A New Deterministic Algorithm for Testing Primality Based on a New Property of Prime Numbers

Srikumar Manghat

Indira Vihar, Hemambika Nagar, Kallekulangara.P.O;
Palakkad-678009, Kerala, India
msrikumar1981@rediffmail.com

Abstract. Although they have been being intensely studied, there remain numerous open questions around prime numbers. For example, no known formula exists that yields all of the prime numbers and no composites. Due to this uncertainty surrounding the theory of prime numbers, popular algorithms proposed in literature till date, rely heavily on probabilistic methods to determine primality. The paper proposes a new theory on the nature of prime numbers. In particular the paper proposes new theorems by which any prime number can be calculated from the knowledge of any other prime number of lower value in a simple way. It is shown in the paper that, in so doing, the theorems prove to be a common thread through which all the prime numbers of a number system can be related. Based on the theorems, a new prime number generating algorithm and a new purely deterministic method to test primality is explained and illustrated with the help of examples.

Keywords: Prime numbers, prime number generating algorithm, primality test.

1 Introduction

A prime number (or a prime) is a natural number such that it has exactly two distinct natural number divisors: 1 and itself. An infinite number of prime numbers exists and this fact has been demonstrated as early as 300 BC by Euclid [1]. Any nonzero natural number **n** can be factored into primes; that is; these can be written as a product of primes or powers of different primes. This factorization is unique except for a possible reordering of the factors.

Although they have been intensely studied, there remain numerous open questions around prime numbers. For example, no known formula exists that yields all of the prime numbers and no composites. For more than a century, the Goldbach's conjecture which asserts that any even natural number bigger than two is the sum of two primes, or the twin prime conjecture which says that there are infinitely many twin primes (pairs of primes whose difference is two), have remained unresolved, notwithstanding the simplicity of their statements. However, it has been demonstrated by mathematicians that the distribution of primes or in other words the statistical behaviour of primes in the large can be modelled. For instance, the prime number theorem, says that the probability that a given, randomly chosen number **n** is prime is

S.M. Thampi et al. (Eds.): SNDS 2012, CCIS 335, pp. 117–126, 2012.

inversely proportional to the logarithm of **n**. The unproven Riemann hypothesis [2] implies a refined statement concerning the distribution of primes and though it has been unproven since its inception in 1859.

Primes have been applied in several fields in information technology, such as public-key cryptography, which makes use of the difficulty of factoring large numbers into their prime factors. Searching for big primes, often using distributed computing, has stimulated studying special types of primes, chiefly Mersenne primes whose primality is comparably quick to decide. As of 2011, the largest known prime number has about 13 million decimal digits [3].

The property of being prime is called primality. The simplest method for verifying the primality of a given number **n** can be done by trial division. The method tests whether **n** is a multiple of an integer **m** between 2 and $\sqrt{\mathbf{n}}$. If **n** is a multiple of any of these integers then it is a composite number, and so not prime; if it is not a multiple of any of these integers then it is prime. As this method requires up to $\sqrt{\mathbf{n}}$ trial divisions, it is only suitable for relatively small values of **n**. More sophisticated algorithms, which are much more efficient than trial division, have been devised to test the primality of large numbers.

Different methods have been proposed in literature to test primality, for example the latest methods by Shafi Goldwasser & Joe Kilian [4]; M.Aggrawal & S.Biswas [5]; Rene Shoof [6]; etc. A common feature of all these latest algorithms, is that they rely primarily on probabilistic methods to determine primality and use deterministic methods only as a secondary instrument.

The paper proposes a new theory on the nature of prime numbers. In particular the paper proposes new theorems by which any prime number can be calculated from the knowledge of any other prime number of lower value in a simple way. It is shown in the paper that, in so doing, the theorems prove to be a common thread through which all the prime numbers of a number system can be related. Based on the theorems, a new prime number generating algorithm and a new purely deterministic method to test primality is explained and illustrated with the help of examples.

