

Matematica Open Source

$$\frac{d}{dx} f(x) \sum_{k=0}^{+\infty} a_k \int f(x) dx \oint_{\Gamma} (X dx + Y dy + Z dz)$$

Un approccio computazionale alla Congettura di Riemann

Marcello Colozzo

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$



Indice

1	Teoria analitica	2
1.1	La legge di distribuzione dei numeri primi. La funzione a gradini $\pi(x)$	2
1.2	Il Teorema dei Numeri Primi. L'approssimazione di Riemann	6
1.3	La funzione logaritmo integrale	10
1.4	La funzione esponenziale integrale	11
1.5	Crittografia a chiave pubblica	17
1.6	La funzione di distribuzione degli zeri della zeta di Riemann	17
1.7	L'analisi di Riesel e Göhl	18
2	Analisi computazionale	33
2.1	Analisi globale	33
2.2	Analisi locale	49
A	La formula di inversione di Möbius e la formula di Riemann – Von Mangoldt	56
A.1	La funzione di Möbius	56
A.2	La formula di Riemann – Von Mangoldt	56

Capitolo 1

Teoria analitica

1.1 La legge di distribuzione dei numeri primi. La funzione a gradini $\pi(x)$

Come è noto, i numeri primi sono elementi di \mathbb{N} che ammettono solo divisori banali. Cioè, $p \in \mathbb{N}$ è numero primo se e solo se p è divisibile per se stesso e per 1. I numeri primi compongono una successione di elementi di \mathbb{N} :

$$\{p_n\}_{n \in \mathbb{N} - \{0\}}, \quad (1.1)$$

dove p_n l' n -esimo numero primo. Ad esempio, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_6 = 7$, $p_7 = 11$, ... La (1.1) è un'applicazione iniettiva:

$$\begin{aligned} g : \mathbb{N} - \{0\} &\rightarrow \mathbb{N} \\ g : n &\rightarrow p_n, \quad \forall n \in \mathbb{N} - \{0\}, \end{aligned} \quad (1.2)$$

il cui grafico è riportato in fig. 1.1.

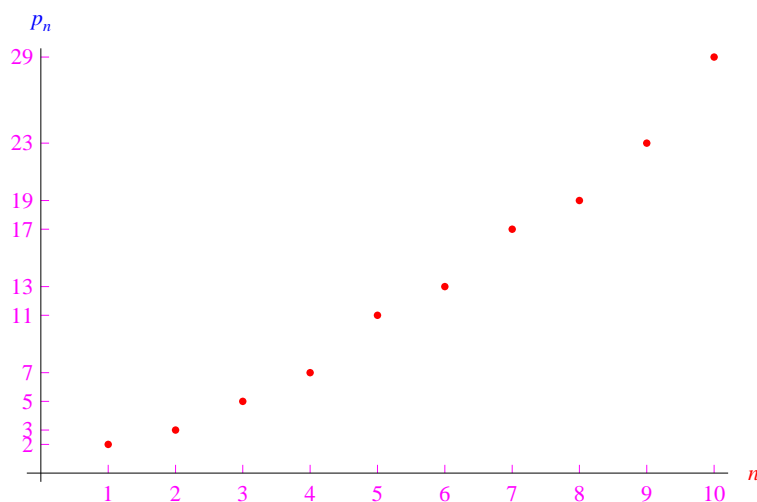


Figura 1.1: Grafico dell'applicazione iniettiva definita dalla (1.2).

Allo stato attuale delle conoscenze, l'espressione analitica (se esiste) della funzione (1.2) è ignota. Dall'iniettività segue l'invertibilità di g :

$$\begin{aligned} g^{-1} : g(\mathbb{N} - \{0\}) &\rightarrow \mathbb{N} - \{0\} \\ g^{-1} : p &\rightarrow n, \quad \forall p \in \mathbb{N} - \{0\}, \end{aligned} \tag{1.3}$$

dove $g(\mathbb{N} - \{0\})$ è l'immagine di $\mathbb{N} - \{0\}$ attraverso g . Ad esempio: $g(3) = 5 \implies g^{-1}(5) = 3$. Pertanto per un assegnato numero primo p , $g^{-1}(p)$ è il numero di primi tra 1 e p , per cui la funzione g^{-1} definisce la *legge di distribuzione dei numeri primi*. È istintivo prolungare g^{-1} da $g(\mathbb{N} - \{0\})$ a tutto \mathbb{N} . Ridifinendo:

$$\begin{aligned} g^{-1} : \mathbb{N} &\rightarrow \mathbb{N} \\ g^{-1} : n &\rightarrow g(n), \quad \forall n \in \mathbb{N}, \end{aligned} \tag{1.4}$$

onde $g^{-1}(n)$ è il numero di primi tra 0 e n . La fig. 1.2 illustra il grafico dell'applicazione inversa (1.4).

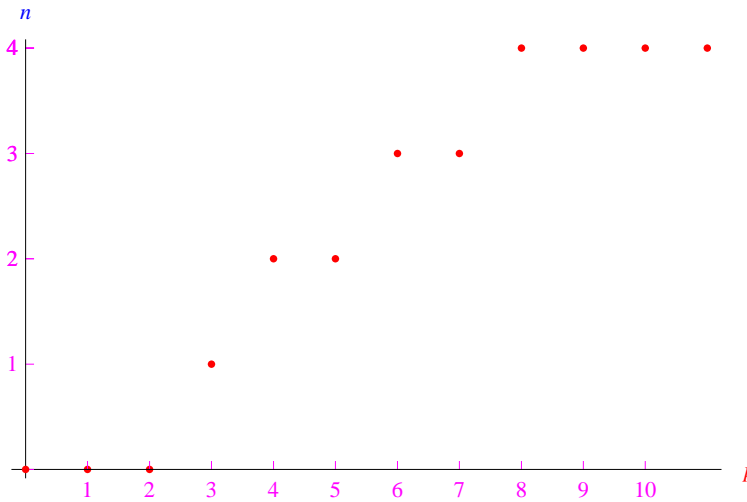


Figura 1.2: Andamento di $g^{-1}(p) = n$.

Per quanto precede, il problema consiste nel trovare l'espressione analitica dell'applicazione (1.4). Per poter attaccare tale problema con i metodi dell'Analisi matematica, è necessario prolungare tale applicazione da \mathbb{N} a $[0, +\infty)$, onde definiamo:

$$\begin{aligned} \pi : [0, +\infty) &\rightarrow \mathbb{R} \\ \pi : x &\rightarrow \pi(x), \quad \forall x \in [0, +\infty) \end{aligned} \tag{1.5}$$

La funzione (1.5) è una funzione reale della variabile reale x tale che $\pi(x)$ è il numero di primi tra 0 e $[x]$, dove il simbolo $[.]$ denota la parte intera di un numero reale. La funzione $\pi(x)$ è non negativa ed è continua a tratti, giacchè ha una **discontinuità di prima specie** in tutti e soli i punti le cui ascisse sono numeri primi. Invero, denotando con \mathcal{D} l'insieme dei punti di discontinuità di $\pi(x)$, si ha:

$$x \in \mathcal{D} \iff x = p$$

In altri termini, l'insieme delle discontinuità di $\pi(x)$ è il codominio dell'applicazione (1.2). In fig. 1.3 riportiamo il grafico della restrizione di $\pi(x)$ all'intervallo $X = [0, 6]$, da cui vediamo che:

$$\lim_{x \rightarrow 2^-} \pi(x) = 0, \quad \lim_{x \rightarrow 2^+} \pi(x) = 1 \implies s(2) = +1,$$

dove s denota il salto di discontinuità della funzione. Nei rimanenti punti di discontinuità (in X):

$$\lim_{x \rightarrow 3^-} \pi(x) = 1, \quad \lim_{x \rightarrow 3^+} \pi(x) = 2 \implies s(3) = +1$$

$$\lim_{x \rightarrow 5^-} \pi(x) = 1, \quad \lim_{x \rightarrow 5^+} \pi(x) = 2 \implies s(5) = +1$$

Per ogni numero primo p_n :

$$\lim_{x \rightarrow p_n^-} \pi(x) = n - 1, \quad \lim_{x \rightarrow p_n^+} \pi(x) = n \implies s(p_n) = +1$$

Per $X = [0, 20]$, otteniamo il grafico di fig. 1.4.

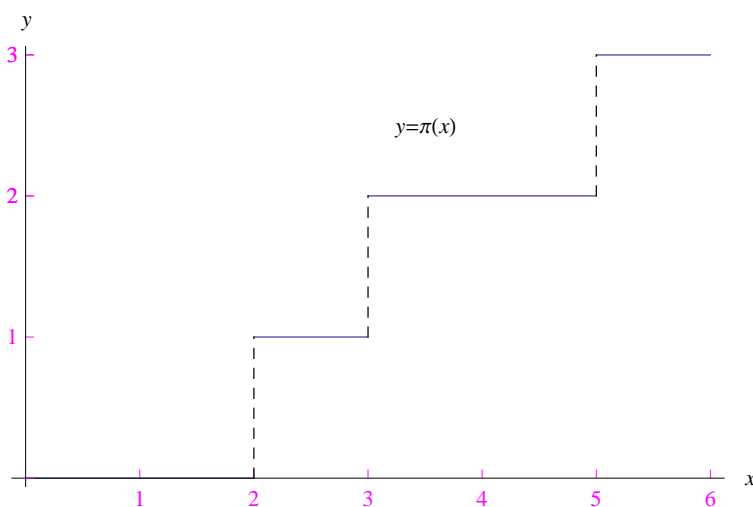


Figura 1.3: Grafico della funzione $\pi(x)$ per $x \in [0, 6]$.

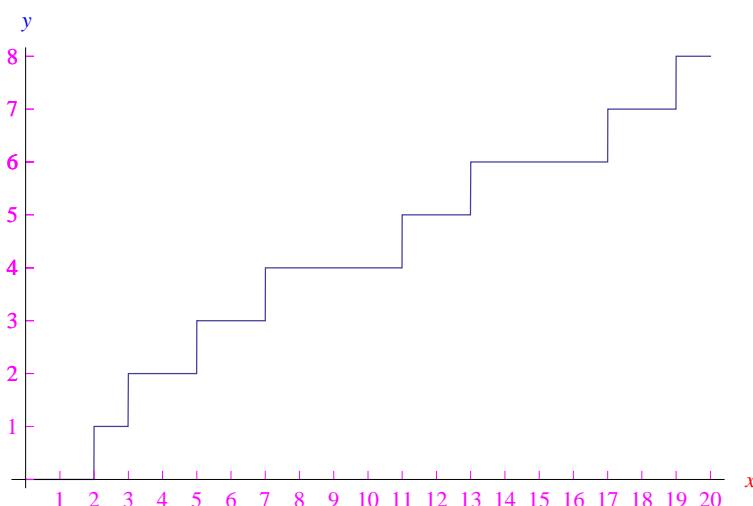


Figura 1.4: Grafico della funzione $\pi(x)$ per $x \in [0, 20]$.

Per $X = [0, 200]$, otteniamo il grafico di fig. 1.5. Al crescere indefinito di x , le discontinuità sono meno evidenti, per cui è possibile tentare un'approssimazione "globale" di $\pi(x)$ con una funzione continua in $[0, +\infty)$. Tale approccio è giustificato dal grafico fig. 1.6

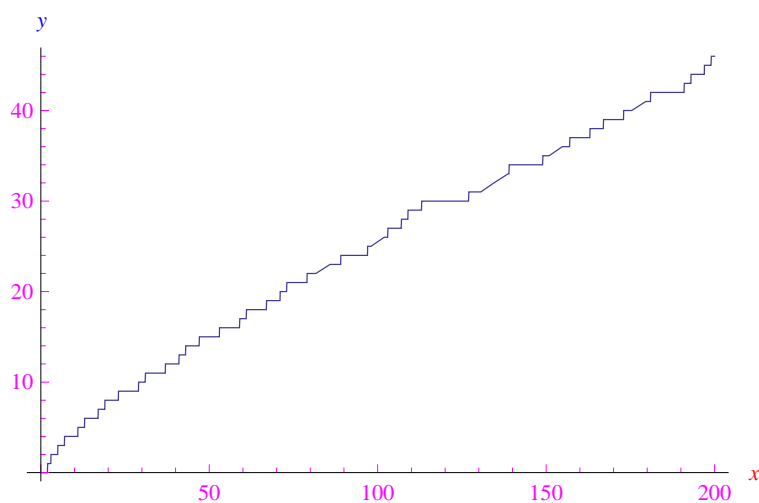


Figura 1.5: Grafico della funzione $\pi(x)$ per $x \in [0, 20]$.

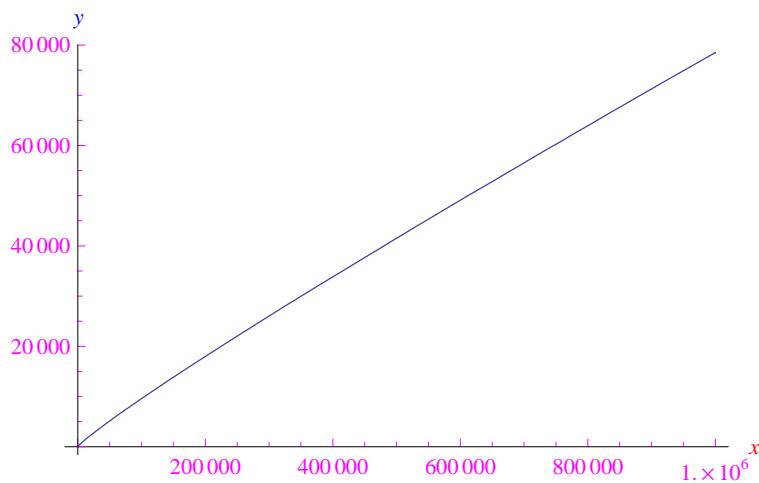


Figura 1.6: Grafico della funzione $\pi(x)$ per $x \in [0, 10^6]$. Si noti la leggera curvatura del grafico per $x < 200000$, che esprime la non linearità della funzione. Si dimostra che nel limite dei grandi x , il grafico è concavo verso il basso. Ciò si traduce in una diminuzione della densità dei numeri primi.

1.2 Il Teorema dei Numeri Primi. L'approssimazione di Riemann

Riguardo al comportamento asintotico di $\pi(x)$, sussiste il seguente teorema:

Teorema 1 (*Teorema dei Numeri Primi (PNT)*)

Per $x \rightarrow +\infty$, $\pi(x)$ e $u(x) = \frac{x}{\ln x}$ sono *infiniti equivalenti*. Cioè:

$$\lim_{x \rightarrow +\infty} \frac{\pi(x)}{u(x)} = 1$$

Per la dimostrazione rimandiamo a [1].

La fig. 1.7 confronta il grafico di $\pi(x)$ con quello di $u(x)$.

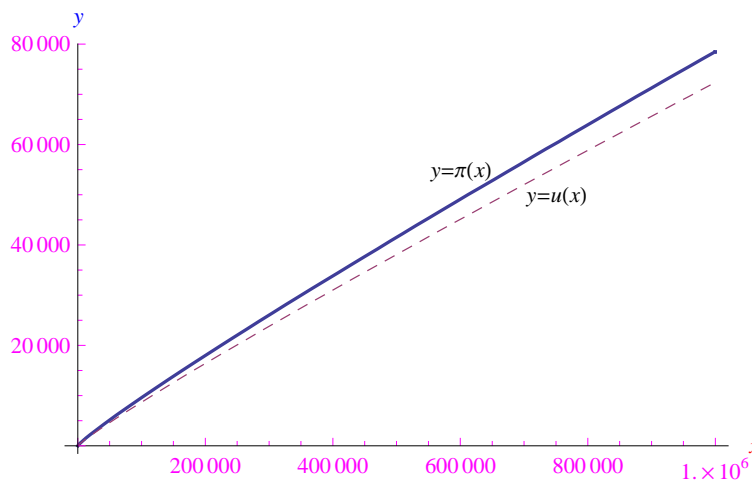


Figura 1.7: La curva in grassetto è il grafico di $\pi(x)$, mentre quella tratteggiata è il grafico di $u(x) = \frac{x}{\ln x}$.

In forza del comportamento “complicato” della funzione $\pi(x)$, ci aspettiamo che quest’ultima non sia elementarmente esprimibile. Incidentalmente, una funzione che approssima $\pi(x)$ fu scoperta da Riemann e si esprime attraverso la funzione logaritmo integrale:

$$R(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} li(x^{1/k}), \quad (1.6)$$

dove $\mu(k)$ è la *funzione di Möbius*:

$$\mu(k) = \begin{cases} (-1)^r, & \text{se } k = \prod_{i=1}^r p_i, \quad \text{con } p_i \neq p_j, \quad \forall i \neq j \\ 0, & \text{altrimenti} \end{cases}, \quad (1.7)$$

mentre $li(x)$ è la funzione logaritmo integrale¹:

$$li(x) = \int_0^x \frac{dt}{\ln t}, \quad \forall x \in [0, 1) \quad (1.8)$$

¹La funzione logaritmo integrale è in realtà estesa anche all’intervallo $(1, +\infty)$ prendendo la parte principale di Cauchy, come esposto nel paragrafo successivo.

Osserviamo che la funzione integranda ha una discontinuità rimovibile in $x = 0$, da cui la sua sommabilità in $[0, 1)$. Inoltre:

$$\int_0^1 \frac{dt}{\ln t} = -\infty,$$

per cui:

$$\lim_{x \rightarrow 1^-} li(x) = -\infty$$

Il grafico di $li(x)$ è riportato in fig. 1.8.

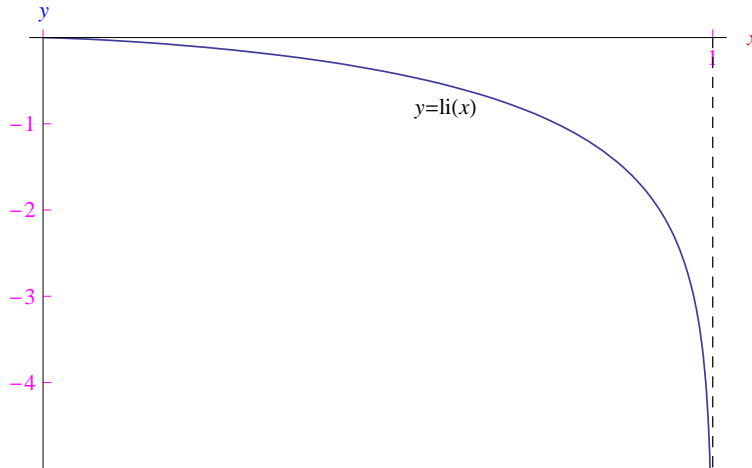


Figura 1.8: Diagramma cartesiano della funzione logaritmo integrale in cui è visibile l'asintoto verticale $x - 1 = 0$.

Dall'espressione (1.6) vediamo che la $R(x)$ è maledettamente complicata, in quanto nella sommatoria compaiono i seguenti termini:

$$li(x^{1/k}) = \int_0^{x^{1/k}} \frac{dt}{\ln t}, \quad \forall x \in [0, 1),$$

alcuni dei quali sono graficati in fig. 1.9.

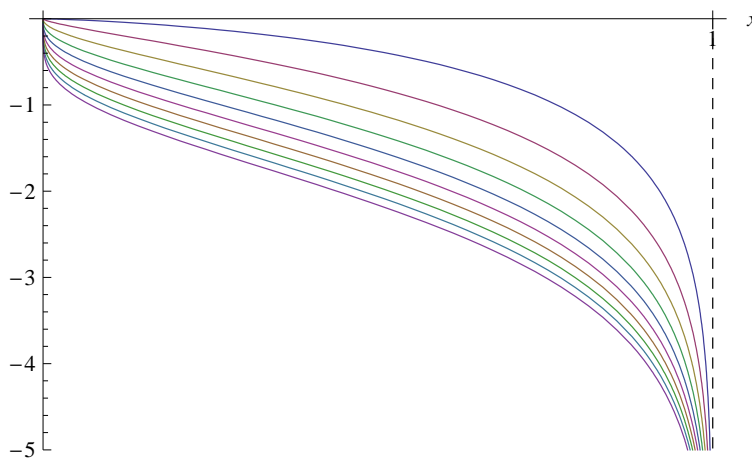


Figura 1.9: Diagramma cartesiano delle funzioni $li(x^{1/k})$ per $k = 1, \dots, 10$.

Nel suo libro [2], Ilan Vardi propone una routine in ambiente *Mathematica* per calcolare/plottare la funzione $R(x)$ a partire da una espressione equivalente nota come *serie di Gram* [8] alla (1.6) che si svincola dalla funzione di Möbius:

$$R(x) = 1 + \sum_{k=1}^{+\infty} \frac{(\ln x)^k}{k!k\zeta(k+1)}, \tag{1.9}$$

dove ζ è la funzione zeta di Riemann che è Built-in in *Mathematica* ed è invocata dal comando `Zeta[]`. Per calcolare/plottare la funzione $R(x)$, dobbiamo approssimare la serie nel secondo termine al secondo membro della (1.9) alla sua somma parziale di ordine N :

$$R_N(x) = 1 + \sum_{k=1}^N \frac{(\ln x)^k}{k!k\zeta(k+1)}, \tag{1.10}$$

risultando:

$$R(x) = \lim_{N \rightarrow +\infty} R_N(x)$$

Per avere 15 cifre di precisione di $x < 10^{12}$, è sufficiente porre $N = 100$ [2]. Osserviamo, tuttavia, che nelle ultime versioni di *Mathematica* che girano sui personal computer attuali, la differenza di *timing* tra la routine di [2] – che utilizza la straordinaria efficienza di *Mathematica* nel trattare le liste – e l’istruzione `Sum` per il calcolo della sommatoria a secondo membro della (1.10), è minima.

