# ACCURACY INCREASE IN DETERMINATION COMPOSITE NUMBER BY PROBABILISTIC PRIMALITY TESTS

**Agafonov A[1]., Balabanov A.[2]**

Technical University of Moldova , E-mail: balsoft@moldovacc.md

**Abstract:** Accuracy increasing problem became important after there were found so-called numbers of Carmichael, and it became evident that the simplest primality test based on Fermat's Little Theorem failed. Since then, many tests have been offered which have been more efficient than Fermat's, and the first successful results were made by Lehmer. The Miller-Rabin test is considered as most important probabilistic test with sufficient accuracy, complexity and computational costs. This article is meant to give some comparison between existing probabilistic primality tests in current use, and also to present results found in which accuracy may be increased.

**Key words**: Probabilistic tests, strong pseudoprime, indicative number, control number.

The most up-to-date tests are based on Fermat's little theorem, which shows that, if $p$ is prime, there does not exist a base $a < p$ with $(a, p) = 1$ such that $a^{p-1} - 1$ possesses a nonzero residue modulo $p$. If such base $a$ exists, $p$ is therefore guaranteed to be composite. However, the lack of a nonzero residue in Fermat's little theorem does *not* guarantee that $p$ is prime. The property of unambiguously certifying composite numbers, while passing some primes, makes Fermat's little theorem a compositeness test which is sometimes called the Fermat compositeness test.

Composite numbers known as Fermat pseudoprimes (or sometimes simply "pseudoprimes") have zero residue for some $a$s and so are not identified as composite. Worse still, there exist numbers known as Carmichael numbers (the smallest of which is 561) which give zero residue for *any* choice of the base $a$ relatively prime to $p$.

Carmichael numbers are relatively scarce; there are only 105212 Carmichael numbers $\leq 10^{15}$ ; these findings at once served as an impulse to find new more efficient tests with which to overcome this embarrassing fact. And so first results were presented by Lehmer, but the problem was only in that Carmichael numbers were identified as composite numbers, which in reality they were not.

Further improvement of probabilistic primality tests is referred to factorization on mathematical expression of Fermat's test and can be shown in following table.

*Table1*

| **Math. formulae** | **Test** | **Special numbers** | **Examples** |
|---|---|---|---|
| $^{*}a^{**n-1} \equiv 1 (\mathrm{mod}\, n$ | Fermat | Absolute pseudoprimes (Carmichael numbers) | 561,1105,1729 … |
| | | Fermat pseudoprimes | 341(***A=2), 217(A=5)… |
| $\left(a^{\frac{n-1}{2}} - 1\right)\left( \equiv 1 (\mathrm{mod}\, n)\right.$ | Euler-Lehmer | Euler Lehmer pseudoprimes | 341(A=2), 217(A=5)… |
| $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n$ | Solovay-Strassen | Pseudoprimes | 341(A=2), 781(A=5)… |
| | | Euler Pseudoprimes | 1373653(A=2 и3), 25326001(A=2,3 и 5)… |
| $n-1 = 2^{s} r$<br>$a^{r} \equiv 1 (\mathrm{mod}\, n)$<br>$a^{2^{j} r} \equiv -1 (\mathrm{mod}\, n)$ | Miller-Rabin | Pseudoprimes | 341(A=2),781(A=5)… |
| | | Strong Pseudoprimes | 1373653(A=2 и3)<br>25326001(A=2,3 и 5)... |

* $a$ is a number, called indicative, and is used as a base in certain tests to determine the character of n, where

** n is a tested number

*** A is so-called control number, which is needed to claim tested number as a composite.

A pseudoprime is a composite number which passes a test, or sequence of tests, that fail for most composite numbers. Unfortunately, some authors drop the "composite" requirement, calling any number that passes the specified tests a pseudoprime, even if it is prime. Pomerance, Selfridge, and Wagstaff (1980) restrict their use of "pseudoprime" to odd composite numbers. "Pseudoprime" used without qualification means Fermat pseudoprime.

Strong pseudoprime is a composite number that passes a test or sequence of tests for more than one indicative numbers.

There is an opinion that there is no longer any reason to use Solovay-Strassen test, because an alternative is available (the Miller-Rabin test) which is both more efficient and always at least as correct.

The most theoretical papers gives a recommendation to take a random base $a$ for testing number $n$ in a range from 2 'till $n-1$, but what shows up in practice is that it is much more effective, and hence more applicable, to use bases taken from initial row of numbers.

Our experiments proved their high efficiency just by one iteration, i.e. A=3.

As long as the Miller-Rabin test is a probabilistic test, there is an opportunity to pass into the determinative class in the case of using all indicative numbers in a range from 2 'till $2\log^2 n$.

Here the simple question is why not use just *prime* numbers as indicative? Actually, it is more than sufficient to take only all prime numbers from a given range, because even working with numbers $\approx 10^{1000}$ we never cross the boundary of known prime number, given in quite acceptable tables.

In conclusion, whether testing will pass from the probabilistic to the determinative class, will be true *only* in such case that the Riemann hypothesis be proved (officially), and while it remains as an open question, we believe another solution which, connected with the presence of strong pseudoprimes, may be possible if:

1. There will be found strong pseudoprime with the same exponent as number M or
2. There will be found an approximate dependence between number of iteration $k$ and strong pseudo prime length.

This dependence has the following appearance: $k = 0.5 \lg n$

According to numerical experiments, this dependence works right up to $10^{57}$; providing evidence that the number of iteration in this case, is less than if the Riemann hypothesis were proven to be true.

## REFERENCE


1. Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
2. Olejnik V.L. Methods of deriving of prime numbers - a flowing state - Chişinău.:Akta Akademia All, 1999.
3. Gelfond A.O. Solution of the equations in a whole numbers .-M.: Science, 1983.
4. Agafonov A.F. The developed probability algorithms of definition of a simplicity of number. - Kishinev: Materials of II International conference on computer science, 2002.
5. Shafarevich I.R. The theory number.-Moscow: Science, 1985.
6. " Introduction to cryptography "/under general edition of V.V.Jashchenko. - M.: The Moscow State University 2000.
7. Maslenikov A. Practical cryptography.-M.: SOLON-pres, 2003.