Matematica Discreta

5 aprile 2020

Indice

Capitolo 1

Numeri interi

1.1 Insiemi numerici

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

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

1.	$(a + b) \in A$	(chiusura rispetto a $+$)	(1.1)
2.	$a + b = b + a$	(commutativita' di $+$)	(1.2)
3.	$(a + b) + c = a + (b + c)$	(associativita' di $+$)	(1.3)
4.	$a + 0 = 0 + a = a$	(0 el. neutro di $+$)	(1.4)
5.	$\exists(-a) \in A. \quad a + (-a) = 0$	(opposto per $+$)	(1.5)
6.	$(ab) \in A$	(chiusura rispetto a $\cdot$)	(1.6)
7.	$(ab)c = a(bc)$	(associativita' di $\cdot$)	(1.7)
8.	$a \cdot 1 = 1 \cdot a = a$	(1 el. neutro di $\cdot$)	(1.8)
9.	$(a + b)c = ac + bc$	(distributivita' 1)	(1.9)
10.	$a(b + c) = ab + ac$	(distributivita' 2)	(1.10)

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

11.	$ab = ba$	(commutativita' di $\cdot$)	(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 $+ : F \times F \to F$ e $\cdot : F \times F \to F$ 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*

$$n \mid a + b \tag{2.1}$$

$$n \mid a - b \tag{2.2}$$

$$n \mid ax \qquad \forall x \in \mathbb{Z} \tag{2.3}$$

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:

$$\begin{aligned} a + b = nh + nk = n(h + k) &\iff n \mid a + b \\ a - b = nh - nk = n(h - k) &\iff n \mid a - b \\ ax = nhx = n(hx) &\iff n \mid ax \end{aligned}$$

che e' la tesi. □

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

Definizione 2.1.5. Siano $a, b \in \mathbb{Z}$. Allora si dice minimo comune multiplo di a e b il numero $d = \operatorname{mcm}(a, b)$ 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 $\operatorname{mcd}(a, b) = 1$ allora a e b si dicono coprimi.

Osservazione. Siano $a, b \in \mathbb{Z}$. Allora valgono le seguenti proprieta' per $\operatorname{mcd}(a, b)$:

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

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

$$a = bq + r, \qquad 0 \leq r < |b| \tag{2.4}$$

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 e' l'unico elemento di questa progressione compreso tra 0 e $b - 1$. □

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

$$\operatorname{mcm}(a, b) \mid c \iff a \mid c \wedge b \mid c \tag{2.5}$$

Dimostrazione. Dimostriamo separatamente i due versi dell'implicazione.

Dato che $\operatorname{mcm}(a, b)$ e' un multiplo di a e di b e per ipotesi c e' un multiplo di $\operatorname{mcm}(a, b)$, allora per transitivita' segue che c e' 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

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

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

2.1.2 Algoritmo di Euclide e Teorema di Bezout

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

$$\operatorname{mcd}(a, b) = \operatorname{mcd}(a, b - a) = \operatorname{mcd}(a - b, b)\,. \tag{2.6}$$

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

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

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

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

Allora per dimostrare la tesi e' 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 $d \in \mathbb{D}_{a,b}$, cioe' $d \mid a$ e $d \mid b$. Allora per la proposizione 2.1.3 segue che $d \mid b-a$, cioe' $d \in \mathbb{D}_{a,b-a}$, cioe' $\mathbb{D}_{a,b} \subseteq \mathbb{D}_{a,b-a}$.

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

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 dovra' essere lo stesso, quindi $\operatorname{mcd}(a,b) = \operatorname{mcd}(a,b-a)$, che e' la tesi. $\square$

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

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

   dove i valori di $\operatorname{mcd}(a-b,b)$ o $\operatorname{mcd}(a,b-a)$ 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*

$$ax + by = \operatorname{mcd}(a,b) \tag{2.7}$$

2.1.3 Conseguenze del teorema di Bezout

Elenchiamo in questa sezione alcune conseguenze del teorema di Bezout sulle proprieta' 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*

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

Intuizione. Se n divide ab, allora tutti i fattori primi che dividono n dovranno essere contenuti in ab. Dato che $\operatorname{mcd}(n,a) = 1$, 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

