

# 1 Funzioni aritmetiche

In Teoria dei Numeri le successioni di numeri (siano essi: interi, razionali, reali o complessi) vengono studiate sotto la terminologia di “funzioni aritmetiche”. Precisamente,

**Definizione 1.1.** Una *funzione aritmetica* è una funzione  $f : \mathbb{N}^+ \rightarrow \mathbb{C}$ , dove  $\mathbb{N}^+$  è l'insieme dei numeri interi positivi e  $\mathbb{C}$  è quello dei numeri complessi (o, equivalentemente, una funzione aritmetica è una successione  $\{a_n : n \geq 1\}$  di numeri complessi, con  $a_n = f(n)$  che definisce “esplicitamente” una funzione  $f : \mathbb{N}^+ \rightarrow \mathbb{C}$ ).

Particolare interesse hanno le funzioni aritmetiche che godono di proprietà di “preservazione del prodotto”. Precisamente,

**Definizione 1.2.** Una *funzione aritmetica*  $f : \mathbb{N}^+ \rightarrow \mathbb{C}$  si dice *moltiplicativa* se, presi  $n, m \in \mathbb{N}^+$ ,

$$\text{MCD}(n, m) = 1 \Rightarrow f(nm) = f(n)f(m) .$$

Una *funzione aritmetica* si dice *totalmente moltiplicativa* se, presi comunque  $n, m \in \mathbb{N}^+$ ,  $f(nm) = f(n)f(m)$ .

**Esempio 1.3. (a)** La *funzione  $\varphi$  di Euler*, dove

$$\varphi(n) := \#(\{k \in \mathbb{N}^+ : \text{MCD}(k, n) = 1 \text{ e } 1 \leq k \leq n\})$$

è una funzione (aritmetica) moltiplicativa (dove  $\#A$  denota il numero degli elementi dell'insieme  $A$ ; cfr. anche Capitolo I, Definizione 2.9, Esercizio 2.13) ma non totalmente moltiplicativa (ad esempio  $\varphi(4) = 2$ , ma  $\varphi(2) = 1$  e quindi  $\varphi(2)\varphi(2) \neq \varphi(4)$ ).

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

**(b)** La funzione  $\tau : \mathbb{N}^+ \rightarrow \mathbb{C}$ , definita ponendo:

$$\tau(n) := \text{numero dei divisori positivi di } n = \#(\{d \in \mathbb{N}^+ : d \mid n\}) =: \sum_{d \mid n} 1$$

è subito visto essere una funzione moltiplicativa (ma non totalmente moltiplicativa perché  $\tau(4) = 3, \tau(2) \cdot \tau(2) = 2 \cdot 2 = 4$ ). Infatti, se  $\text{MCD}(n, m) = 1$ , allora l'applicazione:

$$\{d' \in \mathbb{N}^+ : d' \mid n\} \times \{d'' \in \mathbb{N}^+ : d'' \mid m\} \rightarrow \{d \in \mathbb{N}^+ : d \mid nm\}$$

definita ponendo:

$$(d', d'') \mapsto d' \cdot d''$$

è una biiezione (con funzione inversa  $d \mapsto (d', d'')$ , dove  $d' := \text{MCD}(d, n)$ ,  $d'' := \text{MCD}(d, m)$ ). Da ciò si ricava facilmente che, se  $\text{MCD}(n, m) = 1$ , allora  $\tau(n)\tau(m) = \tau(nm)$ .

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

(c) La funzione  $\sigma : \mathbb{N}^+ \rightarrow \mathbb{C}$  definita ponendo

$$\sigma(n) := \text{somma dei divisori positivi di } n =: \sum_{d|n} d$$

è una funzione moltiplicativa, ma non totalmente.

$n$	1	2	3	4	5	6	7	8	9	10	11	12	...
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	...

(d) Le funzioni sopra considerate  $\tau$  e  $\sigma$  sono dette *funzioni dei divisori*; tali funzioni sono casi particolari (per  $k = 0$  e  $k = 1$ , rispettivamente) della funzione aritmetica:

$$\sigma^k(n) := \sum_{d|n} d^k$$

detta *funzione delle potenze  $k$ -esime dei divisori*, dove  $k \geq 0$  è un intero fissato.

(e) Per ogni fissato  $c \in \mathbb{C}$ , la *funzione costante*

$$\mathbf{c} : \mathbb{N}^+ \rightarrow \mathbb{C}, \quad \mathbf{c}(n) := c$$

è una funzione aritmetica. È subito visto che  $\mathbf{c}$  è moltiplicativa se e soltanto se  $c = 0$  oppure  $c = 1$ . In tali casi, la funzione denotata rispettivamente con  $\mathbf{c} = \mathbf{0}$  oppure con  $\mathbf{c} = \mathbf{1}$  è totalmente moltiplicativa.

(f) La *funzione di immersione*

$$e : \mathbb{N}^+ \rightarrow \mathbb{C}, \quad e(n) := n$$

è una funzione aritmetica totalmente moltiplicativa.

(g) La funzione

$$u : \mathbb{N}^+ \rightarrow \mathbb{C}$$

dove  $u(1) := 1$  e  $u(n) := 0$  se  $n \geq 2$  è detta *funzione unità*.

La ragione di tale denominazione apparirà chiara tra poco. Si noti intanto che, per ogni  $n \in \mathbb{N}^+$ , risulta:

$$u(n) = \left[ \frac{1}{n} \right] \left( = \text{parte intera di } \frac{1}{n} \right).$$

Inoltre, è subito visto che  $u$  è una funzione totalmente moltiplicativa.

Il seguente risultato è molto utile per dimostrare la moltiplicatività di alcune funzioni o per definire nuove funzioni moltiplicative, a partire da funzioni moltiplicative già note.

