2 Il prodotto di Dirichlet di funzioni aritmetiche

Nel paragrafo precedente abbiamo visto che, data una funzione aritmetica moltiplicativa f, anche la funzione

$$\sigma_f(n) := \sum_{d|n} f(d)$$

è una funzione aritmetica moltiplicativa.

Una generalizzazione di questa idea è stata perseguita da E.T. Bell nel 1915 introducendo un nuovo tipo di moltiplicazione tra funzioni aritmetiche, che prende spunto dalla teoria delle serie di Dirichlet.

Definizione 2.1. Siano f e g due funzioni aritmetiche. Definiamo il loro *prodotto (di convoluzione) di Dirichlet* ponendo

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \ .$$

Si vede immediatamente che:

$$\sigma_f = f * \mathbf{1} \tag{2.1.1}$$

e, quindi,

$$\tau = \mathbf{1} * \mathbf{1} \ , \quad \sigma = e * \mathbf{1} \ ,$$

e, più generalmente,

$$\sigma^k = e^k * \mathbf{1} \ , \quad \text{per ogni } k \geq 0 \ .$$

Un ruolo molto importante in relazione al prodotto di Dirichlet ha la funzione μ introdotta da Möbius.

Definizione 2.2. Sia

$$n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$$

la fattorizzazione in primi distinti di un intero $n \geq 2$, con $e_i \geq 1$ per $1 \leq i \leq r$. Si ponga:

$$\mu(n) := \begin{cases} 1 & \text{se } n = 1 \ , \\ (-1)^r & \text{se } n \geq 2 \ \text{ e } \ e_1 = e_2 = \cdots = e_r = 1 \ , \\ 0 & \text{altrimenti} \ . \end{cases}$$

La funzione sopra definita viene chiamata *funzione μ di Möbius* ed è una funzione moltiplicativa, ma non totalmente moltiplicativa.

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	...

È subito visto che $\mu(n) = 0$ se e soltanto se n ha un fattore quadratico > 1.

Proposizione 2.3. *$\mu * \mathbf{1} = u$; cioè, per ogni $n \geq 1$:*

$$\sum_{d|n} \mu(d) = \left\{ \begin{array}{l} 1, \ \textit{se } n = 1 \\ 0, \ \textit{se } n \geq 2 \end{array} \right\} = \left[\frac{1}{n} \right] \ .$$

Dimostrazione. La formula è ovviamente vera per $n = 1$. Poiché $\sigma_\mu = \mu * \mathbf{1}$ è una funzione moltiplicativa (Proposizione 1.4 e (2.1.1)), utilizzando la Proposizione 1.6, basta dimostrare che, per ogni primo p e per ogni $e \geq 1$, risulta:

$$\sigma_\mu(p^e) = \sum_{d|p^e} \mu(d) = 0 \ .$$

Dalla definizione di μ discende immediatamente che:

$$\sum_{d|p^e} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) = 1 - 1 + 0 + \cdots + 0 = 0 \ .$$

$\square$

Teorema 2.4. *Il prodotto di Dirichlet tra funzioni aritmetiche gode delle seguenti proprietà: prese comunque le funzioni aritmetiche f, g ed h:*

(a) $f * g = g * f$ *(proprietà commutativa);*

(b) $(f * g) * h = f * (g * h)$ *(proprietà associativa);*

(c) $f * u = f = u * f$ *(possiede come elemento neutro la funzione u).*

Dimostrazione. (a) Basta osservare che $f * g$ si può anche esprimere nella maniera seguente:

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) \ ,$$

(dove a e b variano tra tutti gli interi positivi tali che il loro prodotto è uguale ad n).

Allora, è subito visto che:

$$\sum_{ab=n} f(a)g(b) = \sum_{ab=n} g(b)f(a) = \sum_{ba=n} g(a)f(b) = \sum_{ab=n} g(a)f(b) = (g * f)(n) \ .$$

(b) Non è difficile assicurarsi che:

$$((f * g) * h)(n) = \sum_{abc=n} f(a)g(b)h(c) = (f * (g * h))(n)$$

(dove a, b e c variano tra tutti gli interi positivi tali che il loro prodotto è uguale ad n).