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

Moltiplicando per b otteniamo

$$abx + nby = b$$

Ma $n \mid abx$ (poiche $n \mid ab$) e $n \mid nby$, dunque $n \mid abx + nby$, cioe' $n \mid b$. $\square$

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

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' $t \leq \operatorname{mcd}(a, b)$. $\square$

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

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 $a\bar{x} + b\bar{y} = \operatorname{mcd}(a, b)$. 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' $t \mid \operatorname{mcd}(a, b)$. $\square$

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

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

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

- Se $t \mid \operatorname{mcd}(a, b)$, 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 $a\bar{x} + b\bar{y} = \operatorname{mcd}(a, b)$. Allora t dovra' dividere anche $a\bar{x} + b\bar{y}$, cioe' $t \mid \operatorname{mcd}(a, b)$.

$\square$

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

$$\operatorname{mcd}(an, bn) = n \operatorname{mcd}(a, b) \tag{2.10}$$

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

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

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

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

$\square$

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

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

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

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

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

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

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

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, $\operatorname{mcd}(a,p) = 1$ oppure p. Tuttavia se $\operatorname{mcd}(a,p) = p$ allora $p \mid a$, che va contro l'ipotesi, dunque $\operatorname{mcd}(a,p) = 1$. 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* $\operatorname{mcd}(a,b) = 1$. *Allora*

$$a \mid c \wedge b \mid c \iff ab \mid c \tag{2.11}$$

Dimostrazione. Per il teorema di Bezout (2.1.10) esistono $x, y \in \mathbb{Z}$ tali che $\operatorname{mcd}(a,b) = 1 = ax + by$, 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*

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

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

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

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

Dimostrazione. Dimostriamo la proposizione per induzione su n.

Caso base. Sia $n = 0$, cioe' $a_1 \ldots a_n = 1$. 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 e' 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 e' la tesi per n.

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

2.2.1 Divisori primi

Proposizione 2.2.7 (Esistenza della scomposizione in primi)**.** *Sia* $n \in \mathbb{Z}, n > 1$. *Allora* n *puo' essere espresso come prodotto di potenze di numeri primi.*

Dimostrazione. Per induzione forte su n.

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

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

- se n e' primo, allora e' un prodotto di primi e quindi la tesi vale;
- se n non e' 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 $n = ab$ dovra' esserlo.

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

Teorema 2.2.8 (Teorema fondamentale dell'aritmetica). *Sia $n \in Z$ 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. □

Proposizione 2.2.9. *Siano $a, b, k \in \mathbb{Z}$, $p \in \mathbb{Z}$ primo. Allora*

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

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

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* $\operatorname{mcd}(a, b) = 1$ *segue che* $\operatorname{mcm}(a, b) = |ab|$.

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 $a \mid \operatorname{mcm}(a, b)$ e $b \mid \operatorname{mcm}(a, b)$. Dato che $\operatorname{mcd}(a, b) = 1$ per la proposizione 2.2.3 segue che $ab \mid \operatorname{mcm}(a, b)$, cioe' $|ab| \leq \operatorname{mcm}(a, b)$. Ma ab e' un multiplo di a e di b, quindi dovra' valere che $|ab| \geq \operatorname{mcm}(a, b)$ in quanto $\operatorname{mcm}(a, b)$ e' il minimo multiplo comune ad a e b. Da cio' segue che $\operatorname{mcm}(a, b) = |ab|$, cioe' la tesi. □

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

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

Intuizione. Se stiamo calcolando $\operatorname{mcd}(a, b)$ 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

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

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. □

Proposizione 2.2.12. *Siano $a, x, y \in \mathbb{Z}$. Allora*

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

Dimostrazione. Per la proposizione 2.2.9 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. □

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

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

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. □

Proposizione 2.2.14. *Siano $a, b, c \in \mathbb{Z}$. Allora*

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

Dimostrazione. Dimostriamo l'implicazione in entrambi i versi.