Section 1 has provided the introduction. The proposed theorem and its proof are given in Section 2. The proposed algorithms for generating prime numbers and for testing primality are described in Section 3. Examples illustrating the operation of the proposed algorithms are shown in Section 4. Section 5 provides the concluding remarks.

2 Proofs

Our objective is to first prove a theorem by which any prime number can be calculated from the knowledge of any other prime number of lower value. Let us begin by proving some smaller theorems and see how these theorems lead us to our final objective.

Theorem 1:
A number **P** of the form

$$\mathbf{P} = 3\mathbf{a},$$

is an odd number, for any odd number **a**.

Proof 1:
We know that any odd number **O** can be expressed in the form:

$$\mathbf{O} = 2\mathbf{n} + \mathbf{b}, \tag{1}$$

where **n** is any integer and **b** is an odd integer.
Now, a number of the form $\mathbf{P} = 3\mathbf{a}$, where **a** is an odd number, can be written as

$$\mathbf{P} = 3\mathbf{a},$$
$$= 2\mathbf{a} + \mathbf{a}$$

Since **P** is a number expressible in the form given by equation (1), we can say that $\mathbf{P} = 3\mathbf{a}$ is an odd number.
Hence the theorem is proved.

Corollary to theorem 1:
Theorem 1 implies that non-prime numbers of any other form are interspersed between non-prime odd numbers of the form $\mathbf{P} = 3\mathbf{a}$, **a** being an odd number. It is, therefore, easy to see that a non-prime number **Q** of the form

$$\mathbf{Q} = \mathbf{C}^2,$$

where **C** is a prime number, occurs in between two non-prime odd numbers, say, $3\mathbf{a_1}$ and $3\mathbf{a_2}$, where $\mathbf{a_1}$ and $\mathbf{a_2}$ are two consecutive odd numbers.

These facts are illustrated below in Table 1, where a set of contiguous non-primes are listed out along with their factors

Table 1. A set of contiguous non-primes and their factors

Odd non-primes	Factors
9	3 × 3
15	3 × 5
21	3 × 7
→ 25	5 × 5
27	3 × 9
33	3 × 11
35	5 × 7
39	3 × 13
45	3 × 15
→ 49	7 × 7
51	3 × 17
55	5 × 11
57	3 × 19

→ : indicates odd non-prime numbers of the form $\mathbf{P} = \mathbf{C}^2$, where **C** is a prime number.

Another fact that emerges (which can be easily verified) is that between two non-prime odd numbers of the form $3\mathbf{a}$, say, $3\mathbf{a_1}$ and $3\mathbf{a_2}$, where $\mathbf{a_1}$ and $\mathbf{a_2}$ are two consecutive odd numbers, there can occur just two other odd numbers, both of which will, obviously, be of some other form. For example, between 3 × 17 and 3 × 19, the two odd numbers are 53 and 55. Therefore, between $3\mathbf{a_1}$ and $3\mathbf{a_2}$ there can occur just one number **Q** of the form

$$\mathbf{Q} = \mathbf{C}^2, \text{ where } \mathbf{C} \text{ is prime,} \tag{2}$$

because $\mathbf{Q} \pm 2$ which can be the only other odd number that can occur between $3\mathbf{a_1}$ and $3\mathbf{a_2}$ is obviously not of the form given by equation (2). In other words, two 'square of prime' numbers cannot occur between $3\mathbf{a_1}$ and $3\mathbf{a_2}$, where $\mathbf{a_1}$ and $\mathbf{a_2}$ are two consecutive odd numbers.

Recapitulating, the two facts that emerge are:

a) Non-prime odd numbers of the form
$$\mathbf{Q} = \mathbf{C}^2, \text{ where } \mathbf{C} \text{ is prime}$$
occur between non-prime odd numbers of the form $3\mathbf{a}$,say, $3\mathbf{a_1}$ and $3\mathbf{a_2}$, where $\mathbf{a_1}$ and $\mathbf{a_2}$ are two consecutive odd numbers.