**Proposizione 1.4.** *Sia  $f : \mathbb{N}^+ \rightarrow \mathbb{C}$  una funzione moltiplicativa.*

*La funzione:*

$$\sigma_f : \mathbb{N}^+ \rightarrow \mathbb{C}, \quad \sigma_f(n) := \sum_{d|n} f(d)$$

*è una funzione moltiplicativa.*

**Dimostrazione.** Abbiamo già osservato che, se  $n, m \in \mathbb{N}^+$  e  $\text{MCD}(n, m) = 1$ , l'applicazione canonica:

$$\{d' \in \mathbb{N}^+ : d' | n\} \times \{d'' \in \mathbb{N}^+ : d'' | m\} \rightarrow \{d \in \mathbb{N}^+ : d | nm\}, \quad (d', d'') \mapsto d'd''$$

è una biiezione. Pertanto, utilizzando questa proprietà e la moltiplicatività di  $f$ , abbiamo:

$$\begin{aligned} \sigma_f(nm) &= \sum_{d|nm} f(d) = \\ &= \sum_{d'|n} \sum_{d''|m} f(d'd'') = \sum_{d'|n} \sum_{d''|m} f(d')f(d'') = \\ &= \left( \sum_{d'|n} f(d') \right) \left( \sum_{d''|m} f(d'') \right) = \sigma_f(n)\sigma_f(m). \end{aligned}$$

□

**Corollario 1.5.** (a)  $\tau = \sigma_1$ .

(b)  $\sigma = \sigma_e$ .

(c) Se, per ogni  $k \geq 0$ , si definisce  $e^k : \mathbb{N}^+ \rightarrow \mathbb{C}$ , ponendo  $e^k(n) := n^k$ , allora  $\sigma^k = \sigma_{e^k}$ . (Si noti che  $e^0 = \mathbf{1}$  e  $e^1 = e$ ).

(d) La funzione  $\sigma^k$  è moltiplicativa, per ogni  $k \geq 0$ .

**Dimostrazione.** (a), (b) e (c) seguono immediatamente dalla definizione della funzione  $\sigma_f$  associata alla funzione  $f$ .

(d) segue dalla Proposizione 1.4, notando che  $e^k$  è una funzione (totalmente) moltiplicativa, per ogni  $k \geq 0$ .

□

**Proposizione 1.6.** Sia  $f$  una funzione moltiplicativa. Sia

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

la decomposizione di  $n \in \mathbb{N}^+$ ,  $n \geq 2$ , in fattori primi distinti, con  $e_i \geq 1$ , per  $1 \leq i \leq r$ . Allora

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \cdot \dots \cdot f(p_r^{e_r}) .$$

**Dimostrazione.** Per la verifica basta procedere per induzione su  $r \geq 1$ .

□

**Corollario 1.7.** Sia

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

la decomposizione di  $n \in \mathbb{N}^+$ ,  $n \geq 2$ , in fattori primi distinti con  $e_i \geq 1$ , per  $1 \leq i \leq r$ . Allora

(a)  $\tau(n) = (e_1 + 1)(e_2 + 1) \cdot \dots \cdot (e_r + 1)$ .

(b)  $\sigma(n) = \left( \frac{p_1^{e_1+1} - 1}{p_1 - 1} \right) \left( \frac{p_2^{e_2+1} - 1}{p_2 - 1} \right) \cdot \dots \cdot \left( \frac{p_r^{e_r+1} - 1}{p_r - 1} \right)$ .

(c)  $\varphi(n) = n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdot \dots \cdot \left( 1 - \frac{1}{p_r} \right) =$   
 $= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdot \dots \cdot (p_r^{e_r} - p_r^{e_r-1})$ .

**Dimostrazione.** Per quanto noto (Esempio 1.3 (a), Corollario 1.5 (c) e Proposizione 1.6), basta dimostrare che, per ogni primo  $p$  e per ogni intero  $e \geq 0$ , si ha:

$$(a') \quad \tau(p^e) = (e + 1);$$

$$(b') \quad \sigma(p^e) = \frac{p^{e+1}-1}{p-1};$$

$$(c') \quad \varphi(p^e) = p^e \left(1 - \frac{1}{p}\right) = p^e - p^{e-1}.$$

Le proprietà (a') e (b') si ricavano immediatamente dal fatto che, essendo  $p$  primo, i divisori positivi di  $p^e$  sono  $1, p, p^2, \dots, p^e$ . Inoltre, è noto che:

$$(p^{e+1} - 1) = (p - 1)(1 + p + p^2 + \dots + p^e) .$$

Per (c'), basta osservare che gli interi tra 1 e  $p^e$  che sono divisibili per  $p$  sono quelli del tipo  $kp$ , con  $k$  che varia comunque tra 1 e  $p^{e-1}$ ; quindi essi sono in numero di  $p^{e-1}$ . Pertanto, gli interi tra 1 e  $p^e$  che sono relativamente primi con  $p^e$  sono gli elementi dell'insieme complementare, dunque sono in numero di  $p^e - p^{e-1}$ .

□

**Osservazione 1.8.** Si noti che, in generale, se  $f$  è totalmente moltiplicativa  $\sigma_f$  è moltiplicativa ma *non* necessariamente totalmente moltiplicativa (ad esempio  $\tau = \sigma_1$  è moltiplicativa ma non totalmente, mentre  $\mathbf{1}$  è totalmente moltiplicativa).

# 1 Esercizi e Complementi

**1.1.** Se  $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$  è la decomposizione di  $n \in \mathbb{N}^+$ ,  $n \geq 2$  in fattori primi distinti (con  $e_i \geq 1$ , per  $1 \leq i \leq r$ ), mostrare che:

$$\sigma^k(n) = \prod_{i=1}^r \frac{(p_i^{k(e_i+1)} - 1)}{(p_i^k - 1)}.$$

[*Suggerimento.*  $\sigma^k$  è una funzione moltiplicativa. È subito visto che, per ogni primo  $p$ ,  $\sigma^k(p) = 1 + p^k$ . Per ogni  $e \geq 1$ ,  $\sigma^k(p^e) = 1 + p^k + (p^2)^k + \cdots + (p^e)^k$ . Si noti, poi, che:  $(1 + p^k + (p^2)^k + \cdots + (p^e)^k)(p^k - 1) = p^{k(e+1)} - 1$ .]

