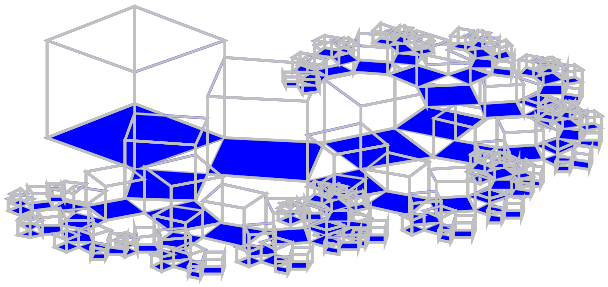


Appunti di aritmetica

Rielaborazione delle lezioni di matematiche elementari da un punto vista superiore, tenute dal professor Mario Dolcher

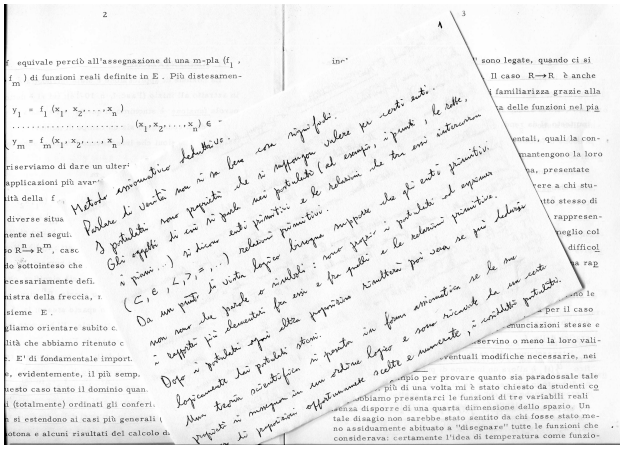
Autore:
Giuseppe Bruno
Trascrizione e impaginazione:
Gli alunni della 3CSCA (2019-20) coordinati
da G. Gasparin

Prima edizione 20 dicembre 2019
ultima revisione 24 dicembre 2019

Indice

Capitolo 1

Note iniziali



Gli appunti che trovate qui di seguito, sono stati rielaborati dal professor Giuseppe Bruno. Costituiscono la sintesi delle lezioni di Matematiche elementari da un punto vista superiore tenute, negli anni '70, dal professor Mario Dolcher, presso la facoltà di matematica dell'Università degli Studi di Trieste.

Ho voluto proporli agli studenti delle mie classi con diversi obiettivi: far conoscere esempi di matematica puntuale e raffinata, stimolare all'approfondimento e alla rielaborazione dei contenuti, abituare alla scoperta delle tecniche dimostrative e, da ultimo, far provare le tecniche di scrittura scientifica usando LaTeX.

I riferimenti ai matematici citati sono riportati dal testo scritto, nel 1972, da Morris Kline "Storia del pensiero matematico" edito da Einaudi.

L'unico testo di riferimento per gli appunti sono le dispense (in particolare i fascicoli I e III) di Analisi Matematica del prof. Mario Dolcher editi nel 1970 dalla Tipografia Moderna di Trieste. Questi preziosi fascicoli, negli anni '90, sono stati ristampati: Elementi di analisi matematica (1-2) di Mario Dolcher Lint Editoriale.

Ho inserito un appendice con le basi di logica tratte da C.D. Pagani S. Salsa Analisi matematica volume 1 edito da Zanichelli.

Gianpaolo Gasparin

Capitolo 2

Simbologia usata

simbolo usato	**descrizione**
$lcm(a, b)$	minimo comune multiplo di a e b
$gcd(a, b)$	massimo comune divisore di a e b
$a \equiv_n b$	a congruo b modulo n
$a \mid b$	a divide b
$\lvert A \rvert$	cardinalità dell'insieme A

Capitolo 3

Appunti di aritmetica

3.1 Metodo assiomatico deduttivo

Parlare di verità non si sa bene cosa significhi. I postulati sono proprietà che si suppongono valere per certi enti. Gli oggetti di cui si parla nei postulati (ad esempio, i punti, le rette, i piani, ...) si dicono enti primitivi e le relazioni che tra essi intercorrono ($\subset$, $\in$, $<$, $>$, $=$, ...) relazioni primitive.

Da un punto di vista logico bisogna supporre che gli enti primitivi non sono che parole o simboli: sono proprio i postulati ad esprimere i rapporti più elementari fra essi e fra quelli e le relazioni primitive. Dopo i postulati ogni altra proposizione risulterà poi vera se può dedursi logicamente dai postulati stessi.

Una teoria scientifica si presenta in forma assiomatica se le sue proprietà si susseguono in un ordine logico e sono ricavate da un certo numero di proposizioni opportunamente scelte e numerate, i cosiddetti postulati.

Ad esempio, dopo aver introdotto in geometria come primitivi i concetti di punto e di retta, postuliamo che "per due punti distinti passa una retta e una sola, cioè esiste un'unica retta cui i due punti appartengono". Questa proposizione non si dimostra poiché non esiste un'altra proprietà che intercorre tra i punti e le rette; di più, ignoriamo perfino, perché manca la definizione, il significato di punto e di retta.

Osservazione critica: un postulato per conto suo non ha interesse, un sistema di postulati sì.

"Dati tre punti A, B, C, non allineati, esiste uno ed un solo piano che li contiene", "se una retta r ha in comune con un piano α due punti distinti A e B, allora ogni altro punto della retta r appartiene ad α" costituiscono un sistema di postulati.

Tre requisiti sono presi in considerazione per un sistema di postulati: la non contraddittorietà, la completezza e l'indipendenza.

Un sistema è non contraddittorio o compatibile se non è possibile dedurre da esso due proposizioni contraddittorie.

La compatibilità è un requisito essenziale.

Pertanto un sistema di postulati S è contraddittorio se da S può seguire una proposizione A e la sua negazione $\overline{A}$.

Dimostriamo che da un sistema assiomatico contraddittorio si può dedurre qualunque proposizione.

Dimostrazione. Consideriamo l'implicazione $\left(A \wedge \overline{A}\right) \rightarrow B$ e proviamo che è vera.

Scritta, infatti, nella forma equivalente $\overline{A \wedge \overline{A}} \vee B = \overline{A} \vee A \vee B$, osserviamo che è vera.

Ma se A è $\overline{A}$ sono entrambe vere, sarà vera anche la proposizione antecedente $A \wedge \overline{A}$ dell'implicazione $\left(A \wedge \overline{A}\right) \rightarrow B$. Per la regola del "modus ponens"([1]) si conclude che risulta vera la B □

L'accertamento della compatibilità dei postulati è fondamentale.

Se concetti primitivi e postulati sono desunti dall'esperienza, si ha una assicurazione intuitiva della loro non contraddittorietà.

Occorre però procedere con logica, che si può raggiungere costruendo un modello mediante enti concreti che non siano contraddittori e verifichino tutti i postulati.

Ad esempio, i postulati della Geometria Euclidea sono compatibili in quanto gli enti geometrici (punti, rette, piani) concreti non si contraddicono.

Osservazione In realtà una dimostrazione soddisfacente della compatibilità dei postulati di un sistema assiomatico non è stata mai data. A tale proposito, proviamo il seguente importante enunciato.

Teorema 1. Condizione necessaria e sufficiente perché una teoria razionale sia non contraddittoria e che non contenga tutte le proposizioni.

Dimostrazione. Infatti la condizione è necessaria in quanto se una teoria è non contraddittoria, non contiene insieme le proposizioni A e $\overline{A}$, cioè non contiene tutte le proposizioni.

Proviamo che la condizione è sufficiente.

Noi sappiamo che se la teoria è contraddittoria, allora contiene tutte le proposizioni. Consideriamo ora la contronominale di questa implicazione: se la teoria non contiene tutte le proposizioni allora la teoria è non contraddittoria. □

Pertanto, per dimostrare la non contraddittorietà di una teoria, occorre stabilire che esiste almeno una proposizione indimostrabile all'interno della teoria presa in esame.

Dato un sistema di postulati, questi sono indipendenti se non è possibile dimostrare alcuno di essi dai rimanenti, oppure se la negazione di uno qualunque di essi congiuntamente agli altri determina un sistema compatibile.

L'indipendenza è un requisito non indispensabile, ma desiderabile. L'indipendenza di un sistema S di postulati A, B, C, D, che individuiamo con $S(A, B, C, D)$, si prova mostrando che:
$S^I(A, B, C, \overline{D})$ è un sistema compatibile;
$S^{II}(A, B, \overline{C}, D)$ è un sistema compatibile;
$S^{III}(A, \overline{B}, C, D)$ è un sistema compatibile;
$S^{IV}(\overline{A}, B, C, D)$ è un sistema compatibile;

[1] Vedi Appendice A

Esempio Consideriamo i 5 postulati di Euclide:

I) Dati due punti distinti, esiste una, e una sola, retta che li contiene.

II) Una linea retta finita si può prolungare continuamente per diritto.

III) Con ogni centro e ogni distanza si può descrivere una circonferenza.

IV) Tutti gli angoli retti sono uguali.

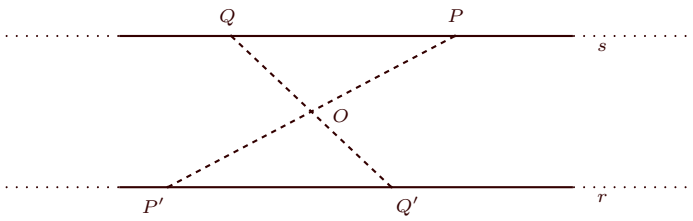
V) Se una retta, cadendo su due rette, forma da una stessa parte angoli interni la cui somma è minore di due retti, allora le due rette, prolungate indefinitamente, si incontrano dalla parte in cui si trovano i due angoli la cui somma è minore di due retti.

Questo ultimo postulato si enuncia solitamente così:

V') Dati nel piano un punto P e una retta r ($P \notin r$), esiste una e una sola retta s passante per P e non avente alcun punto in comune con la r.

A dire il vero, solo l'unicità non può essere provata, mentre l'esistenza è dimostrabile in base ai postulati precedenti. Ecco una possibile dimostrazione.

Dimostrazione. Prendiamo sulla retta r due punti P' e Q' e un punto $P \notin r$. Sia O il punto medio del segmento PP' e Q il simmetrico di Q' nella simmetria centrale di centro O.



La retta s passante per P e Q è la corrispondente di r in questa simmetria.

Supponiamo, per assurdo, che r ed s si intersecano in un punto E. Il simmetrico E' di E appartiene sia ad r, perché $E \in s$ che ad s, in quanto $E \in r$. Allora per E ed E' passano due rette distinte r, s e ciò contraddice il postulato I. □

Bolyai e Lobatchevsky([2]) hanno dimostrato l'indipendenza del V postulato di Euclide dando un modello di elementi concreti che soddisfa tutti i postulati precedenti tranne questo (geometria non-euclidea).

[2]... Non discuteremo i teoremi specifici di geometria non euclidea dovuti a Gauss. Egli non scrisse un'esposizione completamente deduttiva delle sue ricerche e i teoremi che provò sono in gran parte simili a quelli che incontreremo nell'opera di Lobatchevsky e di Bolyai, i due matematici a cui viene generalmente attribuita la creazione della geometria non euclidea. Che cosa debba loro essere attribuito lo discuteremo in seguito, ma essi pubblicarono delle presentazioni organiche di una geometria non euclidea su basi deduttive sintetiche rendendosi pienamente conto che questa nuova geometria era dal punto di vista logico altrettanto legittima di quella di Euclide.

