Aldo Pappalepore
aldo.pappalepore@libero.it

Primality theorems of Congruence and of Complementary Congruence and density of incongruous numbers

Teoremi di primalità della Congruenza e della Congruenza Complementare e densità dei numeri incongrui

Abstract

In the article, a study of congruence and complementary congruence is developed that arrives at the definition of two primality theorems of congruence and compcongruence and the density function of incongruent numbers. The study is preparatory to the demonstration of the Hardy-Littlewood and Goldbach conjectures. The study and opens up new areas of possible research in the field of Number Theory..

Nell'articolo viene sviluppato uno studio sulla congruenza e sulla congruenza complementare che perviene alla definizione di due teoremi di primalità della congruenza e della compcongruenza ed alla funzione di densità dei numeri incongrui. Lo studio è propedeutico alla dimostrazione delle congetture di Hardy-Littlewood e di Goldbach. Lo studio ed apre nuovi ambiti di possibile ricerca nel campo della Teoria dei numeri.

1 Le primalità da Congruenza

1.1 La Congruenza dei numeri naturali

Come è noto la relazione di congruenza [1.2.1 di (a)] 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 ≡ b (mod m).
Nel campo dei numeri naturali si può anche affermare in maniera equivalente che a ≡ b (mod m) se a e b danno lo stesso resto nella divisione intera per m.
Per esempio, 24 ≡ 10 (mod 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 1.1.2 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, ... p_i indicano sempre numeri primi e $\mathbb{P}(M)$ l'insieme dei numeri primi dispari minori o eguali del numero M.

1.2 Teorema della Primalità della Congruenza

Enunciato 1.2.1 *$\forall N_0, n_0 \in N$ con $N_0 \geq 3$, $0 \leq n_0 \leq N_0 - 3$ e pari se N_0 è dispari o viceversa, con $\mathbb{P}\left(\sqrt{(N_0 - n_0)}\right)$ 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 $n_0 \not\equiv N_0 (mod\, p_i)$ $\forall p_i \in \mathbb{P}\left(\sqrt{(N_0 - n_0)}\right)$ oppure che $\mathbb{P}\left(\sqrt{(N_0 - n_0)}\right)$ sia un insieme vuoto.*

Dim. In base alla congruenza dei numeri naturali (1.1) se N_0 e n_0 non appartengono ad una stessa classe di congruenza modulo p_i per tutti gli $p_i \in \mathbb{P}\left(\sqrt{(N_0 - n_0)}\right)$, 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 (1.1.2), $N_0 - n_0$ è un numero primo. Se invece $\mathbb{P}\left(\sqrt{(N_0 - n_0)}\right)$ 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 $\forall p_i \in \mathbb{P}\left(\sqrt{(N_0 - n_0)}\right)$.

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 1.2.2 *Se invece di riferirci all'insieme $\mathbb{P}\left(\sqrt{(\boldsymbol{N_0 - n_0})}\right)$ ci vogliamo riferire, per esigenze di dimostrazioni successive, all'insieme $\mathbb{P}\left(\sqrt{\boldsymbol{N_0}}\right)$, il teorema (1.2.1) si trasforma nel corollario (1.2.3)*

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 $n_0 \not\equiv N_0 (\mathrm{mod}\, p_i)$ $\forall p_i \in \mathbb{P}\left(\sqrt{(N_0)}\right)$.

Corollario 1.2.3 *$\forall N_0, n_0 \in N$ con $N_0 \geq 9$, $0 \leq n_0 \leq N_0 - p_{max}$ e pari se N_0 è dispari o viceversa, con $\mathbb{P}\left(\sqrt{(N_0)}\right)$ insieme dei numeri primi dispari $\leq \sqrt{(N_0)}$ e con p_{max} numero primo più alto di $\mathbb{P}\left(\sqrt{(N_0)}\right)$, 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 $\mathbb{P}\left(\sqrt{(N_0)}\right)$ a $\mathbb{P}\left(\sqrt{(N_0 - n_0)}\right)$, a differenza del teorema (1.2.1), 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 $p_j \in \mathbb{P}\left(\sqrt{(N_0)}\right)$, 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 $p_j \in \mathbb{P}\left(\sqrt{(N_0)}\right) \subset [3, p_{max}.]$ questo implica che $[N_0] \bmod p_j - [n_0] \bmod p_j = [p_j] \bmod p_j = [0]$ 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 $p_j \in \mathbb{P}\left(\sqrt{(N_0)}\right) \subset [3, p_{max}.]$, si avrà che $[N_0] \bmod p_j - [n_0] \bmod p_j = [m] \bmod p_j * [p_j] \bmod p_j = [m] \bmod p_j * [0] = [0]$ 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 $\forall p_i \in \mathbb{P}\left(\sqrt{(N_0)}\right)$.

