Aldo Pappalepore
aldo.pappalepore@libero.it

Investigation of Legendre's conjecture with the Congruence Primality Theorem

Abstract

In the article, a study on the Legendre conjecture is developed that is based on the two primality theorem of congruence.

1 Introduction

Legendre's conjecture states that there is always a prime number between n^2 and $(n + 1)^2$. This conjecture is part of Landau's problems and, to date, has not been proved.

In 1965, Chen Jingrun proved that there is always a number between n^2 and $(n + 1)^2$ that is either a prime or a semi-prime, i.e. the product of two primes.

Furthermore, it is known that there is always a prime number between $n - n^\theta$ and n, with $\theta = 23 / 42 = 0.547...$ (demonstrated by J. Iwaniec and H. Pintz in 1984).

2 The Congruence of Natural Numbers

As is well known, the congruence relation modulus m is an equivalence relation defined on the set of integers Z as follows: if m is a fixed integer greater than 1, two integers a and b are said to be congruent modulus m if $m|(a - b)$; m is called the modulus of congruence and is denoted by $a \equiv b \pmod m$.

In the field of natural numbers, it can also be equivalently stated that $a \equiv b \pmod m$ if a and b give the same remainder in the integer division by m.

For example, $24 \equiv 10 \pmod 7$ because they both give remainder 3 in the integer division by 7. All numbers congruent with each other modulo m constitute an equivalence class, called the congruence class modulo m: two natural numbers belong to the same congruence class if and only if they are congruent modulo m, that is, if and only if they divide by m and give the same remainder r. If, as in the example, the modulus is 7, seven classes are thus formed (as many as there are possible remainders in the division by 7) as follows [0], [1], [2], [3], [4], [5], [6]. Always limiting ourselves to the subset of Z consisting of the natural numbers, to establish to which class modulo m one of them belongs we divide it by m, the remainder indicating the class.

It should be emphasised that for each m we always have that $[m]_{\text{mod } m} = [0]_{\text{mod } m}$.

Comment 2.1 From Number Theory we know that any natural number n will only be non-prime if it is divisible by one or more prime numbers less than or equal to the $\sqrt{n}$. Since all even natural numbers, except 2, are non-prime because they are divisible by 2, it can be asserted that any odd natural number $n > 4$ will only be non-prime if it is divisible by one or more prime numbers odd less than or equal to . $\sqrt{n}$.

From here on, the variables $p, p_1 , p_2, ... p_i$ always denote prime numbers and $\mathbb{P}(M)$ the set of odd prime numbers less than or equal to the number M.

3 Congruence Primality Theorem

Enunciation 3.1 *$\forall N_0$, $n_0 \in N$ with $N_0 \geq 3$, $0 \leq n_0 \leq N_0 - 3$ and even if N_0 is odd or vice versa, with $\mathbb{P}(\sqrt{(N_0 - n_0)})$ set of odd prime numbers $\leq \sqrt{(N_0 - n_0)}$, a necessary and sufficient condition for $N_0 - n_0$ to be a prime number is that $n_0 \not\equiv N_0 \pmod{p_i}$ $\forall p_i \in \mathbb{P}(\sqrt{(N_0 - n_0)})$*

or that $\mathbb{P}(\sqrt{(N_0 - n_0)})$ is an empty set.

Dim. According to the congruence of natural numbers (2.1) if N_0 and n_0 do not belong to the same congruence class modulo p_i for all $p_i \in \mathbb{P}(\sqrt{(N_0 - n_0)})$, this means that $N_0 - n_0$ (an always odd natural number) is not divisible by any odd prime number less than or equal to the $\sqrt{(N_0 - n_0)}$ and that therefore, according to observation (2.1), $N_0 - n_0$ is a prime number. If instead $\mathbb{P}(\sqrt{(N_0 - n_0)})$ turns out to be an empty set (with $n_0 = N_0 - 3$, $N_0 - 4$, $N_0 - 5$, $N_0 - 6$, $N_0 - 7$, $N_0 - 8$) the number $N_0 - n_0$ cannot be divided by any prime and is therefore prime.

Conversely, if $N_0 - n_0$ is a prime number, it will not be divisible by any other lower, equal or non-existent odd prime number of the $\sqrt{(N_0 - n_0)}$ and therefore N_0 and n_0 will always result non congrui $\forall p_i \in \mathbb{P}(\sqrt{(N_0 - n_0)})$.

We set $n_0 \leq N_0 - 3$ because with $n_0 = N_0 - 1$ one would have that $N_0 - n_0 = 1$ which, as is known, is neither a prime nor a compound number, and with $n_0 = N_0 - 2$ one would have that N_0 and n_0 would both be even or odd contrary to the hypothesis. In order then to prevent n_0 from taking negative values, it must be $N_0 \geq 3$.

