Introduzione a una teoria assiomatica materiale

Una teoria assiomatica (o, sistema assiomatico) comprende il seguente insieme di informazioni:

1. Un elenco di **termini primitivi (o indefiniti)**, cioè un elenco di parole per le quali non viene fornita una descrizione precisa, ma solo una spiegazione. Le parole in questo elenco vengono utilizzate nella teoria successiva come se fossero noti e condivisi da tutti.
2. Un elenco di **assiomi** (detti anche **postulati**): sono enunciati che illustrano le proprietà dei termini primitivi e le loro relazioni. Tali enunciati vengono considerati veri.
3. Un elenco di **regole logiche**: queste sono le uniche regole da utilizzare.

A partire da questi dati, è possibile introdurre altri termini (ma solo se definiti con precisione) e altri enunciati (ma solo se essi possono essere dimostrati utilizzando solo le regole logiche specificate e gli assiomi):

4. Le **definizioni**: un elenco di parole (che può essere allungato a piacere) di termini che vengono univocamente precisati, utilizzando i termini primitivi, gli assiomi o le definizioni introdotte in precedenza. Le definizioni rendono più corti ed efficaci gli enunciati.
5. I **teoremi**, cioè enunciati per i quali è possibile dimostrare che sono veri usando solo i temini primitivi, gli assiomi, le regole logiche. In una dimostrazione, è possibile utilizzare anche teoremi già dimostrati in precedenza.

Per precisione, bisognerebbe inserire nella struttura assiomatica anche la lingua nella quale ci esprimiamo. Inoltre, utilizzeremo spesso, senza dichiararlo, i numeri reali, parte della teoria degli insiemi, la logica aristotelica.
Eventuali raffigurazioni possono essere utilizzate solo come supporto, e non costituiscono una dimostrazione.

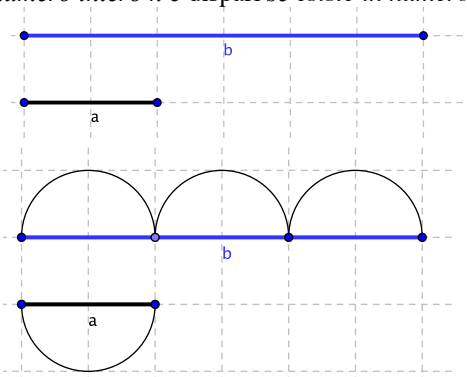
Un sistema assiomatico è **consistente (o coerente)** se non contiene contraddizioni (cioè se non contiene enunciati che sono veri e falsi contemporaneamente).
Un **modello** di un sistema assiomatico si ottiene assegnando ai termini primitivi un significato, in modo che valgano gli assiomi. Esistono modelli concreti (ottenuti utilizzando oggetti e relazioni concreti) e modelli astratti. **Se è possibile trovare un modello concreto per un sistema assiomatico, allora il sistema è consistente**.
Un sistema assiomatico è **completo** se, comunque fissato un enunciato, è possibile dimostrare che esso è vero o è falso. Il sistema assiomatico dell'aritmetica non è completo (Gödel).
In un sistema assiomatico, un assioma è **indipendente** dagli altri se non può essere dedotto come un teorema utilizzando solo gli altri assiomi.
Due modelli di uno stesso sistema assiomatico sono **isomorfi** se esiste una corrispondenza biunivoca tra gli elementi, tale che conservi tutte le relazioni.

Esempi di definizioni

a) *Un numero intero n è* multiplo di *un numero intero m se il numero n può essere ottenuto moltiplicando m per un numero intero, cioè se esiste un opportuno numero intero, che chiamiamo k, tale che n= mk.*
Diciamo anche che *m divide n*, che *m è un divisore di n*. Si utilizza il simbolo $m \mid n$, da leggere '*m* divide *n*'.

b) *Un numero intero n è* pari *se è multiplo di 2.*

c) *Un numero intero n è* dispari *se esiste in numero intero k tale che n= 1+mk.*



a divide b

Un **teorema** *(affermazione dimostrata) è dedotto utilizzando tautologie o argomentazioni valide a partire da una lista di termini non definiti (concetti primitivi), termini definiti (definizioni), ipotesi, teoremi dimostrati in precedenza.*

