An Interval Unifying Theorem about Prime numbers

Moreno Borrallo, Juan

July 14, 2017

e-mail: juan.morenoborrallo@gmail.com

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

Abstract

In this paper it is proved the existence of a prime number in the interval between the square of any natural number greater than one, and the number resulting from adding or subtracting this natural number to its square (Oppermann's Conjecture). As corollaries of this proof, they are proved three classical prime number's conjectures: Legendre's, Brocard's, and Andrica's. It is also defined a new maximum interval between any natural number and the nearest prime number. Finally, it is stated as corollary the existence of infinite prime numbers equal to the square of a natural number, plus a natural number inferior to that natural number, and minus a natural number inferior to that natural number.

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

1 Oppermann's Conjecture

Oppermann's Conjecture[1] can be expressed as follows:

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

Expressed in words, it could be enunciated in the following manner: it exists at least one prime number in the interval between the square of any natural number greater than one, and the number resulting from adding or subtracting this natural number to its square.

1.1 Proof

1.1.1 Previous propositions and considerations

The intervals involved by Oppermann's Conjecture are the following:

$$(A) = (n^2 - n, n^2) \tag{2}$$

$$(B) = (n^2, n^2 + n) \tag{3}$$

(A) and (B) have $(n-1)$ natural numbers.

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

Proposition 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.

Proposition2. *Composite numbers of (A) and (B) cannot be expressed neither a) as the product of two natural numbers greater than n, nor b) as the product of two natural numbers smaller than n; since in those cases their product would be outside (A) and (B).*

Proposition 2 can be verified easily with the minimum product of two natural numbers greater than n:

$$(n+1)(n+1) = n^2 + 2n + 1 > n^2 + n \tag{4}$$

And with the minimum product of two natural numbers smaller than n:

$$(n-1)(n-1) = n^2 - 2n + 1 < n^2 - n \tag{5}$$

Therefore,

Proposition 3. *Each composite number of (A) and (B) can be expressed as a product of a) a number lower than n, and b) a number greater than n.*

Proposition 3 is a corollary of propositions 1 and 2.

We can express this product as:

$$(n-k)(n+m) \tag{6}$$

If we focus on the factor lower than n, in order for this product to be a composite natural number, and to be in (A) or (B),

$$n > (n-k) > 1 \tag{7}$$

We will call (C) to this interval. (C) can be expressed also as follows:

$$(C) = (1, n) \tag{8}$$

(C) has $(n-2)$ natural numbers.

Proposition 4. *Every natural number contained in (C) has a multiple in (A) and (B).*

Proposition 4 is almost trivial because (A) and (B) are wider than (C); thus, every number contained in (C) has a multiple in (A) and another multiple in (B).

Proposition 5. *For all the odd numbers of (A) and (B) to be composite numbers, and taking into account that every natural number contained in (C) has a multiple in (A) and (B), then, if we assign one number of (C) to one of its possible multiples in (A), and to one of its possible multiples in (B), there must be at least two odd numbers of (A) which are multiple of the same odd number of (C), and two odd numbers of (B) which are multiple of the same odd number of (C).*

Proposition 5 can be stated from Proposition 3 and from the Pigeonhole Principle (Dirichlet's principle)[2], which can be stated as follows:

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 $f(x_1) = f(x_2)$.

In our case, set X would be (A) or (B), and Y would be (C). As there is one more element in (A) and one more element in (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 (A), and another (or the same) element of (C) which is factor of two elements of (B).

As every n^2 has the same parity than every n, we can establish a parity bijection between (A) and (C) as follows:

$$\begin{aligned} n^2 &\dashrightarrow n \\ n^2 - 1 &\dashrightarrow n - 1 \\ n^2 - 2 &\dashrightarrow n - 2 \\ &\dots \\ n^2 - n + 2 &\dashrightarrow 2 \end{aligned} \tag{9}$$

As there is one number of (A) still unimpaired ($n^2 - n + 1$), and as $n^2 - n + 2$ is always even, then the element of (A) left must be odd independently of the value of n. Thus, as composite odd numbers must have odd factors, the element of (C) which is factor of two elements of (A) must be odd.

