Testes de Primalidade - Fundamentos e Prática

Aluno: Gervásio Protásio dos Santos Neto Orientador: Routo Terada

IME-USP, São Paulo (PIC 2013/2014 - Bolsista CNPq)

gervasio@ime.usp.br

Resumo

Números primos são de grande interesse para Teoria dos Números e são essenciais em Criptografia. Nesse trabalho estudamos diversos algoritmos usados para decidir se um número é ou não primo, bem como os resultados matemáticos que os fundamentam. Estes algortimos foram implementados e testados e seus desempenhos foram comparados.

1. Introducão

Números primos são essenciais para Criptografia, sendo a base de aplicações amplamente difundidas, como o criptossistema RSA e Criptossistemas de Curvas Elípticas.

Então, é natural que busque-se formas rápidas e eficientes de decidir se um número é ou não primo. Para tal foram desenvolvidos diversos algoritmos que, fundamentando-se em resultados da Teoria dos Números, buscam resolver esse problema. Este projeto de Iniciação Científica, que contou com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), destinou-se ao estudo e implementações de quatro destes algoritmos, procurando também desenvolver o arcabouço matemático que prova sua correção, analisar seu consumo de tempo e buscar possíveis ideias e heurísticas que melhorassem seu funcionamento.

2. Metodologia

Para serem estudados, foram escolhidos o Teste de Wilson[2], o Teste de Miller-Rabin [1][2], o AKS [4], o Teste de Goldwasser-Kilian [5].

Para cada teste buscou-se entender os principais teoremas que os fundamentam e implementá-los, de forma que se pudesse medir empiricamente seu desempenho.

Todos os teste foram realizados em um notebook MacBook Air, 1.7 GHz Intel Core i5, memória de 4GB 1333 MHz DDR3, sistema operacional OS X Mavericks.

Por fim, reuniram-se conclusões sobre eficiência e aplicabilidade dos algoritmos, problemas e dificuldades de implementação e propõe-se ideias que poderiam levar a sua melhoria.

3. Teste de Wilson

Teorema 1 *p é primo* $\iff (p-1)! \equiv -1 \bmod p$.

1. $x \leftarrow (n-1)! \bmod n$
2. Se $x \equiv -1 \bmod n$ **retornar PRIMO**
3. Senão, **retornar COMPOSTO**

4. Algoritmo de Miller-Rabin

Teorema 2 ***(Pequeno Teorema de Fermat)*** *Se p é um número primo, então $\forall a \in \mathbf{Z}_p$, $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$.*

Definição 1 *Um **número de Charmichael** é um inteiro composto n tal que $\forall a \in \mathbb{Z}_n$ tem-se $a^{n-1} \equiv 1 \bmod n$.*

Definição 2 *Seja n um número ímpar composto tal que $n = 2^s t + 1$, com t ímpar. Seja $b \in \mathbb{Z}_n$, $b \neq 0$. Dizemos que n é um **pseudoprimo forte na base b** se*

1. $b^t \equiv 1 \bmod n$, ou;

2. $\exists r$, $0 \leq r < s$, tal que $b^{2^r} t \equiv -1 \bmod n$

1. $n - 1 = 2^s t$
2. **para**: *teste* = $1, \ldots, k$ **faça**:
   (a) Escolher $a \in (2, n-2)$
   (b) $x_0 = a^t \bmod n$; $x_1 = (r_0)^2 \bmod n$
   (c) **para**: *j* = $1, \ldots, s$ **faça**:
      i. **se** $x_j \equiv 1 \bmod n$ e $x_{j-1} \not\equiv \pm 1 \bmod n$: **retornar** COMPOSTO
      ii. $x_{j+1} = (x_j)^2 \bmod n$
   (d) **se** $x_s \neq 1$: **retornar** COMPOSTO
3. **retornar** PRIMO

5. AKS

Teorema 3 p *é primo* $\iff \forall a, p \geq 2$, *tais que mdc(a,p) = 1, vale* $(x+a)^p \equiv x + a^p \bmod p$.

1. **se** $n = a^b, a \in \mathbb{N}, b > 1$ **return** COMPOSTO
2. r = $\min \{m | o_m(n) > (\log n)^2\}$
3. **se** $1 < mdc(a, n) < n$ **return** COMPOSTO
4. **se** $n \leq r$ **return** PRIMO
5. **para** $a = 1, \ldots, \lfloor \sqrt{\varphi(r)} \log n \rfloor$
   (a) **se** $(x-a)^n \not\equiv (x^n - a) \bmod (n, x^r - 1)$ **return** COMPOSTO
6. **return** PRIMO

6. Teste de Goldwasser-Kilian

Definição 3 *A equação $y^2 = x^3 + ax + b \bmod n$, onde $a, b \in \mathbb{Z}_n$ é chamada **Equação de Weiestrass**.*

Definição 4 *Se n da equação de Weiestrass for primo, o conjunto de pares ordenados (x,y), que a satisfazem, juntamente com o ponto no infinito O, formam uma Curva Elíptica E sobre o corpo finito $\mathbb{F}_n$. Denota-se $E(\mathbb{F}_n)$.*

