

## 1. I numeri

### 1.1. Sistemi numerici

Sia  $\mathbb{N}$  un insieme non vuoto, in cui si fissa un elemento detto *zero*, indicato con  $0$ , ed una funzione  $+$  da  $\mathbb{N}$  in  $\mathbb{N}$ . Indicata con  $a^+$  l'immagine di  $a$  tramite  $+$  al variare di  $a \in \mathbb{N}$ , si dice che  $a^+$  é *elemento successivo*, o *successore*, di  $a$ . Si assuma che per l'insieme  $\mathbb{N}$  valgano i seguenti assiomi, detti **Assiomi di Peano**:

1.  $0 \neq a^+ \forall a \in \mathbb{N}$ . Ovvero, non esiste alcun elemento di  $\mathbb{N}$  avente  $0$  come successore;
2. La funzione  $+$  é iniettiva. Ovvero, non esistono due  $a_1, a_2 \in S$  distinti che abbiano uno stesso  $a^+$  come successore;
3. Se  $S \subseteq \mathbb{N}$ ,  $0 \in S$  e  $s^+ \in S \forall s \in S$ , allora  $S = \mathbb{N}$ . Ovvero, se  $S$  é un sottoinsieme anche improprio di  $\mathbb{N}$  che contiene (almeno)  $0$  e che, per ciascun elemento di  $S$ , ne contiene anche l'immagine tramite  $+$ , allora  $S$  e  $\mathbb{N}$  sono lo stesso insieme.

L'insieme  $\mathbb{N}$  cosí definito prende il nome di **insieme dei numeri naturali**.

**Principio 1.1.1** (Principio del buon ordinamento): Sia  $S$  un sottoinsieme non vuoto di  $\mathbb{Z}$  limitato inferiormente (esiste un  $n_0 \in \mathbb{Z}$  tale che  $s \geq n_0, \forall s \in S$ ). Allora  $S$  ha minimo, ovvero esiste un  $m \in S$  tale che  $s \geq m, \forall s \in S$ .

**Teorema 1.1.1** (Teorema di Ricorrenza): Dati un insieme  $S$ , un elemento  $a$  di  $S$  ed una funzione  $\phi$  da  $S$  in sé stesso, esiste una ed una sola funzione  $f: \mathbb{N} \rightarrow S$  tale che

$$f(0) = a, f(n^+) = \phi(f(n))$$

**Principio 1.1.2** (Principio di induzione): Dato un numero fissato  $n_0 \in \mathbb{Z}$ , sia  $P(n)$  una proposizione dipendente da  $n \in \mathbb{Z}$ , con  $n \geq n_0$ . Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$  é vera;
- $\forall n$ , supponendo che sia vera  $P(n)$  é possibile dimostrare che lo sia anche  $P(n+1)$ .

Allora  $P(n)$  é vera  $\forall n \in \mathbb{Z}$

#### Principio di induzione

Si consideri la seguente proposizione, dipendente da  $n$ :

$$\sum_{i=1}^n (2i-1) = n^2, \forall n \geq 1$$

É possibile applicarvi il principio di induzione ponendo  $n_0 = 1$ . Nello specifico:

- $P(1)$  é vera. Infatti,  $\sum_{i=1}^1 (2i-1) = (2 \cdot 1) - 1 = 2 - 1 = 1$  e  $1^2 = 1$ ;
- Supponendo che sia vera  $P(n)$ , si dimostri che é vera  $P(n+1)$ , ovvero che sia vera  $\sum_{i=1}^{n+1} (2i-1) = (n+1)^2$ . Si ha:

$$\sum_{i=1}^{n+1} (2i-1) = (2(n+1)-1) + \sum_{i=1}^n (2i-1) = 2n+1 + \sum_{i=1}^n (2i-1) = 2n+1 + n^2$$

Che é però proprio la formula per il calcolo del quadrato di binomio. Pertanto  $n^2 + 1 + 2n = (n+1)^2 = \sum_{i=1}^{n+1} (2i-1)$

Essendo verificate entrambe le ipotesi del principio di induzione, si ha che  $P(n)$  é vera  $\forall n \geq 1$

Il principio di induzione può essere riespresso in termini diversi.

