321 **PRIMALIDADE EM TEMPO POLINOMIAL - O ALGORITMO AKS.** *Thaisa Raupp Tamusiunas, Alveri Alves Sant Ana (orient.)* (UFRGS).

Existem muitos testes de primalidade conhecidos desde muito tempo, mas basicamente estes testes podem ser classificados em dois tipos: os que trazem resposta correta, mas são tão lentos que se tornam impraticáveis quando se trata de discutir a primalidade de números muito grande, e aqueles que são rápidos mas trazem uma margem de erro embutida. Em agosto de 2002 foi publicado pelos matemáticos indianos M. Agrawal, N. Kayal e N. Saxena, um algorítmo que decide se um dado número é ou não primo, hoje conhecido como algorítmo AKS, e que faz isto em "tempo polinomial". A proposta aqui é a de apresentar uma versão melhorada deste algorítmo, proposta por H. W. Lenstra Jr., descrevendo como e porque o algoritmo funciona, bem como mostrar que ele tem custo polinomial. (Fapergs).