Definizione. *Un* **argomento** *consiste di premesse e di una conclusione. Diciamo che l'argomento è (logicamente)* ***valido*** *se e solo se la conclusione è vera in tutti i casi in cui le premesse sono vere. Se le premesse sono $p_1, \ldots, p_n$ e la conclusione è q, l'argomento è valido se e solo se $(p_1 \wedge \ldots \wedge p_n) \Rightarrow q$ è una tautologia.*

Esempi *(a) Un argomento valido tramite il* modus ponens*: supponiamo di sapere che*
$p \Rightarrow q$*:* Se un parallelogramma è un quadrato, allora è un rettangolo
e che
p: Il parallelogramma considerato è un quadrato.
Possiamo concludere che
Il parallelogramma considerato è un rettangolo.
(b) Un argomento valido per transitività*: supponiamo di sapere*
$p \Rightarrow q$*:* Se un triangolo è isoscele, allora due suoi lati sono congruenti.
e che:
$q \Rightarrow t$*:* Se in un triangolo due lati sono congruenti, allora anche due angoli sono congruenti.
Possiamo allora concludere che
$p \Rightarrow t$*:* Se un triangolo è isoscele, due suoi angoli sono congruenti.

Definizione. ***La dimostrazione*** *di un teorema è una successione di argomenti validi che utilizzano le premesse del teorema e il sistema assiomatico.*
Le giustificazioni permesse all'interno di una dimostrazione sono:
1) per ipotesi
2) per ipotesi assurda
3) per un assioma
4) per un teorema precedente
5) per definizione
6) per un passo di una dimostrazione precedente
7) per una regola di logica

Per provare che un enuciato è falso, è sufficiente fornire un controesempio.

Esempio di sistema assiomatico: **Il Club delle Tartarughe** *[Richard Trudeau, La rivoluzione non euclidea, Boringhieri, 1991, pp.30-34]*
Termini primitivi*: persona, insieme, appartenenza*.
Definizioni*:* *a) Il* Club delle Tartarughe *è un insieme di una o più persone*.
b) Una persona appartenente al Club è detta Tartaruga.
c) I comitati *sono insiemi di una o più Tartarughe*.
d) Una Tartaruga appartenente a un comitato è detta membro *di quel comitato*.
e) Due comitati sono uguali *se ogni membro del primo è anche membro del secondo, e se ogni membro del secondo è anche membro del primo*.
f) Due comitati che non hanno membri in comune sono detti disgiunti.
Assiomi *1. Ogni Tartaruga è membro di almeno un comitato;*
2. Per ogni coppia di due distinte Tartarughe esiste uno ed uno solo comitato di cui entrambe sono membri;
3. Per ogni comitato esiste uno ed uno solo comitato disgiunto da esso.
Utilizzando solo gli assiomi e le regole logiche, è possibile dedurre alcuni enunciati, che vengono chiamati 'teoremi'.
Teorema*: Ogni Tartaruga è membro di almeno due comitati*.
Dimostrazione [provare a farla prima di leggere il seguito]
Passo1: Sia "*t*" una Tartaruga. [ipotesi, definizione]
Passo 2: *t* è membro di un comitato "*C*" [Assioma 1, definizione]
Passo 3. Esiste un comitato, che indichiamo con "*D*", che è disgiunto da *C*. [Assioma 3, definizione]
Passo 4. Sia "*u*" un membro di *D*. [*u* esiste per definizione di comitato]
Passo 5. *u* non è membro di *C*. [Definizione di "disgiunto"]
Passo 6. Esiste un comitato, che indichiamo con "*E*", di cui sia *t* che *u* sono membri. [Assioma 2, definizione].
Passo 7. I comitati *C* ed *E* non sono uguali. [Definizione di "uguale"; 5, 6]
Passo 8. *t* è membro sia di *C* che di *E*. [passi 2, 6]
Passo 9. *t* è membro di almeno due Comitati. [Passi 7, 8]
Passo 10. Di conseguenza ogni Tartaruga è Membro di almeno due comitati. [generalizzazione: i passi precedenti valgono per ogni tartaruga]

Esercizi 1) Nel sistema del Club delle Tartarughe, mostra il *Teorema 2: Ogni comitato ha almeno due membri*.
2) Considera il seguente sistema assiomatico
Assioma1. Ogni formica ha almeno 2 case.
Assioma 2. Ogni casa ha almeno due formiche.
Assioma 3. Esiste almeno una formica.
a) Individua quali sono i termini primitivi in questo sistema assiomatico.
b) Dimostra che c'è almeno una casa.
c) Mostra che ci sono almeno due 2 formiche.
d) Determina quattro modelli non isomorfi.
3) Osserva che i termini utilizzati nelle definizioni sono irrilevanti. Considera, ad esempio, il sistema assiomatico:
Termini primitivi*: persona, insieme, appartenenza*.

