Aldo Pappalepore
aldo.pappalepore@libero.it

Investigation of the n^2 +1 infinite primes conjecture

Investigation of conjecture n^2 +1 infinite primes

Abstract

In the article, a study of Landau's fourth problem on the infinity of prime numbers of type n^2 +1 is developed, a study centred on the primality theorems of congruence and complementary congruence.

1 Introduction

The conjecture, corresponding to Landau's fourth problem, asserts that there are infinite prime numbers of the form n^2 +1.

Three theorems already exist to reinforce the conjecture: Fermat's conjecture on the sums of two squares, Legendre's conjecture (conjecture proven to date: [d]) which states that there is always a prime number between n^2 and $(n + 1)^2$ and Dirichlet's conjecture which states that given two coprime integers a and b, there are infinite arithmetic progressions of the type $a+nb$, with positive integer n, which contain infinite prime numbers.

In fact, the first theorem states that every prime number can be written as the sum of two perfect squares if and only if it is congruent to 1 modulo 4. Since n^2 +1 is always a number congruent to 1 modulo 4 since, with n definitely even, n^2 is always a multiple of 4, in consistency with Fermat's theorem we can write

$5 = 1^2 + 2^2$, $17 = 1^2 + 4^2$, ... $101 = 1^2 + 10^2$, ... $3137 = 1^2 + 56^2$, ... $8101 = 1^2 + 90^2$ .....

and to date there is no mathematical consideration that beyond a certain (maximum) value of n there is no more n such that n^2 +1 is prime.

Legendre's theorem is also a reinforcement of the conjecture. This theorem states that there always exists a prime number between n^2 and $(n + 1)^2$ or, what is equivalent for the first congruence primality theorem, that there always exists a number $n_0 \leq 2n+1$ such that n_0 is not congruent with $(n+1)^2$ $\forall$ pi $\in \mathbb{P}(n + 1)$. Whenever then, based on the value of n, n_0 is equal to 2n, $(n + 1)^2$ and 2n are incongruent $\forall$ pi $\in \mathbb{P}(n + 1)$ and this implies, again by the primality theorem, that $(n + 1)^2$ - 2n is equal to a prime number. But $(n + 1)^2$ - 2n = n^2 +1 and therefore n^2 +1 will equal a prime number.
Here again, there is no mathematical consideration that beyond a certain (maximum) value of n there are no more natural numbers such that $(n + 1)^2$ and 2n are incongruous and that therefore n^2 +1 turns out to be a prime number.

Finally, with regard to Dirichlet's theorem, we observe that all terms n^2 +1 with n even:

5, 17, 37, 65, 101, ...

belong to the arithmetic sequence of the type 1 + 4m:

5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, ...

succession which, for Dirichlet, comprises infinite primes including all those of the type n^2 +1.

Again, there is no mathematical consideration that beyond a certain (maximum) value of n among all the successive infinite primes belonging to the series 1+4m there are not also some n^2 +1.

In short, all three of the above theorems support the existence of an infinite sequence of n^2 + 1 primes,

[n^2 +1(n)]: 5 (2) - 17 (4) - 37 (6) - 101 (10) - 197 (14) - 257 (16) - 401 (20) - 577 (24) - 677 (26) - 1297 (36) - 1601 (40) - 2917 (54) - 3137 (56) - 4357 (66) - 5477 (74) - 7057 (84) - 8101 (90) - 8837 (94) - 12101 (110) - 13457 (116) - 14401 (120) - 15377 (124) - 15877 (126) .....

even if they do not prove the conjecture fully.

2 The primality conditions of n^2 + 1

Let us consider any even positive integer n and see what condition must be satisfied for n^2 +1 to be a prime number.

By the primality theorem of compcongruence n^2 +1 is prime if:

(2,3) $\forall p_i \leq n: n^2 \nmid 1 (\mathrm{mod}\ p)_i$

or if, for each p $[1]_p$ = 1 and its complement equal to p-1, the result is:

(2.4) $\forall p_i \leq n: [n^2]_{p_i} \neq p_i - 1$

Starting then from condition (2.4) we find the conditions that n must satisfy in order for n^2 + 1 to be prime.

Lemma 2.5 *For each m, k εN with m = 1+2k the square of each number represented by one of the rest classes modulo m corresponds to two rest classes modulo m.*

Dim. From modular arithmetic we know that:

(2.6) $[x^2]_m = [+x]_m * [+x]_m$ or $[x^2]_m = [-x]_m * [-x]_m$

where [+x] and [-x] represent two of the rest classes modulo m: [0], [1], [2], [3] ..... [m-1]

Consequently, we can state that each class $[x^2]_m$ of rest modulo m corresponds to two classes, $[+x]_m$ e $[-x]_m$, of rest modulus m, the second of which corresponds to the class $[m - x]_m$.

