A conjecture of existence of prime numbers on arithmetic progressions

Moreno Borrallo, Juan

July 11, 2018

e-mail: juan.morenoborrallo@gmail.com

"Entia non sunt multiplicanda praeter necessitatem" (Ockam, W.)

Abstract

In this paper it is proposed and proved a conjecture of existence of a prime number on the arithmetic progression

$$S_{a,b} = \{ab + 1, ab + 2, ab + 3, ..., ab + (b - 1)\} \quad (1)$$

As corollaries of this proof, they are proved many classical prime number's conjectures and theorems, but mainly Bertrand's theorem, and Oppermann's, Legendre's, Brocard's, and Andrica's conjectures. It is also defined a new maximum interval between any natural number and the nearest prime number. Finally, it is stated a corollary which implies some advance on the conjecture of the existence of infinite prime numbers of the form $n^2 + 1$.

2010MSC: 11A41

Keywords. *Arithmetic progression, Interval, Prime number, Oppermann's Conjecture, Legendre's Conjecture, Brocard's Conjecture, Andrica's Conjecture, Pigeonhole Principle, Generalization of the Chinese Remainder Theorem.*

1 Introduction

To begin with, it is proposed the following

Conjecture. *Let two positive integer numbers be* a *and* b, $a \leq b$. *Then, it can be stated that at least one of the terms of the arithmetic progression* $S_{a,b} = \{ab+1, ab+2, ab+3, ..., ab+(b-1)\}$*is a prime number.*

This conjecture is equivalent to the following:

Conjecture reformulated. *Let two positive integer numbers be* a *and* b, $a \leq b$, *such that* $\gcd(a,b) \geq \sqrt{a}$. *Then, it can be stated that exists at least one prime number* p *such that* $a < p < b$.

There are values of a and b for which the Conjecture is already proved, or is similar to other conjectures or theorems. For instance, the Conjecture for $a = 1$ is proved and called Bertrand's Theorem, and the cases $a = b-1$ and $a = b$ put together conform Oppermann's Conjecture [1].

In bullet points, the article develops the following Lemmas:

- *Any composite number can be expressed as a product of two factors, whether prime or composite.*
- *Each composite number of* $S_{a,b}$ *has some proper divisor at the interval* $(1,b)$, *and every number of the interval* $(1,b)$ *is factor of some number of the interval* $S_{a,b}$.
- *From the Pigeonhole Principle, there must be at least two odd numbers of* $S_{a,b}$ *which have the same proper divisor less than* b.
- *For the Conjecture not to hold, it should be possible to create a system of congruences such that each number contained in* $S_{a,b}$ *is multiple of a number of the interval* $(1,b)$.
- *Using some Lemmas and the Generalization of the Chinese Remainder Theorem, the previous Lemma is proved to be impossible for any* b.
- *Subsequently, it is proved the Conjecture. From this (I hope) theorem, there can be proved as corollaries some well-known conjectures (as considering them the most important, I have developed only Oppermann's, Legendre's, Brocard's and Andrica's) and some other corollaries, from which I have chosen two that I considered most relevant.*

2 Definitions

- We use the notation $\mid Letter \mid$ to express the number of elements of a set or interval.
- We use the notation $\{ Letter \}$ to express an indetermined element of a set or interval.
- We define the arithmetic progression

$$S_{a,b} = \{ab + 1, ab + 2, ab + 3, ..., ab + (b - 1)\}$$

- We define $(C) = (1, b)$ as the interval of natural numbers which can be factors of a composite number of $S_{a,b}$.
- We define $A = \{a, a + 2, a + 4, \ldots, a + 2m\}$ as the set of odd numbers of $S_{a,b}$.
- We define $C = \{3, 5, 7, \ldots, 2m + 1\}$ as the set of odd numbers of (C). Therefore, $\mid C \mid = m$.
- We define $C_2 = \{c_1, c_2, ..., c_k\}$ as the numbers of set C, ordered arbitrarily.
- We define System A as the following system of congruences:

$$\begin{gathered} a \equiv r_1 \,(mod\, c_1) \\ \\ a \equiv r_2 \,(mod\, c_2) \\ a \equiv r_3 \,(mod\, c_3) \\ \ldots \\ a \equiv r_k \,(mod\, c_k) \end{gathered} \tag{2}$$