- Supponiamo che $a \mid c$ e $b \mid c$. Sia $d = \operatorname{mcd}(a, b)$. 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 $\operatorname{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, 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 2.2.15. *Siano $a, b \in \mathbb{Z}$. Allora*

$$\operatorname{mcd}(a, b) \operatorname{mcm}(a, b) = |ab| \tag{2.20}$$

Dimostrazione. Sia $c \in \mathbb{Z}$ tale che $a \mid c$, $b \mid c$. Allora per la proposizione 2.2.14 segue che $\frac{ab}{\operatorname{mcd}(a,b)} \mid c$. Inoltre per la proposizione 2.1.8 segue che $\operatorname{mcm}(a, b) \mid c$. Dunque i due numeri $\frac{ab}{\operatorname{mcd}(a,b)}$ e $\operatorname{mcm}(a, b)$ hanno gli stessi divisori, dunque devono essere uguali a meno del segno, da cui segue

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

□

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 $\operatorname{mcd}(a, b) \mid c$.*

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

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

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

Supponiamo ora che c non sia un multiplo di $\operatorname{mcd}(a, b)$ e supponiamo per assurdo che l'equazione abbia soluzione, cioe' che esistano $x, y \in \mathbb{Z}$ tali che $ax+by = c$. Sia $d = \operatorname{mcd}(a, b)$. Per definizione di $\operatorname{mcd}(a, b)$ 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 $d = \operatorname{mcd}(a, b) \mid c$, che va contro le ipotesi. Dunque l'equazione diofantea non ha soluzione, cioe' 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 $\operatorname{mcd}(a, -b) = \operatorname{mcd}(a, b) = 1$. 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 $a' = \frac{a}{\operatorname{mcd}(a,b)}$ e $b' = \frac{b'}{\operatorname{mcd}(a,b)}$.*

Dimostrazione. Dato che a, b non sono coprimi, allora possiamo dividere entrambi i membri di $ax+by = 0$ per $\operatorname{mcd}(a, b)$ ottenendo l'equazione diofantea equivalente $a'x + b'y = 0$. Ma per il teorema 2.1.16 $\operatorname{mcd}(a', b') = 1$, 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 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 3.1.2. *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':*

Riflessiva:	$a \equiv a \ (m)$	(3.1)
Simmetrica:	$a \equiv b \ (m) \implies b \equiv a \ (m)$	(3.2)
Riflessiva:	$a \equiv b \ (m) \land b \equiv c \ (m) \implies a \equiv c \ (m)$	(3.3)

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

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

$\square$

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

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

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, cioe' $a = cq + r$ e $b = cq' + r'$ per qualche $q, q' \in \mathbb{Z}$. Supponiamo che $r = a \bmod m = b \bmod m = b$. Allora

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

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*

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies a + a' \equiv b + b' \pmod{m} \tag{3.5}$$

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies a - a' \equiv b - b' \pmod{m} \tag{3.6}$$

$$a \equiv b \pmod{m} \wedge a' \equiv b' \pmod{m} \implies aa' \equiv bb' \pmod{m} \tag{3.7}$$

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 $x \in Z$ tale che $ax \equiv c \ (b)$. 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 $by \equiv c \ (a)$.

□

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 e' invertibile modulo m se esiste $x \in \mathbb{Z}$ tale che

$$ax \equiv 1 \ (m) .$$

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

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

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

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 $ax \equiv= 1 \ (m)$. Ma sappiamo che $ax + my$ e' un multiplo di $\operatorname{mcd}(a, m)$, quindi anche 1 dovra' essere un multiplo di $\operatorname{mcd}(a, m)$, cioe' $\operatorname{mcd}(a, m) = 1$, che e' la tesi. □

Corollario 3.2.4. *Se p e' primo e $a \not\equiv 0 \ (p)$, 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 $a \equiv_p 0$. Dunque se $a \equiv_p 0$ allora $\operatorname{mcd}(a, p) = 1$, cioe' per il teorema precedente a e' invertibile modulo p. □

Proposizione 3.2.5. *Siano $a, b, m \in \mathbb{Z}$; allora se a e' invertibile modulo m segue che $\exists x \in \mathbb{Z}$ tale che $ax \equiv b \ (m)$.*

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

Proposizione 3.2.6. *Siano $a, b, m, x \in \mathbb{Z}$; allora l'equazione $ax \equiv b \ (m)$ ha soluzione se e solo se* $\operatorname{mcd}(a, m) \mid b$.

