ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2018, Vol. 39, No. 7, pp. 1010–1015. © Pleiades Publishing, Ltd., 2018.

The Error Probability of the Miller–Rabin Primality Test

S. T. Ishmukhametov[1*], R. Rubtsova[1], and N. Savelyev[1***]**

(Submitted by F. M. Ablayev)

[1] *Institute of Computer Mathematics and Informational Technologies, Kazan (Volga region) Federal University, ul. Kremlevskaya 18, Kazan, Tatarstan, 420008 Russia*

Received December 6, 2017

Abstract—In our paper we give theoretical and practical estimations of the error probability in the well-known Miller–Rabin probabilistic primality test. We show that a theoretical probability of error 0.25 for a single round of the test is very overestimated and, in fact, error is diminishing with the growth of length of numbers involved by a rate limited with $\ln n/\sqrt{n}$.

DOI: 10.1134/S1995080218070132

Keywords and phrases: *Primality testing, Miller–Rabin primality test, the Rabin Theorem, probability error of primality testing.*

1. INTRODUCTION

The Miller–Rabin primality test MRT has a wide application in Cryptography to distinguish composite numbers from primes ones. Garry Miller in [1] suggested a deterministic polynomial test which was based on the unproved Riemann Hypothesis while Michael Rabin [2] refused from the use of the RH and obtained a modern version of the test which became probabilistic. The error probability α in the MRT depends on the number of iterations (called rounds) each of which is diminishing α in 4 times. More exactly, let n be an odd integer which we need to check for primality, and $n-1=2^s t$, where t is odd. At each iteration an individual integer a is chosen to check if some Boolean expression $R(a,n)$ holds:

$$R(a,n):\ n\mathrm{mod}a\neq 0\ \&\ a^t\mathrm{mod}n=1,\ \text{or},\ a^{t2^i}\equiv -1\mathrm{mod}n,\quad 0\leq i<s.$$

This a is called *the base of iteration*. If after k rounds with different bases $a_1,a_2,\ldots,a_k$ all counted values $R(a_1,n),R(a_2,n),\ldots,R(a_k,n)$ are true, then n is called probable prime (that is, prime with a possibility of small error not exceeding $1/4^k$). But if a base a is found such that $R(a,n)$ is false, then the testing n is definitely composite. The MRT improved some previous known primality test of Fermat and Solovay–Strassen [3, 4] but contrary to the last it was able to check correctly Carmichael integers that were composite but defined by error as prime [5]. Our investigation concerns the possible probability of the MRT errors. Practical experiments show a diminishing number of false application of the MRT for larger and larger integers involved. The real probability of error is much lesser that 0,25 in a single iteration and this probability is diminishing with the growth of considered integers. In our paper we show that the real probability of composite n to be defined as prime is less that 10^{-6} when $n>10^9$. This allows us to reduce the number of rounds required to successfully separate composite numbers from primes at an essentially lesser number of rounds.

The latter plays an important role in connection with the grow length of primes used in Cryptographical Protocols like as the RSA Ciphering Algorithm [6] and Elliptic Curves Algorithm [7, 8].

*E-mail: Shamil.Ishmukhametov@kpfu.ru
**E-mail: Ramilya.Rubtsova@kpfu.ru
***E-mail: savelyevno@gmail.com