Aldo Pappalepore
aldo.pappalepore@libero.it

Investigation of the n^2+1 infinite primes conjecture

Indagine sulla congettura n^2+1 primi infiniti

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.

Nell'articolo viene sviluppato uno studio del quarto problema di Landau sull'infinità dei numeri primi del tipo n^2 +1, studio centrato sui teoremi di primalità della congruenza e della congruenza complementare.

1 Introduzione

La congettura, corrispondente al quarto problema di Landau, asserisce che esistono infiniti numeri primi della forma n^2+1.

A rinforzo della congettura esistono già tre teoremi: quello di Fermat sulle somme di due quadrati, quello di Legendre (congettura ad oggi dimostrata: [d]) che afferma che esiste sempre un numero primo compreso fra n^2 ed $(n + 1)^2$ e quello di Dirichlet che afferma che dati due numeri interi coprimi a e b, esistono infinite progressioni aritmetiche del tipo a+nb, con n intero positivo, che contengono infiniti numeri primi.

Infatti il primo teorema afferma che ogni numero primo si può scrivere come somma di due quadrati perfetti se e solo se è congruo a 1 modulo 4. Essendo n^2+1 un numero sempre congruo ad 1 modulo 4 in quanto, con n sicuramente pari, n^2 è sempre multiplo di 4, in coerenza con il teorema di Fermat potremo scrivere in particolare:

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

e ad oggi non c'è alcuna considerazione matematica per cui oltre un certo valore (massimo) di n non esistano più n tali che n^2+1 sia primo.

Anche il teorema di Legendre rappresenta un rinforzo della congettura. Tale teorema sostiene che esiste sempre un numero primo compreso fra n^2 ed $(n + 1)^2$ o, ciò che è equivalente per il primo teorema di primalità della congruenza, che esiste sempre un numero $n_0 \leq 2n+1$ tale che n_0 non è congruo con $(n+1)^2$ $\forall$ pi $\in \mathbb{P}(n+1)$. Ogni volta allora che, in base al valore di n, n_0 risulta uguale a 2n, $(n + 1)^2$ e 2n sono incongrui $\forall$ pi $\in \mathbb{P}(n+1)$ e questo comporta, sempre per il teorema di primalità, che $(n + 1)^2 - 2n$ è uguale ad un numero primo. Ma $(n + 1)^2 - 2n = n^2+1$ e quindi n^2+1 sarà pari ad un numero primo.
Anche in questo caso non c'è alcuna considerazione matematica per cui oltre un certo valore (massimo) di n non esistano più numeri naturali tali che $(n + 1)^2$ e 2n siano incongrui e che quindi n^2+1 risulti essere un numero primo.

Relativamente infine al teorema di Dirichlet osserviamo come tutti i termini n^2+1 con n pari:

5, 17, 37, 65, 101, ………………..

appartengono alla successione aritmetica del tipo 1 + 4m:

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

successione che, per Dirichlet, comprende infiniti primi tra i quali anche tutti quelli del tipo n^2+1. Anche in questo caso non c'è alcuna considerazione matematica per cui oltre un certo valore (massimo) di n tra tutti i successivi infiniti primi appartenenti alla serie 1+4m non ci siano anche alcuni n^2+1.

Insomma tutti e tre i teoremi precedenti supportano l'esistenza di una sequenza infinita di $n^2 + 1$ primi,

[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) ………………

anche se non dimostrano la congettura in modo compiuto.

2 Le condizioni di primalità degli $n^2 + 1$

Consideriamo un numero intero positivo pari n qualsiasi e vediamo quale condizione deve essere soddisfatta affinché $n^2 + 1$ risulti essere un numero primo.

Per il teorema di primalità della compcongruenza $n^2 + 1$ risulta primo se:

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

o se, essendo per ogni p $[1]_p = 1$ ed il suo complemento uguale a p-1, risulta:

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

Partendo allora dalla condizione (2.4) troviamo le condizioni a cui deve soddisfare n affinché $n^2 + 1$ sia primo.

Lemma 2.5 *Per ogni m, k ε N con m = 1+2k al quadrato di ognuna delle classi di resto modulo m corrispondono due classi di resto modulo m.*

Dim. Dall'aritmetica modulare sappiamo che:

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

dove [+x] e [-x] rappresentano due tra le classi di resto modulo m: [0], [1], [2], [3] ……….. [m-1]

Di conseguenza possiamo affermare che ad ogni classe $[x^2]_m$ di resto modulo m corrispondono due classi, $[+x]_m$ e $[-x]_m$, di resto modulo m, la seconda delle quali corrisponde alla classe $[m - x]_m$.

Così per esempio se poniamo x=5 ed m=15 la (2.6) diventa:

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

e quindi alla classe di resto $[25]_{15}$, pari alla $[10]_{15,}$ modulo 15 corrispondono le due classi di resto modulo 15: [+5] e [-5] (corrispondente alla classe [10]). E' bene osservare che le due classi risultano sempre una pari e l'altra dispari: se infatti $[+x]_m$ è pari allora $[-x]_m = [-x + m]_m$ sarà dispari e viceversa.

