

Matematica Discreta

29 marzo 2020

Indice

1	Numeri interi	2
1.1	Insiemi numerici	2
2	Divisori e MCD	4
2.1	Divisori di un numero	4
2.1.1	Definizioni e prime conseguenze	4
2.1.2	Algoritmo di Euclide e Teorema di Bezout	5
2.1.3	Conseguenze del teorema di Bezout	6
2.2	Numeri primi	8
2.2.1	Divisori primi	9
2.3	Equazioni diofantee	12
3	Congruenze	14
3.1	Relazione di congruenza	14
3.2	Equazioni con congruenze lineari	15
3.3	Sistemi di congruenze	18
3.4	Struttura algebrica degli interi modulo m	19
3.5	Binomiale e Triangolo di Tartaglia	20

Capitolo 1

Numeri interi

1.1 Insiemi numerici

Definizione 1.1.1. Si dice **anello** un insieme di elementi A insieme con due operazioni $+: A \times A \rightarrow A$ e $\cdot: A \times A \rightarrow A$ e due elementi $0, 1 \in A$ per cui valgono i seguenti assiomi:

$$\forall a, b, c \in A$$

$$1. \quad (a + b) \in A \quad (\text{chiusura rispetto a } +) \quad (1.1)$$

$$2. \quad a + b = b + a \quad (\text{commutativita' di } +) \quad (1.2)$$

$$3. \quad (a + b) + c = a + (b + c) \quad (\text{associativita' di } +) \quad (1.3)$$

$$4. \quad a + 0 = 0 + a = a \quad (0 \text{ el. neutro di } +) \quad (1.4)$$

$$5. \quad \exists(-a) \in A. \quad a + (-a) = 0 \quad (\text{opposto per } +) \quad (1.5)$$

$$6. \quad (ab) \in A \quad (\text{chiusura rispetto a } \cdot) \quad (1.6)$$

$$7. \quad (ab)c = a(bc) \quad (\text{associativita' di } \cdot) \quad (1.7)$$

$$8. \quad a \cdot 1 = 1 \cdot a = a \quad (1 \text{ el. neutro di } \cdot) \quad (1.8)$$

$$9. \quad (a + b)c = ac + bc \quad (\text{distributivita' 1}) \quad (1.9)$$

$$10. \quad a(b + c) = ab + ac \quad (\text{distributivita' 2}) \quad (1.10)$$

Si dice **anello commutativo** un anello per cui vale inoltre il seguente assioma:

$$11. \quad ab = ba \quad (\text{commutativita' di } \cdot) \quad (1.11)$$

Un tipico esempio di anello commutativo e' \mathbb{Z} : infatti gli anelli generalizzano le operazioni che possiamo fare sui numeri interi e le loro proprieta' fondamentali per estenderle ad altri insiemi con la stessa struttura algebrica.

Definizione 1.1.2. Si dice **campo** un insieme di elementi F insieme con due operazioni $+: F \times F \rightarrow F$ e $\cdot: F \times F \rightarrow F$ e due elementi $0, 1 \in F$ per cui valgono i seguenti assiomi:

$$\forall a, b, c \in F$$

1. $(a + b) \in F$ (chiusura rispetto a $+$) (1.12)
2. $a + b = b + a$ (commutativita' di $+$) (1.13)
3. $(a + b) + c = a + (b + c)$ (associativita' di $+$) (1.14)
4. $a + 0 = 0 + a = a$ (0 el. neutro di $+$) (1.15)
5. $\exists(-a) \in F. \quad a + (-a) = 0$ (opposto per $+$) (1.16)
6. $(ab) \in F$ (chiusura rispetto a \cdot) (1.17)
7. $ab = ba$ (commutativita' di \cdot) (1.18)
8. $(ab)c = a(bc)$ (associativita' di \cdot) (1.19)
9. $a \cdot 1 = 1 \cdot a = a$ (1 el. neutro di \cdot) (1.20)
10. $(a + b)c = ac + bc$ (distributivita') (1.21)
11. se $a \neq 0$ allora $\exists a^{-1} \in F. \quad aa^{-1} = 1$ (inverso per \cdot) (1.22)

La definizione sopra e' equivalente a dire che F e' un anello commutativo per cui ogni elemento non nullo ha un inverso moltiplicativo.