Remark 3.2 *If instead of referring to the set $\mathbb{P}(\sqrt{(\boldsymbol{N_0} - \boldsymbol{n_0})})$ we want to refer, for the sake of later demonstration, to the set $\mathbb{P}(\sqrt{\boldsymbol{N_0}})$, the theorem (*3.1) is *transformed into the corollary (3.3)*

Given a number $N_0 \in N$, a number $n_0 \in N$, smaller than N_0 and such that $(N - n_{00})$ is odd is called the **Prisotto of N_0** if it turns out that $n_0 \not\equiv N_0 \pmod{p_i}$ $\forall$ $p_i \in \mathbb{P}(\sqrt{(N_0)})$.

Corollary 3.3 *$\forall N_0$, $n_0 \in N$ with $N_0 \geq 9$, $0 \leq n_0 \leq N_0 - p_{max}$ and even if N_0 is odd or vice versa, with $\mathbb{P}(\sqrt{(N_0)})$ set of odd prime numbers $\leq \sqrt{(N_0)}$ and with p_{max} prime number higher than $\mathbb{P}(\sqrt{(N_0)})$, a necessary and sufficient condition for $N_0 - n_0$ to be a prime number is that n_0 is a prime number of N_0.*

Dim. substituting $\mathbb{P}(\sqrt{(N_0)})$ a $\mathbb{P}(\sqrt{(N_0 - n_0)})$, in contrast to theorem (3.1), the numbers n_0 smaller than N_0 and belonging to the interval $[N - p_{0max}., N_0 - 3]$ are not considered since they all have at least one congruence class mod p_j, with $p_j \in \mathbb{P}(\sqrt{(N_0)})$, equal to that of the same modulus of N_0. In fact for the $n_0 \in [N_0 - p_{max}., N_0 - 3]$, $N_0 - n_0$ will belong to the interval $[3, p_{max}]$ and thus be equal to a prime or compound number belonging to this interval; in the first case according to modular arithmetic if $N_0 - n_0 = p_j$, with $p_j \in \mathbb{P}(\sqrt{(N_0)}) \subset [3, p_{max}.]$ this implies that $[N_0] \bmod p_j - [n_0] \bmod p_j = [p_j] \bmod p_j = [0]$ whence the congruence mod p_j of n_0 with N_0; if instead $N_0 - n_0$ is equal to a compound number $m^* p_j$, with $p_j \in \mathbb{P}(\sqrt{(N_0)}) \subset [3, p_{max}.]$, we will have that $[N_0] \bmod p_j - [n_0] \bmod p_j = [m] \bmod p_j * [p_j] \bmod p_j = [m] \bmod p_j *[0] = [0]$ whence the congruence mod p_j of n_0 with N_0.

Conversely, if $N_0 - n_0$ is a prime number, belonging to the interval $]p_{max}, N_0]$, it as prime will not be divisible by any other odd prime number less than or equal to p_{max} and thus the $\sqrt{(N_0)}$ and therefore N_0 and n_0 will always be non congrui $\forall p_i \in \mathbb{P}(\sqrt{(N_0)})$.

He placed himself $N_0 \geq 9$ in quanto per valori inferiori p_{max} would not be defined.

According to Corollary 3.3, we can state that the numbers n_0 prisotto of N_0 , subtracted from N_0 , result in all prime numbers in the interval $]p_{max}$, N $]._0$

Remark 3.4 *Both theorem (3.1) and corollary (3.3) tell us nothing about the existence of at least one incongruous n .₀ However, on the basis of Bertrand's postulate (later proved by Pafnuty Chebyshev, Srinivasa Ramanujan and Paul Erdős), which states that for every n ≥ 2 there exists at least one prime p such that n < p < 2n, we can state, with respect to the corollary (3.3), that in the interval] p_{max} , N_0] there will always exist at least one prime being 2 $p_{max} \leq 2\sqrt{N_0} \leq N_0$ for $N_0 \geq 4$. Consequently, in the interval]0, N_0 - p_{max} [there will always exist at least one n_0 prisot of N_0.*

4 Conjecture analysis with the Congruence Primality Theorem

As we know, Legendre's conjecture states that there is always a prime number between n^2 and $(n + 1)^2$.

We can then also say that the conjecture affirms the existence of a prime number in the interval $](n+1)^2 -(2n+1), (n+1)^2 [$. But according to Corollary 3.3, with $N_0 = (n+1)^2$ and $p_{max} \leq \sqrt{N_0} \leq n+1$, there exists a prime number in the above interval if and only if in the interval]0, 2n+1] there exists a prime number (less than N_0 and incongruous for all primes less than or equal to p_{max}) of $(n+1)^2$.