Nikolai Ivanovich Lobatchevsky (1793-1856), russo, studiò all'università di Kazan di cui fu professore e rettore dal 1827 al 1846. Espose le sue vedute sui fondamenti della geometria

Pertanto l'indipendenza del V postulato consente di costruire un'altra geometria, perfettamente compatibile, basata su un sistema di postulati in cui il V è sostituito da uno contrario.

In effetti esistono più geometrie non euclidee, dal momento che al posto del V possiamo introdurre un postulato qualsiasi che però neghi quello di Euclide.

Abbiamo detto che l'indipendenza non è un requisito essenziale. Spesso è utile aggiungere, per fini didattici, qualche postulato dipendente dagli altri per evitare dimostrazioni troppo lunghe. Una teoria non è costruita su un sistema di postulati, fissato una volta per tutte.

Pertanto è opportuno ammettere o no un postulato di volta in volta.

Infine, all'insieme dei postulati posti alla base di un sistema si richiede la completezza (requisito essenziale).

Un sistema assiomatico si dice completo se non può essere aggiunto nessun altro postulato che risulti indipendente dagli altri. Possiamo anche dire che i postulati sono completi se da essi si deduce ogni teorema del sistema.

3.1.1 Osservazioni sul significato di assiomatica

Gli assiomi sono delle preposizioni che si accettano senza dimostrazioni e costituiscono le definizioni implicite degli enti. Non ci si preoccupa di dire che cosa siano gli enti, ma si danno le relazioni a cui tali enti devono soddisfare. Tra un sistema di postulati e una definizione non c'è una differenza sostanziale (per esempio, definizione di gruppo e assiomatica di gruppo). Pertanto l'assiomatica non è solo quella euclidea, ma può essere considerata in ogni definizione (gruppi, numeri di Peano, spazi topologici, geometrie finite,...). L'assiomatica è la descrizione di una struttura (di un sistema di dati) su un insieme. Diamo, ora, la seguente

Definizione 1. Due sistemi assiomatici S' e S'' sono equivalenti quando ogni assioma di S'' è deducibile da S' e viceversa, cioè se ogni assioma di S'' viene ad essere un teorema dedotto da S' e viceversa.

Nel trovare l'equivalenza di due sistemi assiomatici c'è il punto dolente!

Questa definizione è condizionata dal fatto che gli enti primitivi e le relazioni in S' ed S'' sono uguali, ovvero si usa lo stesso linguaggio.

in un lavoro letto di fronte al dipartimento di matematica e fisica dell'università nel 1826. Tuttavia, il lavoro non fu mai stampato e andò perduto. In seguito espose il suo approccio alla geometria non euclidea in una serie di lavori, i primi due dei quali furono pubblicati in riviste di Kazan e il terzo nel « Journal fuï Mathematik »". Il primo era intitolato Sui fondamenti della geoetria e apparve nel 1829-30. Il secondo, intitolato Nuovi fondamenti della geometria con una teoria completa delle parallele (1835-37), è una presentazione migliore delle idee di Lobatchevsky. Egli chiamava la sua nuova geometria « geometria immaginaria » per motivi che sono forse già chiari e che lo diventeranno di più in seguito. Nel 1840 pubblicò un libro in tedesco, intitolato Geomzetrische Untersuchungen zur Theorie der Parallellinien (Ricerche geometriche sulla teoria delle parallele) ". In esso si lamenta per lo scarso interesse nei confronti dei suoi scritti. Pur essendo diventato cieco, dettò un'esposizione completamente nuova della sua geometria e la pubblicò nel 1855 con il titolo di Pangéométrie.

Jinos Bolyai (1802-60), figlio di Wolfgang Bolyai, era un ufficiale ungherese. Sulla geometria non euclidea, che chiamava geometria assoluta, scrisse un lavoro di ventisei pagine intitolato La scienza dello spazio assoluto", che fu pubblicato in appendice al libro del padre intitolato Tentamen Juventutem Studiosam in Elementa Matheseos. Anche se quest'opera in due volumi apparve nel 1832-33, e quindi dopo il primo lavoro di Lobatchevsky, sembra che Bolyai abbia elaborato le sue idee sulla geometria non euclidea prima del 1825 e che entro quel periodo si fosse convinto che la nuova geometria non era contraddittoria. ... (pagg. 1018-19)

Esempio: il reticolo([3])è un insieme ordinato (la relazione d'ordine è indicata con il segno $\prec$), soddisfacente il seguente sistema di postulati S': presi comunque due suoi elementi a, b esistono :

R1) Un loro massimo precedente comune c', ossia: $\begin{cases} c' \prec a, c' \prec b \\ \text{da } x \prec a, x \prec b \end{cases} \Rightarrow x \prec c'$

R2) un loro minimo seguente comune c'', ossia: $\begin{cases} a \prec c'', b \prec c'' \\ \text{da } x \prec a, x \prec b \end{cases} \Rightarrow c'' \prec x$

Il reticolo può definirsi in questo altro modo:
è un insieme dotato di due leggi di composizione, che indichiamo con $\wedge$ e $\vee$, ovunque definite, soddisfacenti entrambe il seguente sistema di assiomi S'':

P1) le due leggi di composizione sono indempotenti: $a \wedge a = a$ $a \vee a = a$;

P2) sono associative: $a \wedge (b \wedge c) = (a \wedge b) \wedge c$; $a \vee (b \vee c) = (a \vee b) \vee c$;

P3) sono commutative: $a \wedge b = b \wedge a$; $a \vee b = b \vee a$;

P4) valgono le proprietà di assorbimento: $a \wedge (a \vee b) = a$; $a \vee (a \wedge b) = a$.

Teorema 2. S' e S'' sono 2 sistemi assiomatici che definiscono lo stesso reticolo

Dimostrazione. S'' si può dedurre da S' e viceversa. Tale deduzione è condizionata da una traduzione di termini (enti, relazioni primitive) proviamo che il sistema S' implica l'esistenza di due operazioni $\wedge$ e $\vee$ che soddisfano S'' e viceversa, assegnate le operazioni, esse definiscono una relazione d'ordine nell'insieme che soddisfa S'. La legge di traduzione è $a \prec b \Leftrightarrow a \wedge b = a$ oppure $a \vee b = b$.

Proviamo che $S' \Rightarrow S''$.

La relazione $\prec$ è riflessiva: $a \prec a \rightarrow a \wedge a = a$, $a \vee a = a$.

Le due operazioni $\wedge$,$\vee$ soddisfano, pertanto, la proprietà P1). La relazione $\prec$ è antisimmetrica: $a \prec b, b \prec a \Rightarrow a = b$, ossia $a \wedge b = a, b \wedge a = b \Rightarrow a = b$. Segue allora che $a \wedge b = b \wedge a$ Analogamente, si ha $a \vee b = b \vee a$. Le due operazioni soddisfano, pertanto, la proprietà P3).

La relazione $\prec$ è transitiva: $a \prec b$, $b \prec c \Rightarrow a \prec c$, ossia $a \wedge b = a$, $b \wedge c = b \Rightarrow a \wedge c = a$. Segue allora che $a \wedge (b \wedge c) = a \wedge b = a$, $(a \wedge b) \wedge c = a \wedge c = a$ $\Rightarrow a \wedge (b \wedge c) = (a \wedge b) \wedge c$). Analogamente, si ha $a \vee (b \vee c) = (a \vee b) \vee c$. Le due operazioni soddisfano, pertanto, la proprietà P2). Inoltre, se $a \prec b \Rightarrow a \vee (a \wedge b) = a \vee a = a$, $a \wedge (a \vee b) = a \wedge b = a$. Vale dunque la proprietà P4).

Proviamo che $S'' \Rightarrow S'$.

La relazione $\prec$ è riflessiva poiché $a \wedge a = a$ oppure $a \vee a = a$, per la proprietà P1). Per dimostrare che $\prec$ è antisimmetrica, supponiamo $a \prec b$, $b \prec a$, ossia $a \wedge b = a$, $b \wedge a = b$; dalla P3), segue allora $a = b$. Per provare che $\prec$ è transitiva, supponiamo $a \prec b$, $b \prec c$, ossia $a \wedge b = a$, $b \wedge c = b$. Si ha allora, dalla P2), $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$.

Resta da constatare che, nell'ordine così stabilito, $a \wedge b$ è il massimo precedente comune di a, b; e che $a \vee b$ è il loro minimo seguente comune. Che $a \wedge b$ preceda a e b discende subito che P1), P2), P3): $(a \wedge b) \wedge a = a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$.

[3]un reticolo (lattice in inglese) è un insieme parzialmente ordinato in cui ogni coppia di elementi ha sia un estremo inferiore (inf) che un estremo superiore (sup).

Sia poi $x \prec a$, $x \prec b$: proviamo che è $x \prec a \wedge b$. Avendosi, per ipotesi, $a \wedge x = x$, $b \wedge x = x$, se ne deduce $(a \wedge b) \wedge x = a \wedge (b \wedge x) = a \wedge x = x$, ossia $x \prec a \wedge b$.

Proviamo ora la tesi analoga per l'operazione $\vee$, tenuto conto che $a \wedge b = a$ equivale ad $a \vee b = b$.

Si dimostra anzitutto facilmente che $a \vee b$ segue tanto a quanto b. Sia poi $a \prec x$, $b \prec x$; proviamo che $a \vee b \prec x$.

Avendosi per ipotesi $a \wedge x = a$, $b \wedge x = b$ si ha anche come si è visto ora, $a \vee x = x$, $b \vee x = x$. Ne viene $x \vee (a \vee b) = (x \vee a) \vee b = x \vee b = x$ donde si deduce che fra i seguenti comuni di a, b l'elemento $a \vee b$ è il minimo. □

Una struttura su un insieme viene assegnata mediante un sistema di assiomi a meno di una equivalenza.

Esempio Uno spazio topologico può essere definito in almeno quattro modi:

Definizione 2. Spazio topologico è un insieme E munito di una famiglia $\mathcal{A}$ di punti di E ($\mathcal{A} \subset \mathcal{P}(E)$)([4]) aventi le seguenti proprietà (assiomi delle strutture topologiche)

A1) $\varnothing \in \mathcal{A}$, $E \in \mathcal{A}$.

A2) ogni intersezione finita di insiemi di $\mathcal{A}$ è ancora un insieme di $\mathcal{A}$.

A3) Ogni riunione di insiemi di $\mathcal{A}$ è ancora un insieme di $\mathcal{A}$.

Gli insiemi di $\mathcal{A}$ sono detti gli "aperti" della topologia definita da $\mathcal{A}$.
$\mathcal{A} = \{\varnothing, E\}$ è la topologia banale, $\mathcal{A} = \mathcal{P}(E)$ è la topologia discreta. Nello spazio topologico E si dice "intorno" di un suo punto x ogni insieme che contiene un insieme aperto contenente x.

Definizione 3. Un insieme E è un spazio topologico se esiste una famiglia $\mathcal{E}$ di sottoinsiemi di E ($\mathcal{E} \subset \mathcal{P}(E)$) aventi le proprietà seguenti:

C1) $\varnothing \in \mathcal{E}$, $E \in \mathcal{E}$.

C2) Ogni riunione finita di insiemi di $\mathcal{E}$ è ancora un insieme di $\mathcal{E}$.

C3) Ogni intersezione di insiemi di $\mathcal{E}$ è ancora un insieme di $\mathcal{E}$.

Gli insiemi di $\mathcal{E}$ sono detti i "chiusi" della topologia definita da $\mathcal{E}$.