In fig. 1.10 confrontiamo l’andamento di $\pi(x)$ con quello di $R(x)$ per $N = 100$ e nell’intervallo $X = [0, 100]$. In fig. 1.11 ripetiamo gli andamenti di $\pi(x)$ e $R_{100}(x)$ in $X = [0, 1000]$.

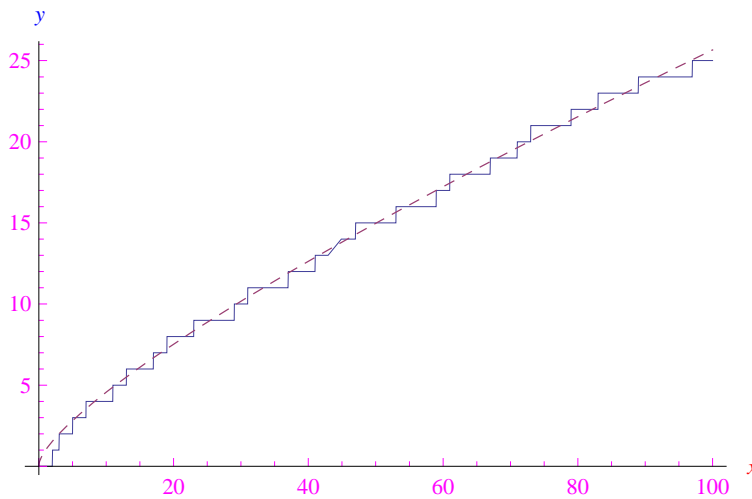


Figura 1.10: L’approssimazione di Riemann per $N = 100$ della funzione $\pi(x)$ nell’intervallo $[0, 100]$.

In fig. 1.12 riportiamo l’andamento della derivata seconda di $R_{100}(x)$, dal cui segno vediamo che il grafico di $R(x)$ volge la concavità verso il basso, come anticipato precedentemente.

Chiudiamo questo paragrafo (e questa Parte 1) riassumendo i risultati raggiunti. Siamo partiti dalla successione $\{p_n\}_{n \in \mathbb{N} - \{0\}}$ che può essere riprodotta (fino a un assegnato $n \gg$

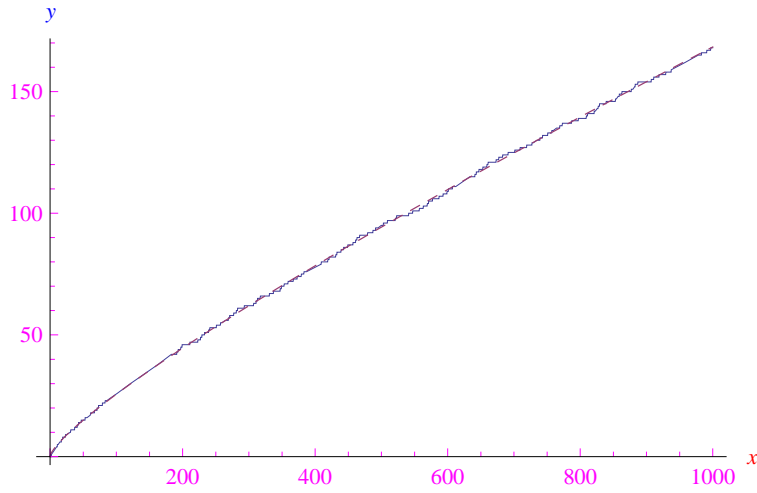


Figura 1.11: L'approssimazione di Riemann per $N = 100$ della funzione $\pi(x)$ nell'intervallo $[0, 1000]$.

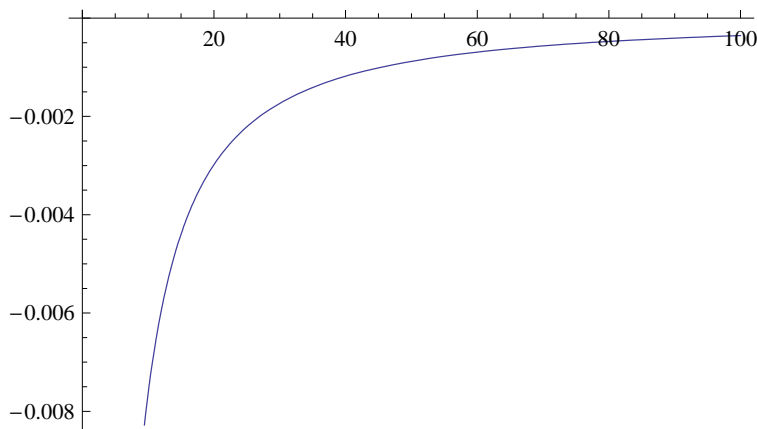


Figura 1.12: Andamento del grafico della funzione $\frac{d^2}{dx^2} R_{100}(x)$ in $[0, 100]$.

1) da un qualunque ambiente di calcolo numerico. Per poter affrontare il problema della determinazione della legge con cui si distribuiscono i termini p_n della successione, abbiamo dapprima considerato l'inversa di tale funzione, per poi considerarne l'estensione al campo reale, ottenendo la funzione a gradini $\pi(x)$. Grazie alla formula approssimata di Riemann, siamo giunti a una buona approssimazione non-locale di $\pi(x)$. Notiamo incidentalmente due aspetti particolari della formula approssimata:

1. $R(x)$ non è elementarmente esprimibile, in quanto espressa attraverso la somma di una serie (cfr. eq. 1.9).
2. Nell'espressione equivalente di $R(x)$ (cfr. eq. 1.10) notiamo la presenza della funzione zeta di Riemann che svolge un ruolo cruciale nella legge di distribuzione dei numeri primi.

1.3 La funzione logaritmo integrale

Il *logaritmo integrale* è la seguente funzione integrale:

$$\begin{aligned}
 li(x) &= \int_0^x \frac{dt}{\ln t}, & \text{se } 0 \leq x < 1 \\
 li(x) &=^* \int_0^x \frac{dt}{\ln t}, & \text{se } x > 1,
 \end{aligned}
 \tag{1.11}$$

dove l'asterisco denota la parte principale di Cauchy:

$${}^* \int_0^{x>1} \frac{dt}{\ln t} = \lim_{\varepsilon \rightarrow 0^+} \left(\int_0^{1-\varepsilon} \frac{dt}{\ln t} + \int_{1+\varepsilon}^x \frac{dt}{\ln t} \right)
 \tag{1.12}$$

Risulta

$$\lim_{x \rightarrow 1} li(x) = -\infty
 \tag{1.13}$$

In fig. 1.13 riportiamo il grafico della restrizione di $li(x)$ all'intervallo $[0, 4]$.

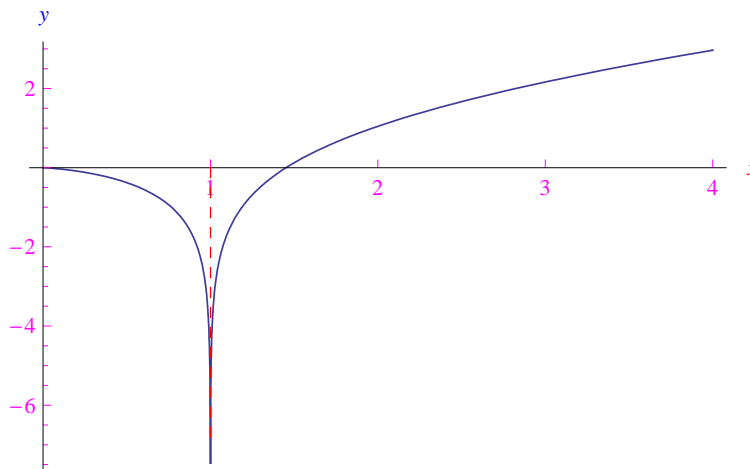


Figura 1.13: Andamento della funzione logaritmo-integrale. Si noti l'asintoto verticale $x = 1$.

La funzione logaritmo integrale è utilizzata nello studio della **distribuzione dei numeri primi**. Ad esempio, consideriamo la funzione

$$g(x) = \int_2^x \frac{dt}{\ln t}, \quad \forall x \in (2, +\infty)$$

Risulta

$$g(x) = li(x) - li(2),$$

graficata in fig. 1.14 dove ne confrontiamo l'andamento con la distribuzione dei primi $\pi(x)$.

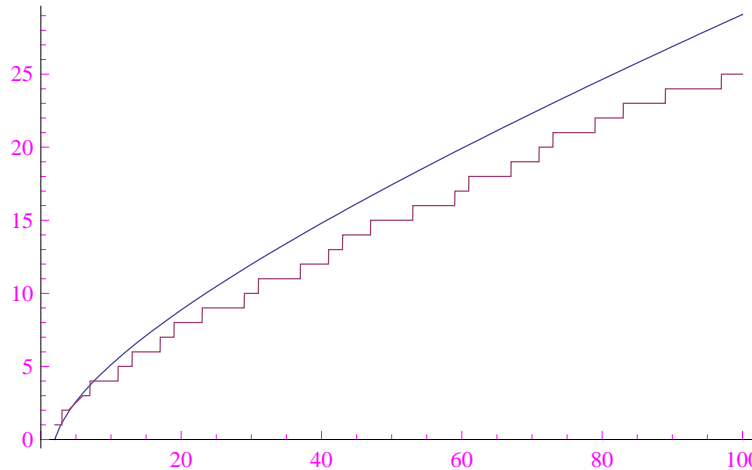


Figura 1.14: Andamento della funzione logaritmo-integrale. Si noti l'asintoto verticale $x = 1$.

Nel campo complesso il logaritmo integrale è dato da

$$li(z) = \int_0^z \frac{dt}{\ln t} \tag{1.14}$$

In fig. riportiamo un `ContourPlot` eseguito con Mathematica.

1.4 La funzione esponenziale integrale

Nel numero precedente abbiamo esaminato la funzione logaritmo integrale che risulta essere una buona approssimazione della funzione $\pi(x)$ di distribuzione dei numeri primi:

$$\pi(x) \sim \int_2^x \frac{dt}{\ln t}, \quad \forall x \in [2, +\infty) \tag{1.15}$$

L'estremo inferiore è fissato a 2, poiché $\pi(x < 2) = 0$. La relazione approssimata (1.15) suggerisce di interpretare l'integrando

$$\frac{1}{\ln x}, \quad \forall x \in [2, +\infty)$$

quale densità (approssimata) dei numeri primi. Infatti, supponendo che $\pi(x)$ sia *esattamente* esprimibile attraverso un integrale

$$\pi(x) = \int_2^x g(t) dt, \quad \forall x \in [2, +\infty),$$

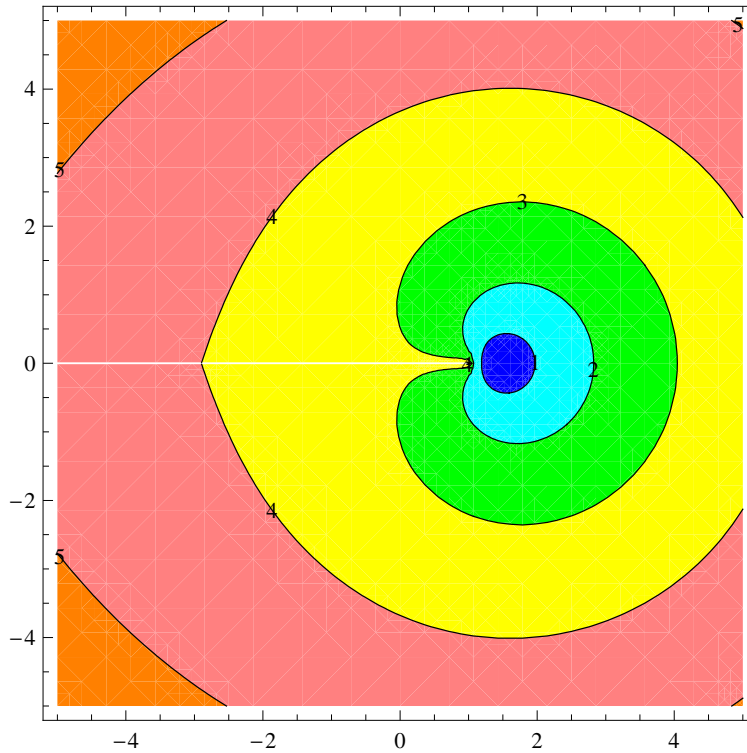


Figura 1.15: Curve di livello della funzione logaritmo integrale.

si ha che per un assegnato $x_0 \in [2, +\infty)$ l'espressione differenziale $g(x_0) dx = d\pi$ è il numero di primi nell'intervallo infinitesimo $[x_0, x_0 + dx]$, onde la funzione

$$g(x) = \frac{d}{dx} \pi(x), \quad \forall x \in [2, +\infty), \quad (1.16)$$

è la densità dei numeri primi.

Osservazione 2 Tali argomentazioni hanno un significato puramente formale giacché i numeri primi non si distribuiscono con continuità, per cui non ha senso una locazione del tipo “numero di primi nell'intervallo infinitesimo $[x_0, x_0 + dx]$ ”.

Un'altra funzione integrale che interviene nell'espressione della funzione di distribuzione dei numeri primi è l'*esponenziale integrale*:

$$\text{Ei}(x) = - \int_{-x}^{+\infty} \frac{e^{-t}}{t} dt, \quad (x < 0), \quad (1.17)$$

Convien eseguire il cambio di variabile

$$\tau = -t \implies dt = -d\tau \quad (1.18)$$

Determiniamo i nuovi estremi di integrazione

$$-x \leq t = -\tau < +\infty \implies x \geq \tau > -\infty \quad (1.19)$$

Cioè

$$\text{Ei}(x) = + \int_x^{-\infty} \frac{e^\tau}{-\tau} d\tau = + \int_{-\infty}^x \frac{e^\tau}{\tau} d\tau, \quad (x < 0)$$

Ridifinando la variabile muta τ in t :

$$\text{Ei}(x) = \int_{-\infty}^x \frac{e^t}{t} dt, \quad (x < 0), \quad (1.20)$$

che è manifestamente convergente. La funzione integranda

$$\varphi(x) \stackrel{\text{def}}{=} \frac{e^x}{x}, \quad (1.21)$$

ha in $x = 0$ una **discontinuità di seconda specie**. Precisamente è infinita:

$$\lim_{x \rightarrow 0^+} \varphi(x) = +\infty, \quad \lim_{x \rightarrow 0^-} \varphi(x) = -\infty \quad (1.22)$$

risultando del prim'ordine rispetto all'**infinito di riferimento** $1/|x|$. Inoltre, comunque prendiamo $a > 0$ la funzione integranda è negativa in $[-a, 0)$ e positiva in $(0, a]$, onde

$$\int_{-a}^0 \frac{e^t}{t} dt = -\infty, \quad \int_0^a \frac{e^t}{t} dt = +\infty,$$

da cui la non integrabilità in ogni intervallo $[-a, a]$:

$$\int_{-a}^a \frac{e^t}{t} dt = \int_{-a}^0 \frac{e^t}{t} dt + \int_0^a \frac{e^t}{t} dt = \infty - \infty$$

In fig. 1.16 sono riportati i rettangoloidi generalizzati nei rispettivi intervalli di integrazione. Risulta comunque convergente la parte principale di Cauchy:

$$* \int_{-a}^a \frac{e^t}{t} dt = \lim_{\varepsilon \rightarrow 0^+} \left(\int_{-a}^{-\varepsilon} \frac{e^t}{t} dt + \int_{\varepsilon}^a \frac{e^t}{t} dt \right)$$

Tale circostanza suggerisce di estendere $\text{Ei}(x)$ a $x > 0$

$$\text{Ei}(x) = * \int_{-\infty}^x \frac{e^t}{t} dt, \quad (x > 0), \quad (1.23)$$

avendosi

$$\lim_{x \rightarrow 0} \text{Ei}(x) = -\infty \quad (1.24)$$

Il comportamento all'infinito è

$$\lim_{x \rightarrow +\infty} \text{Ei}(x) = -\infty, \quad \lim_{x \rightarrow -\infty} \text{Ei}(x) = 0, \quad (1.25)$$

cosicché l'asse x è asintoto orizzontale a sinistra. Per $x \rightarrow +\infty$ il diagramma è privo di asintoti (cfr. fig. 1.17).

Per estendere l'esponenziale integrale al campo complesso, è preferibile rammentare la nozione di integrale complesso. A tale scopo consideriamo una funzione $f(z)$ della variabile complessa $z = x + iy$, che assumiamo continua in un campo connesso A del piano xy [3]. Se $z_0, z_1 \in A$, denotiamo con $\gamma(z_0, z_1)$ un assegnato arco di curva generalmente regolare di estremi z_0 e z_1 .

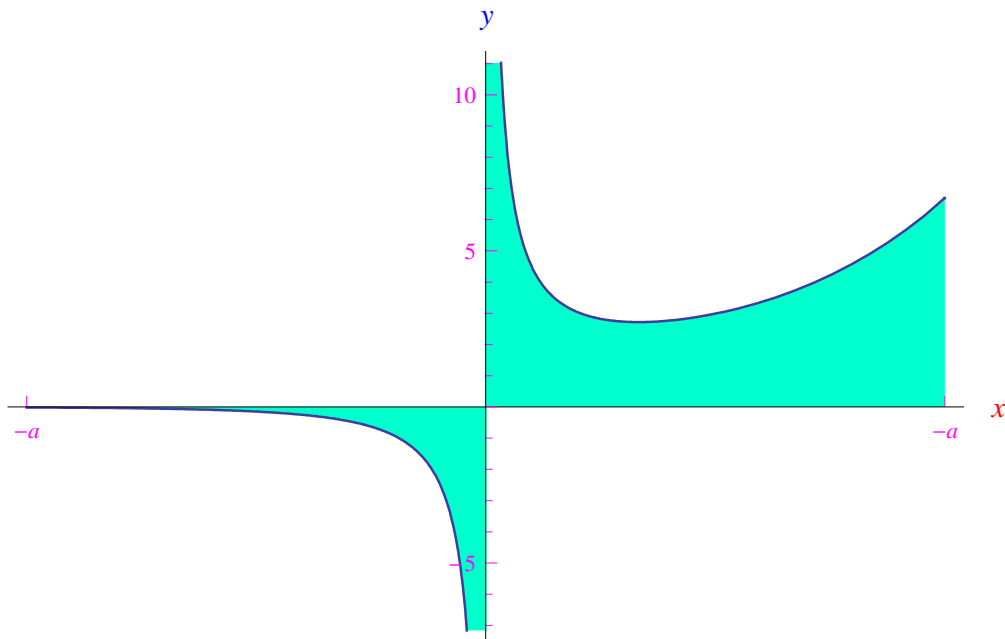


Figura 1.16: La funzione $\varphi(x) = \frac{e^x}{x}$ non è integrabile in $[-a, a]$.

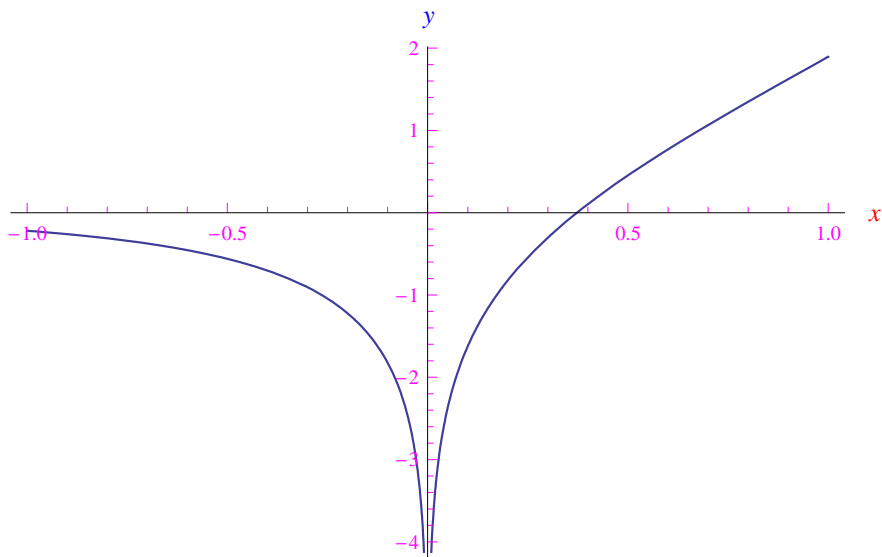


Figura 1.17: Grafico di $Ei(x)$.