**Principio 1.1.3** (Principio di induzione forte): Dato un numero fissato  $n_0 \in \mathbb{Z}$ , sia  $P(n)$  una proposizione dipendente da  $n \in \mathbb{Z}$ , con  $n \geq n_0$ . Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$  é vera;
- $\forall m$  tale che  $n_0 \leq m < n$ , supponendo che sia vera  $P(m)$  é possibile dimostrare che lo sia anche  $P(n)$ .

Allora  $P(n)$  é vera  $\forall n \in \mathbb{Z}$

L'aggettivo *forte* non sta ad indicare che il principio di induzione forte abbia un maggior potere espressivo del principio di induzione "standard"; indica semplicemente che si basa su una ipotesi (la seconda) piú forte di quella usata dalla formulazione precedente. Infatti, una dimostrazione compiuta mediante una delle due forme del principio di induzione può essere convertita in una dimostrazione analoga compiuta nell'altra forma.

**Teorema 1.1.2:** Il principio di induzione, il principio di induzione forte ed il principio del buon ordinamento sono equivalenti.

*Dimostrazione:* La dimostrazione si compone di tre parti.

1. Assumendo come vero il principio di induzione, si dimostri la validità del principio di induzione forte. Sia pertanto  $P(n)$  una proposizione dipendente da  $n$  e sia  $n_0 \in \mathbb{Z}$  un valore fissato. Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$  é vera;
- $\forall m$  tale che  $n_0 \leq m < n$ , supponendo che sia vera  $P(m)$  é possibile dimostrare che lo sia anche  $P(n)$ . In particolare, dunque, se  $P(n-1)$  é vera allora  $P(n)$  é vera. Il principio di induzione implica quindi che  $P(n)$  é vera per ogni  $n \geq n_0$ ;

2. Assumendo come vero il principio di induzione forte, si dimostri la validità del principio del buon ordinamento. Sia pertanto  $S \subseteq \mathbb{Z}$  un sottoinsieme non nullo dei numeri interi inferiormente limitato da  $n_0$ . Si supponga per assurdo il principio del buon ordinamento non sia valido, ovvero che  $S$  non ammetta minimo. Si consideri la proposizione  $P(n)$  dipendente da  $n$ :

$$P(n) = \text{Non esiste alcun numero intero minore o uguale ad } n \text{ che appartenga ad } S$$

É possibile applicare a  $P(n)$  il principio di induzione forte. La prima ipotesi é verificata, perché se  $n_0$  appartenesse ad  $S$ , essendone il limite inferiore, allora ne sarebbe necessariamente anche il minimo. Sia dunque  $n$  un intero maggiore di  $n_0$ . Si assuma allora che  $\forall m$  tale che  $n_0 \leq m < n$ , supponendo che sia vera  $P(m)$  é possibile dimostrare che lo sia anche  $P(n)$ . Si supponga che  $P(n)$  sia falsa: esiste allora qualche  $t \leq n, t \in S$ . Ma questo non é possibile, perché  $\forall t \in \mathbb{Z}, n_0 \leq t \leq n$  si suppone  $P(t)$  vera, e quindi  $t \notin S$ . Occorre allora dedurre che  $S$  ammetta minimo, e quindi se si assume come valido il principio di induzione forte allora é valido il principio del buon ordinamento.

3. Assumendo come vero il principio del buon ordinamento, si dimostri la validità del principio di induzione. Dato un numero fissato  $n_0 \in \mathbb{Z}$ , sia  $P(n)$  una proposizione dipendente da  $n \in \mathbb{Z}$ , con  $n \geq n_0$ . Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$  é vera;
- $\forall n$ , supponendo che sia vera  $P(n)$  é possibile dimostrare che lo sia anche  $P(n+1)$ .  
Si consideri l'insieme  $S \subseteq \mathbb{Z}$  costituito da tutti gli  $n \geq n_0$  per i quali  $P(n)$  é falsa. Se il principio di induzione fosse verificato, tale insieme dovrebbe essere l'insieme vuoto. Si assuma per assurdo che tale insieme non sia vuoto: per il principio del buon ordinamento tale insieme deve ammettere un minimo, sia questo  $m$ , tale per cui  $P(m)$  é falsa.