Definizione 4. K. Kuratowski([5]) ha dato una definizione di topologia, basandosi non sugli aperti ma sulla chiusura, nel modo seguente: dato un insieme E, se ad ogni suo sottoinsieme A associamo un altro sottoinsieme $\overline{A}$; detto chiusura di A, soddisfacente i seguenti assiomi:

[4] $\mathcal{P}(E)$ è l'insieme delle parti di E, ad esempio se $E = \{a, b\}$ allora $\mathcal{P}(E) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$

[5] ... L'opera di Bourbaki, oltre a rivestire caratteri di originalità suoi propri, ha inglobato e sistematizzato quella di altri autori e scuole. Così, ad esempio, nel campo della topologia generale, partendo dai risultati della scuola polacca di Cazimierz Kuratowski, molto attiva fra gli anni '20 e '30 e alla quale si devono teoremi fondamentali sulla connessione, la compattezza, le condizioni di metrizzabilità ecc., sono da ascrivere ai bourbakisti le nozioni e i risultati principali sulla paracompattezza (Dieudonné) e sugli spazi uniformi (Weil). Analogamente, nel campo dell'algebra, l'antecedente storico diretto di Bourbaki può essere ritrovato facilmente nella *Moderne Algebra* di Bartel Leendert van der Waerden, allievo e continuatore dell'opera di Emmy Noether, la cui pubblicazione nel 1930-31 segna l'inizio dell'algebra contemporanea, dando una sistematizzazione definitiva alle nozioni di gruppo, anello, corpo e delle varie altre strutture algebriche, e dimostrandone con rigore le principali proprietà. ... (pag. 1417)

K1) $A \subset \overline{A}$

K2) $\varnothing = \overline{\varnothing}$

K3) $\overline{A \cup B} = \overline{A} \cup \overline{B}$

K4) $\overline{\overline{A}} = \overline{A}$

Allora l'insieme E con questa operazione di chiusura si chiama "spazio di Kuratowski". In uno spazio di Kuratowski si definisce come insieme chiuso quello che coincide con la sua chiusura; come insieme aperto il complementare di un insieme chiuso.

Si dimostra che una famiglia (un sistema) di aperti così definita soddisfa gli assiomi A1), A2) e A3) e pertanto forma una topologia.

Sia E uno spazio topologico (definizione 2), x un suo punto, $\mathcal{I}(x)$ l'insieme degli intorni di x. $\mathcal{I}(x)$ ha sempre le seguenti 4 proprietà:

$\mathcal{I}1$) Ogni parte di E che contenga un intorno di x è ancora un intorno di x.

$\mathcal{I}2$) Ogni intersezione finita di intorni di x è ancora intorno di x.

$\mathcal{I}3$) x appartiene ad ogni suo intorno.

$\mathcal{I}4$) Se $V \in \mathcal{I}(x)\ \exists W \in \mathcal{I}(x) :\ \forall y \in W, V \in \mathcal{I}(y)$.

Definizione 5. Si può definire una topologia in un certo insieme assegnando per ogni punto l'insieme dei suoi intorni.

Sia E un insieme, $\forall x \in E$ si assegni una famiglia $\mathcal{I}(x)$ di punti di E che verifichi gli assiomi precedenti: allora esiste in E un'unica famiglia di aperti $\mathcal{A}$ tale che $\forall x \in E$, $\mathcal{I}(x)$ sia l'insieme dei suoi intorni nella topologia definita da $\mathcal{A}$. Quindi la famiglia $\mathcal{A} = \{A \subset X :\ \forall x \in A,\ A \in \mathcal{I}(x)\}$ verifica gli assiomi della struttura algebrica (ossia è una famiglia di aperti su X.

Tutte queste definizioni sono equivalenti.

La legge di traduzione è la seguente: diremo chiuso un insieme che è complementare di un aperto.

Dato un insieme $A \subset E$, indichiamo il complementare di A (rispetto ad E) con A'.

Mostriamo, ad esempio, che la definizione 2 e la definizione 3 sono equivalenti $2 \Rightarrow 3$

Sia E un insieme con la topologia $\mathcal{A}$ (famiglia di aperti). Consideriamo gli insieme chiusi $C_1, C_2 \ldots C_n \ldots$, cioè $(C_i)' \in \mathcal{A}$. Utilizzando le formule di De Morgan([6]) $\left(\bigcup_{i=1}^{n} C_i\right)' = \bigcap_{i=1}^{n} C_i' \in \mathcal{A} \Rightarrow \bigcup_{i=1}^{n} C_i \in \mathcal{E}$ (famiglia di intorni)

[6]... Un passo più efficace anche se meno ambizioso venne compiuto da Augustus De Morgan, che pubblicò *Forzal Logic* (1847) e molti articoli, alcuni dei quali apparvero nelle « *Transactions of the Cambridge Philosophical Society* ». Egli tentava di correggere i difetti e di perfezionare la logica aristotelica. Nella Formal Logic egli aggiunse alla logica aristotelica un nuovo principio. Nella seconda la premessa « Alcune M sono A » e « Alcune M sono B » non permette alcuna conclusione; e, di fatto, questa logica dice che il termine medio M deve essere usato in modo universale; si deve cioè usare « Tutte le M ». Ma De Morgan rilevava che da « La maggior parte delle M sono A » e « La maggior parte delle M sono B » segue

$$\left(\bigcap_i C_i\right)' = \bigcup_i C_i' \in \mathcal{A} \;\Rightarrow\; \bigcap_i C_i \in \mathcal{E}$$

$\varnothing$ aperto $\Rightarrow\ \varnothing' = E$ chiuso.
E aperto $\Rightarrow\ E' = \varnothing$ chiuso.

$3 \Rightarrow 2$ Sia E un insieme con la topologia $\mathcal{E}$ (famiglia di chiusi). Consideriamo gli insiemi aperti $A_1, A_2, A_3 ... A_n$ con $(A_i)' \in \mathcal{E}$. Utilizzando De Morgan

$$\left(\bigcap_{i=1}^{n} A_i\right)' = \bigcup_{i=1}^{n} A_i' \in \mathcal{E} \;\Rightarrow\; \bigcap_{i=1}^{n} A_i \in \mathcal{A}.$$

$$\left(\bigcup_i A_i\right)' = \bigcap_i A_i' \in \mathcal{E} \;\Rightarrow\; \bigcup_i A_i \in \mathcal{A}$$

$\varnothing$ chiuso $\Rightarrow\ \varnothing' = E$ aperto
E chiuso $\Rightarrow\ E' = \varnothing$ aperto.

3.2 Postulati di Peano sui numeri naturali

([7])In un insieme $\mathbb{N}$ sia definita una applicazione σ detta "successivo", $\sigma : \mathbb{N} \to \mathbb{N}$ tale che:

(A1) $\forall n \in \mathbb{N}\ \exists n' = \sigma(n)$, detto successivo di n;

(A2) $\exists 0 \in \mathbb{N} : 0 \neq n'\ \forall n \in \mathbb{N}$, cioè lo zero non appartiene all'insieme immagine $\sigma(\mathbb{N})$;

(A3) Se $m' = n' \;\Rightarrow\; m = n$;

(A4) Sia $S \subset \mathbb{N}$ che goda di queste proprietà:

a) $0 \in S$

b) $\forall n \in S \;\Rightarrow\; n' \in S$

necessariamente che « Alcune A sono B ». De Morgan espresse questi fatti in forma quantitativa. Se le M sono m, ed a delle M sono in A e b sono in B, allora ci sono $(a + b - m)$ A che sono in B. Il punto essenziale delle osservazioni di De Morgan è che i termini devono essere quantificati. Di conseguenza riusciva ad introdurre molte più forme valide di sillogismo. La quantificazione eliminava anche un difetto della logica aristotelica: la conclusione « Alcune A sono B », che nella logica aristotelica può essere dedotta da « Tutte le A sono B », implica l'esistenza delle A, ma la loro esistenza non è necessaria.

De Morgan avviò anche lo studio della logica delle relazioni. La logica aristotelica si dedica prima di tutto alla relazione « essere », e asserisce o nega questa relazione. Come rilevava De Morgan, con questa logica non si può dimostrare che, se un cavallo è un animale, allora la coda di un cavallo è la coda di un animale. Certamente essa non potrebbe occuparsi di relazioni quali x ama y. De Morgan introdusse un simbolismo per trattare le relazioni, ma non andò molto lontano.

Nell'area della logica simbolica De Morgan è largamente conosciuto per quelle che oggi vengono chiamate leggi di De Morgan. Egli le enunciava così: il contrario di un aggregato è il composto dei contrari degli aggregati; il contrario di un composto è il contrario delle componenti. . . . (pagg. 1384-85)

[7]. . . L'approccio alla teoria degli interi che meglio si adattava alle tendenze e assiomatizzanti della fine dell'Ottocento era quello consistente nell'introdurli mediante un insieme di assiomi. Servendosi di risultati ottenuti da Dedekind nel libro citato sopra, Giuseppe Peano (1858-32), professore all'Università di Torino, fu il primo a farlo nei suoi *"Arithmetices Principia Nova Methodo Exposita* (1889)". Poiché gli assiomi di Peano sono ancora oggi usati molto comunemente, ne daremo un'esposizione dettagliata. . . . (pag. 1153)

allora S coincide con $\mathbb{N}$.

L'insieme $\mathbb{N}$ degli enti, che soddisfano tali postulati, si dice l'insieme dei numeri naturali. Gli enti primitivi sono: zero, numero, successivo.

Il postulato (A1) ci dice che esiste un'applicazione $\sigma : \mathbb{N} \to \mathbb{N}$ detta "sucessivo".

Il postulato (A2) ci dice che 0 non è successivo di alcun numero naturale.

Il postulato (A3) ci dice che σ è iniettiva.

Il postulato (A4) ci dice che vale il principio di induzione.

Verifichiamo che per tale sistema di postulati valgano i requisiti di non contraddittorietà, completezza e indipendenza.

Non contraddittorietà: si prova dimostrando la compatibilità dei numeri reali, a maggior ragione vale quella dei numeri naturali.

Completezza: Mostriamo che i quattro postulati sono completi, cioè sono sufficienti a caratterizzare in modo univoco la struttura $\mathbb{N}$ dei numeri naturali. Chiameremo la terna $(\mathbb{N}, \sigma, 0)$ sistema di Peano e indichiamo con $(\overline{\mathbb{N}}, \overline{\sigma}, \overline{0})$ un qualunque altro sistema, chiamato ancora di Peano, soddisfacente gli assiomi:

(B1) $\forall a \in \overline{\mathbb{N}}\ \exists a' = \overline{\sigma}(a)$, detta successivo di a;

(B2) $\exists \overline{0} \in \overline{\mathbb{N}} :\ \overline{0} \neq a'\ \forall a \in \overline{\mathbb{N}}$

(B3) se $a' = b' \ \Rightarrow\ a = b$

(B4) Sia $T \subset \mathbb{N}$:

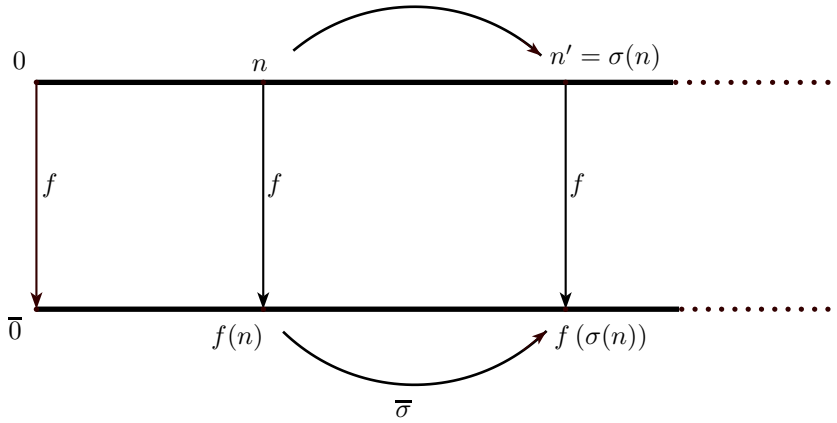
i) $\overline{0} \in T$

ii) $\forall a \in T \ \Rightarrow\ a' \in T$

allora $T = \overline{\mathbb{N}}$ Proviamo che $(\mathbb{N}, \sigma, 0)$ e $(\overline{\mathbb{N}}, \overline{\sigma}, \overline{0})$ sono isomorfi. Consideriamo pertanto una biezione di $\mathbb{N}$ in $\overline{\mathbb{N}}$ che conservi l'applicazione di successivo.