Definizione 3 Si dice **integrale complesso** della $f(z)$ esteso a γ nel verso da z_0 a z_1 , l'**integrale curvilineo** della forma differenziale lineare

$$f(x, y) dx + i f(x, y) dy$$

esteso all'arco γ da $P_0(x_0, y_0)$ a $P_1(x_1, y_1)$, essendo $z_0 = x_0 + iy_0$, $z_1 = x_1 + iy_1$. In simboli:

$$\int_{\gamma(z_0, z_1)} f(z) dz \stackrel{\text{def}}{=} \int_{\gamma(P_0, P_1)} f(x, y) (dx + idy) \quad (1.26)$$

Se γ ha la seguente **rappresentazione parametrica regolare**

$$x = x(t), \quad y = y(t), \quad t \in [a, b],$$

segue dalla definizione di integrale curvilineo di una forma differenziale lineare:

$$\int_{\gamma(z_0, z_1)} f(z) dz = \int_a^b f[x(t), y(t)] [x'(t) + iy'(t)] dt \quad (1.27)$$

Ciò premesso, riprendiamo l'espressione dell'esponenziale integrale scrivendo:

$$\text{Ei}(x) = \int_{-\infty}^x \frac{e^\xi}{\xi} d\xi, \quad x \in \mathbb{R} - \{0\},$$

dove è sottointesa la parte principale di Cauchy. Dal momento che un integrale definito (e generalizzato) è il caso particolare di un integrale curvilineo esteso a un segmento appartenente all'asse x , possiamo scrivere:

$$\text{Ei}(x) = \int_{\gamma(P_\infty, P)} X(\xi) d\xi \quad (1.28)$$

Cioè $\text{Ei}(x)$ è l'integrale curvilineo della forma differenziale lineare $X(\xi) d\xi$ con

$$X(\xi) = \frac{e^\xi}{\xi} \quad (1.29)$$

esteso al segmento dell'asse x di rappresentazione parametrica

$$\xi = t, \quad \eta = 0, \quad t \in (-\infty, x], \quad (1.30)$$

onde

$$\int_{\gamma(P_\infty, P)} X(\xi) d\xi = \int_{-\infty}^x \frac{e^t}{t} dt, \quad (1.31)$$

come deve essere, in virtù della definizione di integrale curvilineo. Questa caratterizzazione formale della $\text{Ei}(x)$ suggerisce la seguente estensione al campo complesso:

$$\text{Ei}(z) = \int_{\gamma(z_\infty, z)} \frac{e^w}{w} dw, \quad (1.32)$$

dove $z = x + iy$, $w = \xi + i\eta$, mentre il cammino di integrazione γ ha la seguente rappresentazione parametrica

$$\xi = t, \quad \eta = v \neq 0, \quad t \in (-\infty, x], \quad (1.33)$$

come illustrato in fig. 1.18. In fig. 1.19 riportiamo un ContourPlot elaborato con **Mathematica**.

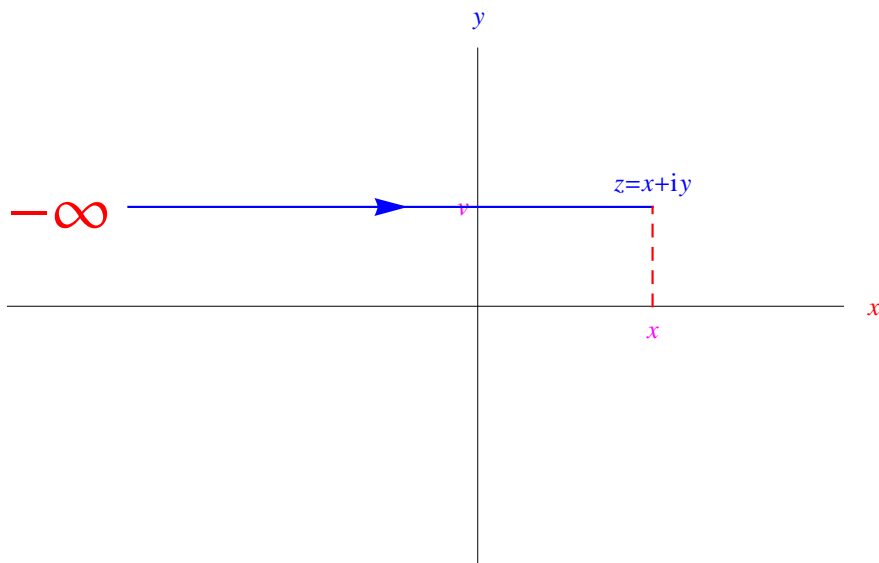


Figura 1.18: Cammino di integrazione per il calcolo di $Ei(z)$. La funzione è calcolata in $z = x + iy$.

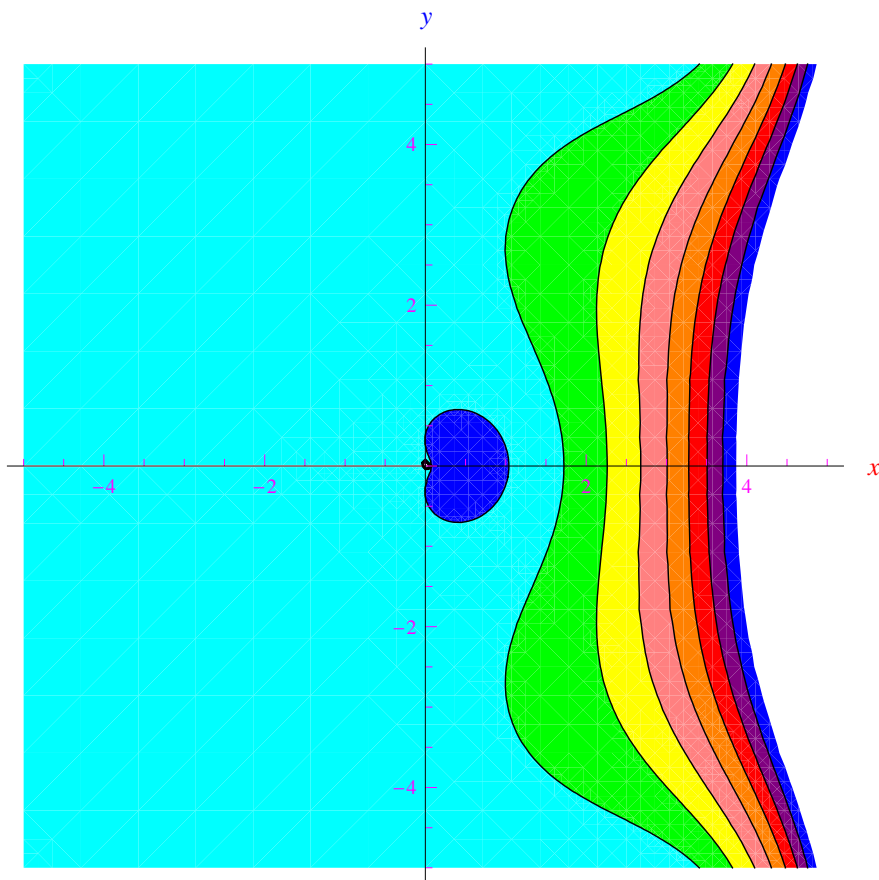


Figura 1.19: ContourPlot di $Ei(z)$.

1.5 Crittografia a chiave pubblica

Ipotesi: Bob e Alice sono due amanti che scambiano messaggi utilizzando il sistema crittografico a chiave pubblica RSA. A grandi linee, tale sistema di cifratura funziona nel seguente modo:

Alice genera un terna ordinata di interi (p, q, e) , dove p, q sono numeri primi > 100 , mentre $e < pq$ è un esponente. La coppia di primi è nota esclusivamente ad Alice, che però rende pubblico e ed $n = pq$. Tramite un canale pubblico (si pensi agli sms) Bob invia un messaggio m codificato come m^e modulo n . Per decodificare il messaggio, Alice deve eseguire l'operazione $(m^e)^d$ dove $d = 1/e$ modulo $(p-1)(q-1)$. Alice può eseguire agevolmente tale operazione poiché è l'unica ad avere accesso a d .

La robustezza dell'algoritmo RSA deriva dal fatto che essendo ignota la funzione di **distribuzione dei numeri primi**, riesce estremamente costoso dal punto di vista computazionale, fattorizzare numeri interi molto grandi. Viceversa, la conoscenza della predetta distribuzione renderebbe vulnerabile l'algoritmo.

Esiste un legame profondo tra la funzione di distribuzione dei primi e gli zeri non banali della **funzione zeta di Riemann**. Vediamo quale.

1.6 La funzione di distribuzione degli zeri della zeta di Riemann

Abbiamo visto nei numeri precedenti che una buona approssimazione della funzione di distribuzione dei numeri primi (f.d.p da qui in poi) è:

$$\int_2^x \frac{dt}{\ln t} \quad (1.34)$$

Questa è l'*approssimazione di Gauss*. Legendre trovò, invece, quest'altra relazione approssimata:

$$\pi(x) \sim \frac{x}{\ln x - 1.08366} \quad (1.35)$$

Nel 1859 Riemann trovò la seguente funzione approssimante

$$R(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} \text{li}(x^{1/k}) \quad (1.36)$$

i cui argomenti sono stati studiati nei numeri precedenti. Più precisamente

$$\pi_0(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} f(x^{1/k}), \quad (1.37)$$

Tale formula venne dimostrata nel 1895 da von Mangoldt [4] ed è nota come *formula di Riemann - von Mangoldt* (per un approfondimento, consultare l'Appendice A) La funzione f si scrive come:

$$f(x) = \begin{cases} f_c(x) + f_d(x), & \text{se } x \geq 2 \\ 0, & \text{se } x < 2 \end{cases}, \quad (1.38)$$

dove $f_c(x)$ riproduce la continuità della f.d.p., mentre $f_d(x)$ genera le discontinuità di prima specie. Tra l'altro, esaminando l'andamento della f.d.p. si capisce subito che una possibile f.d.p. non è elementarmente esprimibile (non esiste, cioè, alcuna funzione dotata di espressione elementare avente quel particolare diagramma cartesiano). Per inciso, l'andamento a gradini è generato via software, e un qualunque ambiente di calcolo utilizza vari certificati di primalità per tracciare il grafico. Ne consegue che per $x \gg 1$ l'elaborazione del grafico diviene progressivamente più lenta.

Esaminiamo ora le componenti della funzione f . Abbiamo:

$$f_c(x) = li(x) - \ln 2 + \int_x^{+\infty} \frac{dt}{t(t^2 - 1) \ln t} \tag{1.39}$$

L'espressione analitica della $f_d(x)$ è invece data da:

$$f_d(x) = - \sum_{\zeta(\rho)=0} Ei(\rho \ln x), \tag{1.40}$$

dove la sommatoria è estesa agli zeri non banali della funzione zeta di Riemann:

$$\rho = \frac{1}{2} + i\alpha,$$

mentre Ei è la funzione **esponenziale integrale** estesa al campo complesso. In definitiva, abbiamo la *formula di Riemann-von Mangoldt*:

$$\pi_0(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} \left[li(x^{1/k}) - \ln 2 + \int_{x^{1/k}}^{+\infty} \frac{dt}{t(t^2 - 1) \ln t} - \sum_{\zeta(\rho)=0} Ei(\rho \ln x^{1/k}) \right] \tag{1.41}$$

In altri termini, per conoscere la funzione $\pi_0(x)$ occorre conoscere la funzione di distribuzione degli zeri non banali della zeta di Riemann.

1.7 L'analisi di Riesel e Göhl

Nel 1970 i matematici svedesi Hans Riesel e Gunnar Göhl pubblicarono sulla rivista *Mathematics of Computation*, un articolo [5] sugli effetti della funzione

$$f_d(x) = - \sum_{\zeta(\rho)=0} Ei(\rho \ln x), \tag{1.42}$$

sull'andamento della distribuzione

$$\pi_0(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} f(x^{1/k}) \tag{1.43}$$

che nel predetto articolo viene troncata a un termine *N-esimo*:

$$\pi_0(x) \simeq \sum_{k=1}^N \frac{\mu(k)}{k} f(x^{1/k}) \tag{1.44}$$

In [5] Riesel e Gohl assumono $N = 154$ per due ragioni:

1. per tale valore di N , l'errore sulla determinazione di $\pi_0(x)$ è $< 10^{-4}$.
2. Risulta

$$\sum_{k=1}^{154} \frac{\mu(k)}{k} \sim 0,$$

come vediamo dal grafico di fig. 1.20.

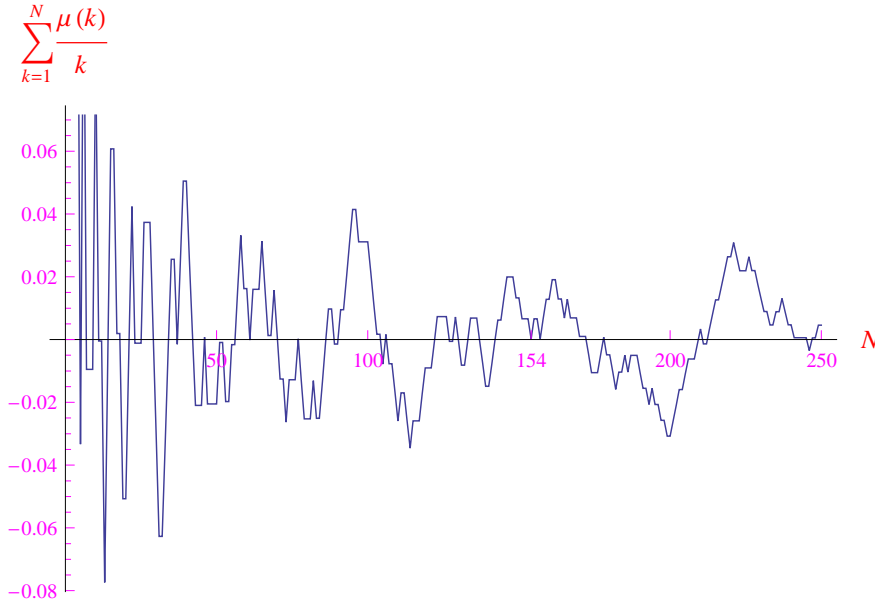


Figura 1.20: Andamento di $\sum_{k=1}^N \frac{\mu(k)}{k}$ in funzione di N .

La condizione 2 consente di approssimare la funzione integrale

$$I(x) \stackrel{def}{=} \int_x^{+\infty} \frac{dt}{t(t^2-1)\ln t} \quad (1.45)$$

Più precisamente, il termine che può essere approssimato è

$$G_N(x) = \sum_{k=1}^N \frac{\mu(k)}{k} \left[-\ln 2 + \int_{x^{1/k}}^{+\infty} \frac{dt}{t(t^2-1)\ln t} \right] \quad (1.46)$$

Cioè

$$G_N(x) = -\ln 2 \sum_{k=1}^N \frac{\mu(k)}{k} + \sum_{k=1}^N \frac{\mu(k)}{k} I(x^{1/k}) \quad (1.47)$$

Per $N = N_0$, dove

$$N_0 \gg 1 \mid \sum_{k=1}^{N_0} \frac{\mu(k)}{k} = 0, \quad (1.48)$$

si ha

$$G_{N_0}(x) = \sum_{k=1}^{N_0} \frac{\mu(k)}{k} I(x^{1/k}) \quad (1.49)$$

Per eseguire la predetta approssimazione, consideriamo innanzitutto la funzione integranda in $I(x)$:

$$g(t) = \frac{1}{t(t^2 - 1) \ln t},$$

che è definita in $(0, 1) \cup (1, +\infty)$. Inoltre:

$$\lim_{t \rightarrow 0^+} g(t) = \lim_{t \rightarrow 0^+} \underbrace{\frac{1}{t^2 - 1}}_{=-1} \cdot \lim_{t \rightarrow 0^+} \frac{1}{t \ln t}$$

L'altro limite:

$$\lim_{t \rightarrow 0^+} \frac{1}{t \ln t} = \frac{1}{0 \cdot \infty} = \lim_{t \rightarrow 0^+} \frac{t^{-1}}{\ln t} = \frac{\infty}{\infty} \stackrel{H}{=} - \lim_{t \rightarrow 0^+} \frac{1}{t} = -\infty,$$

onde

$$\lim_{t \rightarrow 0^+} g(t) = +\infty,$$

cioè la funzione è infinita per $t \rightarrow 0^+$. Calcoliamo:

$$\begin{aligned} \lim_{t \rightarrow 1^-} g(t) &= \lim_{t \rightarrow 1^-} \frac{1}{t(t^2 - 1) \ln t} = \frac{1}{1^- \cdot 0^- \cdot 0^-} = \frac{1}{0^+} = +\infty \\ \lim_{t \rightarrow 1^+} g(t) &= \lim_{t \rightarrow 1^+} \frac{1}{t(t^2 - 1) \ln t} = \frac{1}{1^+ \cdot 0^+ \cdot 0^+} = \frac{1}{0^+} = +\infty, \end{aligned} \tag{1.50}$$

per cui

$$\lim_{t \rightarrow 1} g(t) = +\infty \tag{1.51}$$

Nell'espressione di $G_{N_0}(x)$ è

$$I(x^{1/k}) = \int_{x^{1/k}}^{+\infty} g(t) dt \tag{1.52}$$

Risulta $x^{1/k} > 1$, $\forall x \in (0, +\infty)$ e – tra l'altro – a noi interessa l'intervallo $x > 2$. Riesce

$$0 < \int_{x^{1/k}}^{+\infty} g(t) dt < +\infty, \quad \forall x \in (0, +\infty)$$

giacchè $g(t) > 0$ è per $t \rightarrow +\infty$ un infinitesimo di ordine > 1 . Tuttavia ci si avvicina al valore 1 dell'estremo inferiore di integrazione nel limite dei grandi k :

$$\lim_{k \rightarrow +\infty} I(x^{1/k}) = I(1) = \int_1^{+\infty} g(t) dt$$

Per studiare il comportamento di tale integrale dobbiamo determinare l'ordine di infinito (se esiste) della funzione integranda $g(t)$ per $t \rightarrow 1^+$. Assumendo come infinito di riferimento $\frac{1}{t-1}$, si ha:

$$\lim_{t \rightarrow 1^+} \frac{g(t)}{(t-1)^{-\alpha}} = \lim_{t \rightarrow 1^+} \underbrace{\frac{1}{t(t+1)}}_{=\frac{1}{2}} \cdot \lim_{t \rightarrow 1^+} \frac{(t-1)^{\alpha-1}}{\ln t}$$

L'altro limite si calcola facilmente con la regola di De L'Hospital:

$$\begin{aligned} \lim_{t \rightarrow 1^+} \frac{(t-1)^{\alpha-1}}{\ln t} &= \frac{0}{0} \stackrel{H}{=} \lim_{t \rightarrow 1^+} \frac{(\alpha-1)(t-1)^{\alpha-2}}{\frac{1}{t}} \\ &= (\alpha-1) \lim_{t \rightarrow 1^+} (t-1)^{\alpha-2} = \ell \in \mathbb{R} - \{0\} \iff \alpha = 2 \end{aligned}$$

In altri termini, la funzione integranda è un infinito di ordine 2 per $t \rightarrow 1^+$, per cui l'integrale diverge. Dal segno della funzione segue:

$$\int_1^{+\infty} g(t) dt = +\infty \tag{1.53}$$

L'analisi matematica ci dice, quindi, che il contributo dominante all'integrale $I(x^{1/k})$ proviene dai "grandi" valori di k , poiché in corrispondenza di questi l'estremo inferiore di integrazione è circa 1. Viceversa, nel limite dei piccoli k è $x^{1/k} \gg 1$ e l'integrale è trascurabilmente piccolo, in quanto la funzione integranda si annulla rapidamente (come mostrato nel grafico di fig. 1.21):

$$\lim_{k \rightarrow 0} I(x^{1/k}) = 0 \tag{1.54}$$

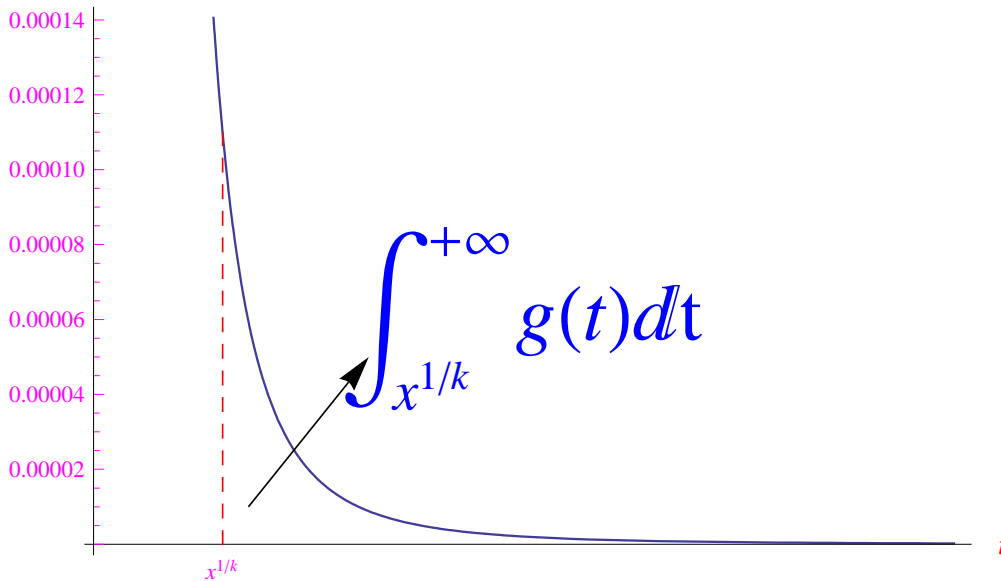


Figura 1.21: Rettangoloide generalizzato relativo alla funzione $g(t)$ e di base $[x^{1/k}, +\infty)$.

L'integrale $I(x)$ non è elementarmente esprimibile, per cui ci affidiamo a **Mathematica** per eseguire un'integrazione numerica. Precisamente, dopo aver generato una lista di valori si esegue un'interpolazione, ottenendo una funzione approssimata $I_{app}(x)$ il cui andamento è riportato in fig. 1.22. A questo punto si definisce la funzione:

$$G_{N_0, app}(x) = \sum_{k=1}^{N_0} \frac{\mu(k)}{k} I_{app}(x^{1/k}), \tag{1.55}$$

che per $N_0 = 154$ ha l'andamento riportato in fig. 1.23.

