ISSN 1512-1232

On finding a prime number following the given prime

Tsabadze Teimuraz

Georgian Technical University, 77 Kostava Str. Tbilisi 0175, Georgia

Prime numbers are such beings
who are always inclined
hide from the explorer
Herman Wayl (1885-1955)

Abstract
This paper introduces one approach for a searching a prime number following the given prime number. The essence of the proposed approach is as follows. A sequence of two-element sets is constructed consisting of numbers enclosed between numbers that are multiples of three. The first set of the sequence contains the given prime number. Then the odd number of the next member of the introduced sequence is examined. Criteria for determining whether an odd number is composite or not are proposed. If it is composite, we pass to the study of the odd number of the next member of the sequence. If it is not composite, then it is the required prime number. The proposed approach is theoretically substantiated. In particular, two propositions are proved and algorithms for its implementation are elaborated.

Keywords: *Prime number, Composite odd number, Sequence of two-element sets, Algorithm, Indicator.*

1. Introduction

As you know, a prime number is an integer that has exactly two distinct divisors. Despite the elementary nature of their definition, these numbers introduced a number of problems, many of which have not been resolved so far (see the epigraph to this article). Since the time of Euclid, the problems of prime numbers have occupied the best mathematical minds. Suffice it to mention such luminaries of mathematics who dealt with this topic, such as Euclid, Eratosthenes, Fermat, Gauss, Euler and many others.

Currently, interest in this topic does not subside, in addition to purely theoretical, there is also great practical interest. Primes are used in many fields, to mention for example the importance of primes in networking, see e.g. [1,5]. Securing communication between two devices is achieved using primes since primes are the hardest to decipher, see the same sources [1, 5].

Of particular interest to researchers are twin primes, which are to some extent related to our work, see e.g. [2,3].

In the presented work, we set the task of finding the first prime prime number that follows a given prime number.

The article contains 5 sections. This section includes several introductory sentences as well as a general description of the proposed approach. The second section provides a detailed description of the proposed approach including various options. It also includes a theoretical basis that justifies the scheme for finding the next prime number. Two propositions are proved and algorithms are elaborated for implementing the considered approach. The third section is devoted to the specific numerical example illustrating the operation of the proposed approach. In Section 4 a brief comparative analysis of the two works closest in terms of subject matter with our approach is

ISSN 1512-1232

carried out. Section 5 summarizes the main content of the article and outlines possible prospects for applications of the proposed approach.

1.1 General description of the proposed approach

The essence of the proposed approach is as follows. Let a prime number $p > 3$ be given. It is easy to find a natural number k such that

$$3k < p < 3k + 3. \tag{1}$$

Pafnuty Chebyshev proved that between any natural numbers n and $2n$ there must be a prime number. It follows that the search area for the prime number following p is limited by the interval $[p+2, 2p-1]$. We consider a sequence of intervals whose start and end values are multiples of three and the first term of the sequence contains p and the last term contains $2p$-1. The sequence will look like this - $[3k, 3(k+1)]$. Based on the already defined search area, the number of intervals in the sequence will be finite. It is clear that within each interval of the sequence there will be two numbers – one is even and the other is odd. Our goal is to find out whether an odd number is composite or not. If it is not composite, it is a prime number and the process is complete. If it is composite, then we pass to consideration of the next interval of our sequence.

2. The approach itself.

As mentioned above, we consider two numbers from each member of the sequence of intervals $[3k, 3(k+1)]$. From this we obtain the following sequence of two-element sets:

$$\{3k + 3(s-1) + 1, 3k + 3(s-1) + 2\},\ s = 1, 2, \ldots. \tag{2}$$

According to (1), the given prime number p belongs to the sequence (2) for s=1. For further presentation we will use the following indicator:

$$\mathrm{I}_{\langle s \rangle} = \begin{cases} 1, & \text{iff } s \text{ is even} \\ 0, & \text{otherwise} \end{cases}. \tag{3}$$

So, the given prime number belongs to the set $\{3k+1, 3k+2\}$, s =1. Two cases are possible here.

