Algoritmos Probabilísticos

Departamento de Ciência da Computação – IME/USP

Segundo Semestre de 2006

Algoritmo de Miller-Rabin

O algoritmo de Miller-Rabin para decidir se um número é primo ou não consiste no seguinte:

```
MILLER-RABIN (n, s)
 1  para j ← 1 até s faça
 2     a ← RAND(1, n − 1)
 3     se MR-TESTEMUNHA(n, a)
 4        então devolva COMPOSTO
 5  devolva PRIMO

MR-TESTEMUNHA (n, a)
 1  seja b_k ... b_0 a representação binária de n − 1
 2  d ← 1
 3  para i ← k até 0 faça
 4     x ← d
 5     d ← d^2 mod n
 6     se d = 1 e x ≠ 1 e x ≠ −1
 7        então devolva VERDADEIRO
 8     se b_i = 1
 9        então d ← d.a mod n
10  se d ≠ 1
11     então devolva VERDADEIRO
12  devolva FALSO
```

Teorema 1 (Chinês do Resto)**.** *Seja $n = n_1 \cdots n_k$ onde os n_i's são dois a dois relativamente primos. Considere a correspondência $a \leftrightarrow (a_1, \ldots, a_k)$ onde $a \in \mathbf{Z}_n$ e $a_i = a \mod n_i$, para $i = 1, \ldots, k$. Essa correspondência é uma bijeção entre $\mathbf{Z}_n$ e $\mathbf{Z}_1 \times \cdots \times \mathbf{Z}_k$.*

Corolário 1. *Se $n_1, \ldots, n_k$ são dois a dois relativamente primos e $n = n_1 \cdots n_k$, então, para quaisquer $a_1, \ldots, a_k$, o sistema com as equações*

$$x \;=\; a_i \mod n_i \qquad \text{para } i = 1, \ldots, k$$

tem uma única solução em $\mathbf{Z}_n$.

Corolário 2. *Se $n_1, \ldots, n_k$ são dois a dois relativamente primos e $n = n_1 \cdots n_k$, então, para todos os inteiros x e a,*

$$x \;=\; a_i \mod n_i \qquad \text{para } i = 1, \ldots, k$$

se e somente se $x \;=\; a \mod n$.

Algoritmo de Solovay-Strassen

O *símbolo de Jacobi* é definido para um número ímpar n e um número a que é relativamente primo com n (ou seja, tal que $\text{mdc}(n, a) = 1$). Quando n é primo, o símbolo de Jacobi coincide com o chamado símbolo de Legendre:

$$\left[\frac{a}{n}\right] \;=\; a^{\frac{n-1}{2}} \mod n.$$

Quando n é composto, o símbolo de Jacobi é definido em função da decomposição de n em fatores primos. Digamos que a fatoração de n seja $p_1^{k_1} \cdots p_t^{k_t}$. Então

$$\left[\frac{a}{n}\right] \;=\; \prod_{i=1}^{t} \left[\frac{a}{p_i}\right]^{k_i}.$$

Note que o símbolo de Jacobi é sempre 1 ou -1. Isso decorre do fato de que o símbolo de Legendre é sempre 1 ou -1, já que $a^{n-1} = 1$ para todo a em $\mathbf{Z}_n^*$, e não há raízes não triviais da unidade em $\mathbf{Z}_n$ quando n é primo. Abaixo apresentamos o algoritmo de Solovay-Strassen.

```
SOLOVAY-STRASSEN (n, s)
 1  para j ← 1 até s faça
 2     a ← RAND(1, n − 1)
 3     se SS-TESTEMUNHA(n, a)
 4        então devolva COMPOSTO
 5  devolva PRIMO

SS-TESTEMUNHA (n, a)
 1  d ← mdc(a, n)
 2  se d ≠ −1
 3     então devolva VERDADEIRO
 4  j ← [a/n]
 5  se j = a^((n−1)/2) mod n
 6     então devolva FALSO
 7     senão devolva VERDADEIRO
```

Como não conhecemos um algoritmo polinomial que, dado n, determina a fatoração de n em primos, a definição do símbolo de Jacobi não implica em um algoritmo polinomial para o seu cálculo. O teorema abaixo apresenta algumas propriedades do símbolo de Jacobi e permite derivarmos um algoritmo que, dados n e a, devolve o valor do símbolo de Jacobi em tempo polinomial.

Teorema 2. *O símbolo de Jacobi satisfaz as seguintes propriedades:*

(1) $\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right]\left[\frac{b}{n}\right]$;
(2) $\left[\frac{a}{n}\right] = \left[\frac{b}{n}\right]$ *sempre que* $a = b \mod n$;
(3) *Para ímpares relativamente primos,* $\left[\frac{a}{n}\right] = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}\left[\frac{n}{a}\right]$;
(4) $\left[\frac{1}{n}\right] = 1$;
(5) $\left[\frac{2}{n}\right] = \begin{cases} -1 & \text{para } n = 3 \text{ ou } n = 5 \mod 8 \\ 1 & \text{para } n = 1 \text{ ou } n = 7 \mod 8 \end{cases}$

Seja $J_n = \{a \in \mathbf{Z}_n^* : \left[\frac{a}{n}\right] = a^{\frac{n-1}{2}} \mod n\}$. Se n é primo, então $J_n = \mathbf{Z}_n^*$.

Lema 1. *Para todo n composto, $|J_n| \leq |\mathbf{Z}_n^*|/2$.*