Definizione 2.7 *Indichiamo col nome di* ***classi-radici(x)*** *le due classi di resto modulo m il cui quadrato è pari alla classe di resto [x] modulo m.*

Lemma 2.8 *Per ogni m, k ε N con m = 3+4k non esistono classi-radici(m-1) modulo m.*

Come noto tutti i numeri naturali dispari m possono essere di due tipi: 3+4k ed 1+4k, con k appartenente a N**.**
Poniamo allora per ipotesi che per gli m = 3+4k sia possibile che alla classe di resto [m-1] modulo m corrispondano due classi-radici(m-1), $[x]_m$ e $[-x]_m$, di resto modulo m. Affinché ciò avvenga deve risultare risolvibile l'equazione:

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

e cioè per m=3+4k:

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

equazione questa irrisolvibile in x in quanto, se x è pari, x^2 a differenza di 2+4k è multiplo di 4; se poi x è dispari la non risolvibilità è ancora più evidente essendo x^2 dispari e 2+4k pari. La stessa non risolvibilità della (2.10) è possibile dimostrarla per tutti i numeri rappresentati dalle due classi.

Lemma 2.11 *Per ogni n, m, k ε N_0 con m = 1+4k esistono sempre classi-radici(m-1) modulo m.*

Dim. Poniamo anche qui per ipotesi che per gli m = 1+4k sia possibile che alla classe di resto [m-1] modulo m corrispondano due classi-radici(m-1), [x] e [-x], di resto modulo m Affinché ciò avvenga deve risultare risolvibile in k l'equazione:

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

e cioè per m=1+4k:

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

equazione questa sempre risolvibile in x per ogni valore di m. Infatti sicuramente almeno una tra le due classi è rappresentabile da un numero pari il cui quadrato è sempre un multiplo di 4.

Teorema di primalità di n^2+1 2.14 *Per ogni n, k ε N ed n pari, n^2+1 è primo se $\forall p_i \in \mathbb{P}(n)$ del tipo p_i = 1+4k risulta che la classe di resto $[n]_{pi}$ modulo p_i è diversa dalle due classi-radici($p_i - 1$) modulo p_i.*

Dim. Anche i numeri primi ovviamente possono essere di due tipi: 3+4k ed 1+4k, con k appartenente a N_0**.** Richiamando la condizione di primalità (2.4) ed in base al Lemma 2.9 tra gli p_i appartenenti a $\mathbb{P}(n)$ non dobbiamo considerare quelli di tipo 3+4k giacché per essi non esiste alcuna classe-radice($p_i - 1$) modulo p_i.

Diversamente invece per i primi del tipo 1+4k (Lemma 2.10) esistono sempre due classi-radici($p_i -$ 1) modulo p_i.

Dato allora un intero positivo pari n qualsiasi, n^2+1 risulta primo se, vedi (2.4), $\forall$ pi $\leq$ n, con pi =1+4k: $[n^2]_{p_i} \neq$ pi –1 con k $\geq$ 0. Ma

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

con $[x]_{pi}$ classe di resto $[n]_{pi}$ modulo p_i. Se $\forall$ $p_i \leq$ n del tipo 1+4k la $[x]_{pi}$ della (2.15) è diversa dalle classi-radici(p_i-1) modulo p_i allora n^2+1 è primo.

Si può facilmente verificare che la suddetta condizione è soddisfatta da una lunga sequenza di n e quindi di primi $n^2 + 1$.

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) …………..

Dimostriamo ora come questa sequenza sia infinita.

3 Teorema dell'infinità degli $n^2 + 1$ primi

Definizione 3.1 *Indichiamo con $\mathbb{P}'(n)$ l'insieme dei primi appartenenti a $\mathbb{P}(n)$ del tipo p=1+4k.*

Enunciato 3.2 *I numeri primi del tipo $n^2 + 1$, con $n \varepsilon N$ e pari, sono infiniti se gli n relativi sono quelli per i quali sussiste la proprietà che $\forall p_i \in \mathbb{P}'(n)$ $[n]_{pi}$ è diverso dalle due classi-radici$(p_i - 1)$ modulo p_i.*

Dim. Tutti gli n che soddisfano le condizioni del Teorema 2.14 sono numeri interi positivi pari le cui classi di resto $[n]_{pi}$ modulo p_i, per ogni $p_i \varepsilon \mathbb{P}'(n)$, sono diverse dalle classi-radici$(p_i - 1)$ modulo p_i (per esempio se n=14 si ha che $\mathbb{P}'(n)$ = {5, 13}; le due classi-radici(5-1) modulo 5 sono $[2]_5$ e $[3]_5$ mentre le due classi-radici(13-1) modulo 13 sono $[5]_{13}$ e $[8]_{13}$; invece le due classi di resto 14 modulo 5 e modulo 13 sono rispettivamente $[4]_5$ e $[1]_{13}$, e cioè diverse dalle rispettive classi-radici precedenti, e pertanto 14^2 +1=197 è un numero primo).

Ciò detto vediamo come calcolare il numero degli n, tali che n^2+1 sia primo, minori di un qualsiasi numero intero positivo pari $N_0 > 5$.

