Peudo-Linear Solovay-Strassen Modified Test for Primality

by

Allan Joseph Menezes

8

Theorem 0.0.1. *Solovay-Strassen Mod Theorem*

If there exist $a = 2, b$ *and* n *an odd integer such that* $\gcd(b, n) = 1$, $3 \not| n$ *and if* $2^{\frac{n-1}{2}} \equiv (\frac{2}{n}) \pmod{n}$ *and* $b^{\frac{n-1}{2}} \equiv -1(\frac{2}{n}) \pmod{n}$ *then* n *is prime.*

Proof. Choose two $a = 2, b$ as in the theorem statement and let the Euler Criterion be true for $a = 2, b$ and n. As well let n be composite and divisible by some prime p and $n = pk$ for some k. The main Lemma that has to be proven here is that such b exists for all n and is less than $\ln n$ and is easy to find in an iterative search. Let

$$A = a^{\frac{n-1}{2}} + b^{\frac{n-1}{2}}$$

$$B = a^{n-1} - b^{n-1} \equiv 0 \pmod{p}$$

$$(B + b^{n-1})^{\frac{1}{2}} = a^{\frac{n-1}{2}} \pmod{p}$$

Then

$$A \equiv a^{\frac{n-1}{2}} + b^{\frac{n-1}{2}} \equiv 0 \pmod{p}$$

$$A \equiv (B + b^{n-1})^{\frac{1}{2}} + b^{\frac{n-1}{2}} \equiv (0 + b^{n-1})^{\frac{1}{2}} + b^{\frac{n-1}{2}} \equiv 2b^{\frac{n-1}{2}} \equiv 0 \pmod{p}$$

Hence $p \mid 2$ or by our choice of b, $\gcd(b, n) = 1$ which is a contradiction as $\gcd(2, n) = 1$ and and n is odd. Hence n has to be prime. Or no such b as in theorem exists for some n and the only b that exists is such that $p \mid b$ and if this is determined to be within $\ln n$ then no problem exists for this primality test as then n is composite in that case. So for the search for b we must determine b, as in the theorem statement, within $\ln n$ and if not found declare this test to be unsuitable for this value of n. □

Chapter 1

Algorithms in pseudo-code

Function:

$Solovay - StrassenMod$

Input: n, a, b, n odd

If $3 \mid n$ return n composite.

If $n = m(m+2)$ or a perfect power return composite

Determine a, b such that $\gcd(a, n) = \gcd(b, n) = 1$

and

$(\frac{a}{n}) = 1$, $(\frac{b}{n}) = -1$. If $(\frac{a,b}{n}) = 0$ return n composite.

If $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ and $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$

Then

Return n is prime

Else

n composite.

End Function $Solovay - StrassenMod$