Aldo Pappalepore
aldo.pappalepore@libero.it

Investigation of Legendre conjecture with the primality theorem of Congruence

Indagine sulla congettura di Legendre con il teorema di primalità della Congruenza

Abstract

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

Nell'articolo viene sviluppato uno studio sulla congettura di Legendre che si basa sul teorema di primalità della congruenza.

1 Introduzione

La congettura di Legendre afferma che esiste sempre un numero primo compreso fra n^2 ed $(n + 1)^2$. Questa congettura fa parte dei problemi di Landau e, fino ad oggi, non è stata dimostrata.

Nel 1965 Chen Jingrun dimostrò che esiste sempre un numero compreso fra n^2 ed $(n + 1)^2$ che sia un primo o un semiprimo, ossia il prodotto di due primi.

Inoltre, è noto che esiste sempre un numero primo fra $n - n^\theta$ ed n, con $\theta = 23 / 42 = 0{,}547...$ (dimostrato da J. Iwaniec e H. Pintz nel 1984).

2 La Congruenza dei numeri naturali

Come è noto la relazione di congruenza modulo m è una relazione di equivalenza definita sull'insieme dei numeri interi Z come segue: se m è un fissato numero intero maggiore di 1, due interi a e b si dicono congrui modulo m se $m|(a - b)$; m è detto modulo della congruenza e la stessa si indica con $a \equiv b \pmod m$.

Nel campo dei numeri naturali si può anche affermare in maniera equivalente che $a \equiv b \pmod m$ se a e b danno lo stesso resto nella divisione intera per m.

Per esempio, $24 \equiv 10 \pmod 7$ perché entrambi danno resto 3 nella divisione intera per 7. Tutti i numeri congrui tra loro modulo m costituiscono una classe di equivalenza, detta classe di congruenza modulo m: due numeri naturali appartengono alla stessa classe di congruenza se e solo se sono congrui modulo m e cioè se e solo se divisi per m danno lo stesso resto r. Se, come nell'esempio, il modulo è 7, si vengono così a formare sette classi (tante quanti sono i possibili resti nella divisione per 7) così indicate: [0], [1], [2], [3], [4], [5], [6]. Limitandoci sempre al sottoinsieme di Z costituito dai numeri naturali, per stabilire a quale classe modulo m appartiene uno di essi lo si divide per m, il resto indica la classe.

E' bene sottolineare come per ogni m si ha sempre che $[m]_{\text{mod } m} = [0]_{\text{mod } m}$.

Osservazione 2.1 Dalla Teoria dei Numeri sappiamo che un numero naturale qualsiasi n sarà non primo solo se divisibile per uno o più numeri primi minori o uguali della $\sqrt{n}$. Giacché tutti i numeri naturali pari, eccetto 2, sono non primi in quanto divisibili per 2, si può asserire che un numero naturale dispari qualsiasi $n > 4$ sarà non primo solo se divisibile per uno o più numeri primi dispari minori o uguali della $\sqrt{n}$.

Da qui in poi, le variabili $p, p_1, p_2, \ldots p_i$ indicano sempre numeri primi e $\mathbb{P}(M)$ l'insieme dei numeri primi dispari minori o eguali del numero M.

3 Teorema di primalità della Congruenza

Enunciato 3.1 *$\forall N_0$, $n_0 \in N$ con $N_0 \geq 3$, $0 \leq n_0 \leq N_0 - 3$ e pari se N_0 è dispari o viceversa, con $\mathbb{P}(\sqrt{(N_0 - n_0)})$ insieme dei numeri primi dispari $\leq \sqrt{(N_0 - n_0)}$, condizione necessaria e sufficiente affinché $N_0 - n_0$ sia un numero primo è che $n_0 \not\equiv N_0 (mod\ p_i)$ $\forall p_i \in \mathbb{P}(\sqrt{(N_0 - n_0)})$*

oppure che $\mathbb{P}(\sqrt{(N_0 - n_0)})$ sia un insieme vuoto.

Dim. In base alla congruenza dei numeri naturali (2.1) se N_0 e n_0 non appartengono ad una stessa classe di congruenza modulo p_i per tutti gli $p_i \in \mathbb{P}(\sqrt{(N_0 - n_0)})$, questo vuol dire che $N_0 - n_0$ (numero naturale sempre dispari) non è divisibile per nessun numero primo dispari minore o uguale della $\sqrt{(N_0 - n_0)}$ e che quindi, in base all'osservazione (2.1), $N_0 - n_0$ è un numero primo. Se invece $\mathbb{P}(\sqrt{(N_0 - n_0)})$ risulta un insieme vuoto (con $n_0 = N_0 - 3$, $N_0 - 4$, $N_0 - 5$, $N_0 - 6$, $N_0 - 7$, $N_0 - 8$) il numero $N_0 - n_0$ non può essere diviso da nessun primo e quindi è primo.

