Journal of Modern Technology and Engineering
Vol.4, No.3, 2019, pp.190-194

ALGORITHM ON FINDING TWIN PRIME NUMBERS

Melike Karatay[1], **Atakan Aylanç**[2], **Serkan Özkan**[2*]

[1]Ege University, İzmir, Turkey
[2]Yaşar University, İzmir, Turkey

Abstract. Prime numbers are widely used in many fields from engineering to medicine, especially cryptology. The security of cryptographic systems is based on difficult mathematical problems such as the factorization problem used in RSA system. The infinity of prime numbers has been proven but the infinity of twin primes, which is a subset of prime numbers, is still unproven. In this study, an algorithm that finds twin primes smaller than $6a + 1$ for any given $a \in \mathbb{Z}^+$ is proposed. In addition, the proposed algorithm was compared with the sieve of Eratosthenes in terms of performance and memory, and the results were discussed.

Keywords: Twin prime numbers, sieve algorithms, algorithm complexity, cryptology.

AMS Subject Classification: 11A41, 11Y11, 11Y16.

Corresponding author: Serkan, Özkan, Yaşar University, Bornova, İzmir, Turkey, Tel.: +905342811392, e-mail: *serkan9448@gmail.com*

Received: 30 July 2019; Accepted:12 November 2019; Published: 25 December 2019.

1 Introduction

Cryptographic systems need very large prime numbers to ensure the intended security. The usage of prime numbers in critical areas like cryptology has increased the importance of these numbers. For this reason, many studies have been made about finding prime numbers and distribution of prime numbers. At the present time, studies on prime numbers still continue.

For $\forall i \in \mathbb{N}$, if $p_i \in Z^+$ is only divisible by 1 and itself, then p_i is called a prime number. The set of prime numbers is denoted by P. Twin prime numbers are, $p_i, p_{i+1} \in P$ where $p_{i+1} - p_i = 2$. The infinity of the twin primes is a conjecture, as it still unproven. Although the infinity of the twin prime numbers can not been proved, an important progress has been made in this regard. D.A. Goldston, J. Pintz, C.Y. Yıldırım and Y. Zhang received the Cole Award for their work on twin prime numbers (Goldston et al., 2006). In addition, Y. Zhang is proved that $\liminf_{i\to\infty}(p_{i+1} - p_i) < 70.000.000$ (Zhang, 2014). After these two important improvements, studies have been made to reduce the k value in $\liminf_{i\to\infty}(p_{i+1} - p_i) \leq k$. J. Maynard proved this expression for $k = 600$ (Maynard, 2013). Finally, it was proved for $k = 246$ within the scope of the Polymath Project initiated by T. Tao to prove the twin prime conjecture (Polymath, 2014).

Also many more studies have been made to find the twin primes. A study on finding twin primes was made in (Nuriyev & Sadıgova, 2002). When this study is examined, it is seen that the algorithm for finding twin prime numbers is missing. In this study, the new algorithm for finding twin prime numbers is written by using the formulas given in the previous study. Then, the algorithm and sieve of Eratosthenes were coded in C programming language and the two programs were compared in terms of performance and memory.

2 Prime Numbers

Prime numbers can be defined as a number that can be only divisible by 1 and itself, which means a positive natural number that has two divisors. 2 is the smallest prime number and only prime number that is even. If a number is not a prime number, then the number is called composite number. From the fundamental theorem of arithmetic, n is a composite number and the elements of the set P is p_i, where $i \geq 1$ and $k_i \in \mathbb{Z}^+$; n can be expressed as $n = p_1^{k_1}.p_2^{k_2}...p_t^{k_t}$. Also, from Euclid's theorem, the set P has an infinite number of elements.

Theorem 1. *There are infinitely many prime numbers.*

There are different classifications of prime numbers which can be expressed in unique forms. The most known prime number classes are Mersenne primes and Fermat numbers. While $n \in \mathbb{N}$, if 2^n–1 is a prime, then these primes is called Mersenne primes. The largest Mersenne prime known to date is $2^{82589933} - 1$, a number with 24.862.048 digits (`http://www.mersenne.org/primes/press/M82589933.html`). In 1637, Fermat formed a unique prime numbers similar to Mersenne primes. For $\forall n, s \in \mathbb{N}$, numbers that can be expressed as $F_s = 2^{2^n} + 1$ is Fermat's number.

To check whether a number is prime or not, prime tests can be used such as Fermat's primality test, Miller-Rabin primality test and AKS. Apart from testing the primality of a single number, it is also a matter of a great interest to find all prime numbers smaller than a specified value. Finding prime numbers smaller than a small limit is not a major problem. However, with the growth of the limit value, the prime numbers are getting bigger. Because of that more efficient algorithms are required. One of the known methods to quickly find prime numbers for large limit values is the sieve of Eratosthenes. Prime number sieves work by creating a list of all integers, subtracting composite numbers with a particular algorithm from the generated list, until only prime numbers remain. The sieve of Eratosthenes is the basis of the sieve algorithms. After the sieve of Eratosthenes Sundram and higher-performing Atkin's sieve algorithms emerged (Ramaswami Aiyar, 1934; Atkin & Bernstein, 2004).