Existence theorem of a prime between n^2 and $(n+1)^2$

Enunciation 4.1 *∀ n, n_0 ∈ N ∃ at least one number $n_0 \leq 2n+1$ such that n_0 is not congruent with $(n+1)^2$ $\forall p_i \in \mathbb{P}(n+1)$*

Dim. Let us start by saying that (n+1) and $(n+1)^2$ are incongruous for those $p_i \leq p_{max}$ for which it does not turn out that $[(n+1)^2]_{p_i}$ is equal to 0 or 1. In fact we know that for modular arithmetic we can write:

(4.2) $[(n+1)^2]_{p_i} = [(n+1)]_{p_i} * [(n+1)]_{p_i}$

and that therefore only for $[(n+1)]_{p_i}$ equal to 0 or 1 it will result that $[(n+1)^2]_{p_i}$ is equal to 0 or 1, i.e. that $[(n+1)^2]_{p_i} = [(n+1)]_{p_i}$ i.e. that $(n+1)^2$ and (n+1) are congruent modulo p_i.

We then denote for any n by p_c the c modules for which $(n+1)^2$ and (n+1) are congruent and with p_{nc} the nc modules for which $(n+1)^2$ and (n+1) are incongruous. Obviously c+nc will be equal to the number of primes in the set $\mathbb{P}(n+1)$.

Let us also bear in mind that for each module p_c , for which $[(n+1)^2]_{p_c} = [(n+1)]_{p_c}$= 0 or 1, the sum or difference of (n+1) with 1 or with $\boldsymbol{p_{nc}}$ implies that the term $[(n+1)\pm 1]_{p_c}$is equal to $[x \pm 1]_{p_c}$ and that the term $[(n+1)\pm \boldsymbol{p_{nc}}]_{p_c}$is equal to $[x \pm \boldsymbol{p_{nc}}]_{p_c}$with x equal to 0 or 1. Consequently the terms $[(n+1)\pm 1]_{p_c}$ e $[(n+1)\pm \boldsymbol{p_{nc}}]_{p_c}$ will certainly be different from x and that therefore (n+1) ±1 and (n+1) $\pm\boldsymbol{p_{nc}}$ will be incongruous for p-modules$_c$ while they may become congruous for other p-modules$_{nc}$ other than $\boldsymbol{p_{nc}}$.

1ª Assumptions: nc = 0 (e.g. n+1=6)

In this case for all modules p_c belonging to $\mathbb{P}(n+1)$ results $[(n+1)^2]_{p_c} = [(n+1)]_{p_c}$ and equal (see above) to 0 or 1. If we then subtract or add to the term (n+1) the term 1, the two terms (n+1)±1 will be incongruous with $(n+1)^2$ for each module p_c , less than 2n+1 and such as to give rise (by the primality theorem of congruence) in the interval $]n^2 , (n+1)^2 [$ to the two primes:

(4.3) $(n+1)^2 - n$ and $(n+1)^2 - (n+2)$

2ª Assumptions: nc = 1 (e.g. n+1=7 or 10)

In this case, with respect to the previous one, adding or subtracting the term 1 to the term (n+1) may result in at most one of (n+1)+1 and (n+1)-1 being congruous with $(n+1)^2$ for the only module p_{nc} (e.g. n+1=10) or neither (e.g. n+1=7) for the same module. Similarly, adding or subtracting the unique p_{nc} to the term (n+1) will result in both $(n+1)+p_{nc}$ and $(n+1)-p_{nc}$ being incongruous with $(n+1)^2$ for all modules $p_i \leq p_{max}$. In fact, for each module p_c both $[(n+1)+p_{nc}]_{p_c}$ and $[(n+1)-p_{nc}]_{p_c}$ will be different from 0 and 1 with the consequence that $(n+1)+p_{nc}$ and $(n+1)-p_{nc}$ will be incongruent with $(n+1)^2$ for these modules while the incongruence between $(n+1)+p_{nc}$ and $(n+1)-p_{nc}$ will remain with $(n+1)^2$ for the module p_{nc} . It should also be noted that since $p_{nc} \leq p_{max} \leq n+1$ it will always result in $(n+1)+p_{nc} \leq 2n+1$. In conclusion, in this hypothesis there will be in the interval $]n^2 , (n+1)^2[$ certainly at least three primes:

(4.4) $(n+1)^2 - [(n+1)\pm1]$ $(n+1)^2 - [(n+1)+p_{nc}]$ $(n+1)^2 - [(n+1)-p\ ]_{nc}$

where the sign ± indicates only one of the two

3ª Assumptions: nc = 2 (e.g. n+1=12)

