Block Notes Matematico

Il crivello di Dirichlet

Il problema dei divisori di Dirichlet

ing. Rosario Turco

Abstract

Nel seguito esamineremo il classico problema dei divisori di Dirichlet ed evidenzieremo un crivello che ne nasce per conseguenza. Nel seguito il simbolo $\lfloor x \rfloor$ o il floor indica "il più grande intero minore o uguale a x".

Il crivello di Dirichlet

Teorema: Sia N un intero positivo e definiamo:

$$D(N)=\sum_{i=1}^{N}\left(\left\lfloor \frac{N}{i} \right\rfloor-\left\lfloor \frac{N-1}{i} \right\rfloor\right) \qquad (1)$$

Allora nella (1) D(N) è il numero di divisori interi del numero N e se D(N)=2 allora N è un numero primo.

Dimostrazione

La (1) la possiamo riscrivere portando fuori di essa i termini i=1 ed i = N, che valgono 1 ciascuno:

$$D(N)=\sum_{i=2}^{N-1}\left(\left\lfloor \frac{N}{i} \right\rfloor-\left\lfloor \frac{N-1}{i} \right\rfloor\right)+2 \qquad (2)$$

La (2) è valida per ogni N>2. Nella (2), quindi, abbiamo tirato fuori il divisore 1 e N (cioè sé stesso). Ora Se indichiamo l'i-esimo termine della (2) con d(i):

$$d(i)=\left\lfloor \frac{N}{i} \right\rfloor-\left\lfloor \frac{N-1}{i} \right\rfloor \qquad (3)$$

poiché i valori di N e N-1 divisi per l'i-esimo termine sono molto prossimi, allora la d(i) è 0 oppure è uguale a 1. Un numero N che ha come divisori solo 1 ed N è un numero primo, per cui deve essere D(N)=2; mentre la sommatoria della (2) deve essere nulla. Ulteriormente per N composto la sommatoria nella (2) è una $\sum_{i\le N-1} 1$ e, inoltre, si ottiene 1 per quei d(i) dove N è multiplo di i; cioè:

$$d(i)=\begin{cases}0 & \text{se } N \text{ non è multiplo di } i\\ 1 & \text{se } N \text{ è multiplo di } i\end{cases} \qquad (4)$$

Se, quindi, il numero N è composto la sommatoria di 1 della (2) è diversa da zero già con un solo 1; per cui è sufficiente trovare il primo d(i) non nullo per poter dire che il numero è composto.

La (4) ci permette di dire che:

$$se\ \forall i\ \text{d(i)=0 N è primo}$$
$$\text{se } \exists \text{i: d(i)=1 N non è primo}$$

Algoritmi di primalità

In appendice "Algoritmo A" è un semplice esempio di elaborazione della (1). Con esso si trova ad esempio usando Prim(N) che il numero di divisori D(5)=2, D(4)=3; ovviamente se D(N)=2, N è primo.

Il difetto dell'algoritmo A è che si deve eseguire tutta la sommatoria (1). Con la (2) sapendo che se D(N)=2 allora N è primo, ne consegue che se N è primo nella (2) la sommatoria è nulla; mentre se la sommatoria non è nulla allora N non è primo. Dobbiamo calcolare tutta la sommatoria? No.

Questo si può fare facendo un ciclo for per i=2…N-1 e arrestandoci alla prima differenza diversa da zero. Ma si deve ciclare fino a N-1? No: è sufficiente fino alla radice di N (vedi "Algoritmo B" funzione Prim2(N)).

Il metodo del crivello di Dirichlet è simile al crivello di Eratostene, che faceva per tentativi e in ciclo la divisione per i numeri a partire da 2 fino alla radice quadrata del numero e si arrestava al primo numero divisore trovato. L'algoritmo B del crivello di Dirichlet nel ciclo, però, fa oltre alla divisione presente nel crivello di Eratostene anche una seconda divisione, due operazioni di floor e una differenza; per cui è leggermente più lento del crivello di Eratostene.

Il problema della (2) è quindi di dover trovare almeno un d(i) uguale a 1 per verificare se il numero è composto; mentre se è primo si deve scorrere tutto il ciclo for. Per ottenere lo stesso scopo della (4) ma con maggiore velocità si può, invece, introdurre la *funzione di Moebius sul numero N* e usarla al posto dei singoli d(i).

Ricordiamo che la funzione di Moebius è tale che:

$$\mu(n)=\begin{cases}1 & \text{se n=1}\\ 0 & \text{se } p^2|n\\ (-1)^k & \text{se k fattori primi}\end{cases}$$