**1.2.** Mostrare che, per ogni  $n \in \mathbb{N}^+$ ,

$$\tau(n) \leq 2\sqrt{n}.$$

[*Suggerimento.* Se  $d \mid n$ , allora  $d$  oppure  $\frac{n}{d}$  è  $\leq \sqrt{n}$ .]

**1.3.** Mostrare che,

$$(a) \quad \sum_{d \mid n} \sigma(d) = n \sum_{d \mid n} \frac{\tau(d)}{d}$$

$$(b) \quad \sum_{d \mid n} d\tau(d) = n \sum_{d \mid n} \frac{\sigma(d)}{d}.$$

[*Dimostrazione.* Si noti che se  $f$  e  $g$  sono due funzioni moltiplicative, allora la funzione  $fg$  definita ponendo  $(fg)(n) := f(n)g(n)$  è una funzione moltiplicativa, così come la funzione  $\frac{f}{g}$ , quando  $g(n) \neq 0$  per ogni  $n \in \mathbb{N}^+$ , definita ponendo  $(\frac{f}{g})(n) := \frac{f(n)}{g(n)}$ . Utilizzando la Proposizione 1.4, per dimostrare (a) e (b) basta dimostrare che tali uguaglianze sussistono se  $n = p^e$ , dove  $p$  è un primo ed  $e \geq 1$ .

$$\begin{aligned} (a) \quad \sum_{d \mid p^e} \sigma(d) &= 1 + (1+p) + (1+p+p^2) + \cdots + (1+p+\cdots+p^e) = \\ &= (e+1) + ep + (e-1)p^2 + \cdots + 2p^{e-1} + p^e = \\ &= p^e \left( \frac{e+1}{p^e} + \frac{e}{p^{e-1}} + \cdots + \frac{2}{p} + 1 \right) = p^e \sum_{d \mid p^e} \frac{\tau(d)}{d}. \end{aligned}$$

$$\begin{aligned} (b) \quad \sum_{d \mid p^e} d\tau(d) &= 1 + p \cdot 2 + p^2 \cdot 3 + \cdots + p^e(e+1) = \\ &= (1+p+p^2+\cdots+p^e) + p(1+p+\cdots+p^{e-1}) + \\ &+ \cdots + p^{e-1}(1+p) + p^e = \end{aligned}$$

$$= \frac{1+p+p^2+\dots+p^e}{p^e} + \frac{1+p+\dots+p^{e-1}}{p^{e-1}} + \dots + \frac{1+p}{p} + 1 = p^e \sum_{d|p^e} \frac{\sigma(d)}{d} . ]$$

**1.4.** Dimostrare che, per  $n \in \mathbb{N}^+$ ,

(a)  $\tau(n)$  è dispari  $\Leftrightarrow n$  è un quadrato;

(b)  $\sigma(n)$  è dispari  $\Leftrightarrow n$  è un quadrato oppure  $n$  è il doppio di un quadrato.

[*Dimostrazione.* Basta osservare che un prodotto di interi è dispari se e soltanto se ogni fattore è dispari e che, per ogni primo  $p$  ed ogni intero  $e \geq 0$ ,

(a)  $\tau(p^e) = e + 1$  è dispari  $\Leftrightarrow e$  è pari  $\Leftrightarrow p^e$  è un quadrato.

(b)  $\sigma(p^e) = 1 + p + \dots + p^e$  è dispari  $\Leftrightarrow p + \dots + p^e$  è pari.

Se  $p = 2$  quest'ultima affermazione è sempre vera. Se  $p$  è dispari:

$p + \dots + p^e$  è pari  $\Leftrightarrow e$  è pari  $\Leftrightarrow p^e$  è un quadrato.]

**1.5.** Se  $\varphi : \mathbb{N}^+ \rightarrow \mathbb{C}$  è la funzione di Euler, mostrare che

$$\sigma_\varphi = e .$$

[*Suggerimento.* L'enunciato equivale a

$$\sum_{d|n} \varphi(d) = n$$

per ogni  $n \in \mathbb{N}^+$ . Per la verifica si procede essenzialmente come nella dimostrazione del Teorema I.5.13, dove si è provato un caso particolare e cioè che:

$$p - 1 = \sum_{d|(p-1)} \varphi(d) .$$

Infatti, si ripartisce l'insieme  $\{1, 2, \dots, n\}$  di cardinalità  $n$  nell'unione disgiunta degli insiemi

$$A_d := \{k \in \mathbb{N}^+ : 1 \leq k \leq n, \text{ MCD}(k, n) = d\}$$

al variare di  $d$  tra i divisori positivi di  $n$ . Si conclude osservando che l'insieme  $A_d$  è in corrispondenza biunivoca con l'insieme

$$B_d := \left\{ h \in \mathbb{N}^+ : 1 \leq h \leq \frac{n}{d}, \text{ MCD} \left( h, \frac{n}{d} \right) = 1 \right\}$$

il quale ultimo ha cardinalità  $\varphi \left( \frac{n}{d} \right)$ , per ogni  $d$  che divide  $n$ . Pertanto,

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

È ovvio poi che:

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

(l'ultima uguaglianza sussiste perché  $\{\frac{n}{d} : d | n\} = \{d : d | n\}$ .)