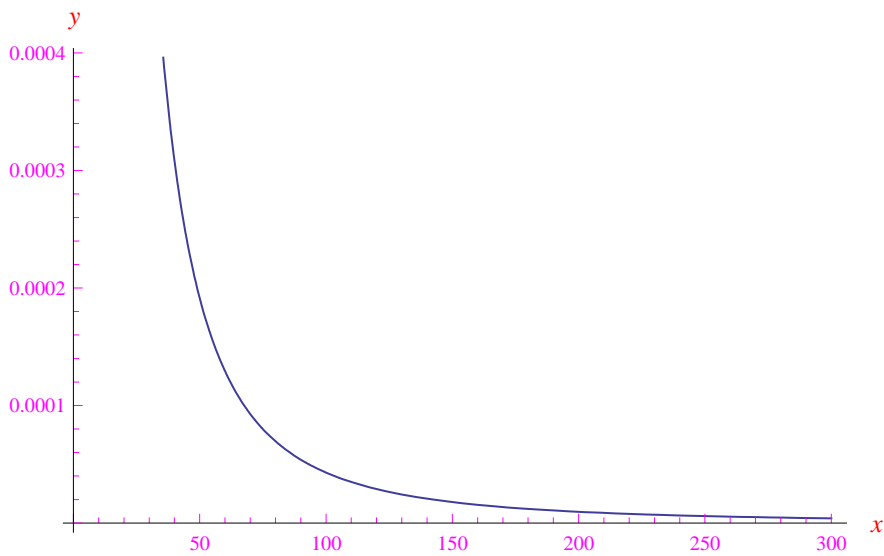


Figura 1.22: Grafico della funzione $I_{app}(x)$ quale risultato di un'integrazione numerica della $g(t)$ in $[x, +\infty)$.

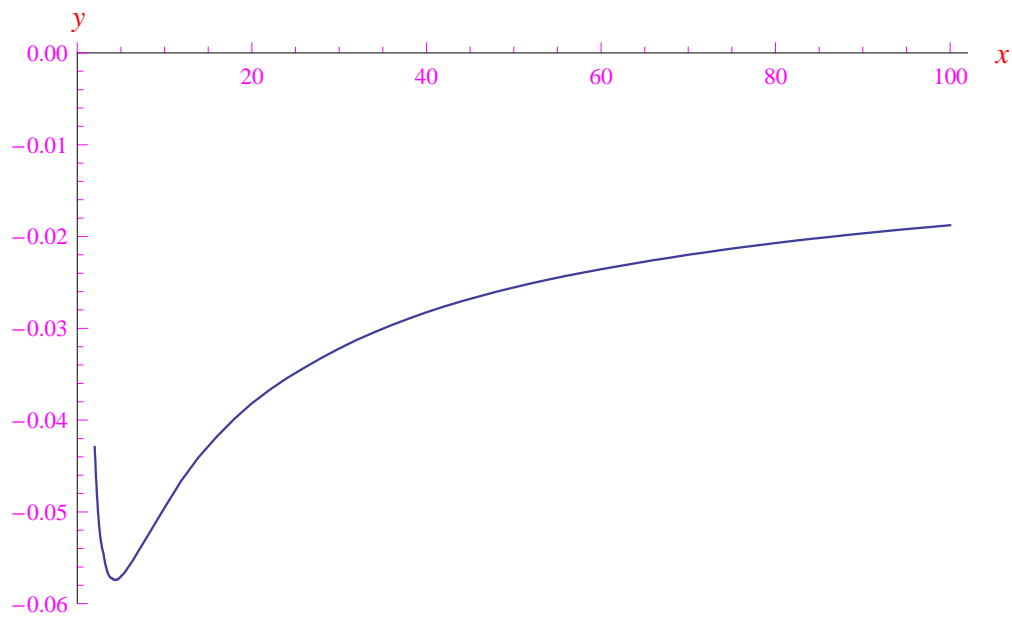


Figura 1.23: Andamento di $G_{N_0, app}(x)$.

Passiamo ora al contributo proveniente da

$$f_d(x) = - \sum_{\zeta(\rho)=0} \text{Ei}(\rho \ln x), \quad (1.56)$$

rammentando che Ei è l'esponenziale integrale (cfr. § 1.4), mentre ρ sono gli zeri non banali della funzione zeta di Riemann. Iniziamo con il dimostrare la proposizione:

Proposizione 4

$$\text{Ei}(\ln x) = li(x), \quad \forall x \in (0, +\infty) \quad (1.57)$$

Dimostrazione. Nel campo reale

$$\text{Ei}(x) = \int_{-\infty}^x \frac{e^t}{t} dt, \quad \forall x \in \mathbb{R}, \quad (1.58)$$

e

$$li(x) = \int_0^x \frac{dt}{t}, \quad \forall x \in (0, +\infty) \quad (1.59)$$

Esplicitiamo

$$\text{Ei}(\ln x) = \int_{-\infty}^{\ln x} \frac{e^t}{t} dt,$$

eseguendo il cambio di variabile

$$t' = e^t \implies dt' = e^t dt, \quad t = \ln t',$$

mentre gli estremi di integrazione diventano:

$$-\infty < t = \ln t' \leq \ln x \iff 0 < t' \leq x,$$

da cui

$$\text{Ei}(\ln x) = \int_0^x \frac{dt'}{\ln t'} = li(x)$$

■

Nel caso in esame abbiamo le funzioni integrali

$$\text{Ei}(\rho \ln x), \quad li(x^\rho)$$

Siamo tentati di scrivere

$$\text{Ei}(\rho \ln x) = li(x^\rho),$$

giacchè

$$\rho \ln x = \ln x^\rho$$

Ma nel campo complesso questa identità non è corretta, in quanto

$$\ln x^\rho = \rho \ln x - 2\pi ni$$

Per maggiori dettagli, si veda [6]–[7]. Nel grafico di fig. 1.24 riportiamo l'andamento di $|\text{Ei} \rho \ln x|$, dove $\rho = \frac{1}{2} + 21.022i$.

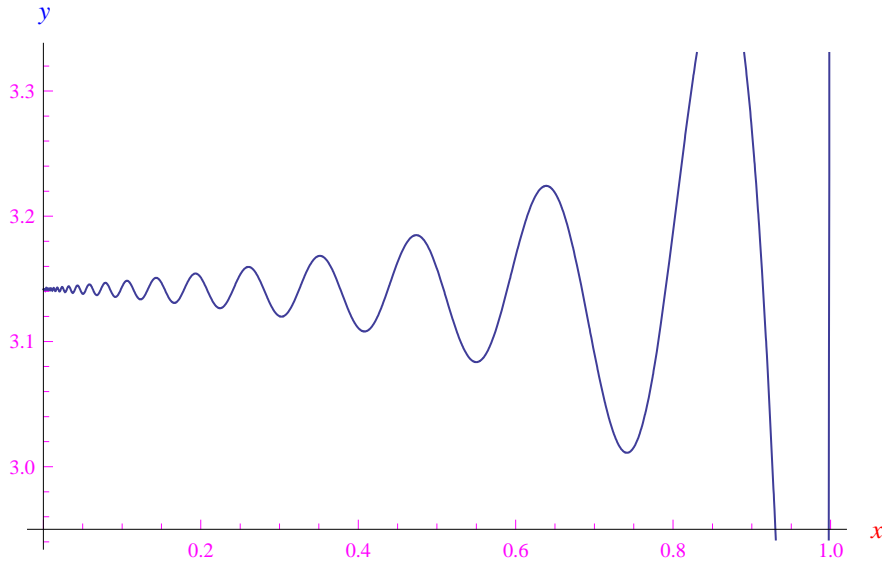


Figura 1.24: Andamento del modulo di $Ei(\rho \ln x)$ con $\rho = \frac{1}{2} + 21.022i$ che è uno degli zeri non banali della funzione zeta di Riemann.

Ciò premesso, per esplicitare la sommatoria

$$f_d(x) = - \sum_{\zeta(\rho)=0} Ei(\rho \ln x), \quad (1.60)$$

appliciamo la congettura di Riemann:

$$\rho_n = \frac{1}{2} + i\alpha_n, \quad n \in \mathbb{Z} \quad (1.61)$$

Si noti che l'espressione analitica della **successione** di elementi di \mathbb{R} :

$$\{\alpha_n\}_{n \in \mathbb{Z}} \quad (1.62)$$

è ignota. Ciò che è invece noto, è l'insieme dei valori assunti dai singoli termini fino a un certo ordine. In parole povere la non conoscenza dell'espressione analitica (se esiste) della predetta successione, implica che la parte immaginaria degli zeri della funzione zeta di Riemann, può essere al più computata manualmente (o via software), e ciò può realizzarsi per un numero finito di elementi. In ogni caso, consideriamo l'espansione da $-\infty$ a $+\infty$:

$$f_d(x) = - \sum_{n=-\infty}^{+\infty} Ei(\rho_n \ln x) \quad (1.63)$$

Per una nota proprietà della funzione zeta:

$$\zeta(\rho_n) = 0 \iff \zeta(\rho_n^*) = 0, \quad (1.64)$$

dove ρ_n^* è il complesso coniugato di ρ_n :

$$\rho_n^* = \frac{1}{2} - i\alpha_n \quad (1.65)$$

Cioè gli zeri della zeta di Riemann si distribuiscono lungo la linea critica per coppie complesse coniugate, da cui la simmetria della distribuzione rispetto all'asse reale, come appare in fig. 1.25. Ciò suggerisce la posizione:

$$\rho_{-n} = \rho_n \quad n \in \mathbb{N}, \quad (1.66)$$

da cui

$$\sum_{n=-\infty}^{+\infty} \text{Ei}(\rho_n \ln x) = \sum_{n=-\infty}^0 \text{Ei}(\rho_n \ln x) + \sum_{n=0}^{+\infty} \text{Ei}(\rho_n \ln x) \quad (1.67)$$

Se nella prima sommatoria eseguiamo il cambio di indice $n' = -n$:

$$\sum_{n=-\infty}^0 \text{Ei}(\rho_n \ln x) = \sum_{n'=0}^{+\infty} \text{Ei}(\rho_{-n'} \ln x) = \sum_{n'=0}^{+\infty} \text{Ei}(\rho_{n'}^* \ln x)$$

Cioè

$$f_d(x) = - \sum_{n=0}^{+\infty} [\text{Ei}(\rho_n \ln x) + \text{Ei}(\rho_n^* \ln x)], \quad (1.68)$$

il cui contributo alla funzione di distribuzione dei primi $\pi_0(x)$ è:

$$H_N(x) = \sum_{k=1}^N \frac{\mu(k)}{k} f_d(x^{1/k}) = - \sum_{k=1}^N \frac{\mu(k)}{k} \sum_{n=0}^{+\infty} \left[\text{Ei}\left(\frac{\rho_n}{k} \ln x\right) + \text{Ei}\left(\frac{\rho_n^*}{k} \ln x\right) \right] \quad (1.69)$$

Ne consegue

$$H_N(x) = \sum_{n=0}^{+\infty} T_n(x), \quad (1.70)$$

essendo

$$T_n(x) = - \sum_{k=1}^N \frac{\mu(k)}{k} \left[\text{Ei}\left(\frac{\rho_n}{k} \ln x\right) + \text{Ei}\left(\frac{\rho_n^*}{k} \ln x\right) \right] \quad (1.71)$$

In altri termini, la funzione $H_N(x)$ è per un assegnato N , il contributo alla funzione di distribuzione $\pi_0(x)$, ed è la somma della serie (1.70), il cui termine n -esimo è il contributo proveniente dallo zero n -esimo della zeta di Riemann.

Proposizione 5 *Le infinite funzioni (1.71) sono reali.*

Dimostrazione. Poniamo

$$\text{Ei}\left(\frac{\rho_n^*}{k} \ln x\right) = \text{Ei}(\alpha z^*), \quad (1.72)$$

essendo

$$\alpha \stackrel{\text{def}}{=} \ln x, \quad z \stackrel{\text{def}}{=} \frac{\rho_n}{k} \quad (1.73)$$

Dalla definizione dell'esponenziale integrale:

$$\text{Ei}(\alpha z^*) = \int_{\gamma(z_\infty, \alpha z^*)} \frac{e^w}{w} dw = \left[\int_{\gamma(z_\infty, \alpha z)} \frac{e^w}{w} dw \right]^* = [\text{Ei}(\alpha z)]^* \quad (1.74)$$

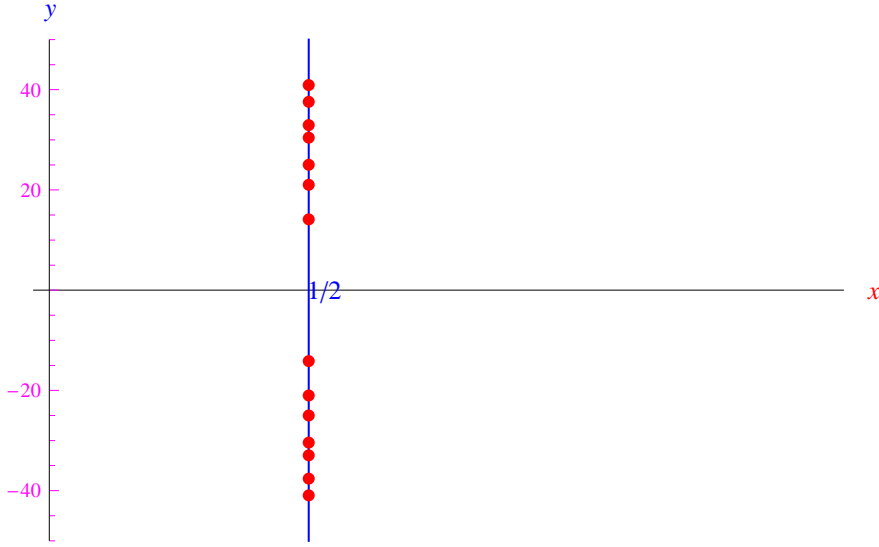


Figura 1.25: Alcuni zeri non banali della funzione zeta di Riemann.

Segue

$$\begin{aligned} \operatorname{Ei}\left(\frac{\rho_n}{k} \ln x\right) + \operatorname{Ei}\left(\frac{\rho_n^*}{k} \ln x\right) &= \operatorname{Ei}\left(\frac{\rho_n}{k} \ln x\right) + \left[\operatorname{Ei}\left(\frac{\rho_n}{k} \ln x\right)\right]^* \\ &= 2 \operatorname{Re}\left[\operatorname{Ei}\left(\frac{\rho_n}{k} \ln x\right)\right] \end{aligned} \quad (1.75)$$

Quindi

$$T_n(x) = -2 \sum_{k=1}^N \frac{\mu(k)}{k} \operatorname{Re}\left[\operatorname{Ei}\left(\frac{\rho_n}{k} \ln x\right)\right], \quad (1.76)$$

cioè l'asserto. ■

Per studiare il comportamento dei singoli termini $T_n(x)$, consideriamo l'espansione esatta:

$$T_n(x) = -2 \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} \operatorname{Re}\left[\operatorname{Ei}\left(\frac{\rho_n}{k} \ln x\right)\right] \quad (1.77)$$

Ricordiamo che $T_n(x)$ è il generico termine di una serie di funzioni uniformemente convergente:

$$H(x) = \sum_{n=0}^{+\infty} T_n(x),$$

cioè la (1.70) senza il pedice N , giacché ora è $N \rightarrow +\infty$. La funzione $H(x)$ riproduce le discontinuità della funzione di distribuzione

$$\pi_0(x) = R(x) + G(x) + H(x) \quad (1.78)$$

Rammentiamo che

$$R(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} \operatorname{li}(x^{1/k}), \quad (1.79)$$

esprimibile come somma della serie di Gram:

$$R(x) = 1 + \sum_{k=1}^{+\infty} \frac{(\ln x)^k}{k! k \zeta(k+1)} \quad (1.80)$$

La funzione $G(x)$ è un ulteriore contributo alla “parte continua” di $\pi_0(x)$:

$$G(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} \left[-\ln 2 + \int_{x^{1/k}}^{+\infty} g(t) dt \right], \quad \text{con } g(t) = \frac{1}{t(t^2 - 1) \ln t} \quad (1.81)$$

Per un assegnato n

$$T_n(x) = \sum_{k=1}^{+\infty} c_k \psi_{k,n}(x) \quad (1.82)$$

Cioè a sua volta, il generico termine $T_n(x)$ è la somma di una serie di funzioni, il cui termine generico è

$$\psi_{k,n}(x) \stackrel{\text{def}}{=} \operatorname{Re} \left[\operatorname{Ei} \left(\frac{\rho_n}{k} \ln x \right) \right], \quad (1.83)$$

mentre i *coefficienti di Möbius*:

$$c_k = -\frac{2\mu(k)}{k}, \quad k \in \mathbb{N} - \{0\} \quad (1.84)$$

Esplicitando ρ_n :

$$\psi_{k,n}(x) = \operatorname{Re} \left\{ \operatorname{Ei} \left[\frac{\ln x}{k} \left(\frac{1}{2} + i\alpha_n \right) \right] \right\}, \quad (1.85)$$

rammentando che gli zeri della zeta di Riemann sono **built-in** in **Mathematica**. Per un assegnato intero naturale n , è univocamente definita la successione di funzioni

$$\{\psi_{k,n}(x)\}_{k \in \mathbb{N} - \{0\}}, \quad (1.86)$$

che dovrà comunque essere troncata a un dato N_0 ed avevamo posto $N_0 = 154$. Segue che il calcolo di un singolo termine $T_n(x)$ richiede la computazione software di N_0 funzioni:

$$\psi_{1,n}(x) = \operatorname{Re} [\operatorname{Ei}(\rho_n \ln x)], \quad \psi_{2,n}(x) = \operatorname{Re} \left[\operatorname{Ei} \left(\frac{\rho_n}{2} \ln x \right) \right], \quad \psi_{N_0,n}(x) = \operatorname{Re} \left[\operatorname{Ei} \left(\frac{\rho_n}{N_0} \ln x \right) \right] \quad (1.87)$$

Da [5] segue

$$\operatorname{Ei} \left(\frac{\rho_n}{k} \ln x \right) \sim \frac{e^{\frac{\rho_n}{k} \ln x}}{\frac{\rho_n}{k} \ln x}, \quad (1.88)$$

da cui l'espressione approssimata

$$\psi_{k,n}(x) \sim \operatorname{Re} \left(\frac{e^{\frac{\rho_n}{k} \ln x}}{\frac{\rho_n}{k} \ln x} \right) \quad (1.89)$$

Esplicitando ρ_n :

$$e^{\frac{\rho_n}{k} \ln x} = e^{\frac{\ln x}{2k} + i \frac{\alpha_n}{k} \ln x} = x^{1/2k} e^{i \frac{\alpha_n}{k} \ln x} \quad (1.90)$$

Se al denominatore del secondo membro della (1.89) esprimiamo il numero complesso ρ_n in forma polare:

$$\rho_n = |\rho_n| e^{i \arg \rho_n},$$

tenendo conto della (1.90) si ha:

$$\frac{e^{\frac{\rho_n}{k} \ln x}}{\frac{\rho_n}{k} \ln x} = \frac{kx^{1/2k}}{|\rho_n| \ln x} e^{i \left(\frac{\alpha_n}{k} \ln x - \arg \rho_n \right)}$$

Prendendo la parte Reale del secondo membro, otteniamo:

$$\psi_{k,n}(x) \sim \frac{kx^{1/2k}}{|\rho_n| \ln x} \cos\left(\frac{\alpha_n}{k} \ln x - \arg \rho_n\right), \quad (1.91)$$

a cui corrisponde la seguente relazione approssimata per il termine *n-esimo*:

$$T_n(x) \sim \frac{1}{|\rho_n| \ln x} \sum_k k c_k x^{1/2k} \cos\left(\frac{\alpha_n}{k} \ln x - \arg \rho_n\right) \quad (1.92)$$

Da tale relazione vediamo che il contributo dominante ai termini $T_n(x)$ proviene dai primi zeri ρ_n :

$$|\rho_{n \gg 1}| \gg 1 \implies |T_{n \gg 1}(x)| \ll 1$$

Dalla (1.91) segue che le funzioni $\psi_{k,n}(x)$ hanno un comportamento oscillante a causa della presenza della funzione coseno:

$$\psi_{k,n}(x) \sim A_{k,n}(x) \cos\left(\frac{\alpha_n}{k} \ln x - \arg \rho_n\right), \quad (1.93)$$

essendo:

$$A_{k,n}(x) = \frac{kx^{1/2k}}{|\rho_n| \ln x} \quad (1.94)$$

Per quanto precede, siamo interessati al comportamento di $\pi_0(x)$ per $x \geq 2$. Tuttavia vale la pena esaminare il comportamento delle varie funzioni per $x < 2$. Ad esempio, l'ampiezza (1.94) è definita in $(0, 1) \cup (1, +\infty)$. In $x = 0$ troviamo un punto di discontinuità eliminabile, giacché

$$\lim_{x \rightarrow 1^-} A_{k,n}(x) = 0^-,$$

mentre in $x = 1$ abbiamo un punto di discontinuità di seconda specie:

$$\lim_{x \rightarrow 1^-} A_{k,n}(x) = -\infty, \quad \lim_{x \rightarrow 1^+} A_{k,n}(x) = +\infty$$

Ne consegue un comportamento oscillante della (1.93) in un intorno di $x = 1$ di raggio comunque piccolo, con ampiezza divergente. A differenza dell'espressione approssimata, quella esatta è divergente negativamente. Infatti calcolando il limite con *Mathematica*, si trova:

$$\lim_{x \rightarrow 1} \psi_{k,n}(x) = -\infty$$

In fig. 1.26 dove riportiamo gli andamenti delle rispettive espressioni (esatta ed approssimata).

Nelle figg. 1.27-1.28-1.29-1.30-1.31 riportiamo i grafici delle funzioni $\psi_{1,n}(x)$ per $n = 1, 2, 3, 4, 5$ per $x \geq 2$. In fig. sono tracciati insieme i grafici di $\psi_{1,n}(x)$ per $n = 1, 2, 3$ nell'intervallo $[0, +\infty)$, da cui è visibile la singolarità in $x = 1$.

