ALGORITMOS DE TEORIA DOS NÚMEROS

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

RESUMO: A Teoria dos Números é um ramo da Matemática que visa, primordialmente, entender as propriedades e relações entre os números. Conceitos como divisibilidade, máximo divisor comum e primalidade são aplicados na Ciência da Computação, principalmente em Criptografia e Criptoanálise. Este trabalho desenvolveu um conjunto de materiais abrangendo esses tópicos para facilitar o estudo da Teoria dos Números. Primeiramente, foram implementados algoritmos da literatura, na linguagem de programação Python, que abordam propriedades básicas dos números, como a divisibilidade, testes de primalidade, Função Totiente de Euler, números triangulares e resíduos quadráticos. Estes algoritmos estão disponíveis em um repositório do GitHub. Em segundo lugar, buscou-se explorar e apresentar diferentes abordagens para a resolução de sistemas de congruências lineares, com ênfase na implementação do Teorema Chinês do Resto. Dessarte, examinou-se o Algoritmo Estendido de Euclides, destacando a influência do custo computacional no cálculo do Máximo Divisor Comum. Em seguida, analisou-se o Teorema Chinês do Resto como uma possibilidade para solucionar sistemas de congruências lineares. Evidenciou-se que a implementação clássica desse teorema possui um custo assintótico quadrático, enquanto o método proposto neste artigo demonstra um limite linear multiplicado por uma função logarítmica. Isso se deve à inclusão de uma etapa adicional de complexidade no processo, envolvendo a verificação de módulos coprimos. Por fim, como produto educacional, foi desenvolvido um site com doze postagens sobre tópicos de Teoria dos Números, visando apresentar conceitos fundamentais de maneira acessível ao leitor. Ademais, o site disponibiliza os materiais produzidos, com pontuações sobre cada temática estudada. Esses produtos mostram-se salutar, uma vez que provêm formas distintas de disseminação do conhecimento matemático.

Palavras-chave: Algoritmos. Custo computacional. Teoria dos Números.

1 INTRODUÇÃO

A Teoria dos Números é um campo da Matemática que tem como objetivo investigar as propriedades dos números inteiros (HARDY et al., 2008). Em resumo, são três principais ramos em que se divide tal área: a Teoria Algébrica, abordando álgebra e números complexos; a Teoria Analítica, com foco na análise real e complexa e, por fim, a Teoria Elementar, a qual busca validar e comprovar conceitos relacionados aos números inteiros.

Dentro da Teoria Elementar, há o estudo de tópicos como divisibilidade, primalidade, equivalência modular e congruências. Apesar de serem poucos explorados na matemática pura, esses conceitos são muito importantes para diversos assuntos da Computação (CORMEN et al., 2001). Primeiramente, a divisibilidade revela-se como uma base subjacente para a fatoração de números inteiros com diversos algarismos — tarefa crítica para a segurança da criptografia moderna.

[1] Acadêmica de Ciência da Computação; anacarlarosa@alunos.utfpr.edu.br.
[2] Docente do Departamento de Matemática; wcorrea@professores.utfpr.edu.br.
[3] Docente do Departamento de Química; fmanso@utfpr.edu.br.

A primalidade, por sua vez, fornece alicerces para os testes utilizados na verificação de números primos em métodos como o RSA e a criação de Tabelas de Hash. Por fim, as noções de equivalência modular e congruências garantem que mensagens permaneçam íntegras durante o processo de codificação e decodificação. Nesse sentido, ao explorar o desenvolvimento de algoritmos de Teoria dos Números, pode-se estudar o potencial de aplicações já existentes.

Este trabalho tem como objetivo apresentar um conjunto de materiais desenvolvidos sobre Teoria dos Números. Em primeiro lugar, tem-se a implementação de algoritmos tradicionais encontrados na literatura. Em segundo lugar, propõe-se uma abordagem para o cálculo dos coeficientes do Algoritmo Estendido de Euclides. Em terceiro lugar, sugere-se uma otimização do custo computacional do Teorema Chinês do Resto. A seleção desses algoritmos se deu diante das inúmeras aplicações no âmbito da Ciência da Computação, principalmente em Criptografia, como a geração de chaves do sistema RSA. Por fim, foi desenvolvido um site que reúne doze publicações abordando diferentes tópicos de Teoria dos Números, contribuindo para a disseminação do conhecimento matemático.

2 METODOLOGIA

Esta seção apresenta os métodos adotados para cada material desenvolvido nesta pesquisa.

