# Terms of primality of a number. New theorem 2 of prime number criteria

Mussabek Islamovich Akylbaev[1], Yessenbek Riskulovich Ushtenov[1], Rabiga Ibrachimovna Kenjebekova[1], Usmanali Musakulovich Ibragimov[2], Guljan Orazbekkizi Jetpisbaeva[2], Serik Sansizbaevich Dairbekov[3]

[1]Kazakhstan Engineering Pedagogical Universuty of Friendship of Nations, Djungildin Str. 13, Shymkent, 160019, Republic of Kazakhstan
[2]South Kazakhstan State University M.Auezov, Kazakhstan
[3]University "Syrdarija", M.Auezov street 11, Djetissai town, 160500, UKO, Republic of Kazakhstan

**Abstract.** We, the authors of this article, decided to analyze the criteria of primality of a number and draw a boundary between sufficient and necessary conditions for primality of a number. And concerning this topic we are giving a new theorem on a prime criterion. And that's why our theorem has its own place in the Theory of numbers in terms of representation of the nature, essence and the properties of prime numbers.

[Akylbaev M.I., Ushtenov Y.R., Kenjebekova R.I., Ibragimov U.M., Jetpisbaeva G.O., Dairbekov S.S. **Terms of primality of a number. New theorem 2 of prime number criteria.** *Life Sci J* 2014;11(6s):90-92] (ISSN:1097-8135). http://www.lifesciencesite.com. 15

**Keywords:** Number theory, terms of primality of a number, cryptography, the RSA system, a new theorem.

## Introduction

Primes play a special role in the theory of numbers because of the "fundamental theorem of arithmetic", which states that every composite number can be represented by one and only one way as a product of prime factors without considering the order of the factors [1], [2], [3], [4].

The first theorem, which asserts the existence of infinitely many primes, was already proved by Euclid in his "The Elements", book 9, sentence 20 [2], [5], [6].

A criterion of prime numbers is considered to be a number-theoretic property that is inherent in only primes and the existence of which can be established regardless of the preliminary screening of a prime number. A simple example is the ratio:

$$\sum_{m=1}^{m=n}\left\{\left[\frac{n}{m}\right]-\left[\frac{n-1}{m}\right]\right\} = 2 \quad (1.1)$$

is true if and only if n is a prime number. Since the summands are equal to 1, if m is a divisor of n, and are equal to zero, if this is not true; then the sum (final) represents the number of d (n), the divisors of n, and the equation d (n) = 2 characterizes primes.

2. Naturally, the formula (1), as well as many other criteria, is not suitable for practical purposes [7].

Number criterion of primality is a sufficient condition for the primality of a number. In addition to the sufficient conditions for number primality there are also the necessary conditions for it.

A prerequisite for primality of a number is the number-theoretic property of a number inherent in a greater extent to primes, but some composite numbers may have this property. Here are examples of the main prerequisites for primality of a number:

1. Every prime number greater than 3 can be represented as:

6k +1 or 6k-1. (1.2)

2. If p is a prime number, then the comparison

p2-1 ≡ 0 (mod 24) is true. (1.3)

The proofs of (1.2) and (1.3) are elementary and therefore we do not give them here.

3. If p is a prime number, then the comparisons

p ≡ a (mod p), (a, p) = 1 (1.4) ,

and a $^{p-1}$≡1 (mod p), (a,p)=1 are correct, (1.5)

that means that a remainder of the division of a $^{p}$ by p is 1, and accordingly the residue of the division of a $^{p}$ by p is equal to a.(Fermat's little theorem) [3].

There are also other necessary conditions for the.primality of a number.

A sufficient condition for the primality of a number is the number-theoretic property inherent in prime numbers and only in prime numbers.

Let's give the main examples of these conditions based on the following theorems:

1. Wilson's theorem. If p is a prime number, then the comparison (p-1)! +1 ≡ 0 (mod p) is true. (1.6)

Converse assertion is also true [9].

2. Leibniz's theorem. If p is a prime number, then the comparison (p-2)! -1 ≡ 0 (mod p) is true. (1.7)

Converse assertion is also true [8].

3.Sierpinski's theorem. If the number is of the p = 4k +1 form and the condition of the comparison is fulfiled:

$$\left(\frac{p-1}{2}\right)!^2 + 1 \equiv 0 \ (\mathrm{mod}\ p) \qquad (1.8)$$

then the number p is simple [8].

There are other theorems giving conditions for the primality. Checking numbers for their primality today is one of the most pressing problems in the number theory, as it relates to the use of prime numbers in cryptography to encrypt and decrypt data transmitted over public communication: the Internet, a cellular telephone, and others.

• There is also a method for determining the number for its primality using factorization (a step expansion of the number to primes), but today the factorization methods are much more difficult than the number primality tests. Primality tests fall into two categories: stochastic and determinate, that is unconditional ones.

There are many tests for primality of numbers, for example: Solovay-Strassen's test, Miller-Rabin's test, Adleman's algorithm, Pomerance's, Rumeli's , Lenstra's algorithm, the check of a number by Fermat's theorem, Lenstra-Cohen's algorithm, the algoritm of Adleman-Huang (1972) and others. All of the above-listed methods and algorithms are probabilistic. Up to 2002 deterministic primality tests only for special numbers were known: the test of Luke - Lehmer for Mersenne 's primes, Pepin's test for Fermat numbers, the test of Lucas - Lehmer - Riesel for Riesel 's numbers, Prot's theorem for Prot's numbers.

Only in 2002 the Indian mathematicians Agrawal, Kaya and Saxena suggested a deterministic algorithm to check numbers for simplicity. It was based on Fermat's little theorem and was modified in its faults. But it isn't practically applied, because it is multistaged and even after many improvements is estimated as O($\log^3 n$ ) of arithmetic operations (n is a number to be tested) [9], [10], [11].