Dimostrazione. Dimostriamo l'implicazione nei due versi.

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

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

  Ma per il corollario 2.1.16 $\operatorname{mcd}(a', m') = 1$, dunque a' e' invertibile modulo m', dunque per la proposizione 3.2.5 segue che $a'x \equiv b' \ (m')$ ha soluzione. Tuttavia $a'x \equiv b' \ (m')$ e' equivalente a $ax \equiv b \ (m)$, dunque anche $ax \equiv b \ (m)$ ha soluzione e in particolare ha le stesse soluzioni di $a'x \equiv b' \ (m')$.

□

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

$$
\begin{aligned}
A \equiv B \ (m) \quad & \iff \quad A + c \equiv B + c \ (m) && (3.8) \\
A \equiv B \ (m) \quad & \implies \quad cA \equiv cB \ (m) && (3.9) \\
A \equiv B \ (m) \quad & \iff \quad (A \bmod m) \equiv (B \bmod m) \ (m) && (3.10) \\
Ad \equiv Bd \ (m) \quad & \implies \quad A \equiv B \ (m) \qquad \textit{se } \operatorname{mcd}(d, m) = 1 && (3.11) \\
Ad \equiv Bd \ (md) \quad & \iff \quad A \equiv B \ (m) && (3.12)
\end{aligned}
$$

Dimostrazione. Dimostriamo le 5 proposizioni.

1. Dato che $c \equiv c \ (m)$, 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 $c \equiv c \ (m)$, si tratta di un caso particolare della 3.7.
3. Dato che $A \equiv (A \bmod m) \ (m)$ e $B \equiv (B \bmod m) \ (m)$, per transitivita' otteniamo che $A \equiv B \ (m)$ e' equivalente a $(A \bmod m) \equiv (B \bmod m) \ (m)$.
4. Se $\operatorname{mcd}(d, m) = 1$ allora esiste l'inverso di d modulo m. Chiamiamo x questo inverso e moltiplichiamo entrambi i membri della congruenza per x, ottenendo

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

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

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

□

Proposizione 3.2.8. *Siano* $a, b, m \in \mathbb{Z}$ *noti,* $x \in \mathbb{Z}$ *non noto. Allora per risolvere l'equazione* $ax \equiv b \ \ (m)$ *possiamo ricondurci ad uno dei seguenti tre casi:*

1. *se* $\operatorname{mcd}(a, m) = 1$*, allora l'equazione ha soluzione* $x \equiv by \ \ (m)$*, dove* y *e' l'inverso di* a *modulo* m*;*

2. *se* $\operatorname{mcd}(a, m) \neq 1$*,* $d = \operatorname{mcd}(a, m) \mid b$*, allora l'equazione e' equivalente all'equazione* $a'x \equiv b' \ \ (m')$*, con* $a' = \frac{a}{d}$*,* $b' = \frac{b}{d}$*,* $m' = \frac{m}{d}$*, che ha soluzione;*

3. *se* $\operatorname{mcd}(a, m) \neq 1$*,* $\operatorname{mcd}(a, m) \nmid b$*, 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 $x \equiv by \ \ (m)$.

2. Per la 3.2.6 l'equazione ha soluzione. Sia $d = \operatorname{mcd}(a, m)$. 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

$$\begin{aligned} \frac{a}{d}x - \frac{b}{d} &= \frac{m}{d}k \\ \iff \frac{a}{d}x &\equiv \frac{b}{d} \ \ \left(\frac{m}{d}\right) \end{aligned}$$

   Ma per il corollario 2.1.16 $\operatorname{mcd}\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, 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*

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

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 $\operatorname{mcd}(m_i, m_j) = 1$*) allora il sistema ha soluzione, ed e' equivalente ad una singola congruenza del tipo*

$$x \equiv x_0 \pmod{m_1 m_2 \dots m_n}. \tag{3.13}$$

Proposizione 3.3.2. *Dato un sistema di congruenze*

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

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

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

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

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

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. $a \equiv b \ (m) \iff [a]_n = [b]_n$.