Dato che l'insieme contiene solo interi  $n$  tali per cui  $n \geq n_0$  (ma non tutti), dovrà aversi che  $m > n_0$ , ovvero che  $m - 1 \geq n_0$ . Ma allora  $P(m - 1)$  deve essere vera, perché altrimenti si avrebbe  $m - 1 \in S$  ed  $m$  non sarebbe il minimo di  $S$ . Applicando la seconda ipotesi sopra definita, si ha che  $P(m + 1 - 1) = P(m)$  è vera, ma questo è in contraddizione con quanto evidenziato in precedenza. Occorre allora dedurre che se si assume come valido il principio del buon ordinamento, allora è valido il principio di induzione forte.

□

## 1.2. Divisione

Dati due numeri interi  $n$  e  $m$ , con  $n > m > 0$ , l'operazione di **divisione** permette due interi  $q$  e  $r$ , chiamati rispettivamente *quoziente* e *resto*, tali che il prodotto fra  $m$  e  $q$  è il multiplo di  $m$  che più si avvicina ad  $n$  per difetto ed il resto  $r = n - mq$  misura lo scarto.

**Teorema 1.2.1:** Siano  $n$  e  $m$  due numeri interi, con  $m \neq 0$ . Esiste una ed una sola coppia di interi  $q$  ed  $r$  tali per cui  $n = mq + r$  e  $0 \leq r < |m|$

Siano  $a$  e  $b$  due numeri interi. Se esiste  $c \in \mathbb{Z}$  tale che  $a = bc$ , si dice che  $b$  divide  $a$ , oppure analogamente che  $a$  è divisibile per  $b$ . Per indicare che  $b$  divide  $a$  viene usata la notazione  $b \mid a$ . Se  $b$  divide  $a$ , si dice anche che  $b$  è multiplo di  $a$ . È immediato verificare che, dato  $a \in \mathbb{Z}$ , sia  $\pm 1$  che  $\pm a$  sono certamente divisori di  $a$ .

Siano  $a, b \in \mathbb{Z}$  non entrambi nulli; si dice che  $d \in \mathbb{Z}$  è un **Massimo Comun Divisore** tra  $a$  e  $b$  se sono verificate entrambe le seguenti due condizioni:

1.  $d \mid a$  e  $d \mid b$ . Ovvero,  $d$  è divisore sia di  $a$  che di  $b$ ;
2. Se  $c \in \mathbb{Z}$  è tale che  $c \mid a$  e  $c \mid b$ , allora  $c \mid d$ . Ovvero, tutti i divisori di  $a$  che sono anche divisori di  $b$  sono anche divisori di  $d$ .

**Teorema 1.2.2:** Dati due numeri  $a, b \in \mathbb{Z}$  non entrambi nulli, se  $d$  e  $\tilde{d}$  sono due Massimi Comun Divisori fra  $a$  e  $b$  allora devono essere uguali in modulo, ovvero deve aversi  $d = \pm \tilde{d}$ .

*Dimostrazione:* Essendo  $d$  un Massimo Comun Divisore per  $a$  e  $b$ , deve valere  $d \mid a$  e  $d \mid b$ . Inoltre, deve valere anche che se  $c \in \mathbb{Z}$  è tale che  $c \mid a$  e  $c \mid b$ , allora  $c \mid d$ .

Essendo però anche  $\tilde{d}$  un Massimo Comun Divisore per  $a$  e  $b$ , deve valere  $\tilde{d} \mid a$  e  $\tilde{d} \mid b$ . Allora è possibile sostituire  $c$  con  $\tilde{d}$  nella seconda espressione ed ottenere che  $\tilde{d} \mid d$ .

È però possibile operare anche in senso contrario: essendo  $\tilde{d}$  un Massimo Comun Divisore per  $a$  e  $b$ , deve valere anche che se  $c \in \mathbb{Z}$  è tale che  $c \mid a$  e  $c \mid b$ , allora  $c \mid \tilde{d}$ , e valendo  $d \mid a$  e  $d \mid b$  deve aversi che  $d \mid \tilde{d}$ . Esistono allora due numeri  $h, k \in \mathbb{Z}$  tali per cui  $\tilde{d} = hd$  e  $d = \tilde{d}$ . Ne segue  $\tilde{d} = (hk)\tilde{d}$ , e quindi  $hk = 1$ . Deve allora aversi  $h = k = 1$  e quindi  $d = \tilde{d}$  oppure  $h = k = -1$  e quindi  $d = -\tilde{d}$ . □

Dal teorema si evince immediatamente che se  $d$  è un Massimo Comun Divisore positivo di due numeri interi  $a$  e  $b$ , allora  $d$  è univoco. Tale valore viene indicato con  $\text{MCD}(a, b)$ .