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

In base al corollario 1.2.3 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 1.2.4 *Ovviamente, a parità di N_0, la differenza tra l'insieme dei numeri incongrui minori di N_0 moduli $\mathbb{P}\left(\sqrt{(\boldsymbol{N_0 - n_0})}\right)$ e quello dei numeri prisotto di N_0 è data da tutti gli $n_0 = N_0 - p_i$ con $p_j \in \mathbb{P}\left(\sqrt{(\boldsymbol{N_0})}\right)$. In pratica il numero di tutti i primi dispari minori o uguali ad N_0 è pari alla somma del numero dei numeri prisotto di N_0 e di quello dei $p_j \in \mathbb{P}\left(\sqrt{(\boldsymbol{N_0})}\right)$.*

Osservazione 1.2.5 *Sia il teorema (1.2.1) che il corollario (1.2.3) nulla ci dicono sulla esistenza di almeno un n_0 incongruo. In base però al postulato [6.3 di (b)] 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 (1.2.3), 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.*

1.3 La Compcongruenza dei numeri naturali

Introduciamo ora la **Congruenza Complementare** (compcongruenza) modulo m come la relazione di corrispondenza 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 compcongrui modulo m se m|(a + b); m è detto modulo della compcongruenza e la stessa la indicheremo con a ‖ b (mod m).

Nel campo dei numeri naturali si può anche affermare in maniera equivalente che a ‖ b (mod m) se a e b danno due resti complementari rispetto ad m nella divisione intera per m. Per esempio, 24 ‖ 39 (mod 7) perché danno come resti nella divisione intera per 7 rispettivamente 3 e 4, cioè due numeri complementari rispetto a 7.

1.4 Teorema della Primalità della Compcongruenza

Enunciato 1.4.1 *$\forall N_0, n_0 \in N$ con $N_0 \geq 2$, $0 \leq n_0 \leq N_0 - 1$ e pari se N_0 è dispari o viceversa, con $\mathbb{P}\left(\sqrt{(N_0 + n_0)}\right)$ 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 $n_0 \nmid N_0 (mod\, p_i)$ $\forall p_i \in \mathbb{P}\left(\sqrt{(N_0 + n_0)}\right)$ oppure che $\mathbb{P}\left(\sqrt{(N_0 + n_0)}\right)$ sia un insieme vuoto.*

Dim. In base alla compcongruenza dei numeri naturali (1.3), se N_0 e n_0 **non** sono compcongrui modulo p_i per tutti gli p_i appartenenti all'insieme $\mathbb{P}\left(\sqrt{(\boldsymbol{N_0 + n_0})}\right)$, questo vuol dire che $N_0 + n_0$ non è divisibile per nessun numero primo minore della $\sqrt{(\boldsymbol{N_0 + n_0})}$ e che quindi, in base all'osservazione (1.1.2), $N_0 + n_0$ è un numero primo. Se invece $\mathbb{P}\left(\sqrt{(\boldsymbol{N_0 + n_0})}\right)$ risulta un insieme vuoto 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 compcongrui $\forall p_i \in \mathbb{P}\left(\sqrt{(N_0 + n_0)}\right)$.

Si è posto $N_0 \geq 2$ in quanto con N_0=1 ed n_0=0 si avrebbe N_0+n_0 =1, numero non primo e non composto.

Osservazione 1.4.2 *Se invece di riferirci all'insieme $\mathbb{P}\left(\sqrt{(\boldsymbol{N_0 + n_0})}\right)$ ci vogliamo riferire, per esigenze di dimostrazioni successive, all'insieme $\mathbb{P}\left(\sqrt{\boldsymbol{2N_0}}\right)$ il teorema (1.4.1) si trasforma nel corollario (1.4.3).*

Assegnati cioè due numeri N_0, $n_0 \in N$, con $n_0 < N_0$ e tali che (N_0+n_0) sia dispari, se risulta che ogni numero primo dispari $p \leq \sqrt{(2N_0)}$ non divide il numero (N_0+n_0) vuol dire che lo stesso è primo.

Dato un numero $N_0 \in N$, un numero $n_0 \in N$, minore o uguale di N_0 e tale che (N_0+n_0) sia dispari si chiama **Prisopra di N_0**, se risulta che $n_0 \nmid N_0 (\text{mod } p_i)\ \forall\ p_i \in \mathbb{P}\left(\sqrt{(2N_0)}\right)$.