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

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

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

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

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

Osservazione. Le operazioni di somma e prodotto sono ben definite: il loro risultato non cambia a seconda dei rappresentanti scelti per le classi di congruenza.

Proposizione 3.4.3. *Per ogni $n \geq 2$ l'insieme $\mathbb{Z}/(n)$ con le operazioni di somma e prodotto tra classi e con gli elementi $[0]_n, [1]_n$ che svolgono il ruolo di 0 e 1 e' un anello commutativo.*

Dimostrazione. E' facile verificare che valgono gli assiomi degli anelli. □

Proposizione 3.4.4. *Per ogni $p \geq 2$, p primo, l'insieme $\mathbb{Z}/(p)$ con le operazioni di somma e prodotto tra classi e con gli elementi $[0]_n, [1]_n$ che svolgono il ruolo di 0 e 1 e' un campo.*

Dimostrazione. Per la proposizione 3.4.3 sappiamo che $\mathbb{Z}/(p)$ e' un anello commutativo. Per la proposizione 3.2.3 un numero e' invertibile modulo p se e solo se e' coprimo con pm; ma tutti i numeri che non sono multipli di p sono coprimi con p, dunque tutte le classi tranne $[0]_p$ sono invertibili, dunque esiste l'inverso per la moltiplicazione per ogni elemento non nullo, cioe' $\mathbb{Z}/(p)$ e' un campo. □

3.5 Binomiale e Triangolo di Tartaglia

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

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

Proposizione 3.5.2. *Sia $n \in \mathbb{Z}$, $k \in \mathbb{Z}$ tale che $0 \leq k \leq n$. Allora*

$$\binom{n}{k} = \binom{n}{n-k} \tag{3.20}$$

Dimostrazione.

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

Proposizione 3.5.3. *Sia $n \in \mathbb{Z}$, $k \in \mathbb{Z}$ tale che $0 \leq k \leq n$. Allora*

$$\binom{n}{k} = \begin{cases} 1 & \textit{se } k = 0 \textit{ oppure } k = n \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \textit{altrimenti.} \end{cases} \tag{3.21}$$

Dimostrazione. Se $k = 0$ allora

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{n!} = 1.$$

Inoltre per la proposizione 3.5.2 segue che

$$\binom{n}{n} = \binom{n}{n-n} = \binom{n}{0} = 1.$$

Se $0 < k < n$ allora

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{(k)!(n-1-k)!}$$

$$= \frac{(n-1)!}{(k-1)!(n-1-k)!(n-k)} + \frac{(n-1)!}{k(k-1)!(n-1-k)!}$$

$$= \frac{(n-1)!k + (n-k)(n-1)!}{k(k-1)!(n-1-k)!(n-k)}$$

$$= \frac{(n-1)!k + n(n-1)! - k(n-1)!}{k!(n-k)!}$$

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

$$= \binom{n}{k}$$

che e' la tesi. □

Teorema 3.5.4 (del binomiale)**.** *Siano $x, y, n \in \mathbb{Z}$. Allora vale che*

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \cdots + \binom{n}{n}x^ny^0 = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \quad (3.22)$$

Definizione 3.5.5. Si dice triangolo di Tartaglia un triangolo che ha le seguenti proprieta':

1. le righe sono numerate a partire da 0;
2. ogni riga ha $n+1$ elementi, che vengono numerati da 0 a n;
3. l'elemento in riga n e posizione k si indica con $T_{n,k}$;
4. $T_{n,0} = T_{n,n} = 1$;
5. per ogni $n \geq 0$, $0 < k \leq n$, $T_{n+1,k} = T_{n,k-1} + T_{n,k}$.

Proposizione 3.5.6. *Sia $n \in \mathbb{Z}$. Allora per ogni $k \in \mathbb{Z}$ tale che $0 \leq k \leq n$ segue che*

$$T_{n,k} = \binom{n}{k} \quad (3.23)$$

Dimostrazione. Per induzione su n.