- We define d as the minimum particular solution of System A.
- We define $R = \{r_1, r_2, ..., r_k\}$ as the set of non negative residues of $\{A\}$ $(mod\, c_k)$ (e.g, if $a \equiv -4\,(mod\, 7)$, then $r = 3$). Note that one residue can be equal or different to another residue, as $\{A\}$ may be multiple of one, two or more $\{C\}$. Also, note that$\{R\}$ is 0 or odd, as it is a residue of some odd number modulo other odd number.
- We define $X = \{x_1, x_2, ..., x_k\}$ as the set of multiples of c_k such that $d = c_k x_k + r_k$.

- We define $S = \{s_1, s_2, s_3, ..., s_n\}$ as the set of non negative residues such that $x_k \equiv s_k \, (mod \, c_k)$. Some element s_k is called "simplified", when it is assigned to be equal to some expression (e.g., $s_1 = (r_2 - r_1) \, m_1$) and this expression is reduced to an equivalent non negative residue $(mod \, c_k)$. For instance, if $s_1 = (3-7) * 5 = -20$, and thus $x_1 \equiv -20 \, (mod \, 5)$, then "$s_1$ simplified" would mean that $s_1 = 0$, so $x_1 \equiv 0 \, (mod \, 5)$.

- We define $M = \{m_1, m_2, m_3, ..., m_n\}$ as the set of minimum multiplicative inverses defined along the paper.

- We define $c_p > c_o > c_n$ as the three greatest odd numbers of set C_2. Thus, $c_p = 2m + 1$, $c_o = 2m - 1$ and $c_n = 2m - 3$.

- We define $c_m < c_n$ as some odd number, such that $gcd \, (c_m, c_n, c_o, c_p) = 1$. Note that $c_m = 2m - k \mid 3 < k < 2m - 2$.

3 Main theorems

- **Pigeonhole Principle .** *Let it be two sets X (with n elements) and Y (with k elements) and an application*

$$f : X \rightarrow Y$$

Then, despite of which application f are we considering, if $n > k$ there are at least two elements of X, x_1 and x_2 ($x_1 \neq x_2$), such that $f(x_1) = f(x_2)$.

- **Generalization of the Chinese Remainder Theorem**. *Let us consider the positive integers $n_1, n_2, \ldots, n_k$ and let them be $q_1, q_2, \ldots, q_k$ any integers. Then, the congruence system*

$$x \equiv q_1 (mod \, n_1), \ldots, x \equiv q_k (mod \, n_k)$$

has a solution if, and only if, $gcd \, (n_i, n_j)$ is divisor of $q_i - q_j$ for every $i \neq j$.

When this condition is satisfied, then the general solution constitutes a single congruence class module n, where n is the least common multiple of $n_1, n_2, \ldots, n_k$.

4 Conjecture proof

4.1 Basic lemmas

- **Lemma 1**. *Any composite number can be expressed as a product of two factors, whether prime or composite.*

Lemma 1 is trivial, because if any natural number could not be expressed as a product of natural numbers greater than one, then it would be prime by definition.

- **Lemma 2.** *Any number in $S_{a,b}$ has a proper divisor less than b.*

The maximum value of an element of $S_{a,b}$, by definition, is $b^2 + b - 1$.

If the two multiples where equal to b, then the resulting number would be b^2, which does not belong to $S_{a,b}$.

If one multiple where equal to b, and the other greater than b, then the minimum resulting number would be $b^2 + b$, which does not belong to $S_{a,b}$ and is greater than any possible number of any $S_{a,b}$.

If the two multiples where greater than b, then the minimum resulting number would be $b^2 + 2b + 1$, which does not belong to $S_{a,b}$ and is greater than any possible number of any $S_{a,b}$.

Thus, at least one factor of every composite number contained in $S_{a,b}$ is less than b.

- **Lemma 3**. *Every natural number of (C) is proper divisor of some number of $S_{a,b}$.*

Lemma 3 is almost trivial because $S_{a,b}$ is wider than (C), as $\mid S_{a,b} \mid = b - 1$, and $\mid (C) \mid = b - 2$; thus, every natural number of (C) is proper divisor of some $\{S_{a,b}\}$.