Viceversa se $N_0 - n_0$ è un numero primo esso non sarà divisibile per nessun altro numero primo dispari inferiore, uguale o inesistente della $\sqrt{(N_0 - n_0)}$ e quindi N_0 ed n_0 risulteranno sempre non congrui $\forall p_i \in \mathbb{P}(\sqrt{(N_0 - n_0)})$.

Si è posto $n_0 \leq N_0-3$ in quanto con $n_0 = N_0 - 1$ si avrebbe che $N_0 - n_0 = 1$ che, come si sa, non è un numero primo e neanche uno composto, e con $n_0 = N_0 - 2$ si avrebbe che N_0 ed n_0 sarebbero entrambi pari o dispari contrariamente all'ipotesi. Al fine di evitare poi che n_0 possa assumere valori negativi deve risultare $N_0 \geq 3$.

Osservazione 3.2 *Se invece di riferirci all'insieme $\mathbb{P}(\sqrt{(\boldsymbol{N_0 - n_0})})$ ci vogliamo riferire, per esigenze di dimostrazioni successive, all'insieme $\mathbb{P}(\sqrt{\boldsymbol{N_0}})$, il teorema (3.1) si trasforma nel corollario (3.3)*

Dato un numero $N_0 \in N$, un numero $n_0 \in N$, minore di N_0 e tale che (N_0-n_0) sia dispari si chiama **Prisotto di N_0** se risulta che $n_0 \not\equiv N_0(mod\ p_i)$ $\forall$ $p_i \in \mathbb{P}(\sqrt{(N_0)})$.

Corollario 3.3 *$\forall N_0$, $n_0 \in N$ con $N_0 \geq 9$, $0 \leq n_0 \leq N_0 - p_{max}$ e pari se N_0 è dispari o viceversa, con $\mathbb{P}(\sqrt{(N_0)})$ insieme dei numeri primi dispari $\leq \sqrt{(N_0)}$ e con p_{max} numero primo più alto di $\mathbb{P}(\sqrt{(N_0)})$, condizione necessaria e sufficiente affinché $N_0 - n_0$ sia un numero primo è che n_0 sia un numero prisotto di N_0.*

Dim. Sostituendo $\mathbb{P}(\sqrt{(N_0)})$ a $\mathbb{P}(\sqrt{(N_0 - n_0)})$, a differenza del teorema (3.1), i numeri n_0 minori di N_0 ed appartenenti all'intervallo $[N_0-p_{max.}, N_0-3]$ non vengono considerati in quanto presentano tutti almeno una classe di congruenza mod p_j, con $p_j \in \mathbb{P}(\sqrt{(N_0)})$, uguale a quella di pari modulo di N_0. Infatti per gli $n_0 \in [N_0- p_{max.}, N_0-3]$, $N_0 - n_0$ apparterrà all'intervallo $[3, p_{max}]$ e quindi sarà uguale ad un numero primo o composto appartenente a questo intervallo; nel primo caso in base all' aritmetica modulare se $N_0 - n_0 = p_j$, con $p_j \in \mathbb{P}(\sqrt{(N_0)}) \subset [3, p_{max.}]$ questo implica che $[N_0]$ mod $p_j - [n_0]$ mod $p_j = [p_j]$ mod $p_j = [0]$ da cui la congruenza mod p_j di n_0 con N_0; se invece $N_0 - n_0$ è uguale ad un numero composto $m * p_j$, con $p_j \in \mathbb{P}(\sqrt{(N_0)}) \subset [3, p_{max.}]$, si avrà che $[N_0]$ mod $p_j - [n_0]$ mod $p_j = [m]$ mod $p_j * [p_j]$ mod $p_j = [m]$ mod $p_j *[0] = [0]$ da cui la congruenza mod p_j di n_0 con N_0.

Viceversa se $N_0 - n_0$ è un numero primo, appartenente all'intervallo $]\ p_{max}, N_0]$, esso in quanto primo non sarà divisibile per nessun altro numero primo dispari inferiore o uguale di p_{max} e quindi della $\sqrt{(N_0)}$ e pertanto N_0 ed n_0 risulteranno sempre non congrui $\forall p_i \in \mathbb{P}(\sqrt{(N_0)})$.

Si è posto $N_0 \geq 9$ in quanto per valori inferiori p_{max} non sarebbe definito.

In base al corollario 3.3 possiamo affermare che i numeri n_0 prisotto di N_0, sottratti ad N_0, danno come risultato tutti i numeri primi compresi nell'intervallo $]p_{max}, N_0]$.

