A-1

FORMA QUADRÁTICA DE EULER E ÁLGEBRAS LAURA

Guilherme Bufáiçal Neves (Acadêmico); Prof. Dr. Cristian Patrício Nóvoa Bustos (Orientador). Núcleo de Pesquisa em Matemática. Universidade Católica de Goiás
Contato: guibufaical@gmail.com, cristiannovoa@netscape.net

O estudo deste projeto visa estudar os números primos e mais especificamente como determinar se um número é primo ou não. A abordagem foi feita de forma computacional, ou seja, utilizando-se a matemática aliada à computação irá verificar-se tal fato. A determinação do número primo vai ser baseada em dois algoritmos de maior aceitação e utilização por sua capacidade temporal de determinação, estes algoritmos são: o RSA e o AKS. Os algoritmos procuram de forma determinística, em um tempo polinomial e a um custo computacional mensurável fazer um teste de primalidade, quer dizer, indicar se um número é primo ou composto. Contudo, com exceção do AKS, apesar de alguns algoritmos trabalharem de forma determinística eles são apenas probabilísticos, ou seja, eles não podem com certeza absoluta afirmar se um número é primo ou não. Eles apenas fornecem uma probabilidade, bastante alta e aceitável no mundo moderno, de afirmar a característica do número. O enfoque maior foi dado ao algoritmo AKS por se tratar do melhor algoritmo em determinação de primalidade conhecido atualmente. A forma de abordagem do AKS foi feita através de apresentações preparadas após o estudo da parte matemática relacionada ao assunto como, por exemplo, Teoria dos Números, Teorema de Fermat, Grupos abelianos, Polinômios. Esta parte foi necessária para se obter um embasamento teórico que possibilitasse uma maior e mais rápida compreensão acerca das operações e do raciocínio utilizado nos algoritmos citados. Neste segundo ano de pesquisa o AKS foi estudado mais profundamente e conseguiu-se implantar o algoritmo com sucesso. A implementação e a verificação prática de todo conteúdo visto serviu para complementar o trabalho da Pesquisa Científica. A importância deste trabalho deve-se ao fato dos números primos terem se tornado vitais para a segurança computacional nos dias de hoje, já que todos os mecanismos de segurança envolvem computadores tanto para acesso, transmissão e integridade de dados na Internet quanto para a segurança de contas, cofres e documentos de importância restrita.

Palavras-chave: 1) Algoritmo AKS; 2) Primalidade; 3) Determinístico; 4) Tempo polinomial.

Apoio: BIC/UCG.