(c) Per (a), basta far vedere che $f * u = f$.

Se $n = 1$, allora è ovvio che $(f * u)(1) = f(1)u(1) = f(1)$. Se $n \geq 2$, allora:

$$(f * u)(n) = \sum_{d|n} f(d)u\left(\frac{n}{d}\right) = f(n)$$

perché $u\left(\frac{n}{d}\right) = 1$ se $d = n$, mentre $u\left(\frac{n}{d}\right) = 0$ se $d \neq n$.

□

Sia A l'*insieme di tutte le funzioni aritmetiche f tali che $f(1) \neq 0$.*

Teorema 2.5. *$(A, *)$ è un gruppo abeliano. In altri termini, tenendo conto del Teorema 2.4, per ogni $f \in A$ esiste un'unica funzione aritmetica f^{-1} in A, chiamata* l'inversa di Dirichlet di f, *tale che:*

$$f * f^{-1} = u = f^{-1} * f \ .$$

Precisamente, f^{-1} è definita per ricorrenza nella maniera seguente:

$$f^{-1}(n) := \begin{cases} \frac{1}{f(1)}, & \textit{se } n = 1; \\ \left(\frac{-1}{f(1)}\right)\left(\sum\limits_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)\right), & \textit{se } n > 1 \ . \end{cases}$$

Dimostrazione. Data la funzione f, per ogni $n \geq 1$ dobbiamo mostrare che l'equazione:

$$(f * f^{-1})(n) = u(n)$$

ha un'unica soluzione, la quale determina il valore $f^{-1}(n)$ della funzione f^{-1} calcolata in n.

Per $n = 1$, abbiamo:

$$(f * f^{-1})(1) = u(1) \ , \text{ ovvero, } f(1)f^{-1}(1) = 1 \ ,$$

e, quindi, essendo $f(1) \neq 0$, allora:

$$f^{-1}(1) = \frac{1}{f(1)}$$

e, dunque, $f^{-1}(1) \neq 0$.

Procediamo per induzione su $n \geq 1$. Supponiamo $n \geq 2$ e di aver determinato univocamente i valori di $f^{-1}(k)$ per ogni k con $1 \leq k < n$. Ci proponiamo di determinare univocamente il valore di $f^{-1}(n)$ in modo tale che:

$$(f * f^{-1})(n) = u(n) = 0 \ .$$

Questa equazione può essere scritta nella maniera seguente:

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0 \ .$$

Dunque, essendo noti (per ipotesi induttiva) i valori di $f^{-1}(d)$ quando $d < n$ ed essendo $f(1) \neq 0$, abbiamo necessariamente che

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \ .$$

Si noti che se $f', f'' \in A$ sono tali che $f * f' = u = f' * f$, $f * f'' = u = f'' * f$, allora $f' = f' * u = f' * (f * f'') = (f' * f) * f'' = u * f'' = f''$.
$\square$

Corollario 2.6. $\mu^{-1} = \mathbf{1}$ *(ovvero* $\mathbf{1}^{-1} = \mu$*).*

Dimostrazione. Semplice conseguenza della Proposizione 2.3 e del Teorema 2.5.

$\square$

Osservazione 2.7. (a) Si noti che la dimostrazione del Teorema 2.5 prova che, se f è una funzione aritmetica, allora:

f è invertibile (rispetto al prodotto di Dirichlet) $\Leftrightarrow f(1) \neq 0 \Leftrightarrow: f \in A$.

(b) Si noti che se $f, g \in A$ allora

$$(f * g)^{-1} = g^{-1} * f^{-1} = f^{-1} * g^{-1} \ .$$

Infatti, $(f * g) * g^{-1} * f^{-1} = f * (g * g^{-1}) * f^{-1} = f * u * f^{-1} = f * f^{-1} = u$.

Proposizione 2.8. *$e = \varphi * \mathbf{1}$; cioè, per ogni $n \geq 1$, risulta:*

$$n = \sum_{d|n} \varphi(d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) \ .$$

Dimostrazione. Questa proprietà della funzione φ è stata essenzialmente già verificata nella dimostrazione del Teorema I.5.13. Per maggiori dettagli cfr. anche l'Esercizio 1.5.