**Teorema 1.2.3:** Per una qualsiasi coppia di numeri interi  $a$  e  $b$  non entrambi nulli esiste sempre ed è univoco  $d = \text{MCD}(a, b)$

*Dimostrazione:* Innanzitutto, è immediato riconoscere che se  $d = \text{MCD}(a, b)$ , allora è vero anche  $d = \text{MCD}(-a, -b)$ . È altrettanto immediato riconoscere che  $\text{MCD}(a, b) = \text{MCD}(b, a)$  per qualsiasi  $a, b$ . Pertanto, senza perdita di generalità, è possibile assumere che  $a$  e  $b$  siano numeri naturali con  $a \geq b$ .

Se  $a = 0$  e  $b \neq 0$  si verifica facilmente che  $\text{MCD}(a, b) = a$ ; allo stesso modo, se  $b = 0$  e  $a \neq 0$  si ha  $\text{MCD}(a, b) = b$ . Si consideri pertanto il caso più generale in cui  $a \neq 0$  e  $b \neq 0$ . Devono allora esistere un quoziente  $q_1$  ed un resto  $r_1$  tali per cui è possibile eseguire la divisione:

$$a = bq_1 + r_1, 0 \leq r_1 < b$$

Se  $r_1 = 0$ , allora  $\text{MCD}(a, b) = b$ , perché  $a = bq_1$  è la definizione stessa di  $b \mid a$  e  $q_1$  è arbitrario. Se così non è, è possibile ripetere l'operazione e risolvere i calcoli con un nuovo resto ed un nuovo quoziente. Più in generale:

$$\begin{array}{lll} (1) & a = bq_1 + r_1 & r_1 \neq 0 \\ (2) & b = r_1q_2 + r_2 & r_2 \neq 0 \\ (3) & r_1 = r_2q_3 + r_3 & r_3 \neq 0 \\ & \dots & \\ (k-1) & r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} & r_{k-1} \neq 0 \\ (k) & r_{k-2} = r_{k-1}q_k & \end{array}$$

Il fatto che prima o poi si giunga ad una  $k$ -esima iterazione in cui  $r_k = 0$  è garantito dal fatto che tale successione è una successione strettamente crescente di numeri non negativi.

L'ultimo resto non nullo, ovvero  $r_{k-1}$ , è precisamente  $\text{MCD}(a, b)$ . Per verificarlo, è sufficiente osservare come questo possieda entrambe le proprietà enunciate nella definizione di Massimo Comun Divisore:

- Alla riga  $(k)$  si ha  $r_{k-2} = r_{k-1}q_k$ , ovvero  $r_{k-1} \mid r_{k-2}$ . Sostituendo la riga  $(k)$  nella riga  $(k-1)$  si ha:

$$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} = r_{k-1}q_kq_{k-1} + r_{k-1} = r_{k-1}(q_kq_{k-1} + 1)$$

Ovvero,  $r_{k-1} \mid r_{k-3}$  (Si noti come il raccoglimento è ammesso dato che  $r_{k-1}$  è definito come non nullo). Risalendo di riga in riga, è facile convincersi che dalla riga  $(2)$  si ottiene  $r_{k-1} \mid r_1$  e  $r_{k-1} \mid b$ . Dalla riga  $(1)$  segue  $r_{k-1} \mid a$ . Avendo dimostrato che  $r_{k-1} \mid a$  e  $r_{k-1} \mid b$ , si ha che  $r_{k-1}$  possiede la prima proprietà dell'MCD.

- Sia  $c \in \mathbb{Z} - \{0\}$ . Siano poi  $a = c\bar{a}$  e  $b = c\bar{b}$ . Sostituendo nella riga  $(1)$  si ottiene:

$$a = bq_1 + r_1 \Rightarrow c\bar{a} = c\bar{b}q_1 + r_1 \Rightarrow r_1 = c\bar{a} - c\bar{b}q_1 \Rightarrow r_1 = c(\bar{a} - \bar{b}q_1)$$

Da cui si ha  $c \mid r_1$ . Ponendo  $r_1 = c\bar{r}_1$  e sostituendo nella riga  $(2)$ , si ha:

$$b = r_1q_2 + r_2 \Rightarrow c\bar{b} = c\bar{r}_1q_2 + r_2 \Rightarrow r_2 = c\bar{b} - c\bar{r}_1q_2 \Rightarrow r_2 = c(\bar{b} - \bar{r}_1q_2)$$

Da cui si ha  $c \mid r_2$ . Discendendo di riga in riga ed applicando lo stesso procedimento, si arriva fino a  $c \mid r_{k-1}$ . Ma questo equivale a dire che, per un  $c$  numero intero generico, se  $c \mid a$  e  $c \mid b$ , allora  $c \mid r_{k-1}$ , e quindi  $r_{k-1}$  possiede anche la seconda proprietà dell'MCD.