I. $p = 3k + 1$.

Thus, p represents the first member of the set $\{3k+1, 3k+2\}$. It is easy to see that the odd number in the next set (s =2) will be 4 units greater than the odd number in the first set and will be the second member of the second set with value p+4. The odd number in the next set (s =3) will be 2 units greater than the odd number in the second set and will be the first member of the third set with value p+6.

In general, an odd number in the s-th set is expressed by the following iterative formula:

$$a_1 = p,\ a_s = a_{s-1} + 2\left(1 + \mathrm{I}_{\langle s \rangle}\right),\ s = 2, 3, \ldots. \tag{4}$$

Here $\mathrm{I}_{\langle s \rangle}$ is determined by expression (3).

ISSN 1512-1232

Based on the above reasoning and expression (4) in the set $\{3k+4=p+3, 3k+5=p+4\}$,(*s*=2), *p*+4 will be odd. The odd number *p*+4 is composite if and only if when

$$p+4 = (2n+1)(2m+1) = 4mn + 2(m+n) + 1, \quad m,n = 1,2,\ldots . \tag{5}$$

Then the even number $p+3 = 4mn + 2(m+n)$, i.e.

$$2mn + m + n = (p+3)/2. \tag{6}$$

This implies

$$m = \frac{(p+3)/2 - n}{2n+1} . \tag{7}$$

Since *m* is a natural number, the inequality $(p+3)/2 - n \geq 2n+1$ must hold, hence

$$n \leq \frac{(p+3)/2 - 1}{3}. \tag{8}$$

The proposed approach provides for the identification of all possible pairs (*n*, *m*) with the help of which it turns out whether 3*k* + 5 is composite or not. Based on formula (7), we introduce the function

$$m(n_i) = \frac{(p+3)/2 - n_i}{2n_i + 1}, \; n_i = i, \; i = 1,2,\ldots . \tag{9}$$

Obviously, the range of *n* is extremely important for our study. The inequality (8) gives the upper bound of that range, however, there is a possibility of a significant reduction of that range.

Proposition 1. *When calculating pairs (n, m), it suffices to restrict ourselves to only those n for which*

$$n \leq \frac{\sqrt{p+4} - 1}{2} \tag{10}$$

Proof:

Let us rewrite equality (5) as follows.

$$(p+3)+1=(2n+1)(2m+1), \quad m,n = 1,2,\ldots . \tag{11}$$

It is clear that this equality is equivalent to equality (6) and, under its conditions, formula (7) is valid again. We want to show that it suffices to consider those values of *n* that are defined by inequality (10) or, which is the same, .

$$2n+1 \leq \sqrt{p+4} . \tag{12}$$

If for some *n* satisfying (12) we find an integer *m*, then from (11) it follows that the odd number *p* + 4 is composite and we proceed to consider the next set of the sequence (2).

Now suppose that for all *n* satisfying inequality (12), all corresponding values of *m* will be fractional. Let us show that for any *n* satisfying the inequality

$$2n+1 > \sqrt{p+4} , \tag{13}$$

the corresponding values of *m* will also be fractional. Assume the opposite, that is, there is *n*, which has corresponding integer *m* (calculated by formula (7)) . So we have found natural numbers *n* and *m* that satisfy equality (6). It is clear that if a pair (*n, m*) satisfies equality (6), then the pair (*m, n*) also satisfies that equality. From formula (7) we easily obtain

ISSN 1512-1232

$$m = \frac{(p+3)/2 - n}{2n+1} \tag{14}$$

From (11) and (13) it follows that

$$2m+1 \le \sqrt{p+4}\,. \tag{15}$$

But it is known that for such m all n are fractional and the pair (m, n) cannot satisfy equality (6). We got a contradiction. □

Given in (10), the new upper limit of the range of values n is much less than ((*p*+3)/2-1) / 3 for large p and the inequality

$$\frac{\sqrt{p+4}-1}{2} < \frac{(p+3)/2-1}{3}$$

takes place when $p > 5$.

Algorithm 1

Here and further on, symbol [ ] denotes an integer part of a number. According to inequality (10) $i = \overline{1, \left[\left(\sqrt{p+4}-1\right)/2\right]}$.

