This is the last preprint. The final paper will appear in the website `http://matematica.uni-bocconi.it/LangZac/home3.htm`**.**

Intervalli fra numeri primi consecutivi

Alessandro Languasco & Alessandro Zaccagnini

1 Introduzione

L'obiettivo di questo articolo è, a nostro giudizio, piuttosto ambizioso: infatti ci proponiamo di spiegare due importanti risultati della Matematica contemporanea in modo accessibile a tutti, nei limiti del possibile. L'argomento che abbiamo scelto, la distribuzione dei numeri primi ed in particolare le sue irregolarità, ci permette di entrare direttamente *in medias res* senza bisogno di complicati preliminari o definizioni di difficile motivazione.

In un nostro recente annuncio su rete [16] abbiamo parlato molto brevemente di un risultato di questa primavera che riguarda la distanza fra numeri primi consecutivi, nel caso particolare in cui questa è relativamente piccola. Qui vogliamo parlare di questo problema, e del suo "gemello" che riguarda distanze relativamente grandi, in modo piú dettagliato. La strategia che useremo per raggiungere l'obiettivo che ci siamo prefissi illustra bene il procedimento di sviluppo della Matematica, che potremmo chiamare di "accumulazione": partendo da risultati già noti costruiremo le dimostrazioni che ci interessano, seguendo molto da vicino lo sviluppo storico della disciplina. Cercheremo di mostrare come alcune idee possano essere successivamente raffinate dando luogo a risultati sempre piú precisi. Per questo motivo, una parte dei risultati piú significativi è dimostrata in Appendice, per non intralciare il nostro discorso, e una parte è citata senza dimostrazione.

Non sarà possibile dare la dimostrazione dei risultati piú forti oggi noti, ma daremo conto delle idee piú importanti, ed in uno dei due casi il nostro risultato non sarà molto distante dal migliore. Le tecniche di cui parliamo non sono completamente elementari, anche se spesso hanno origine da idee relativamente semplici, come per esempio il Crivello di Eratostene di cui abbiamo parlato nel §5 di [14].

Un vincolo che ci siamo dati per raggiungere il nostro obiettivo è quello dell'onestà, di non "barare" nascondendo le difficoltà come se non esistessero: gli enunciati che daremo, per la maggior parte, sono piuttosto semplici da comprendere: la Teoria dei Numeri, a differenza della maggior parte del resto della Matematica, contiene moltissimi enunciati facilmente comprensibili, ed altri che lo sono con

una modesta fatica. Purtroppo, la Matematica che c'è dietro le dimostrazioni non è sempre banale, e per capirne alcune è necessario un notevole sforzo da parte dei Lettori: ci considereremo soddisfatti se saremo riusciti a rendere comprensibili quantomeno i meccanismi delle dimostrazioni, tralasciando i dettagli piú tecnici.

In un certo senso, chiediamo ai nostri Lettori un atteggiamento simile a quello che si tiene quando si legge un libro di fantascienza, che qualche volta si chiama "sospensione dell'incredulità": supponendo che i viaggi interstellari siano possibili, quali conseguenze ne derivano? Dando per buoni alcuni risultati, che descriveremo e commenteremo nei dettagli qui sotto, quali conseguenze possiamo trarne? La differenza fondamentale è che, nel nostro caso, i Lettori interessati potranno studiare anche le dimostrazioni di tutti i risultati che qui ci limitiamo a enunciare, operazione faticosa ma estremamente interessante, mentre non è molto probabile che possano cimentarsi in viaggi interstellari ... In ogni caso, riteniamo che sia una operazione tutt'altro che banale anche comprendere la struttura delle dimostrazioni che descriveremo.

2 Congetture sulle irregolarità nella distribuzione dei numeri primi

2.1 Il Teorema dei Numeri Primi

Uno dei piú importanti risultati nella distribuzione dei numeri primi riguarda la stima asintotica del numero di primi minori o uguali di un certo parametro grande x. Questo teorema (comunemente noto come Teorema dei Numeri Primi, che abbrevieremo con TNP) fu enunciato da Gauss, che ne intuí la validità basandosi sull'analisi di tabelle di primi da lui stesso prodotte, e fu dimostrato per la prima volta indipendentemente da Hadamard e de la Vallée-Poussin nel 1896. Esso rappresenta uno dei piú importanti successi della tecnica analitica proposta da Riemann nel 1858 in un articolo che è oggigiorno identificato come fondativo della disciplina della Teoria Analitica dei Numeri ed in cui è apparsa per la prima volta la funzione di una variabile complessa che ora viene chiamata "funzione ζ di Riemann".[1]

Fino al 1950 circa si è ritenuto che il Teorema dei Numeri Primi non fosse dimostrabile senza fare uso dell'analisi complessa. Tale opinione fu smentita da Erdős e Selberg che, indipendentemente, fornirono una dimostrazione alternativa che non fa uso di tali metodi e che per tale ragione viene chiamata "elementare" (ma che per questo non è da ritenersi "facile"). Tralasciando l'analisi delle tecniche dimostrative, diamo l'enunciato e cerchiamo di capire la rilevanza di questo

[1] Per la precisione, anche Eulero l'aveva usata ma solo per valori reali dell'argomento.

risultato: ne abbiamo parlato anche nel §5 di [14]. Definita la funzione

$$\pi(x) = |\{p \leq x,\ p \text{ è primo}\}|$$

che "conta" i primi fino a $\lfloor x \rfloor$, il TNP si può esprimere in questo modo:

$$\lim_{x \to +\infty} \frac{\pi(x) \log x}{x} = 1.$$

Usualmente si introduce la notazione $f(x) \sim g(x)$ (che si legge "f è asintotico a g") per indicare che $\lim_{x \to +\infty} f(x)/g(x) = 1$; si veda l'Appendice C per maggiori dettagli sulla definizione dei simboli che si usano per indicare l'equivalenza asintotica di funzioni. In tal modo il Teorema dei Numeri Primi si può esprimere nella seguente forma compatta:

$$\pi(x) \sim \frac{x}{\log x}. \tag{1}$$

Sebbene per i nostri scopi l'enunciato (1) sia sufficiente, esiste una versione piú precisa del TNP in cui la funzione $x/\log x$ è sostituita dalla funzione "logaritmo integrale" definita da

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}.$$

È stato dimostrato che $\mathrm{li}(x)$ è una approssimazione migliore a $\pi(x)$ di quanto sia $x/\log x$, ossia che, per x sufficientemente grande, si ha

$$|\pi(x) - \mathrm{li}(x)| \leq \left| \pi(x) - \frac{x}{\log x} \right|.$$

Osserviamo inoltre che il primo termine dello sviluppo asintotico di $\mathrm{li}(x)$ è dato da $x/\log x$, come si può vedere nell'Appendice E.1, e che quindi si può effettivamente pensare all'uso di $\mathrm{li}(x)$ come di un "raffinamento" dell'enunciato (1) del TNP.

Evidentemente, visto che contiene l'operazione di limite, il TNP fornisce solamente un andamento asintotico per $\pi(x)$ nel caso x diventi arbitrariamente grande. È chiaro dunque che l'affermare, grazie al TNP, che la "probabilità" che un intero scelto casualmente sia primo sia pari a $1/\log x$ e, di conseguenza, che sia ragionevole aspettarsi che esista un primo ogni $\log x$ interi circa, ha solamente un significato euristico. Infatti l'esistenza del valore limite di una successione non implica che la successione stessa debba essere regolarmente distribuita nelle vicinanze di tale valore. Si vedano i §§2.3 e 3.1.

Se invece di probabilità si parla piuttosto di densità, allora questa affermazione può essere resa rigorosa. Infatti, se $h \leq x$ è abbastanza grande rispetto a $\log x$, allora nell'intervallo $[x, x+h]$ ci sono $\sim h/\log x$ numeri primi. In effetti, questo è l'enunciato originale di Gauss, che lo ha portato a congetturare il PNT nella forma

$\pi(x) \sim \mathrm{li}(x)$ che risulta piú accurata, dal punto di vista puramente numerico, della relazione (1).

Nasce quindi spontaneamente la domanda se esistano o meno sottosuccessioni di primi consecutivi di grandezza circa uguale a x aventi tra loro distanza minore o maggiore della distanza media attesa ossia di $\log x$: si veda anche la (2). Attualmente è nota l'esistenza di sottointervalli di $[1,x]$ piú lunghi di $\log x$ e privi di numeri primi e, molto recentemente, è stato dimostrato che esistono sottointervalli di $[x,2x]$, significativamente piú corti di $\log x$, che contengono due numeri primi. Nei paragrafi successivi tratteremo in dettaglio alcune idee utilizzabili per capire come si possono dimostrare risultati di questo tipo.

Supponiamo ora di numerare i primi in ordine crescente; allora $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$,... Chiameremo quindi p_n l'n-esimo primo della successione stessa. Un'immediata conseguenza della (1), che in realtà è un enunciato equivalente come dimostriamo nell'Appendice E.2, è la seguente relazione asintotica:

$$p_n \sim n \log n. \tag{2}$$

Prima di dimostrare le relazioni tra (1) e (2) osserviamo che quest'ultima "suggerisce" senza implicare (provate a trovare il perché) che $p_{n+1} - p_n \approx (n+1)\log(n+1) - n\log n \sim \log n$. Ciò giustifica ulteriormente quanto abbiamo scritto poco sopra riguardo la ricerca di primi in intervalli di lunghezza $\log x$.

Per dimostrare che (1) implica (2), osserviamo per prima cosa che da (1) segue $\log(\pi(x)) \sim \log x - \log\log x$ e quindi, visto che $\log\log x = o(\log x)$, si ottiene $\log(\pi(x)) \sim \log x$. Ricordiamo che con la scrittura $f(x) = o(g(x))$ denotiamo il fatto che che $\lim_{x\to+\infty} f(x)/g(x) = 0$: si veda l'Appendice C.

Per definizione si ha che $\pi(p_n) = n$ e, dalla relazione precedente, segue che $\log n = \log(\pi(p_n)) \sim \log p_n$. Allora la relazione (1) si può scrivere nella forma $n \sim p_n/\log p_n \sim p_n/\log n$ che equivale a (2). La dimostrazione dell'effettiva equivalenza tra (1) e (2) è analoga, e si trova nell'Appendice E.2.

La (2) consente di conoscere che tipo di grandezza può avere l'n-esimo primo; in particolare essa implica che per ogni $\varepsilon \in (0,1)$ esiste n_ε tale che

$$(1-\varepsilon)n\log n \le p_n \le (1+\varepsilon)n\log n$$

per $n \ge n_\varepsilon$. Visto che non è specificato il valore di n_ε la disequazione precedente non è molto utile nel caso sia necessario avere stime in intervalli espliciti. D'altra parte sono state dimostrate anche disuguaglianze piú accurate di questa: per esempio, negli anni 30 del ventesimo secolo Rosser ha dimostrato che per $n > 1$ si ha

$$n\log n + n(\log\log n - 10) \le p_n \le n\log n + n(\log\log n + 8). \tag{3}$$

Esistono anche stime piú precise per $n \ge n_0$ (esplicito): si veda per esempio [19, p. 249], e si noti anche che la minorazione in (3) è rilevante solo per $n \ge 2780$.

Notiamo infine un risultato equivalente al Teorema dei Numeri Primi nella forma data in (1):

$$\log P(x) \sim x, \qquad \text{dove} \qquad P(x) = \prod_{p \leq x} p. \tag{4}$$

Si faccia attenzione a non cadere in inganno e a concludere che da (4) segua $P(x) \sim e^x$, che è, tra l'altro, una relazione certamente falsa! È immediato osservare che la funzione $\log P(x)$ può essere espressa come $\sum_{p \leq x} \log p$, chiamata funzione $\theta(x)$ di Chebyshev. La presenza del "peso" $\log p$ nella somma consente una maggiore flessibilità rispetto alla definizione della funzione $\pi(x)$ e permette l'uso di strumenti analitici piú sofisticati quale, per esempio, tutta la tecnica analitica complessa. L'equivalenza tra (1) e (4) si dimostra mediante la formula di somma per parti: si veda l'Appendice D.1.

2.2 La Congettura dei Primi Gemelli

Nel paragrafo precedente abbiamo discusso brevemente la problematica relativa a quanto il TNP può "predire" sulla distanza tra due numeri primi consecutivi ed essenzialmente abbiamo detto che molto poco può essere predetto. Parliamo ora di alcune congetture sulla distribuzione di tali distanze.

È evidente analizzando già i primi elementi della sequenza dei numeri primi dispari che ne esistono alcuni che hanno distanza minimale (cioè 2) ed altri che invece hanno distanza maggiore. Per esempio $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$ sono coppie di primi che hanno distanza minimale. Nulla impedisce però che esistano coppie di numeri primi consecutivi con distanza maggiore; per esempio, la coppia $(13,17)$ ha distanza pari a 4. Per conoscere quale sia la distanza piú grande nota, consigliamo di consultare il sito di T. Nicely `http://www.trnicely.net/gaps/gaplist.html` in cui sono raccolte molte informazioni sui record di distanze fra primi consecutivi. Attualmente la distanza maggiore nota è 337446 che si trova nelle vicinanze di un primo avente 7996 cifre decimali (e che è troppo lungo per poter essere riportato qui ...).

