Esercizio 6.30 Sia b un intero maggiore di 1. Provare che, per ogni intero positivo n, esistono e sono univocamente determinati un numero naturale N ed interi $a_0, \dots, a_N$ tali che

(i) $0 \le a_i \le b-1$ per ogni i,
(ii) $a_N \ne 0$;
(iii) $n = \sum_{i=0}^{N} a_i b^i$.
La $(N+1)-$ upla $a_N, \dots, a_0$ si dice *rappresentazione di n in base b*.

<u>Dimostrazione</u>: Applichiamo il principio di induzione. Se n è un intero positivo minore di b, allora una rappresentazione del tipo desiderato è data da $N = 0$, $a_0 = n$. Questa è anche l'unica esistente, in quanto non potrà essere $N > 0$, altrimenti il secondo membro della (iii) sarebbe maggiore o uguale a b, e quindi strettamente maggiore di n.
Supponiamo ora che sia $n \ge b$, e che la tesi sia vera per ogni intero positivo minore di n. Sia a_0 il resto della divisione euclidea di n per b. Allora a_0 verifica (i). Inoltre il numero $n - a_0$ è divisibile per b (essendo uguale al prodotto di b per il quoziente della divisione). Lo stesso numero è positivo, in quanto n è per ipotesi maggiore di $b-1$, e quindi maggiore di a_0. Consideriamo il numero (intero, positivo)

$$n' = \frac{n - a_0}{b}$$

Dato che a_0 è non negativo, si ha che $n - a_0 \le n$; poiché $b > 1$, ne deriva quindi che $n' < n$. Ad n' si applica dunque l'ipotesi induttiva. Pertanto esistono, e sono univocamente determinati, un numero naturale N' ed interi $a'_0, \dots, a'_{N'}$ verificanti quanto richiesto da (i) e (ii) e tali che si abbia

$$n' = \sum_{i=0}^{N'} a'_i b^i,$$

ossia $\dfrac{n - a_0}{b} = \sum_{i=0}^{N'} a'_i b^i$, da cui

$$n = \sum_{i=0}^{N'} a'_i b^{i+1} + a_0 = \sum_{i=1}^{N'+1} a'_{i-1} b^i + a_0$$

Poniamo ora, per ogni $i = 1, \dots, N'+1$, $a'_{i-1} = a_i$, ed anche $N = N'+1$. Abbiamo così trovato una rappresentazione

$$n = \sum_{i=0}^{N} a_i b^i$$

verificante le condizioni (i) e (ii). Quanto all'unicità, cominciamo con l'osservare che a_0 è univocamente determinato dal fatto di essere il resto della divisione di n per b: infatti, in qualunque rappresentazione del tipo precedente, è evidente che b divide

$$n - a_0 = \sum_{i=1}^{N} a_i b^i,$$

dato che b è divisore di ogni addendo della sommatoria; a ciò si aggiunge il fatto che $0 \le a_0 < b$. A questo punto, l'unicità di N e dei restanti coefficienti a_i segue dall'unicità della rappresentazione trovata per n' (parte dell'ipotesi induttiva).

<u>Osservazione supplementare</u>: Dalla dimostrazione precedente emerge un procedimento ricorsivo per la costruzione della rappresentazione di un intero positivo n in base b. Vengono prodotte, una dopo l'altra, le cifre $a_0, \ldots, a_N$, applicando in maniera iterata la divisione euclidea. Illustriamo il procedimento tramite un esempio: vediamo come si ottenga la rappresentazione decimale del numero $n = 365$.

0) $a_0 = 5$ è il resto della divisione di n per 10;

Si considera quindi il numero $n' = \frac{n - a_0}{b} = \frac{365 - 5}{10} = 36$.

1) $a_1 = 6$ è il resto della divisione di n' per b;

Si passa quindi a $n'' = \frac{n' - a_1}{b} = \frac{36 - 6}{10} = 3$.

2) $a_2 = 3$ è il resto della divisione di n'' per b.

Il procedimento ha termine quando il numero trovato (nel nostro caso, n'') è minore di b (ovvero fornisce esso stesso il resto della propria divisione per b). A questo punto si è trovato a_N, ed in particolare, il valore di N (nel nostro caso, $N = 2$).