British Journal of Applied Science & Technology
14(4): 1-8, 2016, Article no.BJAST.24367
ISSN: 2231-0843, NLM ID: 101664541

SCIENCEDOMAIN *international*
www.sciencedomain.org

An Analysis of the Congruence $1\ mod\ 24$ as a Generator of Prime Numbers Greater or Equal to 5

José William Porras Ferreira[1*] and Willian De Jesus Caballero Guardo[1]

[1]Escuela Naval Almirante Padilla, Cartagena, Colombia.

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJAST/2016/24367
Editor(s):
(1) Qing-Wen Wang, Department of Mathematics, Shanghai University, P.R. China.
Reviewers:
(1) Leo Depuydt, Brown University, Providence, USA.
(2) Octav Olteanu, University Politehnica of Bucharest, Romania.
Complete Peer review History: http://sciencedomain.org/review-history/13307

Original Research Article

Received 17th January 2016
Accepted 4th February 2016
Published 15th February 2016

ABSTRACT

It has always been thought that primes numbers within natural numbers do not fulfill well-defined rules that can express themselves through a sequential structure to facilitate checking their properties. The study of congruence $1\ mod\ 24$, allows us to find some of the properties of prime numbers and demonstrate how these are directly related to this type of congruence that enable us to find all (though not only) the primes $p \geq 5$.

Keywords: Prime numbers; fundamental theorem of arithmetic; congruence $a \bmod b$.

1. INTRODUCTION

The study of prime numbers has always fascinated mathematicians throughout history, always looking for how they are formed and their properties. For example, some mathematicians such as Euclid (330 b. C.-275 b. C.), [1], determined that the prime numbers are infinite. Eratosthenes (284 b. C. - 192 b. C.), [2], recognized the primality of certain numbers through sieve to find *all* the prime numbers gradually as long as one kept going (forever), which bears his name and other as Carl Friedrich Gauss (1777-1855), [3] determined that the density of primes approximates the logarithmic function $Li(x)$, Riemann (1826-1866), [4,5], was able to correct the error of fluctuation between Li (x) and the real value of the primes density less

**Corresponding author: E-mail: jwporrasf45@gmail.com;*

than a value x and perhaps, one of the most prominent theorems related to divisibility is Fermat's little theorem. Fermat in a letter addressed to Frénicle de Bessy (October 8, 1640), but as usual of him, he missed out the necessary proof, expressed the following equation: if we have a prime number p, then for every natural number a we have that a raised to p is congruent with a module p, i.e., $a^p \equiv a \bmod p$, or its equivalent if p is a prime number, then for every natural number a coprime with p, $a^{p-1} \equiv 1 \bmod p$. The first actual published proof of this theorem was made by Leonhard Euler in 1736 [6]. Euler proof begins by showing that $2^{p-1} \equiv 1 \bmod p$ for all relatively primes to p. Euler demonstrated that $2^{p-1} \equiv 1 \bmod p$ for $p \neq 2$, aftter wich he shows that $3^{p-1} \equiv 1 \bmod p$ for $p \neq 3$. He then concludes that the formula holds por all a relatively prime to p, [7,8,9,10,11].

There are also many conjectures about prime numbers, which have not been proven, mostly because there are without evidence in determining of all the properties that contain them.

Here, five properties of congruence will be explored $1 \, mod \, 24$ which enables us to find some fundamental properties of primes and how they are related to this congruence. The document, for better understanding, is organized as follows: section 2 presents some basic concepts related to prime numbers. Following, section 3 presents 5 properties of prime numbers jointly with its corollaries in some cases, related to the residual class $1 \, mod \, 24$, which essentially, turns out to be the fundamental reason of this article. Finally, of all the properties have been accompanied by applications in order to clarify in essence their importance.

2. AN OVERVIEW OF NUMBER THEORY

2.1 Definition 1

Let a and b are integers with $b \neq 0$. We say that b divides a if there is an integer c such that $a = bc$. If b divides a we write $b|a$.

