Sessão 21
Matemática Aplicada II

188 **O ALGORITMO PROBABILÍSTICO DE MILLER- RABIN PARA A PRIMALIDADE DE INTEIROS.** *Jeaniris Feichas Alves, Vilmar Trevisan (orient.)* (Departamento de Matemática Pura e Aplicada, Instituto de Matemática, UFRGS).

Encontrar um algoritmo eficiente para saber se um numero inteiro é primo ou composto é uma questão importante para a criptografia moderna. A partir do conhecido “Pequeno Teorema de Fermat” tem –se que se n é primo , então an-1 mod n = 1 para qualquer inteiro 1 (a (n - 1. A recíproca do Pequeno Teorema de Fermat é falsa, pois existem inteiros compostos n tais an-1 mod n = 1 para vários a conhecidos como “falsas testemunhas”. Assim, o PTF não pode ser usado diretamente como um teste de primalidade. Com uma modificação no Teorema Miller e Rabin (1980) criaram um teste – Btest - que diminui as chances de um “falso testemunho” ser escolhido. Seja n um inteiro ímpar maior do que 4 e sejam s e t inteiros tais que n - 1= 2s t, onde t é ímpar. Seja B(n) o conjunto de inteiros definido por a (B(n) se e somente se 2 (a (n -2 e at mod n =1 ou existe um inteiro i, 0 (i < s tal que a t 2**i mod n = n-1.Pressupondo que n seja ímpar composto e 2 (a (n-2, o Btest(a, n) retorna verdadeiro apenas se a (B(n). Por outro lado, temos que um número arbitrário ímpar n, n > 4 é primo se B(n) = {a(2 (a (n – 2}. Além disso, se n é composto então (B(n) (((n-9)/4. Assim, o Btest(a, n) sempre retorna verdadeiro caso n seja primo maior que 4 e 2 (a (n – 2 e tem probabilidade de ¾ de retornar falso quando n é ímpar composto maior do que 4 e a é escolhido arbitrariamente ente 2 e n - 2. O uso desse teste resulta em um eficiente algoritmo probabilístico para a primalidade de n. Neste trabalho, apresentaremos o Algoritmo de Miller-Rabin, assim como provaremos a sua correção. Além disso, apresentaremos dados que mostram a importância de seu uso em aplicações prática atuais. (PIBIC/CNPq-UFRGS).