Osservazione 3.4 *Sia il teorema (3.1) che il corollario (3.3) nulla ci dicono sulla esistenza di almeno un n_0 incongruo. In base però al postulato di Bertrand (dimostrato successivamente da Pafnuty Chebyshev, Srinivasa Ramanujan e Paul Erdős) che afferma che per ogni $n \geq 2$ esiste almeno un primo p tale che $n < p < 2n$, si può affermare, relativamente al corollario (3.3), che nell'intervallo $]p_{max}, N_0]$ esisterà sempre almeno un primo essendo $2\,p_{max} \leq 2\sqrt{N_0} \leq N_0$ per $N_0 \geq 4$. Conseguentemente nell'intervallo $]0, N_0- p_{max}[$ esisterà sempre almeno un n_0 prisotto di N_0.*

4 Analisi della congettura con il teorema di primalità della Congruenza

Come sappiamo la congettura di Legendre afferma che esiste sempre un numero primo compreso fra n^2 ed $(n + 1)^2$.

Possiamo allora anche dire che la congettura afferma l'esistenza di un numero primo nell'intervallo $](n+1)^2-(2n+1), (n+1)^2[$. Ma in base al Corollario 3.3, con $N_0 = (n+1)^2$ e $p_{max} \leq \sqrt{N_0} \leq n+1$, nell'intervallo suddetto esiste un numero primo se e solo se nell'intervallo $]0, 2n+1]$ esiste un numero prisotto (minore di N_0 ed incongruo per tutti i primi minori o uguali a p_{max}) di $(n+1)^2$.

Teorema dell'esistenza di un primo tra n^2 ed $(n+1)^2$

Enunciato 4.1 *$\forall$ n, $n_0 \in N$ $\exists$ almeno un numero $n_0 \leq 2n+1$ tale che n_0 non è congruo con $(n+1)^2$ $\forall p_i \in \mathbb{P}(n+1)$*

Dim. Iniziamo col dire che (n+1) ed $(n+1)^2$ sono incongrui per quegli $p_i \leq p_{max}$ per i quali non risulta che $[(n+1)^2]_{p_i}$ è uguale a 0 o ad 1. Infatti sappiamo che per l'aritmetica modulare possiamo scrivere:

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

e che quindi solo per $[(n+1)]_{p_i}$ uguale a 0 o ad 1 risulterà che anche $[(n+1)^2]_{p_i}$ è uguale a 0 o ad 1 e cioè che $[(n+1)^2]_{p_i} = [(n+1)]_{p_i}$ ossia che $(n+1)^2$ e (n+1) sono congrui modulo p_i.

Indichiamo allora per qualsiasi n con p_c gli c moduli per i quali $(n+1)^2$ e (n+1) sono congrui e con p_{nc} gli nc moduli per i quali $(n+1)^2$ e (n+1) sono incongrui. Ovviamente c+nc sarà pari al numero di primi presenti nell'insieme $\mathbb{P}(n+1)$.

Teniamo anche presente che per ogni modulo p_c, per i quali $[(n+1)^2]_{p_c} = [(n+1)]_{p_c} = 0$ o ad 1, la somma o la differenza di (n+1) con 1 o con $\boldsymbol{p_{nc}}$ comporta che il termine $[(n+1)\pm 1]_{p_c}$è uguale a $[x \pm 1]_{p_c}$ e che il termine $[(n+1)\pm \boldsymbol{p_{nc}}]_{p_c}$è uguale a quello $[x \pm \boldsymbol{p_{nc}}]_{p_c}$, con x eguale a 0 o ad 1. Di conseguenza i termini $[(n+1)\pm 1]_{p_c}$ e $[(n+1)\pm \boldsymbol{p_{nc}}]_{p_c}$ saranno sicuramente diversi da x e che quindi $(n+1) \pm 1$ ed $(n+1) \pm\boldsymbol{p_{nc}}$ saranno incongrui per i moduli p_c mentre potranno diventare congrui per gli altri moduli p_{nc} diversi da $\boldsymbol{p_{nc}}$.