- **Lemma 4**. *For all the odd numbers of $S_{a,b}$ to be composite numbers, and taking into account Lemma 3, then, if we pair each odd number of (C) with one of its possible multiples in $S_{a,b}$, there must be at least two odd numbers of $S_{a,b}$ which are multiple of the same odd number of (C).*

Lemma 4 can be stated from Lemma 3 and from the Pigeonhole Principle (Dirichlet's principle)[2], specified at the Main theorems section.

In our case, set X would be $S_{a,b}$, and Y would be (C). As there is one more element in $S_{a,b}$ than in (C), in order for this element to be composite, there must exist an element of (C) which is factor of two elements of $S_{a,b}$.

As in (C) at least the last number is even (number 2), then always there are equal or less odd numbers in (C) than even numbers. Subsequently, and as all composite even numbers in $S_{a,b}$ are multiples of two and can be impaired one to one with all the pairs of (C), then the element of (C) which is factor of two elements of $S_{a,b}$ must be odd.

To show it more clearly, consider the two possible cases:

- If b is even, or if a and b are both odd, then we can establish a parity bijection between $S_{a,b}$ and (C) as follows:

$$\begin{aligned} ab &\dashrightarrow b-2 \\ ab+1 &\dashrightarrow b-1 \\ ab+2 &\dashrightarrow b-4 \\ &\dots \\ ab+b-2 &\dashrightarrow 2 \end{aligned} \tag{3}$$

As there is one number of $S_{a,b}$ still unimpaired ($ab+b-1$), and as $ab+b-2$ is even, then the element of $S_{a,b}$ left must be odd. Thus, as composite odd numbers must have odd factors, the element of (C) which is factor of two elements of $S_{a,b}$ must be odd.

- If a is even and b is odd, then we can establish a parity bijection between $S_{a,b}$ and (C) as follows:

$$\begin{aligned} ab &\dashrightarrow b-1 \\ ab+1 &\dashrightarrow b \\ ab+2 &\dashrightarrow b-3 \\ &\dots \\ ab+b-1 &\dashrightarrow 2 \end{aligned} \tag{4}$$

As there is one number of (B) still unimpaired ($ab+b-2$), and as $ab+b-1$ is even, then the element of $S_{a,b}$ left must be odd. Thus, as composite odd numbers must have odd factors, the element of (C) which is factor of two elements of $S_{a,b}$ must be odd.

- **Lemma 5.** *Every three consecutive odd numbers n_1, n_2, n_3 are coprime numbers two to two. Therefore,* $\gcd(n_1, n_2, n_3) = 1$*, and* $lcm\ (n_1, n_2, n_3) = n_1 n_2 n_3$.

If n_1, n_2, n_3 are consecutive odd numbers, then they can be renowned as n_1, n_1+2, n_1+4.

As $2 \nmid n_1$, then subsequently:

$$gcd\,(n_1, n_1+2) = gcd\,(n_1, n_1+4) = gcd\,(n_1+2, n_1+4) = 1$$

Therefore, they are coprime two to two, and therefore $lcm\,(n_1, n_2, n_3) = n_1 n_2 n_3$

- **Lemma 6.** *Let it be the set* $C = \{3, 5, 7, \ldots, 2m+1\}$, *and* $c_n < c_o < c_p$ *the greatest elements of set* C. *Then, if* $\mid C \mid \geq 5$, *we can affirm that it exists some element* $c_m < c_n$ *such that* $\gcd\,(c_m, c_n) = \gcd\,(c_m, c_o) = \gcd\,(c_m, c_p) = 1$, *so* $\gcd\,(c_m, c_n, c_o, c_p) = 1$.

As c_n, c_o, c_p are the greatest elements of set C, then they are consecutive odd numbers, and they can be renowned as c_n, c_n+2, c_n+4.

According to Lemma 5, c_n, c_o, c_p are coprime two to two, so $gcd\,(c_n, c_o, c_p) = 1$.

As $\mid C \mid \geq 5$, then $c_n \neq 3$. As c_n, c_o, c_p are consecutive odd numbers, then at least one of them is divisible by three, and thus $c_m \neq 3$. We have then several cases:

Case 1. If $3 \nmid c_p$, then at least $c_m = c_n - 2$, because then $3 \nmid c_n - 2$, and if some odd prime number $p > 3$ divides $c_n - 2$, then it can not divide any c_n, c_n+2, c_n+4. Subsequently, the Lemma is proved if $3 \nmid c_p$.