So for example if we set x=5 and m=15, (2.6) becomes:

$[25]_{15} = [5]_{15} * [5]_{15}$ or $[25]_{15} = [-5]_{15} * [-5]_{15} = [10]_{15}$

and thus to the rest class $[25]_{15}$, equal to $[10]_{15}$, modulo 15 correspond the two rest classes modulo 15: [+5] and [-5]. It should be noted that the two classes are always one even and the other odd: if in fact $[+x]_m$ è pari allora $[-x]_m = [-x + m]_m$ sarà dispari e viceversa.

Definition 2.7 *We denote* **by** *the name* ***class-root(x)*** *the two rest classes modulo m whose square is equal to the rest class [x] modulo m.*

Lemma 2.8 *For each m, k εN_0 with m = 3+4k there are no class-roots(m-1) modulo m.*

As we know, all the odd natural numbers m can be of two types: 3+4k and 1+4k, with k belonging to N_0 .

Let us then assume by hypothesis that for m = 3+4k it is possible that two class-roots(m-1), $[x]_m$ and $[-x]_m$, of rest modulus m correspond to the rest class [m-1] modulo m. For this to be the case, the equation must be solvable:

(2.9) $[([\pm x]_m)^2]_m = [m-1]_m$

i.e. for m=3+4k:

(2.10) $[([\pm x]_m)^2]_m = [3+4k-1]_m = [2+4k]_m$

This equation is unsolvable in x since, if x is even, x^2 unlike 2+4k is a multiple of 4; then if x is odd, the unsolvability is even more evident being x^2 odd and 2+4k even. The same non-solvability of (2.9) can be proved for all numbers represented by the two classes.

Lemma 2.11 *For every n, m, k εN with m = 1+4k there always exist class-roots(m-1) modulo m.*

Let us also assume here by hypothesis that for m = 1+4k it is possible that two class-roots(m-1), [x] and [-x], of remainder modulus m correspond to the rest class [m-1] modulo m For this to be the case, the equation must be solvable in k:

(2.12) $[([\pm x]_m)^2]_m = [m-1]_m$

i.e. for m=1+4k:

(2.13) $[([x]_m)^2]_m = [1+4k-1]_m = [4k]_m$

equation that is always solvable in x for any value of m. In fact, surely at least one of the two classes can be represented by an even number whose square is always a multiple of 4.

Primality Theorem of $n^2 + 1$ 2.14 *For every n, k εN_0 and n even, $n^2 + 1$ is prime if $\forall p_i \in \mathbb{P}(n)$ of the type p_i = 1+4k it follows that the rest class $[n]_{pi}$ modulo p_i is different from the two class-roots($p_i - 1$) modulus p_i.*

Dim. Prime numbers can also obviously be of two types: 3+4k and 1+4k, with k belonging to N_0 **.** Recalling the condition of primality (2.4) and according to Lemma 2.8 among the p_i belonging to $\mathbb{P}(n)$ we must not consider those of type 3+4k since for them there is no class-root($p_i - 1$) modulo p_i .

In contrast, for primes of the type 1+4k (Lemma 2.11) there are always two class-roots($p_i - 1$) modulo p_i .

Given then any even positive integer n, n^2 +1 is prime if, see (2.4), $\forall$ pi $\leq$ n, with pi =1+4k: $[n^2]_{p_i} \neq$ pi -1 with k $\geq$ 0. But

(2.15) $[n^2]_{p_i} = [n]_{pi} * [n]_{pi} = [x]_{pi} * [x]_{pi}$

with $[x]_{pi}$ rest class $[n]_{pi}$ modulo p_i . If $\forall$ $p_i \leq n$ of type 1+4k the $[x]_{pi}$ of (2.15) is different from the class-roots(p_i -1) modulo p_i then $n^2 + 1$ is prime.

It can easily be verified that the above condition is satisfied by a long sequence of n and thus of the first n^2 + 1.

n^2 +1 (n): 5 (2) - 17 (4) - 37 (6) - 101 (10) ..... 21317 (146) - 22501 (150) - 24337 (156) - 25601 (160) ..... 2464901 (1570) - 2483777 (1576) - 2496401 (1580) ..... 29484901 (5430) - 29658917 (5446) - 29877157 (5466) .....

Let us now demonstrate how this sequence is infinite.

3 Infinity theorem of $n^2 + 1$ primes

Definition 3.1 *Let us denote by* $\mathbb{P}'(n)$ *l'insieme dei primi appartenenti a* $\mathbb{P}(n)$ *of the type p=1+4k.*

Enunciation 3.2 *Prime numbers of the type* $n^2 + 1$*, with* $n \in N$ *and even, are infinite and the relative n are those for which the property that* $\forall p_i \in \mathbb{P}'(n)$ $[n]_{pi}$ *is different from the two class-roots*$(p_i - 1)$ *modulo* p_i.

Dim. All n satisfying the conditions of Theorem 2.13 are even positive integers whose remainder classes $[n]_{pi}$ modulo p_i, for each $p_i \in \mathbb{P}'(n)$, are different from the remainder classes$(p_i - 1)$ modulus p_i (e.g. if n=14 we have that $\mathbb{P}'(n) = \{5, 13\}$; the two rest-root classes (5-1) modulo 5 are $[2]_5$ and $[3]_5$ while the two rest-root classes (13-1) modulo 13 are $[5]_{13}$ and $[8]_{13}$; on the other hand, the two rest-root classes 14 modulo 5 and modulo 13 are $[4]_5$ and $[1]_{13}$, respectively, and that is different from the respective rest-root classes above, and therefore $14^2 +1=197$ is a prime number).

