M207-2

abhijit.chakraborty

November 2020

Introduction

Miller-Rabin primality test is a probabilistic test which gives the chance of a number to be prime with high confidence. The false negative is 0.

Why it works

The whole algorithm is based on the following definition of prime:

Let a number $p = 2^k m$, m is odd. p is prime $\Longrightarrow a^m \equiv 1(mod\, p)$ or $a^{2^r m} \equiv -1(mod\, p)$ for one r in $[0 \ldots k-1]$, for all $1 \leq a < p$.

This can be proven easily. The contrapositive is that if there exists an a such that the above property doesn't hold, then the number is composite.

So we compute $a^{2^r m}(mod\, p)$ (it is computationally easy) and find if p composite by setting a random a.

But if the above property holds we can say it can be prime. Now it can be proven that if p is composite, then less than $\frac{1}{4}\frac{\phi(p)}{p-1}$ a's satisfies the above property. So the error limit is $\frac{1}{4}\frac{\phi(p)}{p-1} < \frac{1}{4}$. So the confidence is at least 75%.

As the complexity of performing this whole test k times $= O(k\, log^2 n)$, it can be done a fair amountof times reducing the false positive limit to some practical level(4^{-k}).

This test is extremely efficient as it does not do long operations. And also the result has high confidence. So it's used in some asymmetric cryptography.