ISSN: 2692-5206
AMERICAN ACADEMIC PUBLISHER
INTERNATIONAL JOURNAL OF MEDICAL SCIENCES

NEW METHODS FOR DETERMINING WHETHER A SUFFICIENTLY LARGE NATURAL NUMBER IS PRIME OR COMPOSITE

Jalolxon T. Nuritdinov

Lecturer of Kokand State Pedagogical Institute

Bexruzbek B. Nematov

Student of Kokand State Pedagogical Institute

Abstract: The theory of prime numbers holds an important place in mathematics and is widely applied in cryptography, algorithms, and many other fields. Determining whether large natural numbers are prime or composite requires considerable time and computational resources using traditional methods. This study introduces new algorithmic methods and approaches for identifying prime numbers, analyzing their speed, efficiency, and accuracy. These new methods are shown to be not only theoretically significant but also applicable in practical computational fields. Simplified rules for divisibility by prime numbers are provided, and a method for deriving these divisibility rules is also explained. This work will be of great importance to engineers and researchers in mathematics and computer science who work with large numbers.

Keywords: Sufficiently large natural number, prime number, numeral systems, divisibility rules.

We present the results of our research aimed at finding a more efficient method than the commonly known approach for determining whether a given natural number is prime or composite.

To determine if a natural number is prime or composite, the following simple verification steps need to be performed:

1. The binary representation of the given natural number is examined, and the following assertion holds true:

Theorem. If there is periodicity in the digits of the natural number represented in the binary system, then the number is definitely composite.

This theorem can be demonstrated through several examples.

Example 1. The number 221 in binary is 11011101_2, which shows periodicity, meaning the combination 1101 repeats twice. To convert this number into the decimal system, we expand it in powers of two:

$$11011101_2 = 1\times2^0 + 0\times2^1 + 1\times2^2 + 1\times2^3 + 1\times2^4 + 0\times2^5 + 1\times2^6 + 1\times2^7.$$

Next, we make the following transformations:

ISSN: 2692-5206
AMERICAN ACADEMIC PUBLISHER
INTERNATIONAL JOURNAL OF MEDICAL SCIENCES

$11011101_2 = 1\times2^0 + 0\times2^1 + 1\times2^2 + 1\times2^3 + 1\times2^4 + 0\times2^5 + 1\times2^6 + 1\times2^7$

$= 1\times2^0 + 0\times2^1 + 1\times2^2 + 1\times2^3 + 2^4(1\times2^0 + 0\times2^1 + 1\times2^2 + 1\times2^3)$

$= (1\times2^0 + 0\times2^1 + 1\times2^2 + 1\times2^3)(1 + 2^4)$.

Therefore, we can conclude that this number is not prime.

Example 2. If the number 119 in binary, written as 1110111_2, is prefixed with a 0, its value doesn't change: $119 = 01110111_2$. We can observe that the combination 0111 repeats twice. From this, we can conclude that 119 is a composite number.

The theorem above is only a necessary condition. That is, if a number's binary representation does not exhibit periodicity in its digits, we cannot conclude that the number is prime. We will explain our reasoning with the following examples.

Examples 3. If we look at the number 123 in binary, which is 1111011_2, we don't see any periodicity, yet this number is composite.

Examples 4. In the number 469 in binary, which is 111010101_2, the combination 01 is periodic, but the combination 111 disrupts the periodicity. Despite this, the number is composite.

As we can see from the above examples, the lack of periodicity in a number's binary representation does not allow us to conclusively say whether the number is prime or composite, so we must proceed to the next step of verification.

2. Let a be an odd number. We can rewrite this number as:

$$a = (a - 3) + 3$$

Since a is an odd number, the number a-3 will be even and divisible by 2 without a remainder. Therefore, we have:

$a = \frac{a-3}{2} \times 2 + 3$.

Let $a_1 = \frac{a-3}{2}$, which is an even number, so it can be divided by 2 again. If a_1 is odd, we rewrite it as:

$a = ((a_1 - 3) + 3) \times 2 + 3$

The number $\frac{a-3}{2} - 3$ is also even and divisible by 2 without a remainder, resulting in the number $a_2 = \frac{\frac{a-3}{2}-3}{2}$.

