Dimostrazione della Formula per la determinazione del numero di divisori-Test di primalità, di Giorgio Lamberti

Eugenio Amitrano aveva proposto l'idea di una formula per calcolare il numero di divisori di un numero, da cui si poteva ricavare un test di primalità. Tutto ciò era basato su una "serie quoziente" S_n , definita nel seguente modo:

$$S_n = \sum_{i=1}^{n} \left[\frac{n}{i} \right] \quad \forall n \in \mathbb{N}$$

, dove $\left[\frac{n}{i} \right]$ identificava la parte intera della divisione.

Ad esempio, questi sono gli sviluppi delle prime 10 serie quozienti:

$$S_1 = \sum_{i=1}^{1} \left[\frac{1}{i} \right] = \left[\frac{1}{1} \right] = 1$$

$$S_2 = \sum_{i=1}^{2} \left[\frac{2}{i} \right] = \left[\frac{2}{1} \right] + \left[\frac{2}{2} \right] = 2+1 = 3$$

$$S_3 = \sum_{i=1}^{3} \left[\frac{3}{i} \right] = \left[\frac{3}{1} \right] + \left[\frac{3}{2} \right] + \left[\frac{3}{3} \right] = 3+1+1 = 5$$

$$S_4 = \sum_{i=1}^{4} \left[\frac{4}{i} \right] = \left[\frac{4}{1} \right] + \left[\frac{4}{2} \right] + \left[\frac{4}{3} \right] + \left[\frac{4}{4} \right] = 4+2+1+1 = 8$$

$$S_5 = \sum_{i=1}^{5} \left[\frac{5}{i} \right] = \left[\frac{5}{1} \right] + \left[\frac{5}{2} \right] + \left[\frac{5}{3} \right] + \left[\frac{5}{4} \right] + \left[\frac{5}{5} \right] = 5+2+1+1+1 = 10$$

$$S_6 = \sum_{i=1}^{6} \left[\frac{6}{i} \right] = \ldots = 6+3+2+1+1+1 = 14$$

$$S_7 = \sum_{i=1}^{7} \left[\frac{7}{i} \right] = \ldots = 7+3+2+1+1+1+1 = 16$$

$$S_8 = \sum_{i=1}^{8} \left[\frac{8}{i} \right] = \ldots = 8+4+2+2+1+1+1+1 = 20$$

$$S_9 = \sum_{i=1}^{9} \left[\frac{9}{i} \right] = \ldots = 9+4+3+2+1+1+1+1+1 = 23$$

$$S_{10} = \sum_{i=1}^{10} \left\lfloor \frac{10}{i} \right\rfloor = \ldots = 10+5+3+2+2+1+1+1+1+1 = 27$$

Se indichiamo con D_n il numero di divisori di n , il numero di divisori è calcolabile mediante la formula:

$D_n = S_n - S_{n-1} \quad \forall n \geq 2$.

Il test di primalità discende da questa formula, in quanto un numero che possiede solo due divisori (che sono 1 e sè stesso) è ovviamente primo (se $D_n = 2$ allora n è primo).

Ad esempio, proviamo il test di primalità sul numero 113 :

$D_{113} = S_{113} - S_{112} = 554 - 552 = 2$; perciò 113 è un numero primo.

Infine, Amitrano concludeva l'articolo dicendo che la validità della formula era una congettura, in quanto non era stata formulata una dimostrazione.

Questa che segue è dunque la mia dimostrazione (Giorgio Lamberti):

Per ogni valore di i , il numero di termini delle serie aumenta sempre con uno scarto di 1 , per esempio, partendo da essere 1 divisore per i=1 , procedendo a 2 divisori per i=2 , poi 3 divisori per i=3 (quindi, lo scarto, ad esempio, di quest'ultimi due è, appunto, 3-2=1): di conseguenza, il numero di termini di una serie S_i per un qualsiasi valore di i è dato dal valore di i stesso.

Il primo termine di ciascuna serie è sempre il valore di i .

Il numero di 1 di ciascuna serie è dato dalla differenza fra il primo termine della serie e il secondo ; per esempio: nelle serie S_3 il numero di 1 (che si trovano in coda alla serie) è dato da 3-1 , dove 3 è il primo termine della serie e 1 è il secondo termine della serie: in effetti, nella serie compaiono complessivamente due 1 ; nella serie S_4 il numero di 1 (che si trovano in coda alla serie) è dato da 4-2 , dove 4 è il primo termine della serie e 2 è il secondo termine della serie. Nella serie S_1 il numero di 1 (che si trovano sempre in coda alla serie) è dato da 1-0 , dove 1 è il primo termine della serie e 0 è il secondo termine della serie (in quanto non c'è un secondo termine, e quindi lo si assume come uguale a 0); in effetti, in coda alla serie c'è un solo 1 , che altro non è se non proprio l'unico 1 che compare nella serie. Nella serie S_2 il numero di 1 (che si trovano sempre in coda alla serie) è dato da 2-1 , dove 2 è il primo termine della serie e 1 è il secondo termine della serie: in effetti, fra i numeri della serie compare complessivamente un solo 1 .

