

# Matematica Discreta

22 marzo 2020

# Indice

<b>1</b>	<b>Numeri interi</b>	<b>2</b>
1.1	Insiemi numerici . . . . .	2
<b>2</b>	<b>Divisori e MCD</b>	<b>3</b>
2.1	Divisori di un numero . . . . .	3
2.1.1	Definizioni e prime conseguenze . . . . .	3
2.1.2	Algoritmo di Euclide e Teorema di Bezout . . . . .	4
2.1.3	Conseguenze del teorema di Bezout . . . . .	5
2.2	Numeri primi . . . . .	7
2.2.1	Divisori primi . . . . .	8
2.3	Equazioni diofantee . . . . .	11
2.4	Congruenze . . . . .	12
2.4.1	Risolvere singole congruenze . . . . .	14
2.4.2	Sistemi di congruenze . . . . .	17

# Capitolo 1

## Numeri interi

### 1.1 Insiemi numerici

## Capitolo 2

# Divisori e MCD

### 2.1 Divisori di un numero

#### 2.1.1 Definizioni e prime conseguenze

**Definizione 2.1.1.** Siano  $a, b \in \mathbb{Z}$ ; allora si dice che  $a$  divide  $b$  se  $\exists k \in \mathbb{Z}$  tale che  $ak = b$ , e si scrive  $a \mid b$ .

**Definizione 2.1.2.** Siano  $a, b \in \mathbb{Z}$ . Allora si dice che  $b$  e' multiplo di  $a$  se  $\exists k \in \mathbb{Z}$  tale che  $b = ak$ .

*Osservazione.* La definizione di multiplo e' speculare a quella di divisore: se  $a$  e' divisore di  $b$  allora  $b$  e' multiplo di  $a$ .

**Proposizione 2.1.3.** Siano  $a, b, n \in \mathbb{Z}$  tali che  $n \mid a$  e  $n \mid b$ . Allora

$$n \mid a + b \quad (2.1)$$

$$n \mid a - b \quad (2.2)$$

$$n \mid ax \quad \forall x \in \mathbb{Z} \quad (2.3)$$

*Dimostrazione.* Per ipotesi, dato che  $n \mid a$  e  $n \mid b$ , allora  $\exists h, k \in \mathbb{Z}$  tali che  $nh = a$  e  $nk = b$ . Dunque:

$$a + b = nh + nk = n(h + k) \iff n \mid a + b$$

$$a - b = nh - nk = n(h - k) \iff n \mid a - b$$

$$ax = nhx = n(hx) \iff n \mid ax$$

che e' la tesi. □

**Definizione 2.1.4.** Siano  $a, b \in \mathbb{Z}$ ; allora si dice  $\text{mcd}(a, b)$  il piu' grande intero positivo tale che  $\text{mcd}(a, b) \mid a$  e  $\text{mcd}(a, b) \mid b$ .

**Definizione 2.1.5.** Siano  $a, b \in \mathbb{Z}$ . Allora si dice minimo comune multiplo di  $a$  e  $b$  il numero  $d = \text{mcm}(a, b)$  tale che  $d$  e' il piu' piccolo multiplo positivo sia di  $a$  che di  $b$ .

**Definizione 2.1.6.** Siano  $a, b \in \mathbb{Z}$ . Se  $\text{mcd}(a, b) = 1$  allora  $a$  e  $b$  si dicono coprimi.

*Osservazione.* Siano  $a, b \in \mathbb{Z}$ . Allora valgono le seguenti proprietà per  $\text{mcd}(a, b)$ :

$$\begin{aligned}\text{mcd}(a, b) &= \text{mcd}(\pm a, \pm b) \\ \text{mcd}(a, 1) &= \text{mcd}(1, a) = 1 \\ \text{mcd}(a, 0) &= \text{mcd}(0, a) = 0 \\ &\neq \text{mcd}(0, 0)\end{aligned}$$

**Teorema 2.1.7** (Esistenza e unicità del resto). *Siano  $a, b \in \mathbb{Z}$ , con  $b \neq 0$ . Allora esistono e sono unici  $q, r \in \mathbb{Z}$  tali che*

$$a = bq + r, \quad 0 \leq r < |b| \quad (2.4)$$

*Tale  $r$  si dice resto della divisione di  $a$  per  $b$ , e si indica anche con  $r = a \bmod b$ .*

*Dimostrazione.* Notiamo inoltre che i numeri della forma  $a - bq$  formano una progressione aritmetica di passo  $b$  al variare di  $q \in \mathbb{Z}$ . Il resto  $r$  definito in questo modo è l'unico elemento di questa progressione compreso tra 0 e  $b - 1$ .  $\square$

**Proposizione 2.1.8.** *Siano  $a, b, c \in \mathbb{Z}$ . Allora*

$$\text{mcm}(a, b) \mid c \iff a \mid c \wedge b \mid c \quad (2.5)$$

*Dimostrazione.* Dimostriamo separatamente i due versi dell'implicazione.

Dato che  $\text{mcm}(a, b)$  è un multiplo di  $a$  e di  $b$  e per ipotesi  $c$  è un multiplo di  $\text{mcm}(a, b)$ , allora per transitività segue che  $c$  è un multiplo di  $a$  e di  $b$ .

Supponiamo che  $c$  sia un multiplo di  $a$  e di  $b$ . Allora per il teorema 2.1.7 esistono  $q, r \in \mathbb{Z}$  tali che

$$c = \text{mcm}(a, b)q + r$$

con  $0 \leq r < \text{mcm}(a, b)$ . Dato che  $a, b$  dividono sia  $c$  (per ipotesi) che  $\text{mcm}(a, b)$  (per definizione di  $\text{mcm}$ ), allora segue che essi dividono anche  $r$ . Ma  $0 \leq r < \text{mcm}(a, b)$ , dunque necessariamente  $r = 0$ , cioè  $c = \text{mcm}(a, b)q$  e quindi  $\text{mcm}(a, b) \mid c$ .  $\square$

## 2.1.2 Algoritmo di Euclide e Teorema di Bezout

**Teorema 2.1.9.** *Siano  $a, b \in \mathbb{Z}$ . Allora*

$$\text{mcd}(a, b) = \text{mcd}(a, b - a) = \text{mcd}(a - b, b). \quad (2.6)$$

*Dimostrazione.* Ovviamente  $\text{mcd}(a, b) = \text{mcd}(b, a)$ , dunque se vale la prima uguaglianza varrà anche la seconda, in quanto

$$\text{mcd}(a, b) = \text{mcd}(b, a) = \text{mcd}(b, a - b) = \text{mcd}(a - b, b).$$

Dunque è sufficiente dimostrare che  $\text{mcd}(a, b) = \text{mcd}(a, b - a)$ . Sia  $\mathbb{D}_{x,y}$  l'insieme dei divisori comuni a  $x$  e  $y$ , cioè

$$\mathbb{D}_{x,y} = \{d \text{ tale che } d \mid x \wedge d \mid y\}$$

Allora per dimostrare la tesi è sufficiente dimostrare che  $\mathbb{D}_{a,b} = \mathbb{D}_{a,b-a}$ , in quanto se i due insiemi sono uguali necessariamente anche i loro massimi saranno uguali.