□

La dimostrazione del Teorema 1.2.3 fornisce implicitamente anche un algoritmo per calcolare, a partire da due numeri interi  $a$  e  $b$  non entrambi nulli, il loro MCD. Tale algoritmo prende il nome di **Algoritmo di Euclide**, ed è strutturato come segue:

1. Si calcola qual'è il più grande intero  $q$  tale per cui è possibile moltiplicarlo per  $b$  ottenendo un valore inferiore ad  $a$ ;
2. Si calcola  $r$  come differenza fra  $qb$  ed  $a$ . Se tale valore è nullo, allora  $q$  è MCD per  $a$  e  $b$ , e l'algoritmo termina;
3.  $b$  diventa il nuovo  $a$ , mentre  $r$  diventa il nuovo  $b$ . Dopodiché, si torna al punto 1.

#### Calcolo dell'MCD

L'MCD dei numeri  $a = 110143$  e  $b = 665$  è 19. Infatti:

$$\begin{aligned} 110143 &= 665 \cdot 165 + 418 \\ 665 &= 418 \cdot 1 + 247 \\ 418 &= 247 \cdot 1 + 171 \\ 247 &= 171 \cdot 1 + 76 \\ 171 &= 76 \cdot 2 + 19 \\ 76 &= 19 \cdot 4 \end{aligned}$$

**Teorema 1.2.4** (Identità di Bézout): Se  $a$  e  $b$  sono due numeri interi non entrambi nulli, allora esistono due numeri interi  $x$  e  $y$  tali per cui vale:

$$ax + by = \text{MCD}(a, b)$$

*Dimostrazione:* Facendo riferimento al Teorema 1.2.3, si consideri la successione di operazioni. In particolare, la riga (1), ovvero  $a = bq_1 + r_1$ , può anche essere riscritta come  $r_1 = a(1) + b(-q_1)$ . Sostituendo nella riga (2), si ha:

$$b = r_1q_2 + r_2 \Rightarrow b = (a - bq_1)q_2 + r_2 \Rightarrow r_2 = b - aq_2 + bq_1q_2 \Rightarrow r_2 = a(-q_2) + b(q_1q_2 + 1)$$

In questo modo, è possibile ciascun resto come combinazione lineare di  $a$  e di  $b$ . In particolare per il resto  $r_{k-1}$ , che è anche l'MCD di  $a$  e di  $b$ , esisteranno due valori  $x$  e  $y$  tali per cui è possibile esprimerlo come combinazione lineare di  $a$  e  $b$ , e quindi  $r_{k-1} = \text{MCD}(a, b) = ax + by$ .  $\square$

La dimostrazione del Teorema 1.2.4 fornisce implicitamente anche un algoritmo per calcolare, a partire da due numeri interi  $a$  e  $b$  non entrambi nulli, una possibile coppia  $x, y$  di interi tali da soddisfare l'identità per  $a$  e  $b$ , fintanto che il loro MCD è noto. Tale algoritmo è strutturato come segue:

1. Si esprime  $r$  in funzione di  $a$  e di  $b$ , spostando quest'ultimo a primo membro ed isolando  $r$  a secondo membro;
2. Se  $r$  è l'MCD di  $a$  e di  $b$ , l'algoritmo termina, perché le soluzioni particolari cercate sono i coefficienti di  $a$  e di  $b$ ;
3. Si passa alla riga successiva e si ripete il procedimento, esprimendo i due nuovi  $a$  e  $b$  in funzione dei precedenti. Si noti come questi, ad ogni iterazione, cambiano di segno.