**1.6.** Mostrare che, per ogni  $n > 2$ ,  $\varphi(n)$  è un intero pari.

[*Dimostrazione.* Se  $n$  contiene un fattore pari, diciamo  $2^e$ , con  $e \geq 2$ , allora  $\varphi(n)$  ha come fattore  $\varphi(2^e) = 2^e - 2^{e-1} = 2^{e-1}$ . Se  $n$  ha un fattore primo dispari, diciamo  $p^e$  con  $e \geq 1$ , allora  $\varphi(n)$  ha come fattore  $\varphi(p^e) = p^e \left(\frac{p-1}{p}\right) = p^{e-1}(p-1)$  che è pari.]

**1.7.** Mostrare che, per ogni  $n \in \mathbb{N}^+$ ,

(a)  $n$  dispari  $\Rightarrow \varphi(2n) = \varphi(n)$ ;

(b)  $n$  pari  $\Rightarrow \varphi(2n) = 2\varphi(n)$ ;

(c)  $\varphi(3n) = \begin{cases} 3\varphi(n), & \text{se } 3 | n; \\ 2\varphi(n), & \text{altrimenti;} \end{cases}$

(d)  $n = 2\varphi(n) \Leftrightarrow n = 2^e$  per qualche  $e \geq 1$ ;

(e) esistono infiniti interi  $n$  per i quali  $\varphi(n)$  è un quadrato.

[*Dimostrazione.* (a) Se  $n$  è dispari, allora  $\text{MCD}(2, n) = 1$  e quindi:

$$\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n) .$$

(b) Se  $n$  è pari allora  $2^e | n$  e  $2^{e+1} \nmid n$  per qualche  $e \geq 1$ . Dunque  $n = 2^e n'$ , con  $n'$  dispari. Quindi  $2n = 2^{e+1} n'$ ,

$$\begin{aligned} \varphi(2n) &= \varphi(2^{e+1} n') = \varphi(2^{e+1})\varphi(n') = 2^e \varphi(n') = \\ &= 2(2^{e-1} \varphi(n')) = 2(\varphi(2^e)\varphi(n')) = 2\varphi(n) . \end{aligned}$$

(c) Se  $3 \nmid n$  allora  $\varphi(3n) = \varphi(3)\varphi(n) = 2\varphi(n)$ . Se  $3 | n$ , allora  $n = 3^e n'$  con  $\text{MCD}(3, n') = 1$ , per qualche  $e \geq 1$ . Quindi:

$$\begin{aligned} \varphi(3n) &= \varphi(3^{e+1} n') = \varphi(3^{e+1})\varphi(n') = 3^e \varphi(n') = \\ &= 3(3^{e-1} \varphi(n')) = 3(\varphi(3^e)\varphi(n')) = 3\varphi(n) . \end{aligned}$$

(d,  $\Leftarrow$ ) segue da (b).

(d,  $\Rightarrow$ ) Se  $n = 2^e n'$ , con  $n'$  dispari, allora

$$\varphi(n) = \varphi(2^e n') = 2^{e-1} \varphi(n') ,$$

quindi, essendo  $n = 2\varphi(n)$ , abbiamo

$$2^e n' = n = 2^e \varphi(n') ,$$

cioè  $n' = \varphi(n')$ . Pertanto  $n' = 1$ .

(e) segue da (d), per  $n = 2^{e+1}$ , con  $e$  pari.]

**1.8.** Se  $n \geq 2$ . Mostrare che:

(a) Se  $n$  ha  $r$  fattori primi distinti, allora:

$$\varphi(n) \geq \frac{n}{2^r} .$$

(b) Se  $n$  ha  $s$  fattori primi dispari distinti, allora:

$$2^s \mid \varphi(n) .$$

[*Suggerimento.* (a) Basta notare che, per ogni primo  $p \geq 2$ ,

$$\left(1 - \frac{1}{p}\right) \geq \frac{1}{2} .$$

(b) Se  $n = 2^{e_0} p_1^{e_1} \cdot \dots \cdot p_s^{e_s}$ , allora:

$$\varphi(n) = 2^{e_0-1} p_1^{e_1-1} \cdot \dots \cdot p_s^{e_s-1} (p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_s - 1)$$

con  $2 \mid (p_i - 1)$  per ogni  $i$ ,  $1 \leq i \leq s$ .]

**1.9.** Sia  $n \geq 2$  un intero composto (cioè, non primo). Mostrare che

$$\varphi(n) \leq n - \sqrt{n} .$$

[*Dimostrazione.* Sia  $p$  un divisore primo di  $n$ , con  $p \leq \sqrt{n}$ , allora  $\varphi(n) \leq n \left(1 - \frac{1}{p}\right) \leq n \left(1 - \frac{1}{\sqrt{n}}\right) = n - \frac{n}{\sqrt{n}} = n - \sqrt{n}$ .]

**1.10.** Mostrare che, per ogni  $n \in \mathbb{N}^+$ ,

$$\varphi(n^2) = n\varphi(n) .$$

[*Dimostrazione.* Se  $n = \prod_{i=1}^r p_i^{e_i}$ , allora:

$$\varphi(n^2) = n^2 \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right) = n\varphi(n) .$$

Si noti che, più generalmente, l'argomento precedente mostra che:  $n \mid m \Rightarrow \varphi(nm) = n\varphi(m)$ .]

**1.11.** Siano  $n, m \in \mathbb{N}^+$ ,  $d := \text{MCD}(n, m)$ ,  $t := \text{mcm}(n, m)$ . Mostrare che:

(a)  $n \mid m \Rightarrow \varphi(n) \mid \varphi(m)$ ;

(b)  $\varphi(n)\varphi(m) = \frac{\varphi(nm)\varphi(d)}{d}$ ;

(c)  $\varphi(n)\varphi(m) = \varphi(d)\varphi(t)$ .