Tra gli insiemi numerici classici, gli insiemi \mathbb{Q}, \mathbb{R} e \mathbb{C} sono tutti esempi di campi: infatti le operazioni di addizione e moltiplicazione sono chiuse rispetto all'insieme, rispettano le proprieta' commutativa, associativa e distributiva ed esistono gli inversi per la somma e per il prodotto (per ogni numero diverso da 0). Il concetto di campo serve quindi a generalizzare la struttura algebrica dei numeri razionali/reali/complessi per altri 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 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 ± 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 $nax + nbh$, 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 (Esistenza della scomposizione in primi). *Sia $n \in \mathbb{Z}, n > 1$. Allora n può essere espresso come prodotto di potenze di numeri primi.*

Dimostrazione. Per induzione forte su n .

- **Caso base.**

Sia $n = 2$. Dato che 2 è primo, allora è esprimibile come prodotto di numeri primi (in particolare è il prodotto di un solo termine, se stesso).

- **Passo induttivo.**

Supponiamo che la tesi sia vera per $2, 3, \dots, n - 1$ (induzione forte) e dimostriamola per n . Abbiamo due casi:

- se n è primo, allora è un prodotto di primi e quindi la tesi vale;
- se n non è primo allora dovranno esistere due numeri $1 < a, b < n$ tali che $n = ab$ (infatti se non esistessero n sarebbe primo). Ma per l'ipotesi induttiva forte sappiamo che tutti i numeri compresi tra 2 e $n - 1$ inclusi sono scomponibili in fattori primi, dunque anche $n = ab$ dovrà esserlo.

Dunque dal caso base e dal passo induttivo segue che la tesi vale per ogni $n \geq 2$. \square

Teorema 2.2.8 (Teorema fondamentale dell'aritmetica). *Sia $n \in \mathbb{Z}$ e siano p_1, p_2, \dots, p_k i primi che dividono n . Inoltre siano e_1, e_2, \dots, e_k i massimi esponenti per cui vale che $p_i^{e_i} \mid n$ per ogni $1 \leq i \leq k$. Allora $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.*

Dimostrazione. Per la proposizione 2.2.7 sappiamo che esistono p_1, \dots, p_n . Per la proposizione 2.2.5 segue che

$$p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \mid n$$

in quanto $p_1^{e_1}, p_2^{e_2}, \dots, p_k^{e_k}$ sono coprimi tra loro.

Dunque $n = m \cdot p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ per qualche $m \in \mathbb{Z}$. Supponiamo per assurdo che $m \neq 1$. Allora per la proposizione 2.2.7 m e' scomponibile in numeri primi; ma dato che m e' un divisore di n segue che i primi che dividono m devono dividere anche n , dunque i primi che dividono m devono essere tra p_1, \dots, p_k .

Supponiamo senza perdita di generalita' che p_i divida m . Allora dato che $m \cdot p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = n$ deve essere $p_i \cdot p_i^{e_i} = p_i^{e_i+1} \mid n$, che e' assurdo in quanto abbiamo supposto che e_i fosse il massimo esponente per cui $p_i^{e_i} \mid n$.

Dunque deve essere $m = 1$, cioe'

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

come volevasi dimostrare. \square

Proposizione 2.2.9. *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 e' un divisore comune ad entrambi, quindi se p^k lo divide deve dividere entrambi i numeri.

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

Proposizione 2.2.10. *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 minimo comune multiplo sara' formato precisamente da tutti i fattori di entrambi i numeri, cioe' 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 $ab \mid \text{mcm}(a, b)$, cioe' $|ab| \leq \text{mcm}(a, b)$. Ma ab e' un multiplo di a e di b , quindi dovra' valere che $|ab| \geq \text{mcm}(a, b)$ in quanto $\text{mcm}(a, b)$ e' il minimo multiplo comune ad a e b . Da cio' segue che $\text{mcm}(a, b) = |ab|$, cioe' la tesi. \square

Proposizione 2.2.11. *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 e' 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 2.2.9 allora vale

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

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

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

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 2.2.12. 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 2.2.9 allora vale

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

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 2.2.13. 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 2.2.10 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 2.2.12.