#### Identità di Bézout

L'MCD dei numeri  $a = 110143$  e  $b = 665$  è 19. Una soluzione particolare che soddisfa l'identità di Bézout per questa coppia è ricavata di seguito:

$$\begin{array}{llll} 110143 = 665 \cdot 165 + 418 & \Rightarrow a & = 165b + 418 & \Rightarrow a - 165b = 418 \\ 665 = 418 \cdot 1 + 247 & \Rightarrow b & = a - 165b + 247 & \Rightarrow 166b - a = 247 \\ 418 = 247 \cdot 1 + 171 & \Rightarrow a - 165b & = 166b - a + 171 & \Rightarrow 2a - 331b = 171 \\ 247 = 171 \cdot 1 + 76 & \Rightarrow 166b - a & = 2a - 331b + 76 & \Rightarrow 497b - 3a = 76 \\ 171 = 76 \cdot 2 + 19 & \Rightarrow 2a - 331b & = 2(497b - 3a) + 19 & \Rightarrow 8a - 1325b = 19 \end{array}$$

Se due numeri interi hanno 1 come Massimo Comun Divisore, allora si dice che tali numeri sono **coprime** o **primi fra di loro**. Tale definizione può essere riformulata anche rispetto al Teorema 1.2.4.

**Teorema 1.2.5:** Due numeri interi  $a$  e  $b$  sono coprime fra di loro se e soltanto se esistono due numeri interi  $x$  e  $y$  tali per cui vale  $ax + by = 1$ .

*Dimostrazione:* Il primo verso dell'implicazione deriva direttamente dalla definizione di numeri coprime. Infatti, due numeri interi  $a$ , e  $b$  si dicono coprime se il loro MCD è 1; sostituendolo nell'identità di Bézout, si ha precisamente  $ax + by = 1$ .

Ciò che manca da dimostrare è il secondo verso, ovvero che se per due numeri interi  $a$  e  $b$  esistono due numeri interi  $x$  e  $y$  tali per cui  $ax + by = 1$ , allora  $a$  e  $b$  sono coprime. Si supponga per assurdo che, se esistono  $x$  e  $y$ , tali per cui  $ax + by = 1$ , allora  $a$  e  $b$  non siano coprime. Questo significa che il loro MCD non è 1, ovvero che  $ax + by \neq 1$ , ma questo è in contraddizione con l'ipotesi assunta per assurdo.  $\square$

### 1.3. Basi

**Teorema 1.3.1** (Esistenza ed unicità della rappresentazione dei numeri interi in una certa base): Sia  $b$  un intero maggiore o uguale a 2. Ogni numero intero  $n$  non negativo può essere scritto in uno ed un solo modo nella forma:

$$n = d_k b^k + d_{k-1} b^{k-1} + \dots + d_1 b + d_0 \quad \text{con } 0 \leq d_i < b \quad \forall i = 0, \dots, k \quad d_k \neq 0 \text{ per } k > 0$$

*Dimostrazione:* La dimostrazione prevede di applicare il principio di induzione forte su  $n$ . Per  $n = 0$  la proposizione è verificata immediatamente. Si assuma allora che la proposizione sia vera per ogni  $m$  con  $0 \leq m < n$  e la si dimostri per  $n$ .

Innanzitutto, si osservi come sia possibile dividere  $n$  per  $b$ , ottenendo:

$$n = bq + r \quad \text{con } 0 \leq r < b$$

per un certo  $q$  ed un certo  $r$ . Per la definizione di divisione, si ha  $q < n$ . Ma allora  $q$  è uno degli  $m$  per i quali è valida l'ipotesi assunta, ovvero che esiste uno ed un solo modo per scrivere  $q$  nella forma:

$$q = c_{k-1} b^{k-1} + c_{k-2} b^{k-2} + \dots + c_1 b + c_0$$

Per certi  $k$  valori  $c_i$  tali per cui  $0 \leq c_i < b$ . Sostituendo la seconda espressione nella prima, si ha:

$$n = bq + r = b(c_{k-1} b^{k-1} + c_{k-2} b^{k-2} + \dots + c_1 b + c_0) + r = c_{k-1} b^k + c_{k-2} b^{k-1} + \dots + c_1 b^2 + c_0 b + r$$

Ponendo  $d_k = c_{k-1}$ ,  $d_{k-1} = c_{k-2}$ , ...,  $d_1 = c_0$ ,  $d_0 = r$ , si ha:

$$n = d_k b^k + d_{k-1} b^{k-1} + \dots + d_1 b + d_0 \quad \text{con } 0 \leq d_i < b \quad \forall i = 0, \dots, k$$

Che è l'ipotesi che si voleva dimostrare.