If the p_{nc} are 2 (p_{nc1} and p_{nc2}) nothing can be said about the terms (n+1)+1 and (n+1)-1 as the former could be congruous for the module p_{nc1} and the latter for the module p_{nc2} . On the other hand, with regard to the terms $(n+1)+p_{nc1}$ and $(n+1)-p_{nc1}$, which, as we have seen, are always incongruous for the module $p_{,c}$ it can be said that certainly one of the two is incongruous with $(n+1)^2$ for the module p_{nc2} since the two equalities $[(n+1)+p_{nc1}]_{p_{nc2}} = [(n+1)^2]_{p_{nc2}}$ and $[(n+1)-p_{nc1}]_{p_{nc2}} = [(n+1)^2]_{p_{nc2}}$. Similarly, it can be stated that certainly one of $(n+1)+p_{nc2}$ and $(n+1)-p_{nc2}$ is incongruous with $(n+1)^2$ for the modulus p_{nc1} . In conclusion in this hypothesis there will be in the interval $]n^2 , (n+1)^2[$ certainly at least two primes:

(4.5) $(n+1)^2 - [(n+1)\pm p_{nc1}]$ $(n+1)^2 - [(n+1)\pm p_{nc2}]$

where the ± sign indicates only one of the two

4ª Assumptions: nc ≥ 3 (e.g. n+1=16)

Let us assume nc=3 (with $p_{nc1} < p_{nc2} < p_{nc3}$) and immediately exclude the terms (n+1)+1 and (n+1)-1 as both could be congruent for the modulus p_{nc} . Suppose then by absurdity that each $(n+1)+p_{nci}$ and $(n+1)-p_{nci}$ are congruent with $(n+1)^2$ for the p-module$_{ncj}$ and for the p-module$_{nck}$ respectively, i.e. that the following equalities occur:

$$[(n+1)+p_{nc1}]_{p_{nc2}} = [(n+1)^2]_{p_{nc2}}$$

$$[(n+1)-p_{nc1}]_{p_{nc3}} = [(n+1)^2]_{p_{nc3}}$$

$$[(n+1)-p_{nc2}]_{p_{nc1}} = [(n+1)^2]_{p_{nc1}}$$

(4.6) $$[(n+1)+p_{nc2}]_{p_{nc3}} = [(n+1)^2]_{p_{nc3}}$$

$$[(n+1)-p_{nc3}]_{p_{nc1}} = [(n+1)^2]_{p_{nc1}}$$

$$[(n+1)+p_{nc3}]_{p_{nc2}} = [(n+1)^2]_{p_{nc2}}$$

from which these other equalities derive:

$$[(n+1)+p_{nc1}]_{p_{nc2}} = [(n+1)+p_{nc3}]_{p_{nc2}} \longrightarrow [(n+1)]_{p_{nc2}} + [p_{nc1}]_{p_{nc2}} = [(n+1)]_{p_{nc2}} + [p_{nc3}]_{p_{nc2}}$$

(4.7) $$[(n+1)-p_{nc2}]_{p_{nc1}} = [(n+1)-p_{nc3}]_{p_{nc1}} \longrightarrow [(n+1)]_{p_{nc1}} - [p_{nc2}]_{p_{nc1}} = [(n+1)]_{p_{nc1}} - [p_{nc3}]_{p_{nc1}}$$

$[(n+1)-p_{nc1}]_{p_{nc3}} = [(n+1)+p_{nc2}]_{p_{nc3}} \longrightarrow [(n+1)]_{p_{nc3}} - [p_{nc1}]_{p_{nc3}} = [(n+1)]_{p_{nc3}} + [p_{nc2}]_{p_{nc3}}$

and finally the latter:

$[p_{nc1}]_{p_{nc2}} = [p_{nc3}]_{p_{nc2}}$

(4.8) $[p_{nc2}]_{p_{nc1}} = [p_{nc3}]_{p_{nc1}}$

$[p_{nc1}]_{p_{nc3}} = [p_{nc2}]_{p_{nc3}}$

which are evidently false being always:

$[p_{ncx}]_{p_{ncy}} \neq [p_{ncz}]_{p_{ncy}}$ with $p_{ncx} \neq p_{ncz}$

It follows that at least three equalities of (4.6) are not possible and that therefore in the interval $]n^2 , (n+1)^2 [$ there are definitely at least three primes.

If, on the other hand, nc > 3, repeating the reasoning done for nc=3, it can easily be verified that the number of non-possible equalities of the type (4.6) increases and thus also the number of primes present in the interval $]n^2 , (n+1) [.^2$

BIBLIOGRAPHY

[a] Alessandro Zaccagnini - Introduction to Analytical Number Theory:
http://people.dmi.unipr.it/alessandro.zaccagnini/psfiles/lezioni/tdn2005.pdf

[b] Francesco Fumagalli - Appunti di Teoria elementare dei numeri:
Theory_of_Numbers.pdf (unifi.it)

[c] Aldo Pappalepore - Congruence, Primality and Density:
https://www.aldopappalepore.it/_downloads/99fd430c6fe12b90fb801cd67dc1d70f