

Rappresentazione degli interi in base n

(13)

Un'altra conseguenza dell'algoritmo della divisione è la possibilità di rappresentare gli interi in una base n intera > 1 .

TEOR. Sia $n \in \mathbb{N}$ e $n > 1$. Ogni intero z può essere scritto in 1 e 1 sol modo nella forma

$$z = r_h n^h + r_{h-1} n^{h-1} + \dots + r_1 n^1 + r_0 n^0,$$

ove $0 \leq r_i < n$ per ogni $i \in \{0, 1, \dots, h\}$ e $h \geq 0$.

La dimostrazione viene svolta per induzione su z , con base induttiva $z=0$. Ma preferiamo fare esempi.

ES. 1 n = 10 $128 = 1 \cdot 10^2 + 2 \cdot 10^1 + 8 \cdot 10^0$

La rappresentazione del numero in base 10 è ottenuta applicando l'algoritmo della divisione come segue:

$$\begin{array}{r} 128 : 10 = 12 \\ \text{resto } 8 \end{array}$$

$$\Rightarrow 128 = 12 \cdot 10 + 8$$

cifra in posiz. 10^0

$$\begin{array}{r} 12 : 10 = 1 \\ \text{resto } 2 \end{array}$$

$$\Rightarrow 12 = 1 \cdot 10 + 2$$

cifra in posiz. 10^1

$$\begin{array}{r} 1 : 10 = 0 \\ \text{resto } 1 \end{array}$$

$$\Rightarrow 1 = 0 \cdot 10 + 1$$

cifra in posiz. 10^0

il quoziente 0 blocca la procedura.

$$128 = 12 \cdot 10 + 8 =$$

$$= (1 \cdot 10 + 2) \cdot 10 + 8 = \text{PROPR. DISTRIBUTIVA}$$

$$= 1 \cdot 10^2 + 2 \cdot 10^1 + 8 \cdot 10^0.$$

Per dire che rappresento z in base n scriverò (14)
 $z_{(n)}$.

NOTA: visto che nella rappresentazione in base n entrano in gioco i resti r_i nella divisione per n che sono esattamente n :

$$0, 1, 2, \dots, n-1$$

le cifre distinte che possono comparire in una rappresentazione in base n sono n .

Se $n > 10$ useremo aggiungere un opportuno numero di cifre alle solite $(0, 1, \dots, 9)$.

Se $n < 10$ useremo solo le prime n cifre nella sequenza precedente.

ESEMPIO. Rappresentare $z = 128_{(10)}$ in base 3

$$128 = 42 \cdot 3 + 2$$

$$42 = 14 \cdot 3 + 0$$

$$14 = 4 \cdot 3 + 2$$

$$4 = 1 \cdot 3 + 1$$

$$1 = \underline{0} \cdot 3 + 1 \quad \text{FINE : } z = 128_{(10)} = 11202_{(3)}$$

Infatti ho visto che $128 =$

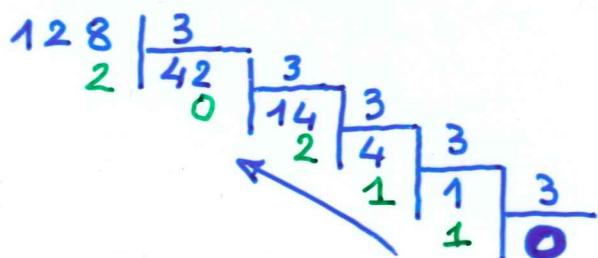
$$42 \cdot 3 + 2 =$$

$$= 14 \cdot 3^2 + 0 \cdot 3 + 2 =$$

$$= 4 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3 + 2 =$$

$$= 1 \cdot 3^4 + 1 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3 + 2.$$

Schema per abbreviare:



ESEMPIO . Scrivere $4331_{(10)}$ in base 12

(15)

12 cifre: 0, 1, ..., 9, A, B

$$\begin{array}{r} 4331 \\ \hline 11 | 360 \quad 12 \\ \text{B} \quad \swarrow 0 \quad 30 \quad | 12 \\ \quad \quad 6 \quad | 2 \quad | 12 \\ \quad \quad \quad 2 \quad | 0 \end{array}$$

Quindi

$$4331_{(10)} = 260B_{(12)}$$

ESEMPIO . Scrivere $21101_{(3)}$ in base 10

$$\begin{aligned} 21101_{(3)} &= (1 + 0 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4)_{(10)} = \\ &= (1 + 9 + 27 + 162)_{(10)} = 199_{(10)} \end{aligned}$$

OSSERVAZIONI

- 1) In qualunque base zero si rappresenta con 0
- 2) Per trovare la rappresentazione in base n di un numero negativo?