$\square$

Corollario 2.9. (a) *$\varphi = e * \mu$ (ovvero, $\varphi(n) = \sum_{d|n} n \frac{\mu(d)}{d}$, per ogni $n \in \mathbb{N}^+$).*

(b) *$\mathbf{1} = \tau * \mu$ (ovvero, $1 = \sum_{d|n} \tau(d) \frac{\mu(n)}{d}$, per ogni $n \in \mathbb{N}^+$).*

(c) *$e = \sigma * \mu$ (ovvero, $n = \sum_{d|n} \sigma(d) \frac{\mu(n)}{d}$, per ogni $n \in \mathbb{N}^+$).*

Dimostrazione. (a) segue dalle Proposizioni 2.3 e 2.8. (b) e (c) sono conseguenze della Proposizione 2.3 e del fatto che $\tau = \mathbf{1} * \mathbf{1}$ e $\sigma = e * \mathbf{1}$.

$\square$

Lo scopo che ci prefiggiamo ora è quello di descrivere meglio gli inversi rispetto al prodotto di Dirichlet di alcune funzioni moltiplicative.

Proposizione 2.10. *Se f è una funzione totalmente moltiplicativa allora $f(1) = 1$ e $f^{-1} = \mu f$, dove il prodotto di giustapposizione di funzioni aritmetiche è definito nella maniera seguente:*

$$(\mu f)(n) := \mu(n) f(n) \ , \quad \text{per ogni } n \geq 1 \ .$$

Dimostrazione. Se f è una funzione moltiplicativa (anche non totalmente) allora necessariamente $f(1) = 1$ perché:

$$f(n) = f(n \cdot 1) = f(n) f(1) \ .$$

Per concludere basta far vedere che:

$$\mu f * f = u \ .$$

Infatti,

$$(\mu f * f)(n) = \sum_{d|n} (\mu f)(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right)$$

e poiché f è totalmente moltiplicativa allora:

$$\begin{aligned} \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) f(n) = \\ &= f(n)\left(\sum_{d|n} \mu(d)\right) = f(n)((\mu * 1)(n)) = f(n)u(n) \ . \end{aligned}$$

Si conclude facilmente osservando che $f(n)u(n) = u(n)$, per ogni $n \geq 1$.

□

Corollario 2.11. **(a)** $e^{-1} = \mu e$.
(b) $\tau^{-1} = \mu * \mu$.
(c) $\sigma^{-1} = \mu e * \mu$.
(d) $\varphi^{-1} = \mu e * \mathbf{1}$ *(ovvero,* $\varphi^{-1}(n) = \sum_{d|n} \mu(d) d$*, per ogni* $n \geq 1$*).*

Dimostrazione. (a) segue immediatamente dalla Proposizione 2.10.
(b) discende dal fatto che $\tau = \mathbf{1} * \mathbf{1}$ e che $\mathbf{1}^{-1} = \mu$.
(c) discende dal fatto che $\sigma = e * \mathbf{1}$, che $e^{-1} = \mu e$ e che $\mathbf{1}^{-1} = \mu$.
(d) segue da $\varphi = e * \mu$, da $\mu^{-1} = \mathbf{1}$ e da $e^{-1} = \mu e$.

□

Nelle seguenti tavole calcoliamo esplicitamente i primi valori delle funzioni inverse (rispetto al prodotto di Dirichlet) delle funzioni aritmetiche moltiplicative sopra esaminate.

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$e^{-1}(n)$	1	-2	-3	0	-5	6	-7	0	0	10	-11	0	...

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$\tau^{-1}(n)$	1	-2	-2	1	-2	4	-2	0	1	4	-2	-2	...

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$\sigma^{-1}(n)$	1	-3	-4	1	-6	12	-8	0	4	18	-12	-8	...

n	1	2	3	4	5	6	7	8	9	10	11	12	...
$\varphi^{-1}(n)$	1	-1	-2	0	-4	2	-6	-1	-2	4	10	2	...