[Dimostrazione. (a) Se

$$n = \prod_{i=1}^r p_i^{e_i}, \quad m = \prod_{j=1}^s p_j^{f_j}, \quad \text{con } s \geq r,$$

allora, ponendo

$$h := \left( \prod_{i=1}^r p_i^{f_i - e_i} \right) \prod_{j=r+1}^s p_j^{f_j},$$

si ha che  $nh = m$ . Dunque:

$$\begin{aligned} \varphi(m) &= m \prod_{j=1}^s \left(1 - \frac{1}{p_j}\right) = nh \left( \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \right) \left( \prod_{j=r+1}^s \left(1 - \frac{1}{p_j}\right) \right) = \\ &= \varphi(n)h \prod_{j=r+1}^s \left(1 - \frac{1}{p_j}\right). \end{aligned}$$

(b) Si noti che:

$$\begin{aligned} \varphi(nm) &= nm \prod_{p|nm} \left(1 - \frac{1}{p}\right) = nm \left( \prod_{p|d} \left(1 - \frac{1}{p}\right) \right) \left( \prod_{\substack{p|n \\ p \nmid d}} \left(1 - \frac{1}{p}\right) \right) \left( \prod_{\substack{p|m \\ p \nmid d}} \left(1 - \frac{1}{p}\right) \right) = \\ &= nm \left( \prod_{p|n} \left(1 - \frac{1}{p}\right) \right) \left( \prod_{\substack{p|m \\ p \nmid d}} \left(1 - \frac{1}{p}\right) \right). \end{aligned}$$

Essendo:

$$\frac{\varphi(d)}{d} = \prod_{p|d} \left(1 - \frac{1}{p}\right), \quad \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \quad \varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

la conclusione è immediata.

(c) Basta applicare (b), osservando che:

$$\begin{aligned} nm &= \text{MCD}(n, m) \cdot \text{mcm}(n, m) \\ \text{MCD}(\text{MCD}(n, m), \text{mcm}(n, m)) &= \text{MCD}(n, m). \end{aligned}$$

**1.12.** Sia  $p$  un primo ed  $e \geq 2$ . Mostrare che

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

[Dimostrazione.  $\varphi(\varphi(p^e)) = \varphi(p^{e-1}(p-1)) = \varphi(p^{e-1})\varphi(p-1) = p^{e-2}(p-1)\varphi(p-1) = p^{e-2}\varphi((p-1)^2)$  (cfr. anche Esercizio 1.10).]

**1.13.** Mostrare che, per  $n \in \mathbb{N}^+$ ,

(a)  $\tau(n) = 2 \Leftrightarrow n$  è primo.

(b)  $\tau(n) = 3 \Leftrightarrow n = p^2$ , dove  $p$  è un primo.

(c)  $\tau(n) = 4 \Leftrightarrow n = pq$  oppure  $n = p^3$ , dove  $p$  e  $q$  sono primi distinti.

[*Dimostrazione.* Se  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  è la fattorizzazione di  $n \geq 2$  in primi distinti, allora:

$$\tau(n) = \prod_{i=1}^r (\epsilon_i + 1)$$

Dunque:

$$\tau(n) = 2 \Leftrightarrow r = 1, \epsilon_1 = 1 ;$$

$$\tau(n) = 3 \Leftrightarrow r = 1, \epsilon_1 = 2 ;$$

$$\tau(n) = 4 \Leftrightarrow r = 1 \text{ ed } \epsilon_1 = 3 \text{ oppure } r = 2 \text{ ed } \epsilon_1 = \epsilon_2 = 1 .]$$

**1.14.** Mostrare che, per  $n \in \mathbb{N}^+$ ,

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

[*Dimostrazione.* Sia  $d | n$ , allora

$$n = dd' \text{ per qualche } d', \text{ con } d' | n .$$

Dunque

$$n^{\tau(n)} = \left( \prod_{d|n} d \right) \left( \prod_{d'|n} d' \right) = \left( \prod_{d|n} d \right)^2 .$$

Si noti che  $n^{\frac{\tau(n)}{2}}$  è sempre un intero, perché se  $\tau(n)$  è dispari allora  $n$  è un quadrato (cfr. Esercizio 1.4(a)).]

**1.15.** Mostrare che, se  $n \in \mathbb{N}^+$ ,

$$\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d} .$$

[*Dimostrazione.* Se  $d | n$ , allora  $dd' = n$  con  $d' | n$ . Dunque:

$$\frac{\sigma(n)}{n} = \frac{1}{n} \left( \sum_{d|n} d \right) = \sum_{d|n} \frac{d}{n} = \sum_{d'|n} \frac{1}{d'} .]$$

**1.16.** Mostrare che, se  $n \in \mathbb{N}^+$ ,

$$\varphi(n) + \sigma(n) = 2n \Leftrightarrow n \text{ è primo .}$$

[*Dimostrazione.* ( $\Leftarrow$ ) È ovvio, perché se  $n = p$  è primo, allora  $\varphi(p) = p - 1$  e  $\sigma(p) = 1 + p$ .

( $\Rightarrow$ ) Si noti che la funzione  $\varphi + \sigma$  definita ponendo  $(\varphi + \sigma)(n) = \varphi(n) + \sigma(n)$ , per ogni  $n \in \mathbb{N}^+$ , è una funzione moltiplicativa. Pertanto, basta mostrare che:

$$\varphi(p^e) + \sigma(p^e) = 2p^e \Leftrightarrow e = 1 .$$

Ora, se  $e \geq 2$

$$\begin{aligned} \varphi(p^e) + \sigma(p^e) &= p^e - p^{e-1} + 1 + p + \cdots + p^{e-1} + p^e = \\ &= 1 + p + \cdots + p^{e-2} + 2p^e = 2p^e \Leftrightarrow 1 + p + \cdots + p^{e-2} = 0 \end{aligned}$$

e ciò è assurdo.]