Ad es. : rappresentare in base 2 il numero

$$(-19)_{(10)}$$

Cerco la rappresentazione di 19 in base 2:

$$\begin{array}{r} 19 \\ \hline 1 | 2 \\ \quad 1 | 2 \\ \quad \quad 0 | 2 \\ \quad \quad \quad 0 | 2 \\ \quad \quad \quad \quad 1 | 2 \\ \quad \quad \quad \quad \quad 0 \end{array} \Rightarrow 19_{(10)} = 10011_{(2)}$$

e poi cambio segno: $-19_{(10)} = -10011_{(2)}$

$$-10011_{(2)} = -2^4 - 0 \cdot 2^3 - 0 \cdot 2^2 - 2 - 1$$

- 3) 347 può essere una rappresentazione di un numero \geq in base 9? È in base 6?

Operazioni su interi in base n intero > 1

Si faamo come con le base $n=10$, ma devo "sapere contare in base n ".

ESEMPIO

$$\begin{array}{r} 1 \ 1 \\ 1 \ 1 \ 2_{(3)} \\ + \\ 1 \ 2 \ 1_{(3)} \\ \hline 1 \ 0 \ 1 \ 0_{(3)} \end{array}$$

In base 3:

$$\begin{aligned} 1+2 &= 10 \\ 2+2 &= 11 \end{aligned}$$

TRADUZIONE:

$$\begin{aligned} (2 + 1 \cdot 3 + 1 \cdot 3^2) + (1 + 2 \cdot 3 + 1 \cdot 3^2) &= \\ \xrightarrow{\text{PROPR. COMM. E ASSOC. SOMMA}} 2+1 + (1 \cdot 3 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^2) &= \\ \xrightarrow{\text{SCELTA DELLA BASE}} 0 + (1 \cdot 3 + 1 \cdot 3 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^2) &= \\ \xrightarrow{\text{PROPR. DISTRIBUTIVA}} 0 + (1+3) \cdot 3 + 2 \cdot 3^2 &= \\ \xrightarrow{\text{SCELTA DELLA BASE e PROPR. DISTR.}} 0 + 1 \cdot 3 + (1+2) \cdot 3^2 &= \\ \xrightarrow{\text{SCELTA DELLA BASE}} 0 + 1 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 &= \end{aligned}$$

$$\begin{array}{r} 1 \ 1 \ 2_{(3)} \times \\ 1 \ 2 \ 1_{(3)} \\ \hline 1 \ 0 \ 0 \ 1 \ 1 \ 2 \\ 1 \ 1 \ 2 \\ \hline 2 \ 2 \ 0 \ 2 \ 2_{(3)} \end{array}$$

In base 3

$$\begin{aligned} 1 \cdot 2 &= 2 \\ 2 \cdot 2 &= 11 \end{aligned}$$

TRADUZIONE

$$\begin{aligned} (2+1 \cdot 3 + 1 \cdot 3^2) \cdot (1+2 \cdot 3 + 1 \cdot 3^2) &\stackrel{\text{DISTR.}}{=} \\ = (2+1 \cdot 3 + 1 \cdot 3^2) + 2 \cdot (2+1 \cdot 3 + 1 \cdot 3^2) \cdot 3 + \\ + (2+1 \cdot 3 + 1 \cdot 3^2) \cdot 3^2 &\stackrel{\text{SCELTA BASE}}{=} \\ = (2+1 \cdot 3 + 1 \cdot 3^2) + (1+3+2 \cdot 3+2 \cdot 3^2) \cdot 3 + \\ + (2 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4) &= \\ = \dots \dots \dots + (1+1 \cdot 3^2+2 \cdot 3^2) \cdot 3 + \dots &= \\ = (2+1 \cdot 3 + 1 \cdot 3^2) + (1 \cdot 3 + 1 \cdot 3^4) + (2 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4) &= \\ = 2+2 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^3 + 2 \cdot 3^4 &= \\ = 2+2 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 & \end{aligned}$$

Ovviamente, dato che $112_{(3)} = 14_{(10)}$ e $121_{(3)} = 16_{(10)}$)
 $112_{(3)} \cdot 121_{(3)} = 22022_{(3)} = 224_{(10)} = 14_{(10)} \cdot 16_{(10)}$.