Corollario 1.4.3 *$\forall\ N_0, n_0 \in N$ con $N_0 \geq 2$, $0 \leq n_0 \leq N_0-1$ e pari se N_0 è dispari o viceversa, con $\mathbb{P}\left(\sqrt{(2N_0)}\right)$ insieme dei numeri primi dispari $\leq \sqrt{(2N_0)}$, condizione necessaria e sufficiente affinché $N_0 + n_0$ sia un numero primo è che n_0 sia un prisopra di N_0.*

Dim. Estendendo l'insieme dei numeri primi del teorema (1.4.1) da $\mathbb{P}\left(\sqrt{(\boldsymbol{N_0 + n_0})}\right)$ **a** $\mathbb{P}\left(\sqrt{(\boldsymbol{2N_0})}\right)$ ed indicando con $\mathbb{P}(\Delta 2N_0)$ l'insieme dei primi presenti in $\mathbb{P}\left(\sqrt{(2N_0)}\right)$ e non in $\mathbb{P}\left(\sqrt{(N_0 + n_0)}\right)$, nulla cambia in quanto per ognuno dei numeri n_0 (incompcongrui con N_0 moduli $\mathbb{P}\left(\sqrt{(N_0 + n_0)}\right)$ tali che $N_0+n_0 = p_j$, con p_j appartenente all'intervallo $[N_0,2N_0]$, non potrà mai verificarsi che n_0 è compcongruo con N_0 moduli $\mathbb{P}(\Delta 2N_0)$, e cioè che $[N_0]_{mod\ p_i} + [n_0]_{mod\ p_i} = [0]_{mod\ p_i}$, per almeno un $p_i \in \mathbb{P}(\Delta 2N_0)$**.** Infatti, tenendo presente che $\sqrt{2N_0} \leq N_0$ con $N_0 \geq 2$ e che quindi tutti i primi p_i appartenenti all'insieme $\mathbb{P}(\Delta 2N_0)$ sono $\leq N_0$ si ha che per ogni p_j appartenente all'intervallo $[N_0,2N_0]$ risulta $[p_j]_{mod\ p_i} \neq [0]$ essendo sempre p_i *e* p_j due numeri primi e diversi tra loro. Di conseguenza per ognuno dei numeri n_0 tali che $N_0+n_0 = p_j$, poiché in base all'aritmetica modulare risulta sempre $[N_0] \text{ mod } p_j + [n_0] \text{ mod } p_j = [p_j]_{mod\ p_i}$ e quest'ultimo è sempre diverso da zero, si può affermare che n_0 è prisopra di N_0.
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 $\sqrt{(2N_0)}$ e quindi N_0 ed n_0 risulteranno sempre non compcongrui $\forall p_i \in \mathbb{P}\left(\sqrt{(2N_0)}\right)$.

Osservazione 1.4.4 *Sia il teorema (1.4.1) che il corollario (1.4.3) nulla ci dicono sulla esistenza di almeno un n_0 prisopra di N_0. Ma in base al postulato di Bertrand [6.3 di (b)] si può affermare che nell'intervallo $[N_0, 2N_0]$ esisterà sempre almeno un primo e conseguentemente nell'intervallo $]0, N_0]$ esisterà sempre almeno un n_0 prisopra di N_0.*

1.5 I numeri e le loro classi di congruenza

La Teoria dei Numeri ci dice che così come esiste nei sistemi numerici posizionali (p.es. quello decimale) una corrispondenza biunivoca tra tutti i numeri possibili esprimibili con n cifre (e quindi appartenenti all'intervallo $]0,\ 10^n - 1]$) e tutte le possibili combinazioni (10^n) delle 10 cifre, analogamente esiste una corrispondenza biunivoca tra tutti i numeri dell'intervallo $]0,\ p_{max}\#]$, con p_{max} primo qualsiasi e p_{max} # il suo primoriale, e le combinazioni delle classi di congruenza di questi numeri aventi per modulo i singoli numeri primi minori ed uguali a p_{max}. L'esistenza di questa corrispondenza biunivoca è facilmente dimostrabile ricorrendo al Teorema Cinese del Resto [2.3.3 di (b)] ed inserendo come moduli del sistema di equazioni p_{max} e tutti i primi minori di esso.

Osservazione 1.5.1 Chiameremo **Tabella numeri-classi $\boldsymbol{p_{max}}$** la tabella che ad ogni numero dell'intervallo $]0,\ p_{max}\#]$ associa la combinazione delle classi di congruenza di questo numero aventi per modulo i singoli numeri primi minori ed uguali a p_{max}.

A scopo esemplificativo consideriamo (vedi appendice A) una **tabella numeri-classi** 7 contenente per ogni numero la corrispondente combinazione delle sue 4 classi di congruenza mod 2, mod 3, mod 5 e mod 7.
In questa tabella si può verificare la corrispondenza biunivoca suddetta. Per es. alla combinazione 1-2-2-3 delle classi di congruenza mod 2, mod 3, mod 5 e mod 7 corrisponde solo il numero 17

nell'intervallo [1, 210] così come al numero 151 corrisponde solo la combinazione 1-1-1-4 delle stesse classi di congruenza sempre nell'intervallo [1, 210].

Come vedremo in seguito la Tabella numeri-classi p_{max} viene introdotta in questo studio per poter calcolare le densità dei numeri prisotto e prisopra di N_0.