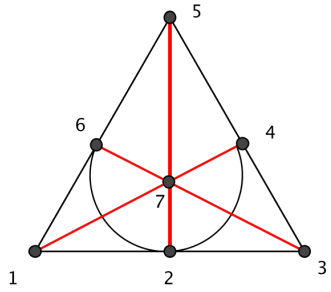
***Definizioni**: Il Club di Facebook è un insieme di uno o più persone.*
Una persona appartenente al Club di Facebook è detta amico.
I gruppi sono insiemi di uno o più amici.
Un amico appartenente a un gruppo è detto componente di quel gruppo.
Due gruppi sono uguali se ogni componente del primo è anche componente del secondo, e se ogni componente del secondo è anche componente del primo.
Due gruppi che non hanno componenti in comune sono detti disgiunti.
***Assiomi** 1. Ogni amico è componente di almeno un gruppo;*
2. Per ogni coppia di due distinti amici esiste uno ed uno solo gruppo di cui entrambi sono componenti;
3. Per ogni gruppo esiste uno ed uno solo gruppo disgiunto da esso.
Mostra che:
***Teorema1**: Ogni amico è componente di almeno due gruppi.*
***Teorema 2**: Ogni gruppo ha almeno due componenti.*

***Ulteriore esempio di sistema assiomatico:* Il Piano di Fano**
Gino Fano (1871–1952), un matematico italiano, ha fornito quello che è considerato il primo esempio di sistema assiomatico 'geometrico' relativo a un modello formato da un numero finito di punti. Tale esempio ha molteplici applicazioni. Illustriamo solo una parte dell'esempio; tale parte viene detta Piano di Fano.
Assiomi per il Piano di Fano
Termini primitivi: punto, linea, incidenza.
***Assiomi 1.** Esiste almeno una linea.*
***2.** Ogni linea ha esattamente tre punti incidenti ad essa.*
***3.** Non tutti i punti sono incidenti alla stessa linea.*
***4.** C'è una e una sola linea incidente ogni coppia di punti distinti.*
***5.** C'è almeno un punto incidente a ogni coppia di linee distinte.*

Due modelli isomorfi soddisfano gli assiomi del Piano di Fano:
Primo modello: è illustrato dalla seguente tabella

punti	*linee*
A, B, C, D, E, F, G	ADB, AGE, AFC, BEC, BGF, CGD, FDE

Secondo modello:



Nella Figura, i punti *sono 7 piccoli cerchietti e le linee sono sei segmenti di retta (ciascuno dei quali contiene tre punti) e una porzione di circonferenza (contenente 4, 2, 6).*
Esercizio 1: *Nel piano di Fano, mostra il* **Teorema 1:** Due distinte linee incidono in esattamente un punto.
Dim. *Siano* r *e* s *due distinte linee. Per l'Assioma 5, esiste (almeno) un punto* A *incidente sia* r *che* s. *Supponiamo che ci sia un secondo punto,* B, *diverso da* A, *incidente sia* r *che* s. *Per l'Assioma 4, le linee* r *e* s *coincidono (perché una sola linea passa per A e B), ma questo contraddice l'ipotesi che* r *e* s *siano linee distinte. Dunque* r *e* s *si intersecano in un unico punto. Possiamo quindi affermare che due linee distinte qualsiasi incidono in un unico punto.*