Dimostriamo che  $\mathbb{D}_{a,b} \subseteq \mathbb{D}_{a,b-a}$ . Sia  $d \in \mathbb{D}_{a,b}$ , cioè  $d \mid a$  e  $d \mid b$ . Allora per la proposizione 2.1.3 segue che  $d \mid b - a$ , cioè  $d \in \mathbb{D}_{a,b-a}$ , cioè  $\mathbb{D}_{a,b} \subseteq \mathbb{D}_{a,b-a}$ .

Dimostriamo ora che  $\mathbb{D}_{a,b-a} \subseteq \mathbb{D}_{a,b}$ . Sia  $d \in \mathbb{D}_{a,b-a}$ , cioè  $d \mid a$  e  $d \mid b - a$ . Allora per la proposizione 2.1.3 segue che  $d \mid a + (b - a)$ , cioè  $d \mid b$ , cioè  $d \in \mathbb{D}_{a,b}$ , cioè  $\mathbb{D}_{a,b-a} \subseteq \mathbb{D}_{a,b}$ .

Dunque dato che valgono sia  $\mathbb{D}_{a,b} \subseteq \mathbb{D}_{a,b-a}$  e  $\mathbb{D}_{a,b-a} \subseteq \mathbb{D}_{a,b}$ , allora vale  $\mathbb{D}_{a,b} = \mathbb{D}_{a,b-a}$ . In particolare il massimo di questi due insiemi dovrà essere lo stesso, quindi  $\text{mcd}(a, b) = \text{mcd}(a, b - a)$ , che è la tesi.  $\square$

Dunque per calcolare il massimo comun divisore si può sfruttare il seguente algoritmo, detto **algoritmo di Euclide**, che si basa sul teorema 2.1.9:

1. Se  $a = 1$  oppure  $b = 1$  allora  $\text{mcd}(a, b) = 1$ .
2. Se  $a = 0$  e  $b \neq 0$  allora  $\text{mcd}(a, b) = b$ .
3. Se  $a \neq 0$  e  $b = 0$  allora  $\text{mcd}(a, b) = a$ .
4. Se  $a \neq 0$  e  $b \neq 0$ , allora
  - se  $a \leq b$  segue che  $\text{mcd}(a, b) = \text{mcd}(a - b, b)$ ;
  - se  $a > b$  segue che  $\text{mcd}(a, b) = \text{mcd}(a, b - a)$

dove i valori di  $\text{mcd}(a - b, b)$  o  $\text{mcd}(a, b - a)$  vengono calcolati riapplicando l'algoritmo.

**Teorema 2.1.10** (di Bezout). *Siano  $a, b \in \mathbb{Z}$ . Allora esistono  $x, y \in \mathbb{Z}$  tali che*

$$ax + by = \text{mcd}(a, b) \quad (2.7)$$

### 2.1.3 Conseguenze del teorema di Bezout

Elenchiamo in questa sezione alcune conseguenze del teorema di Bezout sulle proprietà dei divisori e sul loro rapporto con il massimo comun divisore di due numeri.

**Proposizione 2.1.11.** *Siano  $a, b, n \in \mathbb{Z}$ . Allora*

$$n \mid ab \wedge \text{mcd}(a, n) = 1 \implies n \mid b. \quad (2.8)$$

*Intuizione.* Se  $n$  divide  $ab$ , allora tutti i fattori primi che dividono  $n$  dovranno essere contenuti in  $ab$ . Dato che  $\text{mcd}(n, a) = 1$ , questi fattori non possono essere contenuti in  $a$ , dunque dovranno essere tutti contenuti in  $b$ .

*Dimostrazione.* Per il teorema di Bezout (2.1.10) esistono  $x, y \in \mathbb{Z}$  tali che

$$ax + ny = \text{mcd}(a, n) = 1$$

Moltiplicando per  $b$  otteniamo

$$abx + nby = b$$

Ma  $n \mid abx$  (poiché  $n \mid ab$ ) e  $n \mid nby$ , dunque  $n \mid abx + nby$ , cioè  $n \mid b$ .  $\square$

**Proposizione 2.1.12.** *Siano  $a, b, t \in \mathbb{Z}$  tali che  $t \mid a$ ,  $t \mid b$ . Allora  $t \leq \text{mcd}(a, b)$ .*

*Dimostrazione.* La proposizione deriva direttamente dalla definizione di massimo comun divisore: se  $t$  e' un divisore comune ad  $a$  e  $b$ , allora  $t$  sara' minore o uguale al massimo dei divisori comuni di  $a$  e  $b$ , cioe'  $t \leq \text{mcd}(a, b)$ .  $\square$

**Proposizione 2.1.13.** *Siano  $a, b, t \in \mathbb{Z}$  tali che  $t \mid a$ ,  $t \mid b$ . Allora  $t \mid \text{mcd}(a, b)$ .*

*Dimostrazione.* Per la proposizione 2.1.3, se  $t \mid a$  e  $t \mid b$  allora  $t \mid ax + by$  per ogni  $x, y \in \mathbb{Z}$ . Per il teorema di Bezout (2.1.10) esistono  $\bar{x}, \bar{y} \in \mathbb{Z}$  tali che  $a\bar{x} + b\bar{y} = \text{mcd}(a, b)$ . Ma quest'espressione e' della forma  $ax + by$ , con  $x = \bar{x}$ ,  $y = \bar{y}$ , dunque  $t \mid a\bar{x} + b\bar{y}$ , cioe'  $t \mid \text{mcd}(a, b)$ .  $\square$

**Proposizione 2.1.14.** *Siano  $a, b, t \in \mathbb{Z}$ . Allora*

$$t \mid \text{mcd}(a, b) \iff (\forall x, y \in \mathbb{Z}. \quad t \mid ax + by). \quad (2.9)$$

*Dimostrazione.* Dimostriamo entrambi i versi dell'implicazione.