1.6 Dalla Tabella numeri-classi p_{max} alle Primalità

C'è un criterio per desumere dalla Tabella numeri-classi p_{max} e dalle informazioni in essa contenute quanti sono, oltre ai moduli {2,3,…..,. p_{max}} su cui la tabella è costruita, i numeri primi minori o uguali ad un qualsiasi $N_0 \in]0, p_{max}\#]$ e quelli compresi nell'intervallo [N_0, 2 N_0] ?

Osservazione 1.6.1 *Tra i diversi criteri possibili quello che ci interessa per le nostre dimostrazioni successive consiste nell'applicazione del corollario (1.2.3) della Primalità della Congruenza e di quello (1.4.3) della Primalità della Compongruenza in base ai quali il numero dei primi dispari minori o uguali ad N_0 è, a meno dei primi minori della $\sqrt{(\boldsymbol{N_0})}$ e cio*è *i moduli {2,3,…..,. p_{max}} su cui è costruita la tabella, uguale a quello dei numeri della tabella prisotto di N_0 mentre il numero dei primi presenti nell'intervallo* [N_0, 2 N_0] è uguale a quello dei numeri prisopra di N_0.

Da questa osservazione discende che per ricavare dalla tabella numeri-classi p_{max} i numeri primi minori o uguali di N_0 utilizzando il criterio della Primalità della Congruenza bisogna imporre una condizione che lega N_0 alla tabella numeri-classi p_{max} e cioè che i moduli della tabella devono essere esattamente tutti i primi minori o uguali della $\sqrt{(N_0)}$.

Nel caso della nostra tabella esemplificativa [1, 210] possiamo affermare che soltanto per gli N_0 tali che $7 \leq \sqrt{(N_0)} < 11$ e cioè per gli N_0 maggiori o uguali di 49 e minori di 121 possiamo dire che i numeri della tabella n_0 prisotto di N_0 sono tali per cui $N_0 - n_0$ è un numero primo.

Analogamente per desumere dalla tabella-intervallo $]0, p_{max}\#]$ e dalle informazioni in essa contenute quanti sono i numeri primi presenti nell'intervallo [N_0, 2N_0] con $N_0 \in]0, p_{max}\#]$ utilizzando il criterio (corollario 1.4.3) della Primalità della Compcongruenza bisogna imporre che i moduli {2,3,…..,. p_{max}} della tabella siano esattamente tutti i primi minori o uguali della $\sqrt{(2N_0)}$. Con questa condizione si avrà che i numeri della tabella incompcongrui minori di N_0 sono prisopra di N_0 e cioè tali per cui $N_0 + n_0$ è un numero primo.

Nel caso della nostra tabella [1, 210] per esempio possiamo affermare che soltanto per gli N_0 tali che $7 \leq \sqrt{(2N_0)} < 11$ e cioè per gli N_0 maggiori o uguali di 25 e minori di 61 possiamo dire che i numeri n_0 incompcongrui minori di N_0 sono prisopra di N_0 e cioè che sommati ad N_0 danno i numeri primi dell'intervallo [N_0, 2N_0].

1.7 Da N_0 ai primi dell'intervallo]0, 2N_0]

Se allora, fissato un qualsiasi $N_0 \in N$ maggiore di 49, vogliamo individuare quanti sono i numeri primi minori o uguali ad N_0 occorre trovare innanzitutto il più alto numero primo p_{max} minore o uguale della $\sqrt{(N_0)}$ e considerare poi la tabella numeri-classi p_{max} $]0, p_{max}\#]$, dove $p_{max}\#$ è il primoriale di p_{max} e corrisponde al prodotto dei numeri primi $\leq p_{max}$ *Poiché il primoriale $p_{max}\#$ coincide col primoriale $\sqrt{(\boldsymbol{N_0})}$ # nel prosieguo dello studio scriveremo indifferentemente]0, $p_{max}\#$] o]0, $\sqrt{(\boldsymbol{N_0})}$ #] per indicare la stessa* Tabella numeri-classi p_{max}.

Osservazione 1.7.1 *La condizione che N_0 sia maggiore o eguale di 49 deriva dalla necessità che N_0 appartenga all'intervallo]0, $p_{max}\#$].*

Per quanto scritto nell'osservazione (1.6.1) il numero di primi minori o uguali di N_0 ci è dato, a meno dei primi minori della $\sqrt{(\boldsymbol{N_0})}$ e cioè i moduli 2, 3, ….., p_{max} su cui è costruita la tabella, da quello dei numeri della tabella prisotto di N_0**,** numero che in base all'osservazione (1.2.5) sarà sempre uguale o maggiore di 1.