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 2.2.10 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. \square

Proposizione 2.2.14. 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 transitività $d \mid c$, 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 $\frac{ab}{d^2}$ dovrà dividere $\frac{c}{d}$, che è equivalente a dire che $\frac{ab}{d} \mid c$.
- NON SO FARE QUEST'ALTRA DIMOSTRAZIONE

□

Proposizione 2.2.15. 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 2.2.14 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. □

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 $x = -kb, y = ka$ e' 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 $a \mid y$, cioe' $y = ak$ per qualche $k \in \mathbb{Z}$. Sostituendo ottengo $x = -b\frac{y}{a} = -bk$, che e' 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 e' 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. \square

Capitolo 3

Congruenze

3.1 Relazione di congruenza

Definizione 3.1.1. Siano $a, b, m \in \mathbb{Z}$, $m > 0$. Allora si dice che a è congruo a b modulo m se e solo se $a - b$ è un multiplo di m , e si scrive

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

Teorema 3.1.2. Siano $a, b, m \in \mathbb{Z}$, $m > 0$. Allora la relazione di congruenza $\equiv \pmod{m}$ è una relazione di equivalenza, e dunque soddisfa le proprietà:

$$\text{Riflessiva:} \quad a \equiv a \pmod{m} \quad (3.1)$$

$$\text{Simmetrica:} \quad a \equiv b \pmod{m} \implies b \equiv a \pmod{m} \quad (3.2)$$

$$\text{Riflessiva:} \quad a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m} \quad (3.3)$$

Dimostrazione. Dimostriamo le tre proprietà della congruenza come relazione di equivalenza.

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

□

Teorema 3.1.3. Siano $a, b, m \in \mathbb{Z}$, $m > 0$. Allora

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m \quad (3.4)$$

cioè a è 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 $r = a \bmod m = b \bmod m = r'$. Allora

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

cioe' $a \equiv b \pmod{m}$.

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

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

cioe' r e' il resto di a modulo m . □

Proposizione 3.1.4. *Siano $a, b, a', b', m \in \mathbb{Z}$, $m > 0$. Allora valgono le seguenti*

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies a + a' \equiv b + b' \pmod{m} \quad (3.5)$$

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies a - a' \equiv b - b' \pmod{m} \quad (3.6)$$

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies aa' \equiv bb' \pmod{m} \quad (3.7)$$

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

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

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

□

3.2 Equazioni con congruenze lineari

Proposizione 3.2.1. *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 è quindi equivalente a $ax + by = c$, cioè la coppia (x, y) è una soluzione dell'equazione diofantea. Analogamente se partiamo da $by \equiv c \pmod{a}$.

□

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

Definizione 3.2.2. Siano $a \in \mathbb{Z}$; allora si dice che a è 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'è il prodotto tra i numeri i e j modulo m .

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

Teorema 3.2.3. Siano $a, m \in \mathbb{Z}$. Allora a è 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 è l'inverso di a modulo m .

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

Corollario 3.2.4. Se p è primo e $a \not\equiv 0 \pmod{p}$, allora a è invertibile modulo p .

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

Proposizione 3.2.5. Siano $a, b, m \in \mathbb{Z}$; allora se a è invertibile modulo m segue che $\exists x \in \mathbb{Z}$ tale che $ax \equiv b \pmod{m}$.

Dimostrazione. Dato che a è invertibile modulo m esisterà $x' \in \mathbb{Z}$ 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 $ax \equiv b \pmod{m}$, cioè la tesi. □

Proposizione 3.2.6. 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 sarà anche la combinazione lineare $ax - my$ che è uguale a b , cioè $\text{mcd}(a, m) \mid b$.
- 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' è invertibile modulo m' , dunque per la proposizione 3.2.5 segue che $a'x \equiv b' \pmod{m'}$ ha soluzione. Tuttavia $a'x \equiv b' \pmod{m'}$ è equivalente a $ax \equiv b \pmod{m}$, dunque anche $ax \equiv b \pmod{m}$ ha soluzione e in particolare ha le stesse soluzioni di $a'x \equiv b' \pmod{m'}$.