- Se  $t \mid \text{mcd}(a, b)$ , allora  $t \mid a$  e  $t \mid b$ , dunque per la proposizione 2.1.3 segue che  $t$  dovra' dividere una qualsiasi combinazione lineare di  $a$  e  $b$ , cioe'  $t \mid ax + by$  per ogni  $x, y \in \mathbb{Z}$ .
- Viceversa supponiamo che  $t \mid ax + by$  per ogni  $x, y \in \mathbb{Z}$ . Siano per il teorema di Bezout (2.1.10)  $\bar{x}, \bar{y}$  i numeri tali che  $a\bar{x} + b\bar{y} = \text{mcd}(a, b)$ . Allora  $t$  dovra' dividere anche  $a\bar{x} + b\bar{y}$ , cioe'  $t \mid \text{mcd}(a, b)$ .

$\square$

**Proposizione 2.1.15.** *Siano  $a, b, n \in \mathbb{Z}$ . Allora*

$$\text{mcd}(an, bn) = n \text{mcd}(a, b) \quad (2.10)$$

*Intuizione.* Se due numeri hanno  $n$  come fattore comune, ovviamente il massimo comun divisore dovra' contenere  $n$  e quindi dovra' essere un multiplo di  $n$ .

*Dimostrazione.* Osserviamo che se due numeri hanno gli stessi divisori allora sono uguali, a meno del segno. Sia  $t \in \mathbb{Z}$  tale che  $t \mid an$  e  $t \mid nb$ . Per la proposizione 2.1.14 allora

$$\begin{aligned} & t \mid \text{mcd}(an, bn) \\ \iff & t \mid nax + nby \quad \forall x, y \in \mathbb{Z} \\ \iff & t \mid n(ax + by) \quad \forall x, y \in \mathbb{Z} \end{aligned}$$

dunque scegliendo  $x, y$  tali che  $ax + by = \text{mcd}(a, b)$  per Bezout (2.1.10)

$$\iff t \mid n \text{mcd}(a, b).$$

$\square$

**Corollario 2.1.16.** *Siano  $a, b \in \mathbb{Z}$  e sia  $d = \text{mcd}(a, b)$ . Allora  $\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ .*

*Intuizione.* Se dividiamo due numeri per il loro mcd stiamo eliminando dalla loro fattorizzazione tutti i primi comuni ad entrambi, quindi i due numeri risultanti dall'operazione non potranno avere primi in comune e quindi saranno coprimi.

*Dimostrazione.* Siano  $a', b'$  tali che  $a = a'd, b = b'd$ . Allora per la proposizione 2.1.15

$$\begin{aligned}\text{mcd}(a, b) &= \text{mcd}(a'd, b'd) \\ &= d \text{mcd}(a', b') \\ &= \text{mcd}(a, b) \text{mcd}(a', b').\end{aligned}$$

Dividendo entrambi i membri per  $\text{mcd}(a, b)$  otteniamo

$$\text{mcd}(a', b') = 1$$

che, per definizione di  $a', b'$  e' equivalente a

$$\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

che e' la tesi. □

## 2.2 Numeri primi

**Definizione 2.2.1.** Sia  $p \in \mathbb{Z}$ . Si dice che  $p$  e' primo se se gli unici interi che dividono  $p$  sono  $\pm 1$  e  $\pm p$ .

**Proposizione 2.2.2.** Se  $p$  e' primo e  $p \mid ab$ , allora  $p \mid a$  oppure  $p \mid b$ .

*Dimostrazione.* Supponiamo  $p \nmid a$ . Dato che  $p$  e' primo,  $\text{mcd}(a, p) = 1$  oppure  $p$ . Tuttavia se  $\text{mcd}(a, p) = p$  allora  $p \mid a$ , che va contro l'ipotesi, dunque  $\text{mcd}(a, p) = 1$ . Per la proposizione 2.1.11 allora  $p \mid b$ , che e' la tesi. □

**Proposizione 2.2.3.** Siano  $a, b \in \mathbb{Z}, c \in \mathbb{Z}$  tali che  $\text{mcd}(a, b) = 1$ . Allora

$$a \mid c \wedge b \mid c \iff ab \mid c \quad (2.11)$$

*Dimostrazione.* Per il teorema di Bezout (2.1.10) esistono  $x, y \in \mathbb{Z}$  tali che  $\text{mcd}(a, b) = 1 = ax + by$ , da cui segue  $n = nax + nby$ . Dato che  $a \mid n, b \mid n$ , allora  $ab \mid na$  e  $ab \mid nb$  per la proposizione 2.1.3, quindi per la stessa proposizione  $ab$  dividera' una loro qualunque combinazione lineare  $nak + nbh$ , inclusa quella con  $k = x, h = y$ . Dunque  $ab \mid nax + nby$  che e' equivalente a dire che  $ab \mid n$ , cioe' la tesi. □

**Proposizione 2.2.4.** Siano  $a, b, c \in \mathbb{Z}$ . Allora

$$\text{mcd}(ab, c) = 1 \iff \text{mcd}(a, c) = \text{mcd}(b, c) = 1 \quad (2.12)$$

*Intuizione.* Dimostrazione intuitiva: se  $a$  e  $b$  sono coprimi con  $c$  significa che  $a$  non ha nessun fattore in comune con  $c$ , e stessa cosa per  $b$ . Ma il loro prodotto  $ab$  viene diviso dagli stessi primi che dividono  $a$  e  $b$  separatamente, quindi deve essere anch'esso coprimo con  $c$ .

Al contrario, se  $ab$  non ha fattori primi in comune con  $c$ , allora naturalmente  $a, b$  (essendo divisori di  $ab$ ) non avranno fattori in comune con  $c$ .

**Corollario 2.2.5.** Siano  $a_1, a_2, \dots, a_n \in \mathbb{Z}, c \in \mathbb{Z}$  tali che  $a_1, \dots, a_n$  siano coprimi con  $c$ . Allora anche il loro prodotto  $\prod_{i=1}^n a_i$  e' coprimo con  $c$ .



*Intuizione.* Stessa idea della dimostrazione della proposizione 2.2.4 ma estesa a  $n$  numeri.