To date, the RSA cryptography system uses multi-digit numbers which can not be checked for the primality of a number with 100 percent guarantee and can not be decomposed into prime factors (factorization). This is due to the fact that the verification of large numbers for primality requires a very large number of operations that even a super-modern computers can not afford [12].

The main part

In the connection with this topic we are giving a new theorem of a prime criterion which is being a banal case isn't found in the technical literature.

Theorem 2 of a prime criteria.

The author is Ushtenov Yessenbek Riskulovich, Certificate number 128 of February, 14 2013, registered in the Committee on Intellectual Property Rights of the Ministry of Justice of the Republic of Kazakhstan.

Theorem.

Let n be a positive odd number. If the condition is $\left[\frac{n}{3}\right]$ ! ≡/ 0 (mod n), (2.1) ,

then the assertion that n is a prime number is true. The only exceptions are the numbers n = 9 and n = 25.

Proof.

In accordance with the aforesaid "fundamental theorem of arithmetic" the canonical decomposition of the composite number **s** can be written as $s = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots p_n^{\alpha_n}$ , (2.2)

where $p_1, p_2, p_3 \ldots p_n$ are primes, $\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_n$ are powers of these numbers.

In formula (2.2) the composite number **s** can have two or more prime divisors and the smallest prime divisor of this number can be represented as $p_{k\,min}^{\alpha_n}$ ≥ 3 and, accordingly, the greatest common divisor (simple or composite) will look like:

k ≤ $\frac{s}{3}$ . In view of these statements it is possible to conclude that any composite number can have divisors only from 3 up to the $\left[\frac{s}{3}\right]$ number inclusively in the range of the natural sequence.

It is known that the prime number n has two trivial divisors of 1 n and itself, and it has no divider from the number 3 to the number $\left[\frac{n}{3}\right]$.

If the number $\left[\frac{n}{3}\right]$! Is divided by a prime n**,** the residue is necessarily equal to the number from 1 to n-1. If, however, the number n is a composite, then the remainder of the division of the number $\left[\frac{n}{3}\right]$! by n will be zero.

Based on the foregoing, we have the expression (2.1).

Let's consider the exceptional cases.

Let n=$p^r$ , where p is a prime, r is the power of this number.

In this case, the number n to satisfy the condition (2.1), the condition: $\left[\frac{p^r}{3}\right] \geq r \cdot p$. is necessary.

The examples show that the numbers n= $3^2$ =9 and n= $5^2$ =25 are exceptions to this theorem.

The theorem is proven.

We can make the following corollary from this theorem.

In determining the number for its primality the initial condition is the oddness of the determinate number, if it is a composite number, then the prime factors of this number will be only odd primes. On the basis of this judgment we can assert the following:

The number n is simple, if the condition:

$(2k_1+1)(2k_2+1)(2k_3+1)\cdot \ldots \cdot (2k_i+1) \equiv/ 0 \pmod n$, is true (2.3)

where $k_1=1$, $k_2=2$, $k_3=3$, … и $2k_i+1 \le \left[\frac{n}{3}\right]$.

Exceptions in the case of corollary (2.3) will form the numbers which don't subject to the condition $\left[\frac{p^r}{3}\right] \ge 2r\cdot p$. These exceptions are only three numbers: n = 9, n = 25 and n = 49.

## Conclusion

Of course, our theorem can not have a practical application in determining the primality of multi-digit numbers, and they are much more weaker than the theorem of the Indian mathematicians Agrawal, Kayaly and Saxen. But our theorem is stronger than the theorems of Wilson, Leibniz, and Sierpinski listed earlier in this article, by the fact that there are considerably fewer factors in our formula . And that's why our theorem has its own place in the Theory of numbers in terms of representation of thenature, essence and the properties of prime numbers.

**Corresponding Author:**

4/2/2014

Dr.Mussabek Islamovich Akylbaev
Kazakhstan Engineering Pedagogical Universuty of Friendship of Nations
Djungildin Str. 13, Shymkent, 160019, Republic of Kazakhstan

## References

1. Gauss, C. F., 1986. Disqnisitiones Arithmeticae, 1801. Springer, pp: 15-17.
2. Davenport, H., 1999. The Higher Arithmetic: An Introduction to the Theory of Numbers. Cambridge University Press, pp: 19-27
3. Vinogradov, U.M., 2009. Theory of numbers. Sankt-Peterburg "Land", pp: 15-48.
4. Nasterenko, Y.V., 2008. Theory of numbers. Publish centre "Akademiya". pp: 33-36.
5. Dirihle, L., 1936. Lectures on theory of numbers. Moscow, Leningrad: Scientific technical centre, pp: 21-22.
6. Ingham, A.E., 1990. The Distribution of Prime Numbers. Cambridge University Press, pp: 14-16.
7. Trost, E., 1953. Primzahlen. Basel, Birkhauser, pp: 52-54.
8. Seprinsky, V., 1963. What do we know and what we don't know about simple numbers. Moscow: State publishing physical-mathematics literature, pp: 51-53.
9. Vasylenko, O.N., 2003. Theoretic-numeral algorithms in cryptographs. Moscow, pp: 48-49.
10. Agrawal, M., N. Kayal and N. Saxsena, 2002. PRIMES is in P. Preprint, pp: 21-22.
11. Lenstra jr., H. W. and C. Pomerance, 2011. Primarily testing with Gaussian periods.
12. Akylbayev, M.I. and I.R. Ushtenov, 2014. New theorem about criteria of simple numbers. International magarine funcfional research, 1(2): 255-258.