ISSN 1066-369X, Russian Mathematics (Iz. VUZ), 2014, Vol. 58, No. 8, pp. 43–48. © Allerton Press, Inc., 2014.
Original Russian Text © Sh.T. Ishmukhametov, F.F. Sharifullina, 2014, published in Izvestiya Vysshikh Uchebnykh Zavedenii. Matematika, 2014, No. 8, pp. 53–59.

On Distribution of Semiprime Numbers

Sh. T. Ishmukhametov* **and F. F. Sharifullina****

Kazan (Volga Region) Federal University, ul. Kremlyovskaya 18, Kazan, 420008 Russia

Received January 31, 2013

Abstract—A semiprime is a natural number which is the product of two (possibly equal) prime numbers. Let y be a natural number and $g(y)$ be the probability for a number y to be semiprime. In this paper we derive an asymptotic formula to count $g(y)$ for large y and evaluate its correctness for different y. We also introduce strongly semiprimes, i.e., numbers each of which is a product of two primes of large dimension, and investigate distribution of strongly semiprimes.

DOI: 10.3103/S1066369X14080052

Keywords: *semiprime integer, strongly semiprime, distribution of semiprimes, factorization of integers, the RSA ciphering method.*

By *smoothness* of a natural number n we mean possibility of its representation as a product of a large number of prime factors. A B-*smooth* number is a number all prime divisors of which are bounded from above by B. The concept of smoothness plays an important role in number theory and cryptography.

Possibility of using the concept in cryptography is based on the fact that the procedure of decomposition of an integer into prime divisors (factorization) is a laborious computational process requiring significant calculating resources [1, 2]. The time necessary for factorization of a B-smooth number depends on B, only, not on the value of the number itself. The more the value of the constant B, the more time we need to decompose the number. The well-known two-key RSA ciphering method is based on factoring challenge, and the code key for the method is a large semiprime number. Therefore, investigation of distribution of numbers with various smoothness is an important problem for number theory and its applications in cryptography.

Now we introduce the concept of *strong semiprimeness*; we call the number n strongly semiprime if it is a product of two large prime divisors.

Definition. A number n is called *strongly semiprime* if n is a product of two, possibly equal, prime numbers p and q, and each of them is greater than $n^{1/4}$.

In the sense of smoothness, primes and semiprimes are opposites of smooth numbers. We note that for cryptography there are important, first of all, those strongly semiprimes in a neighborhood of which there is no smooth numbers, otherwise the problem of factorization could be solved too much faster making use of methods of the type of Lenstra's factorization algorithm on elliptic curves or Pollard's $(p-1)$-method ([2]). Therefore, we need to know distribution of not only semiprime numbers but smooth ones, too [3].

The main problem of the paper is investigation of distribution of semiprime and strongly semiprime numbers.

*E-mail: Shamil.Ishmukhametov@kpfu.ru.

**E-mail: sharifullinaff@gmail.com.