b) Between two non-prime odd numbers of the form $3\mathbf{a}$,say, $3\mathbf{a_1}$ and $3\mathbf{a_2}$, where $\mathbf{a_1}$ and $\mathbf{a_2}$ are two consecutive odd numbers, there can occur just one odd number of the form
$$\mathbf{Q} = \mathbf{C}^2, \text{ where } \mathbf{C} \text{ is prime.}$$

Theorem 2:
If a non-prime odd number **Q** of the form
$$\mathbf{Q} = \mathbf{P}^2,$$
where **P** is a prime number greater than or equal to 5, is such that it occurs between two non-prime odd numbers of the form $3\mathbf{a}$, say, $3\mathbf{a_1}$ and $3\mathbf{a_2}$, where $\mathbf{a_1}$ and $\mathbf{a_2}$ are two consecutive odd numbers with $\mathbf{a_2} > \mathbf{a_1}$; and two integers $\mathbf{x_1}$ and $\mathbf{x_2}$ are such that
$$\mathbf{x_1} = \mathbf{Q} - 3\mathbf{a_1},$$
$$\mathbf{x_2} = 3\mathbf{a_2} - \mathbf{Q},$$
then,
$$\mathbf{x_1} = 2\mathbf{x_2}$$

Proof 2:
Any odd number $\mathbf{N} > 1$ can be expressed as
$$\mathbf{N} = (2\mathbf{n} + 1),$$
where **n** is any integer greater than 0.

Now, prime numbers are all odd and the square of any prime number $\mathbf{P} > \mathbf{N}$ can be expressed in terms of **N** as follows:
$$\mathbf{Q} = \mathbf{P}^2 = (2(\mathbf{n}+\mathbf{k}) + 1), \text{ where } \mathbf{k} \text{ is some integer greater than 0.}$$
$$= 2\mathbf{n} + 1 + 2\mathbf{k}$$
$$= \mathbf{N} + 2\mathbf{k}$$

Suppose **N** is of the form $3\mathbf{a}$ (where **a** is odd). Now, let us consider two odd numbers of the form $3\mathbf{a}$ (where **a** is odd) in terms of **k** such that they are closest to $\mathbf{Q} = \mathbf{P}^2$ and one number is greater than **Q** and the other is lesser than **Q**. It is easy to verify that the smaller number is
$$\mathbf{A} = \mathbf{N} \quad \text{(of the form } 3\mathbf{a}\text{, where } \mathbf{a} \text{ is odd)}$$
And the greater number is
$$\mathbf{B} = \mathbf{N} + 3\mathbf{k} \quad \text{(of the form } 3\mathbf{a}\text{, where } \mathbf{a} \text{ is odd)}$$
Now, when $\mathbf{k} = 2$; **A** and **B** are equal to, say, $3\mathbf{a_1}$ and $3\mathbf{a_2}$ respectively such that $\mathbf{a_1}$ and $\mathbf{a_2}$ are two consecutive odd numbers with $\mathbf{a_2} > \mathbf{a_1}$. Also, it follows from theorem 1and its corollary that only one number of the form
$$\mathbf{Q} = \mathbf{P}^2$$

can exist between them. Therefore, the value of $\mathbf{k} = 2$ is the only value of **k** that concerns us.
Let us define the differences

$$\mathbf{x_1} = \mathbf{Q} - \mathbf{A}$$

And

$$\mathbf{x_2} = \mathbf{B} - \mathbf{Q}$$

From the foregoing statements regarding the values of **k**, **A** and **B**; replacing the values of these in the above two equations we have:

$$\mathbf{x_1} = \mathbf{Q} - 3\mathbf{a_1} = 2\mathbf{k} = 2$$

And

$$\mathbf{x_2} = 3\mathbf{a_2} - \mathbf{Q} = \mathbf{k} = 1$$

Therefore the ratio

$$\mathbf{x_1} : \mathbf{x_2} = 2 : 1$$

Hence the theorem is proved.

Theorem 3:
The difference between the square of two prime numbers that are each greater than or equal to 5 is always divisible by 3. Or, if a number **T** is such that

$$\mathbf{T} = \text{abs}(\mathbf{N_1}^2 - \mathbf{N_2}^2)$$

then **T** is always divisible by 3 if both $\mathbf{N_1}$ and $\mathbf{N_2}$ are dissimilar prime numbers and have values greater than or equal to 5.