Guardando le cose da un altro punto di vista, tutto ciò appena detto significa che, considerando i soli valori di i pari, il numero di 1 che compaiono in coda a ciascuna serie sono dati dalla formula $\frac{i}{2}$: se questo è il totale degli 1 che compaiono in coda a ciascuna serie, a questo valore andrà aggiunto il valore di i ; il quale valore di i è una volta pari e una volta dispari (quando sarà pari varrà appunto i , quando sarà dispari varrà di conseguenza i-1): il numero di 1 in coda alle serie S_i e S_{i-1} è uguale; ogni volta che cambia il valore pari di i , che aumenta di 2 unità, il numero di 1 che compaiono in coda alle nuove serie va aumentato di 1 unità: quindi il numero di 1 che compaiono in coda alle serie S_i e S_{i+1} differisce di 1 unità, che, sommata all'altra unità per la quale differiscono sempre queste due serie consecutive per via del loro primo termine, determina una differenza sulla sommatoria dei termini che minimo è 2 unità. Per esempio: considero la serie S_6 , con valore di i=6 e quindi pari; il numero di 1 che compaiono in coda alla serie S_6 è dato da $\frac{6}{2}=3$ (ci sono quindi 1+1+1 in coda alla serie S_6); il valore di i dispari associato a i=6 è i+1=6+1=7 : infatti, la serie S_7 presenta un numero di 1 in coda alla serie uguale a quattro (1+1+1+1). Quindi, la coppia di serie $(S_6;S_7)$ è una delle coppie caratterizzate dal differire, per il risultato della somma dei loro termini, di almeno 2 unità. La prima coppia di serie da costruire secondo questo metodo appena illustrato è la coppia $(S_2;S_3)$; la seconda è la coppia $(S_4;S_5)$; e così via.

Se la differenza tra le serie della coppia $(S_i;S_{i+1})$ è sempre uguale o al più maggiore di 2 , allora la differenza stessa si manterrà uguale a 2 (confermando perciò la primalità del numero i+1) solo se i numeri della serie S_{i+1} che non sono nè il primo termine della serie nè gli ultimi termini della serie, cioè quelli uguali a 1 , si mantengono uguali sia in questa serie che nella serie S_i . Ad esempio, considerando le serie S_6 e S_7 , queste due serie hanno, rispettivamente, 6 e 7 come primo termine e 1+1+1 e 1+1+1+1 come ultimi termini: quindi, dato che gli altri termini che non ho ancora considerato (si potrebbero chiamare termini "centrali") sono uguali sia in una che nell'altra serie, essendo in entrambe 3+2 , allora la differenza tra la somma dei termini di S_7 e la somma di quelli di S_6 si manterrà sul valore 2 , essendo determinata dal primo e dagli ultimi termini di entrambe. Quindi i+1=7 è un numero primo.

Ora, consideriamo il numero i+1=9 : questo è il primo numero dispari che si incontra che non è primo; riflettiamo: perchè mai non è primo? Perchè, come si è già detto, non ha i termini "centrali" di cui parlavo più sopra uguali ai termini centrali di i=8 ; ma perchè mai è vero questo? Questo fatto dipende dai divisori che dividono esattamente i+1=9 restituendo almeno una parte dei termini "centrali" di S_9 .

Infatti, siccome per calcolare i termini "centrali" si divide il valore di i+1 o di i , rispettivamente, per i numeri Naturali compresi tra 2 e il troncamento del risultato di $\frac{i+1}{2}$ e $\frac{i}{2}$, e del risultato della divisione di i e i+1 per questi numeri Naturali si considera solo la parte intera, se così facendo i ottiene d risultati, e d sono il numero dei divisori (esatti) di i , allora i+1 non sarà divisibile per nessuno di quei numeri Naturali, ma comunque otterrà gli stessi d risultati. Per esempio: se i=6 , per calcolare i termini "centrali" di S_6 si divide 6 per 2 e poi per 3 ; così facendo i ottiene d=2 risultati, e 2 sono proprio i divisori (esatti) di i : che sono proprio 2 e 3 . Allora, i+1=7 non sarà mai

divisibile esattamente nè per 2 nè per 3 ; ma comunque, dividendo 7 prima per 2 e poi per 3 e considerando del risultato solo la parte intera (troncamento), i+1 ottiene anch'esso d=2 risultati, che sono 2 e 3 .
Schema:

div 6={2, 3}
div 7={}
.