D'ora in poi chiameremo *primi gemelli* due numeri primi dispari la cui distanza è 2; quindi $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$ sono tutti primi gemelli. Tale denominazione è stata usata per la prima volta da Paul Stäckel nei primi anni del ventesimo secolo, ma era già ben noto l'enunciato di una famosa congettura sulla loro distribuzione che al giorno d'oggi non è né dimostrata né confutata:

Congettura 2.1 (dei Primi Gemelli) *Esistono infiniti primi gemelli.*

La coppia di primi gemelli piú grande nota è formata da $33218925 \cdot 2^{169690} \pm 1$; questi interi hanno 51090 cifre decimali.

Molti sono stati i tentativi di provare a dimostrare la Congettura dei Primi Gemelli 2.1; tra essi ricordiamo i lavori del matematico finlandese Viggo Brun del 1919-20 [2, 3, 4] in cui, partendo dal crivello di Eratostene, modernizzò il concetto di crivello dando inizio a quella che oggigiorno è nota come Teoria dei Crivelli, e la serie di lavori di Hardy e Littlewood [10, 11] (anni 20-30) in cui essi posero le basi del Metodo del Cerchio, un metodo analitico per studiare molti problemi additivi in teoria dei numeri tra cui anche la distribuzione dei primi gemelli.

Nel §4 citeremo un risultato di Brun che fornisce una maggiorazione per il numero di primi gemelli minori di un parametro X e, nel §4.1, dimostreremo un altro teorema di Brun sulla convergenza della serie

$$\sum_{\substack{p \text{ primo tale che} \\ p+2 \text{ sia primo}}} \frac{1}{p}. \tag{5}$$

L'intento originario di Brun era quello di dimostrare che tale serie fosse divergente perché in tal modo egli avrebbe dimostrato la correttezza della Congettura dei Primi Gemelli 2.1, in analogia con fatto che la divergenza della serie $\sum_p p^{-1}$ implica l'esistenza di infiniti numeri primi; si veda l'Appendice A. Purtroppo Brun fallí nel suo intento, ma le conseguenze del suo tipo di approccio furono notevoli: è sufficiente dire che la dimostrazione di Goldston-Pintz-Yıldırım [7] a cui facciamo riferimento in [16] è basata su un moderno metodo di crivello sviluppato da A. Selberg negli anni '50 del secolo scorso.

Una prima generalizzazione della Congettura dei Primi Gemelli 2.1 è quella di chiedersi se esistono infinite terne di primi del tipo $(n, n+2, n+4)$. In questo caso è sufficiente studiare le classi residuali modulo 3 di $n, n+2, n+4$ per accorgersi che l'unica possibile soluzione è $(3,5,7)$. Allora possiamo provare a vedere se esistono soluzioni per $(n, n+2, n+6)$; facendo qualche verifica al calcolatore ci accorgiamo immediatamente che esistono 259 primi $p < 10^5$ tali che $p+2$ e $p+6$ siano entrambi primi. Usualmente questo problema viene chiamato ricerca di *costellazioni di primi*: dati $k+1$ interi distinti $b_0 = 0, \ldots, b_k$, esistono infiniti primi p tali che $p+b_0, \ldots, p+b_k$ siano simultaneamente primi? Dagli esempi precedenti è chiaro che dovranno essere imposte delle condizioni sugli interi $b_0, \ldots, b_k$ per evitare di cadere in casi analoghi a quello $(n, n+2, n+4)$. Per distinguere questi casi osserviamo che, se per qualcuno dei primi $p \leq k+1$ accade che $\{b_0 \pmod p, \ldots, b_k \pmod p\} = \{0, \ldots, p-1\}$, allora gli interi $p = p+b_0, \ldots, p+b_k$ possono essere simultaneamente primi per al piú un unico valore di p. Equivalentemente è chiaro che possiamo studiare le classi di resto modulo p degli interi $m+b_0, \ldots, m+b_k$, con $0 \leq m \leq p-1$. In questo modo calcoliamo tutte le possibili classi di resto; notiamo inoltre che eseguiamo comunque un numero finito di verifiche perché $0 \leq m \leq p-1$, $p \leq k+1$ e la $k+1$-upla $b_0 = 0, \ldots, b_k$ è fissata.

Ad esempio, nel caso $(3,5,7)$ in cui $b_0 = 0, b_1 = 2, b_2 = 4$, posto $p = 3$ i resti di $m, m+2, m+4$ per $m = 0,1,2$ sono rispettivamente $\{0,2,1\}$, $\{1,0,2\}$ o $\{2,1,0\}$. In questa situazione diciamo che $b_0, \ldots, b_k$ è una *costellazione non ammissibile*. Nel caso in cui, per tutti i $p \leq k+1$ almeno un resto modulo p non compaia, diciamo che $b_0, \ldots, b_k$ è una *costellazione ammissibile*. Nel caso $(n, n+2, n+6)$ si ha $b_0 = 0, b_1 = 2, b_2 = 6$; con $p = 2$ i resti di $m, m+2, m+6$ per $m = 0,1$ sono tutti 0 o tutti 1 e con $p = 3$ i resti di $m, m+2, m+6$ per $m = 0,1,2$ sono rispettivamente $\{0,2,0\}$, $\{1,0,1\}$, oppure $\{2,1,2\}$.

L'analogo della Congettura dei Primi Gemelli 2.1 sarà dunque quello di dire che, data una costellazione ammissibile $(b_0, \ldots, b_k)$, il numero di primi p per cui anche $p + b_1, \ldots, p + b_k$ siano primi sia infinito. Chi è curioso può consultare [22] dove c'è un'argomentazione in sostegno della congettura delle costellazioni e vari tabelle relative al confronto fra il numero calcolato di costellazioni e quello "previsto" dalla formula euristica. Altre argomentazioni si possono trovare in Hardy & Wright [12, §22.20] ed in Pólya [18].

Generalizzando ulteriormente la Congettura dei Primi Gemelli 2.1 potremmo chiederci sotto quali condizioni i k numeri $a_1 n + b_1, a_2 n + b_2, \ldots, a_k n + b_k$, in cui $a_i, b_i \in \mathbb{Z}$, $i = 1, \ldots, k$ sono simultaneamente primi. La situazione descritta per i primi gemelli ricade nel caso $k = 2$, $a_1 = a_2 = 1$, $b_1 = 0$ e $b_2 = 2$. Nel caso in cui $k = 1$, abbiamo invece il problema della distribuzione dei numeri primi nella progressione aritmetica di ragione a_1 e resto b_1. Tale problema, a cui abbiamo accennato in [15], è stato risolto da Dirichlet; egli, assumendo la validità della naturale ipotesi $(a_1, b_1) = 1$, ha provato che esistono infiniti primi della forma $a_1 n + b_1$ (si veda [15, Teorema 3.1]).

È chiaro dunque che nella generalizzazione dovremo avere $(a_i, b_i) = 1$, $i = 1, \ldots, k$ e che $a_i > 0$, $i = 1, \ldots, k$ (altrimenti una delle k condizioni diviene banale ed il problema equivarrebbe ad un problema su $k-1$ numeri). Inoltre è necessario supporre che per ogni primo $p \leq k$ esista almeno un n per cui $p \nmid a_i n + b_i$, per ogni $i = 1, \ldots, k$. Quest'ultima ipotesi va inserita per eliminare il caso "esistono infiniti n per cui n e $n+1$ siano entrambi primi?" ($k = 2$, $a_1 = a_2 = 1$, $b_1 = 0$, $b_2 = 1$ ed il primo 2 è minore o uguale a k e certamente divide uno tra n e $n+1$) ed i casi analoghi. La generalizzazione della Congettura dei Primi Gemelli 2.1 e del teorema di Dirichlet sui primi nelle progressioni aritmetiche assume quindi la forma

Congettura 2.2 (delle k-uple, Dickson 1904) *Siano $a_i, b_i \in \mathbb{Z}$, $i = 1, \ldots, k$, tali che ogni $a_i > 0$ ed ogni $(a_i, b_i) = 1$. Inoltre, per ogni primo $p \leq k$ esista almeno un n per cui $p \nmid a_i n + b_i$, per ogni $i = 1, \ldots, k$. Allora esistono infiniti $n \in \mathbb{N}$ per cui $a_i n + b_i$ è primo per ogni $i = 1, \ldots, k$.*

Anche la congettura delle k-uple non è stata né provata né confutata. Si conoscono

maggiorazioni per il numero di $n \leq X$ che la verificano, dove X è un parametro "grande", le cui dimostrazioni sono basate anch'esse su metodi di crivello.

2.3 La Congettura di Cramér

Negli anni 30 del ventesimo secolo, il matematico svedese Harald Cramér escogitò un ragionamento euristico in base al quale sostenne che ci si può aspettare che per infiniti valori dell'intero n si ha

$$\frac{p_{n+1} - p_n}{(\log p_n)^2} \approx 1, \tag{6}$$

e che il rapporto a primo membro non sia mai significativamente piú grande di cosí. Non è facilissimo spiegare esattamente come Cramér abbia potuto immaginare una cosa del genere: ha usato alcuni risultati di teoria della probabilità che non possiamo introdurre in questa sede senza una lunga digressione. In un certo senso, però, possiamo descrivere il suo risultato in questo modo: consideriamo l'insieme $\mathfrak{A}$ di tutte le successioni di interi positivi che soddisfano il Teorema dei Numeri Primi nella forma (1), cioè gli insiemi $A \subset \mathbb{N}$ tali che $|A \cap [1,N]| \sim N/\log N$ quando $N \to +\infty$. Cramér ha dimostrato che un "tipico" elemento di $\mathfrak{A}$ ha la proprietà data qui sopra nella relazione (6); da questo però non è possibile dedurre nulla a proposito di un *singolo elemento* dell'insieme $\mathfrak{A}$. Allo stesso modo, non è possibile affermare che una ben determinata famiglia vive in una casa di proprietà solo perché la "tipica" famiglia italiana vive in una casa di proprietà, o che una certa famiglia abbia 1.6 bambini perché nella "tipica" famiglia ci sono 1.6 bambini. In altre parole, non è evidentemente possibile attribuire a *tutti* i membri di una certa classe una certa proprietà solo perché questa risulta essere tipica dell'elemento "medio" della classe.

Ma, probabilmente, la critica piú severa che sia stata rivolta alla Congettura di Cramér è la seguente: per il "tipico" elemento A di $\mathfrak{A}$ non vale la Congettura dei Primi Gemelli 2.1 nella forma enunciata qui sopra, perché si trovano infinite coppie di elementi di A che distano esattamente 1, cosa che certamente non accade per l'insieme $\mathfrak{P}$ di tutti i numeri primi. La famiglia considerata da Cramér rispecchia solo proprietà analitiche e non quelle aritmetiche dei numeri primi: sono quindi state proposte alcune modifiche, nelle quali si sceglie una famiglia $\mathfrak{A}' \subset \mathfrak{A}$ di successioni che "somigliano" ai numeri primi anche in qualche aspetto aritmetico e non solo nella proprietà di densità espressa dal Teorema dei Numeri Primi (1). Per esempio, ricordando il fatto che un intero $n \geq 2$ è primo se e solo se non è divisibile per nessun intero nell'intervallo $[2, \sqrt{n}]$, è stato proposto di considerare le successioni che, oltre a verificare il Teorema dei Numeri Primi nel senso spiegato qui sopra, sono costituite di interi che non hanno nessun divisore "piccolo" a parte, ovviamente, 1. Abbiamo messo piccolo fra virgolette per sottolineare il

fatto che deve essere inteso in senso relativo all'intero preso in considerazione, e non in senso assoluto.

Il risultato finale è che la costante 1 che compare nella Congettura di Cramér è stata sostituita, da qualche autorevole matematico, con la costante $2e^{-\gamma} \approx 1.123$, e c'è chi addirittura ritiene che la stessa cosa valga con una costante arbitrariamente grande al posto di 1. Purtroppo i grandi intervalli fra numeri primi consecutivi sono cosí rari che è difficile ottenere "verifiche" numeriche dell'attendibilità di queste congetture, perché le differenze previste sono solo dell'ordine del 12%.

Le successioni di $\mathfrak{A}$ *non* soddisfano (tipicamente) il Teorema dei Numeri Primi nelle Progressioni Aritmetiche (si veda il [15, Teorema 3.1]). Torneremo a parlare della classe delle successioni introdotta da Cramér nel §3.1.