Sia $f : \mathbb{N} \to \overline{\mathbb{N}}$, definita in questo modo :

$$\begin{cases} f(0) = \overline{0} \\ f(\sigma(n)) = \overline{\sigma}(f(n)) \end{cases}$$



Dimostriamo che f è un isomorfismo di $\mathbb{N}$ su $\overline{\mathbb{N}}$. Tale che f è definita su tutto $\mathbb{N}$. Sia infatti, $S = \{n \in \mathbb{N} :\ \exists f(n)\}$, cioè l'insieme dove f resta definita. Allora:

$\left.\begin{array}{l} 0 \in S \text{ per definizione di } f \\ n \in S \ \rightarrow f(n') = f(\sigma(n)) = \overline{\sigma}(f(n)) \Rightarrow n' \in S \end{array}\right\} \ \Rightarrow \ S = \mathbb{N}$ per il principio di induzione. Dunque

Teorema 3. f è definita su tutto $\mathbb{N}$ ed è un omomorfismo

Dimostrazione. Verifichiamo che essa è biettiva, ovvero iniettiva e suriettiva.

È iniettiva, cioè se $n \neq m$ e quindi $\sigma(n) \neq \sigma(m) \ \Rightarrow f(n) \neq f(m)$. Infatti, poiché $n \neq m$, possiamo supporre che $m - n \geq 0$ Sia dapprima $m > n > 0$

Per assurdo supponiamo che risulti $f(n) = f(m)$. Dato che $n > 0$, n è successivo di qualche numero, cioè $n = \sigma(s)$ con $s \in \mathbb{N}$. Analogamente $m = \sigma(p)$ con $p \in \mathbb{N}$. Risulta allora $\overline{\sigma}(f(s)) = f(\sigma(s)) = f(\sigma(p)) = \overline{\sigma}(f(p)) \ \Rightarrow \ f(s) = f(p)$.

Reiterando il procedimento si giunge alla seguente conclusione: $f(0) = f(\overline{m})$ con $\overline{m}$ opportuno elemento di $\mathbb{N}$. Abbiamo inoltre che $f(0) = f(\overline{m}) = \overline{0}$. Il numero $\overline{m}$ è il successivo di qualche numero, ovvero $\overline{m} = \sigma(q)$ con $q \in \mathbb{N}$. Pertanto $f(\overline{m}) = f(\sigma(q)) = \overline{\sigma}(f(q)) = \overline{0}$, cioè $\overline{0}$ è il successivo del numero $f(q)$, contro quanto stabilito da postulato (B2).

È suriettiva

Supponiamo che non lo sia, allora $\exists \overline{n} \in \overline{\mathbb{N}} : \ \overline{n} \notin f(\mathbb{N})$. Inoltre $\overline{n}$ sia il minimo degli elementi di $\overline{\mathbb{N}}$ che non appartengono a $f(\mathbb{N})$. Evidentemente $\overline{n} \neq \overline{0}$ $\left(\overline{0} \in f(\mathbb{N})\right)$. Ora $\forall n \in \mathbb{N}$ deve essere $f(n) \neq \overline{n}$, mentre deve esistere un $n^* \in \mathbb{N}$ per cui $\overline{\sigma}(n^*) = \overline{n}$ con $n^* < \overline{n}$. esiste allora un $r \in \mathbb{N} : \ f(r) = n^*$. Quindi $f(\sigma(r)) = \overline{\sigma}(f(r)) = \overline{\sigma}(n^*) = \overline{n}$ contro ipotesi. Sarà dunque $\overline{n} \in f(\mathbb{N})$. □

3.2.1 Indipendenza

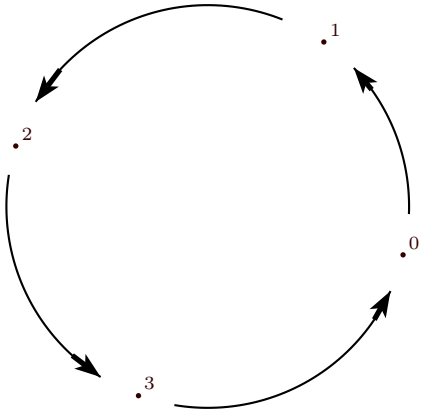
Gli assiomi di Peano sono indipendenti, ovvero nessuno di essi può essere dimostrato a partire dagli altri.

Possiamo convincerci di questo costruendo dei modelli che verifichino tre postulati e il contrario del quarto.

In altre parole, cerchiamo le terne $(S, \sigma, 0)$ per cui un particolare postulato non sia soddisfatto e tutti gli altri invece siano soddisfatti ed S sia non isomorfo all'insieme $\mathbb{N}$ dei numeri naturali.

a) Modello per cui non vale (A1). Assumiamo $S = \{0, 1, 2, 3, 4, 5\}$, manteniamo lo 0 e lasciamo come applicazione "successivo" l'usuale $\sigma : n \rightarrow n + 1$. Evidentemente $\nexists \sigma(5)$. Osserviamo che il postulato (A4) è verificato, infatti non esiste alcun sottoinsieme di S che contenga lo 0 e che risulti stabile rispetto alla σ.

b) Modello per cui non vale (A2). Sia S=$\{0, 1, 2, 3\}$ e σ la funzione così definita: $\sigma(0) = 1, \sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 0$. Osserviamo che 0 risulta successivo di 3.



c) Modello per cui non vale (A3). Sia S=$\{0, 0', 1, 2, 3, \dots\}$ e σ la funzione così definita: $\sigma(0) = 1, \sigma(0') = 1, \sigma(1) = 2, \sigma(2) = 3$. Viene a mancare l'iniettività della funzione, perché da $0 \neq 0' \Rightarrow \sigma(0) = \sigma(0') = 1$. E' un modello con due elementi minimali.

d) Modello in cui non vale (A4). Assumiamo $S = \mathbb{Q}^+$, manteniamo 0 e lasciamo come applicazione "successivo" l'usuale $\sigma : n \to n + 1$.

3.3 Costruzione della struttura algebrica di $\mathbb{N}$

3.3.1 L'addizione in $\mathbb{N}$

Definizione 6. Si definisce somma di due numeri naturali a, b il numero naturale che si indica con $a + b$, tale che: $\begin{cases} a + 0 = a \\ a + b' = (a + b)' \end{cases}$ dove b' indica il successivo di b.

L'applicazione di $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, che associa alla coppia (a, b) il numero $a + b$, si dice addizione.

Proviamo che l'addizione è definita su tutto $\mathbb{N}$. Sia
$S = \{b \in \mathbb{N} : \ \forall a \in \mathbb{N}, \ a + b$ risulti definita$\}$, $0 \in S$ per definizione.

Se $b \in S \ \Rightarrow \ a + b' = (a + b)'$ e poiché $a + b$ è definita $\Rightarrow \ b' \in S$. Per il principio d'induzione segue che $S = \mathbb{N}$

N.B. Posto $\sigma(0) = 1$, si ottiene, $\forall a \in \mathbb{N} : \sigma(a) = \sigma(a+0) = a+\sigma(0) = a+1$.

3.3.2 Proprietà associativa

Proviamo che $a + (b + c) = (a + b) + c$ $(\forall a, b, c \in \mathbb{N})$.

Dimostrazione. Sia $M = \{c \in \mathbb{N} : a + (b + c) = (a + b) + c\}$. $0 \in M$, infatti $a + (b + 0) = a + b$ per definizione e $(a + b) + 0 = a + b$ per definizione $\Rightarrow$ $a + (b + 0) = (a + b) + 0$

Sia $n \in M$ e dimostriamo che $n' \in M$. Per ipotesi si ha: $a + (b + n) = (a + b) + n$. Consideriamo $b + n' = (b + n)'$. Risulta, pertanto, $a + (b + n') = a + (b + n)' = (a + (b + n))' = ((a + b) + n)' = (a + b) + n'$

Dunque, in base al principio di induzione, $\begin{cases} 0 \in M \\ n \in M \ \Rightarrow \ n' \in M \end{cases} \Rightarrow \ M = \mathbb{N}$ dove n' indica il successivo. Vale la proprietà associativa. □

3.3.3 Proprietà Commutativa

Dimostriamo che : $a + b = b + a \quad \forall a, b \in \mathbb{N}$

Dimostrazione. Consideriamo $M' = \{a \in \mathbb{N} : \ a + 0 = 0 + a\}$ $0 \in M'$, infatti $0 + 0 = 0 + 0 = 0$ per definizione. Sia $a \in M' \ \Rightarrow \ a' = a + 0' \ a' + 0 = a + 0' + 0 = a + (0 + 0') = a + 0' = a + 0 + 0' = 0 + a + 0' = 0 + a' \ \Rightarrow \ a' \in M'$. Per il principio di induzione si ha $M' = \mathbb{N}$. Pertanto ogni numero naturale è commutabile con lo zero.

Consideriamo adesso $M'' = \{a \in \mathbb{N} : \ a + 1 = 1 + a\}$ $0 \in M''$, infatti $0 + 1 = 1 + 0$, perché $1 \in M'$. Se $a \in M''$, cioè $a + 1 = 1 + a$, verifichiamo che $a' \in M''$. $a' + 1 = (a + 0') + 1 = (a + 1) + 1 = (1 + a) + 1 = 1 + (a + 1) = 1 + a'$. Dunque da $a \in M''$,segue $a' \in M''$, ovvero, per il principio di induzione, $M'' = \mathbb{N}$. Si trae, pertanto, che in tutto $\mathbb{N}$ vale la proprietà che ogni numero a è commutabile con 1 $(a + 1 = 1 + a)$.

Proviamo infine che $\forall a, b \in \mathbb{N}$, vale la proprietà commutativa. Sia $\overline{M} = \{b \in \mathbb{N} : \ a + b = b + a, \ \forall a \in \mathbb{N}\}$ $0 \in \overline{M}$ perché $M' = \mathbb{N}$. Sia $b \in \overline{M} \ \Rightarrow \ a + b' = a + (b + 1) = (a + b) + 1 = (b + a) + 1 = b + (a + 1) = b + (1 + a) = (b + 1) + a = b' + a$. Pertanto $b' \in \overline{M}$.

Per il principio di induzione $\overline{M} = \mathbb{N}$.

Si conclude che l'addizione è commutativa in $\mathbb{N}$. □

Elemento neutro Per la definizione e la proprietà commutativa dell'addizione si ha: $a + 0 = 0 + a = a \quad \forall a \in \mathbb{N}$. 0 è detto elemento neutro rispetto all'addizione.