Case 2. If $3 \mid c_p$, then $3 \nmid c_o$, $3 \nmid c_n$ and $3 \mid c_n - 2$. Then, it can be reasoned that:

a) If $5 \nmid c_n - 4$, then at least $c_m = c_n - 4$. In this case, $3 \mid c_n - 2$, so $3 \nmid c_n - 4$. Thus, if some prime number $p > 5$ divides $c_n - 4$, then it can not divide any c_n, c_n+2, c_n+4. Subsequently, the Lemma is proved if $3 \mid c_p$ and $5 \nmid c_n - 4$.

b) If $5 \mid c_n - 4$, then at least $c_m = c_n - 6$. In this case, $3 \mid c_n - 2$, so $3 \nmid c_n - 6$, and if $5 \mid c_n - 4$, then $5 \nmid c_n - 6$. Thus, if some prime number $p > 5$ divides $c_n - 6$, then it can not divide any c_n, c_n+2, c_n+4. Subsequently, the Lemma is proved if $3 \mid c_p$ and $5 \mid c_n - 4$.

Note that the proof presented is considering that $\mid C \mid \geq 6$; notwithstanding, is easily verifiable that for $\mid C \mid = 5$, Lemma 6 holds, as in set $C = \{3, 5, 7, 9, 11\}$, we find that $\gcd\,(5, 7, 9, 11) = 1$.

4.2 Proof development

Non-compliance assumption: *Conjecture is false; therefore, it does exist some $S_{a,b}$ for which every natural number of this arithmetic progression is composite.*

Let us recall that, at the Definitions section, we have defined a set of the odd numbers of $S_{a,b}$ as set A, another set of the odd numbers of (C) as set C and one third set of the elements of set C ordered arbitrarily as set C_2.

If the *Non-Compliance assumption* holds, then it is possible to create a system of congruences such that each element of set A is multiple of some element of set C_2, applying the *Generalization of the Chinese Remainder Theorem* **[3]**, specified at the Main theorems section.

Applying the *Generalization of the Chinese Remainder Theorem* to the relationship between sets A and C under the *Non-Compliance assumption*, the positive integers $n_1, n_2, \ldots, n_k$ are the elements of set C_2, the number x is the first element of set A ($a \in \mathbb{N}$), and the integers $q_1, q_2, \ldots, q_k$ are the diference between each element of set A and its first element:

$$
\begin{aligned}
a &\equiv 0 \,(mod\, c_1) \\
a &\equiv -2 \,(mod\, c_2) \\
a &\equiv -4 \,(mod\, c_3) \\
&\ldots \\
a &\equiv -2m \,(mod\, c_k)
\end{aligned}
\tag{5}
$$

Therefore, the system would be System A, defined above at the Definitions section. The integers $q_1, q_2, \ldots, q_k$ are transformed to $r_1, r_2, \ldots, r_k$, as defined at the Definitions section. It can be assured that the *Generalization of the Chinese Remainder Theorem* is applicable because:

- Considering the fact that one residue can be equal or different to another residue, as $\{A\}$ may be multiple of one, two or more $\{C_2\}$, the *Generalization of the Chinese Remainder Theorem* is applicable, as in that case $r_i - r_j = 0$, and every $\gcd(c_i, c_j)$ is divisor of 0.
- In case $\gcd(c_i, c_j) = 1$, then $\gcd(c_i, c_j)$ is divisor of every $r_i - r_j$.
- In case $\gcd(c_i, c_j) > 1$, then $\gcd(c_i, c_j)$ must be divisor of $r_i - r_j$, as $\mid r_i - r_j \mid = \mid c_i - c_j \mid$.

We can prove that there is not a solution for System A lower than $b^2 + b$, and subsequently that the *Non-Compliance Assumption* is false, proving and using three Lemmas:

- **Lemma A**. *It does not exist any set A such that each of its elements is multiple of any element of a set C such that set C has less than three elements.*

Case $\mid C \mid = 1$

The set C of one element is defined as $C = \{3\}$.

As set C has one element, set A has two elements; thus, $A = \{a,\, a + 2\}$.