**Proposizione 2.2.6.** *Siano  $a_1, a_2, \dots, a_n \in \mathbb{Z}, c \in \mathbb{Z}$  tali che  $a_1, \dots, a_n$  siano coprimi tra loro e che per ogni  $i < n$  vale che  $a_i \mid c$ . Allora*

$$a_1 a_2 \dots a_n = \left( \prod_{i=1}^n a_i \right) \mid c. \quad (2.13)$$

*Intuizione.* Quest'ultima proposizione ci dice che se  $a_1, \dots, a_n$  non hanno fattori primi in comune e ognuno di loro divide  $c$ , allora anche il loro prodotto dovrà dividere  $c$ , perché il loro prodotto è formato esattamente dai fattori primi che dividono  $c$ .

*Dimostrazione.* Dimostriamo la proposizione per induzione su  $n$ .

- **Caso base.**

Sia  $n = 0$ , cioè  $a_1 \dots a_n = 1$ . Allora banalmente  $1 \mid c$ .

- **Passo induttivo.**

Supponiamo che la tesi sia vera per  $n - 1$  e dimostriamola per  $n$ . Dunque per ipotesi  $\left( \prod_{i=1}^{n-1} a_i \right) \mid c$ . Ma per il corollario 2.2.5  $a_n$  è coprimo con  $\prod_{i=1}^{n-1} a_i$ , dunque per la proposizione 2.2.3 segue che

$$a_n \left( \prod_{i=1}^{n-1} a_i \right) = \left( \prod_{i=1}^n a_i \right) \mid c$$

che è la tesi per  $n$ .

Dunque la proposizione vale per ogni  $n \in \mathbb{N}$ . □

### 2.2.1 Divisori primi

**Proposizione 2.2.7.** *Siano  $a, b, k \in \mathbb{Z}, p \in \mathbb{Z}$  primo. Allora*

$$p^k \mid \text{mcd}(a, b) \iff p^k \mid a \wedge p^k \mid b \quad (2.14)$$

$$p^k \mid \text{mcm}(a, b) \iff p^k \mid a \vee p^k \mid b. \quad (2.15)$$

*Intuizione.* Il massimo comun divisore di due numeri è un divisore comune ad entrambi, quindi se  $p^k$  lo divide deve dividere entrambi i numeri.

Il minimo comune multiplo invece è formato da tutti i fattori primi comuni e non comuni col massimo esponente, quindi se  $p^k$  divide il minimo comune multiplo dovrà dividere almeno uno dei due numeri di partenza.

**Proposizione 2.2.8.** *Siano  $a, b \in \mathbb{Z}$ . Allora se  $\text{mcd}(a, b) = 1$  segue che  $\text{mcm}(a, b) = |ab|$ .*

*Intuizione.* Se i due numeri sono coprimi, allora non hanno fattori primi in comune, dunque il loro massimo comune multiplo sarà formato precisamente da tutti i fattori di entrambi i numeri, cioè dal loro prodotto.

*Dimostrazione.* Sappiamo per definizione di mcm che  $a \mid \text{mcm}(a, b)$  e  $b \mid \text{mcm}(a, b)$ . Dato che  $\text{mcd}(a, b) = 1$  per la proposizione 2.2.3 segue che  $ab \mid \text{mcm}(a, b)$ , cioè  $|ab| \leq \text{mcm}(a, b)$ . Ma  $ab$  è un multiplo di  $a$  e di  $b$ , quindi dovrà valere che  $|ab| \geq \text{mcm}(a, b)$  in quanto  $\text{mcm}(a, b)$  è il minimo multiplo comune ad  $a$  e  $b$ . Da ciò segue che  $\text{mcm}(a, b) = |ab|$ , cioè la tesi.  $\square$

**Proposizione 2.2.9.** *Siano  $a, x, y \in \mathbb{Z}$ . Allora*

$$\text{mcd}(a, x) = 1 \implies \text{mcd}(a, xy) = \text{mcd}(a, y) \quad (2.16)$$

*Intuizione.* Se stiamo calcolando  $\text{mcd}(a, b)$  dove  $b = xy$  e sappiamo che il fattore  $x$  non è comune tra  $b$  ed  $a$ , allora possiamo escluderlo dal massimo comun divisore.

*Dimostrazione.* Dato che  $\text{mcd}(a, x) = 1$ , allora se un primo  $p$  divide  $a$  sicuramente  $p$  non divide  $x$ . Per la proposizione 2.2.7 allora vale

$$\begin{aligned} p^k &\mid \text{mcd}(a, xy) \\ \iff p^k &\mid a \wedge p^k \mid xy \end{aligned}$$

ma  $p^k \nmid x$  dunque per la 2.1.11

$$\begin{aligned} \iff p^k &\mid a \wedge p^k \mid y \\ \iff p^k &\mid \text{mcd}(a, y). \end{aligned}$$

Dato che  $\text{mcd}(a, xy)$  e  $\text{mcd}(a, y)$  vengono divisi dagli stessi primi, per il teorema fondamentale devono essere uguali.  $\square$

**Proposizione 2.2.10.** *Siano  $a, x, y \in \mathbb{Z}$ . Allora*

$$\text{mcd}(a, \text{mcm}(x, y)) = \text{mcm}(\text{mcd}(a, x), \text{mcd}(a, y)) \quad (2.17)$$

*Dimostrazione.* Per la proposizione 2.2.7 allora vale

$$\begin{aligned} p^k &\mid \text{mcd}(a, \text{mcm}(x, y)) \\ \iff p^k &\mid a \wedge (p^k \mid x \vee p^k \mid y) \\ \iff (p^k &\mid a \wedge p^k \mid x) \vee (p^k \mid a \wedge p^k \mid y) \\ \iff p^k &\mid \text{mcm}(\text{mcd}(a, x), \text{mcd}(a, y)). \end{aligned}$$

Dato che  $\text{mcd}(a, \text{mcm}(x, y))$  e  $\text{mcm}(\text{mcd}(a, x), \text{mcd}(a, y))$  vengono divisi dagli stessi primi, per il teorema fondamentale devono essere uguali.  $\square$

**Proposizione 2.2.11.** *Siano  $a, x, y \in \mathbb{Z}$ . Allora*

$$\text{mcd}(x, y) = 1 \implies \text{mcd}(a, xy) = \text{mcd}(a, x) \text{mcd}(a, y) \quad (2.18)$$

*Intuizione.* Se  $x$  e  $y$  non hanno fattori in comune, i fattori che  $a$  ha in comune con il loro prodotto sono o in  $x$  o in  $y$ , quindi per ottenerli tutti possiamo dividere l'mcd in due e moltiplicare i due risultati.