3 Conseguenze del Teorema dei Numeri Primi

Come prima cosa vogliamo dimostrare che il Teorema dei Numeri Primi implica che, fissato a piacere il numero $\varepsilon > 0$, la disuguaglianza

$$\frac{p_{n+1} - p_n}{\log p_n} \geq 1 - \varepsilon \tag{7}$$

vale per infiniti valori di n. Infatti, se questa disuguaglianza valesse solo per un numero *finito* di valori dell'indice n, allora dovrebbe esistere un intero n_0 per il quale $p_{n+1} - p_n \leq \delta \log p_n$ per tutti gli $n \geq n_0$, con $\delta = 1 - \varepsilon$. Per N abbastanza grande si ponga $p_n = \max\{p\colon p < N\}$ e $p_m = \min\{p\colon p > 2N\}$. Si osservi che $p_m - p_n \geq N$. Allora per la (1) si ha

$$\sum_{j=n}^{m-1} \frac{p_{j+1} - p_j}{\log p_j} \leq \sum_{j=n}^{m-1} \delta = \delta(\pi(2N) - \pi(N)) \sim \delta \frac{N}{\log N}.$$

D'altra parte si ha anche $p_j \leq 2N$ per $j < m$, e quindi

$$\sum_{j=n}^{m-1} \frac{p_{j+1} - p_j}{\log p_j} \geq \sum_{j=n}^{m-1} \frac{p_{j+1} - p_j}{\log(2N)} = \frac{p_m - p_n}{\log(2N)} \geq \frac{N}{\log(2N)} \sim \frac{N}{\log N}.$$

Per N sufficientemente grande queste due relazioni sono incompatibili, e quindi *non è possibile* che il rapporto $(p_{n+1} - p_n)/\log p_n$ sia $\leq \delta$ per tutti gli indici n da un certo punto in poi. In altre parole, questo rapporto deve essere $\geq 1 - \varepsilon$ per infiniti valori di n. Si veda il §5.1 per una dimostrazione alternativa dello stesso risultato.

Si noti che, *mutatis mutandis*, la stessa argomentazione mostra che, per ogni $\varepsilon > 0$, la disuguaglianza

$$\frac{p_{n+1} - p_n}{\log p_n} \leq 1 + \varepsilon \tag{8}$$

vale per infiniti valori dell'indice n.

3.1 Successioni per cui vale il Teorema dei Numeri Primi

Torniamo a parlare dell'insieme di successioni $\mathfrak{A}$ introdotto da Cramér, per le quali vale il Teorema dei Numeri Primi. L'obiettivo di questo paragrafo è mostrare che la sola proprietà caratteristica delle successioni di questo insieme non è sufficiente ad analizzare le proprietà di irregolarità di cui ci stiamo occupando. Per esempio, consideriamo la successione $a_n = \lfloor n \log n \rfloor$, per cui $a_{n+1} - a_n \sim \log n \to \infty$. In questo caso, evidentemente, non vale la Congettura dei Primi Gemelli: infatti, dato $k \in \mathbb{N}$ con $k > 0$, l'equazione $a_n - a_m = k$ ha solo un numero finito di soluzioni. Per esercizio, si dimostri la stessa cosa per la successione dei quadrati perfetti: si dimostri cioè che $n^2 - m^2 = k$ ha un numero finito di soluzioni, che può dipendere da k, per ogni k fissato. Piú in generale, si dimostri che se (a_n) è una successione di interi tale che $a_{n+1} - a_n \to +\infty$, allora l'equazione $a_n - a_m = k$ ha solo un numero finito di soluzioni. (Suggerimento: se $a_{n_0+1} - a_{n_0} > k$, le eventuali soluzioni di $a_n - a_m = k$ hanno $m < n < n_0$).

Viceversa, per la successione b_n definita da $b_n = a_n$ quando n non è un quadrato perfetto, e $b_n = b_{n-1} + 2$ se n è un quadrato perfetto, vale ancora il Teorema dei Numeri Primi ed esistono infiniti valori di n per cui $b_{n+1} - b_n = 2$, cioè vale l'analogo della Congettura dei Primi Gemelli 2.1.

Il Teorema dei Numeri Primi da solo non può dunque essere sufficiente a dimostrare che esistono coppie di primi "vicine" o "lontane," ma solamente i risultati che abbiamo dimostrato sopra nelle (7) e (8). È chiaro che i due esempi qui sopra possono essere modificati in molti modi, per costruire successioni α_n che soddisfano il Teorema dei Numeri Primi, ma per cui il comportamento di $\alpha_{n+1} - \alpha_n$ per un insieme poco denso di valori di n è sostanzialmente arbitrario.

La morale che ne traiamo è questa: il Teorema dei Numeri Primi è un risultato di "regolarità" di distribuzione dei primi, mentre noi cerchiamo comportamenti "eccezionali," cioè deviazioni dal comportamento medio. Ci aspettiamo che queste deviazioni dalla media capitino per infiniti valori dell'indice n, ma che siano cosí poco frequenti da non essere in grado di influenzare il comportamento medio della successione.

4 Intervalli piccoli fra numeri primi consecutivi

Dedichiamo questa sezione ad esporre un risultato non banale sull'esistenza di intervalli piccoli tra numeri primi consecutivi.

Cosa intendiamo per piccoli intervalli? Il Teorema dei Numeri Primi nella forma (2), suggerisce che $p_{n+1} - p_n$ sia di solito (ossia per la maggior parte degli interi n) dello stesso ordine di grandezza di $\log n$ che, a sua volta non differisce molto da $\log p_n$; d'altra parte esso non fornisce alcuna evidenza del fatto che ta-

le distanza possa anche essere occasionalmente molto piú piccola, anche se ciò dovrebbe accadere piuttosto raramente.

Un metodo naturale per studiare l'esistenza di piccole distanze tra primi consecutivi è dunque quello di valutare la quantità

$$E = \liminf_{n\to+\infty} \frac{p_{n+1} - p_n}{\log p_n} \tag{9}$$

al fine di capire se l'ampiezza $p_{n+1} - p_n$ possa essere minore di $\log p_n$ per infiniti valori di n. Ricordiamo che la definizione del *minimo limite* o liminf di una successione a_n è la seguente

$$\liminf_{n\to+\infty} a_n = \lim_{n\to+\infty} \inf_{k\geq n} a_k,$$

ed osserviamo che il Teorema dei Numeri Primi implica che $E \leq 1$ (si veda §3, equazione (8)) mentre la Congettura dei Primi Gemelli 2.1 implica che $E = 0$, perché in questo caso il numeratore della frazione in (9) varrebbe 2 per infiniti valori di n, mentre il denominatore ha limite $+\infty$.

La storia dei progressi nello studio di E contiene nomi che appartengono al Gotha della Matematica:

1926: $E \leq 2/3$ (Hardy e Littlewood, assumendo la validità dell'Ipotesi di Riemann Generalizzata);

1940: $E < 1$ (Erdős);

1966: $E \leq 1/2$ e in seguito $E \leq 0.46650\ldots$ (Bombieri e Davenport);

1977: $E \leq 0.44254\ldots$ (Huxley);

1986: $E \leq 0.2486\ldots$ (Maier).

Recentemente (maggio 2005) però, D. Goldston, J. Pintz e C. Yıldırım [7] hanno dimostrato un importante teorema, e cioè che

$$E = 0.$$

La dimostrazione può essere scaricata liberamente dall'indirizzo web: `http://xxx.sissa.it/abs/math.NT/0508185`.

Una versione semplificata di questo risultato (che però richiede comunque strumenti di crivello moderni e tecniche di integrazione di funzioni di due variabili complesse) scritta da Y. Motohashi [6] può anch'essa essere scaricata liberamente dall'indirizzo web: `http://xxx.sissa.it/abs/math/0505300`.

Ma che cosa significa il risultato in questione? $E = 0$ vuol dire che per ogni $\varepsilon > 0$ esistono infiniti n tali che $p_{n+1} - p_n \leq \varepsilon \log p_n$. In tal modo è evidente che questo teorema può essere considerato un importante passo verso la dimostrazione della Congettura dei Primi Gemelli 2.1.

Non possiamo qui sviluppare quanto serve per dimostrare che $E = 0$, ma ci accontentiamo di provare che $E < 1$ seguendo la dimostrazione di Erdős [5]. Anche per questo scopo limitato non possiamo però dare una dimostrazione completa perché ci serve una maggiorazione per il numero di primi che distano tra loro di una quantità $h \in \mathbb{N}$, dove $h \geq 2$. A tale scopo definiamo la funzione

$$\pi_h(X) = \sum_{\substack{p \leq X \text{ primo tale che} \\ p+h \text{ sia primo}}} 1 = |\{p \leq X : p \text{ primo e } p+h \text{ primo}\}|$$

che conta il numero di primi p minori o uguali di un parametro X per cui anche $p+h$ è primo.

La maggiorazione che ci servirà è contenuta nel seguente

Teorema 4.1 (Brun, si veda Theorem 2.3.2 di [8] o Theorem 3.11 di [9]) *Esiste una costante $C_1 > 0$ tale che, se $X \in \mathbb{N}$ è un parametro arbitrariamente grande, per ogni $h \in \mathbb{N}$ con $h \geq 2$ si ha che*

$$\pi_h(X) \leq C_1 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|h \\ p>2}} \left(\frac{p-1}{p-2}\right) \frac{X}{\log^2 X}. \tag{10}$$

Il Teorema 4.1 è stato dimostrato per la prima volta da Brun negli anni venti (come risultato fondamentale per studiare la convergenza della serie in (5)) ed in seguito ridimostrato da Schnirelmann [20] negli anni trenta mediante un argomento di crivello combinatorico. Attualmente lo sviluppo delle tecniche di crivello consente di ottenere (10) come conseguenza di teoremi piú generali. Purtroppo lo sviluppo della teoria necessaria a fornire in questa sede la dimostrazione del Teorema 4.1 va al di là dello scopo di queste note. Chi vuole approfondire questi argomenti può fare riferimento al recente libro di Greaves [8] o a quello di Halberstam-Richert [9] (quest'ultimo, purtroppo, oramai fuori stampa).

Nell'enunciato del Teorema 4.1 è presente una caratteristica costante detta *costante dei primi gemelli*: il prodotto infinito sui primi $\prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$. Affermiamo che tale prodotto infinito è una costante perché se ne può dimostrare la convergenza. Per alcuni elementi della teoria della convergenza dei prodotti infiniti si veda l'Appendice E.3.

Si ritiene che l'ordine della stima (10) sia essenzialmente corretto. In effetti, G.H. Hardy e J.E. Littlewood [10] nel 1923 hanno congetturato, nel caso h pari,

che il corretto ordine di grandezza asintotico di $\pi_h(X)$ per $X \to +\infty$ sia

$$\pi_h(X) \sim 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|h \\ p>2}} \left(\frac{p-1}{p-2}\right) \frac{X}{\log^2 X}. \tag{11}$$

L'enunciato (11), detto *Congettura Forte dei Primi Gemelli*, evidentemente implica la validità della Congettura 2.1 ed è anch'esso ancora al di là delle attuali conoscenze. Esiste anche una formulazione asintotica per la congettura delle k-uple che implica la validità della Congettura 2.2.

Peraltro la Congettura dei Primi Gemelli 2.1 seguirebbe anche da stime estremamente piú deboli come $\pi_2(X) \geq f(X)$, dove f è una *qualsiasi* funzione che tende all'infinito per $X \to +\infty$; anche questo problema è attualmente fuori portata.

Passiamo ora a dimostrare il

Teorema 4.2 (Erdős [5]) *$E < 1$.*

Come accennavamo precedentemente, un ingrediente fondamentale per dimostrare il Teorema 4.2 è il Teorema 4.1 di Brun. Prima di dimostrare il Teorema 4.2 valutiamo la media per h "vicino" a $\log X$ del prodotto sui divisori primi di h presente nel Teorema 4.1.

Lemma 4.3 *Sia $a > 0$ una costante sufficientemente piccola. Allora esiste una costante $0 < c_1 < (6C)^{-1}$ tale che*

$$\sum_{(1-a)\log X \leq h \leq (1+a)\log X} \prod_{\substack{p|h \\ p>2}} \left(\frac{p-1}{p-2}\right) \leq c_1 \log X, \tag{12}$$

dove $C = C_1 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$ e C_1 è la costante presente nel Teorema 4.1.

Dim. Osserviamo per prima cosa che

$$\prod_{\substack{p|h \\ p>2}} \left(\frac{p-1}{p-2}\right) \leq 3 \prod_{\substack{p|h \\ p>2}} \left(\frac{p+1}{p}\right). \tag{13}$$

Infatti, siccome $(n-1)n/((n-2)(n+1)) \geq 1$ per ogni $n > 2$, si ottiene che

$$\begin{aligned} \prod_{\substack{p|h \\ p>2}} \left(\frac{(p-1)p}{(p-2)(p+1)}\right) &\leq \prod_{3 \leq p \leq h} \left(\frac{(p-1)p}{(p-2)(p+1)}\right) \\ &\leq \prod_{3 \leq n \leq h} \left(\frac{(n-1)n}{(n-2)(n+1)}\right) \leq 3\frac{h-1}{h+1} \leq 3, \end{aligned} \tag{14}$$

in cui il penultimo passaggio viene dimostrato scrivendo tutti i prodotti e svolgendo le necessarie semplificazioni, oppure per induzione.