The same parity bijection can be established between (B) and (C), so the element of (C) which is factor of two elements of (B) must be odd.

Proposition 6. *Every three consecutive odd numbers n_1, n_2, n_3 are coprime numbers two to two. Therefore, $mcm\,(n_1, n_2, n_3) = n_1 n_2 n_3$.*

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 $mcm\,(n_1, n_2, n_3) = n_1 n_2 n_3$.

1.1.2 Proof framework

For the sake of clarity, we expose briefly the reasoning steps that we are going to follow through the demonstration basis and development:

1. We make what we denominate a *Non-Compliance assumption*, supposing that Oppermann's Conjecture is false; we suppose that exists some (A) or some (B) for which every natural number contained in them is composite.

2. As even numbers are always composite numbers, we exclude them of the demonstration and we focus solely on odd numbers defining three sets A, B and C such that they contain the odd numbers of (A), (B) and (C).

3. We state that, 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 any element of set C, and another system of congruences such that each element of set B is multiple of any element of set C, applying the *Generalization of the Chinese Remainder Theorem*[3].

4. We note and demonstrate that the minimum general solution of a system of congruences such that each element of set A is multiple of any element of set C is always greater than $n^2 + n$, and that the minimum general solution of a system of congruences such that each element of set B is multiple of any element of set C is always greater than $n^2 + n$.

5. Thus, as there is not a general solution for a system of congruences such that each element of set A is multiple of any element of set C lower than $n^2 + n$, and as there is not a general solution for a system of congruences such that each element of set B is multiple of any element of set C lower than $n^2 + n$, we conclude that the *Non-Compliance assumption* is false, and therefore we consider demonstrated Oppermann's Conjecture.

1.1.3 Proof development

Non-compliance assumption: *Oppermann's Conjecture is false; therefore, it does exist some (A), some (B), or both (A) and (B), for which every natural number contained in them is composite.*

Even numbers, except of number 2, are always composite. Therefore, we will exclude them of the demonstration, and we will focus on odd numbers.

Composite odd numbers can only be product of odd numbers; therefore, and according to proposition 3, in order to all odd numbers of (A) and (B) to be composite numbers, each of them must be multiple of one odd number of (C).

Now we are going to define a set of the odd numbers of (C) as set C; another set of the odd numbers of (A) as set A; and another set of the odd numbers of (B) as set B.

Set C could be expressed as:

$$C = \{3, 5, 7, \ldots, 2m + 1\} \in N \tag{10}$$

Where m is the number of odd numbers of set C (m = $\|$C$\|$).

Let us define $E(C)_i$ as each element of set C. Thus, $E(C)_1 = 3$, $E(C)_2 = 5$, $E(C)_3 = 7$, ..., $E(C)_n = 2m + 1$.

Each of sets A and B could be expressed as

$$A = \{a, a + 2, a + 4, \ldots, a + 2m\} \in N \tag{11}$$

$$B = \{b, b + 2, b + 4, \ldots, b + 2m\} \in N \tag{12}$$

For the sake of simplicity, we will develope the demonstration focusing on the relationship between sets A and C, as the following reasoning and propositions can be applied quite straightly to the relationship between sets B and C.

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 an element of set C, applying the *Generalization of the Chinese Remainder Theorem* as follows:

Generalization of the Chinese Remainder Theorem. *Let us consider the positive integers* $n_1, n_2, \ldots, n_k$ *and let them be* $a_1, a_2, \ldots, a_k$ *any integers. Then, the congruence system*

$$x \equiv a_1 (mod\, n_1), \ldots, x \equiv a_k (mod\, n_k)$$

has a solution if, and only if, $gcd\,(n_i, n_j)$ *is divisor of* $a_i - a_j$ *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 minimum common multiple of* $n_1, n_2, \ldots, n_k$.

