ESTUDO EM TEORIA DE NÚMEROS: PRIMALIDADE EM TEMPO POLINOMIAL

Wesley Gonçalves Lautenschlaeger
Orientadora: Thaísa Raupp Tamusiunas

INTRODUÇÃO

Em 06 de agosto de 2002 foi publicado o primeiro teste de primalidade que era ao mesmo tempo polinomial e determinístico: o algoritmo AKS. Desenvolvido por Manindra Agrawal, Neeraj Kayal e Nitin Saxena, cientistas da computação do Instituto Indiano de tecnologia de Kanpur, o artigo intitulado "Primes in P" demonstrou grande importância para a Teoria dos Números.

O algoritmo utiliza teoria de grupos e teoria de anéis, além de se basear em resultados de outros testes de primalidade, como, por exemplo, o teste de Fermat (este com custo exponencial).

O ALGORITMO AKS

Entrada: $n \in \mathbb{Z}^+$

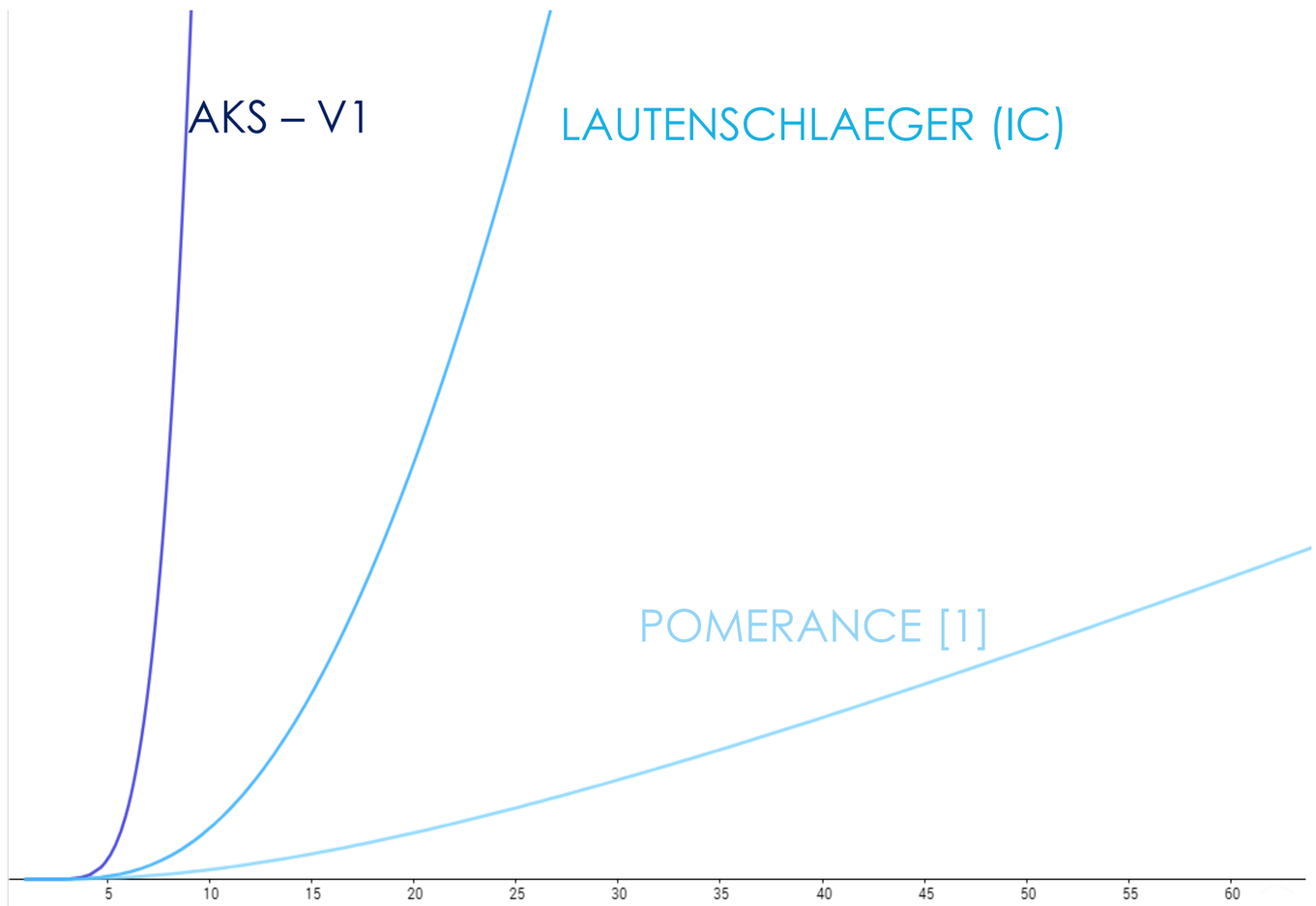
1. Se $(n = a^b$ para $a \in \mathbb{N}$ e $b > 1)$, escreva **composto**.
2. Encontre o menor r tal que $o_r > (\log n)^2$.
3. Se $1 < (a, n) < n$ para algum $a \leq r$, escreva **composto**.
4. Se $n \leq r$, escreva **primo**.
5. Para $a = 1$ até $\lfloor \sqrt{\phi(r)} \log n \rfloor$ faça

   Se $((X + a)^n \neq X^n + a \ (mod\ X^r - 1, n))$, escreva **composto**.
6. Escreva **primo**.

MÉTODOS E RESULTADOS

Apesar de possuir custo polinomial, o algoritmo AKS ainda é lento. O custo da primeira versão publicada é, em notação de custo big-O (limite assintótico superior), de $(\ln(n))^{12}$. A versão com melhor custo já publicada [1] tem custo de $(\ln(n))^6$.

A partir desta motivação, aplicamos conceitos de Álgebra Linear, utilizamos o Teorema da Convolução, bem como resultados da Teoria dos Crivos e o método de Newton. O custo alcançado foi de $(\ln(n))^8$. A imagem mostra a comparação entre as três versões citadas.



PERSPECTIVAS FUTURAS

O custo do algoritmo pode ser otimizado: Agrawal, um dos criadores do algoritmo AKS, sugeriu que

se $(X - 1)^n \equiv X^n - 1 \ (mod\ X^r - 1, n)$, então n é primo ou $n^2 \equiv 1 \ (mod\ r)$.

Esta conjectura, provada falsa por Pomerance, possui a seguinte variação [2]:

se $(X - 1)^n \equiv X^n - 1 \ (mod\ X^r - 1, n)$ e $(X + 2)^n \equiv X^n + 2 \ (mod\ X^r - 1, n)$, então n é primo ou $n^2 \equiv 1 \ (mod\ r)$.

Se o enunciado acima for verdadeiro, o custo do algoritmo seria reduzido para $(\ln(n))^3$.

REFERÊNCIAS

[1] H. W. Lenstra Jr. e Carl Pomerance, "Primality testing with Gaussian periods", versão preliminar, 2005.

[2] Popovych, Roman, A note on Agrawal conjecture, 2008.

Coutinho, S.C., Primalidade em Tempo Polinomial: Uma Introdução ao Algoritmo AKS. 2004.

Agrawal, M., N. Kayal e N. Saxena, Primes is in P, IIT, versão preliminar, 2002.