That said, let us see how to calculate the number of n, such that $n^2 +1$ is prime, less than any even positive integer $N_0 > 5$.

Having then selected an $N_0 > 5$ we denote by $\prod(N_0)$ the product of all primes belonging to $\mathbb{P}'(N_0)$ and consider the number-class table (Appendix A) consisting for each natural number in the interval $[0, \prod(N_0)]$ of the rest classes $[n]_{pi}$ modulo p_i for each p_i belonging to $\mathbb{P}'(N_0)$.

We then delete from this table the rows that have rest classes n of prime modules p_i belonging $\mathbb{P}'(N_0)$ equal to the two class-roots$(p_i - 1)$ modulo p_i . The numbers in the number-classes table, whose rows have been eliminated by the previous sieve, can then only be those which in their combination of rest classes $[n]_{pi}$ modulo p_i do not have, for each p_i belonging to $\mathbb{P}'(N_0)$, the respective two class-roots $(p_i -1)$ modulo p_i .

Then the even numbers **M** in the table that have not been deleted will, according to combinatorial calculation, turn out to be:

(3.3.) $\frac{1}{2} * \prod_{p \in P'(No)}(p-2)$

Thus (3.3) gives us the quantity of numbers **M** of the table-interval $[0, \prod(N_0)]$ whose combination of rest classes $[n]_{pi}$ modulo p_i does not include, for each p_i belonging to $\mathbb{P}'(N_0)$, the respective two class-roots$(p_i -1)$ modulo p_i . But in the interval $[0, \prod(N_0)]$ there are certainly (Bertrand's postulate) primes greater than N_0 , and therefore not contained in the set $\mathbb{P}'(N_0)$, whose class-roots$(p_i -1)$ modulo p_i can be equal to the rest classes $[n]_{pi}$ for the same moduli p_i . This eventuality precludes extending the applicability of the primality theorem 2.13 also for the n included in the interval $]N_0 , \prod(N_0)]$. Instead, we can state that all numbers $\mathbf{M_{N0}}$ less than or equal to N_0 (and thus belonging to the interval $[0, N_0]$) and for which the primality condition of Theorem 2.13 is satisfied are such that $M_{N0}^2 + 1$ is prime.
The existence of these numbers $\mathbf{M_{N0}}$ is guaranteed by verifying their presence already for $N_0 = 6$: n=2 ($n^2 +1=5$), n=4 ($n^2 +1=17$) and n=6 ($n^2 +1=37$).....

If we now consider a number $N_1 > N_0$ and such that $\prod(N_1) > \prod(N_0)$ we will certainly have that:

(3.4) $\frac{1}{2} * \prod_{p \in P'(N1)}(p-2) > \frac{1}{2} * \prod_{p \in P'(No)}(p-2)$

i.e. the quantity of the **M-numbers** of the table-interval $[0, \prod(N_1)]$ is greater than that of the **M-numbers** of the table-interval $[0, \prod(N_0)]$. This implies that the M_{N1} of the interval $[0, N_1]$ are also greater than or equal to the M_{N0} of the interval $[0, N_0]$. Proceeding with successive increasing N_i the number of M_{Ni} grows progressively and there can be no N_{max} such that $\forall n > N\ n_{max}^{\ 2} + 1$ is not prime.

APPENDIX A

NUMBERS-CLASSES TABLE: NUMBERS Ɛ [0, ∏(N0)] - REMAINING CLASSES p Ɛ P'(N0)

N0 = 14 - P'(N0) = {5, 13} - [0, ∏(N0)] = [0. 65].

n	5	13	n	5	13
0	0	0	33	3	7
1	1	1	34	4	8
2	2	2	35	0	9
3	3	3	36	1	10
4	4	4	37	2	11
5	0	5	38	3	12
6	1	6	39	4	0
7	2	7	40	0	1
8	3	8	41	1	2
9	4	9	42	2	3
10	0	10	43	3	4
11	1	11	44	4	5
12	2	12	45	0	6
13	3	0	46	1	7
14	4	1	47	2	8
15	0	2	48	3	9
16	1	3	49	4	10
17	2	4	50	0	11
18	3	5	51	1	12
19	4	6	52	2	0
20	0	7	53	3	1
21	1	8	54	4	2
22	2	9	55	0	3
23	3	10	56	1	4
24	4	11	57	2	5
25	0	12	58	3	6
26	1	0	59	4	7
27	2	1	60	0	8
28	3	2	61	1	9
29	4	3	62	2	10
30	0	4	63	3	11
31	1	5	64	4	12
32	2	6	65	0	0

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

[d] Aldo Pappalepore – Legendre conjecture:
https://www.aldopappalepore.it/_downloads/d956c29eb800c2326b34d848aeb2442e