Teorema 4 *Seja n um inteiro positivo. Seja E o conjunto de pares ordenados que satisfazem a equação de Weiestrass. Seja também m um inteiro. Suponhamos que um primo q é tal que $q|m$ e $q > (n^{1/4} + 1)^2$. Se $\exists P \in E$ tal que $mP = O$; e $(m/q)P \neq O \in E$, então n é primo.*

1. Escolhe-se 3 inteiros aleatórios $a, x, y \in \mathbb{Z}_n$.
2. Define-se $b = y^2 - x^3 - ax$ e a curva E, definida pela equação $y^2 = x^3 + ax + b \bmod n$.
3. Escolhe-se aleatoriamente um ponto P da curva.
4. Conta-se o número m de pontos da curva
5. Encontra-se um primo provável q tal que $m = cq$, para algum $c \in \mathbb{Z}$. Se não formos capazes de achar tal q, voltamos ao passo 1.
6. Computa-se mP e cP. Neste momento, temos as seguintes possibilidades:
   (a) Se $mP \neq O$, n é composto.
   (b) Se $cP = O$, recomeça-se o algoritmo.
   (c) Se $mP = O$ e $cP \neq O$, o Teorema 5 nos diz que n é primo, provido que q é primo.
7. Certifica-se de que q é primo.

7. Resultados

O teste de Wilson (implementado em C) mostrou-se lento, levando em média meio minuto para decidir a primalidade de números da ordem de 10^9. Isso se deve ao cálculo do fatorial, que faz com que o algoritmo seja exponencial no tamanho da entrada. Isso significa que o teste é inviável para aplicações práticas

O teste de Miller-Rabin foi implementado em C e em SAGE e mostrou-se eficiente. Em C, para primos da ordem de 10^9 o tempo médio foi em torno de 61,7 *ns*, com probabilidade de erro de 4^{-30}. Em SAGE para números da ordem de 10^{30} levou-se em média 0.0083 segundos e para números da ordem de 10^{40}, a média foi de 0.0113 segundos.

Em ambas as implementações os tempos para números compostos foram negligenciáveis. Percebeu-se que o algoritmo determinava rapidamente se um número era composto e demorava-se apenas para primos (uma vez que nestes casos, o algoritmo não era interrompido, tendo todos seus passos realizados).

Para o AKS, verificou-se que uma implementação em C do pseudo-código era ineficiente e de difícil implementação. Tentou-se algumas mudanças na busca por melhorias:

- Procurou-se um limite superior diferente para o laço do passo 5 do algoritmo, pois o cálculo de $\varphi(n)$ é uma atividade computacionalmente custosa.

- No passo 5(a), ao invés de verificarmos a desigualdade de polinômios, sorteamos um número, calculamos as funções e vemos se os valores são condizentes.

Verificou-se que a primeira mudança não nos trouxe ganho significativo de performance, enquanto a segunda o fez, mas abrindo mão do determinísmo. Conclui-se que o teste é de interesse apena teórico, por ser responsável por mostrar que existe um algoritmo polinomial determinístico para decidir primalidade.

O algoritmo de Goldwasser- Kilian pode ser usado para certificar rapidamente (tempo polinomial) a primalidade de um número. Caso a última etapa do algoritmo seja utilizada em todos os possíveis valores de q, teremos um algoritmo recursivo que será chamada $O(\log n)$ vezes. O certificado devolvido é uma tupla (n, a, b, m, q) que pode ser usada para rapidamente verificar que o número n é primo através da aplicação do Teorema 5.

O algoritmo foi implementado em SAGE e mostrou-se, em geral, satisfatoriamente rápido. Foram rodados testes para verificar o tempo médio necessário para decidir a primalidade de um número (as entradas eram números primos aleatórios) e para verificar o certificado de primalidade. Para números da ordem de 10^{30} observou-se em média 2.5 segundos para obter o certificado de primalidade; caso já se tivesse um certificado, este era testado com tempo médio de 0.078 segundos. Com entradas da ordem de 10^{40} observou-se um tempo médio de 42.95 segundos para obtenção de um certificado e 0.448 segundos para a verificação de um certificado.

Referências

[1] Routo Terada, *Segurança de Dados*. Blucher, São Paulo, Segunda Edição, 2008.

[2] E. Kranakis. *Primality and Criptography*. Wiley, 1986.

[3] N. Koblitz. *A Course in Number Theory and Criptography*. Springer-Verlag, 1994.

[4] M. Agrawal, N. Kayal, N. Saxena. *PRIMES is in P*. *Annals of Mathematics*, 160 (2):781–793, 2002

[5] S. Goldwasser, J. Kilian. *Primality Testing Using Elliptic Curves*. *Journal of the ACM*, Vol 46, No. 4, Julho 1999, pp. 450-472.

IME-USP

CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico

UNIVERSIDADE DE SÃO PAULO SCIENTIA VINCES