Proof 3:
Let us consider two odd non-primes $\mathbf{N_1}^2$ and $\mathbf{N_2}^2$ such that $\mathbf{N_1}$ and $\mathbf{N_2}$ are both prime numbers. By theorem 1 and its corollary, $\mathbf{N_1}^2$ and $\mathbf{N_2}^2$ are located amidst non-prime odd numbers of the form 3**a**, **a** being odd. Let us assume that $\mathbf{N_1}^2$ is located between numbers $3\mathbf{a_1}$ and $3\mathbf{a_2}$; and $\mathbf{N_2}^2$ is located between numbers $3\mathbf{a_3}$ and $3\mathbf{a_4}$ such that $\mathbf{a_1} < \mathbf{a_2} < \mathbf{a_3} < \mathbf{a_4}$ and; ($\mathbf{a_1}$, $\mathbf{a_2}$) and ($\mathbf{a_3}$, $\mathbf{a_4}$) are consecutive odd number pairs.
Let us define numbers $\mathbf{x_1}$, $\mathbf{x_2}$, $\mathbf{x_3}$, $\mathbf{x_4}$ such that

$$\mathbf{x_1} = 3\mathbf{a_1} - \mathbf{N_1}^2$$
$$\mathbf{x_2} = \mathbf{N_1}^2 - 3\mathbf{a_2}$$
$$\mathbf{x_3} = 3\mathbf{a_3} - \mathbf{N_2}^2$$
$$\mathbf{x_4} = \mathbf{N_2}^2 - 3\mathbf{a_4}$$

This is graphically shown below in Fig. 1:

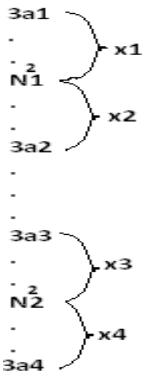

Fig. 1. Graphical illustration

Theorem 2 states that for $\mathbf{N_1}, \mathbf{N_2} \geq 5$,

$$\mathbf{x_1} = 2\mathbf{x_2}$$

and $$\mathbf{x_3} = 2\mathbf{x_4}$$

Thus,

$$\mathbf{x_2} = (1/3)(\mathbf{x_1} + \mathbf{x_2})$$
$$= (1/3)(3\mathbf{a_2} - 3\mathbf{a_1})$$
$$= (\mathbf{a_2} - \mathbf{a_1})$$

Similarly, $$\mathbf{x_3} = (2/3)(\mathbf{x_3} + \mathbf{x_4})$$
$$= (1/3)(3\mathbf{a_4} - 3\mathbf{a_3})$$
$$= 2(\mathbf{a_4} - \mathbf{a_3})$$

Since $(\mathbf{a_1}, \mathbf{a_2})$ and $(\mathbf{a_3}, \mathbf{a_4})$ are consecutive odd number pairs,

$$\mathbf{a_2} - \mathbf{a_1} = \mathbf{a_4} - \mathbf{a_3} = 2$$

Therefore,

$$\mathbf{x_2} = 2$$

and $$\mathbf{x_3} = 2\times2 = 4$$

Now, (making use of the figure 1 above)

$$\mathbf{T} = \text{abs}(\mathbf{N_1}^2 - \mathbf{N_2}^2) = \text{abs}(\mathbf{x_2} + (3\mathbf{a_2} - 3\mathbf{a_3}) + \mathbf{x_3})$$
$$= \text{abs}(3\mathbf{a_2} - 3\mathbf{a_3} + \mathbf{x_3} + \mathbf{x_2})$$

Or, replacing the values of $\mathbf{x_2}$ and $\mathbf{x_3}$, $$= \text{abs}(3\mathbf{a_2} - 3\mathbf{a_3} + 6)$$

$\mathbf{T} = \text{abs}(\mathbf{N_1}^2 - \mathbf{N_2}^2)$ is thus always divisible by 3.
Hence the theorem is proved.