Using formula (9), we fill in the following table

Table1

n_i	$m(n_i)$
1	$m(1)$
2	$m(2)$
…	…
$\left[\left(\sqrt{p+4}-1\right)/2\right]$	$m\left[\left(\sqrt{p+4}-1\right)/2\right]$

If $m(i)$ is a fraction, we proceed to the calculation of $m(i+1)$. If no $m(i)$ takes an integer value, then equality (6) is not satisfied and p+4 is the prime number following the given p. This is where the process ends. If an integer $m(i)$ is encountered, then it becomes clear that the pair $(n_i, m(i))$ will satisfy equality (6), which confirms that $p + 4$ is a composite number and, using formula (4), we proceed to consider the next set of sequence (2).

II. $p = 3k + 2$.

Thus, p represents the second member of the set $\{3k+1, 3k+2\}$. It is easy to see that the odd number in the next set (s =2) will be 2 units greater than the odd number in the first set and will be the first member of the second set with value p+2. The odd number in the next set (s =3) will be 4 units greater than the odd number in the second set and will be the second member of the third set with value p+6.

In general, an odd number in the s-th set is expressed by the following iterative formula:

$$b_1 = p,\ b_s = b_{s-1} + 2\left(2 - \mathrm{I}_{\langle s \rangle}\right),\ s = 2, 3, \ldots . \tag{16}$$

Here $\mathrm{I}_{\langle s \rangle}$ is determined by expression (3).

Based on the above reasoning and expression (16) in the set $\{3k+4 = p+2, 3k+5 = p+3\}$,($s$=2), p+2 will be odd. The odd number p+2 is composite if and only if when

$$p+2 = (2n+1)(2m+1) = 4mn + 2(m+n) + 1, \quad m,n = 1,2,\ldots . \tag{17}$$

ISSN 1512-1232

Then the even number p+3 = 4mn + 2(m+n)+2, i.e.

$$(p+3)/2=2mn + m+n+1. \tag{18}$$

This implies

$$m=\frac{(p+3)/2-n-1}{2n+1}\ . \tag{19}$$

Since m is a natural number, the inequality $(p+3)/2-n-1\geq 2n+1$ must hold, hence

$$n\leq\frac{(p+3)/2-2}{3}. \tag{20}$$

As in the previous case, we should identify all possible pairs (n, m) with the help of which it turns out whether 3k + 4 is composite or not. Based on formula (19), we introduce the function

$$m(n_i)=\frac{(p+3)/2-n_i-1}{2n_i+1},\ n_i=i,\ i=1,2,\ldots\ . \tag{21}$$

Obviously, the range of n is extremely important for our study. The inequality (20) gives the upper bound of that range, however, there is a possibility of a significant reduction of that range.

Proposition 2. *When calculating pairs (n, m), it suffices to restrict ourselves to only those n for which*

$$n\leq\frac{\sqrt{p+2}-1}{2} \tag{22}$$

The proof of this Proposition is similar to the proof of Proposition 1.

Given in (22), the new upper limit of the range of values n is much less than ((p+3)/2-2) / 3 for large p and the inequality

$$\frac{\sqrt{p+2}-1}{2}<\frac{(p+3)/2-2}{3}$$

takes place when p > 7.

Algorithm 2

According to inequality (22) $i=\overline{1,\left[\left(\sqrt{p+2}-1\right)/2\right]}$. Using formula (21), we fill in the following table

Table 2

n_i	$m(n_i)$
1	$m(1)$
2	$m(2)$
…	…
$\left[\left(\sqrt{p+2}-1\right)/2\right]$	$m\left[\left(\sqrt{p+2}-1\right)/2\right]$

If $m(i)$ is a fraction, we proceed to the calculation of $m(i+1)$. If no $m(i)$ takes an integer value, then equality (18) is not satisfied and p+2 is the prime number following the given p. This is where the

ISSN 1512-1232

process ends. If an integer $m(i)$ is encountered, then it becomes clear that the pair $(n_i,m(i))$ will satisfy equality (18), which confirms that $p + 2$ is a composite number and, using formula (16), we proceed to consider the next set of sequence (2).