According to the Pigeonhole Principle, both a and $a + 2$ must be multiples of 3. Notwithstanding, if $3 \mid a$, then $3 \nmid a + 2$.

Therefore, it can not exist any set A such that each of its elements is multiple of any element of a set C of one element.

Case $\mid C \mid = 2$

The set C of two elements is defined as $C = \{3, 5\}$.

As set C has two elements, set A has three elements; thus, $A = \{a,\, a + 2,\, a + 4\}$.

According to the Pigeonhole Principle, at least two of the elements of set A must be multiples of the same element of set C.

The distance between a and $a + 4$ is less than 5; therefore, there can not exist two elements of set A multiples of 5.

There is no distance between the elements of set A which is multiple of 3. Therefore, if any of the three is multiple of 3, then the remaining two elements can not be multiples of 3.

As there can not be two elements of set A multiples of 5, and there can not be two elements of set A multiples of 3, it can not exist any set A such that each of its elements is multiple of any element of a set C of two elements.

Therefore, Lemma A is demonstrated.

- **Lemma B**. *The least common multiple of the last three elements of a set C equal or greater than 3 is always greater than* $b^2 + b$.

According to Lemma A, set C must be at least of 3 elements.

At the Definitions Section, set C was defined as $C = \{3, 5, 7, \ldots, 2m+1\}$. Therefore, $\mid C \mid = m$.

As set C is formed by the odd numbers of $(C) = (1, b)$, then b must be lower than the odd number next to the last element of set C. That is,

$$b < 2m + 3 \tag{6}$$

Therefore, we can state that:

$$max\,(b) = 2m + 2 \tag{7}$$

Consequently, substituting, we can state that:

$$max\,(b^2 + b) = (2m + 2)^2 + 2m + 2 \tag{8}$$

Operating,

$$max\,(b^2 + b) = 4m^2 + 10m + 6 \tag{9}$$

Thus, Lemma B is affirming that:

$$lcm\,(3, 5, 7, \ldots, 2m + 1) > 4m^2 + 10m + 6 \tag{10}$$

According to Lemma 5, we can affirm that

$$min\,(lcm\,(3, 5, 7, \ldots, 2m + 1)) = (2m - 3)(2m - 1)(2m + 1)$$

$$(2m - 3)(2m - 1)(2m + 1) = 8m^3 - 12m^2 - 2m + 3 \tag{11}$$

Substituting on (10),

$$8m^3 - 12m^2 - 2m + 3 > 4m^2 + 10m + 6 \tag{12}$$

Operating, this expression is equivalent to:

$$8m^3 - 8m^2 - 12m - 3 > 0 \tag{13}$$

It is easy to verify that this inequation has the following critic point:

$$m > \frac{1}{4}(3 + \sqrt{21}) \tag{14}$$

For every $m > \frac{1}{4}(3 + \sqrt{21})$, the inequation holds true. As we have stated in Lemma A that $min\,(m) = 3$, and $\frac{1}{4}(3 + \sqrt{21}) < 3$, then the inequation holds true for every number of elements of set C equal or greater than 3.

Subsequently, it is proved that the least common multiple of the last three elements of set C is greater than $b^2 + b$ for every number of elements of set C equal or greater than 3. Therefore, it is proved Lemma B.

- **Lemma C**. *Regarding the minimum solution d of System A, we can affirm that either* $d = 0$, $d = 1$, $d \in C$, *or* $d > b^2 + b$.

According to the *Generalization of the Chinese Remainder Theorem,*

$$a \equiv d \, (mod \, lcm \, (3, 5, 7, \ldots, 2m + 1)) \tag{15}$$

Where d is the particular solution to the system of congruences. Therefore, and noting that $a \in \mathbb{N}$, the general solution of the system of congruences such that each element of set A is multiple of any element of set C can be expressed as

$$a = d + mcm \, (3, 5, 7, \ldots, 2m + 1)t \; \forall t \geq 0 \tag{16}$$

The minimum solution of the system of congruences can be found for $t = 0$. Thus,

$$min \, (a) = d \tag{17}$$

Therefore, if it is proved that $min \, (d) > max \, (b^2 + b)$, then a system of congruences such that each element of set A is multiple of any element of set C can not exist.