Esercizio 2: Il piano di Fano è formato da 7 punti.
Dim. *Per l'Assioma 1, esiste (almeno) una linea* t. *Per l'Assioma 2, esistono esattamente 3 punti* A, B, C *incidenti la linea* t. *Per l'Assioma 3, esiste (almeno) un punto* D *che non incide la linea* t. *Dunque ci sono almeno 4 punti* A, B, C, *e* D. *Poiché D non incide* t, *per l'Assioma 4 c'è una linea* a *diversa da* t *che incide* A *e* D. *Allo stesso modo, ci sono una linea* b *diversa da* t *che incide* B *e* D *e una linea* c *diversa da* t *che incide* C *e* D. *Le rette* a, b *e* c *sono distinte tra loro e distinte da* t *(per gli Assiomi 2 e 3). Per l'Assioma 2, la linea* a *incide un terzo punto* A' *diverso da* A *e da* D. *Analogamente, per l'Assioma 2, la linea* b *incide un terzo punto* B' *diverso da* B *e da* D *e la linea* c *incide un terzo punto* C' *diverso da* C *e da* D. *Per l'assioma 4 nessuno tra i punti* A', B', C' *può coincidere con* A, B, C (*altrimenti dovrebbero coincidere coppie di linee che sappiamo essere distinte).*
Dunque nel piano ci sono almeno 7 punti: A, B, C, A', B', C', *e* D. *Dobbiamo mostrare che non ci sono altri punti. Supponiamo che ci sia anche un altro punto* Q *diverso dai precedenti. Il punto Q non incide* t, *poiché* A, B, *e* C *sono gli unici punti che incidono* t *per l'Assioma 2. Per il teorema 1, la linea* t *e la linea che incide* D *e* Q *incidono esattamente in un punto,* R. *Tale punto R (per l'Assioma 2) deve coincidere con uno dei punti A, B, C (che sono i soli punti che incidono* t). *Supponiamo che* R = A. *Poiché* A' *appartiene alla linea* a *per A e P e il punto* A = R *appartiene alla linea per* D *e* Q, *i quattro punti distinti* R = A, A', D *e* Q *risulterebbero incidere la stessa linea, contraddicendo l'Assioma 2. In modo analogo, si esclude che* R *possa coincidere con* B *o con* C. *Quindi, i punti nel piano di Fano sono 7.*
Esercizi
a) *Mostra il Teorema 3:* Ogni punto nel piano di Fano incide esattamente 3 linee distinte.
b) *Mostra il Teorema 4:* Nel piano di Fano ci sono esattamente 7 linee.

Bibliografia: Richard Trudeau, La rivoluzione non euclidea, Boringhieri, 1991
Sitografia: http://web.mnstate.edu/peil/geometry/C1AxiomSystem/AxSysWorksheet.htm - E1_2

Argomentazione valida e dimostrazioni dirette e indirette

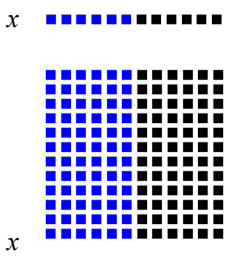
In base agli argomenti che vengono utilizzati, le dimostrazioni sono dette **dirette** o **indirette**. Talora la dimostrazione viene articolata e suddivisa in vari casi, qualora l'ipotesi *p* lo renda vantaggioso.
Per fornire esempi, si utilizzeranno gli assiomi e alcune definizioni dell'aritmetica e dell'insiemistica, utilizzati e studiati nella carriera pre-universitaria.

> *Schema di una **dimostrazione diretta** dell'implicazione* $p \Rightarrow q$
> *Enunciato:* $p \Rightarrow q$
> *Dimostrazione*
> *Supponi p*
> .....
> ....
> *Allora q.* ■

Esempi di dimostrazione diretta

a) *Se* $x \in \mathbb{Z}$ *è pari, allora* x^2 *è pari.*
Dimostrazione. Supponiamo che x sia pari.
Per definizione di numero pari sappiamo che esiste un numero intero k tale che x=2k. Dunque:
$x^2 = x \cdot x = (2k) \cdot (2k) =$ *[sostituendo l'espressione x=2k]*
$= 2 (k \cdot 2k) =$ *[per la proprietà associativa della moltiplicazione]*
$= 2 \cdot h$ *[ponendo* $h = k \cdot 2k$*]*
Osserviamo che h è un numero intero, e dunque $2 \cdot h$ *è un numero pari, per definizione di numero pari.*
Concludiamo che x^2 *è un numero pari.* ■
Rappresentazione grafica della dimostrazione, che ne illustra la motivazione: se *n* è un numero pari, è possibile dividerlo in parti uguali (in modo che ciascuna parte sia un numero intero). Raffiguriamo in nero e in blu le due parti ottenute.