3. Example

Let a prime number 941 be given. It is easy to determine its place in the sequence (2): $\{3k+3(s-1)+1, 3k+3(s-1)+2\}$, $s=1,2,\ldots$. Here s=1 and k=313. Hence 941 is located in the set {940, 941}. So we are dealing with the second case discussed above: **II.** $p = 3k + 2$.

Calculate the odd number in the next set of sequence (2) using formula (16):

$$b_2 = 941 + 2\left(2 - \mathrm{I}_{\langle s\rangle}\right) = 943, \ \ s = 2.$$

Here $\mathrm{I}_{\langle s\rangle}$ is determined by expression (3). It is obvious that $943 \in \{943, 944\}$.

The number 943 will be composite if and only if when

$$943 = (2n+1)(2m+1) = 4mn + 2(m+n) + 1, \quad m,n = 1,2,\ldots . \tag{23}$$

Then the even number $944 = 4mn + 2(m+n)+2$, i.e.

$$472 = 2mn + m + n + 1.$$

This implies

$$m = \frac{471 - n}{2n+1} \tag{24}$$

By Proposition 2

$$n \le \frac{\sqrt{p+2}-1}{2} = \frac{\sqrt{943}-1}{2} \Rightarrow n \le 14 \tag{25}$$

Now we should identify all possible pairs (n, m) with the help of which it turns out whether 943 is composite or not. Based on formula (24), we introduce the function

$$m(n_i) = \frac{471 - n_i}{2n_i + 1}, \ n_i = i, \ \ i = \overline{1,14}. \tag{26}$$

According to Algorithm 2 and using formula (26), we fill in the following table

Table 3

n_i	$m(n_i)$
1	*470/3*
2	469/5
3	468/7
4	467/9
5	466/11
6	465/13
7	464/15
8	463/17
9	462/19
10	461/21
11	460/23=20

ISSN 1512-1232

We found a pair of integers (n=11, m=20). It means that this pair satisfies equality (24), which confirms that 943 is a composite number. According to Algorithm 2, with the help of formula (16), we pass to the next set of sequence (2): $\{946, 947\}$.

The number 947 will be composite if and only if when

$$947 = (2n+1)(2m+1) = 4mn + 2(m+n) + 1, \quad m,n = 1,2,\ldots . \tag{27}$$

Then the even number $948 = 4mn + 2(m+n)+2$, i.e.

$$474=2mn + m+n+1.$$

This implies

$$m = \frac{473-n}{2n+1} \tag{28}$$

By Proposition 2

$$n \le \frac{\sqrt{p+2}-1}{2} = \frac{\sqrt{947}-1}{2} \Rightarrow n \le 14 \tag{29}$$

Now we should identify all possible pairs (n, m) with the help of which it turns out whether 947 is composite or not. Based on formula (28), we introduce the function

$$m(n_i) = \frac{473-n_i}{2n_i+1},\ n_i = i,\ i = \overline{1,14}. \tag{30}$$

According to Algorithm 2 and using formula (30), we fill in the following table

Table 4

n_i	$m(n_i)$
1	*472/3*
2	471/5
3	470/7
4	469/9
5	468/11
6	467/13
7	466/15
8	465/17
9	464/19
10	463/21
11	462/23
12	461/25
13	460/27
14	459/29

As follows from the table, all values of m turned out to be fractional. Hence for any pair (n,m) equality (27) is not satisfied and 947 is a prime number.

Thus, the next prime number after the given 941 will be 947.

ISSN 1512-1232

4. Two related works

In work [4] a method for finding a prime number that is the successor of a given prime number P_i is given. Without going into detailed description of the method, we will focus on its general scheme. The author introduces the concept of a potential divisor D of P_i with a range from 2 to (P_i -1)/2. For each such divisor, the slack S is determined (a **slack variable** is a variable that is added to an inequality constraint to transform it into an equality). Then, by processing the list of slacks, the parameter E is determined. And, finally, the author derives the final formula for determining the prime number following the given prime number: $P_{i+1} = P_i + E$.

To compare this method with our approach, consider the example given in section 3. The prime number 941 is given. It is required to find the next prime number. Using our approach, 12 computational operations were spent: one to determine the number 943 and its location in a sequence of two-element sets and 11 to determine the fact that the number 943 is composite. Further, 15 computational operations were spent: one to determine the number 947 and its location in the sequence of two-element sets and 14 - to determine the fact that the number 947 is prime. In total, 12+15=27 computational operations were required.

