constantes positivas c e n_0 tais que $0 \leq c \cdot g(n) \leq f(n)$ para todo $n \geq n_0\}$.
- Notação Θ: limita assintoticamente uma função acima e abaixo. Pela definição, $\Theta(g(n)) = \{f(n)$: existem constantes positivas c_1, c_2 e n_0 tais que $0 \leq c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$ para todo $n \geq n_0\}$.

No caso do Teorema Chinês do Resto Tradicional, o custo $O(n^2)$ é justificado pelo fato de que, como mostrado na Figura 2, cada linha e coluna precisam ser percorridas, resultando em um custo quadrático.

Por outro lado, a abordagem proposta dispensa a verificação de módulos coprimos, uma vez que propõe uma conjectura para o algoritmo. Isso representa uma otimização ao eliminar uma etapa do processo. O custo $O(n \cdot \log(\min(a,b)))$ é alcançado devido à utilização do Algoritmo Estendido de Euclides para calcular inversos, conforme demonstrado por Cormen *et. al.* (2001) com um custo de $O(\log(\min(a,b)))$, além de percorrer as n equações do sistema. A Figura 3 ilustra o pseudocódigo dessa nova abordagem.

```
def TEOREMA_CHINES_N(m, n, a, b, c, d): #Custo assintotico de O(log(min(a,b)))
    if m == 0 or n == 0: return 0, 0 #Teta(1)
    if m != 1:
        m, a, b = SIMPLIFICA(m, a, b) #O(log(min(a,b)))
        if a == -1: return 0, 0
    if n != 1:
        n, c, d = SIMPLIFICA(n, c, d) #O(log(min(a,b)))
        if c == -1: return 0, 0
    i = INVERSO(b, d) #O(log(min(a,b)))
    x = (i * b * (c - a) + a) #Teta(1)
    gama = b * d * mdc #Teta(1)
    if x < 0: x = gama + x #Teta(1)
    return x % gama, gama
```

Fig. 3: Representação da nova abordagem para o Teorema Chinês do Resto

4. Considerações

Este trabalho apresentou uma abordagem matemática para otimizar computacionalmente o Teorema Chinês do Resto. Diante da proposição da conjectura, os testes realizados com a implementação computacional retornaram soluções corretas para sistemas com módulos não coprimos.

Referências

[1] CORMEN, T.H. et. al. **Introduction To Algorithms**. MIT Press, 2001.

[2] HARDY, G.H. et. al. **An Introduction to the Theory of Numbers**. Oxford: OUP Oxford, 2008.

[1]Afiliação: Universidade Tecnológica Federal do Paraná. Este autor foi apoiado pela Fundação Araucária.
[2]Afiliação: Universidade Tecnológica Federal do Paraná.
[3]Afiliação: Universidade Tecnológica Federal do Paraná.

Apoios:
CAPES CNPq FAPESP INCTMat ARAUCÁRIA