Allora

$$\prod_{\substack{p|h\\p>2}}\left(\frac{p-1}{p-2}\right)\leq 3\prod_{\substack{p|h\\p>2}}\left(1+\frac{1}{p}\right)=3\sum_{\substack{d|h\\d>2}}\frac{\mu^2(d)}{d}, \tag{15}$$

dove $\mu(d)$ è la funzione di Möbius (si veda [15, Definizione B.3]). L'ultima relazione è un'applicazione della formula di Möbius (si veda il Teorema F.2). Osservando ora che $\mu^2(n)\in\{0,1\}$ per ogni n, possiamo dunque scrivere

$$\sum_{(1-a)\log X\leq h\leq(1+a)\log X}\prod_{\substack{p|h\\p>2}}\left(\frac{p-1}{p-2}\right)\leq 3S, \tag{16}$$

in cui abbiamo definito

$$S:=\sum_{(1-a)\log X\leq h\leq(1+a)\log X}\sum_{\substack{d|h\\d>2}}\frac{1}{d}.$$

Dobbiamo quindi fornire una maggiorazione per S. In questo caso, la nostra strategia è quella di invertire l'ordine tra le due somme. Ponendo pertanto $h=dl$, possiamo scrivere la somma piú interna nel modo seguente

$$\sum_{\substack{d|h\\d>2}}\frac{1}{d}=\sum_{\substack{dl=h\\d>2}}\frac{1}{d}.$$

Scambiamo adesso l'ordine delle somme; la piú esterna è quindi una somma su d e la piú interna una somma su l. Osserviamo che la somma piú esterna dovrà variare nell'intervallo $(1-a)\log X\leq d\leq(1+a)\log X$ mentre la piú interna ha l'intervallo di variazione dato da $((1-a)\log X)/d\leq l\leq((1+a)\log X)/d$. Abbiamo così trasformato il nostro problema nel dover maggiorare la quantità

$$\sum_{\substack{(1-a)\log X\leq d\leq(1+a)\log X\\d>2}}\frac{1}{d}\sum_{((1-a)\log X)/d\leq l\leq((1+a)\log X)/d}1.$$

Chiaramente la somma piú interna indica ora il numero di interi compresi nell'intervallo $[((1-a)\log X)/d,((1+a)\log X)/d]$ ed un facile calcolo dimostra che esso è al piú

$$\begin{aligned}\left\lfloor\frac{(1+a)\log X}{d}\right\rfloor-\left\lfloor\frac{(1-a)\log X}{d}\right\rfloor+1&\leq\frac{(1+a)\log X}{d}-\frac{(1-a)\log X}{d}+2\\&=\frac{2a}{d}\log X+2.\end{aligned}$$

Pertanto, sfruttando quanto abbiamo appena scritto, otteniamo

$$S \leq \sum_{\substack{(1-a)\log X \leq d \leq (1+a)\log X \\ d>2}} \frac{1}{d}\left(\frac{2a}{d}\log X + 2\right).$$

Visto che gli addendi di quest'ultima somma sono tutte quantità positive, la possiamo maggiorare semplicemente rilassando le condizioni sull'intervallo di variabilità di d. Abbiamo così che

$$S \leq 2a\log X \sum_{\substack{d \leq (1+a)\log X \\ d>2}} \frac{1}{d^2} + \sum_{\substack{d \leq (1+a)\log X \\ d>2}} \frac{2}{d}.$$

Osserviamo che la prima somma è una somma parziale della serie convergente $\sum_{d=3}^{+\infty} 1/d^2$ e quindi la maggioriamo con quest'ultima; inoltre utilizziamo la relazione (35) sulla seconda somma. In tal modo otteniamo finalmente che

$$S \leq 2a\log X \sum_{d=3}^{+\infty} \frac{1}{d^2} + 2\log((1+a)\log X) + 2 \leq c_2 \log X, \tag{17}$$

dove $c_2 = c_2(a) > 0$ è un'opportuna costante.

Possiamo adesso concludere la dimostrazione del Lemma 4.3. Infatti per la (16) e la (17) sappiamo che esso è vero ponendo $c_1 = 3c_2$. Inoltre, analizzando la dipendenza di c_2 da a, è immediato osservare che, per $a \to 0^+$, c_2 può essere reso arbitrariamente piccolo e, di conseguenza, anche c_1 può essere reso tale. In conclusione, per a sufficientemente piccolo, si ottiene $3c_2 = c_1 < (6C)^{-1}$. □

A questo punto ci siamo procurati tutti gli strumenti necessari per "attaccare" la dimostrazione Teorema 4.2.

Dim. del Teorema 4.2. Chiaramente cercheremo di sfruttare il Lemma 4.3 per ottenere la dimostrazione del Teorema 4.2 ossia per verificare che $E < 1$. Dobbiamo per prima cosa fissare qualche notazione e fare un paio di ragionamenti preliminari.

Sia $X > 2$ un parametro e siano $p_1, \ldots, p_m$ i primi contenuti nell'intervallo $(X/2, X]$. Grazie al Teorema dei Numeri Primi nella forma (1) sappiamo che, fissato $\varepsilon > 0$, si ha

$$m > (\frac{1}{2} - \varepsilon)\frac{X}{\log X}, \tag{18}$$

per X sufficientemente grande. Proveremo, per X sufficientemente grande, che

$$\text{esiste } i \in \{1, \ldots, m-1\} \text{ tale che } p_{i+1} - p_i < (1-a)\log X \tag{19}$$

perché, in tal caso, segue che

$$\liminf_{n\to+\infty}\frac{p_{n+1}-p_n}{\log p_n}\leq\lim_{X\to+\infty}\frac{(1-a)\log X}{\log(X/2)}.$$

Quindi, siccome per $X\to+\infty$ il termine di destra tende a $(1-a)$, otteniamo $E\leq(1-a)$ da cui discende $E<1$ visto che, nel Lemma 4.3, $a>0$ è una costante sufficientemente piccola non meglio quantificabile.

Passiamo quindi a dimostrare la (19). Definiamo $\Delta_i=p_{i+1}-p_i$ per ogni $i\in\{1,\dots,m-1\}$. Abbiamo già visto nel paragrafo §3 come debbano esistere infinite soluzioni a $(p_{n+1}-p_n)/\log p_n\leq 1+\varepsilon$ altrimenti si otterrebbe una contraddizione. Cerchiamo ora di raffinare questo tipo di ragionamento osservando che in questo caso $\log p_n\approx\log X$ e facendo vedere che se tali distanze fossero tutte piú grandi di $(1-a)\log X$ con $a\in(0,1)$, avremmo che l'intervallo $(X/2,X]$ sarebbe troppo "piccolo" per contenere tutti i suoi primi. È per questo che nel Lemma 4.3 abbiamo stimato il contributo degli h "vicini" a $\log X$.

Contiamo immediatamente la distanza massima tra due primi che appartengono a $(X/2,X]$. Chiaramente abbiamo

$$p_m-p_1=\sum_{i=1}^{m-1}\Delta_i\leq\frac{X}{2}. \tag{20}$$

Contiamo ora i Δ_i "vicini" a $\log X$. Definiamo

$$\mathcal{A}=\{i\in\{1,\dots,m-1\}:(1-a)\log X\leq\Delta_i\leq(1+a)\log X\}$$

e $N_1=|\mathcal{A}|$. Il numero di Δ_i "lontani" da $\log X$ sarà dato allora da $N_2=m-1-N_1$. È anche immediato notare che $m=N_1+N_2+1=\pi(X)-\pi(X/2)$.

Purtroppo non possiamo calcolare esattamente N_1 ma, mediante il Lemma 4.3, siamo in grado di maggiorarlo. Infatti in tal modo abbiamo, scrivendo con $\sum'$ la somma sugli h per cui $(1-a)\log X\leq h\leq(1+a)\log X$, che

$$N_1\leq\sum{}'1\leq\sum{}'\left(C\prod_{\substack{p\mid h\\ p>2}}\left(\frac{p-1}{p-2}\right)\frac{X}{\log^2 X}\right)\leq c_1C\frac{X}{\log X}.$$

Procediamo ora per assurdo. Se la (19) non avesse soluzione, allora si avrebbe che $\Delta_i\geq(1-a)\log X$ per ogni $i=1,\dots,m-1$. Mostriamo adesso che allora l'intervallo $(X/2,X]$ sarebbe troppo "piccolo" per contenere tutti i suoi primi. Infatti

$$\begin{aligned}\sum_{i=1}^{m-1}\Delta_i&=\sum_{\substack{i=1\\ \Delta_i\in\mathcal{A}}}^{m-1}\Delta_i+\sum_{\substack{i=1\\ \Delta_i\notin\mathcal{A}}}^{m-1}\Delta_i\geq N_1(1-a)\log X+N_2(1+a)\log X\\ &\geq(c_1C\frac{X}{\log X})(1-a)\log X+\left[N_1+N_2-c_1C\frac{X}{\log X}\right](1+a)\log X.\end{aligned} \tag{21}$$

L'ultima disequazione si ottiene dalla precedente sommando e sottraendo la quantità $N_1 2a\log X + c_1 C(1+a)X$. Siccome $m-1 = N_1 + N_2$, per (18) e (21), si ottiene

$$\begin{aligned} p_m - p_1 = \sum_{i=1}^{m-1} \Delta_i &> X c_1 C(1-a) + X(\frac{1}{2} - \varepsilon - c_1 C)(1+a) - (1+a)\log X \\ &= X(\frac{1}{2} + a(\frac{1}{2} - \varepsilon - 2c_1 C) - \varepsilon) - (1+a)\log X > \frac{X}{2}, \end{aligned} \tag{22}$$

per X sufficientemente grande e perché $c_1 C < 1/6$ ed ε può essere scelto sufficientemente piccolo.

La dimostrazione si conclude osservando che (22) è in contraddizione con (20) e quindi l'ipotesi che (19) non avesse soluzione è falsa. Deve pertanto esistere almeno un intervallo tra primi consecutivi appartenenti a $(X/2, X]$ che è "piccolo" ossia la (19) è verificata. Ciò implica, come abbiamo già visto, che $E < 1$ ossia la tesi del Teorema 4.2. □

4.1 Convergenza della serie di Brun

In (5) abbiamo definito la serie dei reciproci dei primi gemelli ed abbiamo accennato al fatto che essa è convergente. Proviamo ora quest'ultimo fatto. Ci servirà una forma debole del Teorema 4.1 cioè il fatto che esista una costante $K > 0$ tale che

$$\pi_2(X) \leq K \frac{X}{\log^2 X}. \tag{23}$$

Osserviamo inoltre che nella scrittura

$$\sum_{\substack{p \text{ primo tale che} \\ p+2 \text{ sia primo}}} \frac{1}{p} \tag{24}$$

consideriamo solo il primo elemento della coppia dei primi gemelli. Ciò non comporta alcun problema perché l'unico primo che compare sia come primo che come secondo termine di una coppia di primi gemelli è 5 (come abbiamo già fatto notare nel §2.2 è sufficiente verificare che l'unica terna di primi della forma $(n, n+2, n+4)$ è $(3,5,7)$ studiando le classi di resto modulo 3 di n, $n+2$, $n+4$). Inoltre, notando che

$$\frac{1}{p} < \frac{1}{p} + \frac{1}{p+2} < \frac{2}{p},$$

otteniamo, per il criterio del confronto delle serie a termini non negativi, che la convergenza di (24) equivale alla convergenza della serie

$$\sum_{\substack{p \text{ primo tale che} \\ p+2 \text{ sia primo}}} \left(\frac{1}{p} + \frac{1}{p+2}\right) \tag{25}$$

la cui formulazione rende piú evidente il fatto che stiamo sommando su *tutti* i primi gemelli (e stiamo contando due volte il 5, ma questo non costituisce un problema per la convergenza).

Il valore limite della serie (25) viene chiamato *costante di Brun*.

Dimostriamo adesso la convergenza di (24). Se la Congettura dei Primi Gemelli 2.1 fosse falsa (ossia esistesse solamente un numero finito di primi gemelli) allora la serie in questione sarebbe in realtà una somma finita e non avremmo nulla da dimostrare. Supponiamo dunque che esistano infiniti primi gemelli e enumeriamoli: sia q_r l'r-esimo primo gemello. Allora abbiamo che

$$r = \pi_2(q_r) \leq K\frac{q_r}{\log^2 q_r} < K\frac{q_r}{\log^2(r+1)}$$

perché $q_r > r+1$ per ogni $r \in \mathbb{N}$. Allora, passando ai reciproci, si ottiene

$$\frac{1}{q_r} < K\frac{1}{r\log^2(r+1)}.$$

Pertanto possiamo concludere che

$$\sum_{\substack{p \text{ primo tale che} \\ p+2 \text{ sia primo}}} \frac{1}{p} = \sum_{r=1}^{+\infty} \frac{1}{q_r} < K\sum_{r=1}^{+\infty} \frac{1}{r\log^2(r+1)}$$

e, visto che la serie nel termine piú a destra è convergente, abbiamo, per il criterio del confronto delle serie a termini non negativi, che anche la serie in (24) è convergente cosí come quella in (25).

5 Intervalli grandi fra numeri primi consecutivi

Qui mostriamo come, raffinando successivamente la stessa idea, si riescano a trovare risultati sempre piú forti: si noti però che per ottenere ciascun risultato diventa necessario avere sempre qualche informazione supplementare rispetto al caso precedente. Nel primo caso ci servirà la formula di Stirling, nel secondo una delle forme del Teorema dei Numeri Primi, nel terzo un risultato piuttosto forte sulla distribuzione dei numeri che non hanno fattori primi "grandi."

5.1 Esistono lunghi intervalli senza numeri primi

La dimostrazione tradizionale dell'esistenza di intervalli arbitrariamente lunghi privi di numeri primi è la seguente: fra $n!+2$ ed $n!+n$ vi sono $n-1$ interi consecutivi composti, dato che $n!+k$ è divisibile per k se $k \in [2,n]$. Detto p il massimo

numero primo $\leq n!+2$ e p' il minimo numero primo $\geq n!+n$, si ha che p e p' sono numeri primi consecutivi, ed inoltre $p'-p \geq n$. Dato che n è arbitrario, ne segue che si possono trovare intervalli di interi composti consecutivi lunghi a piacere.