## 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:

$$(2.1.1) \quad \sigma_f = f * \mathbf{1}$$

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  $\mu$  introdotta da Möbius.

**Definizione 2.2.** Sia

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

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  $\mu$  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  $n \geq 1$ :

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

**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  $\mu$  discende immediatamente che:

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

□

**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:

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

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

**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  $\varphi$  è stata essenzialmente già verificata nella dimostrazione del Teorema I.5.13. Per maggiori dettagli cfr. anche l'Esercizio 1.5. □

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

(c)  $e = \sigma * \mu$  (ovvero,  $e = \sum_{d|n} \sigma(d) \frac{\mu(n)}{d}$ , 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  $\sigma = e * \mathbf{1}$ . □

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  $\mu$  e dal fatto che  $e^{-1} = \mu e$  si ricava immediatamente che:

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

dove  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  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  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  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  $e \geq 1$ ,  $(\mu f * \mathbf{1})(p^e) = \mu(1)f(1) + \mu(p)f(p) + 0 \cdot f(p^2) + \dots + 0 \cdot f(p^e) = 1 - f(p)$ .

□

**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  $n > 1$ :

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

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  $n = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_r^{\epsilon_r}$  la fattorizzazione in primi distinti di  $n \geq 2$  (con  $\epsilon_i \geq 1$  per  $1 \leq i \leq r$ ). Mostrare che valgono le seguenti uguaglianze:

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

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

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

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

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

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

[*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  $\frac{1}{e}(p) = \frac{1}{p}$ );
- $\tau$  nel caso (c) (con  $\tau(p) = 2$ );
- $\sigma$  nel caso (d) (con  $\sigma(p) = 1 + p$ );
- $\sigma^k$  nel caso (e) (con  $\sigma^k(p) = 1 + p^k$ );
- $\varphi$  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  $\frac{1}{n} \varphi(n) = (\frac{1}{e} \varphi)(n) = (\frac{1}{e} \mu * \mathbf{1})(n) = \sum_{d|n} \frac{1}{d} \mu(d).$

**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)

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

(b)

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

**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),

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

### 3 Formula di inversione di Möbius

Denotiamo con  $M$  l'insieme delle funzioni aritmetiche moltiplicative, diverse dalla funzione costante su 0. Abbiamo già notato che:

$$f \in M \Rightarrow f(1) = 1 \quad (\text{infatti, } f(n) = f(n \cdot 1) = f(n)f(1), \text{ con } n \geq 2)$$

quindi  $M \subset A := \{f : f \text{ è una funzione aritmetica con } f(1) \neq 0\}$ .

**Proposizione 3.1.** (a) Presi comunque  $f, g \in M$ , allora  $f * g \in M$ .

(b) Siano  $f, g \in A$ . Se  $f \in M$  e  $f * g \in M$  allora  $g \in M$ .

(c)  $(M, *)$  è un gruppo abeliano, sottogruppo di  $(A, *)$ .

**Dimostrazione.** (a) La dimostrazione è del tutto simile a quella della Proposizione 1.4. Siano  $n, m \in \mathbb{N}^+$  con  $\text{MCD}(n, m) = 1$ . Allora:

$$\begin{aligned} [(f * g)(n)][(f * g)(m)] &= \left[ \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \right] \left[ \sum_{d'|m} f(d')g\left(\frac{m}{d'}\right) \right] = \\ &= \sum_{d|n} \sum_{d'|m} f(d)f(d')g\left(\frac{n}{d}\right)g\left(\frac{m}{d'}\right) = \\ &= \sum_{dd'|nm} f(dd')g\left(\frac{nm}{dd'}\right) = \\ &= \sum_{e|nm} f(e)g\left(\frac{nm}{e}\right) = (f * g)(nm) \end{aligned}$$

dove  $d$  (rispettivamente,  $d'$ ;  $e$ ) varia tra tutti i divisori positivi di  $n$  (rispettivamente,  $m$ ;  $nm$ ).

(b) Procediamo per assurdo: supponiamo che  $g \notin M$ . Siano  $n, m \in \mathbb{N}^+$  con  $\text{MCD}(n, m) = 1$  e con  $nm$  minimo in modo tale che  $g(nm) \neq g(n)g(m)$ .

**Caso 1:**  $nm = 1$ . Allora  $n = m = 1$ . In tal caso, si avrebbe che  $g(1) \neq g(1)g(1)$  e, quindi,  $g(1) \neq 1$ . Pertanto:

$$(f * g)(1) = f(1)g(1) \neq f(1) = 1$$

e ciò è assurdo perché  $f * g$  è moltiplicativa e quindi  $(f * g)(1) = 1$ .

**Caso 2:**  $nm > 1$ . Presi comunque  $a, b \in \mathbb{N}^+$  con  $\text{MCD}(a, b) = 1$  ed  $ab < nm$ , per la minimalità di  $nm$ , abbiamo che

$$g(ab) = g(a)g(b) .$$

D'altro lato

$$\begin{aligned}
(f * g)(nm) &= (g * f)(nm) = \sum_{\substack{a|n \\ b|m \\ ab \neq nm}} g(ab) f\left(\frac{nm}{ab}\right) + g(nm)f(1) = \\
&= \left( \sum_{\substack{a|n \\ a < n}} g(a) f\left(\frac{n}{a}\right) \right) \left( \sum_{\substack{b|m \\ b < m}} g(b) f\left(\frac{m}{b}\right) \right) + g(nm) = \\
&= \left( \sum_{a|n} g(a) f\left(\frac{n}{a}\right) \right) \left( \sum_{b|m} g(b) f\left(\frac{m}{b}\right) \right) - g(n)g(m) + g(nm) = \\
&= [(g * f)(n)][(g * f)(m)] - g(n)g(m) + g(nm) = \\
&= [(f * g)(n)][(f * g)(m)] - g(n)g(m) + g(nm)
\end{aligned}$$

Quindi, poiché  $g(nm) - g(n)g(m) \neq 0$  si avrebbe che

$$(f * g)(nm) \neq [(f * g)(n)][(f * g)(m)]$$

e ciò è assurdo.

