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 $f : \mathbb{N}^+ \to \mathbb{C}$, 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 $f : \mathbb{N}^+ \to \mathbb{C}$).

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

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

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

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 φ di Euler*, dove

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

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 $\tau : \mathbb{N}^+ \to \mathbb{C}$, definita ponendo:

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

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 MCD $(n, m) = 1$, allora l'applicazione:

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

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 $\sigma : \mathbb{N}^+ \to \mathbb{C}$ 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 τ e σ 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*

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

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*

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

è una funzione aritmetica totalmente moltiplicativa.

(g) La funzione

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

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 $f : \mathbb{N}^+ \to \mathbb{C}$ una funzione moltiplicativa.*
La funzione:

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

è una funzione moltiplicativa.

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

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

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)** $\tau = \sigma_{\mathbf{1}}$.

(b) $\sigma = \sigma_e$.

(c) *Se, per ogni* $k \geq 0$, *si definisce* $e^k : \mathbb{N}^+ \to \mathbb{C}$, *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* σ^k *è moltiplicativa, per ogni* $k \geq 0$.

Dimostrazione. (a), (b) e (c) seguono immediatamente dalla definizione della funzione σ_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*

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

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*

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

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

□

Corollario 1.7. *Sia*

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

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

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

(c) $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right) =$

$$= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdot \ldots \cdot (p_r^{e_r} - p_r^{e_r-1}).$$

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′) $\tau(p^e) = (e+1)$;

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

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

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

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

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 σ_f è moltiplicativa ma *non* necessariamente totalmente moltiplicativa (ad esempio $\tau = \sigma_{\mathbf{1}}$ è moltiplicativa ma non totalmente, mentre $\mathbf{1}$ è totalmente moltiplicativa).

1 Esercizi e Complementi

1.1. Se $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ 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*. σ^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) $\sum_{d|n} \sigma(d) = n \sum_{d|n} \frac{\tau(d)}{d}$

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

[*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 $\left(\frac{f}{g}\right)(n) := \frac{f(n)}{g(n)}$. 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 $e \geq 1$.

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

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

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

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

Se $p=2$ quest'ultima affermazione è sempre vera. Se p è dispari:
$p+\cdots+p^e$ è pari $\Leftrightarrow$ e è pari $\Leftrightarrow$ p^e è un quadrato.]

1.5. Se $\varphi : \mathbb{N}^+ \to \mathbb{C}$ 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 $\{1,2,\ldots,n\}$ di cardinalità n nell'unione disgiunta degli insiemi

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

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

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

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 $\{\frac{n}{d} : d \mid n\} = \{d : d \mid n\}$).]

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

(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 $\mathrm{MCD}(2, n) = 1$ e quindi:

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

(b) Se n è pari allora $2^e \mid n$ 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 $3 \mid n$, allora $n = 3^e n'$ con $\mathrm{MCD}(3, n') = 1$, 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 $n = 2^{e_0} p_1^{e_1} \cdot \ldots \cdot p_s^{e_s}$, allora:

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

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:

$$\varphi(n^2) = n^2 \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p^r}\right) = n\varphi(n) \ .$$

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

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

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

Essendo:

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

la conclusione è immediata.

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

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

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:

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

Dunque:

$$\tau(n) = 2 \Leftrightarrow r = 1,\ e_1 = 1\ ;$$
$$\tau(n) = 3 \Leftrightarrow r = 1,\ e_1 = 2\ ;$$
$$\tau(n) = 4 \Leftrightarrow r = 1 \text{ ed } e_1 = 3 \text{ oppure } r = 2 \text{ ed } e_1 = e_2 = 1\ .]$$

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

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

[*Dimostrazione*. Sia $d \mid n$, allora

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

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 $d \mid n$, allora $dd' = n$ con $d' \mid n$. 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.]