Cos'è una EQUAZIONE?

Esempi

a) $2x^2 - 3x + 1 = 0$

b) $x + 2y - 5 = 0$

c) $e^x = x$

d) $x \ln y = 5$

e) $x^2 + 1 = 0$

f) $x^2 - 1 = (x-1)(x+1)$

Non sono esempi:

g) $x \ln y - 5$

h) $\sqrt{x} - 2$

g) e h) sono "leggi" che possono definire una FUNZIONE (pure di chiarezza DOMINIO e CODOMINIO) ma mancando il segno di uguaglianza NON sono equazioni.

Le equazioni presentano sempre un' UGUAGLIANZA tra due "espressioni letterali" in cui almeno una delle lettere è assunta come INCognita (valore non noto da determinare).

PROBLEMI SULLE EQUAZIONI

A) Che cosa significa soluzione di una eq.?

Vuol dire trovare numeri (in un opportuno insieme numerico determinato dal problema o ... dalla necessità di trovare soluzioni) che sostituiti al posto delle incognite x, y, \dots diano una identità

Es.: $x + 2y = 5$ ha tra le sue soluzioni $\begin{cases} x=1 \\ y=2 \end{cases}$
poiché $1 + 2 \cdot 2 = 5$.

Per poter parlare convenientemente di soluzioni' se le incognite sono più di una conviene "ordinarle" - l'ordine è del tutto arbitrario - : $x, y, z \dots$ ad es. si devono ordinare in questa sequenza e rappresentare le soluzioni di una eq. in

2 incognite come coppie ordinate: $(x, y) = (,)$

3 " " Terne ordinate: $(x, y, z) = (, ,)$

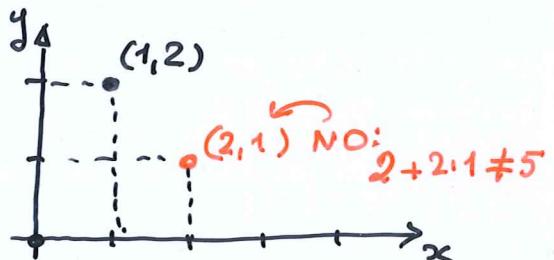
ecc.

Coppie ordinate significa che è importante in quale delle due posizioni si mette un certo numero: ad es. posso rappresentare una sol. di $x+2y=5$ come

$$(x, y) = (1, 2)$$

ma non come

$$(x, y) = (2, 1)$$



L'insieme delle coppie ordinate di elementi di due insiemi (anche diversi) : I, J viene di solito indicata con $I \times J$ e chiamato prodotto cartesiano di I e J .

Quindi ad es. la sol. $(2, 1)$ che ho trovato prima appartiene a $\mathbb{Z} \times \mathbb{Z} \dots$ ma anche $\mathbb{R} \times \mathbb{R}$ ecc.

B) L'equazione per caso non è MAI RISOLUBILE?

Cioè comunque io scelga l'insieme numero non esistono numeri che sostituiti al posto delle incognite diano una identità?

Es: $x+1=x$
 $0 \cdot x=1$

EQUAZIONI IMPOSSIBILI

C) DOVE o QUANDO l'equazione è risolubile?

ES. 1 $x^2 + 1 = 0$ non è risolubile se cerco le sol. in \mathbb{R} , ma lo è se le cerco in \mathbb{C} : $x = \pm i$

ES. 2 $x+2y=5$ è risolubile anche in \mathbb{Z} come mostra la sol. (2,1)

$2x+2y=5$ Non è risolubile in \mathbb{Z} poiché $2+5$

Allora QUANDO UN'EQ del tipo $ax+by=c$ è risolubile in \mathbb{Z} ?

D) QUANTE sol. ha una equazione?