Considering the whole universe of possible sets C_2, and considering Lemmas 5 and 6, we can reason:

- d is a solution of a System A if and only if

$$\begin{gathered} d \equiv r_1 \, (mod \, c_1) \\ d \equiv r_2 \, (mod \, c_2) \\ d \equiv r_3 \, (mod \, c_3) \\ \ldots \\ d \equiv r_k \, (mod \, c_k) \end{gathered} \tag{18}$$

- Let it be $\mid C_2 \mid \geq 5$. Considering Lemma 5, at least the three greatest odd numbers of set C_2 are coprime, and considering Lemma 6, set C_2 contains at least some other odd number coprime to this three numbers. This elements of C_2, as defined at the Definitions section, are $c_p > c_o > c_n > c_m$, and dividing d, they leave the corresponding non negative residues r_p, r_o, r_n, r_m.

Then, solving the system of congruences, and as $d \in \mathbb{N}$, it is clear that:

Step 1)

$$d = r_p + (2m+1)x_p \ \mid x_p \in \mathbb{N} \tag{19}$$

Step 2)

Thus,

$$r_p + (2m+1)x_p \equiv r_o \,(mod\,(2m-1)) \tag{20}$$
$$(2m+1)\,x_p \equiv (r_o - r_p)\ (mod\,(2m-1))$$

If we call the minimum multiplicative inverse of $(2m+1)$ mod $(2m-1)$ as m_1,

$$x_p \equiv (r_o - r_p)\,m_1\,(mod\,(2m-1) \tag{21}$$

Thus, $s_1 = (r_o - r_p)\,m_1$ simplified, as defined at the Definitions section.

Subsequently,

$$d = r_p + (2m+1)x_p = r_p + (2m+1)\,(s_1 + (2m-1)x_o) =$$
$$= (r_p + (2m+1)s_1) + (2m+1)(2m-1)x_o \ \mid x_o \in \mathbb{N} \tag{22}$$

Step 3)

Thus,

$$(r_p + (2m+1)s_1) + (2m+1)(2m-1)x_o \equiv r_n\,(mod\,(2m-3)) \tag{23}$$

$$(2m+1)(2m-1)x_o \equiv (r_n - (r_p + (2m+1)s_1))\ (mod\,(2m-3)) \tag{24}$$

If we call the minimum multiplicative inverse of $(2m+1)(2m-1)$ mod $(2m-3)$ as m_2,

$$x_o \equiv (r_n - (r_p + (2m+1)s_1))\,m_2\,(mod\,(2m-3)) \tag{25}$$

Let us define s_2 as $(r_n - (r_p + (2m+1)s_1))\,m_2$ simplified.

Subsequently,

$$d = (r_p + (2m+1)s_1) + (2m+1)(2m-1)\,(s_2 + (2m-1)x_n) =$$

$$= (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2) + (2m+1)(2m-1)(2m-3)x_n \ \mid x_n \in \mathbb{N} \tag{26}$$

Step 4)

Thus,

$$(r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2) + (2m+1)(2m-1)(2m-3)x_n \equiv r_m \,(mod\,(2m-k)) \tag{27}$$

$$(2m+1)(2m-1)(2m-3)x_n \equiv (r_m - (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2))\ (mod\,(2m-k)) \tag{28}$$

If we call the minimum multiplicative inverse of $(2m+1)(2m-1)(2m-3)$ mod $(2m-k)$ as m_3,

$$x_n \equiv (r_m - (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2))\, m_3 \,(mod\,(2m-k)) \tag{29}$$

Let us define s_3 as $(r_m - (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2))\, m_3$ simplified.

Subsequently,

$$d = (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2) + (2m+1)(2m-1)(2m-3)\,(s_3 + (2m-k)x_m)$$

$$d = (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2 + (2m+1)(2m-1)(2m-3)s_3) +$$

$$(2m+1)(2m-1)(2m-3)(2m-k)x_m \ \mid x_m \in \mathbb{N} \tag{30}$$

Therefore, at least, the minimum particular solution for a set C_2 such that $\mid C_2 \mid \geq 5$ is

$$min(d) = (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2 + (2m+1)(2m-1)(2m-3)s_3) \tag{31}$$

Thus, if there are n numbers coprime two to two in set C_2,

$$min(d) = r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2 + (2m+1)(2m-1)(2m-3)s_3 + ...$$

$$... + (2m+1)(2m-1)(2m-3)...(2m-k)s_{n-1} \tag{32}$$

Let us analyze the range of values of r_p and the set $S = \{s_1, s_2, s_3, ..., s_{n-1}\}$, in order to prove Lemma C.