*Dimostrazione.* Dato che  $\text{mcd}(x, y) = 1$  allora per la proposizione 2.2.8 vale che  $\text{mcm}(x, y) = |xy|$ . Dunque  $\text{mcd}(a, xy) = \text{mcd}(a, |xy|) = \text{mcd}(a, \text{mcm}(x, y)) = \text{mcm}(\text{mcd}(a, x), \text{mcd}(a, y))$  per la proposizione 2.2.10.

Verifichiamo ora che  $\text{mcd}(a, x)$  e  $\text{mcd}(a, y)$  sono coprimi. Per ipotesi sappiamo che  $x, y$  sono coprimi; ma dato che  $\text{mcd}(a, x)$  e  $\text{mcd}(a, y)$  sono divisori di  $x$  e  $y$  rispettivamente, allora dovranno essere anche loro coprimi.

Dunque per la proposizione 2.2.8 segue che

$$\text{mcd}(a, xy) = \text{mcm}(\text{mcd}(a, x), \text{mcd}(a, y)) = \text{mcd}(a, x) \text{mcd}(a, y)$$

che e' la tesi. □

**Proposizione 2.2.12.** *Siano  $a, b, c \in \mathbb{Z}$ . Allora*

$$a \mid c \wedge b \mid c \iff \frac{ab}{\text{mcd}(a, b)} \mid c \quad (2.19)$$

*Dimostrazione.* Dimostriamo l'implicazione in entrambi i versi.

- Supponiamo che  $a \mid c$  e  $b \mid c$ . Sia  $d = \text{mcd}(a, b)$ . Allora dato che  $d \mid a$ ,  $d \mid b$  per transitivita'  $d \mid c$ , dunque  $\frac{a}{d} \mid \frac{c}{d}$  e  $\frac{b}{d} \mid \frac{c}{d}$ . Ma dato che per il corollario 2.1.16 sappiamo che  $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$ , dunque per la 2.2.3 segue che il loro prodotto  $\frac{ab}{d^2}$  dovra' dividere  $\frac{c}{d}$ , che e' equivalente a dire che  $\frac{ab}{d} \mid c$ .

- NON SO FARE QUEST'ALTRA DIMOSTRAZIONE □

**Proposizione 2.2.13.** *Siano  $a, b \in \mathbb{Z}$ . Allora*

$$\text{mcd}(a, b) \text{mcm}(a, b) = |ab| \quad (2.20)$$

*Dimostrazione.* Sia  $c \in \mathbb{Z}$  tale che  $a \mid c$ ,  $b \mid c$ . Allora per la proposizione 2.2.12 segue che  $\frac{ab}{\text{mcd}(a, b)} \mid c$ . Inoltre per la proposizione 2.1.8 segue che  $\text{mcm}(a, b) \mid c$ . Dunque i due numeri  $\frac{ab}{\text{mcd}(a, b)}$  e  $\text{mcm}(a, b)$  hanno gli stessi divisori, dunque devono essere uguali a meno del segno, da cui segue

$$\text{mcd}(a, b) \text{mcm}(a, b) = |ab|.$$

□

## 2.3 Equazioni diofantee

**Definizione 2.3.1.** Siano  $a, b, c \in \mathbb{Z}$  noti,  $x, y \in \mathbb{Z}$  incognite. Allora un'equazione lineare della forma  $ax + by = c$  si dice equazione diofantea.

**Teorema 2.3.2.** Siano  $a, b, c \in \mathbb{Z}$ . Allora l'equazione diofantea  $ax + by = c$  ammette soluzioni se e solo se  $\text{mcd}(a, b) \mid c$ .

*Dimostrazione.* Supponiamo che  $c = k \text{mcd}(a, b)$  per qualche  $k \in \mathbb{Z}$ . Allora per il teorema di Bezout 2.1.10 esistono  $x', y' \in \mathbb{Z}$  tali che  $ax' + by' = \text{mcd}(a, b)$ . Moltiplicando entrambi i membri per  $k$  otteniamo

$$k \text{mcd}(a, b) = k(ax' + by') = akx' + bky' = a(kx') + b(ky')$$

dunque  $x = kx'$  e  $y = ky'$  risolvono l'equazione diofantea.

Supponiamo ora che  $c$  non sia un multiplo di  $\text{mcd}(a, b)$  e supponiamo per assurdo che l'equazione abbia soluzione, cioè che esistano  $x, y \in \mathbb{Z}$  tali che  $ax + by = c$ . Sia  $d = \text{mcd}(a, b)$ . Per definizione di  $\text{mcd}(a, b)$  e per la proposizione 2.1.3, dato che  $d \mid a$  e  $d \mid b$  segue che  $d \mid ax$ ,  $d \mid by$  e dunque  $d \mid ax + by$ . Ma  $ax + by = c$ , quindi  $d = \text{mcd}(a, b) \mid c$ , che va contro le ipotesi. Dunque l'equazione diofantea non ha soluzione, cioè la tesi.  $\square$

**Teorema 2.3.3.** Siano  $a, b \in \mathbb{Z}$  coprimi. Allora le soluzioni dell'equazione diofantea omogenea  $ax + by = 0$  sono tutte e solo della forma  $x = -kb, y = ka$  al variare di  $k \in \mathbb{Z}$ .

*Dimostrazione.* Dimostriamo innanzitutto che  $x = -kb, y = ka$  è una soluzione.

$$\begin{aligned} ax + by &= a(-kb) + b(ka) \\ &= -kab + kab \\ &= 0 \end{aligned}$$

Mostriamo ora che non vi possono essere altre soluzioni. Dato che  $ax + by = 0$ , allora  $ax = -by$ . Dato che  $a \mid ax$  allora  $a \mid -by$ ; inoltre per ipotesi  $\text{mcd}(a, -b) = \text{mcd}(a, b) = 1$ . Dunque per il teorema 2.1.11 segue che  $a \mid y$ , cioè  $y = ak$  per qualche  $k \in \mathbb{Z}$ . Sostituendo ottengo  $x = -b \frac{y}{a} = -bk$ , che è la tesi.  $\square$

**Corollario 2.3.4.** Se  $a, b$  non sono coprimi, allora tutte le soluzioni dell'equazione  $ax + by = 0$  saranno della forma  $x = -kb', y = ka'$  dove  $a' = \frac{a}{\text{mcd}(a, b)}$  e  $b' = \frac{b}{\text{mcd}(a, b)}$ .