- Anche qui talvolta dipende dall'insieme in cui si cercano le soluzioni. Ad es.

$$2x^2 - 3x + 1 = 0 \quad \text{ha sol. } x_1 = 1, x_2 = \frac{1}{2}$$

Se voglio soluzioni in \mathbb{Z} ne ho una sola, se mi bastano ^{soltan} soluzioni reazionali ne ho due.

- $x+2y=5$, invece, ha infinite coppie (x,y) soluzione indipendentemente dal cercarle in \mathbb{Z} , \mathbb{R} ecc.
- $x^2 - 1 = (x-1)(x+1)$ ha addirittura per soluzioni tutti i numeri dell'insieme numerico in cui le cerco, poiché è una IDENTITA'.

E) Quali sono i metodi per trovare ALMENO UNA soluzione?

F) Quali sono le considerazioni per trovare TUTTE le soluzioni dell'equazione?

Nettiamo le domande (B), (C) sotto l'etichetta "RISOLUBILITÀ", le (E), (F) sotto l'etichetta "RISOLUZIONE".

Equazioni lineari diofantee

---> Conguenze
di numeri

(17)

Con questo nome si indicano equazioni del tipo

$$ax + by = c \quad \text{ove } a, b, c \in \mathbb{Z}$$

e le soluzioni (x, y) sono cercate nelle coppie ordinate di numeri interi (relativi).

Teorema (condizione necessaria e sufficiente di RISOLUBILITÀ). C.u.s. perché

$$(*) \quad ax + by = c \quad \text{con } a, b, c \in \mathbb{Z}$$

ammetta sol. intere è che

M.C.D.(a, b) divide c.

con $a \in \mathbb{Z}$
 $b \in \mathbb{Z}$

Dime. Sia (x_0, y_0) una sol. di $(*)$ e d un divisore comune di a e di b: $a = da'$, $b = db'$
 $da'x_0 + db'y_0 = c \Rightarrow d(a'x_0 + b'y_0) = c$
cioè d divide c.

Dunque se $(*)$ è risolubile ogni divisore comune ad a e b divide c, in part. M.C.D.(a, b).

Viceversa, se d è un M.C.D.(a, b) con l'algoritmo euclideo trovo x_1 e y_1 t.c.

$$ax_1 + by_1 = d.$$

Quindi se d divide c, esiste $\exists c_1 \in \mathbb{Z}$ t.c. $dc_1 = c$,
 $ax_1c_1 + by_1c_1 = dc_1 = c$.

Dunque se M.C.D.(a, b) divide c la coppia di interi (x_1c_1, y_1c_1) è UNA soluzione di $(*)$. ■

Quante sono le soluzioni?

Proposizione (Ricerca di TUTTE le soluz. della equaz. diofantea (*)). Se $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ è una soluzione di

$$(*) \quad ax + by = c, \quad a, b, c \in \mathbb{Z}$$

tutte e sole le soluzioni di (*) hanno la forma

$$(•) \quad (x_0 + \frac{b}{d} h, y_0 - \frac{a}{d} h)$$

ove d è un M.C.D(a,b) e h varia comunque in \mathbb{Z} .

NOTA: $\frac{b}{d}$ e $\frac{a}{d}$ sono interi: b_1, a_1 .

Dim. Le coppie ordinate (•) sono soluzioni poiché appartengono a $\mathbb{Z} \times \mathbb{Z}$ e

$$a(x_0 + \frac{b}{d} h) + b(y_0 - \frac{a}{d} h) = ax_0 + by_0 = c.$$

Viceversa se $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$ è un'altra sol. di (*) si ha

$$\begin{cases} ax_0 + by_0 = c \\ ax_1 + by_1 = c \end{cases} \Rightarrow a(x_1 - x_0) + b(y_1 - y_0) = 0$$

e, dividendo per $d = \text{M.C.D}(a, b)$

$$\Rightarrow a_1(x_1 - x_0) = b_1(y_1 - y_0)$$

cioè b_1 divide $a_1(x_1 - x_0)$, ma b_1 non ha fattori in comune con $a_1 \Rightarrow b_1$ divide $x_1 - x_0$:

$$x_1 - x_0 = b_1 h \quad \text{con } h \in \mathbb{Z}$$

$$\Rightarrow a_1 b_1 h = b_1 (y_1 - y_0) \Rightarrow y_1 - y_0 = a_1 h$$

Quindi

$$x_1 = x_0 + \frac{b}{d} h, \quad y_1 = y_0 - \frac{a}{d} h. \quad \blacksquare$$