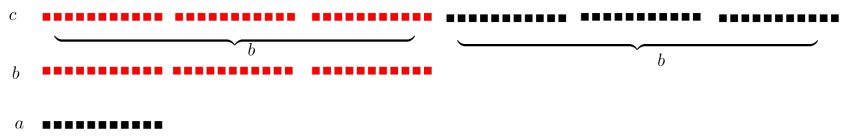
Il numero x^2 può essere raffigurato tramite un quadrato di lato *x*. Colorando opportunamente le colonne, si 'vede' che x^2 è pari, perché può essere diviso in due parti uguali (in modo tale che ciascuna sia un numero intero)



Si intuisce che anche il lato sinistro verticale blu del quadrato (che è uguale a *x*) è pari, e dunque può essere diviso a metà. Colorando differentemente tali due metà e le 'righe' che da esso nascono, il quadrato risulta diviso in quattro parti uguali. Dimostrare per esercizio che se $x \in \mathbb{Z}$ *è pari, allora* x^2 *è multiplo di 4.*

b) *Se* $x \in \mathbb{Z}$ *è dispari, allora* x^2 *è dispari.*
Dimostrazione. Supponiamo che x sia dispari.
Per definizione di numero dispari sappiamo che esiste un numero intero k tale che x=1+2k. Dunque:
$x^2 = x \cdot x = (1+2k) \cdot (1+2k) =$ *[sostituendo l'espressione x=1+2k]*
$= 1+2k +(2k) \cdot (1+2k) =$ *[per la proprietà distributiva della moltiplicazione rispetto alla somma]*
$= 1+2k +(2k)+ (2k) \cdot (2k)$ *[per la proprietà distributiva della moltiplicazione rispetto alla somma]=*
$= 1+2 \cdot (2k) +(2k) \cdot (2k) =$ *[sommando due termini uguali]*
$= 1+2 \cdot (2k) +2 \cdot (k \cdot 2k) =$ *[per la proprietà associativa del prodotto]*
$= 1 + 2 \cdot [2k + k \cdot 2k]$ *[raccogliendo a fattor comune, per la proprietà distributiva]*
$= 1 + 2 \cdot h$ *[ponendo* $h = 2k + k \cdot 2k$*]*
Osserviamo che h è un numero intero, e dunque $1 + 2 \cdot h$ *è un numero dispari per definizione di numero dispari.*
Concludiamo che x^2 *è un numero dispari.* ■

c) *Siano a, b, c* $\in \mathbb{Z}$. *Se a|b e b|c, allora a|c.*
Dimostrazione. Supponiamo che gli interi a, b, c siano tali che a | b and b | c. Per definizione di divisibilità, sappiamo che a | b significa che esiste un intero k tale che b = ak. Analogamente, b | c significa che esiste un intero h tale che c = bh. Dunque, c = bk = (ah)k = a(hk), ove l'ultima uguaglianza segue dalla proprietà associativa della moltiplicazione. Poniamo t = hk e osserviamo che t è un numero intero e dunque il numero at è divisibile per a (cioè a | at). Poiché c = at, concludiamo che a | c. ■



Esempi di dimostrazione diretta per casi

a) *Se $x \in \mathbb{Z}$ non è multiplo di 3, allora x^2 non è multiplo di 3.*
Dimostrazione. Supponiamo che $x \in \mathbb{Z}$ non sia multiplo di 3. Allora si presentano due differenti casi: o esiste $k \in \mathbb{Z}$ tale che $x= 1+3k$, oppure esiste $h \in \mathbb{Z}$ tale che $x= 2+3h$.
PRIMO CASO: Supponiamo che esiste $k \in \mathbb{Z}$ tale che $x= 1+3k$.
Allora, $x^2= (1+3k)^2 =$ (per ipotesi)
$= (1+3k)(1+3k) =$ (per definizione di potenza)
$= 1+3k+ 3k(1+3k) =$ (per la proprietà distributiva della moltiplicazione rispetto alla somma)
$= 1+3[k+ k(1+3k)]$ (per la proprietà distributiva della moltiplicazione rispetto alla somma)
$= 1 + 3k'$ posto $k'= [k+ k(1+3k)]$
Osservo che $1 + 3k'$ non è multiplo di 3 (perche' si ottiene da un mutiplo di 3 sommandogli 1)
Dunque, nel primo caso, x^2 non è multiplo di 3.
SECONDO CASO: Supponiamo che esiste $h \in \mathbb{Z}$ tale che $x=2+3h$.
Allora, $x^2= (2+3h)^2 =$ (per ipotesi)
$= (2+3h)(2+3h) =$ (per definizione di potenza)
$= 4+6h+ 3h(2+3h) =$ (per la proprietà distributiva della moltiplicazione rispetto alla somma)
$= 1+3+6h+ 3h(2+3h) =$
$= 1+3[1 +2h+ h(2+3h)]$ (per la proprietà distributiva della moltiplicazione rispetto alla somma)
$= 1 + 3h'$ posto $h' = [1 +2h+ h(2+3h)]$
Osservo che $1 + 3h'$ non è multiplo di 3 (perche' si ottiene da un mutiplo di 3 sommandogli 1)
Dunque, nel secondo caso, x^2 non è multiplo di 3.
Poiché sono stati analizzati tutti i possibili casi, concludiamo che x^2 non è multiplo di 3. ■