1ª Ipotesi: nc = 0 (p.es. n+1=6)

In questo caso per tutti i moduli p_c appartenenti a $\mathbb{P}(n+1)$ risulta $[(n+1)^2]_{p_c} = [(n+1)]_{p_c}$ ed uguali (vedi sopra) a 0 o ad 1. Se quindi sottraiamo o addizioniamo al termine (n+1) il termine 1 si avrà che i due termini $(n+1)\pm1$ saranno incongrui con $(n+1)^2$ per ogni modulo p_c, inferiori a 2n+1 e tali quindi da dar luogo (per il teorema di primalità della congruenza) nell'intervallo $]n^2, (n+1)^2[$ ai due primi:

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

2ª Ipotesi: nc = 1 (p.es. n+1=7 o 10)

In questo caso, rispetto al precedente, sommando oppure sottraendo il termine 1 a quello (n+1) può risultare al massimo uno solo tra (n+1)+1 e (n+1)-1 congruo con $(n+1)^2$ per l'unico modulo p_{nc} (p. es. n+1=10) oppure nessuno dei due (p,es, n+1=7) sempre per lo stesso modulo. Analogamente sommando oppure sottraendo l'unico p_{nc} al termine (n+1) risulteranno sia $(n+1)+p_{nc}$ che $(n+1)-p_{nc}$ incongrui con $(n+1)^2$ per tutti i moduli $p_i \leq p_{max}$. Infatti per ogni modulo p_c sia $[(n+1)+p_{nc}]_{p_c}$ che $[(n+1)-p_{nc}]_{p_c}$ saranno diversi da 0 e da 1 con la conseguenza che $(n+1)+p_{nc}$ e $(n+1)-p_{nc}$ saranno incongrui con $(n+1)^2$ per questi moduli mentre rimarrà l'incongruenza tra $(n+1)+p_{nc}$ e $(n+1)-p_{nc}$ con $(n+1)^2$ per il modulo p_{nc}. E' bene sottolineare inoltre che essendo $p_{nc} \leq p_{max} \leq n+1$ risulterà sempre $(n+1)+p_{nc} \leq 2n+1$. In conclusione in questa ipotesi ci saranno nell'intervallo $]n^2, (n+1)^2[$ sicuramente almeno tre primi:

(4.4) $(n+1)^2 - [(n+1)\pm 1]$ $\quad$ $(n+1)^2 - [(n+1)+p_{nc}]$ $\quad$ $(n+1)^2 - [(n+1)-p_{nc}]$

dove il segno ± sta ad indicare solo uno dei due

3ª Ipotesi: nc = 2 (p.es. n+1=12)

Se i p_{nc} sono 2 (p_{nc1} e p_{nc2}) nulla possiamo dire sui termini (n+1)+1 e (n+1)-1 in quanto il primo potrebbe essere congruo per il modulo p_{nc1} ed il secondo per il modulo p_{nc2}. Circa invece i termini $(n+1)+ p_{nc1}$ e $(n+1)- p_{nc1}$, che come visto sono sempre incongrui per i moduli p_c, si può affermare che sicuramente uno dei due è incongruo con $(n+1)^2$ per il modulo p_{nc2} non potendosi verificare contemporaneamente le due eguaglianze $[(n+1)+p_{nc1}]_{p_{nc2}} = [(n+1)^2]_{p_{nc2}}$ ed $[(n+1)-p_{nc1}]_{p_{nc2}} = [(n+1)^2]_{p_{nc2}}$. Analogamente si può affermare che sicuramente uno tra $(n+1)+p_{nc2}$ e $(n+1)-p_{nc2}$ è incongruo con $(n+1)^2$ per il modulo p_{nc1}. In conclusione in questa ipotesi ci saranno nell'intervallo $]n^2, (n+1)^2[$ sicuramente almeno due primi:

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

dove il segno ± sta ad indicare solo uno dei due

4ª Ipotesi: nc ≥ 3 (p.es. n+1=16)

Mettiamoci nella ipotesi di nc=3 (con $p_{nc1} < p_{nc2} < p_{nc3}$) ed escludiamo subito i termini (n+1)+1 e (n+1)-1 in quanto entrambi potrebbero essere congrui per i moduli p_{nc}. Supponiamo poi per assurdo che ogni $(n+1)+p_{nci}$ ed $(n+1)-p_{nci}$ siano congrui con $(n+1)^2$ rispettivamente per il modulo p_{ncj} e per il modulo p_{nck} e cioè che si verifichino le seguenti uguaglianze:

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

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

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

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

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

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

da cui discendono queste altre eguaglianze:

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

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

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

ed infine queste ultime:

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

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

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

che sono evidentemente false essendo sempre:

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

Ne risulta che almeno tre eguaglianze delle (4.6) non sono possibili e che quindi nell'intervallo $]n^2, (n+1)^2[$ ci sono sicuramente almeno tre primi.

Se invece nc > 3, ripetendo il ragionamento fatto per nc=3, si verifica facilmente che aumenta il numero di eguaglianze del tipo (4.6) non possibili e quindi anche il numero di primi presenti nell'intervallo $]n^2, (n+1)^2[$.

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/_downloads/394a65a2c2c6bc8a27c5aab800f93b84