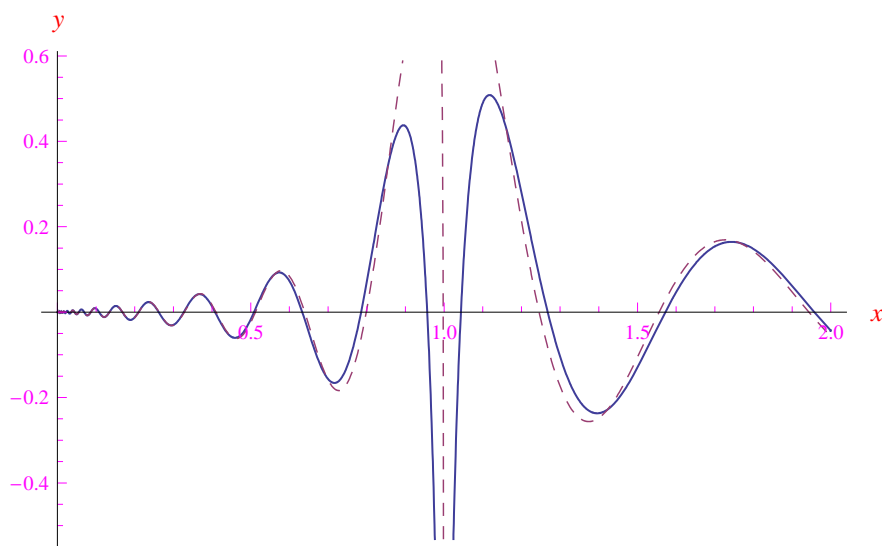


Figura 1.26: La curva continua è il grafico di $\psi_{1,1}(x)$ nell'intervallo $[0, 2]$, mentre la curva in tratteggio è il grafico dell'espressione approssimata.

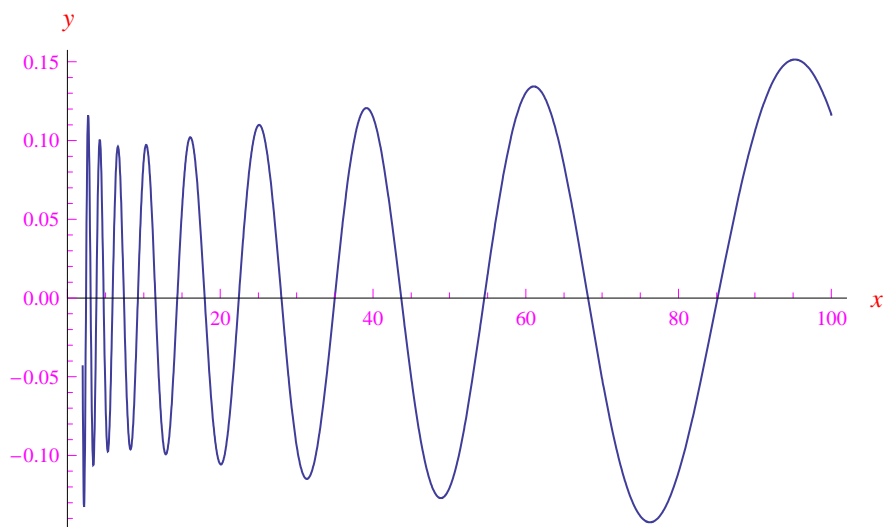


Figura 1.27: $y = \psi_{1,1}(x)$

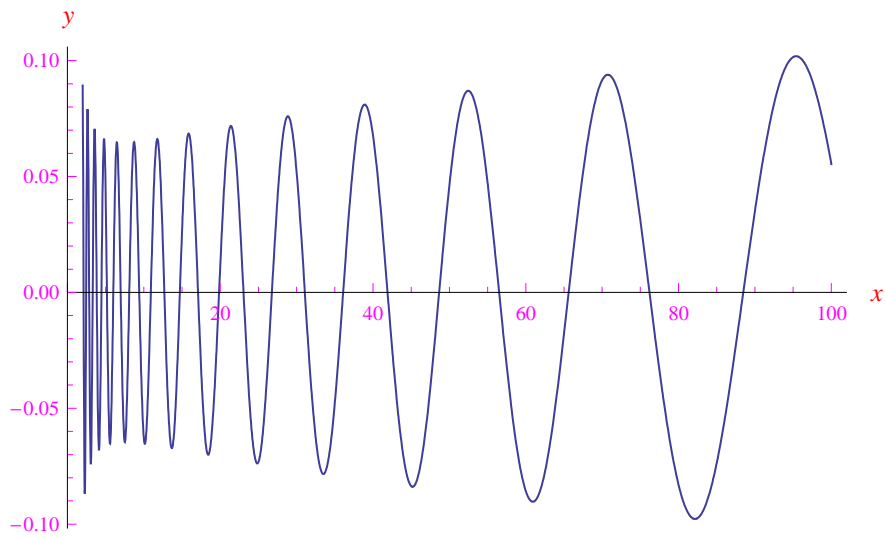


Figura 1.28: $y = \psi_{1,2}(x)$

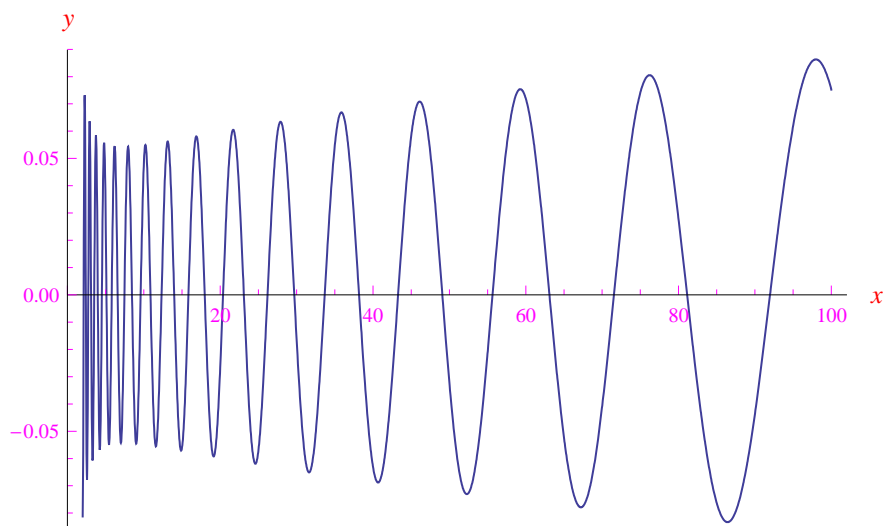


Figura 1.29: $y = \psi_{1,3}(x)$

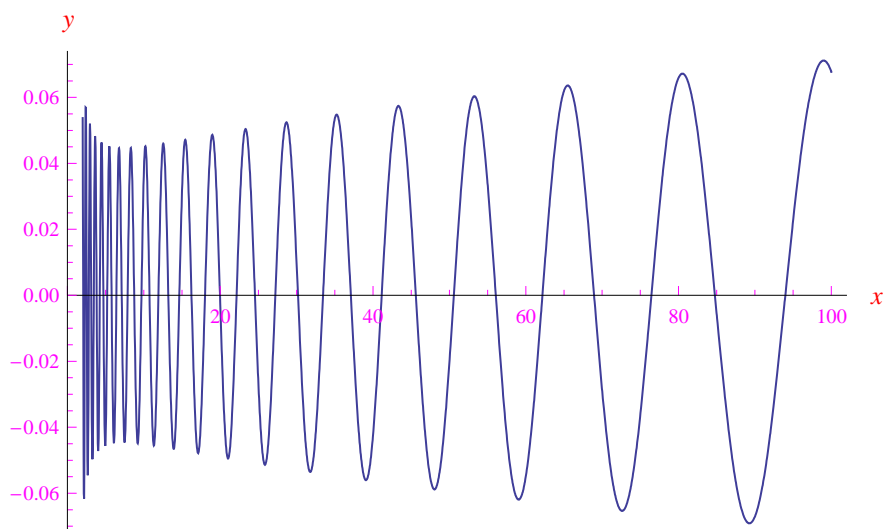


Figura 1.30: $y = \psi_{1,4}(x)$

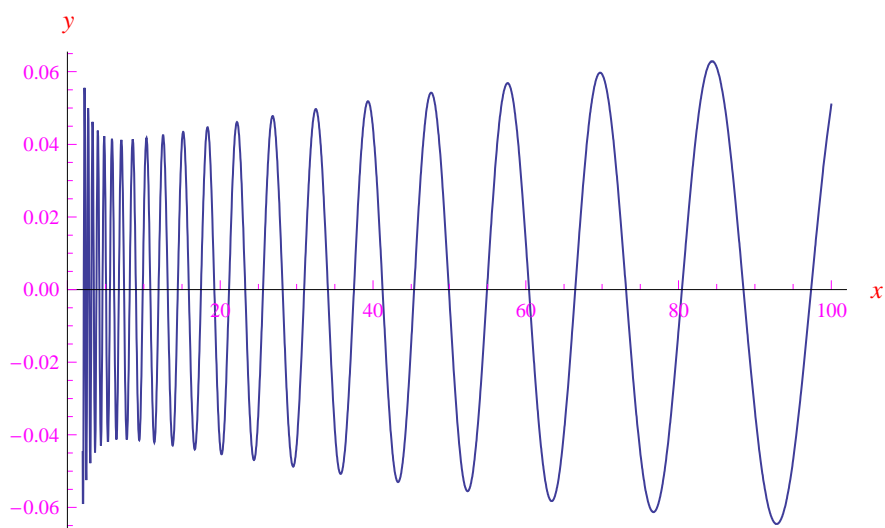


Figura 1.31: $y = \psi_{1,5}(x)$

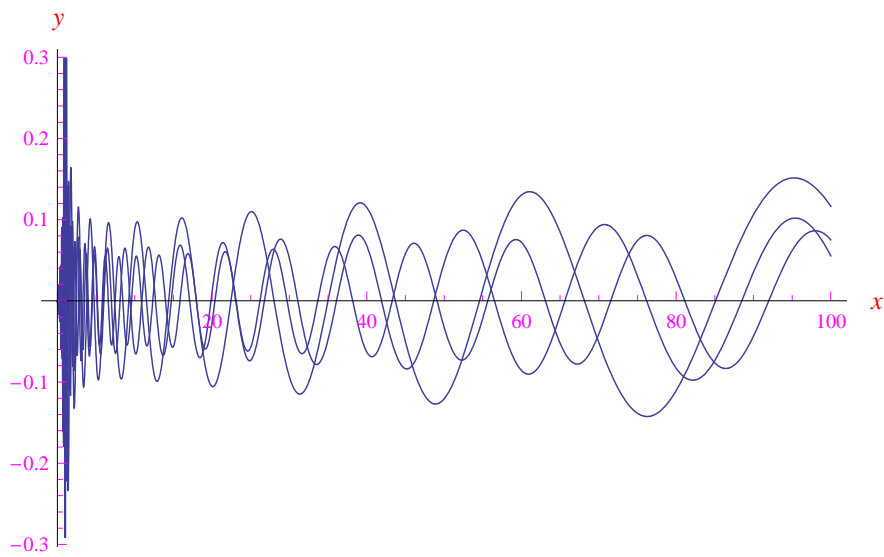


Figura 1.32: $y = \psi_{1,n}(x)$ per $n = 1, 2, 3$.

Capitolo 2

Analisi computazionale

2.1 Analisi globale

Per scrivere un programma con **Mathematica** che sia in grado di riprodurre le discontinuità di prima specie della distribuzione $\pi_0(x)$, utilizziamo innanzitutto un'approssimazione del termine $G(x)$ proposta da [5]:

$$G(x) \simeq \frac{1}{\pi} \arctan\left(\frac{\pi}{\ln x}\right), \quad (2.1)$$

dopodiché definiamo la “componete continua” della $\pi_0(x)$

$$R_0(x) \stackrel{def}{=} R(x) + G(x), \quad (2.2)$$

dove $R(x)$ è l'approssimazione di Riemann espressa attraverso la serie di Gram (§ 1.2) troncata a un ordine N (un valore tipico è $N = 100$)

$$R(x) = 1 + \sum_{k=1}^{+\infty} \frac{(\ln x)^k}{k!k\zeta(k+1)} \simeq 1 + \sum_{k=1}^{100} \frac{(\ln x)^k}{k!k\zeta(k+1)} \quad (2.3)$$

In fig. 2.1 riportiamo i grafici delle restrizioni delle funzioni $\pi_0(x)$ e $R_0(x)$ all'intervallo $[12, 100]$.

Riprendiamo ora il termine correttivo $H(x)$ (eq. (1.70)) iniziando la somma da $n = 1$ giacché **Mathematica** enumera con questa modalità gli zeri della zeta di Riemann che sono **built-in**, onde definiamo dapprima la seguente funzione che restituisce l'*n-esimo* zero:

```
rho[n] := N[ZetaZero[n]]
```

$H(x)$ si presenta nella forma:

$$H(x) = -2 \sum_{n=1}^{+\infty} \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} \operatorname{Re} \left[\int_{-\infty + i\frac{\alpha_n \ln x}{k}}^{\frac{\ln x}{2k} + i\frac{\alpha_n \ln x}{k}} \frac{e^{\xi + i\eta}}{\xi + i\eta} (d\xi + id\eta) \right], \quad (2.4)$$

che è mostruosamente complicata pur troncando le serie alle somme parziali $H_N(x)$ e $T_n(x)$:

$$H_N(x) = \sum_{n=1}^N T_n(x), \quad T_n(x) = \sum_{k=1}^{N_0} c_k \psi_{k,n}(x) \quad (2.5)$$

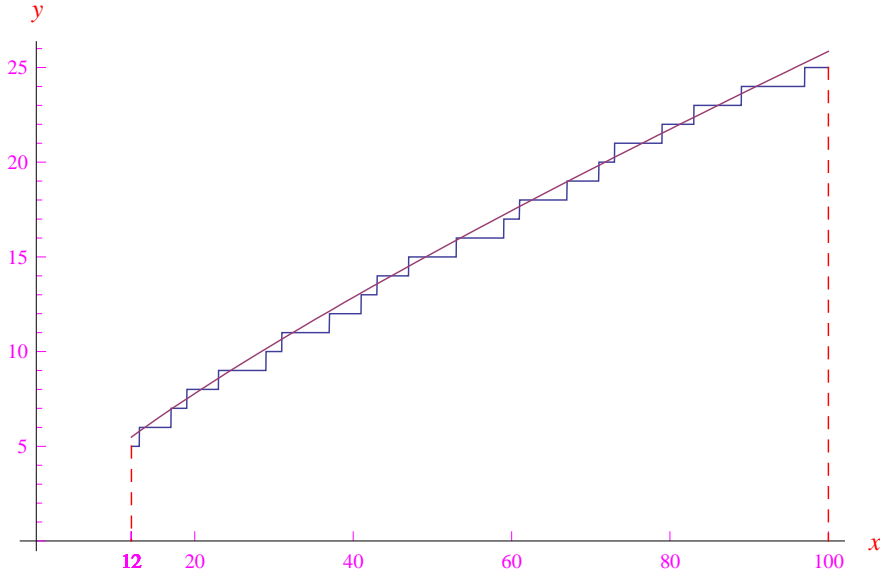


Figura 2.1: $y = \pi_0(x)$ (distribuzione a gradini) e $y = R_0(x)$ (x), data dalla (2.2).

I parametri liberi della routine sono (N, N_0) . Per quanto detto, l'intero naturale non nullo N è il numero di zeri della zeta, mentre N_0 è già stato esaminato nel numero precedente dove avevamo posto $N_0 = 154$, mentre [9] utilizza per l'altro parametro il valore $N = 50$. In parole povere dobbiamo calcolare il contributo proveniente dai primi 50 zeri non banali della zeta di Riemann.

L'esecuzione della sommatoria per il calcolo di $T_n(x)$ ha un elevato costo computazionale a causa delle funzioni non elementarmente esprimibili.

$$\psi_{1,n}(x), \psi_{2,n}(x), \dots, \psi_{N_0,n}(x),$$

per cui applichiamo il procedimento elaborato in questo [handbook](#). Quindi trasformiamo i vari termini in vettori riga e vettori colonna, dopodiché eseguiamo un prodotto righe per colonne (prodotto scalare). Scriviamo:

$$T_n(x) = C\Psi_n(x), \tag{2.6}$$

dove C è il vettore riga dei coefficienti di Möbius:

$$C = (c_1 \quad c_2 \quad \dots \quad c_{N_0}), \tag{2.7}$$

mentre

$$\Psi_n(x) = \begin{pmatrix} \psi_{1,n}(x) \\ \psi_{2,n}(x) \\ \dots \\ \psi_{N_0,n}(x) \end{pmatrix}, \tag{2.8}$$

definisce il vettore colonna. Calcoliamo dapprima la lista dei coefficienti di Möbius:

```
listaMoebius=Table[
N[MoebiusMu[k]]/k,
{k,154}
]
```

Utilizzando l'istruzione `Select` ridefiniamo gli indici dei coefficienti in modo da scartare quelli nulli (aumenterebbero solo il carico computazionale):

```
IndiciMoebius=Select[
Range[154],
listaMoebius[[#]] != 0 &
];
```

Di seguito la lista dei coefficienti di Möbius non nulli:

```
CoefficientiMoebius = listaMoebius[[IndiciMoebius]];
```

Tale lista non è altro che la matrice (2.7) ma di ordine $N'_0 < N_0$, giacché abbiamo rimosso i coefficienti nulli. Il vettore colonna Ψ_n (con N'_0 colonne) è generato dalla riga di codice:

```
psi[x_,n_]=Re[ExpIntegralEi[(rho[n]/IndiciMoebius)*Log[N[x]]]
```

Rammentiamo che $\rho[n]$ è l' n -esimo zero della zeta già definito in precedenza. Quindi:

```
T[x_, n_] := CoefficientiMoebius. psi[x, n]
```

A questo punto, sulla falsariga dell'**approcio** citato in precedenza, eseguiamo una decomposizione dell'intervallo $X_0 = [2, b]$ con $b > 2$ espresso come parametro libero, assegnando $b + 550$ punti:

$$x_k = 2 + k \frac{b-2}{b+50}, \quad k = 0, 1, \dots, b+550, \quad (2.9)$$

che compongono il seguente sottoinsieme di X_0

$$X'_0 = \left\{ x_k = 2 + k \frac{b-12}{b+50}, \quad k = 0, 1, \dots, b+550 \right\} \quad (2.10)$$

I valori assunti da $T_n(x)$ in X'_0 genera la lista di $b + 551$ elementi:

$$\{T_n(x_k)\}_{k \in \{0, \dots, b+550\}} \quad (2.11)$$

Dobbiamo adesso comunicare a *Mathematica* come calcolare questa lista. La decomposizione dell'intervallo X_0 si ottiene con l'istruzione `Range`:

```
Dec[b_] := Range[
(*punto iniziale*)
2.,
(*punto finale*)
N[b],
(*step*)
N[(b - 2)/(b + 550)]
];
```

Dal momento che in *Mathematica* le funzioni definite dall'utente hanno l'attributo `Listable` (cioè agiscono sulle liste), definiamo una funzione dell'indice n , ove quest'ultimo individua lo zero della zeta di Riemann:

```
Tlist[b_,n_] := T[Dec[b],n]
```

Per un assegnato $b > 2$ tale istruzione restituisce la lista $\{T_n(x_k)\}$. L'argomento di `ListLinePlot` è l'insieme delle coppie ordinate $(x_k, T_n(x))$ giacché tale istruzione esegue un tracciamento per punti per poi unirli con una linea continua. Dobbiamo allora trasformare la lista generata da `Tlist` in una lista di coppie ordinate. Per *Mathematica* una lista altro non è che un vettore (i.e. matrice riga), per cui definiamo:

```
M[b_,n_] := {
  (*prima riga*)
  Dec[b],
  (*seconda riga*)
  Tlist[b,n]
}
```

Cioè la matrice $2 \times (b + 551)$:

$$M(b, n) = \begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{b+550} \\ T_n(x_0) & T_n(x_1) & T_n(x_2) & \dots & T_n(x_{b+550}) \end{pmatrix} \quad (2.12)$$

Passando alla matrice trasposta:

$$M^T(n) = \begin{pmatrix} x_0 & T_n(x_0) \\ x_1 & T_n(x_1) \\ x_2 & T_n(x_2) \\ \dots & \dots \\ x_{b+550} & T_n(x_{b+550}) \end{pmatrix}, \quad (2.13)$$

si ottiene la giusta sequenza di coppie ordinate. Nel notebook di *Mathematica* scriviamo:

```
plotT[b_, n_] := ListLinePlot[
  Transpose[M[b, n]]
]
```

Per $n = 1$ otteniamo il grafico di fig. 2.2. Nelle figg. 2.3-...-2.6 riportiamo i grafici dei termini correttivi $T_2(x), \dots, T_4(x), T_{30}(x), T_{90}(x)$. Tali funzioni hanno in comune l'andamento oscillatorio a causa della presenza di $\cos(a \ln x)$, dove $a > 0$ è una costante (cfr. eq. 1.93) nel proprio sviluppo in serie. Si noti l'ampiezza progressivamente decrescente quando si passa da $T_n(x)$ a $T_{n'>n}(x)$. Questo comportamento conferma l'analisi fatta in precedenza, e cioè che il contributo dominante proviene dai primi zeri della funzione zeta.