Sieve of Eratosthenes: To find all prime numbers smaller than $N \in \mathbb{Z}^+$, firstly all integers from 2 to N are listed. The first number in the list is 2 and it's a prime number. All the multiples of 2 greater than 2, are deleted from the list. The next number that has not been deleted in the list is 3 and it's a prime. All the multiples of 3 greater than 3, are deleted from the list. The next number that has not been deleted in the list is 5. Number 4 was ommited because it was deleted in the first step since it is a multiple of 2. When the same operation is performed for all numbers, only the prime numbers remain in the list (Crandall & Pomerance, 2006).

3 Twin Prime Numbers

If the difference between two consecutive prime is 2, these numbers are called twin prime numbers. Examples are 3-5, 5-7, 11-13. Even though a method for finding twin prime numbers is not proposed, there are many studies on the distribution of twin prime numbers. One of these studies is also known as Elliot-Halberstam conjecture.In addition, Euler proved in 1737 that, for $\forall i \in \mathbb{N}$ and p_i is the series of prime numbers, the harmonic series $\sum_{i=0}^{\infty} 1/p_i$ is divergent. Also, V. Brun proved that, for $s_2 = \{i | p_{i+1} – p_i \leq 2, \forall p_i \in P\}$, the sum $\sum_{i \in s_2} 1/p_i$ is finite. But in order for this expression to be infinite series, first of all, twin primes conjecture must be correct. As can be seen here, there is a big difference between distribution of prime numbers and the distribution of twin prime numbers.

The largest twin prime numbers found so far are $2996863034895, 2^{1290000} \pm 1$ numbers found in 2016 (`https://primes.utm.edu/primes/page.php?id=122213`). The methods mentioned in the section "prime numbers" are used to find prime numbers. There is no common method used in the literature to find twin primes. For simplest way to find twin prime numbers, Sieve of Eratosthenes can be used by checking the difference between consecutive prime numbers. Besides this method, twin prime numbers can be found by performing the same process in other sieve algorithms.

Let $K = \{k|l_1 = 6k+1 \in P$ and $l_2 = 6k-1 \in P\}$. In this case the following theorems are correct (Nuriyev & Sadıgova, 2002).

Theorem 2. *$\mathbb{N}$ is set of natural numbers. For $\exists m, n \in \mathbb{N}$, $k = 6mn \pm m \pm n \Rightarrow k \notin K$.*

Theorem 3. $M_j = \{k|k = 6mn \pm m \pm n, m = j, j, n \in \mathbb{N}\}$

$$= \{k|k = (6j-1)n \pm j, n \in \mathbb{N}\} \cup \{k|k = (6j+1)n \pm j, n \in \mathbb{N}\}$$

and $A_i = \{k \in \mathbb{N}|6i^2 - 2i \leq k < 6(i+1)^2 - 2(i+1), i \in \mathbb{N}\}$, $A_i \setminus (M_i \cap A_i) = P_i$ then $P_i \subset K$.

3.1 The Algorithm

Given in theorem 2, for $m, n \in Z^+$ we are trying to find k = 6mn ± m ± n. Since the minimum equality we can get is k = 6mn − m − n, it is quite clear that we have to try different m and n's while $6mn-m-n \leq k$. For $k = 6mn–m–n$, we can rewrite the equation as $n = (k+m)/(6m-1)$ which gives the maximum possible value of n for any given k and m. To reduce repetition we start the value n from m in every iteration. So in the first step of each iteration values of m and n will be equal, thus we can get $6m^2 - 2m \leq k$. If we consider the equality of $6m^2 - 2m = k$, we can get $m = (-4 + \sqrt{4+24k})/12$, which is the upper boundary for m. As a result of these calculations the boundaries for m and n are; $1 \leq m \leq (-4 + \sqrt{4+24k})/12$ and $m \leq n \leq (k+m)/(6m-1)$. With this boundaries all the twin primes up to $6k+1$ can be found. The value $a > 3$ is any integer number and the desired upper bound for value k.

```
Start
Enter the a value
for $k = 3$ to a do
          flag = true
          for $m = 1$ to ceil($(-4 + \sqrt{4+24k})/12$) do
              for $n = 1$ to $(k+m)/(6m-1)$ do
                  if ($6mn + m + n = k$ or $6mn + m - n = k$ or $6mn - m + n = k$ or $6mn + m + n = k$)
                      flag = false
                      $m = k + 1$
                      break;
          if (flag = true)
             print "$6k - 1$ and $6k + 1$ are twin primes" End
```

4 Result and Analysis

The algorithm for finding the twin numbers given in section 3 and the sieve of Eratosthenes's algorithm is written in C programming language. Both programs were run on a computer with i7-7700HP CPU, 2.8 GHz and 8192 MB RAM. Figure 1. shows the performance evaluation of the programs with twin prime numbers up to 300.000. The proposed algorithm up to 50.000 was found to be faster than the sieve of Eratosthenes. In numbers greater than 50.000, it operates about 1 second slower than the sieve of Eratosthenes. In addition, while the proposed algorithm can find twin prime numbers up to 300.000, in a conventional C program, sieve of Eratosthenes