*Dimostrazione.* Dato che  $a, b$  non sono coprimi, allora possiamo dividere entrambi i membri di  $ax + by = 0$  per  $\text{mcd}(a, b)$  ottenendo l'equazione diofantea equivalente  $a'x + b'y = 0$ . Ma per il teorema 2.1.16  $\text{mcd}(a', b') = 1$ , dunque per il teorema 2.3.3 le sue soluzioni saranno tutte e solo della forma  $x = -kb', y = ka'$ . Ma questa equazione è equivalente all'originale, dunque anche le soluzioni di  $ax + by = 0$  saranno tutte e solo della forma  $x = -kb', y = ka'$ .  $\square$

**Teorema 2.3.5.** Siano  $a, b \in \mathbb{Z}$ . Allora le soluzioni dell'equazione diofantea  $ax + by = c$  si ottengono sommando ad una soluzione particolare (se esiste) una soluzione qualsiasi dell'equazione omogenea associata  $ax + by = 0$ .

*Dimostrazione.* Dimostriamo innanzitutto che se  $(x, y)$  e' una soluzione della diofantea non omogenea e  $(x_0, y_0)$  e' una soluzione dell'omogenea, allora  $(x + x_0, y + y_0)$  e' ancora soluzione della non omogenea.

$$\begin{aligned} a(x + x_0) + b(y + y_0) &= ax + ax_0 + by + by_0 \\ &= (ax + by) + (ax_0 + by_0) \\ &= c + 0 \\ &= c \end{aligned}$$

Dimostriamo ora che tutte le soluzioni sono di questa forma. Sia  $(\bar{x}, \bar{y})$  una soluzione particolare della diofantea non omogenea e  $(x, y)$  un'altra soluzione qualsiasi, e mostriamo che la loro differenza e' una soluzione dell'omogenea associata.

$$\begin{aligned} a(x - \bar{x}) + b(y - \bar{y}) &= ax - a\bar{x} + by - b\bar{y} \\ &= (ax + by) - (a\bar{x} + b\bar{y}) \\ &= c - c \\ &= 0 \end{aligned}$$

che e' la tesi. □

## 2.4 Congruenze

**Definizione 2.4.1.** Siano  $a, b, m \in \mathbb{Z}$ ,  $m > 0$ . Allora si dice che  $a$  e' congruo a  $b$  modulo  $m$  se e solo se  $a - b$  e' un multiplo di  $m$ , e si scrive

$$a \equiv b \pmod{m}$$

**Teorema 2.4.2.** Siano  $a, b, m \in \mathbb{Z}$ ,  $m > 0$ . Allora la relazione di congruenza  $\equiv \pmod{m}$  e' una relazione di equivalenza, e dunque soddisfa le proprieta':

$$\text{Riflessiva:} \quad a \equiv a \pmod{m} \quad (2.21)$$

$$\text{Simmetrica:} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m} \quad (2.22)$$

$$\text{Riflessiva:} \quad a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m} \quad (2.23)$$

*Dimostrazione.* Dimostriamo le tre proprieta' della congruenza come relazione di equivalenza.

1.  $a - a = 0 = 0m$ , dunque  $a \equiv a \pmod{m}$ .
2. Se  $a - b = km$  allora  $b - a = -(a - b) = -km = (-k)m$ , cioe'  $b \equiv a \pmod{m}$ .
3. Se  $a - b = km$  e  $b - c = hm$  allora  $a - c = (a - b) + (b - c) = km + hm = (k + h)m$ , cioe'  $a \equiv c \pmod{m}$ .

□

**Teorema 2.4.3.** Siano  $a, b, m \in \mathbb{Z}$ ,  $m > 0$ . Allora

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m \quad (2.24)$$

cioe'  $a$  e' congruo a  $b$  se e solo se  $a$  e  $b$  hanno lo stesso resto quando divisi per  $m$ .

*Dimostrazione.* Dimostriamo l'implicazione nei due versi.

Siano  $r = a \bmod m$ ,  $r' = b \bmod m$  i resti di  $a$  e  $b$  modulo  $m$ , cioè  $a = cq + r$  e  $b = cq' + r'$  per qualche  $q, q' \in \mathbb{Z}$ . Supponiamo che  $r = a \bmod m = b \bmod m = b$ . Allora

$$\begin{aligned} a - b &= cq + r - cq' - r' \\ &= c(q - q') \end{aligned}$$

cioè  $a \equiv b \pmod{m}$ .

Ora supponiamo che  $a \equiv b \pmod{m}$  e dimostriamo che i resti di  $a$  e  $b$  modulo  $m$  siano uguali. Per la proposizione 2.1.7 esistono  $q, r \in \mathbb{Z}$  tale che  $b = mq + r$  e  $0 \leq r < m$ . Allora per definizione di congruenza per qualche  $k \in \mathbb{Z}$  avremo

$$\begin{aligned} a &= b + mk \\ &= mq + r + mk \\ &= m(q + k) + r \end{aligned}$$

cioè  $r$  è il resto di  $a$  modulo  $m$ . □

**Proposizione 2.4.4.** *Siano  $a, b, a', b', m \in \mathbb{Z}$ ,  $m > 0$ . Allora valgono le seguenti*

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies a + a' \equiv b + b' \pmod{m} \quad (2.25)$$

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies a - a' \equiv b - b' \pmod{m} \quad (2.26)$$

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies aa' \equiv bb' \pmod{m} \quad (2.27)$$

*Dimostrazione.* 1. Per definizione di congruenza  $m \mid a - b$  e  $m \mid a' - b'$ . Per la proposizione 2.1.3 segue che  $m \mid (a - b) + (a' - b')$ , cioè  $m \mid (a + a') - (b + b')$ , che è equivalente a  $a + a' \equiv b + b' \pmod{m}$ .

2. Per definizione di congruenza  $m \mid a - b$  e  $m \mid a' - b'$ . Per la proposizione 2.1.3 segue che  $m \mid (a - b) - (a' - b')$ , cioè  $m \mid (a - a') - (b - b')$ , che è equivalente a  $a - a' \equiv b - b' \pmod{m}$ .