Quindi, i divisori (esatti) di i non possono essere divisori esatti anche di i+1 : viceversa, vale che i divisori esatti di i+1 non potranno mai essere divisori esatti anche di i . Perciò, se i+1 non ha alcun divisore esatto che restituisca i termini "centrali", i+1 avrà comunque gli stessi d risultati che ottiene i mediante i suoi divisori esatti: perchè di tutte le divisioni si considera sempre solo la parte intera. Accade perciò che quando i+1 ha propri divisori esatti, siccome i+1 è maggiore di i , allora il termine "centrale" che deriva dalla divisione di i+1 per il suo divisore esatto sarà maggiore di 1 unità rispetto al termine "centrale" che deriva dalla divisione dal risultato troncato di i per lo stesso divisore.
Schema:

div 8={2, 4}
div 9={3}

$\frac{8}{3} = 2$
$\frac{9}{3} = 3 \rightarrow$ il termine "centrale" che deriva dalla divisione esatta è sempre maggiore di 1 unità rispetto al termine centrale che deriva dalla divisione troncata.

Perciò, siccome i è minore di i+1 , quando si divide sia i=8 che i+1=9 prima per 2 e poi per 4 , si ottengono gli stessi risultati. Di conseguenza, il risultato che "sballa", rendendo cioè diversa la somma dei termini "centrali" di S_i e S_{i+1} è proprio il divisore esatto di i+1 , cioè 3 . Da cui, si deduce il Teorema 1 generale: "Se esiste almeno un divisore esatto di i+1 tra i numeri Naturali che si utilizzano per dividere sia i che i+1 per calcolare i termini "centrali", allora $S_{i+1} - S_i$ sarà maggiore di 2". (I numeri Naturali che si utilizzano per dividere sia i che i+1 per calcolare i termini "centrali", sono i numeri Naturali compresi tra 2 e, rispettivamente, la parte intera del risultato delle divisioni $\frac{i}{2}$ e $\frac{i+1}{2}$).

Un numero primo è un numero che ha per divisori solo sè stesso e l'unità: dato che questi divisori sono quindi già 2 , non è ammesso un terzo divisore, cioè non è ammessa una quantità maggiore di divisori. Perciò, un numero primo è riconoscibile dal fatto che non ha più di 2 divisori, ma ne ha proprio sempre e solo 2 .
Ma è dunque ovvio, che se si dividesse i e i+1 entrambi per 1 , vuol dire che si sta dividendo un numero candidato primo per l'unità; mentre quando si dividesse sia i che i+1 per un numero Naturale maggiore della loro metà (arrotondata sempre per difetto), siccome del risultato della divisione si considera solo la parte intera, allora questo risultato sarebbe per ognuno di quei valori sempre l'equivalente della divisione di i e i+1 , rispettivamente, per i e i+1 , il che vuol dire che si sta dividendo il numero candidato primo per sè stesso. Infatti, se è vero che possiamo assumere che

un numero è diviso per sè stesso quando dà per risultato 1 , allora, siccome delle nostre divisioni consideriamo solo la parte intera, i numeri i e i+1 , divisi per qualsiasi numero Naturale maggiore della loro metà (arrotondata sempre per difetto), è come se fossero divisi, rispettivamente, proprio per i e i+1 . A questo punto, si è già diviso il numero candidato primo per due tipi di divisori: l'unità e sè stesso. Prendiamo ora ad esempio il numero i+1=9 : la sommatoria dei termini della serie S_9 è: 9+4+3+2+1+1+1+1+1 . Cosa vogliono dire i termini di questa sommatoria? Vogliono dire che, i termini uguali a 1 , è come se fossero (sempre) il risultato di 9 diviso sè stesso, mentre il termine uguale a 9 è come se fosse il risultato di 9 diviso l'unità: perciò, se tra gli altri termini rimanenti (che sono i termini che ho chiamato "centrali") non ci sono divisori esatti di i+1=9 , allora 9 avrà soltanto, come divisori esatti, ovviamente sè stesso e l'unità (cioè 2 divisori): e la conseguenza di ciò, per il Teorema 1 generale che ho dedotto più sopra, è che la somma dei termini "centrali" sarà uguale a alla somma dei termini "centrali" della serie S_8 . Se quest'ultima cosa è vera, la differenza tra le serie della coppia $(S_8 ; S_9)$ è 2 , perchè, si è detto molto più sopra nel documento, "il numero di 1 che compaiono in coda alle serie S_i e S_{i+1} , con i che è pari, differisce di 1 unità, che, sommata all'altra unità per la quale differiscono sempre queste due serie consecutive per via del loro primo termine, determina una differenza sulla sommatoria dei termini che minimo è 2 unità". Un numero anche non primo ha sempre almeno due divisori, che sono sè stesso e l'unità: quindi, gli altri suoi divisori vanno ricercati analizzando i risultati dei termini "centrali" delle serie, cioè contando quanti di questi termini scaturiscono da una divisione senza resto. Ovviamente, il valore i+1=9 non determina quindi che 9 è un numero primo.

E così si dimostra sia la validità della formula per calcolare il numero di divisori che la validità del test di primalità ad essa associato.

Giorgio Lamberti, 05/03/2013