Osservazione 2.12. Dalla definizione di μ e dal fatto che $e^{-1} = \mu e$ si ricava immediatamente che:

$$e^{-1}(n) = \begin{cases} 1, & \text{se } n = 1 \ ; \\ (-1)^r n, & \text{se } n \geq 2 \text{ e } e_1 = e_2 = \cdots = e_r = 1 \ ; \\ 0, & \text{altrimenti} \ ; \end{cases}$$

dove $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ è la fattorizzazione in primi distinti di $n \geq 2$, con $e_i \geq 1$ per $1 \leq i \leq r$.

Proposizione 2.13. *Sia f una funzione moltiplicativa non costante su 0. Allora:*

(a) *$\mu f * \mathbf{1}$ è una funzione moltiplicativa.*

(b) *Se $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ è la decomposizione in fattori primi distinti di $n \geq 2$ (con $e_i \geq 1$ per $1 \leq i \leq r$) allora:*

$$(\mu f * \mathbf{1})(n) = \prod_{i=1}^{r} (1 - f(p_i)) \ .$$

Dimostrazione. (a) Si noti, in generale, che se f, g sono funzioni moltiplicative, allora la funzione fg ottenuta per prodotto di giustapposizione e definita ponendo $(fg)(n) := f(n)g(n)$ è anch'essa una funzione moltiplicativa. L'enunciato segue ora dalla Proposizione 1.4.

(b) Basta osservare che, per ogni primo p e per ogni $e \geq 1$, $(\mu f * \mathbf{1})(p^e) = \mu(1)f(1) + \mu(p)f(p) + 0 \cdot f(p^2) + \cdots + 0 \cdot f(p^e) = 1 - f(p)$.

□

Corollario 2.14. *Per ogni $n \geq 2$, si ha:*

$$\varphi^{-1}(n) = \prod_{p|n} (1 - p) \ .$$

Dimostrazione. Dal momento che $\varphi = e * \mu$ (Corollario 2.9 (a)), allora $\varphi^{-1} = e^{-1} * \mu^{-1} = \mu e * \mathbf{1}$. La conclusione discende immediatamente dalla Proposizione 2.13 (b).

□

2 Esercizi e Complementi

2.1. Mostrare che, per ogni $k \geq 0$,

(a) $(e^k)^{-1} = \mu e^k$

(b) $(\sigma^k)^{-1} = \mu e^k * \mu$.

[*Suggerimento.* (a) Basta osservare che e^k è una funzione totalmente moltiplicativa e, quindi, si può applicare la Proposizione 2.10.

(b) Si noti che $\sigma^k = \sigma_{e^k} = e^k * \mathbf{1}$, quindi $(\sigma^k)^{-1} = (e^k)^{-1} * \mu$.]

2.2. Sia f una funzione moltiplicativa, non costante su 0. Mostrare che:

$$f \text{ è totalmente moltiplicativa} \Leftrightarrow f^{-1} = \mu f.$$

[*Dimostrazione.* ($\Rightarrow$) già dimostrata nella Proposizione 2.10.

($\Leftarrow$). Basta mostrare che, per ogni primo p e per ogni intero $e \geq 1$, $f(p^e) = (f(p))^e$. Si noti che, dall'uguaglianza $u = f^{-1} * f = \mu f * f$, ricaviamo che per ogni $n > 1$:

$$\sum_{d|n} \mu(d) f(d) f\Big(\frac{n}{d}\Big) = 0 \ .$$

In particolare, per $n = p^e$,

$$\mu(1) f(1) f(p^e) + \mu(p) f(p) f(p^{e-1}) = 0$$

cioè

$$f(p^e) - f(p) f(p^{e-1}) = 0 \ .$$

Da tale relazione si ricava facilmente per induzione, su $e \geq 1$, che $f(p^e) = (f(p))^e$.]

2.3. Sia $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ la fattorizzazione in primi distinti di $n \geq 2$ (con $e_i \geq 1$ per $1 \leq i \leq r$). Mostrare che valgono le seguenti uguaglianze:

(a) $\displaystyle\sum_{d|n} \mu(d) d = \prod_{i=1}^{r} (1 - p_i)$.

(b) $\displaystyle\sum_{d|n} \frac{\mu(d)}{d} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

(c) $\displaystyle\sum_{d|n} \mu(d) \tau(d) = (-1)^r$.