Nel nostro caso, però, siccome non ci interessa la grandezza "assoluta" degli intervalli, ma piuttosto quella relativa, per la formula di Stirling nella forma $\log n! \sim n\log n$ (si veda l'Appendice D.2) abbiamo

$$\frac{p'-p}{\log p} \geq \frac{n}{n\log n}(1+o(1)) \to 0. \tag{26}$$

Questo risultato è dunque piú debole di quello che segue dal Teorema dei Numeri Primi, ma l'idea di costruire una sequenza di interi composti consecutivi garantendo la loro divisibilità per opportuni interi "piccoli" è buona e può essere riciclata.

In un certo senso in questa costruzione c'è uno "spreco" perché, per esempio, sappiamo che se $n \geq 2$ allora $n!+4$ non può essere primo dato che è certamente divisibile per 2. Il fattore 4 in $n!$ fa dunque aumentare il valore del prodotto $n!$, e quindi il denominatore a destra nella (26), ma non fa allungare la sequenza di numeri composti trovata. Avere usato numeri composti non porta nessun beneficio. Quindi conviene usare i soli numeri primi: questo permette di trovare una sequenza di numeri composti consecutivi della stessa lunghezza, ma collocata prima nella sequenza degli interi, e che quindi darà luogo ad un rapporto $(p'-p)/\log p$ piú grande, essendo invariato il numeratore e diminuito il denominatore.

L'informazione supplementare che serve in questo caso è la forma del Teorema dei Numeri Primi data dalla (4), che afferma che $\log P(x) \sim x$ quando $x \to +\infty$. Si noti che, mentre la Formula di Stirling è relativamente semplice da dimostrare (si veda il §D.2), il Teorema dei Numeri Primi, nella forma (1) o in quella equivalente (4), è un risultato profondo.

Ripetiamo quindi la stessa costruzione, ma utilizzando solo i numeri primi nell'intervallo $[2,n]$: detto $P(n)$ il prodotto di tutti questi numeri primi, gli $n-1$ numeri consecutivi $P(n)+2$, $P(n)+3$, $\ldots$, $P(n)+n$ sono tutti composti. Infatti, per $m = 2, 3, 4, \ldots, n$ si ha che $P(n)+m$ è divisibile per p, se p è un fattore primo qualsiasi di m, e quindi $P(n)+m$ non è primo.

Anche in questo caso, dunque, abbiamo trovato $n-1$ interi consecutivi non primi, ma è importante notare che, grazie alla formula di Stirling ed al Teorema dei Numeri Primi, $P(n)$ è *molto* piú piccolo di $n!$. Piú precisamente, per la formula di Stirling si ha $\log n! \sim n\log n$, mentre per la (4) si ha $\log P(n) \sim n$, e quindi si "risparmia" un fattore logaritmico al denominatore, pur considerando, essenzialmente, lo stesso insieme di numeri primi, e cioè quelli $\leq n$. Infatti, la

corrispondente della (26) è

$$\frac{p'-p}{\log p} \geq \frac{n}{n(1+o(1))} \to 1,$$

e quindi abbiamo trovato una formula equivalente alla (7).

Vediamo un semplice esempio numerico: per $n = 10$ abbiamo $n! = 3628800$ mentre $P(n) = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. La prima delle nostre costruzioni garantisce l'esistenza di 9 interi composti consecutivi a partire da 3628802, la seconda a partire da 212, rendendo immediatamente evidente che la seconda costruzione è molto piú "efficiente" della prima. Per la precisione, è possibile essere appena piú efficienti considerando gli $n-1$ interi $P(n)-n$, $P(n)-n+1$, ..., $P(n)-2$. In questo caso, abbiamo 9 interi composti consecutivi a partire da 200.

Prima di passare al pezzo forte di questo paragrafo, vogliamo mostrare come sia possibile interpretare questa ultima costruzione in modo leggermente diverso, che risulterà utile per il seguito. Sia $N = P(n)$, consideriamo il sistema di congruenze $z \equiv 0 \bmod p$, dove p varia nell'insieme di tutti i numeri primi $\leq n$. Non è difficile verificare che una soluzione di questo sistema, l'unica per il Teorema Cinese del Resto B.1, è $z \equiv 0 \bmod N$. La costruzione qui sopra garantisce che per $m = 2, 3, 4, \ldots, n$ si ha che $z+m$ è divisibile per p, se p è un fattore primo qualsiasi di m, e quindi (purché non scegliamo proprio la soluzione $z = 0$) $z+m$ non è primo. L'idea che andiamo a sviluppare è proprio questa: costruiamo un opportuno sistema di congruenze utilizzando i numeri primi in un certo intervallo.

5.2 Intermezzo

Fissiamo la notazione che useremo nel resto del paragrafo. Prenderemo un numero reale $x \geq 1$ (che faremo tendere ad infinito), e considereremo l'insieme $\mathfrak{P}$ di tutti i numeri primi $p \leq x$. Costruiremo un intero z definito per mezzo di congruenze simultanee modulo i numeri primi $p \in \mathfrak{P}$. Per il Teorema Cinese del Resto B.1, z è definito modulo $P(x)$, dove $P(x)$ indica il prodotto di tutti i numeri primi $p \in \mathfrak{P}$: noi sceglieremo come z^* l'*unica* soluzione di questo sistema di congruenze che appartiene all'intervallo $[1, P(x)]$. Poi prenderemo una funzione $u = u(x)$, con il ruolo seguente: la costruzione dell'insieme di congruenze garantirà che z^*+n sia divisibile per almeno un numero primo $p \in \mathfrak{P}$ *per ogni* $n \in [0, u]$, e quindi sia un numero composto. Nell'esempio contenuto nel §5.1 avevamo $u(x) = x$.

Prendiamo ora il massimo numero primo $p \leq z^* \leq P(x)$. Il suo successore p' dista almeno u, cioè $p'-p \geq u$, dato che gli interi intermedi, per la nostra costruzione, sono tutti composti. In definitiva, abbiamo dunque trovato una *minorazione* per il numeratore ed una *maggiorazione* per il denominatore del rapporto

$(p'-p)/\log p$, e quindi abbiamo la disuguaglianza

$$\frac{p'-p}{\log p} \geq \frac{u}{\log P(x)}, \tag{27}$$

che è ciò che ci interessa: il problema sarà nell'ottimizzazione della scelta delle congruenze per rendere piú grande possibile il numeratore.

Un'ultima avvertenza: supporremo tacitamente in quanto segue che x sia sufficientemente grande. In particolare, quando scegliamo i valori dei parametri che dipendono da x, come nel caso appena menzionato di u, le disuguaglianze enunciate potrebbero non valere per x troppo piccolo, ma questo fatto è irrilevante ai fini del nostro obiettivo.

5.3 Un piccolo miglioramento

Per migliorare il risultato del §5.1, introduciamo un parametro $y = y(x) < x$ e suddividiamo i numeri primi dell'insieme $\mathfrak{P}$ come segue: $\mathfrak{P}_1 = \mathfrak{P} \cap [1,y]$ e $\mathfrak{P}_2 = \mathfrak{P} \cap (y,x]$. Si tratta di usare astutamente un'idea simile al Crivello di Eratostene (si veda il §A3 di [14]), e cioè di ottimizzare la scelta della classe di resto di z mod p per tutti i numeri primi $p \in \mathfrak{P}_1$. Poniamo $\mathcal{A}_0 = [0,u] \cap \mathbb{N}$ ed $N_0 = |\mathcal{A}_0|$; poi chiamiamo p_1, p_2, …, p_k i numeri primi dell'insieme $\mathfrak{P}_1$ disposti in ordine crescente. Vogliamo costruire l'insieme $\mathcal{A}_j$ di cardinalità N_j a partire da $\mathcal{A}_{j-1}$ per $j = 1, 2, \ldots, k$, dove $k = \pi(y)$.

Supponiamo dunque di aver definito $\mathcal{A}_{j-1}$, e consideriamo i suoi elementi modulo p_j: deve esistere almeno una classe r_j mod p_j che contiene almeno N_{j-1}/p_j elementi; infatti, se *tutte* le classi modulo p_j contenessero meno di N_{j-1}/p_j elementi, allora $\mathcal{A}_{j-1}$ conterrebbe meno di N_{j-1} elementi, in contrasto con la definizione di N_{j-1}. Imponiamo che $z \equiv -r_j \bmod p_j$, e definiamo $\mathcal{A}_j = \{n \in \mathcal{A}_{j-1} : n \not\equiv r_j \bmod p_j\}$. Per quanto detto, abbiamo che

$$N_j \leq \left(1 - \frac{1}{p_j}\right) N_{j-1}.$$

Ripetendo questo procedimento k volte (cioè per tutti i numeri primi nell'insieme $\mathfrak{P}_1$) troviamo che

$$N_k \leq N_0 \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right) \leq (u+2) \prod_{p \leq y} \left(1 - \frac{1}{p}\right).$$

A questo punto è chiaro quale sia l'informazione supplementare sulla distribuzione dei numeri primi di cui abbiamo bisogno: ci serve una stima per il prodotto

all'estrema destra, e questa ci è fornita dal Teorema di Mertens A.2, enunciato in Appendice. In definitiva troviamo che

$$N_k \leq (e^{-\gamma} + o(1)) \frac{u}{\log y}.$$

Prendiamo $y = x^{\delta}$ per qualche $\delta < 1$ fissato, ed $u = \delta^2 e^{\gamma} x$, dove δ è una costante il cui valore sarà scelto in seguito.

Notiamo che N_k risulta $< (\delta + o(1))x/\log x$ e quindi $N_k < \pi(x) - \pi(y) = |\mathfrak{P}_2|$ per x sufficientemente grande. Questo significa che i numeri primi che avevamo messo "da parte" nell'insieme $\mathfrak{P}_2$ sono piú numerosi degli elementi dell'insieme $\mathcal{A}_k$. Se scriviamo gli elementi di $\mathcal{A}_k$ ed i primi in $\mathfrak{P}_2$ rispettivamente in ordine crescente $n_1 < n_2 < \cdots < n_r$ e $q_1 < q_2 < \cdots < q_s$, per quanto detto abbiamo $r \leq s$, e possiamo porre $z \equiv -n_i \bmod q_i$ per $i = 1, \ldots s$, ed eventualmente $z \equiv 0 \bmod q_i$ per $i = r+1, \ldots, s$.

Avendo usato *tutti* i numeri primi di $\mathfrak{P}$ una ed una sola volta, il sistema di congruenze che abbiamo costruito ha una soluzione modulo $P(x)$: chiamiamo z^* l'unica soluzione che giace in $[1, P(x)]$. Resta da dimostrare che $z^* + n$ non è primo per ogni $n \in [0, u]$: per fare questo dobbiamo distinguere vari casi, mostrando sempre che $z^* + n$ è divisibile per almeno un numero primo dell'insieme $\mathfrak{P}$.

1. Se esiste un intero $j \in [1, k]$ tale che $n \in \mathcal{A}_{j-1} \setminus \mathcal{A}_j$, vuol dire che $n \equiv r_j \bmod p_j$ e quindi $z^* + n$ è divisibile per p_j, dato che $z^* \equiv -r_j \bmod p_j$.

2. In caso contrario, $n \in \mathcal{A}_k$, e dunque è uno degli interi $\{n_1, \ldots, n_s\}$. Se $n = n_t$ per un $t \in \{1, \ldots, s\}$, allora, per costruzione, $z^* \equiv -n_t \bmod q_t$ e quindi $z^* + n$ è divisibile per q_t.

A questo punto sappiamo che tutti gli interi $z^* + n$ con $n \in [0, u]$ sono divisibili per un numero primo di $\mathfrak{P}$: per poter concludere che questi sono tutti numeri composti, bisogna mostrare che $z^* + n$ non è proprio un numero primo dell'insieme $\mathfrak{P}$. Osserviamo che questo implica che $z^* + n \leq x$ e quindi che $z^* \leq x$. In questo caso, peraltro piuttosto improbabile ma non impossibile, il nostro ragionamento fallisce: ci viene in soccorso un'osservazione fatta sopra, e cioè che gli interi $P(x) - z^* - n$, con $n \in [0, u]$ sono di nuovo interi composti consecutivi, poiché se $p \in \mathfrak{P}$ divide $z^* + n$ allora divide anche $P(x) - z^* - n$. Notiamo che $u \leq 2x$ e quindi $z^* + n \leq 3x$ per ogni $n \in [0, u]$: dato che per $x \geq 5$ si ha $P(x) > 4x$, abbiamo che $P(x) - z^* - n \geq P(x) - 3x > x$, e quindi $P(x) - z^* - n$, che è divisibile per un numero primo $\leq x$, non è primo.

In conclusione, in entrambi i casi abbiamo trovato almeno u interi composti consecutivi nell'intervallo $[1, P(x)]$: o questo accade per $z^* + n$ con $n \in [0, u]$, o,

nel caso meno probabile, per $P(x) - z^* - n$ con $n \in [0,u]$. Ricordando la (27) e la definizione di u, possiamo concludere dicendo che con questa costruzione si trova

$$\frac{p_{n+1} - p_n}{\log p_n} \geq \frac{\delta^2 e^\gamma x}{x(1+o(1))} = \delta^2 e^\gamma + o(1) \geq e^\gamma - \varepsilon \tag{28}$$

per infiniti n, avendo scelto $\delta^2 = 1 - \varepsilon/2$ ed x sufficientemente grande.