2.2 Definition 2

An integer $p > 1$ is a prime if only its divisors are 1 and p. If p is not a prime, then it is a composite number [12].

2.3 Fundamental Theorem of Arithmetic

Every natural composite number $n > 1$ can be factored uniquely as

$$n = {p_1}^{k_1} {p_2}^{k_2} \times \cdots \times {p_s}^{k_s}$$

where $p_1, p_2, \cdots p_s$ are different primes and $k_1, k_2, \cdots, k_s$ are positive integers. This factorization is called the *prime factorization* of n, [13,14,15].

2.4 Definition 3

If n is a positive integer, we say that two integers a and b are *congruent module* n If there is a $k \in \mathbb{Z}$ such that $a - b = kn$. We will use $a \equiv b \, mod \, n$ notation to indicate that a and b are *congruent module* n.

In mathematics, *congruent module* n is knows as *modular arithmetic* [16]. Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value—the **modulus**. The modern approach to modular arithmetic was developed by Carl Friedrich Gauss in 1798 when Gauss was 21 and first published in 1801 in his book *Disquisitiones Arithmeticae* (In Latin, in English:: *Arithmetical Investigations*), when he was 24. In this book Gauss brings together results in number theory obtained by mathematicians such as Fermat, Euler, Lagrange and Legendre and adds important new results of his own [17,18].

The congruence relation module n in $\mathbb{Z}$ is equivalence and therefore divides $\mathbb{Z}$ into equivalence classes so that any of two of them are disjoint, i.e.:

$$\mathbb{Z} = \cup_{j=0}^{n-1} [j] \quad \text{with} \quad [j] = \{j + kn: \ k \in \mathbb{Z}\}$$

where [j] is the j-th equivalence class module n. Whenever an integer z belongs to any of the n equivalence classes, we will say that it is *a representative of that class* [19,20].

3. THE CONGRUENCE $\mathbf{1 \, mod \, 24}$ AS A GENERATOR OF PRIMES≥5

3.1 Theorem 1

Let p and q prime greater or equal to 5, then $(pq)^2 \equiv 1 \, mod \, 24$.

Proof. Let be p and q prime greater or equal to 5. Then, *Porras* and *Andrade* [21] proved that p and q are representatives of the residual class $1 \, mod \, 6$ or $5 \, mod \, 6$. To carry out the test, we consider three cases:

Case 1. Let be p and q representatives of the class $1 \, mod \, 6$.

Indeed, if m and n are positive integers such that $p = 1 + 6m$ and $q = 1 + 6n$. Therefore,

$$\begin{aligned}(pq)^2 - 1 &= \left((1+6m)(1+6n)\right)^2 - 1\\ &= [(1+6m)(1+6n)-1][(1+6m)(1+6n)+1]\\ &= [1+6(m+n)+36mn-1][1+6(m+n)+36mn+1]\\ &= [6(m+n)+36mn][2+6(m+n)+36mn]\\ &= 6*2[(m+n)+6mn][1+3(m+n)+18mn]\\ &= 12[(m+n)+6mn][1+3(m+n)+18mn]\\ &= 24w \qquad (1)\end{aligned}$$

being $w \in \mathbb{N}$. Now we shall verify what w is in (1),

Clearly, $m + n \in \mathbb{N}$ which can be odd or even. Consider initially that $m + n$ is even, i.e. $m + n = 2k$, with $k \in \mathbb{N}$, then,

$$\begin{aligned}(pq)^2 - 1 &= 12[(m+n)+6mn][1+3(m+n)+18mn]\\ &= 12[2k+6mn][1+3(2k)+18mn]\\ &= 24[k+3mn][1+6k+18mn] \qquad (2)\end{aligned}$$

so in this case $w = [k + 3mn][1 + 6k + 18mn]$. Similarly, considering the case of odd $m + n$, i.e. $m + n = 2k + 1$, one gets that $w = [2k + 1 + 6mn][2 + 3k + 9mn]$. Which complete the demonstration for case 1.