Proprietà della cancellazione Dimostriamo che $k + n = m + n \ \Rightarrow \ k = m \quad (k, m, n \in \mathbb{N})$. Consideriamo $P = \{n \in \mathbb{N} : \ [(k + n = m + n) \ \Rightarrow \ k = m]\}$. $O \in P$, infatti $k + 0 = m + 0 \ \Rightarrow \ k = m$ per definizione. Se $n \in P$, proviamo che $n' \in P$. Se $k + n' = m + n' \ \Rightarrow \ (k + n)' = (m + n)'$. Se due numeri successivi sono uguali, allora anche i precedenti lo devono essere (postulato della iniettività dell'applicazione "successivo"). Dunque $k + n = m + n$ e, per l'ipotesi induttiva, si trae $k = m$. Quindi $n' \in P \ \Rightarrow \ P = \mathbb{N}$.

Proprietà Se $m + n = 0 \ \Rightarrow \ m = n = 0$

Supponiamo per assurdo $n \neq 0$, allora n è successivo di qualche numero. Sia $n = p' \ \Rightarrow \ m + p' = (m + p)' = 0$. Questa conclusione è assurda, in quanto lo 0 è successiva del numero $m + p$, contro il postulato $(A2)$. Analogamente si ragiona se $m \neq 0$.

3.3.4 La moltiplicazione in $\mathbb{N}$

Definizione 7. Si definisce prodotto di due numeri naturali a,b il numero naturale, che si indica con $a \cdot b$, tale che : $\begin{cases} a \cdot 0 = 0 \\ a \cdot b' = a \cdot b + a \end{cases}$ L'applicazione di $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, che associa alla coppia (a, b) il numero $a \cdot b$, si dice moltiplicazione.

Mediante il principio di induzione proviamo che la moltiplicazione è ovunque definita in $\mathbb{N}$. Sia $S = \{b \in \mathbb{N} : \forall a \in \mathbb{N} \quad a \cdot b \text{ risulta definita}\}$ $0 \in S$ per definizione. Se $b \in S$, verifichiamo che $b' \in S$. Infatti: $a \cdot b' = ab + a$ e poiché $a \cdot b$ è definita $\Rightarrow$ $b' \in S$. Pertanto, $S = \mathbb{N}$.

Teorema 4. Soltanto lo zero non è successivo di alcun numero.
Ossia $n = m' \Leftrightarrow n \neq 0$.

Dimostrazione. L'implicazione $\Rightarrow$ discende dal postulato (A1); se n è successivo di qualche numero allora è non nullo.

$\Leftarrow$ Supponiamo, per assurdo, che esista $\overline{0} \in \mathbb{N}$, $\overline{0} \neq 0$, non successivo di alcun numero. Ovvero, $\exists \overline{0} \neq 0 \; e \; \overline{0} \notin \sigma(\mathbb{N})$.

Consideriamo l'insieme S così definito: $S = \mathbb{N} - \{\overline{0}\}$, $0 \in S$ per come è definito S. $n \in S \Rightarrow n' \in S$ per lo stesso motivo.

In base al principio di induzione, risulta $S = \mathbb{N}$, contro l'ipotesi che $S = \mathbb{N} - \overline{0}$ □

Proprietà distributiva a destra della moltiplicazione rispetto all'addizione Proviamo che $(a + b) \cdot c = a \cdot c + b \cdot c \; \forall a, b, c \in \mathbb{N}$

Dati a, b, definiamo così l'insieme $M = \{c \in \mathbb{N} : (a+b) \cdot c = a \cdot c + b \cdot c\}$ $0 \in M$, infatti $(a+b) \cdot 0 = 0$ e $a \cdot 0 + b \cdot 0 = 0 + 0 = 0$. Quindi, $(a+b) \cdot 0 = 0 = a \cdot 0 + b \cdot 0$. Supponiamo $c \in M$ e verifichiamo che $c' \in M$: $(a+b) \cdot c' = (a+b) \cdot c + (a+b) = a \cdot c + b \cdot c + a + b = a \cdot c + a + b \cdot c + b = (a \cdot c + a) + (b \cdot c + b) = a \cdot c' + b \cdot c'$. Ossia $(a + b) \cdot c' = a \cdot c' + b \cdot c' \Rightarrow c' \in M$. Sempre per il principio di induzione $\Rightarrow$ $M = \mathbb{N}$.

Proprietà commutativa. Dimostriamo che $a \cdot b = b \cdot a \; \forall a, b \in \mathbb{N}$
Consideriamo $M = \{b \in \mathbb{N} : \; 0 \cdot b = b \cdot 0\}$ $0 \in M$ in quanto $0 \cdot 0 = 0 \cdot 0 = 0$. Sia $b \in M$, allora risulta: $0 \cdot b' = 0 \cdot b + 0 = 0 + 0 = 0$ $b' \cdot 0 = 0 \Rightarrow b' \in M$. Cioè $M = \mathbb{N}$.

Fissato $a \in \mathbb{N} - \{O\}$, esaminiamo l'insieme $S = \{b \in \mathbb{N} : a \cdot b = b \cdot a\}$, $0 \in S$ perché $a \cdot 0 = 0$ e $0 \cdot a = 0 \Rightarrow 0$ è commutativo con ogni $a \in M$. Dunque $0 \in S$.

Sia $b \in S$ e proviamo allora che $b' \in S$. $a \cdot b' = a \cdot b + a = b \cdot a + a = (b + 1) \cdot a = b' \cdot a$ Pertanto $b' \in S \Rightarrow S = \mathbb{N}$([8])

Elemento neutro Abbiamo posto $0' = 1$.
Si ha allora $a \cdot 0' = a \cdot 0' + a = 0 + a = a \Rightarrow a \cdot 1 = a$. Quindi $a \cdot 1 = 1 \cdot a = a \; \forall a \in \mathbb{N}$. 1 è detto elemento neutro rispetto alla moltiplicazione.

Proprietà associativa Constatiamo che $a \cdot (b \cdot c) = (a \cdot b) \cdot c \; \forall a, b, c \in \mathbb{N}$.
Consideriamo l'insieme $M = \{c \in \mathbb{N} : \; a \cdot (b \cdot c) = (a \cdot b) \cdot c\}$, $0 \in M$, infatti $a \cdot (b \cdot 0) = a \cdot 0 = 0$, $(a \cdot b) \cdot = 0$ quindi $a \cdot (b \cdot 0) = (a \cdot b) \cdot 0$.

Se $c \in M$, verifichiamo che $c' \in M$

$a \cdot (b \cdot c') = a \cdot (b \cdot c + b) = a \cdot (b \cdot c) + a \cdot b = (a \cdot b) \cdot c + (a \cdot b) \cdot c + (a \cdot b) \cdot 1 = (a \cdot b) \cdot (c + 1) = (a \cdot b) \cdot c'$.

Dunque $c' \in M \quad \Rightarrow \quad M = \mathbb{N}$, cioè la moltiplicazione è un'operazione associativa su tutto $\mathbb{N}$.

[8] Poiché vale la proprietà distributiva a destra e la proprietà commutativa, resta verificata anche la proprietà distributiva a sinistra. Infatti : $c \cdot (a+b) = (a+b) \cdot c = a \cdot c + b \cdot c \; \forall a, b, c \in \mathbb{N}$

3.4 Relazione d'ordine in $\mathbb{N}$

Dati $a, b \in \mathbb{N}$ definiamo in $\mathbb{N}$ la seguente relazione binaria, indicata con il segno $\leq$:
$a \leq b \Leftrightarrow \exists n \in \mathbb{N} : \ b = a + n$.
$a \leq b$ si legge a minore o uguale a b.
La relazione risulta essere d'ordine.
È riflessiva: $a \leq a, \forall a \in \mathbb{N}$, poiché $a = a + 0$
È antisimmetrica.
Siano dunque $a \leq b$ e $b \leq a$
$a \leq b \ \Rightarrow \ \exists \, x \in \mathbb{N} : \ a + x = b$
$b \leq a \ \Rightarrow \ \exists y \in \mathbb{N} : \ b + y = a$
Si ha: $a + (x + y) = (a + x) + y = b + y = a \ \Rightarrow \ x + y = 0 \ \Rightarrow \ x = y = 0$
Ossia $a = b$
È transitiva.
Supponiamo $a \leq b$ e $b \leq c$
$a \leq b \ \Rightarrow \ \exists x \in \mathbb{N} : \ b = a + x$
$b \leq c \ \Rightarrow \ \exists y \in \mathbb{N} : \ c = b + y$
Pertanto, $c = (a + x) + y = a + (x + y) \ \Rightarrow \ a \leq c$

Teorema 5. La relazione $\leq$ è di ordine totale in $\mathbb{N}$. Ovvero, presi due elementi qualsiasi $a, b \in \mathbb{N}$, sussiste una ed una sola delle seguenti eventualità:

I) $a = b$;

II) $a < b$, cioè $b = a + n$ con $n \neq 0$;

III) $b < a$, cioè $a = b + m$ con $m \neq 0$;

Dimostrazione. Ricordando che $\begin{cases} a + n = a + m & \Rightarrow \quad n = m \\ n + m = 0 & \Rightarrow \quad n = m = 0 \end{cases}$ supponiamo, per assurdo, che valgono contemporaneamente i casi I e II. Quindi, $a = b$ e $b = a + n (n \neq 0) \ \Rightarrow \ a = a + n \ \Rightarrow \ a + 0 = a + n \ \Rightarrow \ n = 0$, contro l'ipotesi fatta.

Si conclude allora che le circostanze I e II sono incompatibili.

Analogamente si prova che anche I e III sono incompatibili.

Supponiamo ora che valgono contemporaneamente II e III: $b = a + n \ (n \neq 0)$ e $a = b + m \ (m \neq 0) \ \Rightarrow \ a = a + n + m \ \Rightarrow \ n + m = 0 \ \Rightarrow \ n = 0$ e $m = 0$; contro l'ipotesi fatta.

Pertanto la validità di una relazione esclude quella delle altre due. □

N.B.: al posto di $a \leq b$ si scrive anche $b \geq a$ e si legge b maggiore o uguale ad a.

Dimostriamo ora che vale sempre almeno una delle eventualità.

Fissato un elemento $a \in \mathbb{N}$, consideriamo l'insieme
$S = \{b \in \mathbb{N} : \text{ vale o la I, o la II, o la III}\}$. Se $a = 0 \ \Rightarrow \ b = 0 \in S$ perché vale la I. Se $a \neq 0 \ \Rightarrow \ b = 0 \in S$ perché $a = 0 + a \ \Rightarrow \ a > 0$, vale dunque la III.

Supposto che $b \in S$, poniamo che $b' \in S$. Distinguiamo, infatti, i seguenti casi:

1) Se vale la I, cioè $b = a \ \Rightarrow \ b' = a + 1 \ \Rightarrow \ a < b' \ \Rightarrow$ vale la II. Pertanto $b' \in S$.

2) Se vale la II, cioè $a < b, b = a+m$ con $m \neq 0$. Risulta allora: $b' = (a+m)' = a + m'$ con $m' \neq 0$. Dunque $b' = a + m' => a < b'$. Vale la II $\Rightarrow\ b' \in S$.