Theorem 4:

If $\mathbf{P}$ is a prime number greater than or equal to 5, and if $\mathbf{P}^2$ is expressed as

$$\mathbf{P}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$

where $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, etc; are integers such that each of them has a value less than 3×5^2 and $\mathbf{d}$ is an integer with value less than 5^2, and $\mathbf{t}$, $\mathbf{n}$, etc; are integers such that $\mathbf{t} > \ldots > \mathbf{n} > \ldots > 2$; then the coefficient of 5^2, $\mathbf{c}$, is a non-zero integer that is never divisible by 3.

Proof 4:

Using theorem 3, a prime number $\mathbf{P}$ greater than or equal to 5, can be written as

$$\mathbf{P}^2 = (\mathbf{P_1}^2 + 3\mathbf{i_1})$$

where $\mathbf{i_1}$ is an integer and $\mathbf{P_1}$ is some prime number.

Let us choose $\mathbf{P_1}$ as the least prime number for which theorem 3 is applicable, i.e., let $\mathbf{P_1} = 5$. Then,

$$\mathbf{P}^2 = (5^2 + 3\mathbf{i_1})$$
$$= (3\mathbf{s}5^{2\mathbf{t}} + \ldots + 3\mathbf{r}5^{2\mathbf{n}} + \ldots + (3\mathbf{k} + 1)5^2 + 3\mathbf{i})$$

because $3\mathbf{i_1}$ can be expressed as: $3\mathbf{i_1} = 3\mathbf{s}5^{2\mathbf{t}} + \ldots + 3\mathbf{r}5^{2\mathbf{n}} + \ldots + 3\mathbf{k}5^2 + 3\mathbf{i}$, where $\mathbf{i}$, $\mathbf{s}$, $\mathbf{r}$, $\mathbf{k}$, etc; are integers such that each of them has a value less than 5^2 and $\mathbf{t}$, $\mathbf{n}$, etc; are integers such that $\mathbf{t} > \ldots > \mathbf{n} > \ldots > 2$. Thus, $\mathbf{P}^2$ can be written as:

$$\mathbf{P}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$

where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2,and the coefficient of 5^2, **c**, is never divisible by 3. Hence the theorem is proved.

Theorem 5:
If **C** is an odd composite number such that it is a product of two or more prime numbers with values other than 3 and 5, and if $\mathbf{C}^2$ is expressed as

$$\mathbf{C}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$

where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2, and **t**, **n**, etc; are integers such that **t** >…> **n** >…>2; then the coefficient of 5^2, **c**, is always either 0 or divisible by 3.

Proof 5:
Using theorem 3, the square of an odd composite number **C** that is a product of two or more prime numbers with values other than 3and 5, can be written in the general form as

$$\mathbf{C}^2 = (\mathbf{P}^2 + 3\mathbf{i}_1)^{\mathbf{l}}(\mathbf{P}^2 + 3\mathbf{i}_2)^{\mathbf{m}}.....$$

where $\mathbf{i}_1$, $\mathbf{i}_2$, **l**, **m**, ...etc; are all integers and **P** is some prime number.

Let us choose **P** as the least prime number for which theorem 3 is applicable, i.e., let **P** = 5. Then,

$$\begin{aligned}\mathbf{C}^2 &= (5^2 + 3\mathbf{i}_1)^{\mathbf{l}}(5^2 + 3\mathbf{i}_2)^{\mathbf{m}}.....\\ &= 5^{2\mathbf{n}} + 3\mathbf{i}_{\mathbf{e}}\\ &= (3\mathbf{s}5^{2\mathbf{t}} + \ldots + (3\mathbf{r} + 1)5^{2\mathbf{n}} + \ldots + 3\mathbf{k}5^2 + 3\mathbf{i})\end{aligned}$$

because $3\mathbf{i}_{\mathbf{e}}$ can be expressed as: $3\mathbf{i}_{\mathbf{e}} = 3\mathbf{s}5^{2\mathbf{t}} + \ldots + 3\mathbf{r}5^{2\mathbf{n}} + \ldots + 3\mathbf{k}5^2 + 3\mathbf{i}$ where $\mathbf{i}_{\mathbf{e}}$ is an integer and **i**, **s**, **r**, **k**, etc; are integers such that each of them has a value less than 5^2 and **t**, **n**, etc; are integers such that **t** >…> **n** >…>2. Thus, $\mathbf{C}^2$ can be written as:

$$\mathbf{P}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$

where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2, and the coefficient of 5^2, **c**, is always either 0 or divisible by 3.
Hence the theorem is proved.