Case 2. Let be p and q representatives of the class $5\ mod\ 6$.

The demonstration turns out to be similar to case 1.

Case 3. Let p be a representative of the residual class $1\ mod\ 6$ and q from $5\ mod\ 6$. Then, $p = 1 + 6m$ and $q = 5 + 6n$, with $m, n \in \mathbb{N}$. As a result,

$$\begin{aligned}(pq)^2 - 1 &= \left((1+6m)(5+6n)\right)^2 - 1\\ &= [(1+6m)(5+6n)-1][(1+6m)(5+6n)+1]\\ &= [5+6(5m+n)+36mn-1][5+6(5m+n)+36mn+1]\\ &= [4+6(5m+n)+36mn][6+6(5m+n)+36mn]\\ &= 2*6[2+3(5m+n)+18mn][1+(5m+n)+6mn]\\ &= 12[2+3(5m+n)+18mn][1+(5m+n)+6mn]\\ &= 24z \qquad (3)\end{aligned}$$

where $z \in \mathbb{N}$, comes up when the term $5m + n$ is given a similar treatment as it was given to $m + n$ in (2). Thus, case 3 is shown, and in consequence the proposed theorem.

3.2 Corollary 1

If p is a prime $p \geq 5$, then $p^2 \equiv 1\ mod\ 24$.

Proof. The test is immediate, and it is considering in Theorem 1 the case which in, $p = q$.

3.3 Theorem 2

If p is prime $p \geq 5$, and $k \in \mathbb{N}$, then $p^{2k} \equiv 1\ mod\ 24$.

Proof. We use the principle of mathematical induction over k.

The case $k = 1$ turns out to be an immediate consequence of corollary 1.

If we assume that the claim is valid for the case k. I.e., there is $m \in \mathbb{N}$, such as $p^{2k} = 1 + 24m$. Now, now we will demonstrate the case $(k+1)$. In effect,

$$\begin{aligned} p^{2(k+1)} &= p^{2k} * p^2 \\ &= (1+24m)(1+24n) \\ &= 1 + 24(m+n) + 24^2 mn \\ &= 1 + 24[(m+n) + 24mn] \\ &= 1 + 24w \end{aligned} \tag{4}$$

with $w \in \mathbb{N}$. This proves the theorem.

3.4 Corollary 2

Every composite number that has the form $({p_1}^{k_1} \times \cdots \times {p_n}^{k_n})^2$ with p_i primes, $p_i \geq 5$, $k_i \in \mathbb{N}$ for $i = 1, \cdots, n$, is congruent $1\ mod\ 24$.

Proof. The show is the result of the previous theorem, to the extent that $({p_1}^{k_1} \times \cdots \times {p_n}^{k_n})^2 = {p_1}^{2k_1} \times \cdots \times {p_n}^{2k_n}$.

3.5 Theorem 3

There are infinite primes p congruent $1\ mod\ 24$.

Proof. According with Dirichlet's Theorem: "*for any two positive coprime integers a and b, there are infinitely many primes of the form $a + bm$, where n is a non-negative integer* $(n = 1, 2, ...)$", then with $a = 1$ and $b = 24$, in the form $1 + 24m$ there are infinitely many primes.

3.6 Application I

Derived from section 3.2 corollary 1, $p^2 \equiv 1\ mod\ 24$ as long as p is prime, $p \geq 5$. . Immediately, there is $m \in \mathbb{N}$ such that $p^2 = 1 + 24m$. We question which sequential form can take all m in such a way that $p = \sqrt{1 + 24m}$ is sequentially prime. Indeed, we know that all primes p, $p \geq 5$ are representatives of residual classes $1\ mod\ 6$ or $5\ mod\ 6$.