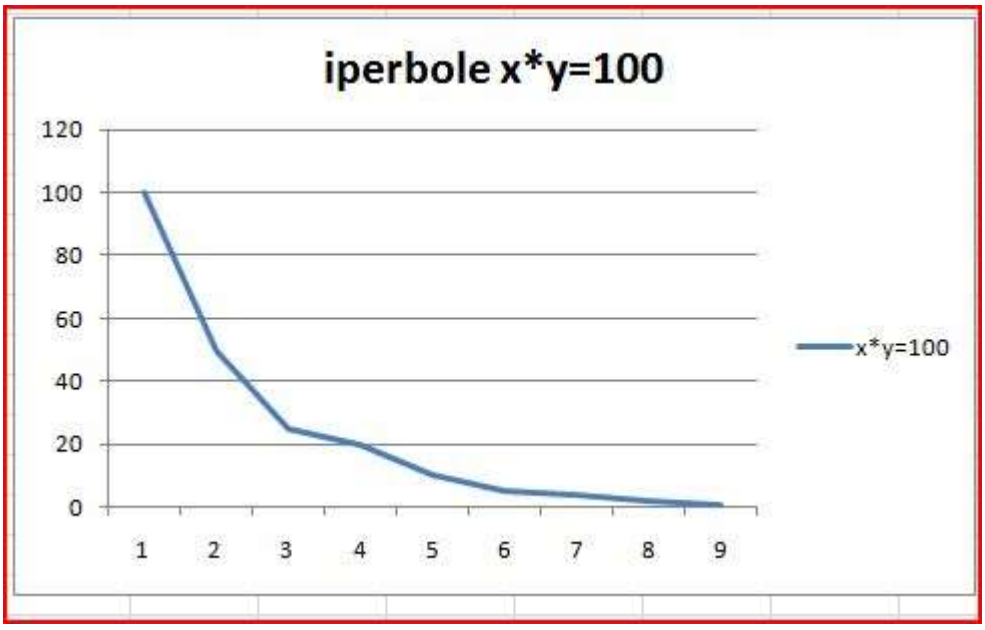
Per cui se la funzione di Moebius è uguale a 0, N è un composto, se è uguale a 1 significa che k è pari ed N è un composto, mentre se la funzione di Moebius è -1 e k=1 allora N è un primo. Il k=1 lo possiamo ricavare con la funzione $\omega(n)$ che dà il numero di fattori distinti (Vedi Algoritmo C). L'algoritmo C è sicuramente più veloce di quelli A e B, ma rientra nelle tecniche di primalità MPQS finora note. In altri termini il crivello di Dirichlet sebbene interessante non è certo tra quelli che possano apportare novità tali da avere algoritmi di primalità più veloci.

Il problema dei divisori di Dirichlet

Il problema dei divisori di Dirichlet studia in quanti modi si può scomporre n in prodotto di due numeri x e y e, quindi, si riconduce a trovare d(k), il numero di divisori di k:

$$d(n) := \{(x, y) \in NxN : xy = n\} \quad (5)$$

Il numero d(n) espresso dalla (5) è il numero di punti (x,y) a coordinate intere e positive sull'iperbole equilatera x*y=n e la somma d(1) + d(2) + ... + d(n) corrisponde ai punti $0<y\leq n/x$.



Iperbole equilatera xy=100

Una approssimazione analitica di questo numero è l'area sotto l'iperbole data dall'integrale:

$$\int_1^N \frac{N}{x} dx = N \log(N) \quad (6)$$

In altri termini la (6) dice che in media un numero N ha log(N) divisori.

In base a tecniche sul "problema del cerchio di Gauss" (Vedi [4]), Dirichlet arrivò ad un risultato più preciso, suddividendo l'area sotto l'iperbole in un quadrato di vertici $Q = (0,0)(0,\sqrt{n})(\sqrt{n},\sqrt{n})(\sqrt{n},0)$, un trapezio curvilineo $T1 = (0,\sqrt{n})(\sqrt{n},\sqrt{n})(1,n)(0,n)$ e un altro trapezio $T2 = (\sqrt{n},0)(n,0)(n,1)(\sqrt{n},\sqrt{n})$.

Considerò le due zone trapezoidali (problema del cerchio di Gauss) contenente lo stesso numero di punti interi, e ricavò alla fine che il numero di punti è $n\log n + n(2\gamma - 1) + O(\sqrt{n})$. Dove γ è la costante di Eulero-Mascheroni. Mentre in media il numero di divisori è $\log n + (2\gamma - 1)$.

Algoritmo A

```
Prim(N) = local(S=0, ret=0); {
 if(N==2,return(1););
 S = 2 + sum(i=2,N-1,floor(N/i)-floor((N-1)/i)) ;
 print("Divisori di N = ", S);
 if(S == 2, ret=1;);
 return(ret);
}
```

Algoritmo B

```
Prim2(N) = local(lim=0, ret=1); {
 if(N==2,return(1););
 lim=floor(sqrt(N))+1;
 for(i=2,lim,
    if( (floor(N/i)-floor((N-1)/i))!=0, ret=0; i=N;);
 );
 return(ret);
}
```

Algoritmo C

```
Prim3(N) = local(ret=0); {
 m=moebius(N);
 f=omega(N);
 if(m==0|m==1, return(0); );
 if(f==1&m==-1, return(1););
  return(ret);
}
```

Riferimenti

[1] http://www.research.att.com/~njas/sequences/A006218

[2] http://en.wikipedia.org/wiki/Divisor_summatory_function

[3] http://mathworld.wolfram.com/DirichletDivisorProblem.html

[4] Area e punti interi – Leonardo Colzani . Dipartimento di Matematica Università degli studi di Milano-Bicocca