Per poter sommare $H_N(x)$ (nel procedimento appena visto) a $R_0(x)$, dobbiamo dapprima trasformare quest'ultima funzione in una lista in modo da ricostruire in software l'espressione:

$$R_0(x) + H_N(x) = \pi_0(x) \quad (2.14)$$

Sul notebook di *Mathematica* battiamo il seguente codice:

```
R0List[b_] := R0[Dec[b]];
primiList[b_] := PrimePi[Dec[b]];
```

ove la seconda riga di codice restituisce la funzione built-in `PrimePi` applicata all'insieme X'_0 . Rammentiamo che `PrimePi[x]` ci dice quanti primi ci sono tra 0 e x . La funzione $H_N(x)$ è definita dall'istruzione:

$$H[b_, p_] := \text{Sum}[\text{Tlist}[b, n], \{n, p\}]$$

Qui l'intero naturale p svolge il ruolo di N o meglio, è un parametro libero che ci permette di aggiungere progressivamente i vari zeri. Ad esempio, per $p = 1$ otteniamo il grafico di fig. 2.8, cui è $b = 20$. Tale valore di b implica che stiamo considerando i primi 8 numeri primi: 2, 3, 5, 7, 11, 13, 17, 19. Confrontando lo stesso valore di b , plottiamo $R_2(x) = R_0(x) + T_1(x) + T_2(x)$, da cui vediamo la comparsa di oscillazioni come mostrato in fig. 2.9. Nelle rimanenti figg. 2.10-2.28 i grafici sono stati ottenuti aggiungendo progressivamente i vari termini correttivi.

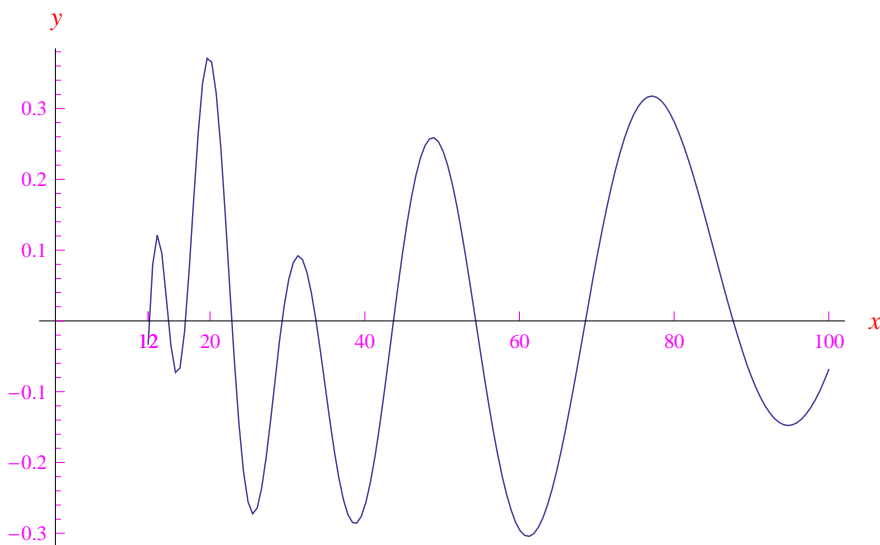


Figura 2.2: Grafico del termine correttivo $T_1(x)$.

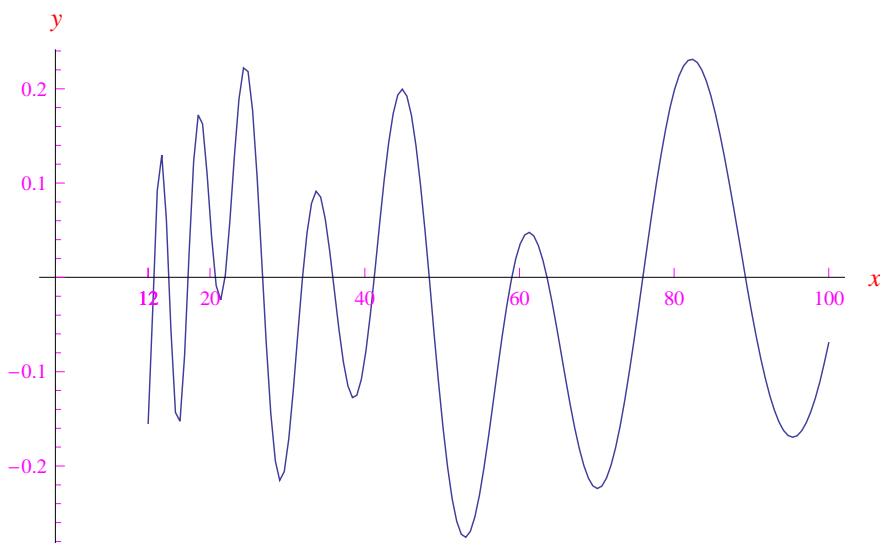


Figura 2.3: Grafico del termine correttivo $T_2(x)$.

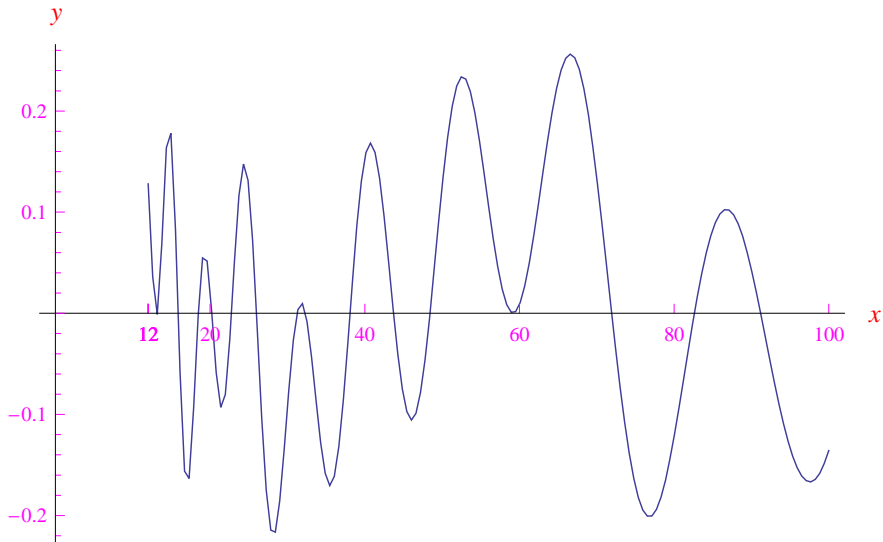


Figura 2.4: Grafico del termine correttivo $T_3(x)$.

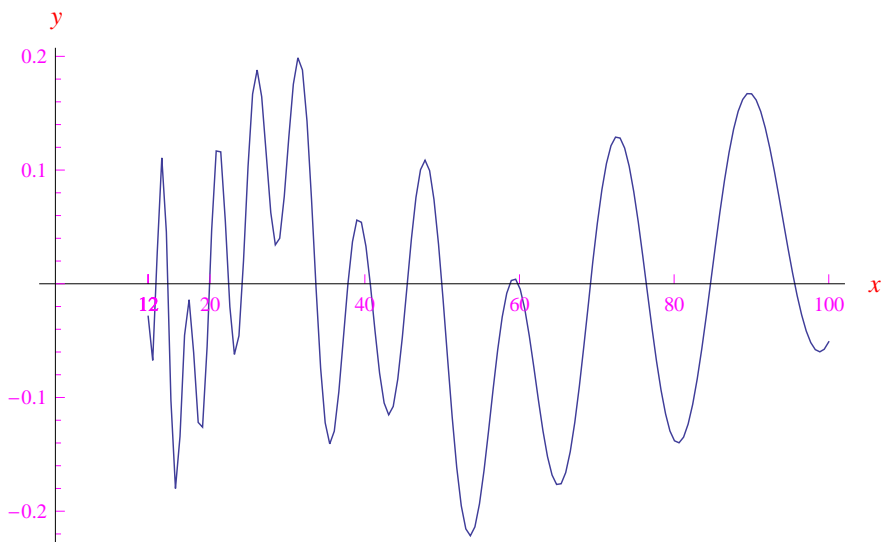


Figura 2.5: Grafico del termine correttivo $T_4(x)$.

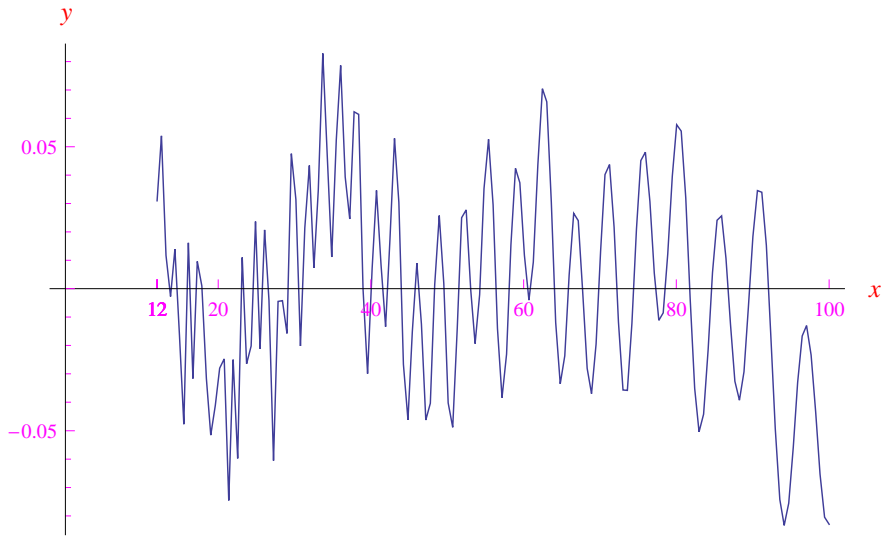


Figura 2.6: Grafico del termine correttivo $T_{30}(x)$.

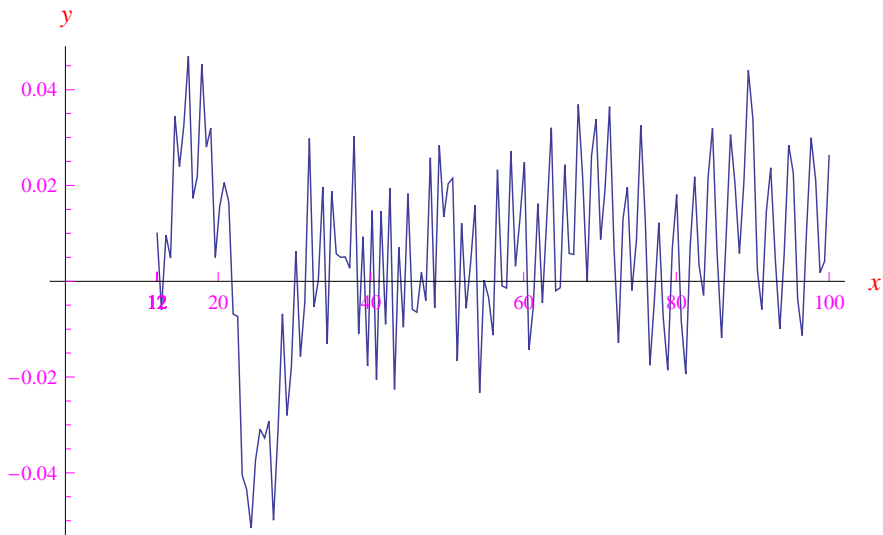


Figura 2.7: Grafico del termine correttivo $T_{90}(x)$.

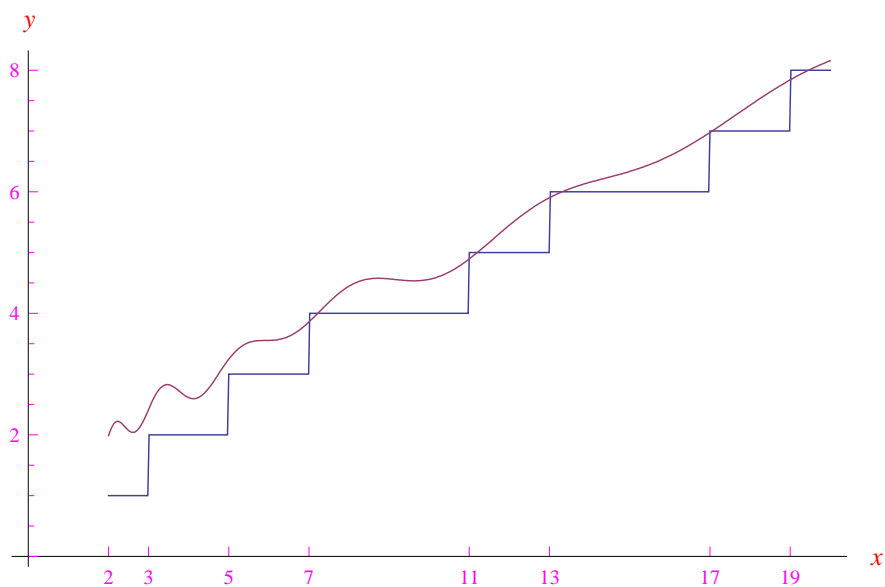


Figura 2.8: Andamento di $R_1(x) = R_0(x) + T_1(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$ ricostruita con l'istruzione PrimePi.

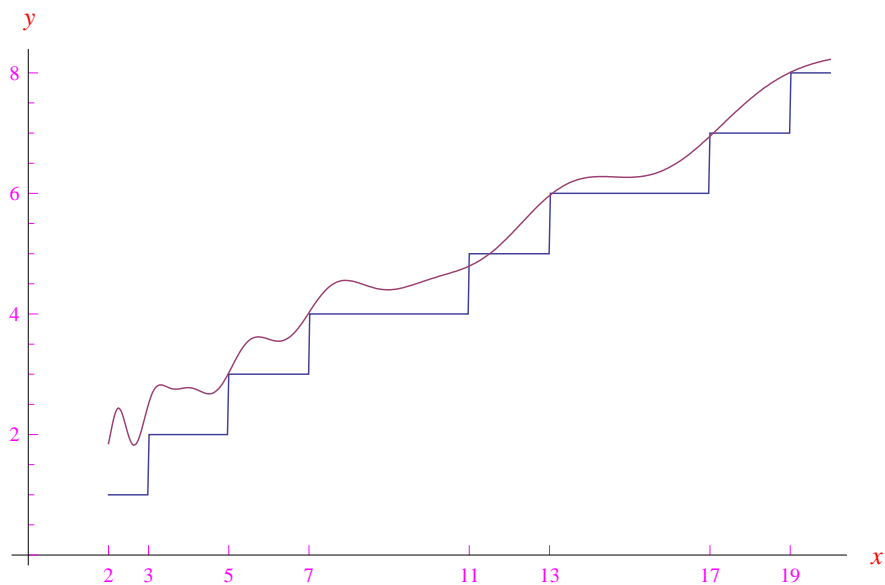


Figura 2.9: Andamento di $R_2(x) = R_0(x) + H_2(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

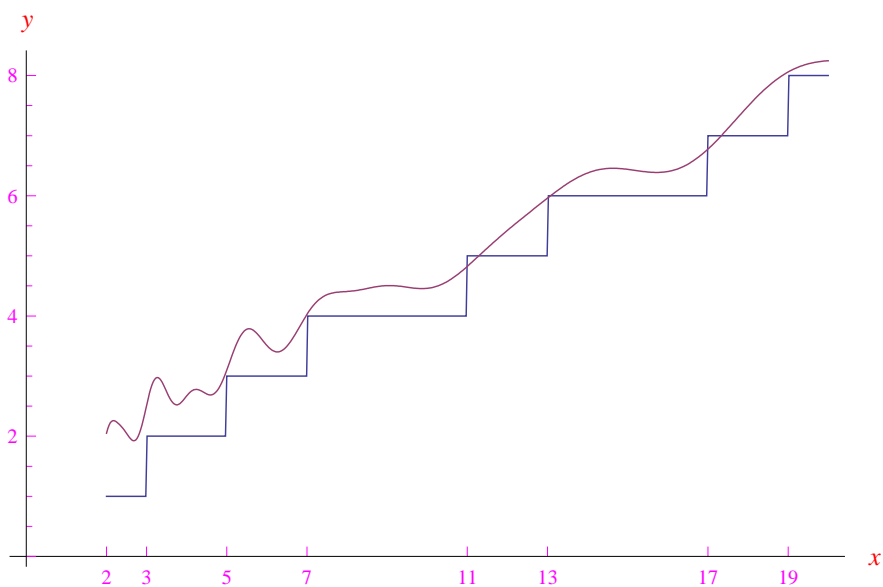


Figura 2.10: Andamento di $R_3(x) = R_0(x) + H_3(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

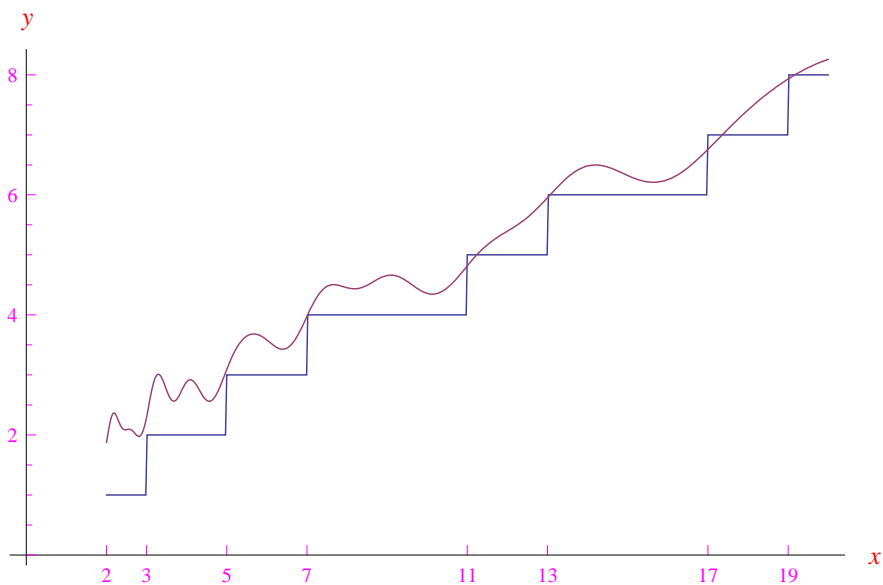


Figura 2.11: Andamento di $R_4(x) = R_0(x) + H_4(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

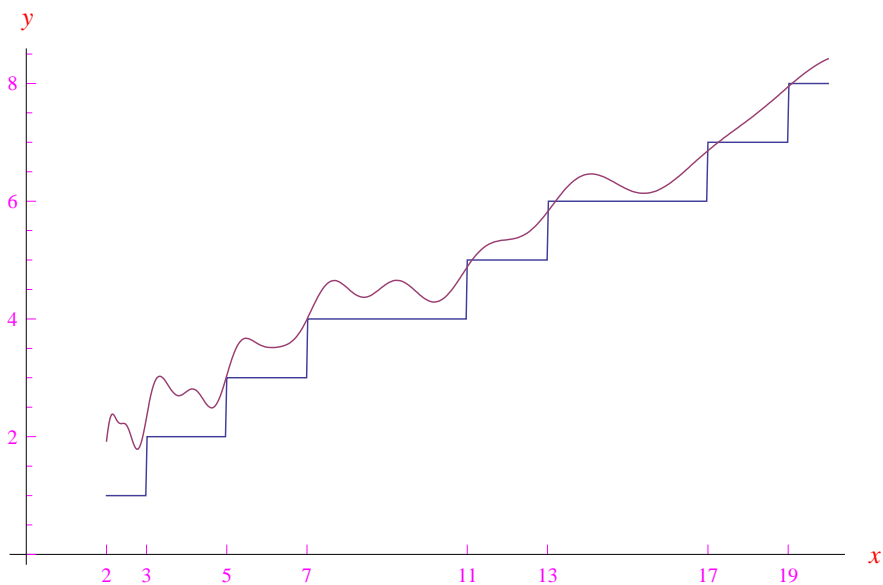


Figura 2.12: Andamento di $R_5(x) = R_0(x) + H_5(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.