3) Se vale la III, cioè $b < a$, si ha $a = b + m$ con $m \neq 0$. Consideriamo due sottocasi:

   a) Sia m il successivo di un numero non nullo r, ovvero $m = r'$ con $r \neq 0$, allora si ottiene: $a = b + r' = (b + r)' = (r + b)' = r + b' = b' + r$. Ovvero $a = b' + r$ con $r \neq 0$ dunque $a > b'$. Il numero b' soddisfa la III $\Rightarrow\ b' \in S$.

   b) Supponiamo che m sia successivo dello zero, cioè $m = 0'$.
   Si ha: $a = b + m = b + 0' = b + 1 = b'$.
   Pertanto $a = b'$, vale così la I $\Rightarrow\ b' \in S$

   In conclusione, comunque si fissi $a \in \mathbb{N}$ e comunque si scelga $b \in S$, il successivo $b' \in S$, cioè:
   $0 \in S$
   $b \in S\ \Rightarrow\ b' \in S\ \Rightarrow\ S = \mathbb{N}$.

   Pertanto in $\mathbb{N}$ l'ordine è totale, cioè presi due qualsiasi elementi sono confrontabili in uno e in un solo modo.

La relazione $<$ definita in $\mathbb{N}$ è legata alle due operazioni, nel senso delle due proposizioni:

Proposizione 1. $a < b\ \Rightarrow\ a + c < b + c \quad \forall c \in \mathbb{N}$

Dimostrazione. Da $a < b$ segue $b = a + n$ con $n \neq 0$. Quindi $b + c = a + c + n$, da cui $a + c < b + c$ □

Proposizione 2. $a < b\ \Rightarrow\ a \cdot c < b \cdot c \quad \forall c \in \mathbb{N} - \{0\}$

Dimostrazione. Per ipotesi si ha $b = a + n$ con $n \neq 0$. Moltiplicando il primo e il secondo membro dell'uguaglianza per $c \neq 0\ \Rightarrow\ b \cdot c = (a + n) \cdot c = a \cdot c + n \cdot c$ con $n \cdot c \neq 0\ \Rightarrow\ a \cdot c < b \cdot c$.
Se $c \geq 0$, si ottiene da $a < b$, $a \cdot c \leq b \cdot c$ □

Teorema 6. L'ordine in $\mathbb{N}$ è archimedeo. Ovvero, presi due suoi elementi, non nulli $a, b\ \exists c \in \mathbb{N} :\ a < b \cdot c$.

Dimostrazione. È sufficiente scegliere $c \in \mathbb{N} :\ a < c$. Moltiplichiamo adesso entrambi i membri della disuguaglianza per $b\ \Rightarrow\ ba < bc$. Poiché $b \neq 0\ \Rightarrow\ 1 \leq b\ \Rightarrow\ 1 \cdot a \leq ba\ (a \neq 0)\ \Rightarrow\ a \leq ba$. Pertanto, $a \leq ba < bc\ \rightarrow\ a < bc$. □

Teorema 7. In $\mathbb{N}$ non esiste un elemento compreso fra un elemento ed il suo successivo, cioè, $\nexists b \in \mathbb{N} :\ a < b < a + 1$.

Dimostrazione. Supponiamo, per assurdo, che esista un tale elemento: $\exists b \in \mathbb{N} :\ a < b$. Quindi $\exists n \in N - \{0\} :\ b = a + n$. Ora, poiché $n \neq 0$ è successivo di qualche numero, risulta $b \geq a + 1$. Si ha allora $a + 1 \leq b$ e per ipotesi $b < a + 1$,ossia $a + 1 < a + 1$. Assurdo! □

In particolare fra 0 ed il successivo, 1, non ci sono altri numeri naturali.

3.5 Minimo e massimo dei sottoinsiemi di $\mathbb{N}$

Teorema 8. Ogni sottoinsieme K di numeri naturali, non vuoto, ha un minimo.

Dimostrazione. Sia P_n la proposizione: "ogni numero di K è $\geq n$".

Evidentemente la proposizione P_0 è vera. D'altra parte, non per ogni n la proposizione P_n è vera: $K \neq \varnothing\ \exists m \in K :\ P_{m+1}$ non è vera. Ne segue che l'implicazione $P_n \rightarrow P_{n+1}$ non è valida per ogni n: esiste dunque un numero $\overline{n}$ tale che $P_{\overline{n}}$ è vera e la $P_{\overline{n}+1}$ è falsa. Ciò significa: ogni numero di K è $\geq \overline{n}$ ed esiste in K almeno un numero minore di $\overline{n}+1$, dunque $\leq \bar{n}$.

Un tale numero di K, essendo $\geq \overline{n}$ e $\leq \overline{n}$, è necessariamente $\overline{n}$. Dunque,$\overline{n} \in K$ ed ogni numero di K è $\geq \overline{n}$, cioè come si vuole per affermare che $\overline{n}$ è il minimo di K. □

Evidentemente, esistono invece insiemi non vuoti di numeri naturali privi di massimo: tale è, ad esempio, l'insieme $\mathbb{N}$ stesso ed ogni insieme del tipo $\{n \in N :\ n \geq k\}$, quale che sia $k \in \mathbb{N}$.

Definizione 8. Un insieme ($E \subset \mathbb{N}$) si dice superiormente limitato se esiste un numero h tale che $n \in E$ implica $n \leq h$.

Ogni numero h è detto una limitazione superiore per l'insieme E.

Teorema 9. Ogni insieme E di numeri naturali non vuoto e superiormente limitato ha un massimo.

Dimostrazione. Sia P_n la proposizione: "esiste in E almeno un numero $\geq n$". La P_0 è vera, essendo E non vuoto. D'altra parte, non per ogni n P_n è vera, essendosi supposto E superiormente limitato. Ne segue che l'implicazione $P_n \rightarrow P_{n+1}$ non è valida per ogni n; esiste dunque un numero m tale che P_m è vera e la P_{m+1} è falsa.

Ciò significa che esiste in E almeno un numero $\geq m$, ed ogni numero di E è $< m+1$. Un tale numero è necessariamente m. Dunque, $m \in E$ e ogni numero di E è minore di $m+1$, quindi $\leq m$; ciò è quanto si vuole per affermare che m è il massimo di E. □

$\mathbb{N}$, insieme totalmente ordinato, si dice bene ordinato in quanto ogni suo sottoinsieme non vuoto ha minimo. Dal buon ordinamento di $\mathbb{N}$ segue un'altra formulazione del principio di induzione completo.

Teorema 10. Ad ogni numero naturale n sia associata una proposizione P_n. Se, per un $\overline{n} \in \mathbb{N}$, $P_{\overline{n}}$ è vera e se sono vere tutte le P_r con $\overline{n} \leq r < n$, segue che è vera anche P_n, allora P_n è vera per ogni $n > \overline{n}$.

Dimostrazione. Sia $E = \{n \in N :\ n \geq \overline{n}$ e $P_n\ falsa\}$. Supponiamo, per assurdo, che $E \neq \varnothing$. Allora E, sottoinsieme non vuoto di numeri naturali, ammette un elemento minimo k. Evidentemente $k > \overline{n}$. Per tutti i numeri r tali che $\overline{n} \leq r < k$, la P_r è vera, pertanto è vera anche la P_k. Assurdo quindi $E = \varnothing \rightarrow P_n$ è vera per ogni $n > \overline{n}$. □

3.5.1 osservazione conclusiva

L'insieme $\mathbb{N}$ è dotato delle operazioni di addizione (associativa, commutativa, esistenza dell'elemento neutro) e di moltiplicazione (associativa, commutativa,

distributiva rispetto all'addizione, esistenza dell'elemento neutro). Inoltre $\mathbb{N}$ è un insieme totalmente ordinato e bene ordinato; tale ordine infine è compatibile con la struttura algebrica, cioè con le operazioni (proporzione 1, proporzione 2).

3.6 Postulati dell'ordine sui numeri naturali

Nell'insieme $\mathbb{N}$ è definita una relazione d'ordine detta "ordine naturale", che viene indicata col segno $<$, al quale, come è noto, si dà significato irriflessivo mentre si usa il segno $\leq$ col significato "$<$ oppure $=$".

L'ordine naturale in $\mathbb{N}$ soddisfa i seguenti postulati:

I) $\mathbb{N}$ è un insieme totalmente ordinato;

II) Ogni sottoinsieme non vuoto di $\mathbb{N}$ ha un minimo. indichiamo con 0 il minimo di $\mathbb{N}$.

III) Ogni numero ha un immediato seguente o un successivo (ossia $\forall n \in \mathbb{N}; \exists n' \in \mathbb{N}$ tale che $n < n'$ e tale che $n < x \leq n' \ \rightarrow \ x = n'$);

III') $\forall n \in \mathbb{N}$ l'insieme $S_n = \{m \in \mathbb{N} : \ n < m\} \neq \varnothing$. Detto $n' = \min S_n$, n' è il successivo di n;

IV) Ogni numero $\neq 0$, è successivo di qualche altro.

Tali postulati definiscono lo stesso insieme $\mathbb{N}$ dei numeri naturali. Gli enti primitivi sono: ordine e numero.

Dimostriamo ora l'equivalenza dei postulati dell'ordine con quelli di Peano.

$$Ordine \ \underset{\Leftarrow}{\overset{A}{\Rightarrow}} \ Peano$$

Per i postulati (II) e (III), definiamo un'applicazione σ che dia il minimo dei "successivi". Cioè $\sigma : \mathbb{N} \to \mathbb{N}$ con $\sigma(n) = \min S_n$, dove $S_n = \{m \in \mathbb{N} : \ n < m\}$ Tale minimo è unico in quanto $\mathbb{N}$ è un insieme totalmente ordinato.

Dimostrazione. $\overset{A}{\Rightarrow}$ Resta così verificato che σ è una applicazione di $\mathbb{N}$ in $\mathbb{N}$. Proviamo che σ è iniettiva. Supponiamo $\sigma(m) = \sigma(n)$. Se fosse $m > n$ si avrebbero le due circostanze:

1) $m = \sigma(n) \ \Rightarrow \ \sigma(m) > m = \sigma(n)$

2) $m > \sigma(n) \ \Rightarrow \ \sigma(m) > m = \sigma(n)$

In ogni caso, dunque, $\sigma(m) > \sigma(n)$. Se invece $m < n$ si concluderebbe, in modo analogo, che $\sigma(m) < \sigma(n)$. Necessariamente deve essere $m = n$.

Pertanto abbiamo definito un'applicazione σ del "successivo" che soddisfa i postulati (A1) e (A3) di Peano.

Per il postulato (IV) si ha: $0 \notin S_n, \ \forall n \in \mathbb{N} \ \Rightarrow \ 0 \notin \sigma(\mathbb{N})$. Vale perciò il postulato (A2) di Peano.

Verifichiamo, infine, che vale il principio di induzione.

Ovvero: se $S \subset \mathbb{N}$ e S soddisfa le condizioni: $\alpha)$ $0 \in S$; $\beta)$ se $n \in S \ \Rightarrow \ n' \in S \ \Rightarrow \ S = \mathbb{N}$

Per assurdo $S \neq \mathbb{N}$. Indichiamo con $S' = \mathbb{N} - S$. Per l'ipotesi fatta, S', complementare di S rispetto ad $\mathbb{N}$, non è vuoto. Tale S', in base al postulato

(II), ha un minimo: sia $\overline{m} = \min S'$. Poiché $0 \in S \ \rightarrow \ 0 \notin S'$, dunque $\overline{m} \neq 0$. Per il postulato (IV), $\overline{m}$ è il successivo di qualche numero, cioè $\overline{m} = n'$. Ma $n \in S$ e $n' \notin S$. Assurdo!

