269 **O TESTE DE PRIMALIDADE DE MILLER-RABIN.** *Carlos Hoppen, Vilmar Trevisan*. (Instituto de Matemática, UFRGS).

Determinar a primalidade de um número é um problema difícil de crescente interesse em Teoria dos Números, devido a sua aplicação em criptografia, vastamente presente na comunicação eletrônica de dados. Com o auxílio de um computador, é possível fatorar um número em seus divisores e, então, verificar se ele é primo sem muita dificuldade, desde que o número de dígitos não seja muito grande. Para números maiores, porém, métodos indiretos são necessários. O objetivo do presente trabalho é apresentar um desses métodos, o Algoritmo de Miller-Rabin. Esse algoritmo consiste em aplicar o Teste de Miller a um número p, ou seja, verificar se ele satisfaz a propriedade $a^{p-1} \equiv 1 \pmod{p}$ para uma base a qualquer. Pelo Pequeno Teorema de Fermat, se o número é primo, então ele satisfaz essa propriedade. A recíproca não é verdadeira, mas uma análise probabilística feita por Rabin mostrou que esse algoritmo é confiável. Mais precisamente, se o número p passa no Teste de Miller k vezes, então ele é primo com probabilidade, pelo menos, $1-1/4^k$. (FAPERGS).