We initially assumed that p is a representative of the residual class $1\ mod\ 6$. That is, $p = 1 + 6t,$, with $t \geq 1$.. As such

$$\begin{aligned} &(1+6t)^2 = 1 + 24m \\ &1 + 12t + 36t^2 = 1 + 24m \\ &t(1+3t) = 2m \end{aligned}$$

In order to ensure that $m \in \mathbb{N}$, then if t is odd, then $(1+3t)$ is even and m is integer and if t is even, then m is integer also, then with $t \geq 1$, $m \in \mathbb{N}$.

On the other contrary, let p be is a representative of the residual class $5\ mod\ 6$, $p = 5 + 6t$ for some $t \in \mathbb{N} \cup \{0\}$. As a result

$$\begin{aligned} &(5+6t)^2 = 1 + 24m \\ &25 + 60t + 36t^2 = 1 + 24m \\ &24 + 60t + 36t^2 = 24m \\ &2 + 5t + 3t^2 = 2m \\ &(t+1)(3t+2) = 2m \end{aligned}$$

in order to ensure that $m \in \mathbb{N}$, then if t, is odd, then $(t+1)$ is even and m is integer and if t is even,$(3t+2)$ is even and m is integer and also if $t = 0$, $m = 1$, then with $t \geq 0$, $m \in \mathbb{N}$.

Table 1 shows the sequential results of prime numbers in accordance with the restrictions imposed in sequential terms for m, and previously deducted.

Table 1 displays clearly that the numbers in bold are primes greater or equal to 5, and all the existing composite numbers in the same table have decompositions in factors of primes greater or equal to 5.

3.7 Application II

Other sequential representations for m can even generate for all primes $p \geq 5$. For example, if $m = 1$ or $m = 2 + 5k$ or $m = 5(k+1)$, $k \in \mathbb{N} \cup \{0\}$.

Table 2 has all the integer values of $\sqrt{a} = \sqrt{1 + 24m}$ within the sequential frame set to m previously, $1 \leq m \leq 1162$. Blank cells correspond to all primes p where sequentially $5 \leq p \leq 167$ and blue cells correspond to composite numbers in accordance with the corollary 2 established in section 3.4.

In addition from Table 2, it is deduced that by generating all primes sequentially and in a very simple way, we can eliminate all the values $\sqrt{a} \notin \mathbb{N}$ and all the composite numbers ${p_1}^{r_1}{p_2}^{r_2}{p_3}^{r_3} \dots {p_n}^{r_n} = \sqrt{a}$. The remaining values $\sqrt{a} \in \mathbb{N}$ corresponds to all primes sequentially $p \geq 5$.

Table 1. Values of $p = \sqrt{1+24m}$ with $2m = t(1+3t)$ or $2m = (t+1)(3t+2)$

t	$m = t(1+3t)/2$	$1+24m$	$\sqrt{1+24m}$	$m = (t+1)(3t+2)/2$	$1+24m$	$\sqrt{1+24m}$
0				1	25	**5**
1	2	49	**7**	5	121	**11**
2	7	169	**13**	12	289	**17**
3	15	361	**19**	22	529	**23**
4	26	625	25=5*5	35	841	**29**
5	40	961	**31**	51	1225	35=5*7
6	57	1369	**37**	70	1681	**41**
7	77	1849	**43**	92	2209	**47**
8	100	2401	49=7*7	117	2809	**53**
9	126	3025	55=5*11	145	3481	**59**
10	155	3721	**61**	176	4225	65=5*13
11	187	4489	**67**	210	5041	**71**
12	222	5329	**73**	247	5929	77=7*11
13	260	6241	**79**	287	6889	**83**
14	301	7225	85=5*17	330	7921	**89**
15	345	8281	91=7*13	376	9025	95=5*19