Per es. con N_0 = 315 si avrà che $\sqrt{315}$=17,746 e quindi p_{max} sarà uguale a 17, p_{max}# (2*3*5*7*11*13*17) sarà uguale a 510510 ed al numero 315 corrisponderà, nell'intervallo [0 , p_{max}#], una ed una sola combinazione delle sue classi di congruenza mod 2, mod 3, mod 5, mod 7, mod 11, mod 13 e mod 17. Tutti gli n_0 minori di N_0 ed incongrui con esso relativamente agli $p_i \leq p_{max}$, cioè tutti gli n_0 prisotto di N_0, sottratti ad N_0 danno come risultato tutti i numeri primi minori di N_0**,** ad eccezione dei primi 2,3,5,7,11,13,17 su cui è costruita la tabella. Invece in base al corollario (1.2.3) ed all'osservazione (1.6.1), nulla si può dire circa gli altri numeri della tabella m_0 magggiori di 315 ed incongrui con esso moduli p_i appartenenti a $\mathbb{P}\left(\sqrt{(315)}\right)$.

Analogamente se vogliamo individuare, attraverso una tabella numeri-classi p_{max}, quanti sono i numeri primi presenti nell'intervallo [N_0, $2N_0$] con qualsiasi $N_0 \geq 121$, occorre trovare innanzitutto il più alto numero primo p_{max} minore della $\sqrt{2N_0}$ e considerare quindi la tabella numeri-classi p_{max}]0, $\sqrt{(2\boldsymbol{N_0})}$#].

Osservazione 1.7.2 *Anche qui la condizione che N_0 sia maggiore o eguale di 121 deriva dalla necessità che $2N_0$ appartenga all'intervallo]0, $\sqrt{(2\boldsymbol{N_0})}$#].*

Per quanto scritto nell'osservazione (1.6.1) il numero di primi presenti nell'intervallo [N_0, $2N_0$] ci è dato da quello dei numeri della tabella prisopra di N_0, numero che in base all'osservazione (1.4.4) sarà sempre uguale o maggiore di 1.

Se si mantiene l'esempio precedente di N_0 = 315, occorre in questo caso calcolare la $\sqrt{2 * 315}$ che è 25,1, da cui discende che p_{max} sarà uguale a 23, $\sqrt{(2\boldsymbol{N_0})}$# (uguale a 2*3*5*7*11*13*17*19*23) sarà uguale a 223092870 ed al numero 315 corrisponderà, nell'intervallo]0, $\sqrt{(2\boldsymbol{N_0})}$#], una ed una sola combinazione delle sue classi di congruenza mod 2, mod 3, mod 5, mod 7, mod 11, mod 13, mod 17, mod 19, mod 23. Tutti gli n_0 minori di N_0 ed incompcongrui con esso, cioè tutti gli n_0 prisopra di N_0, sommati ad N_0 daranno come risultato tutti i numeri primi compresi nell'intervallo [N_0**,** **2** N_0]. Invece in base al corollario (1.4.3) ed all'osservazione (1.6.1), nulla si può dire circa gli altri numeri della tabella m_0 maggiori di 315 ed incompcongrui con esso moduli $\mathbb{P}\left(\sqrt{(315)}\right)$.

2 La distribuzione dei numeri primi

2.1 Il Teorema fondamentale dei numeri primi

La Congettura di Gauss, risalente al 1792 e poi diventato Teorema dei Numeri Primi (TNP), sulla distribuzione dei numeri primi è:

(2.1.1) $\pi(N) \approx \frac{N}{logN} \approx \int_2^N \frac{dt}{logt} \approx Li(N)$

dove π(N) è il numero dei primi minori o uguali ad N.

Questa congettura fu dimostrata per la prima volta nel 1986 da Hadamard e de La Vallée Poussin utilizzando metodi della teoria delle funzioni complesse legati alle proprietà della funzione ζ di Riemann. I matematici del tempo, ed in particolare G. H. Hardy, ritenevano che l'analisi complessa era necessariamente coinvolta nel Teorema e che metodi con sole variabili reali erano da considerare inadeguati. Ma nel 1949 Erdös e Selberg [3.4 di (a)] pubblicano indipendentemente una

dimostrazione elementare (cioè con sole variabili reali), basata sulla tecnica combinatoria, del Teorema dei numeri primi.

La dimostrazione di Selberg - Erdős [3.4 di (a)] ha messo quindi in gioco la presunta superiorità (profondità) dell'analisi complessa per la dimostrazione del TNP, mostrando che anche i metodi tecnicamente elementari, che abbiamo adottato anche in questo studio, hanno la loro efficacia dimostrativa.

2.2 La densità media degli n_0 incongrui di N_0 nella tabella $]0, \sqrt{(N_0)}\#]$

Fissato un qualsiasi $\boldsymbol{N_0 \in N}$ maggiore di 49, consideriamo (vedi par. 1.6 ed 1.7) la relativa tabella numeri-classi p_{max} dell'intervallo $]0, p_{max}\ \#]$, dove p_{max} è il più alto numero primo minore o uguale della $\sqrt{(N_0)}$, e calcoliamo il numero di tutti (maggiori e minori di N_0) gli n_0 incongrui di N_0 presenti in tabella.