Esercizi*:* Siano n e m numeri naturali. Tramite una dimostrazione diretta dimostra i seguenti enunciati.
a) Se n è multiplo di 3, anche nm è multiplo di 3.
b) Il numero $n(n+1)$ è pari.
c) Il numero $n(n+1)(n+2)$ è multiplo di 3.
d) Se n è multiplo di 3, anche $n^2 - n$ è multiplo di 3.
e) Se n è multiplo di 3, il numero n^2 è multiplo di 9.
f) Se n è multiplo di 3, il numero n^2 è multiplo di 9.
g) Se n e m sono multipli di 3, anche $n+m$ è multiplo di 3.

Le dimostrazioni che non sono dirette, vengono chiamate indirette. Le dimostrazioni indirette possono essere di vario tipo. Una tra le possibili modalità di dimostrazione indiretta è la **dimostrazione per contrapposizione**: poiché sappiamo che $p \Rightarrow q$ è logicamente equivalente alla contronominale $\neg q \Rightarrow \neg p$, dimostriamo che $\neg q \Rightarrow \neg p$ e ne deduciamo che anche $p \Rightarrow q$ è vera.

*Schema di una **dimostrazione indiretta per contrapposizione** dell'implicazione $p \Rightarrow q$*
Enunciato: $p \Rightarrow q$
Dimostrazione
Supponi $\neg q$
.....
....
Allora $\neg p$. ■

Esempio: Confronto tra dimostrazione diretta e indiretta dello stesso enunciato:

Dimostriamo il seguente enunciato. *Se $x \in \mathbb{Z}$ è un numero tale che $5x + 7$ è pari, allora x is dispari.*

Dimostrazione diretta*. Supponiamo che $5x + 7$ sia pari. Per definizione di numero pari sappiamo che esiste un numero intero k tale che $5x+7=2k$, e dunque $5x=2k–7$. Ricaviamo che*
$x=2k–7–4x= 1–8+2k–4x = 1+ 2\cdot(–4+k–2x)$.
Posto $h = –4+k–2x$, notiamo che h è un numero intero e che $1+2h$ è un numero dispari. Poiché $x= 1+2h$, concludiamo che x è dispari. ■

Dimostrazione indiretta per contrapposizione*. Supponiamo che x sia un numero intero che non sia dispari. Allora x è pari, e dunque esiste un numero intero k tale che $x = 2k$. Pertanto:*
$5x + 7 = 5 \cdot (2k) + 7 = 10k+7=1 + 2 \cdot (5k+3)$.
Posto $t = 5k+3$, notiamo che t è un numero intero e che $1+2t$ è un numero dispari. Poiché $5x + 7 = 1+2t$, concludiamo che $5x + 7$ è dispari. ■

Esempio di dimostrazione indiretta per contrapposizione:

a) *Sia n un numero naturale tale che $2 \mid n^2$. Allora $2 \mid n$.*
Dimostrazione: supponiamo che non sia vero che $2|n$, cioè supponiamo che n sia dispari. Ma allora esiste un numero naturale h tale che $n= 1+2h$. Ne segue che $n^2 = (1+2h)^2 = 1+2h + 2h+2 \cdot 2h^2= 1+2(2h+ 2h^2)$ è un numero dispari. Dunque non è vero che $2|n^2$. Per contrapposizione, segue che, se $2 \mid n^2$, allora $2 \mid n$.