Table 2. All integer values of $\sqrt{1+24m}$ with $m = 1$ or $m = 2+5k$ or $m = 5(k+1)$

m	$a = 1+24m$	$\sqrt{a}$	m	$a = 1+24m$	$\sqrt{a}$
1	25	5	287	6889	83
2	49	7	330	7921	89
5	121	11	345	8281	91=7*13
7	169	13	392	9409	97
12	289	17	425	10201	101
15	361	19	442	10609	103
22	529	23	477	11449	107
35	841	29	495	11881	109
40	961	31	532	12769	113
57	1369	37	590	14161	119=7*17
70	1681	41	672	16129	127
77	1849	43	715	17161	131
92	2209	47	737	17689	133=7*19
117	2809	53	805	19321	139
145	3481	59	852	20449	143=11*13
155	3721	61	925	22201	149
187	4489	67	950	22801	151
210	5041	71	1027	24649	157
222	5329	73	1080	25921	161=7*23
247	5929	77=7*11	1107	26569	163
260	6241	79	1162	27889	167

3.8 Theorem 4

If $a \in \mathbb{N}$, is representative of the residual class $1 \bmod 24$, such that $\sqrt{a} \notin \mathbb{N}$, then a is a prime or a composite number of the form pq, where $q - p = 24s$, for some $s \in \mathbb{N}$ and p is a prime ≥ 5.

Proof. Let $a \in \mathbb{N}$ is representative of the residual class $1 \bmod 24$, then, there is $m \in \mathbb{N}$ such that $a = 1 + 24m$. We consider that a is not a prime. Therefore, $a = {p_1}^{k_1} \times {p_2}^{k_2} \times \cdots \times {p_n}^{k_n}$ being p_j prime and $k_1, k_2, \cdots, k_n \in \mathbb{N}$. Given that $\sqrt{a} \notin \mathbb{N}$, there is at least one j, $1 \leq j \leq n$ such that k_j is not divisible by 2. Be $k_j = 1 + 2l$ with $l \in \mathbb{N}$. Then we have that,

$$\begin{aligned} a &= {p_1}^{k_1} \times \cdots \times {p_j}^{k_j} \times \cdots \times {p_n}^{k_n} \\ &= {p_1}^{k_1} \times \cdots \times p_j \times {p_j}^{2l} \times \cdots \times {p_n}^{k_n} \\ &= p_j \times {p_1}^{k_1} \times \cdots \times {p_j}^{2l} \times \cdots \times {p_n}^{k_n} \\ &= p_j q \end{aligned} \tag{5}$$

being $q = {p_1}^{k_1} \times \cdots \times {p_j}^{2l} \times \cdots \times {p_n}^{k_n}$. Thus $1 + 24m = p_j q$, with p_j prime $p_j \geq 5$. Then,

$$\begin{aligned} q - p_j &= {p_1}^{k_1} \times \cdots \times {p_j}^{2l} \times \cdots \times {p_n}^{k_n} - p_j \\ &= \frac{a}{p_j} - p_j \\ &= \frac{a - {p_j}^2}{p_j} \\ &= \frac{(1+24m) - (1+24n)}{p_j} \\ &= \frac{24(m-n)}{p_j} \\ &= 24s \end{aligned} \tag{6}$$

with $s \in \mathbb{N}$ given that p_j is a divisor of $(m - n)$ as $q - p_j \in \mathbb{N}$. Therefore, the theorem is proved.

3.9 Application III

Table 3, essentially proves the importance of their relationships in conjunction with each of the relevant terms mentioned in the Theorem 4. $m = 2 + 5k$ or $m = 5(k + 1)$, $k \in \mathbb{N} \cup \{0\}$ are considered as sequential structure for m. The composite numbers according to theorem 4 are highlighted in blue, the numbers that are not highlighted correspond to prime numbers.

3.10 Theorem 5

Let $a = 1 + 24m$, with $m \in \mathbb{N}$. If $m = 1 + 5s$ with $s \geq 1$, then exists $q \in \mathbb{N}$ such that $a = 5q$, and $q - 5 = 24s$.