Eliminiamo allora da questa tabella le righe che presentano una o più classi di congruenza dei moduli p_i $(2, 3, 5, \ldots\ldots, p_{max})$ uguali alla classe corrispondente al resto di N_0 per gli stessi moduli.

I numeri M della tabella, non eliminati attraverso il precedente crivello, possono essere allora solo quelli che nella tabella numeri-classi p_{max} presentano per ogni $p_i \in \mathbb{P}\left(\sqrt{(N_0)}\right)$ una delle p_i -1 possibili classi di congruenza diverse da quella corrispondente di N_0. (se per es. (N_0) mod7 = 3, (M) mod7 dovrà essere eguale ad una delle 6 (7-1) possibili altre classi di congruenza: 0,1,2,4,5,6)

Le righe della tabella non cancellate allora, in base al calcolo combinatorio, risulteranno essere:

(2.2.1) $\prod_{p=2}^{p_{max}}(p-1)$

La (2.2.1) ci fornisce quindi la quantità di tutti i numeri **M** della tabella **incongrui (minori e maggiori) di N_0 per i soli moduli p_i** appartenenti all'insieme $\mathbb{P}\left(\sqrt{(N_0)}\right)$.

Calcoliamo ora la **densità media $Dnc_{]0,\sqrt{N_0}\#]}$** di questi numeri M esistenti nell'intervallo $]0, \sqrt{(N_0)}\ \#]$ con $\sqrt{(N_0)}\ \# = 2*3*\ldots\ldots*p_{max}$, si può scrivere:

(2.2.2) $Dnc_{]0,\sqrt{N_0}\#]} = \frac{\prod_{p=2}^{p_{max}}(p-1)}{2*3*\ldots*pmax} = \frac{\prod_{p=2}^{p_{max}}(p-1)}{\prod_{p=2}^{p_{max}} p} = \prod_{p=2}^{p_{max}} \frac{(p-1)}{p}$

[*formula questa che moltiplicata per* $\sqrt{(N_0)}\ \#$ *corrisponde alla funzione di Eulero* $\varphi(n)$ *con* $n=\sqrt{(N_0)}\ \#$, *e fornisce il numero di coprimi minori di* $\sqrt{(N_0)}\ \#$, *numero che comprende anche quello dei primi minori di* N_0 *eccezion fatta per i primi appartenenti all'insieme* $\mathbb{P}\left(\sqrt{(N_0)}\right)$]

In base al corollario (1.2.3) della Primalità della Congruenza ed al fatto che tutti i numeri M minori di N_0 (**M_{N0}**) sono **prisotto di N_0**, possiamo affermare che, per ognuno di questi numeri M_{N0}, N_0-M_{N0} è un numero primo e che la densità media $Dnc_{]0,N_0]}$ degli M_{N0} nell'intervallo $]0, N_0]$ ci è data da:

(2.2.3) $Dnc_{]0,N_0]} = \frac{Q(M_{N0})}{N_0}$ indicando con $Q(M_{N0})$ il numero degli M_{N0} presenti nell'intervallo $]0, N_0]$.

Come da osservazione (1.2.4) il numero di **tutti** i primi $\pi(N_0)$ minori o eguali ad N_0 è dato dalla somma del numero degli M_{N0} e di quello di tutti i $p_j \in \mathbb{P}\left(\sqrt{(N_0)}\right)$ che, come sappiamo, non rientrano tra gli N_0 - M_{N0}.

Sappiamo poi dal TNP (2.1) che la densità media $Dprimi_{N0}$ dei numeri primi minori di N_0, che coincide, a meno degli p_i appartenenti all'insieme $\mathbb{P}\left(\sqrt{(N_0)}\right)$, con la densità media Dnc_{N0} dei numeri M_{N0} **prisotto di N_0** ci è data da:

(2.2.4) $$Dprimi_{]0,N_0]} = \frac{\pi(N_0)}{N_0} = \frac{1}{logN_0} \approx Dnc_{]0,N_0]}$$

da cui:

(2.2.5) $$M_{N0} \approx \pi(N_0) \approx \frac{N_0}{logN_0}$$

Per la densità $Dprimi_{N0}$ bisogna cioè considerare, oltre ai numeri M_{N0} minori di N_0 ed incongrui con esso, anche gli pi appartenenti all'insieme $\mathbb{P}\left(\sqrt{(N_0)}\right)$ e conseguentemente risulta sempre $Dprimi_{N0} > Dnc_{N0}$. Calcoliamo allora l'errore che si compie ponendo Dprimi = Dnc_{N0}. In base al TNP (2.1) si può scrivere:

(2.2.6) $$Dnc_{]0,N_0]} = \frac{\left(\frac{N_0}{logN_0} - \frac{\sqrt{N_0}}{log\sqrt{N_0}}\right)}{N_0} \qquad \text{e} \qquad Dprimi_{]0,N_0]} = \frac{1}{logN_0}$$