Dunque vale anche il postulato (A4) di Peano. □

Dimostrazione. $\overset{B}{\Longleftarrow}$ Mostriamo che dai postulati di Peano seguono quelli dell'ordine:

(I) $\mathbb{N}$ è un insieme totalmente ordinato: già verificato.

(II) S sottoinsieme non vuoto ha un minimo: già verificato

(III) Ogni numero ha un immediato seguente: in base al postulato (A1) di Peano.

(IV) Ogni numero $\neq 0$ è successivo di qualche altro.

Dimostrazione. Per assurdo supponiamo che esista $\alpha \in N - \{0\}$ tale che, $\forall n \in \mathbb{N}, \ \alpha \neq n'$. Consideriamo l'insieme $S = \mathbb{N} - \{\alpha\}$. $0 \in S$, perché $\alpha \neq 0$. Se $n \in S \ \rightarrow \ n' \in S$, dato che è escluso solo α. Dunque $S = \mathbb{N}$.

Non può esistere, pertanto, un numero α come quello ipotizzato. □

□

3.7 La divisione in $\mathbb{N}$

Teorema 11. Dati due numeri naturali qualunque a, b con $b \neq 0$, esiste una e una sola coppia di numeri (q, r) soddisfacente alle due condizioni: $a = qb + r$, $0 \leq r \leq b - 1$.

Dimostrazione. Consideriamo l'insieme dei multipli di b : $0, b, 2b, 3b, \ldots, nb, \ldots$ il quale è privo di massimo poiché , essendo $b \neq 0$, ognuno di essi è superato dal seguente; pertanto l'insieme stesso è superiormente illimitato. Dunque esistono multipli di b maggiori di a. Consideriamo allora l'insieme $\{k \in \mathbb{N} : kb > a\}$: esso ha minimo, che indichiamo con $q + 1$. Si ha dunque $qb \leq a < (q + 1)b$. Da $qb \leq a \ \Rightarrow \ \exists r \geq 0 : \ a = qb + r$. Esiste pertanto la coppia (q, r). Inoltre dalla $a < (q + 1)b \ \Rightarrow \ \exists c > 0 : \ (q + 1)b = a + c$. Cioè $qb + b = a + c$. Ma $a = qb + r \ \Rightarrow \ qb + b = qb + r + c \ \Rightarrow \ b = r + c$ con $c > 0$. Ossia $r < b$.

Proviamo l'unicità della coppia. Sia $a = qb + r = q'b + r'$, con $r < b$, $r' < b$. Supposto, ad esempio, $q \leq q'$, dunque $q' = q + h$, si ha $qb + r = (q+h)b+r' \implies r = hb+r'$. Quest'ultima uguaglianza implica $h = 0$ e dunque $q = q'$. Essendo allora tanto r quanto r' soluzioni dell'equazione $a = qb + x$. se ne deduce $r = r'$. □

La legge che alla coppia (a, b) associa la detta coppia (q, r) si dice divisione di a per b: q ed r si dicono rispettivamente il quoziente e il resto della divisione stessa.

3.7.1 Divisibilità

Se a, b sono due numeri naturali, si dice che b è multiplo di a oppure che a è un divisore di b o che b è divisibile per $a \Leftrightarrow \exists k \in \mathbb{N} : \ b = ka$.

N.B. 0 è multiplo di ogni numero naturale. Infatti: $0 = 0n \ \forall n \in \mathbb{N}$.

Definiamo la relazione binaria « divisore »([9]) che indichiamo con $|$: $a \,|b \ \Leftrightarrow \exists k \in \mathbb{N} : \ b = ka$.

Essa è una relazione d'ordine non totale.

È riflessiva: $a \,|a \ \forall a \in \mathbb{N}$. Infatti $\exists 1 \in \mathbb{N} : \ a = 1 \cdot a$

È antisimmetrica: $a \,|b \ \Rightarrow \ \exists k : \ b = ka \ b \,|a \ \Rightarrow \ \exists h : \ a = hb$ e pertanto si ha $a = h(ka) = (hk)a \ \Rightarrow \ hk = 1 \ \Rightarrow \ h = k = 1 \implies a = b$.

Risulta infine transitiva: $a \,|b \,, b \,|c \ \Rightarrow a \,|c$, infatti $b = ka, c = hb \Rightarrow c = hka$.

Osserviamo che $a \nmid b$ non implica $b \,|a$, ad esempio , $2 \nmid 5$ e $5 \nmid 2$. Dunque l'ordine non è totale. Se $a, b, c \in \mathbb{N}$, risulta evidente che: $a \,|b \ \Rightarrow \ a \,|bc$; $a \,|b = ac \,|bc \ (c \neq 0)$; $a \,|b \,, \ a \,|c \ \Rightarrow \ a \,|(b + c)$, ed anche $a \,|(b - c)$ se $b > c$.

N.B. Ogni numero naturale $n > 1$ ammette almeno due divisori: l'unità 1 e il numero stesso n.

Definizione 9. Un numero naturale maggiore di 1 si dice primo se è divisibile solo per se stesso e per l'unità.

In $\mathbb{N} - \{0\}$ consideriamo le seguenti tre classi di numeri:

a) la classe costituita dal numero 1, che non si considera primo;

b) quella formata dai numeri > 1, che non hanno divisori propri, cioè diversi dall'unità e da se stessi (numeri primi);

c) la classe formata dai numeri > 1 che hanno divisori propri (numeri composti).

Queste tre classi costituiscono una partizione di $\mathbb{N} - \{0\}$.

Ogni numero composto si può esprimere mediante determinati numeri primi minori di esso e moltiplicati fra loro. Sussistono, infatti, le seguenti proposizioni:

Teorema 12. Il divisore minimo, diverso da 1, di un numero composto è un numero primo.

Dimostrazione. Sia a un numero composto: come tale, avrà anche divisori diversi da 1 e da a stesso.

Sia p il minimo divisore di a, diverso da 1: tale numero p deve essere primo. Infatti, se non lo fosse, ammetterebbe a sua volta un divisore $d < p$ e questo, essendo p divisore di a, sarebbe anch'esso divisore di a.

Così a avrebbe un divisore d minore di p e diverso da 1, contro l'ipotesi ammessa che p sia il minimo divisore di a, diverso da 1. Vuol dire allora che p non può essere composto, quindi è un numero primo. □

Teorema 13. Ogni numero composto è uguale a un prodotto di fattori primi.

Dimostrazione. Sia a un numero composto. Poiché il minimo divisore p di $a \neq 1$, è un numero primo, si ha: $a = pq$.

Se q è primo, come lo è p, il numero a risulta uguale al prodotto pq di due fattori primi e il teorema è dimostrato.

[9] $a \,|b$ si legge a divide b, cioè a è un divisore di b.

Se invece q non è primo, il suo minimo divisore $\neq 1$ è un numero primo p' (che potrebbe anche essere uguale a p), per cui si ha: $q = p'q' \Rightarrow a = pp'q'$.

Se q' è primo, a risulta uguale al prodotto di tre fattori primi e il teorema è dimostrato. Se q' non è primo, il suo minimo divisore $\neq 1$ è un numero primo p'' e si ha: $q' = p''q'' \Rightarrow a = pp'p''q''$.

Se q'' è primo, il teorema è dimostrato ... e così si continua col medesimo ragionamento. Poiché i numeri $q, q', q'', \ldots$ sono decrescenti la loro successione termina con un numero primo. Il teorema è così dimostrato. □

Teorema 14. Il prodotto di fattori primi in cui si può scomporre un dato numero composto è unico.

Dimostrazione. Sia a un numero composto. Supponiamo che esso ammetta due scomposizioni in fattori primi. Quindi: $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot ... \cdot q_s^{\beta_s}$.

Ogni p_i $(1 \leq i \leq r)$ si trova fra i $q_j (1 \leq j \leq s)$, poiché il prodotto $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$ è divisibile per p_i e tale è anche il prodotto $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot ... \cdot q_s^{\beta_s}$.

Allora almeno uno dei fattori di $q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_s^{\beta_s}$ è divisibile per p_i ed essendo $q_1, q_2, ..., q_s$ primi, resta verificata da tutti i p_1 che compaiono fra i q_j.

Con ragionamento del tutto analogo si prova che i q_j si trovano fra i p_i.

Si ricava per tanto che $p_i = q_j$. Sia allora: $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \cdots \cdot q_r^{\beta_r}$. Proviamo che gli esponenti sono pure uguali. Sia invece, ad esempio, $\alpha_1 > \beta_1$. Ciò implica che $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$ e $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r}$ sono divisibili per $p_1^{\beta_1}$ (per la potenza cioè elevata ad esponente non maggiore) e quindi si ha: $\overline{a} = \dfrac{a}{p_1^{\beta_1}} = p_1^{\alpha_1 - \beta_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r} = 1 \cdot p_2^{\beta_2} \cdot \cdots \cdot p_r^{\beta_r}$. Ma allora si contraddice quanto dimostrato nella prima parte del ragionamento: il primo prodotto avrebbe il fattore p_1, mentre il secondo non lo avrebbe. Perciò $\alpha_1 = \beta_1$ e così via $\alpha_i = \beta_i$ per ogni $i = 1, 2, \ldots, r$. □

Osservazione Tutti i numeri primi p, esclusi 2 e 3, si possono scrivere nella forma: $p = 6n \pm 1$ con $n \in \mathbb{N} - \{0\}$.

Teorema 15. Esistono infiniti numeri primi.

Dimostrazione. Supponiamo, per assurdo, che p sia il più grande numero primo e consideriamo il numero naturale così definito:
$M = (2 \cdot 3 \cdot 5 \cdot 7 \cdot ... \cdot p) + 1$. M risulta pertanto il prodotto di tutti i numeri primi minori o uguali a p aumentato di 1. Evidentemente M non è divisibile per alcuni dei numeri primi compresi fino a p ed oltre $M > p$. Si possono avere allora due casi:

i) M è un nuovo numero primo e il teorema resta così dimostrato;

ii) M non è primo.

In questo caso ha tutti i divisori primi maggiori di p. Infatti, dividendo M per 2 o per 3 o per 5 o ... o per p si ottiene come resto sempre 1. □

Minimo comune multiplo ($lcm(.)$) fra due numeri $a, b \in \mathbb{N} - \{0\}$.

Due numeri $a, b \in \mathbb{N} - \{0\}$ hanno sempre multipli in comune (almeno il loro prodotto ab). Se consideriamo l'insieme dei multipli comuni di a, b tale sottoinsieme di $\mathbb{N} - \{0\}$ ha un minimo.

Pertanto esiste il minimo comune multiplo, che indichiamo con $lcm(a, b)$.

Teorema 16. Se il numero M è multiplo comune di a e b, allora M è multiplo del loro minimo comune multiplo, cioè $lcm(a,b)$.

Dimostrazione. Sia $m = lcm(a,b)$. Per assurdo, diciamo che M non è multiplo di $m \Rightarrow M = qm + r$ con $0 < r < m$. M è multiplo di a e $b \Rightarrow M = aM'$, $M = bM''$, m è multiplo di a e $b \Rightarrow m = am'$, $m = bm''$. Pertanto $r = M - qm = \begin{cases} aM' - am'q = a(M' - m'q) \\ bM'' - bm''q = b(M'' - m''q) \end{cases}$ quindi r risulta multiplo comune di a e b. Poiché $m > r$, m non è più il minimo, contro l'ipotesi. □

Massimo comune divisore ($gcd(.,.)$) fra due numeri $a, b \in \mathbb{N} - \{0\}$
Divisori comuni di due numeri esistono sempre, basti pensare all'unità.