Figura 2.13: Andamento di $R_7(x) = R_0(x) + H_7(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

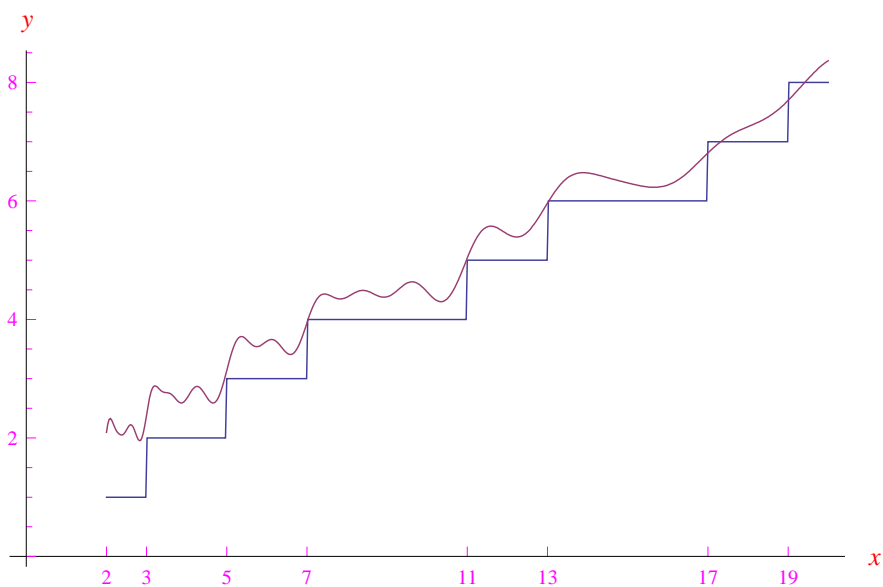


Figura 2.14: Andamento di $R_8(x) = R_0(x) + H_8(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

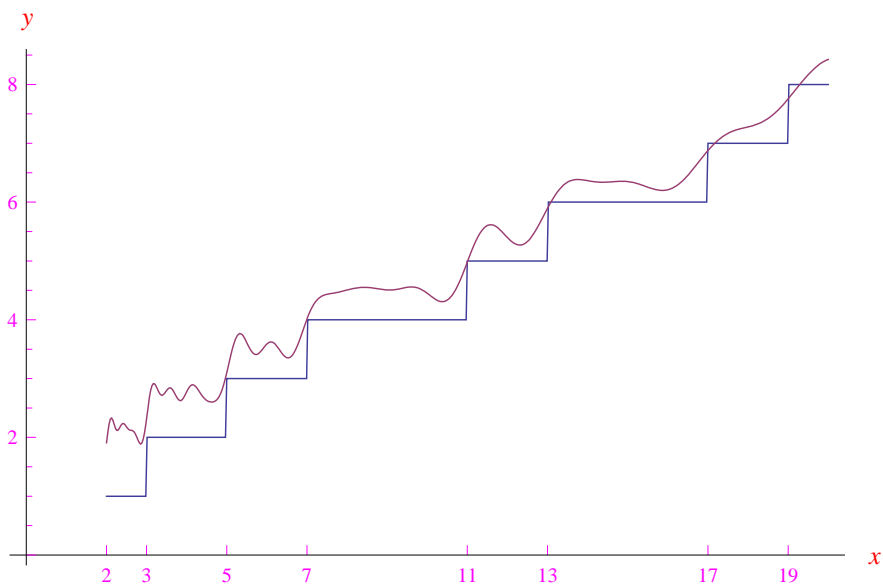


Figura 2.15: Andamento di $R_9(x) = R_0(x) + H_9(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

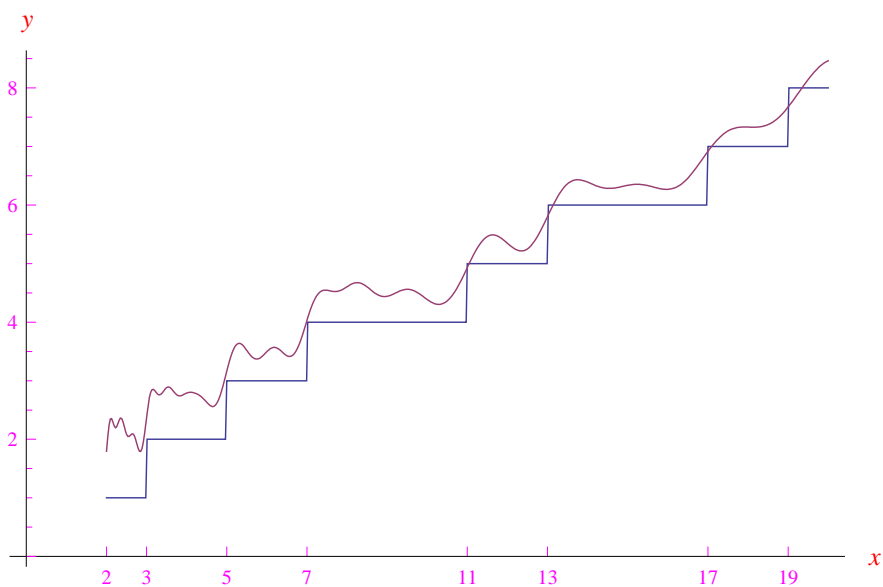


Figura 2.16: Andamento di $R_{10}(x) = R_0(x) + H_{10}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.



Figura 2.17: Andamento di $R_{11}(x) = R_0(x) + H_{11}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

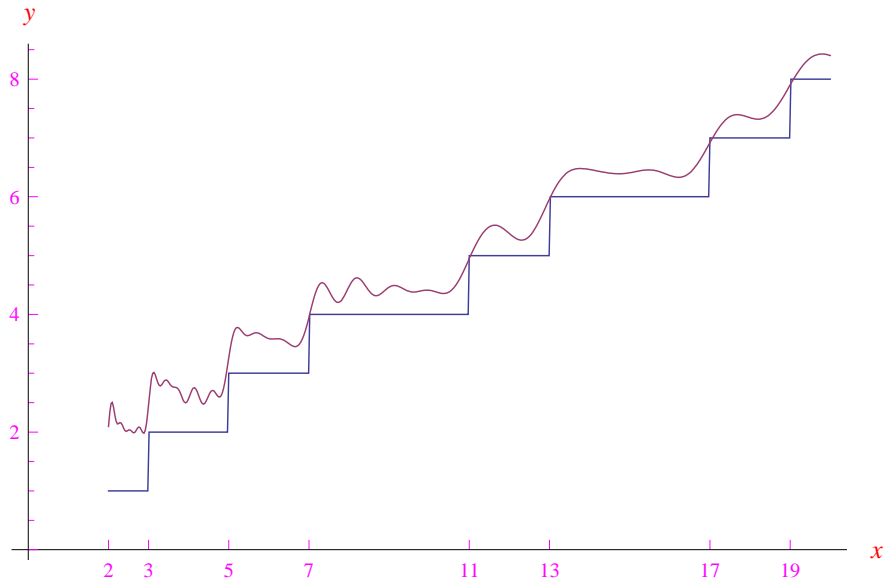


Figura 2.18: Andamento di $R_{15}(x) = R_0(x) + H_{15}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

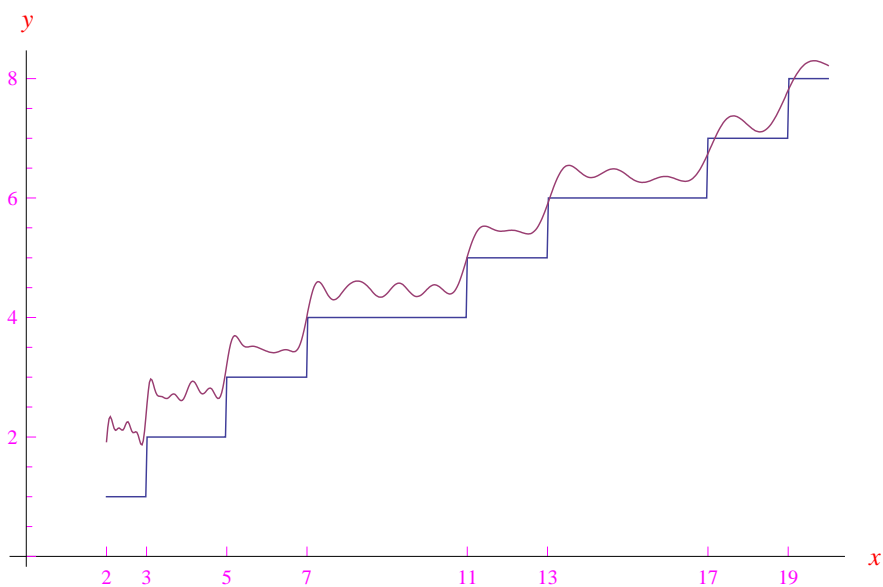


Figura 2.19: Andamento di $R_{18}(x) = R_0(x) + H_{18}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

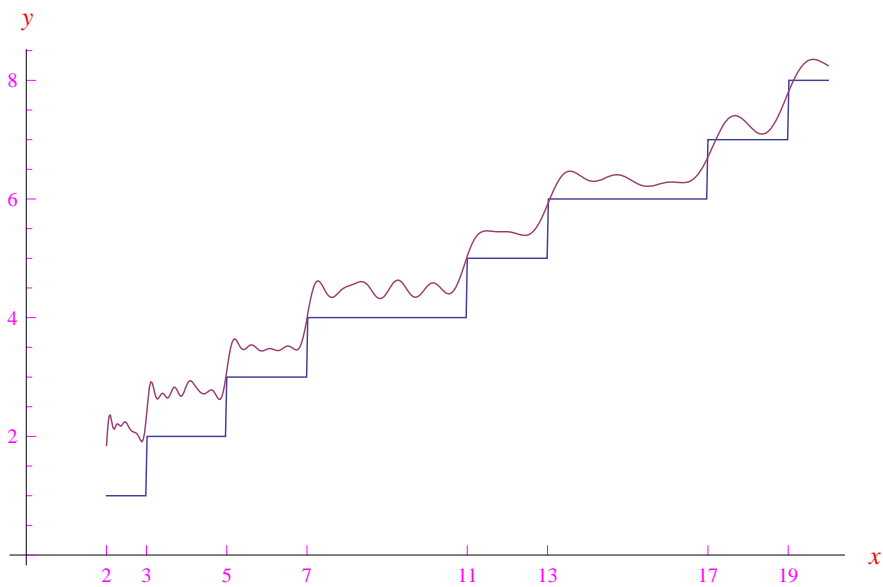


Figura 2.20: Andamento di $R_{19}(x) = R_0(x) + H_{19}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

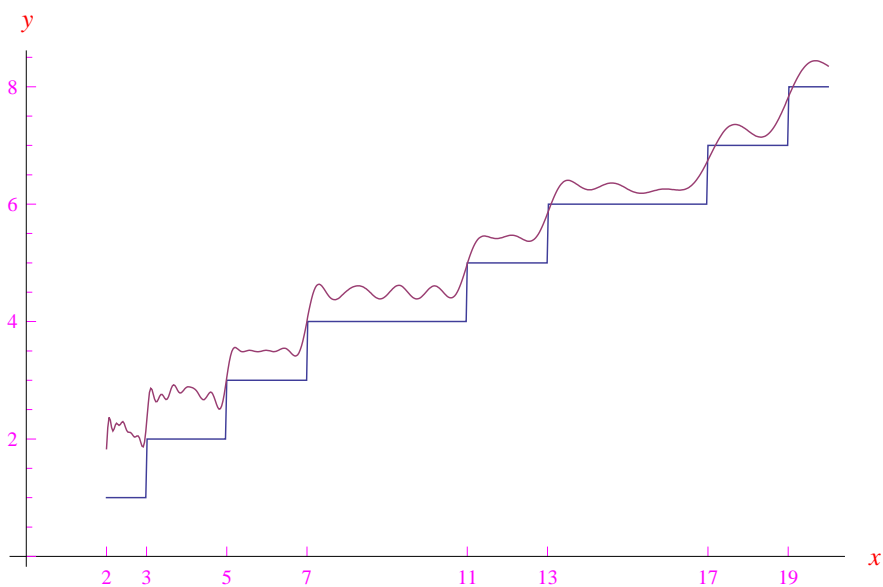


Figura 2.21: Andamento di $R_{20}(x) = R_0(x) + H_{20}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

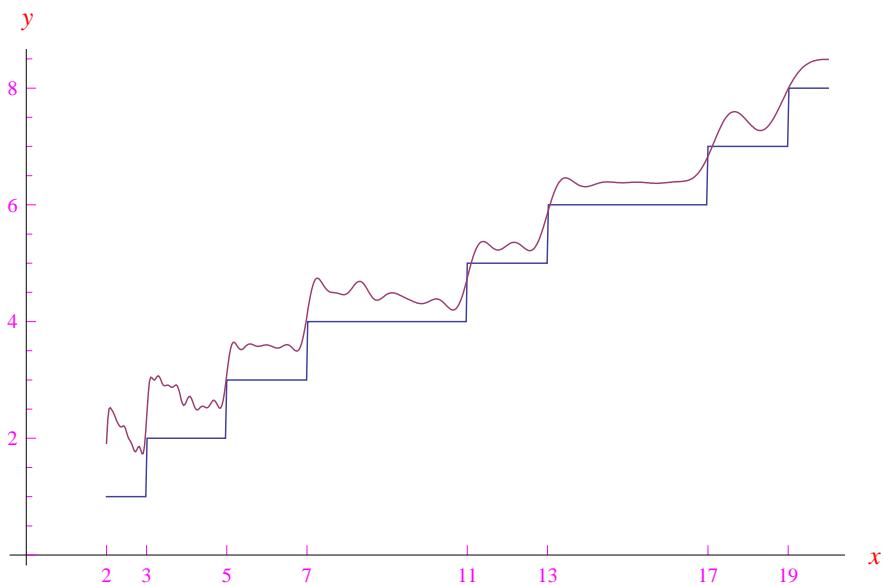


Figura 2.22: Andamento di $R_{25}(x) = R_0(x) + H_{25}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

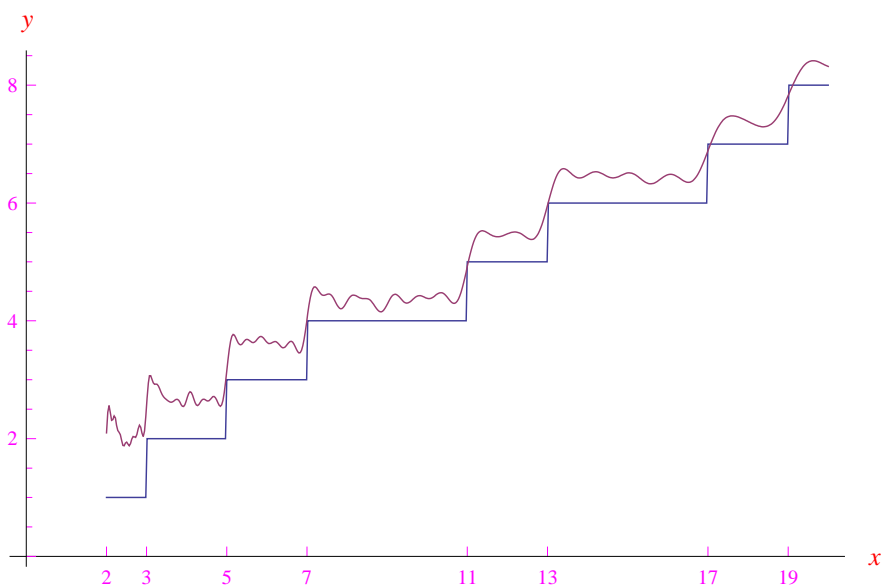


Figura 2.23: Andamento di $R_{30}(x) = R_0(x) + H_{30}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

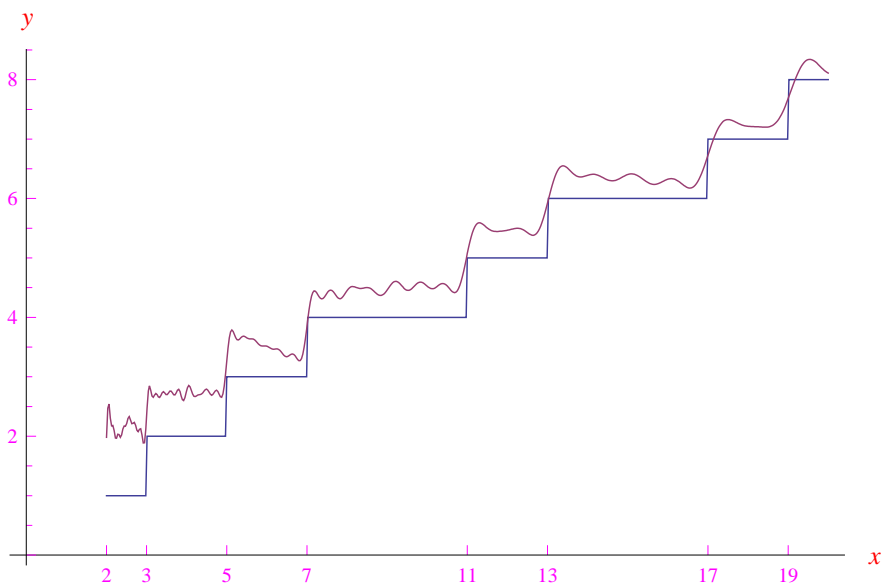


Figura 2.24: Andamento di $R_{35}(x) = R_0(x) + H_{35}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

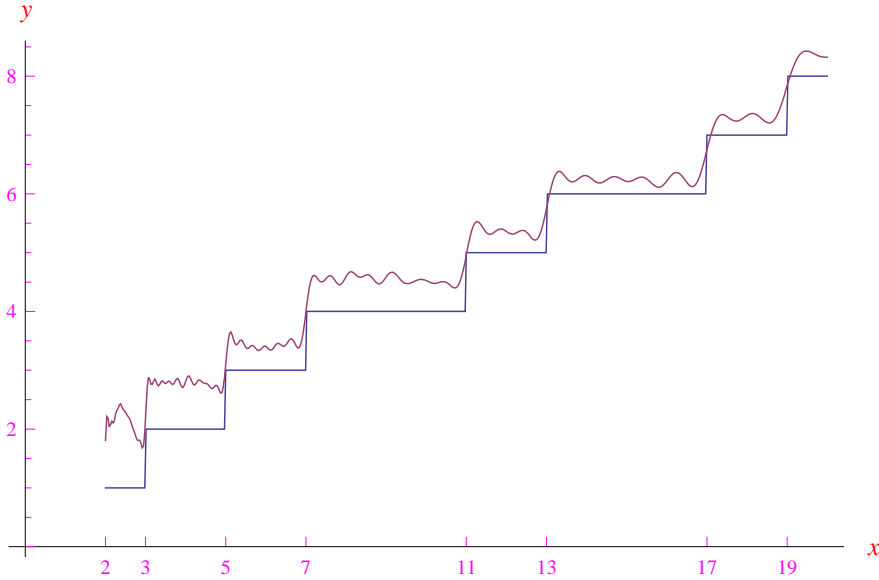


Figura 2.25: Andamento di $R_{40}(x) = R_0(x) + H_{40}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

2.2 Analisi locale

Abbiamo visto che l'espressione esatta della funzione di distribuzione $\pi_0(x)$ è:

$$\pi_0(x) = R_0(x) + H(x), \tag{2.15}$$

dove i termini a secondo membro sono stati studiati nei numeri precedenti. Chiediamoci: qual'è la differenza tra $\pi_0(x)$ e la funzione $\pi(x)$? Rammentiamo innanzitutto che assegnato un numero primo p_m dove m è un intero naturale, si ha:

$$\lim_{x \rightarrow p_m^-} \pi(x) = m - 1, \quad \lim_{x \rightarrow p_m^+} \pi(x) = m, \tag{2.16}$$

e

$$\pi(p_m) = m \tag{2.17}$$

Ne consegue che $\pi(x)$ è definita in ogni $x = p_m$, ma è ivi non regolare, risultando convergente a sinistra e a destra, come vediamo dal grafico di fig. 2.29. Secondo [5]-[9] la funzione $\pi_0(x)$ ha una discontinuità di prima specie in ogni $x = p_m$, ma a differenza del caso di $\pi(x)$, si tratta di una **discontinuità simmetrica**:

$$\pi_0(p_m) = \frac{1}{2} \left[\lim_{x \rightarrow p_m^-} \pi(x) + \lim_{x \rightarrow p_m^+} \pi(x) \right] = m - \frac{1}{2} \tag{2.18}$$

o ciò che è lo stesso:

$$\pi_0(p_m) = \pi(p_m) - \frac{1}{2} \tag{2.19}$$

La fig. 2.30 illustra quanto appena scritto, mentre la fig. 2.31 rappresenta il caso

$$\pi_0(3) = \frac{3}{2}, \quad \pi_0(2) = \frac{1}{2}, \tag{2.20}$$

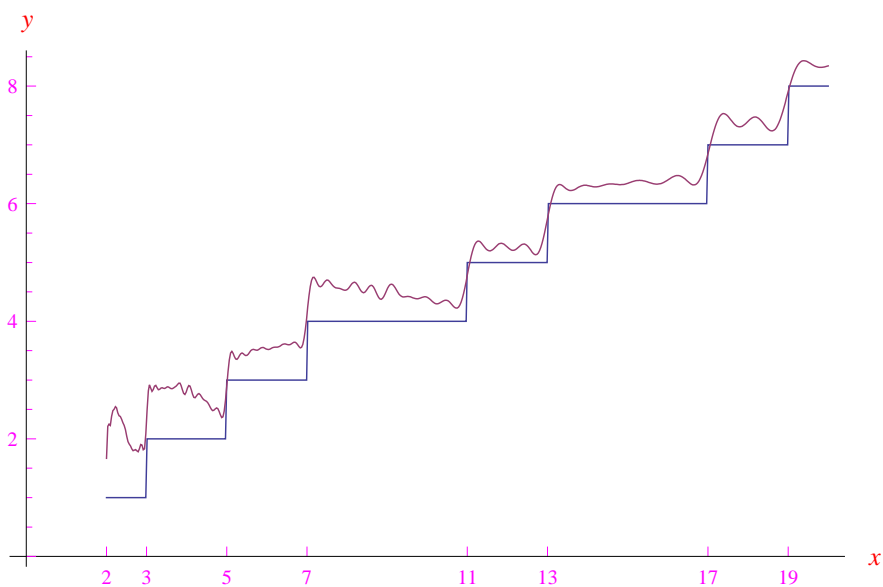


Figura 2.26: Andamento di $R_{45}(x) = R_0(x) + H_{45}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

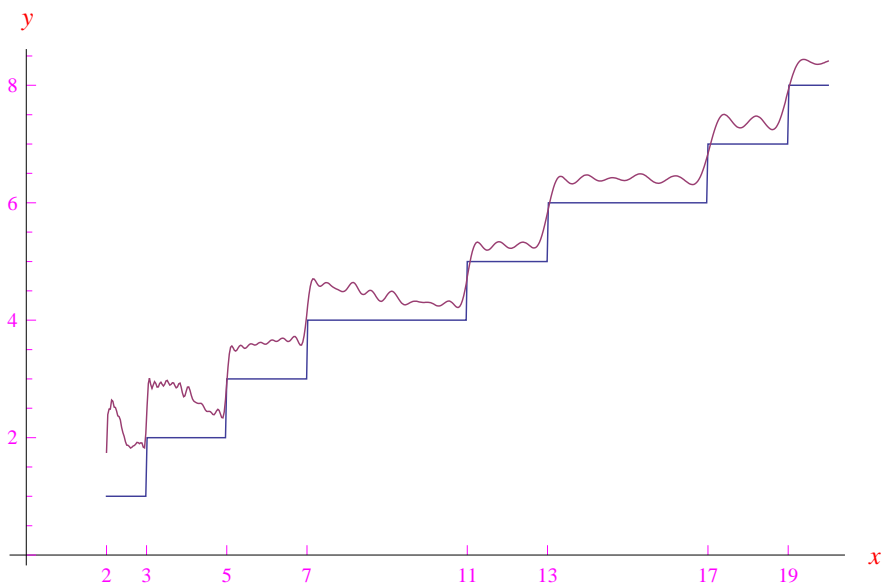


Figura 2.27: Andamento di $R_{48}(x) = R_0(x) + H_{48}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

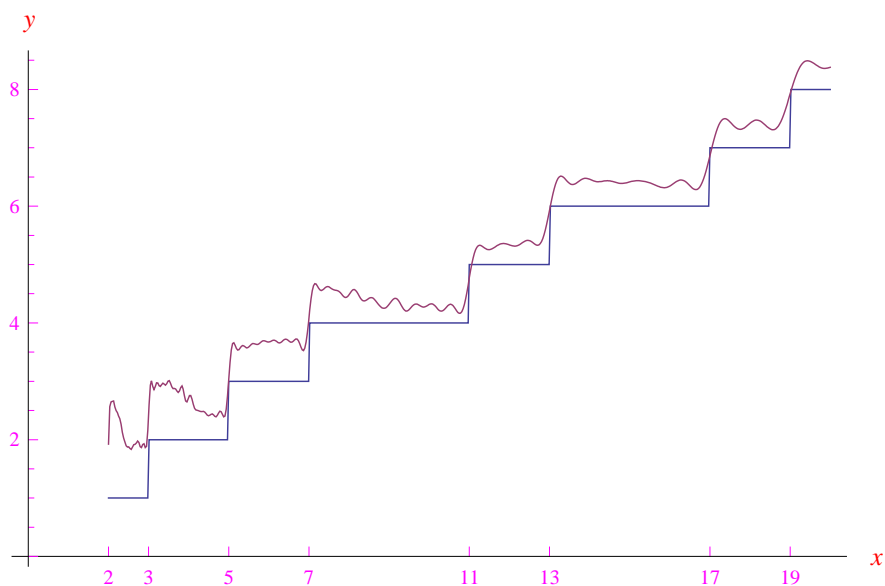


Figura 2.28: Andamento di $R_{50}(x) = R_0(x) + H_{50}(x)$ nell'intervallo $[2, 20]$ confrontato con la distribuzione a gradini $\pi(x)$.

