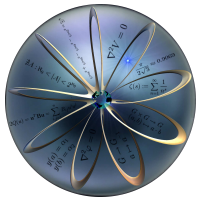

planetmath.org

Math for the people, by the people.

Miller-Rabin prime test

Canonical name	MillerRabinPrimeTest
Date of creation	2013-03-22 14:54:18
Last modified on	2013-03-22 14:54:18
Owner	mathwizard (128)
Last modified by	mathwizard (128)
Numerical id	9
Author	mathwizard (128)
Entry type	Algorithm
Classification	msc 11Y11
Synonym	Rabin prime test
Related topic	SolovayStrassenTest
Related topic	FermatCompositenessTest
Defines	strong pseudoprime

The Miller-Rabin prime test is a probabilistic test based on the following

Theorem 1. *Let $N \geq 3$ be an odd number and $N - 1 = 2^t n$, n odd. If and only if for every $a \in \mathbb{Z}$ with $\gcd(a, N) = 1$ we have*

$$a^n \equiv 1 \mod N \qquad \text{or} \tag{1a}$$

$$a^{2^s n} \equiv -1 \mod N \tag{1b}$$

for some $s \in \{0, \ldots, t-1\}$, then N is prime. If N is not prime, then let A be the set of all a satisfying the above conditions. We have

$$Card(A) \leq \frac{1}{4}\varphi(N),$$

where φ is Euler's Phi-function.

A composite number N satisfying conditions (**??**) for some $a \in \mathbb{Z}$ is called a *strong* in the basis a. Note that this theorem states that there are no such things as Carmichael numbers for strong pseudoprimes (i.e. composite numbers that are strong pseudoprimes for all values of a). From this theorem we can construct the following algorithm:

1. Choose a random $2 \leq a \leq N - 1$.
2. If $\gcd(a, N) \neq 1$, we have a non-trivial divisor of N, so N is not prime.
3. If $\gcd(a, N) = 1$, check if the conditions (**??**) are satisfied. If not, N is not prime, otherwise the probability that N is not prime is less than $\frac{1}{4}$.

In general the probability, that the test falsely reports N as a prime is far less than $\frac{1}{4}$. Of course the algorithm can be applied several times in order to reduce the probability, that N is not a prime but reported as one.

When comparing this test with the related Solovay-Strassen test one sees that this test is superior is several ways:

- There is no need to calculate the Jacobi symbol.
- The amount of *false witnesses*, i.e. numbers a that report N as a prime when it is not, is at most $\frac{N}{4}$ instead of $\frac{N}{2}$.
- One can even show that N which passes Miller-Rabin for some a also passes Solovay-Strassen for that a, so Miller-Rabin is always better.

Note that when the test returns that N is composite, then this is indeed the case, so it is really a compositeness test rather than a test for primality.