Selezionato allora un $N_0 > 5$ indichiamo con $\prod(N_0)$ il prodotto di tutti i primi appartenenti a $\mathbb{P}'(N_0)$ e consideriamo la tabella numeri-classi (appendice A) costituita per ogni numero naturale dell'intervallo $[0, \prod(N_0)]$ dalle classi di resto $[n]_{pi}$ modulo p_i per ogni p_i appartenente a $\mathbb{P}'(N_0)$.

Eliminiamo quindi da questa tabella le righe che presentano classi di resto n dei moduli primi p_i appartenenti $\mathbb{P}'(N_0)$ uguali alle due classi-radici$(p_i - 1)$ modulo p_i. I numeri della tabella numeri-classi, le cui righe sono state eliminate attraverso il precedente crivello, possono essere allora solo quelli che nella loro combinazione di classi di resto $[n]_{pi}$ modulo p_i non presentano, per ogni p_i appartenente a $\mathbb{P}'(N_0)$, le rispettive due classi-radici$(p_i -1)$ modulo p_i.

Allora i numeri pari **M** della tabella non cancellati, in base al calcolo combinatorio, risulteranno essere:

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

La (3.3) ci fornisce quindi la quantità dei numeri **M** della tabella-intervallo $[0, \prod(N_0)]$ la cui combinazione di classi di resto $[n]_{pi}$ modulo p_i non comprende, per ogni p_i appartenente a $\mathbb{P}'(N_0)$, le rispettive due classi-radici$(p_i -1)$ modulo p_i. Ma nell'intervallo $[0, \prod(N_0)]$ sono presenti sicuramente (postulato di Bertrand) primi maggiori di N_0, e quindi non contenuti nell'insieme $\mathbb{P}'(N_0)$, le cui classi-radici$(p_i$-1) modulo p_i possono essere uguali alle classi di resto $[n]_{pi}$ per gli stessi moduli p_i. Questa eventualità esclude di estendere anche per gli n compresi nell'intervallo $]N_0, \prod(N_0)]$ l'applicabilità del teorema di primalità 2.14. Possiamo invece affermare che tutti i numeri $\mathbf{M_{N0}}$ minori o uguali ad N_0 (e quindi appartenenti all'intervallo $[0, N_0]$) e per i quali è rispettata la condizione di primalità del teorema 2.14 sono tali per cui $M_{N0}{}^2 + 1$ è primo.
L'esistenza di questi numeri $\mathbf{M_{N0}}$ ci viene garantita dalla verifica della loro presenza già per $N_0 = 6$: n=2 (n^2+1=5), n=4 (n^2+1=17) ed n=6 (n^2+1=37)………..

Se ora consideriamo un numero $N_1 > N_0$ e tale che $\prod(N_1) > \prod(N_0)$ avremo sicuramente che:

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

e cioè la quantità dei numeri **M** della tabella-intervallo $[0, \prod(N_1)]$ è maggiore di quella dei numeri **M** della tabella-intervallo $[0, \prod(N_0)]$. Questo comporta che anche gli M_{N1} dell'intervallo $[0, N_1]$ sono maggiori o eguali degli M_{N0} dell'intervallo $[0, N_0]$. Procedendo con N_i successivi crescenti il numero degli M_{Ni} cresce progressivamente e non ci può essere nessun N_{max} tale per cui $\forall n > N_{max}$ $n^2 + 1$ non è primo.

APPENDICE A

TABELLA NUMERI-CLASSI: NUMERI Ɛ [0, ∏(N0)] - CLASSI DI RESTO MODULO p Ɛ P'(N0)

N_0 = 14 - P'(N_0) = {5, 13} - [0, ∏(N_0)] = [0. 65]

n	**5**	**13**
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	0	5
6	1	6
7	2	7
8	3	8
9	4	9
10	0	10
11	1	11
12	2	12
13	3	0
14	4	1
15	0	2
16	1	3
17	2	4
18	3	5
19	4	6
20	0	7
21	1	8
22	2	9
23	3	10
24	4	11
25	0	12
26	1	0
27	2	1
28	3	2
29	4	3
30	0	4
31	1	5
32	2	6

n	**5**	**13**
33	3	7
34	4	8
35	0	9
36	1	10
37	2	11
38	3	12
39	4	0
40	0	1
41	1	2
42	2	3
43	3	4
44	4	5
45	0	6
46	1	7
47	2	8
48	3	9
49	4	10
50	0	11
51	1	12
52	2	0
53	3	1
54	4	2
55	0	3
56	1	4
57	2	5
58	3	6
59	4	7
60	0	8
61	1	9
62	2	10
63	3	11
64	4	12
65	0	0

BIBLIOGRAFIA

[a] Alessandro Zaccagnini - Introduzione alla Teoria Analitica dei Numeri:
http://people.dmi.unipr.it/alessandro.zaccagnini/psfiles/lezioni/tdn2005.pdf

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

[c] Aldo Pappalepore – Congruenza, Primalità e Densità:
https://www.aldopappalepore.it

[d] Aldo Pappalepore – La congettura di Legendre:
https://www.aldopappalepore.it/_downloads/4707fa05bd47675b98ad24f2c77c0074