By definition, $1 \leq r_p \leq 2m$. As pointed at the Definitions section, r_p is 0 or odd, and thus either $r_p = 0$, or $r_p = 1$, or $r_p \in C$.

By definition, every element of set S is non negative, so it is clear that if $s_{n\geq 3} \neq 0$, then $min(d) \geq (2m+1)(2m-1)(2m-3)$, and as proved in Lemma B, $max\,(b^2+b) < (2m+1)(2m-1)(2m-3)$, so if $s_{n\geq 3} \neq 0$, then $min(d) > b^2 + b$ and Lemma C holds.

By definition, $s_3 = (r_m - (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2))\, m_3$ simplified.

By definition, as it is a multiplicative inverse, $m_3 \neq 0$ and $m_3 \nmid (2m-k)$. Thus, $s_3 = 0$ if and only if

$$r_m - (r_p + (2m+1)s_1 + (2m+1)(2m-1)s_2) = 0 \tag{33}$$

As $m > 0$, $2m+1 > r_m$ and $(2m+1)\,(2m-1) > r_m$ the only possible solution for (36) would imply that $s_1 = 0$, $s_2 = 0$ and $r_p = r_m$. In this case, note that $min(d) = r_p$, so either $d = 0$, $d = 1$, or $d \in C$.

Subsequently, for all sets C_2 such that $\mid C_2 \mid \geq 5$, we can affirm that the minimum solution d of System A is either $d = 0$, $d = 1$, $d \in C$, or $d > b^2 + b$.

It is easily verifiable that Lemma C holds also for $\mid C_2 \mid = 3$ and $\mid C_2 \mid = 4$. According to Lemma A, it does not exist any set A such that each of its elements is multiple of any element of a set C such that set C has less than three elements. Therefore, Lemma C is demonstrated.

Subsequently, it is proved that the minimum particular solution to the system of congruences is greater than $b^2 + b$ for every number of elements of set C equal or greater than 3.

Therefore, and according to Lemma B, $a > b^2 + b \; \forall t \geq 0$; subsequently, a system of congruences such that each element of set A is multiple of any element of set C lower than $b^2 + b$ can not exist, as by definition $a < b^2 + b$.

Subsequently, as there is not a solution for a system of congruences such that each element of set A is multiple of any element of set C lower than $b^2 + b$, it is proved that it is impossible that each element of set A is multiple of an element of set C.

Thus, the *Non-Compliance assumption* is false, and it is proved that at least one number of the arithmetic progression $S_{a,b}$ is prime.

Therefore, it is demonstrated the Conjecture.

5 COROLLARIES

5.1 First corollary: Oppermann's Conjecture

Oppermann's Conjecture can be expressed as follows:

$$\forall n > 1 \in \mathbb{N}, \exists P_a, P_b / n^2 - n < P_a < n^2 < P_b < n^2 + n \tag{34}$$

As noted in the Introduction section, this is equivalent to the Conjecture proved, for the cases $a = b - 1$ and $a = b$ put together, so the Conjecture proof implies directly Oppermann's Conjecture proof.

5.2 Second corollary: Legendre's Conjecture

Legendre's Conjecture[4] states that for every natural number n, exists at least a prime number p such that $n^2 < p < (n+1)^2$.

As $(n+1)^2 = n^2 + 2n + 1$, and according to Oppermann's Conjecture proved, we know that:

$$n^2 < P_a < n^2 + n < P_b < (n+1)^2 \tag{35}$$

Therefore,

$$n^2 < P_a < P_b < (n+1)^2 \tag{36}$$

Therefore, it is demonstrated Legendre's Conjecture.

5.3 Third corollary: Brocard's Conjecture

Brocard's Conjecture[5] states that, if p_n and p_{n+1} are two consecutive prime numbers greater than two, then between p_n^2 and p_{n+1}^2 exist at least four prime numbers.