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 $C = \{3, 5, 7, \ldots, 2m+1\} \in N$, the number x is the first element of set A (a), and the integers $a_1, a_2, \ldots, a_k$ are the diference between each element of A and its first element. Therefore, the system would be as follows:

$$\begin{gathered} a \equiv 0\,(mod\, E(C)_i) \\ a \equiv -2\,(mod\, E(C)_i) \\ a \equiv -4\,(mod\, E(C)_i) \\ \ldots \\ a \equiv -2m\,(mod\, E(C)_i) \end{gathered} \tag{13}$$

Where some $E(C)_i$ appear two times, as there exists one element of C which is multiple of two elements of set A.

A lucky (and fast!) conclusion supposition. If the system did not have a solution, then we could conclude at this point stating that, as the system did not have a solution, then it would be impossible that each odd number of set A was multiple of an odd number of set C, and as we stated at Proposition 3 that any odd composite number in set A must be multiple of an odd number of set C, thus we would be able to affirm that there would be at least one element of set A which were prime. However, the system has (at least) the following solution:

$$a \equiv 0\,(mod\,3)$$
$$a \equiv -2\,(mod\,5)$$

$$a \equiv -4\,(mod\,7)$$

$$\ldots$$

$$a \equiv -2m\,(mod\,E(C)_i) \tag{14}$$

The system can be re-expressed as follows:

$$a \equiv 0\,(mod\,3)$$
$$a \equiv 3\,(mod\,5)$$

$$a \equiv 3\,(mod\,7)$$

$$\ldots$$

$$a \equiv \left\{ \begin{array}{ll} 0\,(mod\,E(C)_i) & \textbf{if } E(C)_i \mid a \\ 3\,(mod\,E(C)_i) & \textbf{if } E(C)_i \nmid a \end{array} \right\} \tag{15}$$

Where $E(C)_i$ is the element of set C which is multiple of two elements of set A.

It can be seen that, ordered the way above, $a_i - a_j = 0$ for every $gcd\,(n_i, n_j) > 1$; thus, the system has a solution, as every $gcd\,(n_i, n_j) > 1$ is divisor of 0, and every $gcd\,(n_i, n_j) = 1$ is divisor of $a_i - a_j$ independently of the value of $a_i - a_j$.

Therefore, we can not assume *A lucky (and fast!) conclusion supposition* as true.

Proposition 7. *It does not exist any set A such that each of their elements is multiple of any element of a set C such that C has less than three elements.*

Case $\|C\| = 1$

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 $\|C\| = 2$

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, Proposition 7 is demonstrated.

Proposition 8. *The minimum common multiple of the last three elements of a set C equal or greater than 3 is always greater than* $n^2 + n$.

According to Proposition 7, set C must be at least of 3 elements.

According to (9), set C was defined as $C = \{3, 5, 7, \ldots, 2m+1\} \in N$. Therefore, $\|C\| = m$.

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

$$n < 2m + 3 \tag{16}$$

Therefore, we can state that:

$$max\,(n) = 2m + 2 \tag{17}$$

Consequently, substituting, we can state that:

$$max\,(n^2 + n) = (2m+2)^2 + 2m + 2 \tag{18}$$

Operating,

$$max\,(n^2 + n) = 4m^2 + 10m + 6 \tag{19}$$

Thus, Proposition 8 is affirming that:

$$mcm\,(2m-3,\,2m-1,\,2m+1) > 4m^2+10m+6 \tag{20}$$

According to Proposition 6,

$$mcm\,(2m-3,2m-1,2m+1) = (2m-3)(2m-1)(2m+1) = 8m^3-12m^2-2m+3 \tag{21}$$

Substituting on (20),

$$8m^3-12m^2-2m+3 > 4m^2+10m+6 \tag{22}$$

Operating, this expression is equivalent to:

$$8m^3-8m^2-12m-3 > 0 \tag{23}$$

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

$$m > \frac{1}{4}(3+\sqrt{21}) \tag{24}$$

For every $m > \frac{1}{4}(3+\sqrt{21})$, the inequation holds true. As we have stated in Proposition 7 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 minimum common multiple of the last three elements of set C is greater than n^2+n for every number of elements of set C equal or greater than 3. Therefore, it is proved Proposition 8.