As noted above, the first stage of the method in [4] is the determination of potential divisors in the amount of (943 -1)/2 -2+1=470 . For each of these potential divisors, a slack is calculated, and after processing the list of slacks, the parameter E is determined, by adding which to the given prime number the required prime number is obtained. Thus, the minimum number of computational operations for the example under consideration is much more than 470. Thus, the our approach is much more efficient than the method considered in [4].

In [5] a new formula that computes the next prime for any given number is proposed. Author intro duces the function *nextp(n)* finds the first prime number that is greater than a given number n:

$$nextp(n) = n + \sum_{i=1}^{n} \prod_{x=n+1}^{n+i} \left(1 - S(x)\right).$$

Consider how the authors define $S(x)$:

«Every prime is of the form $6k \pm 1$ where k an integer… Let x be a real number, the floor of x, denoted by $\lfloor x \rfloor$ is the largest integer that is less or equal to x.

$$S(x) = \frac{S_1(x) + S_2(x)}{2},$$

where

$$S_1(x) = \frac{(-1)}{\left\lfloor \frac{\lfloor \sqrt{x} \rfloor}{6} \right\rfloor + 1} \sum_{k=1}^{\left\lfloor \frac{\sqrt{x}}{6} \right\rfloor + 1} \left\lfloor \left\lfloor \frac{x}{6k+1} \right\rfloor - \frac{x}{6k+1} \right\rfloor,$$

$$S_2(x) = \frac{(-1)}{\left\lfloor \frac{\lfloor \sqrt{x} \rfloor}{6} \right\rfloor + 1} \sum_{k=1}^{\left\lfloor \frac{\sqrt{x}}{6} \right\rfloor + 1} \left\lfloor \left\lfloor \frac{x}{6k-1} \right\rfloor - \frac{x}{6k-1} \right\rfloor.»$$

Without going into details of calculating $S(x)$, let us see how this formula will look like for the example considered in section 3 n = 941:

ISSN 1512-1232

$$nextp(941) = 941 + \sum_{i=1}^{941} \prod_{x=942}^{941+i} \left(1 - S(x)\right).$$

Considering that the expression for calculating $S(x)$ is rather complicated, it is obvious that the number of operations required to determine $nextp(941)$ is dramatically more than 941. Recall that using our approach, it took 27 computational operations to find the next prime number after 941. This means that the our approach is much more efficient than the method considered in [5].

5. Conclusion

The presented paper proposes an approach for finding a prime number following the given prime number.

The main results of the presented work are given below:

- Formalisms have been developed to determine in which two-place set the next odd number is located and what ordinal place it occupies.+
- A theoretical basis for finding the next prime is developed, in particular, two Propositions are proved.
- Two Algorithms for implementing the considered approach are elaborated.
- A detailed example is given that clearly illustrates the step-by-step operation of the proposed approach.

A further development of this direction may be the creation of a method for determining a prime number preceding the given prime number. This will allow us to create a p-neighborhood for any given prime number $p>3$, which can be useful, e.g., in the field of cryptography and cybersecurity.

References

[1] IEEE. IEEE P1363: Standard Specifications for Public Key Cryptography. IEEE P1363a D11, Amendment 1: Additional Techniques. December 16, 2002.

[2] James Maynard. Small gaps between primes. Annals of Mathematics,181:383–413, 2015.

[3] Kevin Ford, Ben Green, Sergei Konyagin, and Terence Tao. Large gaps between consecutive prime numbers.

Annals of Mathematics, 183:935–974, 2016.

[4] Reena Joshi, Towards Proving the Twin Prime Conjecture using a Novel Method For Finding the Next

Prime Number PN+1 after a Given Prime Number PN, arXiv:2004.14819 [math.GM].

[5] Issaam Kaddoura, Samih Abdul-Nabi, On formula to compute primes and nth prime, J. Applied Mathematical Sciences 6(73), February 2012, 3751-3757.

Article received: 2023-05-15