060 **ALGORITMO AKS.** *Daniel Tartari Generali, Vilmar Trevisan (orient.)* (UFRGS).
A determinação da primalidade de um número muito grande é um problema matemático clássico muito estudado e especialmente complexo do ponto de vista computacional. Os primeiros algoritmos criados para testar a primalidade de um número remontam a Grécia antiga. Hoje, os números primos são utilizados em sistemas de criptografia, os quais constituem os mecanismos de proteção ao acesso, transmissão e integridade de dados em uma rede digital aberta, como é a Internet. Até 2002, os principais algoritmos desenvolvidos para esta finalidade se enquadravam em duas grandes classes: os determinísticos de tempo não-polinomial (afirmam com 100% de certeza a primalidade de um número, mas o cálculo é realizado em tempo exponencial), e os não-determinísticos de tempo polinomial (a complexidade do algoritmo é uma função polinomial do número de dígitos da entrada, mas não dão certeza absoluta quanto à primalidade). Assim, o desafio era obter um algoritmo de complexidade polinomial e determinístico. Tal meta foi alcançada em 2002 quando Agrawal, Kayal, Saxena divulgaram o algoritmo AKS. A proposta deste trabalho é explorar a teoria matemática na qual está baseada a construção do AKS. A análise dos aspectos computacionais, o teorema central que prova o funcionamento do algoritmo e sua performance são os assuntos centrais a serem abordados. (PIBIC).