3. Per definizione di congruenza, scriviamo  $a - b = km$  e  $a' - b' = hm$ , che è equivalente a  $b = a - km$  e  $b' = a' - hm$ . Dunque

$$\begin{aligned} bb' &= (a - km)(a' - hm) \\ &= aa' - ahm - a'km + khm \\ &= aa' - (ah + a'k - kh)m \end{aligned}$$

che è equivalente a

$$\begin{aligned} aa' - bb' &= (ah + a'k - kh)m \\ \iff aa' &\equiv bb' \pmod{m}. \end{aligned}$$

□

**Proposizione 2.4.5.** *Siano  $a, b, c \in \mathbb{Z}$ ; sia  $ax + by = c$  un'equazione diofantea. Allora tutte le soluzioni della diofantea sono soluzioni delle equazioni  $ax \equiv c \pmod{b}$  e  $by \equiv c \pmod{a}$ .*

*Dimostrazione.* Dimostriamo entrambi i versi dell'implicazione.

1. Siano  $x, y \in \mathbb{Z}$  tali che  $ax + by = c$ . Dato che  $ax + by$  e' uguale a  $c$  segue che  $ax + by \equiv c \pmod{b}$ . Ma  $b \equiv 0 \pmod{b}$ , dunque  $x$  sara' anche soluzione di  $ax \equiv c \pmod{b}$ . Analogo ragionamento considerando  $ax + by \equiv c \pmod{a}$ .
2. Sia  $x \in \mathbb{Z}$  tale che  $ax \equiv c \pmod{b}$ . Allora per definizione di congruenza esiste  $k \in \mathbb{Z}$  per cui  $ax - c = bk$ . Sia  $y = -k$ ; l'equazione e' quindi equivalente a  $ax + by = c$ , cioe' la coppia  $(x, y)$  e' una soluzione dell'equazione diofantea. Analogo ragionamento se partiamo da  $by \equiv c \pmod{a}$ .

□

Tramite questa proposizione possiamo risolvere ogni equazione contenente congruenze risolvendo l'equazione diofantea associata, o viceversa.

#### 2.4.1 Risolvere singole congruenze

**Definizione 2.4.6.** Siano  $a \in \mathbb{Z}$ ; allora si dice che  $a$  e' invertibile modulo  $m$  se esiste  $x \in \mathbb{Z}$  tale che

$$ax \equiv 1 \pmod{m}.$$

In particolare tra tutti gli  $x$  che soddisfano la relazione precedente, il numero  $x$  tale che  $0 \leq x < m$  si dice inverso di  $a$  modulo  $m$ .

Per calcolare gli inversi modulo  $m$  basta fare una tabella  $m \times m$  in cui le righe e le colonne contengono i numeri tra 0 e  $m - 1$ , e nella casella  $ij$  c'e' il prodotto tra i numeri  $i$  e  $j$  modulo  $m$ .

Notiamo che non sempre i numeri diversi da 0 ammettono inverso modulo  $m$ .

**Teorema 2.4.7.** Siano  $a, m \in \mathbb{Z}$ . Allora  $a$  e' invertibile modulo  $m$  se e solo se  $\text{mcd}(a, m) = 1$ .

*Dimostrazione.* Supponiamo  $\text{mcd}(a, m) = 1$ . Allora per il teorema di Bezout 2.1.10  $\exists x, y \in \mathbb{Z}$  tali che

$$\begin{aligned} ax + my &= 1 \\ \iff ax - 1 &= m(-y) \\ \iff ax &\equiv 1 \pmod{m} \end{aligned}$$

dunque  $x$  e' l'inverso di  $a$  modulo  $m$ .

Supponiamo che  $a$  sia invertibile modulo  $m$ , cioe' che  $\exists x \in \mathbb{Z}$  tale che  $ax \equiv 1 \pmod{m}$ . Ma sappiamo che  $ax + my$  e' un multiplo di  $\text{mcd}(a, m)$ , quindi anche 1 dovra' essere un multiplo di  $\text{mcd}(a, m)$ , cioe'  $\text{mcd}(a, m) = 1$ , che e' la tesi. □

**Corollario 2.4.8.** Se  $p$  e' primo e  $a \not\equiv 0 \pmod{p}$ , allora  $a$  e' invertibile modulo  $p$ .

*Dimostrazione.* Se  $p$  e' primo, allora necessariamente  $p$  e' coprimo con tutti i numeri che non sono suoi multipli, cioe' con tutti gli  $a$  tali che  $a \not\equiv_p 0$ . Dunque se  $a \not\equiv_p 0$  allora  $\text{mcd}(a, p) = 1$ , cioe' per il teorema precedente  $a$  e' invertibile modulo  $p$ . □

**Proposizione 2.4.9.** Siano  $a, b, m \in \mathbb{Z}$ ; allora se  $a$  e' invertibile modulo  $m$  segue che  $\exists x \in \mathbb{Z}$  tale che  $ax \equiv b \pmod{m}$ .

*Dimostrazione.* Dato che  $a$  e' invertibile modulo  $m$  esistera'  $x' \in \mathbb{Z}$  tale che  $ax' \equiv 1 \pmod{m}$ . Moltiplicando entrambi i membri per  $b$  otteniamo  $ax'b \equiv b \pmod{m}$ , dunque la  $x \equiv x'b \pmod{m}$  soddisfa  $ax \equiv b \pmod{m}$ , cioe' la tesi.  $\square$

**Proposizione 2.4.10.** Siano  $a, b, m, x \in \mathbb{Z}$ ; allora l'equazione  $ax \equiv b \pmod{m}$  ha soluzione se e solo se  $\text{mcd}(a, m) \mid b$ .

*Dimostrazione.* Dimostriamo l'implicazione nei due versi.