Thus, since numbers in a number system are either prime or are a product of two or more prime numbers with one or more of them having values equal to 3 or 5 or are a product of two or more prime numbers with values other than 3 and 5; the following corollary to theorems 4 & 5:

Corollary to theorems 4 & 5:
Theorems 4 & 5, thus, imply that if a number **Q** is an odd number and **Q** is not divisible by 3 and 5 and if $\mathbf{Q}^2$ is expressed as

$$\mathbf{Q}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$

where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2 and **t**, **n**, etc; are integers such that **t** >…> **n** >…>2, then **Q** is a prime number if the coefficient of 5^2, **c**, is a non-zero integer that is never divisible by 3.

This corollary is the basis for developing the primality algorithms that follow.

3 Algorithms

By theorems 4 & 5, it is possible to calculate the next prime number in the sequence from a prime number whose value is known.

The algorithm to calculate the next prime number from a previously known prime number is as follows:

Algorithm 1:

1. Let **M** is a known prime number.
2. Find the value of **k**(**i**) from the formulae
   $$\mathbf{k(i)} = (\mathbf{O(i}\text{-}1) + 2),$$
   using the value of **O**(**i**-1) as
   $$\mathbf{O(i}\text{-}1) = \mathbf{M}.$$
3. If **k**(**i**) is divisible by 3 or 5, then **O**(**i**) is non-prime. Proceed to step 6.
4. If **k**(**i**) is not divisible by 3 and 5, express $\mathbf{k(i)}^2$ as
   $$\mathbf{k(i)}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$
   where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2 and **t**, **n**, etc; are integers such that $\mathbf{t} > \ldots > \mathbf{n} > \ldots > 2$.
5. The current value of **O**(**i**) which is
   $$\mathbf{O(i)} = \mathbf{O(i}\text{-}1) + 2$$
   is a prime number if the coefficient of 5^2, **c**, is a non-zero integer that is not divisible by 3, by theorems 4 & 5. Output **O**(**i**) as the result and stop. If **c** is 0 or divisible by 3, then **O**(**i**) is non-prime by theorems 4 & 5. Proceed to step 6.
6. Calculate the new value of **k**(**i**) using
   $$\mathbf{k(i)} = (\mathbf{O(i}\text{-}1) + 2),$$
   the new value of **O**(**i**-1) being
   $$\mathbf{O(i}\text{-}1) = \mathbf{O(i)}.$$
7. Go to step 3.

From the nature of the algorithm, it is clear that, starting from a prime number of lowest value, any prime number of any desired value can be calculated with the help of theorems 4 & 5. Therefore, theorems 4 & 5 serve as a link by which all prime numbers in a number system can be related. Prime numbers, which were hitherto considered to be distributed throughout the number system following no particular rule, seem to follow the rules set by theorems 4 & 5.

Theorems 4 & 5 can also be used to formulate a simple procedure to check the primality of any odd number. Suppose **X** is the odd number whose primality needs to be checked. The procedure is as follows:

Algorithm 2:

1. If **X** is divisible by 3 or 5, then **X** is non-prime.
2. If **X** is not divisible by 3 and 5, express $\mathbf{X}^2$ as
$$\mathbf{X}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$
where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2 and **t**, **n**, etc; are integers such that **t** >…> **n** >…>2.
3. **X** is a prime number if the coefficient of 5^2, **c**, is a non-zero integer that is not divisible by 3, by theorems 4 & 5.