□

Proposizione 3.2.7. *Se vogliamo semplificare una congruenza possiamo sfruttare le seguenti regole:*

$$A \equiv B \pmod{m} \iff A + c \equiv B + c \pmod{m} \quad (3.8)$$

$$A \equiv B \pmod{m} \implies cA \equiv cB \pmod{m} \quad (3.9)$$

$$A \equiv B \pmod{m} \iff (A \bmod m) \equiv (B \bmod m) \pmod{m} \quad (3.10)$$

$$Ad \equiv Bd \pmod{m} \implies A \equiv B \pmod{m} \quad \text{se } \text{mcd}(d, m) = 1 \quad (3.11)$$

$$Ad \equiv Bd \pmod{md} \iff A \equiv B \pmod{m} \quad (3.12)$$

Dimostrazione. Dimostriamo le 5 proposizioni.

1. Dato che $c \equiv c \pmod{m}$, si tratta di un caso particolare della 3.5. Inoltre l'implicazione inversa si ricava dalla 3.6, dunque si tratta di un'equivalenza.
2. Dato che $c \equiv c \pmod{m}$, si tratta di un caso particolare della 3.7.
3. Dato che $A \equiv (A \bmod m) \pmod{m}$ e $B \equiv (B \bmod m) \pmod{m}$, per transitività otteniamo che $A \equiv B \pmod{m}$ è 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 3.2.8. *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 3.2.6. Infatti

1. Per la 3.2.6 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 3.2.6 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 $\text{mcd}(\frac{a}{d}, \frac{m}{d}) = 1$, dunque possiamo trovare la soluzione sfruttando il primo caso.

3. Per la 3.2.6 l'equazione non ha soluzione.

□

3.3 Sistemi di congruenze

Teorema 3.3.1 (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

$$x \equiv x_0 \pmod{m_1 m_2 \dots m_n}. \quad (3.13)$$

Proposizione 3.3.2. 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

$$x \equiv x_0 \pmod{\text{mcm}(m_1, m_2, \dots, m_n)} \quad (3.14)$$

3.4 Struttura algebrica degli interi modulo m

Definizione 3.4.1. Siano $a, n \in \mathbb{Z}$; allora si dice classe di resto $[a]_n$ l'insieme

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}. \quad (3.15)$$

Il numero a si dice rappresentante della classe $[a]_n$.

Due classi di resto si dicono uguali se contengono gli stessi elementi. Il rappresentante di una classe non e' unico, anzi per ogni classe ci sono infinite scelte che corrispondono a tutti i numeri appartenenti alla classe. Vale quindi la seguente osservazione:

Osservazione. $a \equiv b \pmod{n} \iff [a]_n = [b]_n$.

Notiamo che per ogni numero n ci sono esattamente n classi di resto modulo n : infatti ce n'e' una esattamente per ogni possibile resto della divisione per n , cioe' per ogni numero tra 0 e $n - 1$ inclusi.

Definizione 3.4.2. Si dice insieme degli interi modulo n l'insieme

$$\mathbb{Z}/(n) = \{[0]_n, [1]_n, \dots, [n-1]_n\}. \quad (3.16)$$

Possiamo definire due operazioni in $\mathbb{Z}/(n)$ che sono le operazioni di somma (+) e prodotto (\cdot) tali che:

$$[a]_n + [b]_n = [a + b]_n \quad \forall [a]_n, [b]_n \in \mathbb{Z}/(n) \quad (3.17)$$

$$[a]_n \cdot [b]_n = [ab]_n \quad \forall [a]_n, [b]_n \in \mathbb{Z}/(n) \quad (3.18)$$

Proposizione 3.4.3. Per ogni $n \geq 2$ l'insieme $\mathbb{Z}/(n)$ e' un anello.