La complicazione di questa costruzione può apparire sproporzionata rispetto al miglioramento, piuttosto modesto, della (28) rispetto alla (7): in fondo, si guadagna solo un fattore ≈ 1.78. Si tratta però di un passo essenziale verso la dimostrazione del risultato che vedremo nel prossimo paragrafo, e ci è parso piú semplice isolarlo dalla intricata dimostrazione che ci aspetta.

Concludiamo anche questo paragrafo con un esempio numerico, mostrando come determinare 100 interi composti consecutivi: prendiamo $n = 100$, $x = 67$ ed $y = 23$. Scegliamo z che soddisfi le congruenze $z \equiv -r_p \bmod p$ per tutti i $p \leq y$, secondo i dati raccolti nella tabella seguente:

p	2	3	5	7	11	13	17	19	23
r_p	0	0	0	0	1	6	11	2	14

Il sistema di congruenze ha la soluzione $z \equiv 95137140 \bmod 223092870$ dove $223092870 = P(23)$. Con una certa dose di pazienza[2] si può verificare che nell'intervallo $[0,100]$ vi sono esattamente 10 interi n per cui $n \not\equiv r_j \bmod p_j$ per $j = 1, \ldots, 9$ (e sono precisamente 13, 17, 29, 31, 41, 43, 47, 53, 61, 73), ma abbiamo ancora 10 numeri primi a disposizione, quelli nell'intervallo $y < p \leq x$: poniamo dunque $z \equiv -n_i \bmod q_i$ come spiegato nel testo, ed avremo definito $z \bmod P(67)$. A partire da questo z vi sono 101 interi consecutivi non primi: diamo la soluzione esplicita del sistema di congruenze in nota, dato che $P(67)$ ha 25 cifre,[3] ma osserviamo che *tutti* i calcoli fatti per determinare le congruenze coinvolgono numeri interi ≤ 100. Il rapporto $(p_{n+1} - p_n)/\log p_n$ che corrisponde a questa costruzione vale approssimativamente 1.74.

Notiamo che il primo intervallo contenente almeno 100 interi composti consecutivi si trova a partire dal numero primo $p = 370261$. È importante osservare che almeno uno di questi 100 interi consecutivi, e precisamente $370267 = 479 \cdot 773$, ha *tutti* i fattori primi > 100 e quindi la costruzione descritta qui sopra non può determinare questo intervallo "ottimale."

[2] Non tantissima: le prime 4 congruenze implicano che i numeri sopravvissuti ai primi 4 passi sono 1 e i primi fra 11 e 97; con $p = 11$ si eliminano 1, 23, 67, 89; con $p = 13$ si eliminano 19, 71, 97; con $p = 17$ si eliminano 11 e 79; con $p = 19$ si elimina 59; con $p = 23$ si eliminano 37 e 83.

[3] 25352195970309900350179 50 mod 78583215510802670558790 90, salvo errori.

5.4 Un ulteriore rafforzamento

Piuttosto che dimostrare una serie di risultati sempre piú forti, ci concentriamo su un solo risultato non banale, che è appena piú debole del miglior risultato oggi noto. L'informazione supplementare di cui abbiamo bisogno in questo caso, come abbiamo detto sopra, riguarda la "densità" degli interi che non hanno fattori primi relativamente piccoli: si tratta del Teorema A.3 in Appendice, che fornisce una limitazione superiore per la funzione Ψ definita nella relazione (31).

Teorema 5.1 *Scelta comunque la costante $A > 0$, per infiniti valori dell'indice n si ha*

$$\frac{p_{n+1} - p_n}{\log p_n} \geq A \frac{\log\log p_n}{(\log\log\log p_n)^2}.$$

Si noti che questo risultato è molto piú forte della (28): infatti, non solo la costante e^γ è stata rimpiazzata da una costante positiva arbitraria, ma, soprattutto, ora il secondo membro è una funzione di n che tende ad infinito con n. Il miglior risultato dimostrato ad oggi è di János Pintz [17], e vede la costante $2e^\gamma$ al posto di A al secondo membro, ed un ulteriore fattore $\log\log\log\log p_n$, sempre al secondo membro.

Passiamo dunque alla dimostrazione. Anche qui prendiamo $x \geq 1$ e consideriamo tre parametri con le limitazioni $y < w < x < u$. L'idea di base è costruire un intero $z < P(x)$ tale che $\big(z+n, P(x)\big) > 1$ per ogni $n \in [0,u]$. Suddividiamo dunque l'insieme $\mathfrak{P}$ dei numeri primi $p \leq u$ in quattro classi: $\mathfrak{P}_1 = \mathfrak{P} \cap [1,y]$, $\mathfrak{P}_2 = \mathfrak{P} \cap (y,w]$, $\mathfrak{P}_3 = \mathfrak{P} \cap (w,x]$, $\mathfrak{P}_4 = \mathfrak{P} \cap (x,u]$. Per cominciare imponiamo che $z \equiv 0 \bmod p$ per ogni $p \in \mathfrak{P}_2$.

Poniamo $\mathcal{A}_0 = \{n \in [0,u] : \big(z+n, P(x)\big) = 1\}$ ed $N_0 = |\mathcal{A}_0|$. Allora $n \in \mathcal{A}_0$ solo se si verifica una delle condizioni seguenti:

1. n ha tutti i fattori primi $\leq y$; il numero di questi interi è $B_1 = \Psi(u,y)$.
2. n ha un fattore primo $p \in \mathfrak{P}_3 \cup \mathfrak{P}_4$; sia B_2 il numero di questi interi.

Per il Lemma A.3 si ha $B_1 \leq C(A) u \exp(-A(\log u)/\log y) \log y$ per $y \geq e^A$, dove $A > 0$ è arbitrario. Per la formula di Mertens (30) si ha

$$B_2 \leq \sum_{w \leq p \leq u} \frac{u}{p} \leq u \log\frac{\log u}{\log w}(1 + o(1)).$$

Ora ripetiamo lo stesso ragionamento illustrato nel §5.3, con una diversa scelta di $\mathcal{A}_0$. Ordiniamo i primi dell'insieme $\mathfrak{P}_1$, scrivendo $p_1 < p_2 < \cdots < p_k$, dove $k = \pi(y)$. Per $i \geq 1$ definiamo induttivamente N_i ed $\mathcal{A}_i$ a partire da N_{i-1} ed $\mathcal{A}_{i-1}$. Scegliamo $r_i \bmod p_i$ in modo che l'equazione $n \equiv r_i \bmod p_i$ sia risolubile per

almeno N_{i-1}/p_i interi $n \in \mathcal{A}_{i-1}$, ed imponiamo $z \equiv -r_i \bmod p_i$. Ora definiamo $\mathcal{A}_i = \{n \in \mathcal{A}_{i-1} : n \not\equiv r_i \bmod p_i\}$ ed $N_i = |\mathcal{A}_i|$. Quindi

$$N_i \leq \left(1 - \frac{1}{p_i}\right) N_{i-1},$$

e per il Teorema di Mertens A.2 si ha

$$N_k \leq \prod_{p \leq y} \left(1 - \frac{1}{p}\right) N_0 = \frac{e^{-\gamma}}{\log y} N_0 \, (1 + o(1)).$$

Poniamo per brevità $\mathcal{L} = \log x$. Ora finalmente scegliamo

$$y = \exp\left(\frac{A\mathcal{L}}{\log \mathcal{L}}\right), \qquad w = \frac{x}{\log \mathcal{L}}, \qquad u = A\, x \frac{\mathcal{L}}{(\log \mathcal{L})^2}.$$

Da queste definizioni, con semplici calcoli deduciamo che $N_0 \leq B_1 + B_2 \leq (A + o(1))\, x\, (\log \mathcal{L})^{-1}$ e quindi che, per x sufficientemente grande, si ha

$$N_k \leq e^{-\gamma} \frac{x}{\mathcal{L}} (1 + o(1)) \leq \pi(x) - \pi(w).$$

Questo significa che vi sono piú numeri primi $q \in \mathfrak{P}_3$ di quanti elementi vi siano in $\mathcal{A}_k$: se $\mathcal{A}_k = \{n_1, n_2, \ldots, n_j\}$ e $\mathfrak{P}_3 = \{q_1, q_2, \ldots, q_m\}$, per $i = 1, \ldots, j$ poniamo $z \equiv -n_i \bmod q_i$, e per $i = j+1, \ldots, m$ poniamo $z \equiv 0 \bmod q_i$. Tutte le congruenze scritte fin qui sono indipendenti e quindi, per il Teorema Cinese del Resto B.1 ammettono una soluzione simultanea $z^* \in [1, P(x)]$. Per questo z^* si ha $(z^* + n, P(x)) > 1$ per tutti gli $n \in [0, u]$, e quindi nessuno degli interi $z^* + n$ con $n \in [0, u]$ può essere primo.

Consideriamo ora il massimo numero primo $p < z^*$ ed il suo successore p': il nostro obiettivo finale è dimostrare che

$$\frac{p' - p}{\log p} \cdot \frac{(\log\log\log p)^2}{\log\log p} \geq A + o(1),$$

perché questa disuguaglianza, evidentemente, implica la tesi. Per quanto abbiamo appena visto si ha $p < z^* \leq P(x)$ e $p' \geq z^* + u$. Da questo deduciamo che

$$\frac{p' - p}{\log p} \cdot \frac{(\log\log\log p)^2}{\log\log p} \geq \frac{u}{\log P(x)} \cdot \frac{(\log\log\log p)^2}{\log\log p}.$$

Per concludere osserviamo che la funzione $t \mapsto (\log\log t)/(\log\log\log t)^2$ è crescente per $t \geq e^{e^e}$ e quindi, per x sufficientemente grande, si ha

$$\frac{p' - p}{\log p} \cdot \frac{(\log\log\log p)^2}{\log\log p} \geq \frac{u}{\log P(x)} \cdot \frac{(\log\log\log P(x))^2}{\log\log P(x)} \geq A + o(1)$$

per il Teorema dei Numeri Primi nella forma (4), come si voleva.

A Lemmi per i grandi intervalli

Raccogliamo qui alcuni dei risultati intermedi che ci servono, con qualche commento sulla loro importanza.

Teorema A.1 (Mertens) *Esiste una costante reale e positiva A_1 tale che*

$$\left|\sum_{p\le x}\frac{\log p}{p}-\log x\right|\le A_1 \tag{29}$$

per ogni $x\ge 1$. Esistono una costante reale e positiva A_2 ed una costante reale B tali che si ha

$$\left|\sum_{p\le x}\frac{1}{p}-\log\log x-B\right|\le\frac{A_2}{\log x} \tag{30}$$

per $x\ge 2$.

Questi due risultati sono tra loro equivalenti, e sono una conseguenza non difficile, e al tempo stesso non banale, della formula di Stirling per mezzo della formula di sommazione parziale dell'Appendice D.1: in [14, § A.1] abbiamo già dato una dimostrazione parziale della prima delle due formule. Si possono anche dimostrare a partire dal Teorema dei Numeri Primi, ma se ne può fare a meno.

Teorema A.2 (Mertens) *Per $x\to+\infty$ si ha*

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)\sim\frac{e^{-\gamma}}{\log x},$$

dove $\gamma=0.5772156649\ldots$ è la costante di Eulero-Mascheroni.

Questa formula (a parte per il valore della costante) è una conseguenza del Teorema dei Numeri Primi, e si dimostra utilizzando la (30). Quindi, tutte le successioni A della famiglia $\mathfrak{A}$ di Cramér soddisfano una relazione simile, con una costante $c=c(A)>0$ al posto di $e^{-\gamma}$, che dipende da quali interi compaiono effettivamente nella successione, e non solo dalla loro densità. Per esempio, la successione dei numeri primi *dispari* soddisfa il Teorema dei Numeri Primi, ed anche il Teorema di Mertens con la costante $2e^{-\gamma}$. Questo è un altro esempio della doppia natura "aritmetica" ed "analitica" dei problemi della Teoria dei Numeri: l'aspetto analitico è responsabile dell'ordine di grandezza delle varie funzioni di cui trattiamo in questo articolo, mentre l'aspetto aritmetico dà origine alle costanti. Un esempio chiarissimo di questo fenomeno è dato dalla formula (11) in cui è evidente la diversa natura dei fattori che compaiono.