Osservazione 2.2.6 *Accertato che risulta sempre $Dprimi_{]0,N_0]} > Dnc_{]0,N_0]}$ si può facilmente calcolare che l'errore percentuale che si commette nel porre $Dprimi_{]0,N_0]} = Dnc_{]0,N_0]}$ è del 20% per $N_0 = 10^2$, del 2% per $N_0 = 10^4$, dello 0,02% per $N_0 = 10^8$ e che esso è via via decrescente per valori crescenti di N_0.*

APPENDICE A

Tabella indicante la corrispondenza biunivoca tra i numeri da 1 a 210 e tutte le combinazioni delle classi di congruenza modulo 2 - 3 – 5– 7

num.	moduli	num.	moduli	num.	moduli
	2 – 3 – 5 - 7		2 – 3 – 5 - 7		2 – 3 – 5 - 7
1)	1 - 1 - 1 - 1	71)	1 - 2 - 1 - 1	141)	1 - 0 - 1 - 1
2)	0 - 2 - 2 - 2	72)	0 - 0 - 2 - 2	142)	0 - 1 - 2 - 2
3)	1 - 0 - 3 - 3	73)	1 - 1 - 3 - 3	143)	1 - 2 - 3 - 3
4)	0 - 1 - 4 - 4	74)	0 - 2 - 4 - 4	144)	0 - 0 - 4 - 4
5)	1 - 2 - 0 - 5	75)	1 - 0 - 0 - 5	145)	1 - 1 - 0 - 5
6)	0 - 0 - 1 - 6	76)	0 - 1 - 1 - 6	146)	0 - 2 - 1 - 6
7)	1 - 1 - 2 - 0	77)	1 - 2 - 2 - 0	147)	1 - 0 - 2 - 0
8)	0 - 2 - 3 - 1	78)	0 - 0 - 3 - 1	148)	0 - 1 - 3 - 1
9)	1 - 0 - 4 - 2	79)	1 - 1 - 4 - 2	149)	1 - 2 - 4 - 2
10)	0 - 1 - 0 - 3	80)	0 - 2 - 0 - 3	150)	0 - 0 - 0 - 3
11)	1 - 2 - 1 - 4	81)	1 - 0 - 1 - 4	151)	1 - 1 - 1 - 4
12)	0 - 0 - 2 - 5	82)	0 - 1 - 2 - 5	152)	0 - 2 - 2 - 5
13)	1 - 1 - 3 - 6	83)	1 - 2 - 3 - 6	153)	1 - 0 - 3 - 6
14)	0 - 2 - 4 - 0	84)	0 - 0 - 4 - 0	154)	0 - 1 - 4 - 0
15)	1 - 0 - 0 - 1	85)	1 - 1 - 0 - 1	155)	1 - 2 - 0 - 1
16)	0 - 1 - 1 - 2	86)	0 - 2 - 1 - 2	156)	0 - 0 - 1 - 2
17)	1 - 2 - 2 - 3	87)	1 - 0 - 2 - 3	157)	1 - 1 - 2 - 3
18)	0 - 0 - 3 - 4	88)	0 - 1 - 3 - 4	158)	0 - 2 - 3 - 4
19)	1 - 1 - 4 - 5	89)	1 - 2 - 4 - 5	159)	1 - 0 - 4 - 5
20)	0 - 2 - 0 - 6	90)	0 - 0 - 0 - 6	160)	0 - 1 - 0 - 6
21)	1 - 0 - 1 - 0	91)	1 - 1 - 1 - 0	161)	1 - 2 - 1 - 0
22)	0 - 1 - 2 - 1	92)	0 - 2 - 2 - 1	162)	0 - 0 - 2 - 1
23)	1 - 2 - 3 - 2	93)	1 - 0 - 3 - 2	163)	1 - 1 - 3 - 2
24)	0 - 0 - 4 - 3	94)	0 - 1 - 4 - 3	164)	0 - 2 - 4 - 3
25)	1 - 1 - 0 - 4	95)	1 - 2 - 0 - 4	165)	1 - 0 - 0 - 4
26)	0 - 2 - 1 - 5	96)	0 - 0 - 1 - 5	166)	0 - 1 - 1 - 5
27)	1 - 0 - 2 - 6	97)	1 - 1 - 2 - 6	167)	1 - 2 - 2 - 6
28)	0 - 1 - 3 - 0	98)	0 - 2 - 3 - 0	168)	0 - 0 - 3 - 0
29)	1 - 2 - 4 - 1	99)	1 - 0 - 4 - 1	169)	1 - 1 - 4 - 1
30)	0 - 0 - 0 - 2	100)	0 - 1 - 0 - 2	170)	0 - 2 - 0 - 2
31)	1 - 1 - 1 - 3	101)	1 - 2 - 1 - 3	171)	1 - 0 - 1 - 3
