

É possível determinar se um inteiro é primo ou composto de forma eficiente?

Uma dificuldade em resolver esse problema reside em fornecer uma definição formal do que é considerado um processo eficiente. Com o advento da teoria da complexidade de algoritmos, esse impasse foi superado, e desde então passou a ser dada uma atenção maior a esse antigo problema.

A despeito de diversos esforços, essa questão permaneceu ainda por um bom tempo em aberto. Finalmente em 2002, os indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena publicam o artigo *Primes is in P*, no qual apresentam pela primeira vez o algoritmo AKS, respondendo afirmativamente à questão acima.

Os objetivos desta apresentação são os seguintes: apresentar o algoritmo AKS, provar que ele funciona corretamente e que se trata de um algoritmo eficiente.