Poniamo

$$\Psi(x,y) = |\{n \leq x\colon\ p \mid n \Rightarrow p \leq y\}|. \tag{31}$$

L'obiettivo è il conteggio degli interi $n \leq x$ che non hanno fattori primi "grandi," dove la grandezza dei fattori primi è misurata dal parametro y. Cominciamo con una semplice osservazione: per ogni $\sigma > 0$ si ha

$$\Psi(x,y) = \sum_{\substack{n\leq x \\ p|n\Rightarrow p\leq y}} 1 \leq \sum_{\substack{n\leq x \\ p|n\Rightarrow p\leq y}} \left(\frac{x}{n}\right)^{\sigma} \leq \sum_{\substack{n\geq 1 \\ p|n\Rightarrow p\leq y}} \left(\frac{x}{n}\right)^{\sigma}$$

È evidente che questa relazione è interessante solo per $\sigma < 1$, poiché per $\sigma \geq 1$ il secondo membro è $\geq x$: vogliamo dunque scegliere σ in modo "ottimale" per ottenere una buona maggiorazione. Una prima trasformazione, standard ma non banale, consiste nel riscrivere l'ultima espressione a destra nella forma

$$x^{\sigma} \prod_{p\leq y} \left(1 - p^{-\sigma}\right)^{-1}. \tag{32}$$

Per fare questo si usa una proprietà nota come prodotto di Eulero che riguarda le funzioni moltiplicative della definizione F.1: si veda il Teorema 286 di Hardy & Wright [12]. L'idea è di Rankin che l'ha sviluppata proprio per dimostrare una forma piú forte del risultato del nostro §5.4. La deduzione principale è contenuta nel risultato che segue.

Teorema A.3 *Fissato arbitrariamente $A > 0$, esiste una costante positiva $C(A)$ tale che per $x \geq 1$ ed $y \geq e^A$ si ha*

$$\Psi(x,y) \leq C(A) x e^{-Au} \log y,$$

dove $u = (\log x)/\log y$.

Dim. La dimostrazione si ottiene prendendo $\sigma = 1 - A(\log y)^{-1}$ in (32), ed usando le formule di Mertens (29) e (30). □

B Il Teorema Cinese del Resto

Il prossimo risultato deve il suo nome ad un aneddoto secondo il quale i generali cinesi dell'antichità contavano i soldati delle loro compagnie facendoli disporre in fila per 7, per 11 e per 13, prendendo nota del numero di soldati dell'eventuale fila incompleta.

Teorema B.1 (Teorema Cinese del Resto) *Se* n_1, $n_2 \in \mathbb{Z}^*$ *ed* $(n_1, n_2) = 1$, *il sistema*

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \end{cases}$$

ha un'unica soluzione $\bmod n_1 n_2$.

Una dimostrazione si può trovare nel §2 di [13]. Osserviamo che, per esempio, il sistema

$$\begin{cases} x \equiv 5 \bmod 14 \\ x \equiv 9 \bmod 33 \end{cases} \qquad \text{ha la soluzione} \quad x \equiv 75 \bmod 462.$$

Questo significa che due congruenze sono sempre *compatibili* (o indipendenti, se si vuole) se $(n_1, n_2) = 1$, mentre possono essere incompatibili se $(n_1, n_2) > 1$, come mostrano gli esempi che seguono:

$$\begin{cases} x \equiv 2 \bmod 14 \\ x \equiv 0 \bmod 10 \end{cases} \implies x \equiv 30 \bmod 70; \quad \begin{cases} x \equiv 2 \bmod 14 \\ x \equiv 1 \bmod 10 \end{cases} \quad \text{è impossibile.}$$

Chiaramente il Teorema Cinese del Resto può essere generalizzato al caso in cui sia necessario avere la soluzione di un sistema di $k > 2$ congruenze modulo k interi tra loro coprimi. È infatti sufficiente raggruppare a coppie tali congruenze e applicare ripetutamente il Teorema B.1.

Essendo le loro compagnie formate al piú da 1000 uomini, i generali cinesi potevano quindi applicare questo metodo per calcolarne gli effettivi disponibili ordinando gli uomini in file di 7, 11, 13 e conoscendo il numero di soldati delle eventuali file incomplete (infatti $7 \cdot 11 \cdot 13 = 1001$).

C Notazioni per funzioni infinitesime e asintotiche

Useremo la notazione $o(1)$ per indicare una non specificata funzione infinitesima, cioè una funzione che ha limite 0 per $x \to +\infty$. Questa notazione è molto comoda tutte le volte che non è possibile o non è necessario specificare le funzioni infinitesime coinvolte, ma può sembrare paradossale: infatti scriveremo $o(1) + o(1) = o(1)$ per indicare che la somma di una, non meglio specificata, funzione infinitesima e di un'altra funzione infinitesima, a sua volta non specificata, è una terza funzione infinitesima. In altre parole, ogni istanza di $o(1)$ indica una *diversa* funzione infinitesima. Prima dell'introduzione di questo tipo di simbolismo, la relazione qui sopra sarebbe stata scritta $f_1(x) + f_2(x) = f_3(x)$ con $f_j(x)$ infinitesime: in un articolo come questo, avremmo probabilmente dovuto introdurre una

trentina di funzioni infinitesime, non meglio precisate, e in definitiva irrilevanti. In questo modo si guadagna molto in leggibilità e in semplicità di scrittura.

Osserviamo che in questo modo possiamo indicare con $a+o(1)$ una generica funzione che ha limite a per $x \to +\infty$, e che, se $a \neq 0$, allora $1/(a+o(1)) = 1/a+o(1)$.

Useremo anche una generalizzazione di questa notazione: scriveremo $f(x) = o(g(x))$ per indicare che $f(x)/g(x)$ è una funzione infinitesima, come se si potesse moltiplicare. Infatti, da $f(x)/g(x) = o(1)$ deduciamo $f(x) = g(x) \cdot o(1)$ che per brevità si scrive $f(x) = o(g(x))$.

La relazione $f(x) \sim g(x)$ per $x \to +\infty$ significa che le due funzioni hanno lo stesso ordine, ossia, per definizione, che $\lim_{x\to+\infty} f(x)/g(x) = 1$. Come nel caso precedente, è una notazione sintetica molto comoda per migliorare la leggibilità.

Osserviamo che $f(x) \sim g(x)$ equivale a $f(x) = g(x)(1+o(1))$ ossia che l'errore che si commette sostituendo g a f è $o(g)$ (in altre parole $f(x)-g(x) = o(g(x))$). Un errore comune nel trattare $\sim$ è quello di dimenticare la presenza di $o(g)$ interpretando tale relazione come un'uguaglianza diretta tra f e g. È evidente che ciò può condurre ad errori marchiani.

Nel caso si abbia che $h = o(g)$ ed $f \sim g$ allora si ha che $f+h \sim g$. La dimostrazione è immediata (basta scrivere le definizioni). Abbiamo usato questo fatto quando abbiamo parlato delle varie formulazioni equivalenti del TNP.

D La Formula di sommazione parziale

La formula di sommazione parziale (o di somma per parti) è un utile strumento che consente di esprimere somme mediante integrali.

Teorema D.1 *Data una successione di numeri complessi $(a_n)_{n\in\mathbb{N}}$ ed una funzione $\phi : (0,+\infty) \to \mathbb{C}$ di classe $\mathcal{C}^1((0,+\infty))$, sia*

$$A(x) = \sum_{n\leq x} a_n.$$

Allora, per $x \geq 1$ si ha

$$\sum_{n\leq x} a_n\phi(n) = A(x)\phi(x) - \int_1^x A(t)\phi'(t)dt.$$

Anche in questo caso tralasciamo la dimostrazione, che il lettore interessato può trovare in [1, Theorem 4.2], per concentrarci sulle sue conseguenze.

D.1 Equivalenza delle formulazioni del Teorema dei Numeri Primi

Vediamo ora come applicare il Teorema D.1 per dimostrare l'equivalenza tra le formulazioni (1) e (4) del Teorema dei Numeri Primi. Supponiamo di sapere che (1) è vera. Applichiamo il Teorema D.1 al caso $a_n = 1$ se n è primo, $a_n = 0$ se n è composto e $\phi(x) = \log x$. Otteniamo quindi $A(x) = \pi(x)$ e

$$\theta(x) = \sum_{p \le x} \log p = \sum_{n \le x} a_n \log n = \pi(x)\log x - \int_1^x \frac{\pi(t)}{t} dt.$$

Per la relazione (1) si ha allora che $\pi(t) = t/\log t(1+o(1))$ che inserito nell'integrale soprastante fornisce la relazione

$$\theta(x) = x(1+o(1)) + \mathrm{li}(x)(1+o(1)) \sim x,$$

ossia la (4).

Nel caso in cui si sappia che la (4) è vera allora si applica il Teorema D.1 al caso $n \ge 2$, $a_n = \log n$ se n è primo, $a_n = 0$ se n è composto e $\phi(x) = 1/\log x$. Si ha allora $A(x) = \theta(x)$ ed il Teorema D.1 fornisce

$$\pi(x) = \sum_{p \le x} 1 = \sum_{2 \le n \le x} \frac{a_n}{\log n} = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t \log^2 t} dt.$$

Assumendo ora la validità di $\theta(t) = t(1+o(1))$, otteniamo che

$$\begin{aligned} \pi(x) &= \frac{x}{\log x}(1+o(1)) + \int_2^x \frac{1+o(1)}{\log^2 t} dt \\ &= \frac{x}{\log x}(1+o(1)) + \left(\mathrm{li}(x) - \frac{x}{\log x}\right)(1+o(1)). \end{aligned}$$

Grazie alla (38) sappiamo che $\mathrm{li}(x) - x/\log x = o(x/\log x)$. Combinando le due relazioni precedenti otteniamo $\pi(x) \sim x/\log x$, ossia la (1).

D.2 La Formula di Stirling

Teorema D.2 *Per $n \to +\infty$ si ha $\log n! = n\log n - n + c(n)\log n + 1$ dove $0 \le c(n) \le 1$.*

Nell'Appendice A1 di [14] abbiamo dimostrato che $\log n! \ge n\log n - n$, che è sufficiente per l'uso che ne facciamo qui, e che la relazione $\log n! \sim n\log n$ è

una forma piú debole del Teorema D.2. Se ne può dimostrare un ulteriore rafforzamento, per esempio la forma enunciata all'inizio dell'Appendice citata, ma in questa sede la complicazione aggiuntiva non ci è sembrata appropriata.

Nel seguito indicheremo con $\lfloor x \rfloor$ la *parte intera* del numero reale x, e cioè il massimo numero intero $n \leq x$, e con $\{x\}$ la sua *parte frazionaria* e cioè $\{x\} = x - \lfloor x \rfloor$. Osserviamo che si ha $0 \leq \{x\} < 1$ per ogni numero reale x.

Dim. Per il Teorema D.1 con $a_n = 1$ e $\phi(x) = \log x$, se $n \geq 1$ si ha

$$\log n! = \sum_{k=1}^{n} \log k = n \log n - \int_1^n \frac{\lfloor x \rfloor}{x} dx = n \log n - (n-1) + \int_1^n \frac{\{x\}}{x} dx.$$

La tesi segue integrando dato che $0 \leq \{x\} \leq 1$. □

D.3 La costante di Eulero-Mascheroni ed altre conseguenze

Grazie al Teorema D.1 con $a_n = 1$ e $\phi(x) = 1/x$ abbiamo che

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &= \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2} dt = 1 - \frac{\{x\}}{x} + \int_1^x \frac{dt}{t} - \int_1^x \frac{\{t\}}{t^2} dt \\ &= 1 - \frac{\{x\}}{x} + \log x - \int_1^x \frac{\{t\}}{t^2} dt. \end{aligned} \tag{33}$$

Per l'ultimo integrale abbiamo

$$0 \leq \int_1^x \frac{\{t\}}{t^2} dt \leq \int_1^x \frac{1}{t^2} dt = 1 - \frac{1}{x},$$

e dunque

$$\sum_{n \leq x} \frac{1}{n} - \log x \geq 1 - \frac{\{x\}}{x} - \left(1 - \frac{1}{x}\right) = \frac{1 - \{x\}}{x} > 0 \tag{34}$$

$$\sum_{n \leq x} \frac{1}{n} - \log x \leq 1. \tag{35}$$

Cogliamo questa occasione per definire anche una quantità che ricorre spesso nella trattazione sui primi e che abbiamo già nominato nel Teorema A.2: la *costante di Eulero-Mascheroni*. Osserviamo che dalla (33) segue che

$$\sum_{n \leq x} \frac{1}{n} = 1 - \frac{\{x\}}{x} + \log x - \int_1^{+\infty} \frac{\{t\}}{t^2} dt + \int_x^{+\infty} \frac{\{t\}}{t^2} dt. \tag{36}$$

Siccome $0 \leq \{t\} \leq 1$, otteniamo che gli ultimi due integrali sono convergenti. In particolare, per ogni $u \geq x$, si ha che

$$0 \leq \int_x^u \frac{\{t\}}{t^2} dt \leq \int_x^u \frac{1}{t^2} dt = -\frac{1}{u} + \frac{1}{x} \to \frac{1}{x},$$

per $u \to +\infty$. Allora

$$0 \leq \int_x^{+\infty} \frac{\{t\}}{t^2}\, dt \leq \frac{1}{x} = o(1)$$

per $x \to +\infty$. Detta *costante di Eulero-Mascheroni* la quantità

$$\gamma = 1 - \int_1^{+\infty} \frac{\{t\}}{t^2} dt \approx 0.5772156649\ldots,$$

abbiamo dunque che

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma - \frac{\{x\}}{x} + o(1) = \log x + \gamma + o(1)$$

per $x \to +\infty$. In conclusione notiamo come la formulazione precedente possa essere anche scritta come

$$\lim_{x \to +\infty} \left(\sum_{n \leq x} \frac{1}{n} - \log x \right) = \gamma$$

che è la definizione tradizionale della costante di Eulero-Mascheroni.