Per quanto riguarda l'unicità di questa scrittura, questa segue dall'unicità di  $q$  e di  $r$ . □

Dati  $b \in \mathbb{Z}$  con  $b \geq 2$  e un numero naturale  $n$  tale che:

$$n = d_k b^k + d_{k-1} b^{k-1} + \dots + d_1 b + d_0 \quad \text{con } 0 \leq d_i < b \quad \forall i = 0, \dots, k \quad d_k \neq 0 \text{ per } k > 0$$

Gli interi  $d_0, d_1, \dots, d_k$  si dicono le **cifre** di  $n$  in **base**  $b$ .

Per indicare in quale base  $n$  sta venendo espresso, se ne riportano ordinatamente le cifre aggiungendo la base in pedice alla cifra più a destra. Nel caso in cui il pedice sia assente, si sta sottointendendo che tale numero sta venendo espresso in base 10.

Una base  $b$  fa uso di un numero di cifre pari a  $b - 1$ , partendo da 0; nel caso in cui la base sia maggiore di 10, si usano dei simboli extra per rappresentare le cifre mancanti.

Se è nota la (unica) rappresentazione di un numero intero non negativo in una certa base  $b$ , è sempre possibile ricavarne la rappresentazione in base 10 semplicemente svolgendo l'equazione della definizione. Si noti però come tale equazione possa anche essere riscritta come:

$$\begin{aligned} n &= d_k b^k + d_{k-1} b^{k-1} + d_{k-2} b^{k-2} + d_{k-3} b^{k-3} + \dots + d_1 b + d_0 \\ &= (d_k b + d_{k-1}) b^{k-1} + d_{k-2} b^{k-2} + d_{k-3} b^{k-3} + \dots + d_1 b + d_0 \\ &= ((d_k b + d_{k-1}) b + d_{k-2}) b^{k-2} + d_{k-3} b^{k-3} + \dots + d_1 b + d_0 \\ &= (((d_k b + d_{k-1}) b + d_{k-2}) b + d_{k-3}) b^{k-3} + \dots + d_1 b + d_0 \\ &= \dots \\ &= (\dots((d_k b + d_{k-1}) b + d_{k-2}) b + d_{k-3}) b^{k-3} + \dots + d_1) b + d_0 \end{aligned}$$

Questa forma è nettamente più convoluta, ma più semplice da utilizzare per effettuare la conversione. Infatti, sono necessarie solo  $k$  moltiplicazioni per  $b$  e  $k$  addizioni.

#### Conversione da base qualsiasi a base 10

$$61405_7 = (((6 \cdot 7 + 1)7 + 4)7 + 0)7 + 5 = ((42 + 1)7 + 4)49 + 5 = (301 + 4)49 + 5 = 14950$$

Per effettuare la conversione inversa, ovvero ricavare la rappresentazione di un numero  $n$  in base  $b$  a partire dalla sua rappresentazione in base 10, si osservi come le cifre  $d_0, d_1, \dots, d_k$  di  $n$  non siano altro che i resti delle divisioni:

$$\begin{aligned} n &= bq + d_0 \quad 0 \leq d_0 < b \\ q &= q_1 b + d_1 \quad 0 \leq d_1 < b \\ q_1 &= q_2 b + d_2 \quad 0 \leq d_2 < b \\ &\dots \end{aligned}$$

E così via, finché non si ottiene quoziente nullo.

#### Conversione da base 10 a base qualsiasi

$$\begin{aligned} 14950 &= 7 \cdot 2135 + 5 \\ 2135 &= 7 \cdot 305 + 0 \\ 305 &= 7 \cdot 43 + 4 \\ 43 &= 7 \cdot 6 + 1 \\ 6 &= 7 \cdot 0 + 6 \end{aligned}$$

Leggendo dal basso verso l'alto, si ha  $14950 = 61405_7$

È facile verificare come maggiore è il numero di cifre che la base in cui un numero è espresso ha a disposizione, minore è il numero di cifre necessarie per rappresentarlo. In particolare, il numero di cifre in base  $b$  di un intero non negativo  $n$  è dato da:

$$k + 1 = \lfloor \log_b(n) \rfloor + 1 = \left\lfloor \frac{\ln(n)}{\ln(b)} \right\rfloor + 1$$

Perché  $b^k \leq n < b^{k+1}$