2.1 Implementação de algoritmos tradicionais

Em relação aos algoritmos tradicionais, foram escolhidos os seguintes tópicos para a implementação computacional na linguagem de programação *Python*:

- Algoritmo Estendido de Euclides: apresenta a versão tradicional do algoritmo e a abordagem proposta;
- Divisibilidade: enfoque na definição de dois números serem divisíveis entre si, números primos e Função Totiente de Euler;
- Números Triangulares: verifica se um número é triangular e retorna a visualização desse número;
- Resíduos Quadráticos: testa se um número é resíduo quadrático em relação a um número primo;
- RSA: fornece a implementação desse algoritmo com base nas bibliotecas Cryptography e Pycryptodome;
- Teorema Chinês do Resto: explora a versão tradicional do algoritmo e a abordagem proposta.

2.2 Algoritmo Estendido de Euclides

O Algoritmo de Euclides consiste em um método de divisões sucessivas utilizado para determinar o Máximo Divisor Comum (MDC) entre dois inteiros. A sua versão estendida, conhecida como Algoritmo Estendido de Euclides, baseia-se na Relação de Bézout, a qual estabelece que o MDC entre dois números pode ser representado como uma combinação linear desses mesmos números.

Em (ROSA; MANSO; CORRÊA, 2023), propomos uma nova perspectiva para o Algoritmo Estendido de Euclides, de modo a determinar os coeficientes da Relação de Bézout em um conjunto de iterações. Primeiramente, é preciso calcular o Máximo Divisor Comum com base na Figura 1.

		q_0	q_1	$\cdots$	q_{n-1}	q_n	q_{n+1}
$\frac{a}{r_n}$	$\frac{b}{r_n}$	$\frac{r_0}{r_n}$	$\frac{r_1}{r_n}$	$\cdots$	$\frac{r_{n-1}}{r_n}$	$\frac{r_n}{r_n}$	0

Figura 1 – Elementos do Máximo Divisor Comum no método desenvolvido

O segundo passo consiste em verificar se a posição n é um número par ou ímpar, a fim de iniciar um conjunto de iterações para o cálculo de alfa, uma variável que é utilizada para determinar os coeficientes x e y.

Caso n seja par, temos que $i = \frac{n}{2}$, senão $i = \frac{n-1}{2}$. Assim, inicia-se as iterações com $\alpha_0 = 1$ até

$$\alpha_i = \frac{\alpha_{i-1} \cdot r_{[}n-k] - q_{[}n-l]}{r_{[}n-l]}$$

Inicialmente, caso n seja par, temos que $(k,l) = (2,0)$. Senão, $(k,l) = (3,1)$. A cada iteração, essas variáveis são incrementadas: $k = k+2$ e $l = l+2$. Por fim, obtêm-se os coeficientes y e x, sendo eles dados por:

$$y = \frac{\alpha_i \cdot \frac{a}{r_n} - q_0}{\frac{r_0}{r_n}} \quad \text{e} \quad x = \frac{y \cdot \frac{b}{r_n} - 1}{-\frac{a}{r_n}}$$

Desse modo, implementou-se computacionalmente o método desenvolvido, na linguagem de programação Python, a fim de verificar a corretude dos cálculos diante de diferentes possibilidades para a função MDC.

2.3 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 versão tradicional possui um custo assintótico de $\Theta(n^2)$. Em (ROSA; MANSO; CORRÊA, 2024), abordamos 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. 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 $j = \text{mdc}(b,d)$. 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 $(c-a)$.

2.4 Site e materiais

O site foi desenvolvido com o objetivo de explorar tópicos de Teoria dos Números de forma mais acessível à comunidade não acadêmica. Ao longo de seis meses, foram publicadas doze matérias que abrangem desde conceitos fundamentais de divisibilidade até aplicações, como o algoritmo RSA. Além disso, foram disponibilizadas 162 páginas de slides sobre esses conceitos.

3 RESULTADOS E DISCUSSÃO

O primeiro resultado corresponde à disponibilização dos algoritmos tradicionais implementados, que podem ser verificados no GitHub[1]. O repositório está organizado de acordo com os tópicos descritos, e a documentação fornece informações sobre a execução dos algoritmos.

Em seguida, temos que a abordagem proposta para o Algoritmo Estendido de Euclides apresenta o mesmo custo assintótico da versão tradicional, que é $O(\log(\min(a,b)))$. A Figura 2 ilustra o pseudocódigo do método.

