Solovay-Strassen test

Canonical name	SolovayStrassenTest
Date of creation	2013-03-22 14:27:33
Last modified on	2013-03-22 14:27:33
Owner	mathwizard (128)
Last modified by	mathwizard (128)
Numerical id	7
Author	mathwizard (128)
Entry type	Algorithm
Classification	msc 11Y11
Related topic	MillerRabinPrimeTest

It is known that an odd number n is prime if and only if for every $1 < a < n$ such that $(a, n) = 1$ we have

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n} \tag{1}$$

where $\left(\frac{a}{n}\right)$ is the Jacobi symbol. (The only if part is obvious; the if part follows from Theorem **??**.) From this we can derive the following algorithm.

1. Choose a random number a between 1 and $n - 1$.

2. Check if $(a, n) = 1$ (for example using the Euclidean algorithm). If it is not, then n is not prime and (a, n) is a divisor of n.

3. Check if Equation (**??**) holds. If it does not, then n is not prime. Otherwise n is a candidate for primality.

By repeating this algorithm we can increase the chance that the result is correct. In order to estimate the probability of error, we make use of Theorem **??**, which says that every independent iteration of the algorithm has a chance of at most 50% of being wrong. Hence, after t iterations there is at most a 2^{-t} chance of getting a wrong result.

Theorem 1. *Let $n \geq 3$ be an odd composite integer. Then at least half of the elements of $\mathbb{Z}_n^*$ do not satisfy Equation* (**??**).

Proof. It suffices to exhibit one element $a \in \mathbb{Z}_n^*$ which does not satisfy Equation (**??**). Indeed, if there exists one such element, then the set of all elements which do satisfy Equation (**??**) forms a proper subgroup of $\mathbb{Z}_n^*$, from which we conclude that the elements satisfying Equation (**??**) number no more than half of the elements of $\mathbb{Z}_n^*$.

We consider separately the cases where n is squarefree and not squarefree. If n is squarefree, let p be a prime dividing n and let b be a quadratic nonresidue mod n. Using the Chinese Remainder Theorem, choose an integer $a \in \mathbb{Z}_n^*$ such that:

$$\begin{aligned} a &\equiv b \pmod{p}, \\ a &\equiv 1 \pmod{\frac{n}{p}}. \end{aligned}$$

The Jacobi symbol $\left(\frac{a}{n}\right)$ is given by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{n/p}\right) = \left(\frac{b}{p}\right)\left(\frac{1}{n/p}\right) = (-1)\cdot 1 = -1.$$

We will assume that $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ and derive a contradiction. The equation $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ implies that $a^{\frac{n-1}{2}} \equiv -1 \pmod{\frac{n}{p}}$. However, since $a \equiv 1 \pmod{\frac{n}{p}}$, we must have $a^{\frac{n-1}{2}} \equiv 1 \pmod{\frac{n}{p}}$, so that $1 \equiv -1 \pmod{\frac{n}{p}}$, which is a contradiction.

Now suppose that n is not squarefree. Let p be a prime such that $p^2 \mid n$, and set $a = 1 + \frac{n}{p}$. By the binomial theorem, we have

$$a^p = \left(1 + \frac{n}{p}\right)^p = 1 + \binom{p}{1}(n/p) + \binom{p}{2}(n/p)^2 + \cdots + \binom{p}{p}(n/p)^p \equiv 1 \pmod{n},$$

so the multiplicative order of a mod n is equal to p, and hence in particular $a^{n-1} \not\equiv 1 \pmod{n}$, since $p \nmid n-1$. On the other hand,

$$\left(\frac{a}{n}\right) = \left(\frac{1+\frac{n}{p}}{n}\right) = \left(\frac{1+\frac{n}{p}}{p}\right)\left(\frac{1+\frac{n}{p}}{n/p}\right) = \left(\frac{1}{p}\right)\left(\frac{1}{n/p}\right) = 1,$$

so a does not satisfy Equation (**??**). □