32)	0 - 2 - 2 - 4	102)	0 - 0 - 2 - 4	172)	0 - 1 - 2 - 4
33)	1 - 0 - 3 - 5	103)	1 - 1 - 3 - 5	173)	1 - 2 - 3 - 5
34)	0 - 1 - 4 - 6	104)	0 - 2 - 4 – 6	174)	0 - 0 - 4 - 6
35)	1 - 2 - 0 - 0	105)	1 - 0 - 0 - 0	175)	1 - 1 - 0 - 0
36)	0 - 0 - 1 - 1	106)	0 - 1 - 1 - 1	176)	0 - 2 - 1 - 1
37)	1 - 1 - 2 - 2	107)	1 - 2 - 2 - 2	177)	1 - 0 - 2 - 2
38)	0 - 2 - 3 - 3	108)	0 - 0 - 3 - 3	178)	0 - 1 - 3 - 3
39)	1 - 0 - 4 - 4	109)	1 - 1 - 4 - 4	179)	1 - 2 - 4 - 4
40)	0 - 1 - 0 - 5	110)	0 - 2 - 0 - 5	180)	0 - 0 - 0 - 5
41)	1 - 2 - 1 - 6	111)	1 - 0 - 1 - 6	181)	1 - 1 - 1 - 6
42)	0 - 0 - 2 - 0	112)	0 - 1 - 2 - 0	182)	0 - 2 - 2 - 0
43)	1 - 1 - 3 - 1	113)	1 - 2 - 3 - 1	183)	1 - 0 - 3 - 1
44)	0 - 2 - 4 - 2	114)	0 - 0 - 4 - 2	184)	0 - 1 - 4 - 2
45)	1 - 0 - 0 - 3	115)	1 - 1 - 0 - 3	185)	1 - 2 - 0 - 3
46)	0 - 1 - 1 - 4	116)	0 - 2 - 1 - 4	186)	0 - 0 - 1 - 4
47)	1 - 2 - 2 - 5	117)	1 - 0 - 2 - 5	187)	1 - 1 - 2 - 5
48)	0 - 0 - 3 - 6	118)	0 - 1 - 3 - 6	188)	0 - 2 - 3 - 6
49)	1 - 1 - 4 - 0	119)	1 - 2 - 4 - 0	189)	1 - 0 - 4 - 0
50)	0 - 2 - 0 - 1	120)	0 - 0 - 0 - 1	190)	0 - 1 - 0 - 1
51)	1 - 0 - 1 - 2	121)	1 - 1 - 1 - 2	191)	1 - 2 - 1 - 2
52)	0 - 1 - 2 - 3	122)	0 - 2 - 2 - 3	192)	0 - 0 - 2 - 3
53)	1 - 2 - 3 - 4	123)	1 - 0 - 3 - 4	193)	1 - 1 - 3 - 4
54)	0 - 0 - 4 - 5	124)	0 - 1 - 4 - 5	194)	0 - 2 - 4 - 5
55)	1 - 1 - 0 - 6	125)	1 - 2 - 0 - 6	195)	1 - 0 - 0 - 6
56)	0 - 2 - 1 - 0	126)	0 - 0 - 1 - 0	196)	0 - 1 - 1 - 0
57)	1 - 0 - 2 - 1	127)	1 - 1 - 2 - 1	197)	1 - 2 - 2 - 1
58)	0 - 1 - 3 - 2	128)	0 - 2 - 3 - 2	198)	0 - 0 - 3 - 2
59)	1 - 2 - 4 - 3	129)	1 - 0 - 4 - 3	199)	1 - 1 - 4 - 3
60)	0 - 0 - 0 - 4	130)	0 - 1 - 0 - 4	200)	0 - 2 - 0 - 4
61)	1 - 1 - 1 - 5	131)	1 - 2 - 1 - 5	201)	1 - 0 - 1 - 5
62)	0 - 2 - 2 - 6	132)	0 - 0 - 2 - 6	202)	0 - 1 - 2 - 6
63)	1 - 0 - 3 - 0	133)	1 - 1 - 3 - 0	203)	1 - 2 - 3 - 0
64)	0 - 1 - 4 - 1	134)	0 - 2 - 4 - 1	204)	0 - 0 - 4 - 1
65)	1 - 2 - 0 - 2	135)	1 - 0 - 0 - 2	205)	1 - 1 - 0 - 2
66)	0 - 0 - 1 - 3	136)	0 - 1 - 1 - 3	206)	0 - 2 - 1 - 3
67)	1 - 1 - 2 - 4	137)	1 - 2 - 2 - 4	207)	1 - 0 - 2 - 4
68)	0 - 2 - 3 - 5	138)	0 - 0 - 3 - 5	208)	0 - 1 - 3 - 5
69)	1 - 0 - 4 - 6	139)	1 - 1 - 4 - 6	209)	1 - 2 - 4 - 6
70)	0 - 1 - 0 - 0	140)	0 - 2 - 0 - 0	210)	0 - 0 - 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)