Proposition 9. *The minimum general solution of a system of congruences such that each element of set A is multiple of any element of set C is always greater than* n^2+n.

According to the Generalized Chinese Remainder Theorem

$$a \equiv c\,(mod\,mcm\,(3,5,7,\ldots,2m+1)) \tag{25}$$

Where c is the particular solution to the system of congruences. Therefore, 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

$$a = c + mcm\,(3,5,7,\ldots,2m+1)t\,\forall t{\in}Z \tag{26}$$

The minimum general solution of the system of congruences can be found for $t = 0$, that is, it is the particular solution to the system. Thus,

$$min\,(a) = c \tag{27}$$

The minimum particular solution c to the system of congruences must be equal or greater than the minimum common multiple of the last three elements of set C. Therefore,

$$c \geq mcm\,(2m-3,\, 2m-1,\, 2m+1) > n^2+n \tag{28}$$

Subsequently, $a > n^2+n \,\forall t{\in}Z$; thus, a system of congruences such that each element of set A is multiple of any element of set C lower than n^2+n can not exist, as by definition $a < n^2+n$.

Subsequently, as there is not a general solution for a system of congruences such that each element of set A is multiple of any element of set C lower than n^2+n, 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 (A) is prime.

The *Proof Development* section is entirely applicable to the relationship between sets B and C, as set B is defined exactly as set A. Therefore, applying the *Proof Development* section to set B (simply substituting the letters"a, A" with "b, B"), it is proved that it is impossible that each element of set B 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 (B) is prime. Therefore, it is demonstrated Oppermann's Conjecture.

2 COROLLARIES

2.1 First 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:

$$n^2 < P_a < n^2+n < P_b < (n+1)^2 \tag{29}$$

Therefore,

$$n^2 < P_a < P_b < (n+1)^2 \tag{30}$$

Therefore, it is demonstrated Legendre's Conjecture.

2.2 Second 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,

$$2 < p_n < p_{n+1} \tag{31}$$

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

$$p_n < M < p_{n+1} \tag{32}$$

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

Subsequently,

$$p_n^2 < M^2 < p_{n+1}^2 \tag{33}$$

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

$$p_n^2 < P_a < p_n^2 + p_n < P_b < M^2 \tag{34}$$

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

$$M^2 < P_c < M^2 + M < P_d < p_{n+1}^2 \tag{35}$$

Therefore,

$$p_n^2 < P_a < P_b < P_c < P_d < p_{n+1}^2 \tag{36}$$

Therefore, it is demonstrated Brocard's Conjecture.

2.3 Third 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:

$$n^2 + n + 1 \leq P_n < (n+1)^2 < p_{n+1} \leq n^2 + 3n + 1 \tag{37}$$

It is easily verifiable that:

$$\sqrt{n^2 + 3n + 1} - \sqrt{n^2 + n + 1} < 1 \tag{38}$$

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.

2.4 Fourth corollary: a new maximum interval between every natural number and the nearest prime number

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

$$n^2 + 3n - (n^2 + n + 1) = 2n - 1 \tag{39}$$

Therefore, and stating that:

$$n = \sqrt{n^2 + n + 1} \tag{40}$$

It can be determined that:

$$\forall n \in N, \exists P_a, P_b / (n - (2\sqrt{n} - 1)) \leq P_a \leq n \leq P_b \leq (n + (2\sqrt{n} - 1)) \tag{41}$$

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

$$\forall n \in N, \exists P / n \leq P \leq (n + (2\sqrt{n} - 1)) \tag{42}$$

2.5 Fifth 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:

$$p_i = n^2 \pm k / 0 < k < n \tag{43}$$

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 $n^2 \pm k / 0 < k < n$.

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