UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

CENTRO DE INFORMÁTICA

2009.2

UM ESTUDO SOBRE ALGORITMOS DE TESTE DE PRIMALIDADE: HISTÓRICO, COMPARATIVO E APLICAÇÕES

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno Amirton Bezerra Chagas {abc@cin.ufpe.br}

Orientador Liliane Rose Benning Salgado {liliane@cin.ufpe.br}

12 de Agosto de 2009

Sumário

1. Contexto

Ao longo da história, os números primos sempre instigaram a curiosidade de leigos e matemáticos. Há evidências que os povos da Babilônia já possuíam o conceito de números que não podiam ser divididos em partes inteiras a não ser por 1 e por eles mesmos. Os gregos posteriormente se dedicaram ao estudo de algumas propriedades de tais números, e a partir daí iniciou-se um tema estudado por matemáticos até os dias atuais.

Estes números, que apresentam algumas características únicas, foram por muito tempo estudados apenas por curiosidade matemática ou até mesmo pelo misticismo associado a alguns números primos em escritos religiosos de diversas crenças. A descoberta do maior número primo era no passado algo que trazia reconhecimento e satisfação pessoal, mas pouca utilidade prática para o mundo em geral.

O estudo dos números primos faz parte de um ramo da matemática chamada Teoria dos Números. Pesquisadores ligados a esta área, até pouco tempo atrás, acreditavam estar envolvidos em pesquisas de matemática pura, sem nenhuma aplicação, na crença de que os números primos iriam permanecer para sempre como elementos estudados apenas por sua beleza matemática, sem relação com o mundo real.

Esta crença foi superada quando em 1978, Rivest, Shamir e Adleman revelaram ao mundo o algoritmo de criptografia de chave pública RSA. Este algoritmo faz uso de números primos e aritmética modular para a geração das chaves pública e privada, de forma a se aproveitar da complexidade do problema da fatoração.

Outras aplicações para números primos foram encontradas, como o tamanho de tabelas hash, geração pseudo-aleatória de números e otimização da alocação de recursos em redes de telefonia móvel. No entanto, a maior parte do estudo atual sobre números primos se deve ainda a área de criptografia.

Com o crescimento do poder computacional, chaves maiores são necessárias, a fim de tornar a probabilidade de um atacante quebrar o sistema desprezível. Para a geração de tais chaves, é necessário o uso de números primos cada vez maiores. Neste ponto, entram os algoritmos de teste de primalidade.

O problema de verificar se um número é primo ou não foi resolvido polinomial e deterministicamente em 2002, sem depender de conjecturas em aberto por Agrawal, Kayal e Saxena. Esta solução computacional é conhecida como o algoritmo AKS.

Anteriormente, tudo o que existia eram algoritmos que se baseavam em conjecturas não provadas, como a hipótese de Riemman ou algoritmos probabilísticos, que forneciam uma resposta com uma determinada probabilidade de erro. Obviamente, também existem algoritmos exponenciais que resolvem este problema por força-bruta, completamente fora da realidade para razões práticas.

Apesar de ser eficiente do ponto de vista teórico, AKS não é usado na prática por ainda carregar um expoente muito alto, que inviabiliza sua utilização em aplicações reais. Ainda são amplamente usados os algoritmos probabilísticos, especialmente o de Miller-Rabin, para a geração de números primos. Para a descoberta de novos grandes números primos, geralmente são definidas algumas restrições (como limitar o teste a números de Mersenne), que permitem o uso de algoritmos determinísticos e rápidos (como o teste de Lucas-Lehmer).

2. Objetivos

A proposta para este trabalho de graduação é estudar e detalhar os algoritmos que fazem parte da história dos testes de primalidade. Será descrito o estado da arte, cronologicamente, para preencher uma lacuna bibliográfica constatada em relação ao tópico desta pesquisa.

Além disto, pretendo analisar o algoritmo AKS e as melhorias propostas desde sua publicação. O estudo será realizado com foco nos fundamentos teóricos computacionais envolvidos.

Pretendo também implementar uma ferramenta que ofereça a comparação dos algoritmos mais relevantes, com o intuito de utilizá-la para fins didáticos em aulas ou apresentações sobre testes de primalidade. A quantidade de testes implementados nesta ferramenta será definida de acordo com o andamento da pesquisa.

3. Cronograma

O cronograma abaixo demonstra algumas datas para as atividades principais do processo de desenvolvimento do trabalho de graduação. Os prazos podem ser alterados conforme o estudo e aprofundamento do trabalho ou o acontecimento de imprevistos.

ATIVIDADES	**AGOSTO**			**SETEMBRO**			**OUTUBRO**			**NOVEMBRO**		
Levantamento da literatura												
Definição do estado-da-arte												
Implementação de algoritmos de teste de primalidade												
Estudo do algoritmo AKS												
Análise da implementação de AKS, em busca de melhorias												
Execução e análise dos algoritmos com fins comparativos												
Elaboração do relatório												
Elaboração da apresentação												

4. Referências

AGRAWAL, Manindra; KAYAL, Neeraj; SAXENA, Nitin. PRIMES is in P. **Annals Of Mathematics**, n. 2, p.781-793, 2004.

ARBOUW, Ernst. **How the Queen of Sciences is put to work**. Disponível em: <http://www.uk.rug.nl/archief/jaargang36/24/15a.php>. Acesso em: 12 ago. 2009.

MCGREGOR-DORSEY, Zachary S. **Methods of Primality Testing**. Disponível em: <http://www-math.mit.edu/phase2/UJM/vol1/DORSEY-F.PDF>. Acesso em: 12 ago. 2009.

MOTOHASHI, Yoichi. **Prime Numbers – Your Gems**. Disponível em: <http://arxiv.org/PS_cache/math/pdf/0512/0512143v1.pdf>. Acesso em: 12 ago. 2009.

WEISSTEIN, Eric W**. Lucas-Lehmer Test**. Disponível em: <http://mathworld.wolfram.com/Lucas-LehmerTest.html>. Acesso em: 12 ago. 2009.

YANG, Guu-chang; KWONG, Wing C.. Performance Analysis of Extended Carrier-Hopping Prime Codes for Optical CDMA. **IEEE Transactions On Communications**, v. 53, n. 5, p.876-881, maio 2005. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1431132&isnumber=30867>. Acesso em: 12 ago. 2009.

5. Possíveis Avaliadores

Anjolina Grisi de Oliveira

6. Assinaturas

Liliane Rose Benning Salgado

Orientador

Amirton Bezerra Chagas

Aluno