b) *Siano $a, b \in \mathbb{Z}$ tali che 7 non divide ab. Allora, 7 non divide a e 7 non divide b.*
Dimostrazione. Supponiamo che non sia vero che '7 non divide a e 7 non divide b'. Allora, deve accadere che 7 divide a oppure 7 divide b, cioè $7 \mid a$ o $7 \mid b$. Consideriamo separatamente i due casi (che non si autoescludono).
PRIMO CASO: supponiamo che $7 \mid a$; sappiamo dunque che esiste un intero k tale che $a = 7k$; concludiamo che $ab = (7k)\ b = 7\ (kb)$ e quindi $7 \mid ab$.
SECONDO CASO: supponiamo che $7 \mid b$; sappiamo dunque che esiste un intero h tale che $b = 7h$; concludiamo che $ab = a\ (7h) = (a7)\ h = 7(ah)$ e quindi $7 \mid ab$.
In entrambi i casi abbiamo concluso che $7 \mid ab$; dalla negazione del conseguente, abbiamo quindi mostrato la negazione dell'antecedente. Possiamo quindi concludere che l'enunciato da dimostrare è vero. ■

Un modo per articolare una dimostrazione indiretta è detto **dimostrazione per assurdo o per contraddizione**: per mostrare che $p \Rightarrow q$, si suppone che p sia vera, ma la tesi q sia falsa; a partire da queste assunzioni, si determina una proposizione r della quale si puo mostrare contemporaneamente sia che r è vera, sia che r è falsa: dunque r deve essere contemporaneamerte vera e falsa, e questo è impossibile. Si deduce che, allora, quando p è vera, anche q deve necessariamente essere vera, e dunque $p \Rightarrow q$.

*Schema di una **dimostrazione indiretta per assurdo (o per contraddizione)** dell'implicazione $p \Rightarrow q$*
Enunciato: $p \Rightarrow q$
Dimostrazione
Supponi p e $\neg q$ (cioè $p \wedge \neg q$. L'ipotesi $\neg q$ è detta ipotesi assurda o ipotesi per assurdo)
.....
....
Allora $r \wedge \neg r$ per una opportuna proposizione r.
Dunque $p \Rightarrow q$ ■

Esempi di dimostrazione indiretta per assurdo

a) Se A e B sono due insiemi, allora $(A \backslash B) \cap (B \backslash A) = \emptyset$
Dimostrazione per assurdo.
Supponiamo che A e B siano due insiemi. Supponiamo per assurdo che l'intersezione $(A \backslash B) \cap (B \backslash A)$ non sia vuota. Supponiamo quindi che ci sia un elemento x appartenente a $(A \backslash B) \cap (B \backslash A)$. Poiché x appartiene all'intersezione $(A \backslash B) \cap (B \backslash A)$, si deve avere che x appartiene sia a $(A \backslash B)$ che a $(B \backslash A)$. Allora
$x \in (A \backslash B)$ significa che $x \in A$ e $x \notin B$: in particolare, $x \in A$.
$x \in (B \backslash A)$ significa che $x \notin A$ e $x \in B$: in particolare, $x \notin A$.
Abbiamo mostrato contemporaneamente che $x \in A$ e $x \notin A$, trovando una contraddizione. Dunque, l'ipotesi assurda che $(A \backslash B) \cap (B \backslash A)$ non fosse vuota è falsa, e dunque $(A \backslash B) \cap (B \backslash A) = \emptyset$. ■

b) Se a, b sono due numeri naturali tali che $ab > 16$ allora o $a > 4$ o $b > 4$.
Dimostrazione per assurdo.
Supponiamo che a, b siano due numeri naturali tali che $ab > 16$. Per assurdo, supponiamo che $a \leq 4$ e $b \leq 4$ (cioè che sia falso che $a > 4$ o $b > 4$). Ma, allora, $ab \leq 16$: ma questa è una contradizione rispetto all'ipotesi iniziale.
[nota: questa dimostrazione è riconducibile a una dimostrazione per contrapposizione]

Esercizio*:* Siano n e m numeri naturali. Dimostra, tramite una dimostrazione indiretta, che:
a) se n^2 è multiplo di 3, anche n è multiplo di 3.
b) se $2n$ è multiplo di 3, anche n è multiplo di 3.
c) Mostra che se n e m sono multipli di 3, anche il prodotto nm è multiplo di 3.

Sitografia: https://www.people.vcu.edu/~rhammack/BookOfProof/