(d) $\displaystyle\sum_{d|n} \mu(d) \sigma(d) = (-1)^r \prod_{i=1}^{r} p_i$.

(e) $\sum_{d|n} \mu(d)\sigma^k(d) = (-1)^r \prod_{i=1}^{r} p_i^k$.

(f) $\sum_{d|n} \mu(d)\varphi(d) = \prod_{i=1}^{r} (2 - p_i)$.

[*Suggerimento.* Semplice applicazione della Proposizione 2.13 dove f è la funzione:

- e nel caso (a) (con $e(p) = p$);
- $\frac{1}{e}$ nel caso (b) (con $\frac{1}{e}(p) = \frac{1}{p}$);
- τ nel caso (c) (con $\tau(p) = 2$);
- σ nel caso (d) (con $\sigma(p) = 1 + p)$);
- σ^k nel caso (e) (con $\sigma^k(p) = 1 + p^k$);
- φ nel caso (f) (con $\varphi(p) = p - 1$).

Si osservi che la formula (b) è strettamente collegata alla formula seguente (Corollario 1.7 (c)):

$$\varphi(n) = n \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) .$$

Infatti, la (b) si può ricavare anche dalla formula precedente, tenendo presente l'Esercizio 1.5 e notando che:

$$\varphi * \mathbf{1} = e \Rightarrow \varphi = e * \mu \Rightarrow \frac{1}{e}\varphi = \frac{1}{e}(e * \mu) \Rightarrow \frac{1}{e}\varphi = \mathbf{1} * \frac{1}{e}\mu = \frac{1}{e}\mu * \mathbf{1}$$

cioè $\frac{1}{n}\varphi(n) = \left(\frac{1}{e}\varphi\right)(n) = \left(\frac{1}{e}\mu * \mathbf{1}\right)(n) = \sum_{d|n} \frac{1}{d}\mu(d)$.]

2.4. Siano f, g, h tre funzioni aritmetiche. Mostrare che:
(a) $(f + g) * h = (f * h) + (g * h)$;
(b) se f è totalmente moltiplicativa, allora:

$$f(g * h) = fg * fh ,$$

(dove, al solito, $(f + g)(n) := f(n) + g(n)$ e $(fg)(n) := f(n)g(n)$, per ogni n).

[*Dimostrazione.*
(a)

$$\begin{aligned} ((f+g)*h)(n) &= \sum_{d|n}(f+g)(d)h\Big(\frac{n}{d}\Big) = \sum_{d|n}(f(d)+g(d))h\Big(\frac{n}{d}\Big) = \\ &= \sum_{d|n} f(d)h\Big(\frac{n}{d}\Big) + \sum_{d|n} g(d)h\Big(\frac{n}{d}\Big) = \\ &= (f*h)(n) + (g*h)(n) . \end{aligned}$$

(b)

$$\begin{aligned}(f(g*h))(n) &= f(n)\sum_{d|n} g(d)h\Big(\frac{n}{d}\Big) = f(d)f\left(\frac{n}{d}\right)\sum_{d|n} g(d)h\Big(\frac{n}{d}\Big) = \\ &= \sum_{d|n} f(d)g(d)f\Big(\frac{n}{d}\Big)\,h\Big(\frac{n}{d}\Big) = (fg*fh)(n)\ .]\end{aligned}$$

2.5. Sia f una funzione moltiplicativa, non costante su 0. Mostrare che:

(a) se n è privo di fattori quadratici, allora:

$$f^{-1}(n) = \mu(n)f(n)\ ;$$

(b) per ogni primo p,

$$f^{-1}(p^2) = (f(p))^2 - f(p^2)\ .$$

[*Suggerimento.* (a) Si noti che, per ogni primo p,

$$0 = u(p) = (f*f^{-1})(p) = f^{-1}(p) + f(p)$$

quindi:

$$f^{-1}(p) = -f(p) = \mu(p)f(p)\ .$$

(b) Per ogni primo p si ha:

$$0 = u(p^2) = (f*f^{-1})(p^2) = f^{-1}(p^2) + f(p)f^{-1}(p) + f(p^2)$$

quindi, tenendo conto di (a),

$$f^{-1}(p^2) = (f(p))^2 - f(p^2)\ .]$$