According to the conjecture's statement,

$$2 < p_n < p_{n+1} \tag{37}$$

As the minimum distance between primes is two, we can state that:

$$p_n < M < p_{n+1} \tag{38}$$

Where M is some natural number between p_n and p_{n+1}. Subsequently,

$$p_n^2 < M^2 < p_{n+1}^2 \tag{39}$$

As $M \geq p_n + 1$, and according to the demonstrated Oppermann's conjecture,

$$p_n^2 < P_a < p_n^2 + p_n < P_b < M^2 \tag{40}$$

Idem, as $p_{n+1} \geq M+1$, and according to Oppermann's Conjecture proved,

$$M^2 < P_c < M^2 + M < P_d < p_{n+1}^2 \tag{41}$$

Therefore,

$$p_n^2 < P_a < P_b < P_c < P_d < p_{n+1}^2 \tag{42}$$

Therefore, it is demonstrated Brocard's Conjecture.

5.4 Fourth corollary: Andrica's Conjecture

Andrica's Conjecture[6] states that for every pair of consecutive prime numbers p_n and p_{n+1}, $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$

According to the demonstrated Oppermann's Conjecture, the maximum distance between p_n and p_{n+1} is:

$$n^2 + n + 1 \leq P_n < (n+1)^2 < p_{n+1} \leq n^2 + 3n + 1 \tag{43}$$

It is easily verifiable that:

$$\sqrt{n^2 + 3n + 1} - \sqrt{n^2 + n + 1} < 1 \tag{44}$$

For every value of n. As $n^2 + 3n + 1 \geq p_{n+1}$, and $P_n \geq n^2 + n + 1$, then $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$

Therefore, it is demonstrated Andrica's Conjecture.

5.5 Fifth corollary: a new maximum interval between every natural number and the nearest prime number

According to the exposed in the fourth corollary, it can be stated that the maximum distance between every natural number and the nearest prime number will be:

$$n^2 + 3n - (n^2 + n + 1) = 2n - 1 \tag{45}$$

Therefore, and stating that:

$$n = \sqrt{n^2 + n + 1} \tag{46}$$

It can be determined that:

$$\forall n \in \mathbb{N}, \exists P_a, P_b / (n - (2\sqrt{n} - 1)) \leq P_a \leq n \leq P_b \leq (n + (2\sqrt{n} - 1)) \tag{47}$$

And therefore, we can define a new maximum interval between every natural number and the nearest prime number as:

$$\forall n \in \mathbb{N}, \exists P / n \leq P \leq (n + (2\sqrt{n} - 1)) \tag{48}$$

5.6 Sixth corollary: the existence of infinite prime numbers of the form $n^2 \pm k/0 < k < n$

According to the demonstrated Oppermann's Conjecture, it can be stated that every prime number p_i will be of the following form:

$$p_i = n^2 \pm k/0 < k < n \tag{49}$$

Subsequently, as it is widely proved the existence of infinite prime numbers, and every prime number can be expressed as $n^2 \pm k/0 < k < n$, then it is proved the existence of infinite prime numbers of the form $n^2 \pm k/0 < k < n$.

Acknowledgements

Thanks to Fernando Chamizo for his unvaluable comments and correspondence during this years of Mathematical growth.

Thanks to you, Elena, for being there... ¡always!

References

[1] Oppermann, L. (1882), "*Om vor Kundskab om Primtallenes Mængde mellem givne Grændser*", Oversigt over det Kongelige Danske Videnskabernes Selskabs Forhandlinger og dets Medlemmers Arbejder, p. 169–179.

[2] Herstein, I. N. (1964), *"Topics In Algebra"*, Waltham: Blaisdell Publishing Company, p.90, ISBN 978-1114541016.

[3] Ireland, Kenneth; Rosen, Michael (1990), *"A Classical Introduction to Modern Number Theory"* (2nd ed.), Springer-Verlag, p.34-36, ISBN 0-387-97329-X.

[4] Stewart, Ian (2013), *"Visions of Infinity: The Great Mathematical Problems"*, Basic Books, p. 164, ISBN 9780465022403.

[5] Weisstein, Eric W. "*Brocard's Conjecture*". MathWorld.

[6] Andrica, D. (1986). "*Note on a conjecture in prime number theory*". Studia Univ. Babes–Bolyai Math. 31 (4): 44–48. ISSN 0252-1938. Zbl 0623.10030