Thus, we have:

ISSN: 2692-5206
AMERICAN ACADEMIC PUBLISHER
INTERNATIONAL JOURNAL OF MEDICAL SCIENCES

$$a = ((a_2 \times 2) + 3) \times 2 + 3$$

We continue this process until it becomes convenient to check whether the number a_i is divisible by 3. If a_i is divisible by 3 without a remainder, then the number a is also divisible by 3, meaning it is not a prime number. Using this method, we can test whether a given odd number, ending in 1, 3, 7, or 9, is divisible by prime numbers. In performing these checks, the following divisibility rules will be useful.

Divisibility rule for 3: If the sum of the digits of a given number is divisible by 3 without a remainder, then the number itself is divisible by 3 without a remainder.

Divisibility rule for 7: If you take the last digit of the given number, multiply it by 2, and subtract this from the rest of the number after removing the last digit, and the result is divisible by 7 or equals 0, then the original number is divisible by 7 without a remainder.

Example 5. The given number is 406.

4 0 6

40-6×2=28 .

28:7=4.

Divisibility rule for 11: If the difference between the sum of the digits in even positions and the sum of the digits in odd positions is divisible by 11 without a remainder or equals 0, then the number itself is divisible by 11 without a remainder.

Divisibility rule for 13: If you multiply the last digit of a given number by 4, then add this result to the rest of the number after removing the last digit, and the result is divisible by 13 without a remainder, then the number is divisible by 13.

Example 6. The given number is 195.

19+5×4=39,

39 is divisible by 13, so 195 is divisible by 13.

195:13=15

If the given number is very large and the above method is applied, the resulting number, obtained by removing the last digit and adding the last digit multiplied by 4 to the remaining number, will also be large. Therefore, we apply this method to the next resulting number, and then again to the next resulting number, and so on. We repeat this process periodically until we get a number that is easy to divide by 13.

Example 7. The given number is 1607502.

160750+2×4=160758,

ISSN: 2692-5206
AMERICAN ACADEMIC PUBLISHER
INTERNATIONAL JOURNAL OF MEDICAL SCIENCES

16075+8×4=16107,

1610+7×4=1638,

163+8×4=195,

19+5×4=39

This method also applies to the divisibility rule for 7.

Divisibility rule for 17: If you multiply the last digit of a given number by 5 and subtract this from the rest of the number after removing the last digit, and the result is divisible by 17 without a remainder or equals 0, then the number is divisible by 17.

Example 8. The given number is 425.

42-5×5=17

Thus, the number 425 is divisible by 17.

425:17=25

Divisibility rule for 19: If you multiply the last digit of the given number by 2 and add it to the rest of the number after removing the last digit, and the result is divisible by 19 without a remainder, then the number is divisible by 19.

Example: The given number is 228.

22+2×8=38.

38 is divisible by 19, so 228 is divisible by 19.

228:19=12.

Divisibility rule for 23: If you multiply the last digit of the given number by 7 and add it to the rest of the number after removing the last digit, and the result is divisible by 23, then the number is divisible by 23.

Divisibility rule for 29: If you multiply the last digit of the given number by 3 and add it to the rest of the number after removing the last digit, and the result is divisible by 29, then the number is divisible by 29.

Divisibility rules for prime numbers larger than 29 are similar to those for 13, 17, 19, and 23. However, the number used to multiply the last digit and whether it is added or subtracted from the rest of the number differs for each prime. Below are the numbers to multiply the last digit by for larger primes, and whether to add or subtract:

- For 31: Multiply by 3 and add to the rest of the number.

ISSN: 2692-5206
AMERICAN ACADEMIC PUBLISHER
INTERNATIONAL JOURNAL OF MEDICAL SCIENCES

- **For 37:** Multiply by 11 and subtract from the rest of the number.

- **For 41:** Multiply by 4 and subtract from the rest of the number.

- **For 43:** Multiply by 13 and add to the rest of the number.

- **For 47:** Multiply by 14 and subtract from the rest of the number.

- **For 53:** Multiply by 16 and add to the rest of the number.

- **For 59:** Multiply by 6 and add to the rest of the number.

- **For 61:** Multiply by 6 and subtract from the rest of the number.

References:

1. Yagudayev B.Y. *In the World of Amazing Numbers*. "O'qituvchi", Tashkent, 1973, 232 pages.

2. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. *Fundamentals of Cryptography: Textbook*, 2nd edition. Moscow: Helios ARV, 2002, 480 pages.

3. Vasilenko O. N. *Number-Theoretic Algorithms in Cryptography*. Moscow, MCCME, 2003, 328 pages.