Caso base. Sia $n = 0$, allora dato che $0 \leq k \leq n$ segue che $k = 0$. Dunque

$$T_{0,0} = 1 = \binom{0}{0}.$$

Passo induttivo. Supponiamo che la tesi sia vera per n e dimostriamola per $n+1$.

– Se $k = 0$ oppure $k = n+1$ allora per definizione del triangolo di Tartaglia $T_{n+1,0} = T_{n+1,n+1} = 1$ che e' esattamente $\binom{n+1}{0} = \binom{n+1}{n+1}$ (per la proposizione 3.5.3),

– Se $0 < k < n+1$ allora per definizione del triangolo di Tartaglia segue che

$$T_{n+1,k} = T_{n,k-1} + T_{n,k} = \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

dove l'ultimo passaggio viene dalla proposizione 3.5.3.

Dunque la tesi e' vera per ogni $n \in \mathbb{Z}$. □

Proposizione 3.5.7. *Il triangolo di Tartaglia gode delle seguenti proprieta':*

1. *la somma degli elementi della riga n e' 2^n;*
2. *la somma a segni alterni degli elementi di ogni riga e' 0;*
3. *nella riga n, l'elemento al posto k e l'elemento al posto $n-k$ hanno lo stesso valore.*

Dimostrazione. Dimostriamo le tre proposizioni.

1. Dimostriamo che $2^n = \sum_{k=0}^{n} T_{n,k} = \sum_{k=0}^{n} \binom{n}{k}$.

$$2^n = (1+1)^n = \sum_{k}^{0} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k}$$

2. La somma a segni alterni della riga n-esima e'

$$\sum_{k=0}^{n} (-1)^k T_{n,k} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0}^{n} (-1)^k 1^{n-k} \binom{n}{k} = (1-1)^k = 0^k = 0.$$

3. Dobbiamo dimostrare che $T_{n,k} = T_{n,n-k}$. Ma dato che $T_{n,k} = \binom{n}{k}$ e $T_{n,n-k} = \binom{n}{n-k}$, allora questo e' equivalente a dimostrare che $\binom{n}{k} = \binom{n}{n-k}$, che e' vero per la proposizione 3.5.2. □

Proposizione 3.5.8. *Se p e' primo, allora per ogni k tale che $0 < k < p$ vale che*

$$\binom{p}{k} \equiv 0 \ \ (p) \tag{3.24}$$

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 $\binom{p}{k} \equiv 0 \pmod{p}$. □

Proposizione 3.5.9. *Siano $x, y, p \in \mathbb{Z}$, p primo. Allora*

$$(x+y)^p \equiv x^p + y^p \pmod{p} \tag{3.25}$$

Dimostrazione. Per il teorema del Binomiale (3.5.4) sappiamo che

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

Ma per la proposizione 3.5.8 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. □

Corollario 3.5.10. *Siano $x_1, x_2, \ldots, x_n, p \in \mathbb{Z}$, p primo. Allora*

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod{p} \tag{3.26}$$

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.

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

(per la proposizione 3.5.9)

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

(per ipotesi induttiva)

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

che e' la tesi per n.

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

Teorema 3.5.11 (Piccolo Teorema di Fermat)**.** *Se p e' primo, allora $x^p \equiv x \pmod{p}$.*

Dimostrazione.

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

(per il corollario 3.5.10)

$$\begin{aligned} &\equiv \overbrace{1^p + \cdots + 1^p}^{x \text{ volte}} \ \ (p) \\ &\equiv \overbrace{1 + \cdots + 1}^{x \text{ volte}} \ \ (p) \\ &\equiv x \ \ (p) \end{aligned}$$

che e' la tesi. □

Corollario 3.5.12. *Se p e' primo e $x \not\equiv 0 \ \ (p)$ allora $x^{p-1} \equiv 1 \ \ (p)$.*

Dimostrazione. Per il piccolo teorema di Fermat (3.5.11) vale che $x^p \equiv x \ \ (p)$. Dato che $x \not\equiv 0 \ \ (p)$ allora segue che p e x sono coprimi, dunque x e' invertibile modulo p. Moltiplicando entrambi i membri per l'inverso x^{-1} otteniamo

$$\begin{aligned} &x^p x^{-1} \equiv x \cdot x^{-1} \ \ (p) \\ \iff &x^{p-1} \equiv 1 \ \ (p) \end{aligned}$$

che e' la tesi. □

3.6 Congruenze esponenziali

Iniziamo con un esempio di congruenza esponenziale.