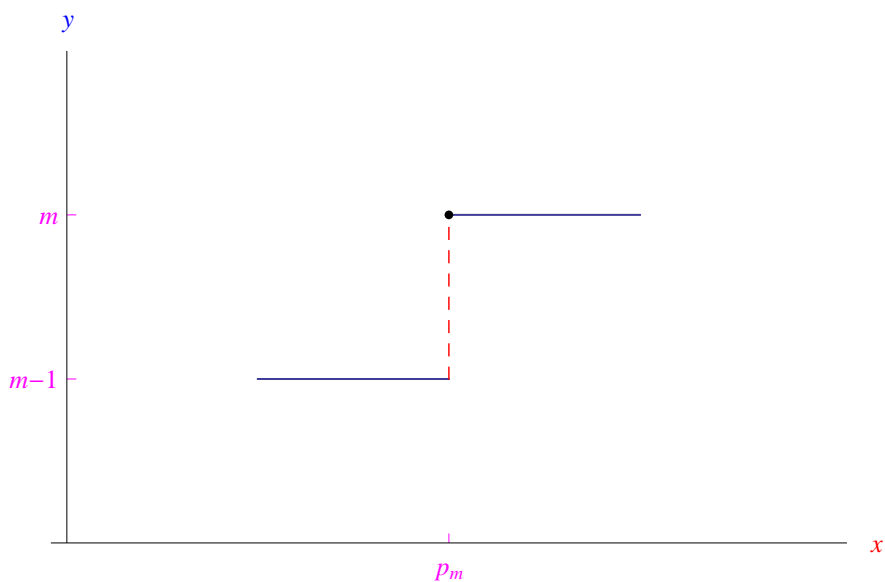


Figura 2.29: Andamento del grafico di $\pi(x)$ in un intorno di un qualunque numero primo p_m . Risulta $\pi(p_m) = m$, ma la funzione non tende ad alcun limite per $x \rightarrow p_m$. Risulta tuttavia convergente a destra e a sinistra di p_m con limiti diversi tra loro.

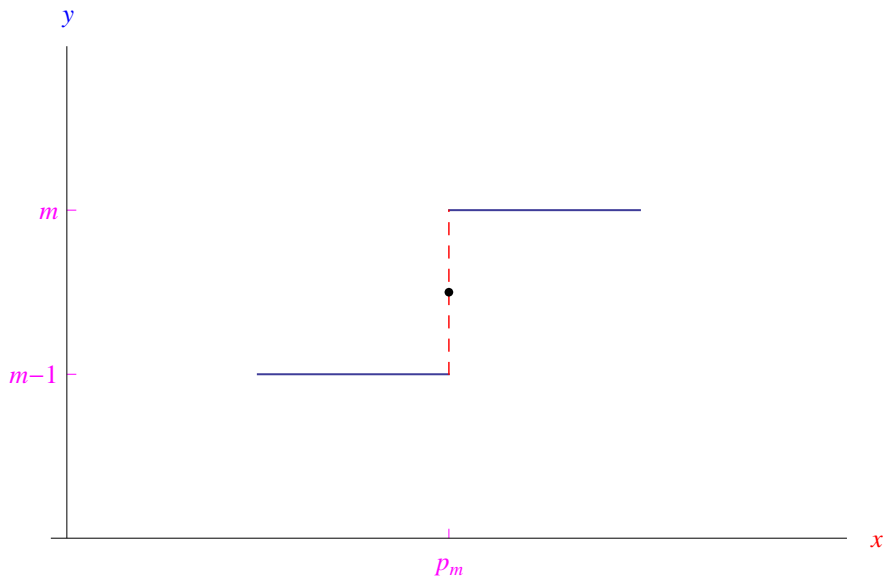


Figura 2.30: Andamento del grafico di $\pi_0(x)$ in un intorno di un qualunque numero primo p_m . Risulta $\pi_0(p_m) = m - \frac{1}{2}$, ma la funzione non tende ad alcun limite per $x \rightarrow p_m$. Risulta tuttavia convergente a destra e a sinistra di p_m con limiti diversi tra loro.

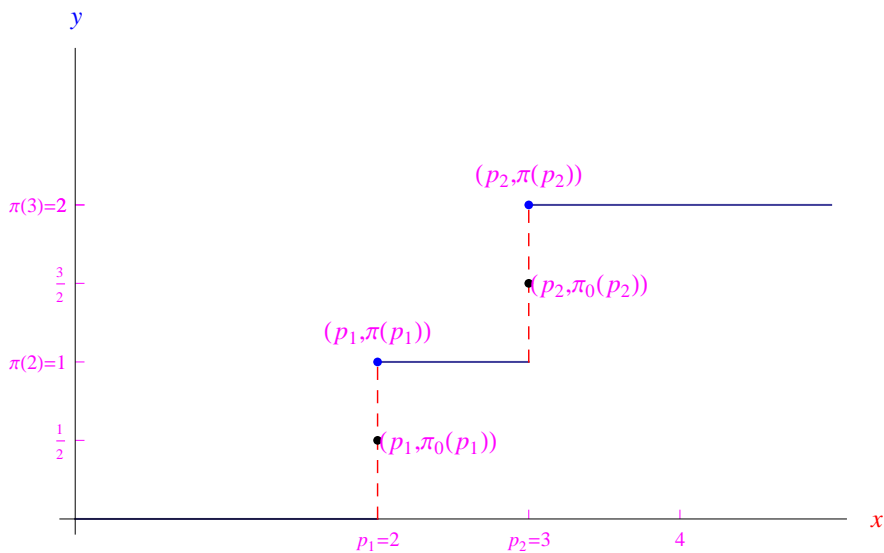


Figura 2.31: La funzione di distribuzione $\pi(x)$ dei numeri primi non è continua in $x = p_n$, ma è ivi definita ed assume il valore $\pi(p_m) = m$. La funzione $\pi_0(x)$ data dalla formula di Riemann – von Mangoldt ha lo stesso andamento a gradini della $\pi(x)$, ma – secondo l’analisi di Riesel e Göhl – in ogni punto di discontinuità assume il valor medio dei limiti destro e sinistro, per cui il grafico passa per il punto medio del segmento che rappresenta il singolo gradino.

Abbiamo eseguito una routine in ambiente *Mathematica* simile alla precedente, con la differenza di aver assegnato un intervallo centrato in $p_{20} = 71$, considerando il contributo proveniente dai primi 100 zeri della funzione zeta. Il risultato è riportato in fig. 2.32. Ci aspettiamo, dunque, un comportamento locale illustrato in fig. 2.33, in cui abbiamo posto:

$$\pi_0^{(N)}(x) \stackrel{def}{=} R_0(x) + \sum_{n=1}^N T_n(x), \tag{2.21}$$

che al crescere indefinito di N determina univocamente la successione di elementi di \mathbb{R} :

$$\left\{ \pi_0^{(N)}(p_m) \right\}_{N \in \mathbb{N} - \{0\}} \tag{2.22}$$

Per quanto precede, tale successione converge a $\pi^{(0)}(p_m) = \pi(p_m) - \frac{1}{2}$:

$$\lim_{N \rightarrow +\infty} \pi_0^{(N)}(p_m) = \pi_0(p_m) = m - \frac{1}{2} \tag{2.23}$$

Per definizione di limite:

$$\forall \varepsilon > 0, \exists \nu_\varepsilon \in \mathbb{N} \mid N > \nu_\varepsilon \implies \left| \pi_0^{(N)}(p_m) - \pi_0(p_m) \right| < \varepsilon \tag{2.24}$$

Per ogni x :

$$\lim_{N \rightarrow +\infty} \pi_0^{(N)}(x) = \pi_0(x)$$

Cioè la successione di funzioni $\left\{ \pi_0^{(N)}(x) \right\}$ converge a $\pi_0(x)$.

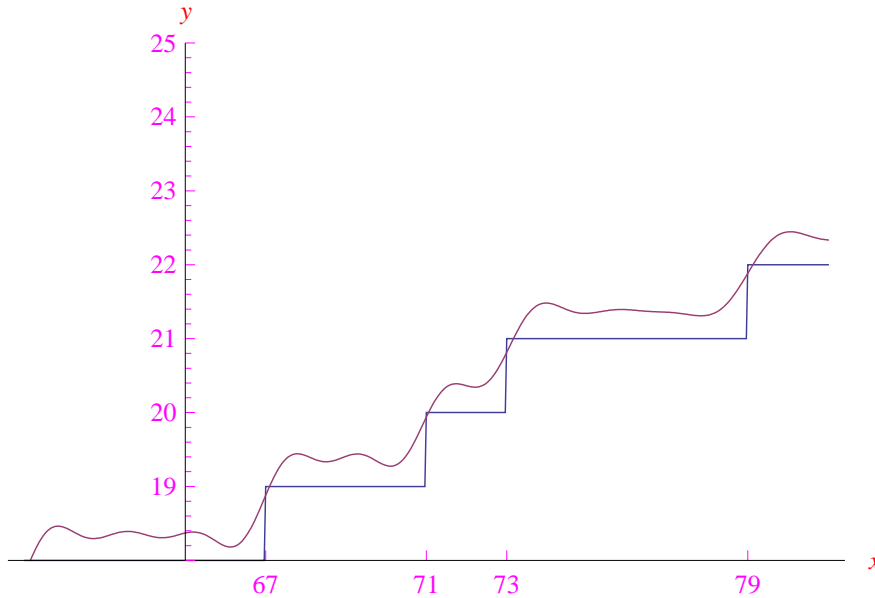


Figura 2.32: Andamento di $\pi_0^{(100)}(x) \stackrel{def}{=} R_0(x) + \sum_{n=1}^{100} T_n(x)$ nell'intervallo $[63, 83]$.

Riprendiamo la (1.92) scrivendola per

$$\rho_n = \left(\frac{1}{2} + \sigma_n \right) + i\alpha_n, \tag{2.25}$$

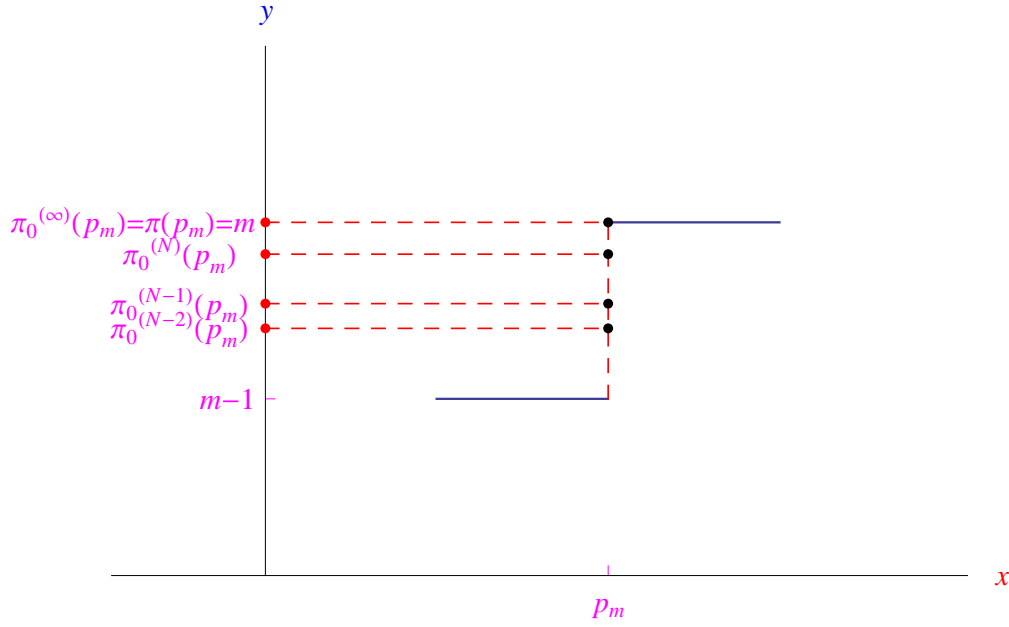


Figura 2.33: Al crescere indefinito dell'ordine di approssimazione N , il punto $(p_n, \pi_0^{(N)}(p_n))$ si avvicina progressivamente a $(p_n, \pi_0(p_n))$.

dove il numero reale σ_n è definito da

$$\sigma_n = \begin{cases} 0, & \text{se la Congettura di Riemann è vera} \\ \neq 0, & \text{altrimenti} \end{cases} \quad (2.26)$$

Riesce:

$$T_n(x) \simeq \frac{1}{|\rho_n| \ln x} \sum_{k=1}^{154} k c_k x^{\frac{1}{2k}(1+2\sigma_n)} \cos\left(\frac{\alpha_n}{k} \ln x - \arg \rho_n\right) \quad (2.27)$$

Con tale approssimazione la disuguaglianza (2.24) diventa:

$$\left| R_0(p_m) - m + \frac{1}{2} + \frac{1}{\ln p_m} \sum_{n=1}^N \frac{1}{|\rho_n|} \sum_{k=1}^{154} k c_k x^{\frac{1}{2k}(1+2\sigma_n)} \cos\left(\frac{\alpha_n}{k} \ln x - \arg \rho_n\right) \right| < \varepsilon, \quad (2.28)$$

che rappresenta un possibile test per la verifica della Congettura di Riemann. Abbiamo considerato la formula approssimata per il termine correttivo $T_n(x)$ al fine di alleggerire il carico computazionale. In linea di principio, si può utilizzare l'espressione esatta, comunque troncata alla somma parziale di ordine $N_0 = 154$:

$$T_n(x) = -2 \sum_{k=1}^{N_0} \frac{\mu(k)}{k} \operatorname{Re} \left[\operatorname{Ei} \left(\frac{\rho_n}{k} \ln x \right) \right], \quad (2.29)$$

con

$$\rho_n = \left(\frac{1}{2} + \sigma_n \right) + i\alpha_n \quad (2.30)$$

Dopo una serie di passaggi:

$$\left| R_0(p_m) - m + \frac{1}{2} - 2 \sum_{n=1}^N \sum_{k=1}^{N_0} \frac{\mu(k)}{k} \operatorname{Re} \left\{ \operatorname{Ei} \left[\frac{1}{2k} (1 + 2\sigma_n) \ln p_m + i \frac{\alpha_n}{k} \ln p_m \right] \right\} \right| < \varepsilon, \quad (2.31)$$

per $N > \nu_\varepsilon$, essendo ν_ε un indice dipendente da $\varepsilon > 0$. Il problema che si apre, volendo testare la congettura di Riemann, consiste nell'assegnare un'espressione a σ_n . Proviamo ad assumere una distribuzione di numeri reali random compresi tra 0 e 1. Ripetendo la routine con Mathematica, troviamo il grafico di fig. 2.34, da cui vediamo che la disuguaglianza precedente viene manifestamente violata.

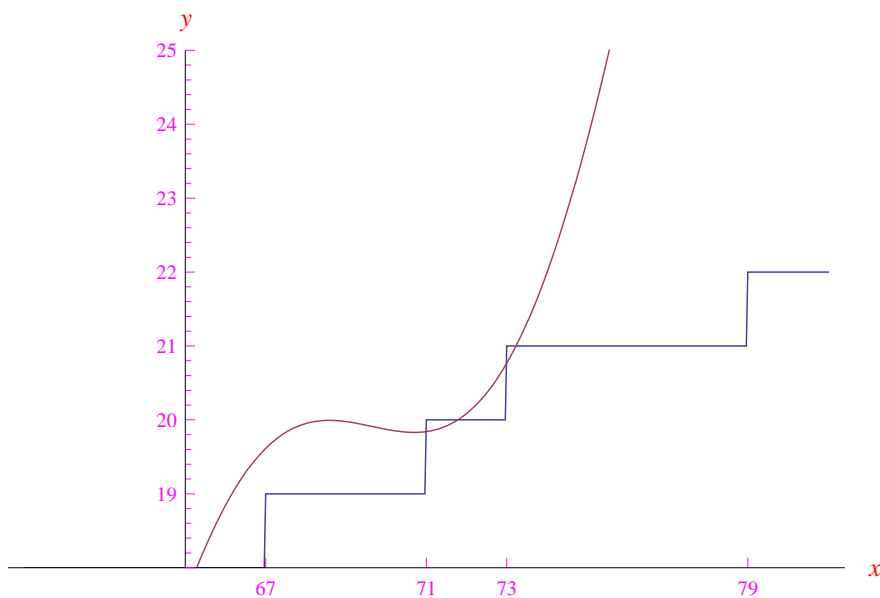


Figura 2.34: Andamento di $\pi_0^{(3)}(x) \stackrel{def}{=} R_0(x) + \sum_{n=1}^3 T_n(x)$ nell'intervallo $[63, 83]$, assumendo non vera la Congettura di Riemann.

Appendice A

La formula di inversione di Möbius e la formula di Riemann – Von Mangoldt

A.1 La funzione di Möbius

Abbiamo visto che la funzione di Möbius è

$$\mu(k) = \begin{cases} (-1)^r, & \text{se } k = \prod_{i=1}^r p_i, \text{ con } p_i \neq p_j, \forall i \neq j, \\ 0, & \text{altrimenti} \end{cases}, \quad (\text{A.1})$$

In realtà tale funzione è generata dalla seguente **serie di Dirichlet** per la reciproca della funzione zeta di Riemann $\zeta(z)$:

$$\frac{1}{\zeta(z)} = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k^z}, \quad (\text{A.2})$$

che converge per $\text{Re } z > 1$ e si annulla in $z = 1$.

A.2 La formula di Riemann – Von Mangoldt

Definiamo la funzione reale della variabile reale x

$$f(x) = \sum_{k=1}^{+\infty} \frac{\pi_0(x^{1/k})}{k}, \quad (\text{A.3})$$

rammentando che

$$\pi_0(x) = \begin{cases} \pi(x), & \text{se } x \neq p_m \\ \pi(x) - \frac{1}{2}, & \text{se } x = p_m \end{cases} \quad (\text{A.4})$$

essendo p_m il primo m -esimo. La (A.3) può essere invertita utilizzando la **formula di inversione di Moebius**, ottenendo

$$\pi_0(x) = \sum_{k=1}^{+\infty} \frac{\mu(k)}{k} f(x^{1/k}) \quad (\text{A.5})$$

La formula di Riemann – Von Mangoldt fornisce un'ottima approssimazione della $f(x)$:

$$f(x) = f_c(x) + f_d(x), \quad x \in [2, +\infty), \quad (\text{A.6})$$

dove

$$f_c(x) = li(x) - \ln 2 + \int_x^{+\infty} \frac{dt}{t(t^2 - 1) \ln t}, \quad f_d(x) = - \sum_{\rho \in B} \text{Ei}(\rho \ln x) \quad (\text{A.7})$$

Bibliografia

- [1] Newman D.J.: *Analytic number theory*, Springer, 1998.
- [2] Vardi I.: *Computational Recreations in Mathematics*, Addison-Wesley, 1991
- [3] Gizzetti A.: *Lezioni di Analisi Matematica*, Veschi, 1971
- [4] von Mangoldt H.: Zu Riemanns Abhandlung “über die Anzahl der Primzahlen unter einer gegebenen Grösse”, *J. Reine Angew. Math.*, v. 114, 1895.
- [5] Riesel R., Göhl G., Some Calculations Related to Riemann’s Prime Number Formula, *Mathematics of Computations*, Vol. 24, N. 112, 1970.
- [6] Fichera G., De Vito L.: *Funzioni analitiche di una variabile complessa*, Veschi, 1987.
- [7] Edwards H.M., *Riemann’s Zeta Function*, Academic Press, New York, 1974
- [8] Riesel H.: *Prime Numbers and Computer Method for Factorization*, Boston, 1985
- [9] Wagon S.: *Guida a Matematica*, McGrawHill, 1995.