4 Examples

Suppose a prime number 79 is given and it is required to find the value of the next highest prime number. Following Algorithm 1 of the previous section we have:

1. **M** = 79
2. Putting the value of **O**(**i**-1) = **M** in equation
$$\mathbf{k}(\mathbf{i}) = (\mathbf{O}(\mathbf{i}\text{-}1) + 2)$$
we have
$$\mathbf{k}(\mathbf{i})^2 = 81^2 = 6561$$
3. Value of **k**(**i**) = 81 is divisible by 3. So,
$$\mathbf{O}(\mathbf{i}) = \mathbf{O}(\mathbf{i}\text{-}1) + 2 = 81$$
is not prime.
4. The new value of **k**(**i**) is obtained by putting **O**(**i**-1) = **O**(**i**) in the equation
$$\mathbf{k}(\mathbf{i}) = (\mathbf{O}(\mathbf{i}\text{-}1) + 2) = 83$$
Or,
$$\mathbf{k}(\mathbf{i})^2 = 83^2 = 6889$$
5. **k**(**i**) is not divisible by 3 and 5 and $\mathbf{k}(\mathbf{i})^2$ can be expressed as
$$\mathbf{k}(\mathbf{i})^2 = 83^2 = 3\times3\times5^4 + (3\times16 + 1)\times5^2 + 3\times13,$$
which is of the form,
$$\mathbf{k}(\mathbf{i})^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$
where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2 and **t**, **n**, etc; are integers such that **t** >…> **n** >…>2, as required by theorems 4 & 5.
6. Since the coefficient of 5^2, **c** = (3×16 + 1), is a non-zero integer that is not divisible by 3, hence, by theorems 4 & 5,
$$\mathbf{O}(\mathbf{i}) = \mathbf{O}(\mathbf{i}\text{-}1) + 2 = 83,$$
is the next highest prime number.

In order to test the primality of an odd number, say, **X** = 187, following algorithm 2, we have:

1. **X** is not divisible by 3 and 5 and $\mathbf{X}^2$ can be expressed as
$$\mathbf{X}^2 = 187^2 = (3\times18 + 1)\times5^4 + 3\times7\times5^2 + 3\times23,$$
which is of the form,
$$\mathbf{X}^2 = (\mathbf{a}5^{2\mathbf{t}} + \ldots + \mathbf{b}5^{2\mathbf{n}} + \ldots + \mathbf{c}5^2 + 3\mathbf{d})$$
where **a**, **b**, **c**, etc; are integers such that each of them has a value less than 3×5^2 and **d** is an integer with value less than 5^2 and **t**, **n**, etc; are integers such that $\mathbf{t} > \ldots > \mathbf{n} > \ldots > 2$, as required by theorems 4 & 5.
2. Since the coefficient of 5^2, $\mathbf{c} = 3\times7$, is divisible by 3, hence, by theorems 4 & 5, **X** is not a prime number.

5 Conclusion

The paper proposes a new theory on the nature of prime numbers. In particular the paper proposes new theorems by which any prime number can be calculated from the knowledge of any other prime number of lower value in a simple way. It is shown in the paper that, in so doing, the theorems prove to be a common thread through which all the prime numbers of a number system can be related. Based on the theorems, a new prime number generating algorithm and a new method to test primality is explained and illustrated with the help of examples.

References

1. Euclid's 'Elements', Book 9, Proposition 10
2. Peter, B., Choi, S., Rooney, B., et al. (eds.): The Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike. CMS Books in Mathematics. Springer, New York (2008)
3. Great Internet Mersenne Prime Search Home, `http://www.mersenne.org/`
4. Goldwasser, S., Kilian, J.: Primality testing using elliptic curves. Journal of the ACM (JACM) 46(4), 450–472 (1999)
5. Aggrawal, M., Biswas, S.: Primality and identity testing via Chinese remaindering. In: 40th Annual Symposium on Foundations of Computer Science, pp. 202–208 (1999)
6. Schoof, R.: Four Primality testing algorithms; arXiv.org > math > arXiv:0801.3840 (2004)