3.5 Binomiale e Triangolo di Tartaglia

Definizione 3.5.1. Si dice **coefficiente binomiale** $\binom{n}{k}$ il numero intero definito come

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (3.19)$$

Teorema 3.5.2 (del binomiale). *Siano $x, y, n \in \mathbb{Z}$. Allora vale che*

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \dots + \binom{n}{n}x^ny^0 = \sum_{k=0}^n \binom{n}{k}x^{n-k}y^k \quad (3.20)$$

Proposizione 3.5.3. *Se p e' primo, allora per ogni k tale che $0 < k < p$ vale che*

$$\binom{p}{k} \equiv 0 \pmod{p} \quad (3.21)$$

Dimostrazione. Consideriamo un k generico tale che $0 < k < p$. Allora

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \iff p! = \binom{p}{k}(p-k)!k!$$

Ma $p \mid p!$, dunque $p \mid \binom{p}{k}(p-k)!k!$, dunque per la proposizione 2.2.2 segue che

$$p \mid \binom{p}{k} \text{ oppure } p \mid (p-k)! \text{ oppure } p \mid k!.$$

Notiamo che sia k che $p-k$ sono numeri minori di p , dunque $k!$ e $(p-k)!$ sono un prodotto di numeri minori di p . Ma p e' primo, dunque e' coprimo con tutti i numeri che non siano un multiplo di p (e quindi e' coprimo con tutti i numeri compresi tra 0 e p esclusi), dunque per la proposizione 2.2.5 p deve essere coprimo anche con $k!$ e con $(p-k)!$.

Da cio' segue che p non puo' dividere $k!$ e $(p-k)!$. L'ultima possibilita' e' che $p \mid \binom{p}{k}$, che e' equivalente a dire che $\binom{p}{k} \equiv 0 \pmod{p}$. \square

Proposizione 3.5.4. *Siano $x, y, p \in \mathbb{Z}$, p primo. Allora*

$$(x+y)^p \equiv x^p + y^p \pmod{p} \quad (3.22)$$

Dimostrazione. Per il teorema del Binomiale (3.5.2) sappiamo che

$$(x+y)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y^1 + \dots + \binom{p}{i}x^{p-i}y^i + \dots + \binom{p}{p}y^p$$

Ma per la proposizione 3.5.3 tutti i termini intermedi di questa somma sono congrui a 0 modulo p , dunque:

$$\begin{aligned} &\equiv \binom{p}{0}x^p + \binom{p}{p}y^p \pmod{p} \\ &\equiv x^p + y^p \pmod{p} \end{aligned}$$

come volevasi dimostrare. \square

Corollario 3.5.5. *Siano $x_1, x_2, \dots, x_n, p \in \mathbb{Z}$, p primo. Allora*

$$(x_1 + x_2 + \dots + x_n)^p \equiv x_1^p + x_2^p + \dots + x_n^p \pmod{p} \quad (3.23)$$

Dimostrazione. Per induzione su n .

- **Caso base.**

Sia $n = 1$. Allora $x_1^p \equiv x_1^p \pmod{p}$ ovviamente.

- **Passo induttivo.**

Supponiamo che la tesi sia vera per $n - 1$ e dimostriamola per n .

$$(x_1 + x_2 + \dots + x_n)^p \equiv ((x_1 + x_2 + \dots + x_{n-1}) + x_n)^p \pmod{p}$$

(per la proposizione 3.5.4)

$$\equiv (x_1 + x_2 + \dots + x_{n-1})^p + x_n^p \pmod{p}$$

(per ipotesi induttiva)

$$\equiv x_1^p + x_2^p + \dots + x_{n-1}^p + x_n^p \pmod{p}$$

che e' la tesi per n .

Dunque dal caso base e dal passo induttivo segue che la tesi vale per ogni n . \square

Teorema 3.5.6 (Piccolo Teorema di Fermat). *Se p e' primo, allora $x^p \equiv x \pmod{p}$.*

Dimostrazione.

$$x^p \equiv \overbrace{(1 + \dots + 1)}^{x \text{ volte}}^p \pmod{p}$$

(per il corollario 3.5.5)

$$\equiv \overbrace{1^p + \dots + 1^p}^{x \text{ volte}} \pmod{p}$$

$$\equiv \overbrace{1 + \dots + 1}^{x \text{ volte}} \pmod{p}$$

$$\equiv x \pmod{p}$$

che e' la tesi. \square