(c) Da (b) segue immediatamente che

$$f \in M \Rightarrow f^{-1} \in M$$

poiché  $f * f^{-1} = u \in M$ . Pertanto,  $M$  è un gruppo, sottogruppo di  $A$  (rispetto al prodotto di Dirichlet), infatti, da quanto sopra, si ricava immediatamente che:

$$f, g \in M \Rightarrow f * g^{-1} \in M .$$

□

**Teorema 3.2. (R. Dedekind, 1857)** (a) *L'applicazione:*

$$- * \mathbf{1} : A \longrightarrow A , \quad f \mapsto \sigma_f = f * \mathbf{1} ,$$

*è una biiezione avente come inversa l'applicazione:*

$$- * \mu : A \longrightarrow A , \quad F \mapsto F * \mu .$$

*La restrizione di  $- * \mathbf{1}$  ad  $M$ , cioè:*

$$- * \mathbf{1} : M \rightarrow M , \quad f \mapsto f * \mathbf{1} ,$$

è anch'essa una biiezione avente come inversa l'applicazione:

$$- * \mu : M \rightarrow M , \quad F \mapsto F * \mu .$$

(b) (**Formula di inversione di A.F. Möbius**). Presa comunque una funzione  $F \in A$  (rispettivamente,  $F \in M$ ) esiste un'unica funzione  $f \in A$  (rispettivamente,  $f \in M$ ) tale che:

$$F(n) = \sum_{d|n} f(d) , \quad \text{per ogni } n \in \mathbb{N}^+ .$$

Tale funzione  $f$  è tale che

$$f(n) = \sum_{d|n} F(d) \mu \left( \frac{n}{d} \right) , \quad \text{per ogni } n \in \mathbb{N}^+ .$$

**Dimostrazione.** (a) discende immediatamente dal fatto  $\mathbf{1} * \mu = u$  (Proposizione 2.3) e dal fatto che, se  $f, F \in M$ , allora  $f * \mathbf{1}$  e  $F * \mu$  appartengono ancora ad  $M$  (Proposizione 3.1(a)).

(b) è una semplice riformulazione di (a).

□

### 3 Esercizi e Complementi

**3.1.** Sia  $n \geq 1$ . Un numero complesso del tipo  $z = \cos \alpha + i \sin \alpha = e^{i\alpha}$ , con  $\alpha \in \mathbb{R}$ , è detto una *radice  $n$ -esima dell'unità* se  $z^n = 1$  ed è detto una *radice  $n$ -esima primitiva dell'unità* se, inoltre,  $z^k \neq 1$  per  $1 \leq k \leq n-1$ . È ben noto che  $\zeta_n := e^{\frac{2\pi i}{n}}$  è una radice primitiva  $n$ -esima dell'unità. Nel seguito porremo, per semplicità,  $\zeta$  al posto di  $\zeta_n$ , qualora ciò non sia causa di ambiguità. È subito visto che:

$$\{\zeta^k : 1 \leq k \leq n \text{ e } \text{MCD}(k, n) = 1\}$$

coincide con l'insieme delle radici primitive  $n$ -esime dell'unità.

Il polinomio nell'indeterminata  $X$  (a coefficienti — a priori — complessi)

$$\Phi_n(X) := \prod_{\substack{1 \leq k \leq n \\ \text{MCD}(k, n) = 1}} (X - \zeta^k)$$

è detto  *$n$ -esimo polinomio ciclotomico*. Esso ha grado  $\varphi(n)$  ed ha ovviamente come radici (nel campo  $\mathbb{C}$  dei numeri complessi) tutte e sole le radici primitive  $n$ -esima dell'unità (le quali sono tra loro distinte e sono in numero di  $\varphi(n)$ ).

Utilizzando opportunamente la formula di inversione di Möbius, mostrare che, per ogni  $n \geq 1$ :

$$(a) \quad \mu(n) = \sum_{\substack{1 \leq k \leq n \\ \text{MCD}(k, n) = 1}} \zeta^k ;$$

$$(b) \quad X^n - 1 = \prod_{d|n} \Phi_d(X) \quad \text{e} \quad \Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} ;$$

(c) Dedurre da (b) che  $\Phi_n(X) \in \mathbb{Z}[X]$ .

[Suggerimento. (a) Per ogni  $n \geq 1$ , poniamo:

$$f(n) := \sum_{\substack{1 \leq k \leq n \\ \text{MCD}(k, n) = 1}} \zeta^k \in \mathbb{C} .$$

Allora,  $F(n) := \sum_{d|n} f(d)$  è la somma di *tutte* le radici  $n$ -esime dell'unità (cioè di tutte le radici del polinomio  $X^n - 1$ ), quindi:

$$F(n) = \sum_{k=1}^n \zeta^k = \sum_{k=1}^n e^{\frac{2\pi k i}{n}} = \begin{cases} 0, & \text{se } n > 1 \\ 1, & \text{se } n = 1 \end{cases} = u(n)$$

(essendo la somma di tutte le radici di un polinomio monico di grado  $n \geq 1$  a coefficienti complessi uguale all'opposto del coefficiente del termine di grado  $n-1$ ). Pertanto  $F = f * \mathbf{1} = u$ , dunque  $\mu = \mu * u = f$ .

(b) Dal momento che le radici di  $X^n - 1$  sono le radici di un polinomio  $\Phi_d(X)$  per un qualche  $d \mid n$ , si ha:

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

cioè

$$\log(X^n - 1) = \sum_{d \mid n} \log \Phi_d(X) .$$

da cui ricaviamo che:

$$\log \Phi_n(X) = \sum_{d \mid n} \mu(d) \log(X^{\frac{n}{d}} - 1)$$

e dunque:

$$\Phi_n(X) = \prod_{d \mid n} (X^{\frac{n}{d}} - 1)^{\mu(d)} .$$

(c) è una conseguenza immediata di (b).]