Demonstration. Let $a = 1 + 24m$, with $m \in \mathbb{N}$. If $m = 1 + 5s$ for $s \geq 1$ it can be deduced that

$$\begin{aligned} a &= 1 + 24(1 + 5s) \\ &= 25 + 120s \\ &= 5(5 + 24s) \\ &= 5q \end{aligned}$$

where $p = 5 + 24s$, then, $q - 5 = 24s$.

Observation. Table 4 shows calculations that support what was proved previously.

Table 3. Prime and composite numbers when $\sqrt{a}$ is not integer in $a = 1 + 24m$

m	$a = 1 + 24m$	$N_c = pf$	$f - p = 24s$	m	$a = 1 + 24m$	$N_c = pf$	$f - p = 24s$
10	241			102	2449	31·79	24·2
17	409			105	2521		
20	481	13·37	24·1	107	2569	7·367	24·15
25	601			110	2641	19·139	24·5
27	649	11·59	24·2	112	2689		
30	721	7·103	24·4	115	2761	11·251	24·10
32	769			120	2881	43·67	24·1
37	889	7·127	24·5	122	2929	29·101	24·3
42	1009			125	3001		
45	1081	23·47	24·1	127	3049		
47	1129			130	3121		
50	1201			132	3169		
52	1249			135	3241	7·463	24·19
55	1321			137	3289	11·299	24·12
60	1441	11·131	24·5	140	3361		
62	1489			142	3409	7·487	24·20
65	1561	7·223	24·9	147	3529		
67	1609			150	3601	13·277	24·11
72	1729	7·247	24·10	152	3649	41·89	24·2
75	1801			157	3769		
80	1921	17·113	24·4	160	3841	23·167	24·6
82	1969	11·179	24·7	162	3889		
85	2041	13·157	24·6	165	3961	17·233	24·9
87	2089			167	4009	19·211	24·8
90	2161			170	4081	7·583	24·24
95	2281			172	4129		
97	2329	17·137	24·5	175	4201		
100	2401	7·343	24·14	177	4249	7·607	24·25

Table 4. Values of $a = 1 + 24m$ with $m = 1 + 5s$, where $a = 5q$ and $q - 5 = 24s$ to $s \geq 1$

s	$m = 1 + 5s$	$a = 1 + 24s$	$a = 5q$	$q - 5 = 24s$
1	6	145	5·29	24·1
2	11	265	5·53	24·2
3	16	385	5·77	24·3
4	21	505	5·101	24·4
5	26	625	5·125	24·5
6	31	745	5·149	24·6
7	36	865	5·173	24·7
8	41	985	5·197	24·8
9	46	1105	5·221	24·9
10	51	1225	5·245	24·10
11	56	1345	5·269	24·11
12	61	1465	5·293	24·12
13	66	1585	5·317	24·13
14	71	1705	5·341	24·14
15	76	1825	5·365	24·15
16	81	1945	5·389	24·16