Esempio 3.6.1. Trovare tutte le soluzioni di $3^x \equiv 5 \ \ (7)$.

Soluzione. Proviamo per tentativi:

$$\begin{aligned} x = 0 &\implies 3^0 \equiv 1 \not\equiv 5 \ \ (7) \\ x = 1 &\implies 3^1 \equiv 3 \not\equiv 5 \ \ (7) \\ x = 2 &\implies 3^2 \equiv 9 \equiv 2 \not\equiv 5 \ \ (7) \\ x = 3 &\implies 3^3 \equiv 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \not\equiv 5 \ \ (7) \\ x = 4 &\implies 3^4 \equiv 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4 \not\equiv 5 \ \ (7) \\ x = 5 &\implies 3^5 \equiv 3^2 \cdot 3^3 \equiv 2 \cdot 6 \equiv 12 \equiv 5 \ \ (7) \\ x = 6 &\implies 3^6 \equiv 3^3 \cdot 3^3 \equiv 6 \cdot 6 \equiv 36 \equiv 1 \not\equiv 5 \ \ (7) \end{aligned}$$

Dunque $x = 5$ e' una soluzione. Non possiamo dire pero' che le soluzioni sono tutti i numeri della forma $x = 5 + 7k$, perche' possiamo notiare che i numeri sembrano ripetersi con periodo 6 e non 7 (infatti $3^0 \equiv 3^6 \equiv 1 \ \ (7)$).

Dimostriamo che se $x = 5$ e' soluzione, allora anche $x = 5 + 6k$ lo e'. Infatti

$$3^{5+6k} \equiv 3^5 \cdot 3^{6k} \equiv 3^5 \cdot 1^k \equiv 5 \ \ (7).$$

Dunque le soluzioni sono tutte le x tali che $x \equiv 5 \ \ (6)$. Questo vale anche per x negativi, ma dobbiamo definire x^{-1} non come $\frac{1}{x}$ ma come l'inverso di x modulo m.

Definizione 3.6.2. Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora si dice ordine di a modulo m il piu' piccolo intero positivo $\operatorname{ord}_m(a)$ tale che

$$a^{\operatorname{ord}_m(a)} \equiv 1 \ \ (m)\,. \tag{3.27}$$

Osservazione. Notiamo che $\operatorname{ord}_m(a)$ deve essere positivo, e dunque in particolare maggiore di 0. Inoltre la condizione $a \nmid m$, che equivale a $a \not\equiv 0 \ \ (m)$ serve ad evitare la congruenza banale $0^x \equiv b \ \ (m)$, che ha soluzione se e solo se $b \equiv 0 \ \ (m)$.

Proposizione 3.6.3. *Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora per ogni $k \in \mathbb{Z}$ vale che*

$$a^{k \operatorname{ord}_m(a)} \equiv 1 \ \ (m)\,. \tag{3.28}$$

Dimostrazione.

$$a^{k \operatorname{ord}_m(a)} \equiv (a^{\operatorname{ord}_m(a)})^k \equiv 1^k \equiv 1 \ \ (m)\,.$$

□

Proposizione 3.6.4. *Siano $a, m \in \mathbb{Z}$, $a \nmid m$. Allora*

$$a^x \equiv 1 \ \ (m) \iff x \equiv 0 \ \ (\operatorname{ord}_m(a)) \tag{3.29}$$

Dimostrazione. Per definizione di congruenza

$$x \equiv 0 \ \ (\operatorname{ord}_m(a)) \iff x \mid \operatorname{ord}_m(a) \iff x = \operatorname{ord}_m(a) \cdot k$$

per qualche $k \in \mathbb{Z}$.