Esempi

(19)

1) $2x + 6y = 15$ non ha soluzioni intere

2) $9x + 15y = 27$ ha sol. intere

una è data da $(x_0, y_0) = (3, 0)$ e visto che $a_1 = 3$, $b_1 = 5$, l'insieme delle soluzioni è dato da

$$\{(3 + 5h, 0 - 3h), h \in \mathbb{Z}\}$$

3) $728x + 441y = 455$

a) RISOLUBILITÀ

$$728 = 441 \cdot 1 + 287$$

$$441 = 287 \cdot 1 + 154$$

$$287 = 154 \cdot 1 + 133$$

$$154 = 133 \cdot 1 + 21$$

$$133 = 21 \cdot 6 + 7$$

$$21 = 7 \cdot 3 + 0$$

$$455 = 7 \cdot 65 + 0$$

$$\Rightarrow \text{M.C.D.}(728, 441) = 7$$

\Rightarrow risolubilità.

b) RICERCA di UNA SOLUZIONE

$728 = a$, $441 = b$. Rileggo la sequenza precedente:

$$287 = a - b$$

$$154 = b - (a - b) = -a + 2b$$

$$133 = (a - b) - (2b - a) = 2a - 3b$$

$$21 = 2b - a - (2a - 3b) = 5b - 3a$$

$$\bullet 65 \quad 7 = 2a - 3b - 6(5b - 3a) = 20a - 33b$$

$$\Rightarrow 455 = 7 \cdot 65 = 20 \cdot 65 a + (-33 \cdot 65) b : \begin{cases} x_0 = 1300 \\ y_0 = -2145 \end{cases}$$

c) l'insieme delle soluzioni:

$$\{(1300 + 63h, -2145 - 104h), h \in \mathbb{Z}\}$$



Un commento alle soluzioni dell'es. 3

19/05

A) Che 7 fosse un comune divisore di 728, 441 (e 455) si poteva intuire:

$$728 = 7 \cdot 104 = 2^2 \cdot 7 \cdot 23$$

2 non divide 441 ma 7 sì: $441 = 7 \cdot 63 = 3^2 \cdot 7^2$
(e $455 = 7 \cdot 65 = 5 \cdot 7 \cdot 13$)

La fattorizzazione iniziali dice anche che
 $\text{MCD}(728, 441) = 7$.

Quindi si poteva "dividere l'equazione" per 7
 $104x + 63y = 65$.

La divisione non comporta comunque un vantaggio nel numero di passaggi.

L'ALG. EUCL. delle divisioni successive richiede 6 divisioni e la successiva ricerca di una soluzione porta:

$$1 = \underline{104} \cdot 20 + \underline{63}(-33)$$

e, moltiplicando per 65, la stessa soluzione particolare.

B) Si può invece rendere più maneggevole la rappresentazione dell'insieme delle soluzioni osservando che, per $h=-20$, si ha

$$\begin{cases} x_1 = 1300 - 63 \cdot 20 = 40 \\ y_1 = -2145 + 104 \cdot 20 = -65 \end{cases}$$

\Rightarrow ins. delle soluzioni $\{(40+63k, -65-104k), k \in \mathbb{Z}\}$

o anche ($h=-21$)

ins. delle soluzioni $\{(-23+63k', 39-104k'), k' \in \mathbb{Z}\}$

Qualche esercizio per il fine settimana.

1. Utilizzare l'algoritmo euclideo per determinare se è risolubile (e, se sì, quali sono le sol.) dell'eq. diofantea:

$$3x + 53y = 5.$$

2. Considerare il numero intero MILLE.

Quante divisioni devo fare per rappresentarlo in base 3?

Più in generale, quante devo fare per rappresentarlo in base n ?

3. Quanti sono i fattori distinti (non necessariamente primi) del numero che, in base 10, si scrive come

$$441441?$$

Fare anche i quesiti sulla "divisibilità in \mathbb{Z} " postati in rete con queste lesioni