4. CONCLUSIONS

The congruence $1\,mod\,24$ stablishes a direct interconnection with prime numbers and by using this, we can get all the primes $p \geq 5$. There is no other congruence known that allows this, what this shows is that all the same primes and numbers greater than five arise or are generated from an own sequential structure of congruence $1\,mod\,24$ as it was proved in the first four properties proposed in this paper. Furthermore, all of the composite numbers in $a = 1 + 24m$ to $m \geq 1$, have only two forms: one when $\sqrt{a}$ is integer, in this case the composite numbers N_c are $N_c = [p_1{}^{r_1} p_2{}^{r_2} p_3{}^{r_3} \ldots p_n{}^{r_n}]^2$ and another when $\sqrt{a}$ is not integer, in this case the composite numbers N_c are $N_c = pf$ and $f - p = 24s$ existing special cases such as that which was proposed in the Theorem 5.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Williamson J. The elements of Euclid, with dissertations, Clarendon Press, Oxford. 1782;63.
2. Horsley S. The sieve of eratosthenes. Being an account of his method of finding all the prime numbers. Philosophical Transactions (1683-1775). 1772;62: 327-347.
3. Selberg A. An elementary proof of the prime number theorem. Annals of Mathematics. 1949;2(50):305-313. Re-printed in: "Atle Selber Collected Papers. Springer-Verlag, Berlin Heidelberg New York. 1989;1:379-387.
4. Riemann B. On the number of Prime Numbers less than a given quantity. Translated by D.R. Wilkins. 1998;9.
5. Edwards HM. Riemann's zeta function, New York: Academic Press, Zbl 0315.10035; 1974.
6. Leonhard Euler (Presented: August 2, 1736; Published: 1741). "Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio" (English: "A proof of certain theorems regarding prime numbers"), Commentarii Academiae Scientiarum Petropolitanae. 1741;8:141–146.
7. Long Calvin T. Elementary introduction to number theory (2nd ed.). Lexington: D. C. Heath and Company, LCCN 77171950; 1972.
8. Grytczuk A, Luca F, Wójtowicz M. Another note on the greatest prime factors of Fermat numbers. Southeast Asian Bulletin of Mathematics (Springer-Verlag). 2001; 25(1):111–115.
DOI: 10.1007/s10012-001-0111-4
9. Burton David M. The history of mathematics / an introduction (7th ed.). McGraw-Hill, ISBN 978-0-07-338315-6; 2011.
10. Ore Oystein. Number Theory and Its History, Dover, ISBN 978-0-486-65620-5; 1988.
11. Smyth C. A coloring proof of a generalisation of Fermat's little theorem. Amer. Math. Monthly. 1986;93:469–471.
12. Nagell T. Primes. §3 in introduction to number theory. New York: Wiley. 1951; 13-14.
13. Mora FW. Introduction to the theory of numbers. School of mathematics, Technology Institute from Costa Rica (Spanish: Introducción a la Teoría de Números. Escuela de Matemáticas, Instituto Tecnológico de Costa Rica); 2014.
14. Euler L. An arithmetic theorem proved by a new method, New Memoirs of the St. Petersburg Imperial Academy of Sciences. 8:74-104. Available on-line in: Ferdinand Rudio, ed., Leonhardi Euleri Commentationes Arithmeticae (English:

Reviews Arithmetic), volume 1, in: Leonhardi Euleri Opera Omnia, series 1, volume 2 (Leipzig, Germany: B.G. Teubner); 1915.

15. Euclid. The thirteen books of the Elements, 2 (Books III-IX), Translated by Thomas Little Heath (Second Edition Unabridged ed.), New York: Dover, ISBN 978-0-486-60089-5; 1956.
16. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein. Introduction to algorithms, second edition. MIT Press and McGraw-Hill, ISBN 0-262-03293-7. Section 31.3: Modular Arithmetic. 2001;862–868.
17. Carl Friedrich Gauss, Tr. Arthur A. Clarke: Disquisitiones Arithmeticae, (English: Arithmetical Investigations) Yale University Press, ISBN 0-300-09473-6; 1965.
18. David Eugene Smith. A source book in mathematics. Dover Publications Inc., New York. 1959;2.
19. Pettofrezzo Anthony J, Byrkit Donald R. Elements of number theory. Englewood Cliffs: Prentice Hall, LCCN 71081766; 1970.
20. Dorronsoro J, Hernandez E. Numbers, groups and rings. In Spanish: “Números, grupos y anillos”, Addison-Wesley Iberoamericana España S.A.; 1996.
21. Porras-Ferreira JW, Andrade CA. The formation of prime numbers and the solution for Goldbach’s conjectures. World Open Journal of Advanced Mathematics. 2014;2(1):01-32.

    Available:http://scitecpub.com/Journals.php

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/13307