**3.2.** Sia  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  la fattorizzazione in primi irriducibili di  $n \geq 2$  (con  $e_i \geq 1$  per  $1 \leq i \leq r$ ). Sia  $t \in \mathbb{C}$  fissato. Si definisca:

$$\omega_t(n) := \begin{cases} 1 & \text{se } n = 1; \\ t^r, & \text{altrimenti .} \end{cases}$$

Mostrare che:

(a)  $\omega_t : \mathbb{N}^+ \rightarrow \mathbb{C}$  è una funzione moltiplicativa.

(b)  $\sum_{d \mid n} \omega_t(d) = \sum_{i=1}^r (1 + e_i t)$ .

[*Dimostrazione.* (a) è di immediata verifica. (b) Essendo  $\omega_t$  una funzione moltiplicativa anche  $\sigma_{\omega_t}$  è una funzione moltiplicativa. È facile verificare che, per ogni primo  $p$  e per ogni intero  $e \geq 1$ , si ha:

$$\sigma_{\omega_t}(p^e) = \sum_{d \mid p^e} \omega_t(d) = 1 + \underbrace{t + \dots + t}_{e\text{-volte}} = 1 + et .]$$

**3.3.** Sia  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$  la decomposizione di  $n \geq 2$  (con  $e_i \geq 1$  per  $1 \leq i \leq r$ ) come prodotto di fattori primi distinti. Sia  $t$  un numero complesso fissato. Si ponga

$$\lambda_t(n) := \begin{cases} 1, & \text{se } n = 1; \\ t^{\left(\sum_{i=1}^r e_i\right)}, & \text{altrimenti .} \end{cases}$$

Mostrare che:

(a)  $\lambda_t : \mathbb{N}^+ \rightarrow \mathbb{C}$  è una funzione totalmente moltiplicativa.

$$(b) \sum_{d|n} \lambda_t(d) = \sum_{i=1}^r \frac{(t^{\epsilon_i} + 1 - 1)}{(t-1)}.$$

[*Dimostrazione.* (a) è di verifica immediata. (b) Poiché  $\lambda_t$  è totalmente moltiplicativa,  $\sigma_{\lambda_t}$  è moltiplicativa. Non è difficile assicurarsi che:

$$\sigma_{\lambda_t}(p^e) = \sum_{d|p^e} \sigma_{\lambda_t}(d) = 1 + t + t^2 + \dots + t^e = \frac{t^{e+1} - 1}{t - 1} .]$$

### 3.4. (Funzione di J. Liouville).

Si consideri la funzione introdotta nell'Esercizio 3.3 per  $t = -1$ . Si chiama *funzione di Liouville* la funzione totalmente moltiplicativa

$$\lambda(n) := \begin{cases} 1, & \text{se } n = 1; \\ (-1)^{\left(\sum_{i=1}^r \epsilon_i\right)}, & \text{altrimenti;} \end{cases}$$

dove  $n = p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_r^{\epsilon_r}$  è la fattorizzazione in primi distinti di  $n \geq 2$  (con  $\epsilon_i \geq 1$  per  $1 \leq i \leq r$ ). Mostrare che:

$$(a) \sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{se } n \text{ è un quadrato;} \\ 0, & \text{altrimenti;} \end{cases}$$

$$(b) \lambda^{-1} = \mu\lambda = |\mu|;$$

$$(c) \sum_{d|n} \lambda^{-1}(d) = \begin{cases} 1, & \text{se } n = 1; \\ 2^r, & \text{altrimenti.} \end{cases}$$

[*Suggerimento:* (a) Osserviamo che  $\sigma_{\lambda}$  è una funzione moltiplicativa perché  $\lambda$  è una funzione totalmente moltiplicativa. Notiamo anche che  $n$  è un quadrato se e soltanto se  $\epsilon_i$  è pari, per ogni  $1 \leq i \leq r$ .

Inoltre, per ogni primo  $p$  e per ogni intero  $e \geq 1$ , abbiamo

$$\sigma_{\lambda}(p^e) = 1 + (-1) + 1 + \dots + (-1)^e = \begin{cases} 1, & \text{se } e \text{ è pari;} \\ 0, & \text{se } e \text{ è dispari.} \end{cases}$$

(b) Poiché  $\lambda$  è totalmente moltiplicativa,  $\lambda^{-1}(n) = \mu(n)\lambda(n)$  per ogni  $n \in \mathbb{N}^+$  (Proposizione 2.10). Si noti che

$$\mu(n)\lambda(n) = \begin{cases} 1, & \text{se } n = 1 \\ (-1)^r \cdot (-1)^r, & \text{se } \epsilon_i = 1, \forall i \\ 0 \cdot (-1)^{\left(\sum_{i=1}^r \epsilon_i\right)}, & \text{altrimenti} \end{cases} = \mu(n)\mu(n) = |\mu(n)|$$

(c) Da (b) sappiamo che  $\lambda^{-1} = |\mu|$  è una funzione moltiplicativa. Inoltre, per ogni primo  $p$  e per ogni intero  $e \geq 1$ , abbiamo:

$$\sigma_{\lambda^{-1}}(p^e) = \sigma_{|\mu|}(p^e) = 1 + |\mu(p)| = 2 .$$

Si noti che  $\sigma_{\lambda^{-1}} = \omega_2$  (funzione definita nell'Esercizio 3.2 per  $t = 2$ ), cioè, per ogni  $n \geq 1$ ,

$$\sum_{d|n} \lambda^{-1}(d) = \omega_2(n) .$$

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