[1] Disponível em: https://github.com/anacarlaguallio/IC. Acesso em: 20 set. 2024.

```
def MDC_ESTENDIDO(a, b): #Custo assintotico de O(log(min(a,b)))
    resto_i, quociente_i = MDC(a,b)  # O(log(min(a,b)))
    resto_i, quociente_i = DIVISAO(resto_i, quociente_i) #O(log(min(a,b)))
    n = len(resto_i) - 1 #Teta(1)
    alfa[0] = 1 #Teta(1)

    if n % 2 == 0: #Trecho com custo de Teta(1)
        i = n / 2
    else:
        i = (n - 1)/2

    for j in range(1, i): # Trecho com custo de O(log(min(a,b)))
        alfa[j] = (alfa[j - 1] * resto_i[0]/ resto_i[n] - quociente_i[2]) / (
    resto_i[2]/resto_i[n])

    y = (alfa[i] * a/ resto_i[n] - quociente_i[0] ) / (resto_i[0]/ resto_i[n]) #
    Teta(1)
    x = (y * b/ resto_i[n] - 1) / -(a/resto[n]) #Teta(1)
    return x, y
```

Figura 2 – Pseudocódigo do método apresentado

Acerca do Teorema Chinês do Resto, a versão tradicional possui um custo computacional de $\theta(n^2)$. 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, com um custo de $O(\log(\min(a,b)))$, além de percorrer as n equações do sistema. A Figura 3 ilustra o pseudocódigo da abordagem proposta.

```
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
```

Figura 3 – Representação da nova abordagem para o Teorema Chinês do Resto

Por fim, em relação ao site, as publicações desenvolvidas incluem: “O que é Teoria dos Números?”; “Algoritmo Estendido de Euclides”; “Noções Elementares e Tabela Hash”; “Introdução à Aritmética Modular”; “Grupos e Subgrupos”; “Teoria dos Grupos e Grupos Modulares”; “Introdução às Equações Lineares Modulares”; “Teorema Chinês do Resto”; “Teoremas Importantes da Teoria dos Números”;

"Noções de Criptografia e Algoritmo RSA"; e "Introdução às Funções Aritméticas". Todos os materiais estão disponíveis[2].

4 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo apresentar um conjunto de materiais desenvolvidos sobre Teoria dos Números. Primeiramente, foram introduzidos os algoritmos tradicionais implementados. Posteriormente, propusemos novas abordagens, incluindo um método para o Algoritmo Estendido de Euclides, mantendo o mesmo custo computacional da versão clássica, e uma otimização do Teorema Chinês do Resto, aplicado à resolução de sistemas de congruências lineares. A análise revelou que a versão tradicional possui um custo assintótico de $\Theta(n^2)$, enquanto o algoritmo desenvolvido atinge um limite de $O(n \cdot \log(\min(a,b)))$. Por fim, o site apresenta um conjunto de materiais, contribuindo para a disseminação do conhecimento matemático. A contínua exploração da Teoria dos Números não apenas alimenta o avanço do conhecimento, mas também fornece ferramentas essenciais para resolver problemas complexos que moldam a sociedade moderna.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Fundação Araucária — Brasil (Edital UTFPR/-PROPPG n.o 02/2023 — PIBIC).

REFERÊNCIAS

CORMEN, T.H. et al. **Introduction To Algorithms**. [S.l.]: MIT Press, 2001. (Mit Electrical Engineering and Computer Science). ISBN 9780262032933. Disponível em: .

HARDY, G.H. et al. **An Introduction to the Theory of Numbers**. [S.l.]: OUP Oxford, 2008. (Oxford mathematics). ISBN 9780199219865.

ROSA, Ana Carla Quallio; MANSO, Fernando Cézar Gonçalves; CORRÊA, Wellington José. Uma abordagem matemática para a otimização do custo computacional do Teorema Chinês do Resto. In: ANAIS da XI Bienal da Matemática. UFSCar, São Carlos, SP: [s.n.], 2024.

ROSA, Ana Carla Quallio; MANSO, Fernando Cézar Gonçalves; CORRÊA, Wellington José. Uma nova perspectiva para o Algoritmo de Euclides: Uma abordagem computacional para o cálculo dos coeficientes da Relação de Bézout. In: XIII Seminário de Extensão e Inovação e XXVIII Seminário de Iniciação Científica e Tecnológica da UTFPR. Ponta Grossa, PR: [s.n.], 2023.

[2] Disponível em: https://teorianumeros.com/. Acesso em: 20 set. 2024.