E Altri risultati sulla distribuzione dei numeri primi

E.1 Il comportamento asintotico del logaritmo integrale

Vogliamo adesso spiegare perché nel §1 abbiamo detto che lo sviluppo asintotico di $\mathrm{li}(x)$ ha come primo termine $x/\log x$. Mediante un'integrazione per parti possiamo scrivere che

$$\mathrm{li}(x) = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{\log^2 t}.$$

Integrando nuovamente per parti l'integrale nel termine di destra abbiamo anche

$$\int_2^x \frac{dt}{\log^2 t} = \frac{x}{\log^2 x} - \frac{2}{\log^2 2} + 2\int_2^x \frac{dt}{\log^3 t}.$$

Pertanto, combinando le due equazioni precedenti, otteniamo

$$\mathrm{li}(x) = \frac{x}{\log x} + \frac{x}{\log^2 x} - \frac{2}{\log 2} - \frac{2}{\log^2 2} + 2\int_2^x \frac{dt}{\log^3 t}. \tag{37}$$

Potremmo continuare ad integrare per parti, ma per i nostri scopi è sufficiente fermarci a questo punto. È necessario però capire che tipo di ordine abbia l'integrale a destra nella (37). Osserviamo che

$$\int_2^x \frac{dt}{\log^3 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^3 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^3 t} \leq \frac{\sqrt{x}}{\log^3 2} + \frac{x}{\log^3 \sqrt{x}}$$
$$\leq 8\frac{x}{\log^3 x} + \frac{\sqrt{x}}{\log^3 2} \leq K\frac{x}{\log^3 x},$$

dove $K > 0$ è una costante sufficientemente grande. Allora, dalla (37) segue che

$$\left|\mathrm{li}(x) - \frac{x}{\log x}\right| \leq \frac{2}{\log 2} + \frac{2}{\log^2 2} + \frac{x}{\log^2 x}\left(1 + \frac{2K}{\log x}\right) \leq K'\frac{x}{\log^2 x}, \tag{38}$$

dove $K' > 0$ è una costante opportuna e x è sufficientemente grande.

Piú in generale, ma con le stesse tecniche, si può dimostrare che

$$\mathrm{li}(x) = \frac{x}{\log x}\left(1 + \sum_{j=1}^{n-1} \frac{j!}{\log^j x}\right) + n! \int_2^x \frac{dt}{\log^{n+1} t} + c_n, \tag{39}$$

dove $x \geq 2$ e $c_n \in \mathbb{R}$ non dipende da x.

E.2 Altra equivalenza tra formulazioni del Teorema dei Numeri Primi

Abbiamo già dimostrato nel §1 che (1) implica (2). Proviamo adesso il viceversa.

Dato $x \geq 2$, definiamo n in modo tale che $p_n \leq x < p_{n+1}$ e quindi $\pi(x) = n$. Dividendo per $n\log n$ abbiamo che

$$\frac{p_n}{n\log n} \leq \frac{x}{n\log n} < \frac{p_{n+1}}{n\log n} = \frac{p_{n+1}}{(n+1)\log(n+1)} \frac{(n+1)\log(n+1)}{n\log n}.$$

Se vale (2), allora, visto che

$$\lim_{n\to+\infty} \frac{(n+1)\log(n+1)}{n\log n} = 1,$$

per il teorema dei carabinieri otteniamo

$$\frac{x}{\pi(x)\log\pi(x)} = \frac{x}{n\log n} \sim 1. \tag{40}$$

Consideriamo ora il logaritmo del termine piú a sinistra; tale calcolo fornisce $\log\pi(x) + \log\log\pi(x) - \log x = o(1)$ da cui, raccogliendo $\log\pi(x)$, abbiamo

$$\log\pi(x)\left(1 + \frac{\log\log\pi(x)}{\log\pi(x)} - \frac{\log x}{\log\pi(x)}\right) = o(1).$$

Poiché

$$\lim_{x\to+\infty} \log\pi(x) = +\infty \quad \text{e} \quad \frac{\log\log\pi(x)}{\log\pi(x)} = o(1),$$

segue che $\log x \sim \log\pi(x)$. Inserendo quest'ultima relazione in (40) abbiamo che

$$\frac{x}{\pi(x)\log x} \sim \frac{x}{\pi(x)\log\pi(x)} \sim 1$$

da cui, considerando i reciproci, segue (1).

E.3 Convergenza del prodotto infinito nella costante dei primi gemelli

Data una successione $a_m \in \mathbb{C}$, il prodotto infinito associato a tale successione è definito come

$$\lim_{n\to+\infty} \prod_{m=1}^{n} (1+a_m)$$

e, se tale limite esiste, viene indicato con la notazione

$$\prod_{n=1}^{+\infty} (1+a_n)\,. \tag{41}$$

Consideriamo ora il problema della convergenza. Osserviamo per prima cosa che se $a_n \geq 0$ allora, siccome

$$a_1+a_2+\ldots+a_m \leq (1+a_1)(1+a_2)\cdots(1+a_m) \leq \exp(a_1+a_2+\ldots+a_m),$$

la convergenza o la divergenza del prodotto infinito in (41) è equivalente alla convergenza o alla divergenza della serie $\sum_{n=1}^{+\infty} a_n$.

Nel caso in cui $a_n \leq 0$, poniamo $b_n = -a_n$ e scriviamo il prodotto in (41) come

$$\prod_{n=1}^{+\infty} (1-b_n)\,.$$

In tal caso è necessario assumere che $b_n \neq 1$ per ogni $n \in \mathbb{N}$. Si può dimostrare (si veda [21, §1.41]) che

1. se $b_n \geq 0$, $b_n \neq 1$ per ogni $n \in \mathbb{N}$ e $\sum_{n=1}^{+\infty} b_n$ è convergente, allora abbiamo che $\prod_{n=1}^{+\infty}(1-b_n)$ è convergente;

2. se $0 \leq b_n < 1$ per ogni $n \in \mathbb{N}$ e la serie $\sum_{n=1}^{+\infty} b_n$ è divergente, allora abbiamo che $\prod_{n=1}^{+\infty}(1-b_n)$ tende a 0 (in questo caso si dice che il prodotto *diverge a* 0);

3. se $0 \leq b_n < 1$ per ogni $n \in \mathbb{N}$, allora la convergenza o la divergenza della serie $\sum_{n=1}^{+\infty} b_n$ è equivalente alla convergenza o alla divergenza del prodotto $\prod_{n=1}^{+\infty}(1-b_n)$.

Per quanto riguarda la convergenza del prodotto infinito $\prod_{p>2}\left(1-(p-1)^{-2}\right)$ che definisce la costante dei primi gemelli abbiamo che, grazie al punto 3., essa equivale dunque alla convergenza di $\sum_{p>2}(p-1)^{-2}$. Osserviamo adesso che

$$\sum_{3\leq p\leq x}\frac{1}{(p-1)^2} \leq \sum_{2\leq n\leq x}\frac{1}{n^2}.$$

Abbiamo quindi una serie a termini non negativi maggiorata da un'altra serie convergente. Per il criterio del confronto abbiamo allora che la serie $\sum_{p>2}(p-1)^{-2}$ è convergente e quindi che anche il prodotto infinito che definisce la costante dei primi gemelli è convergente.

F La Formula di Möbius

Abbiamo usato la formula di Möbius nella dimostrazione del Lemma 4.3 per esprimere un prodotto sui primi divisori di un intero mediante una somma sui divisori dell'intero stesso. Ciò si può fare se la funzione coinvolta ha buone proprietà.

Definizione F.1 *Diremo funzione moltiplicativa una $f : \mathbb{N} \to \mathbb{C}$ non identicamente nulla tale che $f(mn) = f(n)f(m)$ se $(m,n) = 1$. Diremo inoltre funzione completamente moltiplicativa una $f : \mathbb{N} \to \mathbb{C}$ non identicamente nulla tale che $f(mn) = f(n)f(m)$ per ogni $m,n \in \mathbb{N}$.*

Esempi di funzioni completamente moltiplicative sono le potenze n^α, $\alpha \in \mathbb{C}$ fissato. Esistono però funzioni moltiplicative che non lo sono completamente. Ad esempio la funzione μ di Möbius è moltiplicativa ma non lo è completamente (si osservi che $\mu(4) = 0$ ma $\mu(2) = -1$). È immediato notare che il prodotto di due funzioni moltiplicative è moltiplicativo cosí come accade per il prodotto di due funzioni completamente moltiplicative. Non vogliamo qui trattare la teoria delle funzioni moltiplicative ma ricordare solamente il seguente risultato.

Teorema F.2 (Formula di Möbius, Theorem 2.18 di [1]) *Assumiamo che f sia una funzione moltiplicativa. Allora*

$$\sum_{d|n}\mu(d)f(d) = \prod_{p|n}(1-f(p)).$$

In un passaggio nella dimostrazione del Lemma 4.3 abbiamo usato la Formula di Möbius per il caso $f(n) = \mu(n)/n$; si noti che tale f è una funzione moltiplicativa essendo il prodotto di funzioni moltiplicative.

References

[1] T.M. Apostol, *Introduction to Analytic Number Theory,* Springer-Verlag, Berlin, Heidelberg, New York, 1976.

[2] V. Brun, "La serie 1/5 + 1/7 + [etc.] où les denominateurs sont "nombres premiers jumeaux" est convergente ou finie", *Bull. Sci. Math.*, 43, pagine 100-104,124-128, 1919.

[3] V. Brun, "Le crible d'Eratosthène et le théorème de Goldbach", *C.R. Acad. Sci. Paris*, 168, pagine 544-546, 1919.

[4] V. Brun, "Le crible d'Eratosthène et le théorème de Goldbach", *Videnskapsselskaptes Skrifter, Mat. Naturv. Klasse. (Kristiania)*, 1, pagine 1-36, 1920.

[5] P. Erdős, "The difference of consecutive primes", *Duke Math. J.*, 6, pagine 438–441, 1940.

[6] D. A. Goldston, Y. Motohashi, J. Pintz, C. Y. Yıldırım, "Small gaps between primes exist", *arXiv website*, 2005, disponibile all'indirizzo `http://xxx.sissa.it/pdf/math.NT/0505300`.

[7] D. A. Goldston, J. Pintz, C. Y. Yıldırım, "Primes in Tuples I", *arXiv website*, 2005, disponibile all'indirizzo `http://xxx.sissa.it/abs/math.NT/0508185`.

[8] G. Greaves, *Sieves in number theory,* Springer-Verlag, Berlin, 2001.

[9] H. Halberstam, H.-E. Richert, *Sieve methods,* Academic Press, London-New York, 1974.

[10] G.H. Hardy, J.E. Littlewood, "Some problems on Partitio Numerorum:III. On the expression of a number as a sum of primes", *Acta Math.*, 44, pagine 1-70, 1923.

[11] G.H. Hardy, J.E. Littlewood, "Some problems on Partitio Numerorum:V. A further contribution to the study of Goldbach's problems", *Proc. London Math. Soc.*, 22, pagine 46-56, 1923.

[12] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers,* Oxford Science Publications, Oxford, quinta edizione, 1979.

[13] A. Languasco, A. Zaccagnini, *Introduzione alla Crittografia,* Ulrico Hoepli Editore, Milano, 2004.

[14] A. Languasco, A. Zaccagnini, "Alcune proprietà dei numeri primi, I", *Sito web Bocconi-Pristem*, 2005, disponibile all'indirizzo http://matematica.uni-bocconi.it/LangZac/home.htm.

[15] A. Languasco, A. Zaccagnini, "Alcune proprietà dei numeri primi, II", *Sito web Bocconi-Pristem*, 2005, disponibile all'indirizzo http://matematica.unibocconi.it/LangZac/home2.htm.

[16] A. Languasco, A. Zaccagnini, "Esistono piccoli intervalli fra primi consecutivi!", *Sito web Bocconi-Pristem*, 2005, disponibile all'indirizzo http://matematica.unibocconi.it/LangZac/risultatoteorianumeri.htm.

[17] J. Pintz, "Very large gaps between consecutive primes", *J. Number Theory*, 63, pagine 286–301, 1997.

[18] G. Pólya, "Heuristic reasoning in the theory of numbers", *American Mathematical Monthly*, 66, pagine 375–384, 1959.

[19] P. Ribenboim, *The New Book of Prime Numbers Records,* Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[20] L. Schnirelmann, "Über additive Eigenschaften von Zahlen", *Math. Ann.*, 107, pagine 649-690, 1933.

[21] E.C. Titchmarsh, *Theory of Functions,* Oxford U.P., Oxford, seconda edizione, 1986.

[22] A. Zaccagnini, "Variazioni Goldbach: problemi con numeri primi", *L'Educazione Matematica, Anno XXI, Serie VI*, 2, pagine 47-57, 2000, disponibile all'indirizzo http://www.math.unipr.it/~zaccagni/psfiles/papers/Goldbach_I.pdf.

Alessandro Languasco
Dipartimento di Matematica Pura e Applicata,
via Belzoni 7, 35131 Padova
e-mail: languasco@math.unipd.it
pagina web: http://www.math.unipd.it/~languasc

Alessandro Zaccagnini
Dipartimento di Matematica,
Parco Area delle Scienze, 53/a – Campus Universitario, 43100 Parma
e-mail: alessandro.zaccagnini@unipr.it
pagina web: http://www.math.unipr.it/~zaccagni/home.html