- Supponiamo che  $ax \equiv b \pmod{m}$  ammetta soluzione. Allora esiste  $y \in \mathbb{Z}$  tale che  $ax - my = b$ . Dato che  $a$  e  $m$  sono multipli di  $\text{mcd}(a, m)$ , allora lo sara' anche la combinazione lineare  $ax - my$  che e' uguale a  $b$ , cioe'  $\text{mcd}(a, m) \mid b$ .
- Supponiamo che  $d = \text{mcd}(a, m)$  divida  $b$ . Allora  $d \mid a$ ,  $d \mid b$ ,  $d \mid m$ . Siano  $a' = \frac{a}{d}$ ,  $b' = \frac{b}{d}$ ,  $m' = \frac{m}{d}$ . Allora

$$\begin{aligned} ax &\equiv b \pmod{m} \\ \iff ax - b &= mk && \text{per qualche } k \in \mathbb{Z} \\ \iff a'dx - b'd &= m'dk && \text{per qualche } k \in \mathbb{Z} \\ \iff a'x - b' &= m'k && \text{per qualche } k \in \mathbb{Z} \\ \iff a'x &\equiv b' \pmod{m'}. \end{aligned}$$

Ma per il corollario 2.1.16  $\text{mcd}(a', m') = 1$ , dunque  $a'$  e' invertibile modulo  $m'$ , dunque per la proposizione 2.4.9 segue che  $a'x \equiv b' \pmod{m'}$  ha soluzione. Tuttavia  $a'x \equiv b' \pmod{m'}$  e' equivalente a  $ax \equiv b \pmod{m}$ , dunque anche  $ax \equiv b \pmod{m}$  ha soluzione e in particolare ha le stesse soluzioni di  $a'x \equiv b' \pmod{m'}$ .

$\square$

**Proposizione 2.4.11.** Se vogliamo semplificare una congruenza possiamo sfruttare le seguenti regole:

$$A \equiv B \pmod{m} \iff A + c \equiv B + c \pmod{m} \quad (2.28)$$

$$A \equiv B \pmod{m} \implies cA \equiv cB \pmod{m} \quad (2.29)$$

$$A \equiv B \pmod{m} \iff (A \bmod m) \equiv (B \bmod m) \pmod{m} \quad (2.30)$$

$$Ad \equiv Bd \pmod{m} \implies A \equiv B \pmod{m} \quad \text{se } \text{mcd}(d, m) = 1 \quad (2.31)$$

$$Ad \equiv Bd \pmod{md} \iff A \equiv B \pmod{m} \quad (2.32)$$

*Dimostrazione.* Dimostriamo le 5 proposizioni.

1. Dato che  $c \equiv c \pmod{m}$ , si tratta di un caso particolare della 2.25. Inoltre l'implicazione inversa si ricava dalla 2.26, dunque si tratta di un'equivalenza.
2. Dato che  $c \equiv c \pmod{m}$ , si tratta di un caso particolare della 2.27.
3. Dato che  $A \equiv (A \bmod m) \pmod{m}$  e  $B \equiv (B \bmod m) \pmod{m}$ , per transitivita' otteniamo che  $A \equiv B \pmod{m}$  e' equivalente a  $(A \bmod m) \equiv (B \bmod m) \pmod{m}$ .



4. Se  $\text{mcd}(d, m) = 1$  allora esiste l'inverso di  $d$  modulo  $m$ . Chiamiamo  $x$  questo inverso e moltiplichiamo entrambi i membri della congruenza per  $x$ , ottenendo

$$\begin{aligned} Ad &\equiv Bd \pmod{m} \\ \iff Adx &\equiv Bdx \pmod{m} \\ \iff A \cdot 1 &\equiv B \cdot 1 \pmod{m} \\ \iff A &\equiv B \pmod{m}. \end{aligned}$$

5. Per definizione di congruenza esiste  $y \in \mathbb{Z}$  tale che

$$\begin{aligned} Ad &= Bd + mdy \\ \iff A &= B + my \\ \iff A &\equiv B \pmod{m}. \end{aligned}$$

□

**Proposizione 2.4.12.** Siano  $a, b, m \in \mathbb{Z}$  noti,  $x \in \mathbb{Z}$  non noto. Allora per risolvere l'equazione  $ax \equiv b \pmod{m}$  possiamo ricondurci ad uno dei seguenti tre casi:

1. se  $\text{mcd}(a, m) = 1$ , allora l'equazione ha soluzione  $x \equiv by \pmod{m}$ , dove  $y$  e' l'inverso di  $a$  modulo  $m$ ;
2. se  $\text{mcd}(a, m) \neq 1$ ,  $d = \text{mcd}(a, m) \mid b$ , allora l'equazione e' equivalente all'equazione  $a'x \equiv b' \pmod{m'}$ , con  $a' = \frac{a}{d}$ ,  $b' = \frac{b}{d}$ ,  $m' = \frac{m}{d}$ , che ha soluzione;
3. se  $\text{mcd}(a, m) \neq 1$ ,  $\text{mcd}(a, m) \nmid b$ , allora l'equazione non ha soluzione.

*Dimostrazione.* I tre casi sono conseguenza diretta della proposizione 2.4.10. Infatti

1. Per la 2.4.10 l'equazione ha soluzione. Se  $y$  e' l'inverso di  $a$ , moltiplicando entrambi i membri per  $y$  otteniamo la soluzione  $x \equiv by \pmod{m}$ .
2. Per la 2.4.10 l'equazione ha soluzione. Sia  $d = \text{mcd}(a, m)$ . Allora la congruenza e' equivalente a  $ax - b = mk$  per qualche  $k \in \mathbb{Z}$ . Dato che  $a, b, m$  sono divisibili per  $d$ , dividendo per  $d$  otteniamo l'equazione equivalente

$$\begin{aligned} \frac{a}{d}x - \frac{b}{d} &= \frac{m}{d}k \\ \iff \frac{a}{d}x &\equiv \frac{b}{d} \pmod{\frac{m}{d}} \end{aligned}$$

Ma per il corollario 2.1.16  $\text{mcd}\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ , dunque possiamo trovare la soluzione sfruttando il primo caso.

3. Per la 2.4.10 l'equazione non ha soluzione.

□

### 2.4.2 Sistemi di congruenze

**Teorema 2.4.13** (Teorema Cinese del Resto). *Dato un sistema di congruenze in forma normale*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

*se i moduli  $m_1, m_2, \dots, m_n$  sono a due a due coprimi (cioe' se per ogni  $i \neq j$  vale che  $\text{mcd}(m_i, m_j) = 1$ ) allora il sistema ha soluzione, ed e' equivalente ad una singola congruenza del tipo*

$$x \equiv x_0 \pmod{m_1 m_2 \dots m_n}. \quad (2.33)$$

**Proposizione 2.4.14.** *Dato un sistema di congruenze*

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases}$$

*se  $x_0$  e' una soluzione particolare, allora tutte le soluzioni del sistema si ottengono sommando a  $x_0$  un multiplo di  $\text{mcm}(m_1, m_2, \dots, m_n)$ ; o equivalentemente la soluzione del sistema e' una singola congruenza della forma*

$$x \equiv x_0 \pmod{\text{mcm}(m_1, m_2, \dots, m_n)} \quad (2.34)$$