Per l'unicita' del resto della divisione euclidea (2.1.7) possiamo scrivere che $x = q \operatorname{ord}_m(a) + r$ per qualche $q, r \in \mathbb{Z}$ con $0 \leq r < \operatorname{ord}_m(a)$. Questo e' equivalente a dire

$$\begin{aligned} a^x &= a^{q \operatorname{ord}_m(a) + r} \\ &= a^{q \operatorname{ord}_m(a)} \cdot a^r \end{aligned}$$

che equivale a

$$\begin{aligned} a^x &\equiv a^{q \operatorname{ord}_m(a)} \cdot a^r \ \ (m) \\ &\equiv 1 \cdot a^r \ \ (m) \\ &\equiv a^r \ \ (m) \end{aligned}$$

dove abbiamo sfruttato la proposizione 3.6.3 per dire che $a^{q \operatorname{ord}_m(a)} \equiv 1 \ \ (m)$.

Dunque dato che $a^x \equiv a^r \ \ (m)$ segue che $a^x \equiv 1 \ \ (m)$ se e solo se $a^r \equiv 1 \ \ (m)$. Ma $r < \operatorname{ord}_m(a)$, dunque se r fosse maggiore di 0 avremmo trovato un numero minore di $\operatorname{ord}_m(a)$ per cui $a^r \equiv 1 \ \ (m)$, che e' assurdo poiche' va contro la minimalita' di $\operatorname{ord}_m(a)$.

Segue che $r = 0$, cioe' $x = q \operatorname{ord}_m(a)$, cioe' equivalentemente $x \equiv 0 \ \ (\operatorname{ord}_m(a))$, come volevasi dimostrare. □

Proposizione 3.6.5. *Siano $a, b, m \in \mathbb{Z}$, $a \nmid m$. Se $x_0 \in \mathbb{Z}$ e' una soluzione di $a^x \equiv b \ \ (m)$ allora le soluzioni sono tutte e solo della forma*

$$x \equiv x_0 \ \ (\operatorname{ord}_m(a))\,. \tag{3.30}$$

Dimostrazione. Dimostriamo che se $x = x_0 + k \operatorname{ord}_m(a)$ allora x e' soluzione.

$$\begin{aligned} a^{x_0 + k \operatorname{ord}_m(a)} &\equiv a^{x_0} a^{k \operatorname{ord}_m(a)} \pmod{m} \\ &\equiv b \cdot 1 \pmod{m} \\ &\equiv b \pmod{m}. \end{aligned}$$

Dimostriamo ora che se x e' soluzione, allora $x \equiv x_0 \pmod{\operatorname{ord}_m(a)}$, cioe' equivalentemente $x - x_0 = k \operatorname{ord}_m(a)$.

$$\begin{aligned} a^{x-x_0} &\equiv a^x a^{-x_0} \pmod{m} \\ &\equiv b \cdot b^{-1} \pmod{m} \\ &\equiv 1 \pmod{m}. \end{aligned}$$

Ma per la proposizione 3.6.4 $a^{x-x_0} \equiv 1 \pmod{m}$ se e solo se $x - x_0 \equiv 0 \pmod{\operatorname{ord}_m(a)}$, cioe' se e solo se $x \equiv x_0 \pmod{\operatorname{ord}_m(a)}$, che e' la tesi. □

Proposizione 3.6.6. *Siano $a, p \in \mathbb{Z}$, $a \nmid p$, p primo. Allora vale che* $\operatorname{ord}_p(a) \mid p - 1$.

Dimostrazione. Per il corollario al piccolo teorema di Fermat (3.5.12) sappiamo che $a^{p-1} \equiv 1 \pmod{p}$, cioe' $p - 1$ e' una soluzione dell'equazione $a^x \equiv 1 \pmod{p}$.

Per la proposizione 3.6.4 segue che $p - 1 \equiv 0 \pmod{\operatorname{ord}_p(a)}$, cioe' $\operatorname{ord}_p(a) \mid p - 1$, che e' la tesi. □

Dunque se dobbiamo trovare l'ordine di un numero a modulo un primo p ci basta provare tutti i divisori di $p - 1$ fino a quando non troviamo il minimo divisore che soddisfa la proprieta'.