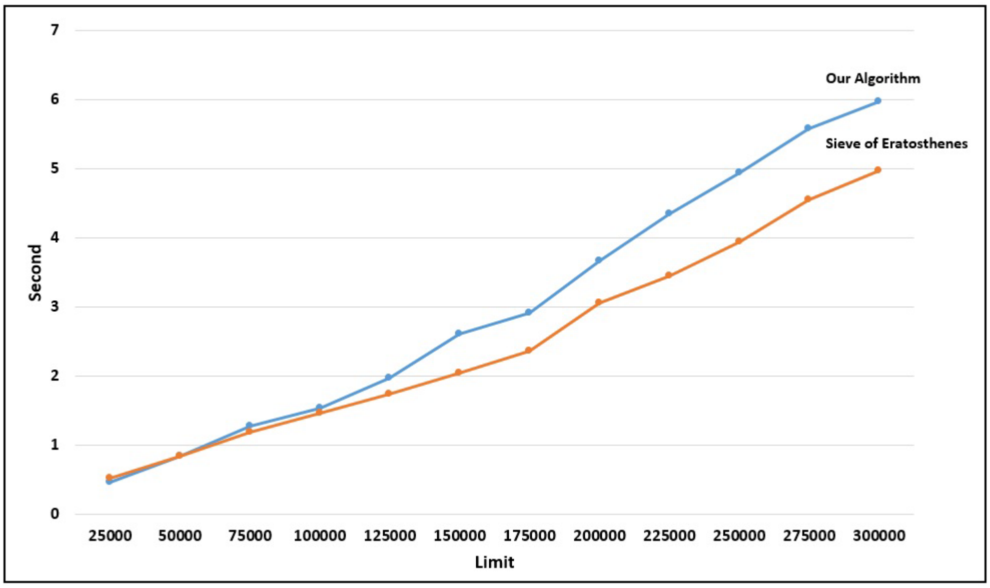

Figure 1: Performance comparison of proposed algorithm and sieve of Eratosthenes.

algorithm can not find twin prime numbers for boundaries greater than 300.000 due to the memory requirements.

The sieve of Eratosthenes can be thought to be more efficient after a certain point, but while the sieve of Eratosthenes is finding twin prime numbers, it must keep all integers up to specified limit value in the memory. The fact that the sieve of Eratosthenes could not find the twin prime numbers after 300.000 is because of the memory problem it creates. The proposed algorithm does not require a large amount of memory space. On a computer with high computing power, it can perform operations faster, since there is no need for memory space.

When a change is made on the proposed algorithm by storing all numbers up to the limit value in the memory, it is seen that the performance of both programs for the boundary of 300.000 gives approximate results. However, one of the most important features of the proposed algorithm is that it does not require a large memory space.

5 Conclusion

At present, there is no known algorithm for finding twin prime numbers. The proposed algorithm finds all twin prime numbers up to a specified value. The sieve of Eratosthenes is a method used to find prime numbers, but twin prime numbers can be found by adding additional conditions to the algorithm. When the sieve of Eratosthenes is compared with the proposed algorithm, it is seen that there is no significant performance difference between them.

Beside performance, there is a memory space that programs need. In the proposed algorithm, no data storage process is performed. However, in the sieve of Eratosthenes, all positive integers up to the specified upper limit should be kept in memory. In terms of memory requirement, the proposed algorithm is far better than the sieve of Eratosthenes. In future studies, the algorithm proposed in this study will be optimized in terms of performance by reducing its complexity. In addition, contributions will be made to the twin prime conjecture by using the proposed algorithm.

6 Acknowledgement

We would like to thank Prof. Dr. Urfat Nuriyev for helping us to work.

References

Atkin, A., & Bernstein, D. (2004). Prime sieves using binary quadratic forms. *Mathematics of Computation*, *73*(246), 1023-1030.

Crandall, R., & Pomerance, C.B. (2006). *Prime numbers: a computational perspective* (Vol. 182). Springer Science & Business Media.

Goldston, D. A., Motohashi, Y., Pintz, J., & Yıldırım, C. Y. (2006). Small gaps between primes exist. *Proceedings of the Japan Academy, Series A, Mathematical Sciences. 82*(4), 61-65.

http://www.mersenne.org/primes/press/M82589933.html. Access Date: 29/11/2019.

https://primes.utm.edu/primes/page.php?id=122213. Access Date: 29.11.2019.

Maynard, J. (2013). Small gaps between primes. *Annals of Mathematics*, 383-413.

Nuriyev, U.G., & Sadıgova, H.G. (2002). Nuriyev, U.G., Sadıgova, H.G. (2002). Twin on prime numbers. *Math. World,* 11 (in Turkish)

Polymath, D.H.J. (2014). The "bounded gaps between primes" Polymath project-a retrospective. arXiv preprint arXiv:1409.8361.

Ramaswami Aiyar, V. (1934). Sundaram's sieve for prime numbers. *The Mathematics Student*, *2*(2), 73.

Zhang, Y. (2014). Bounded gaps between primes. *Annals of Mathematics*, 1121-1174.