



## UMA INTRODUÇÃO AO ALGORITMO AKS

Ísis Vieira Fernandes<sup>1</sup>, Leomaques Francisco Silva Bernardo<sup>2</sup>

### RESUMO

A Teoria dos Números é uma das áreas de grande relevância na Matemática e tem por objetivo estudar os números inteiros e suas propriedades. O surgimento da Teoria dos Números deu-se em civilizações bem antigas. É possível encontrar os conceitos de números primos e compostos nos Elementos de Euclides, obra do matemático Euclides escrita por volta de 300 a.C. e que consiste de 13 livros ou capítulos. Ao longo dos séculos muitos problemas importantes foram estudados na Teoria dos Números. Um problema que merece destaque é a discussão se um dado número inteiro é ou não primo. Vários matemáticos se destinaram a estudar testes de primalidade que são testes para determinar se um dado número inteiro é primo. Estes testes são importantes visto que os métodos de Criptografia usados atualmente usam números primos suficientemente grandes. Neste contexto o objetivo principal desse trabalho é estudar o famoso teste de primalidade chamado de Algoritmo AKS que foi criado pelos matemáticos indianos Agrawal, Kayal e Saxena e publicado em agosto de 2002.

**Palavras-chave:** números primos, algoritmos, teste de primalidade.

---

<sup>1</sup>Aluna do curso de Licenciatura em Matemática, Unidade Acadêmica de Matemática, UFCEG, Campina Grande, PB, e-mail: isisvf11@gmail.com

<sup>2</sup>Doutor, professor, Unidade Acadêmica de Matemática, UFCEG, Campina Grande, PB, e-mail: leomaques@mat.ufcg.edu.br



## ***AN INTRODUCTION TO AKS ALGORITHM***

### **ABSTRACT**

The Theory of Numbers is one of the areas with great relevance in maths and the objective is to study integer numbers and its properties. The emerge of the Theory of Numbers comes from old civilizations. It is possible to find the concepts of prime and composite numbers on the Elements of Euclid written around 300 years B.C which consists of 13 books or chapters. During the centuries many important problems were studied on the Theory of Numbers. An issue that calls attention is the discussion if an integer number is not prime. These tests are important once the current cryptography methods make use of prime numbers sufficiently large. In this context, the main goal is to study the famous AKS algorithm primality test created by the Indian mathematicians Agrawal, Kayal, and Saxena, published in August 2002.

**Key Words:** prime numbers, algorithms, primality test.