Consideriamo l'insieme dei divisori comuni di due numeri $a, b \in \mathbb{N} - \{0\}$ esso è un insieme superiormente limitato (i divisori comuni non possono superare il minore fra a e b), quindi deve ammettere un massimo, che indichiamo con $gcd(a,b)$.

Definizione 10. Due numeri a e b sono primi fra loro (o coprimi) se e solo se $gcd(a,b) = 1$

Lemma 1. Dati $a, b \in \mathbb{N} - \{0\}$, supponiamo che sia: $ab = \delta n$ allora risulta:

1) Se δ è un divisore comune di a e b allora n è multiplo comune di a, b.

2) Se n è multiplo comune di a e b allora δ è un divisore comune di a, b.

Dimostrazione. 1) Se δ è un divisore comune di a e b, si ha $a = a'\delta$, $b = b'\delta$. Da $ab = \delta n \Rightarrow a'\delta b'\delta = \delta n \Rightarrow \begin{cases} (a'\delta)b'\delta = \delta n \Rightarrow ab' = n \\ a'\delta(b'\delta) = \delta n \Rightarrow a'b = n \end{cases}$ Si vede quindi che n è multiplo di a e anche di b.

2) Poiché n è multiplo di a e di b, si ha: $n = ha$, $n = kb$. Dunque $ab = \delta n \Rightarrow ab = \delta ha \Rightarrow b = \delta h$. Analogamente $ab = \delta n \Rightarrow ab = \delta kb \Rightarrow a = \delta k$. Anche qui si vede subito che δ è divisore sia di a che di b.

□

Teorema 17. Dati due numeri $a, b \in \mathbb{N} - \{0\}$ e indicati con $m = lcm(a,b)$ e $d = gcd(a,b)$ si ha $ab = md$.

Dimostrazione. Poiché d è divisore comune di a e b, si ha $ab = nd$. Allora n, in base al lemma precedente, è multiplo comune di a e b, ovvero n è multiplo di m. Poniamo $n = km$. Di seguito, $ab = nd = kmd = m(kd)$. Essendo m multiplo comune di a e b, si trae che kd è divisore comune. Deve essere $k = 1$, altrimenti esisterebbe un divisore comune maggiore di d, contro il fatto che questo è il massimo. Pertanto, $ab = md$. □

Teorema 18. I divisori comuni di a e b sono tutti e soli i divisori del loro massimo comune divisore d.

Dimostrazione. Supponiamo che δ sia un divisore comune di a e b allora $ab = \delta n$ ove n è multiplo comune (lemma precedente). Quindi $ab = dm \Rightarrow \delta km = dm \Rightarrow \delta k = d \Rightarrow \delta$ è un divisore di d. □

Teorema 19. Se $d = gcd(a,b)$, $d' = gcd(ac,bc)$ $(c \neq 0) \Rightarrow d' = dc$.

Dimostrazione. Poiché $d\,|a\,, d\,|b$ si ha $dc\,|ac$, quindi $dc\,|d'$. Poniamo $d' = dcn$. Essendo $ac = d'p = dcnp,\ bc = d'q = dcnq\ \Rightarrow\ a = dnp = (dn)p,\ b = dnq = (dn)q$. Segue che $dn\,|a\ ,\ dn\,|b\ \Rightarrow\ dn\,|d\ \wedge\ dc\,|bc\ \Rightarrow\ \ n = 1$. Pertanto $d'\,|dc$ □

Teorema 20. Se $c\,|ab\ \ e\ gcd(a,c) = 1\ \Rightarrow\ c\,|b$

Dimostrazione. La proprietà è vera se $b = 0$. Se $b \neq 0$, da $gcd(a,c) = 1$ segue, per il teorema precedente, $gcd(ab, bc) = b$. Quindi, se c, oltre a dividere ab, divide bc esso divide necessariamente b. □

Teorema 21. Se $gcd(a,b) = 1,\ a\,|c\ ,\ b\,|c\ \Rightarrow\ ab\,|c$

Dimostrazione. Possiamo supporre $c \neq 0$. Si ha:
$\left.\begin{array}{l} a\,|c\ \Rightarrow\ ab\,|bc \\ b\,|c\ \Rightarrow\ ab\,|ac \end{array}\right\}\ \Rightarrow\ ab\,|gcd(ac, bc)$ Poiché $gcd(ac, bc) = c$, si ha $ab\,|c$. □

Teorema 22. Se un prodotto di n fattori ($n \geq 2$) è multiplo di un numero naturale c e $n-1$ fattori sono primi con c, allora l'ennesimo fattore è multiplo di c.

Cioè: $a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1} \cdot a_n = kc, \quad gcd(a_i, c) = 1\ \forall i = 1, 2, \ldots n-1\ \Rightarrow\ c\,|a_n$.

Dimostrazione. Si ragiona per induzione.

La proposizione è vera per due fattori, supponiamola altrettanto vera per $n-1$ fattori. Sia dunque il prodotto in parentesi $(a_1 \cdot a_2 \cdot \cdots \cdot a_{n-2})$ primo con c. Vogliamo verificare che pure il prodotto $(a_1 \cdot a_2 \cdot \cdots \cdot a_{n-2} \cdot a_{n-1})$ è primo con c. Se così non fosse, si avrebbe $\gcd((a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1}), c) = d > 1$ e $\gcd(a_i, d) = 1$ per $i = 1, 2, ..., n-2$. Per l'ipotesi induttiva a_{n-1} è divisibile per d e ciò è assurdo in quanto a_{n-1} e c sono primi fra loro. Dunque il prodotto dei primi $n-1$ fattori è primo con c quindi si ritorna al caso del prodotto di due numeri $(a_1 \cdot a_2 \cdot \cdots \cdot a_{n-1}) \cdot a_n\ \Rightarrow\ a_n$ è multiplo di c. □

Corollario 1. Siano $p_1, p_2, \ldots, p_n$ numeri primi (non necessariamente distinti). Il loro prodotto $p = p_1 \cdot p_2 \cdot \cdots \cdot p_n$ non ha divisori primi all'infuori dei p_i stessi.

Osservazione Tenere conto di questo corollario quando si dimostra l'unicità della scomposizione di un numero in fattori primi.

3.7.2 L'algoritmo di Euclide

La ricerca del massimo comune divisore di due numeri naturali

Teorema 23. Per due numeri naturali a e b, non entrambi nulli, l'algoritmo può essere descritto, aritmeticamente, nel seguente modo. Supponiamo $b \neq 0$, in quanto $gcd(0, a) = a$. Allora, con successive divisioni, si può scrivere:

$$\begin{aligned}
a &= q_1 b + r_1 && (0 < r_1 < b)\\
b &= q_2 r_1 + r_2 && (0 < r_2 < r_1)\\
r_1 &= q_3 r_2 + r_3 && (0 < r_3 < r_2)\\
r_2 &= q_4 r_3 + r_4 && (0 < r_4 < r_3)\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n && (0 < r_n < r_{n-1})\\
r_{n-1} &= q_{n+1} r_n + 0 && (r_{n+1} = 0)
\end{aligned}$$

Osservando i secondi membri delle uguaglianze, si vede che i successivi resti formano una successione decrescente: $b > r_1 > r_2 > r_3 > r_4 > .... > 0$. Quindi, dopo al più b operazioni, si ottiene come resto lo 0.

Tesi: $gcd(a, b) = r_n$.

Dimostrazione. Che r_n sia divisore di a e b lo si verifica risalendo a ritroso le divisioni sopra eseguite: $r_n \,|r_{n-1}$, $r_n \,|r_{n-2}$ Così proseguendo, si deduce che $r_n \,|r_2$, $r_n \,|r_1$ e quindi $r_n \,|b$ e così pure $r_n \,|a$. Sia d un divisore comune di a e b. Esso è un divisore di r_1 e, con ragionamento analogo, di $r_2, \ldots, r_{n-1}$ e quindi di r_1. Si è trovato che ogni divisore comune di a e b è un divisore di $r_n \;\Rightarrow\; r_n = gcd(a, b)$ □

Problema 1. $gcd(44, 19) =?$
$44 : 19 = 2$
6
$19 : 6 = 3$
1
$6 : 1 = 6$
0
$\Rightarrow gcd(44, 19) = 1$

Problema 2. $gcd(204, 126) =?$
$204 : 126 = 1$
78
$126 : 78 = 1$
48
$78 : 48 = 1$
30
$48 : 30 = 1$
18
$30 : 18 = 1$
12
$18 : 12 = 1$
6
$12 : 6 = 2$
0
$\Rightarrow gcd(204, 126) = 6$

Teorema 24 (di Bezout)**.** Siano a, b due numeri naturali e sia $gcd(a, b) = d$. Allora esistono $x \in \mathbb{Z}$ e $y \in \mathbb{Z}$: $ax + by = d$.

Dimostrazione. Ricaviamo dalla sequenza di divisioni dell'algoritmo euclideo i vari resti:
$r_1 = a - q_1 b$
$r_2 = b - q_2 r_1$
$r_3 = r_1 - q_3 r_2$
$r_4 = r_2 - q_4 r_3$
...
...
...
$r_n = r_{n-2} - q_n r_{n-1}$
Consideriamo il primo resto. Da $r_1 = a - q_1 b$ segue che $\exists\ x_1 = 1,\ y_1 = -q_1$. Ossia $r_1 = ax_1 + by_1$. Per quanto riguarda il secondo resto, si ha: $r_2 = b - q_2 r_1 = b - q_2(ax_1 + by_1) = b - aq_2 x_1 - bq_2 y_1 = a(-q_2 x_1) + b(1 - q_2 y_1) \ \Rightarrow\ \exists\ x_2 = -q_2 x_1,\ y_2 = 1 - q_2 y_1$. Pertanto $r_2 = ax_2 + by_2$. Così proseguendo, si giunge a $d = r_n = ax + by$. □

Per esempio, vediamo come si ottengono x e y a partire da $a = 1854$ e $b = 252$. Applichiamo l'algoritmo euclideo:
$1854 = 252 \cdot 7 + 90$
$252 = 90 \cdot 2 + 72$
$90 = 72 \cdot 1 + 18$
$72 = 18 \cdot 4 + 0$
Pertanto $gcd(1854, 252) = 18$
Ricaviamo i vari resti:
$90 = 1854 - 252 \cdot 7$
$72 = 252 - 90 \cdot 2 = 252 - (1854 - 252 \cdot 7) \cdot 2 = 252 - 1854 \cdot 2 + 252 \cdot 7 \cdot 2 = 252 \cdot 15 - 1854 \cdot 2$
$18 = 90 - 72 \cdot 1 = 1854 - 252 \cdot 7 - (252 \cdot 15 - 1854 \cdot 2) =$
$1854 - 252 \cdot 7 - 252 \cdot 15 + 1854 \cdot 2 = 1854 \cdot 3 - 252 \cdot 22 = 1854 \cdot 3 + 252 \cdot (-22)$
In conclusione $x = 3$ e $y = -22$.

Osservazione : l'insieme $\mathbb{N} - \{0\}$ ordinato per "divisibilità" è un reticolo. Essendo che, nel caso in questione, i precedenti di un elemento sono i divisori, si ha che detti a, b due interi positivi, il loro massimo precedente comune è $gcd(a, b)$ e il loro minimo seguente comune è $lcm(a, b)$.

3.7.3 Funzioni aritmetiche

Le funzioni aritmetiche sono quelle funzioni definite in $\mathbb{N} - \{0\}$ con valori in $\mathbb{N} - \{0\}$, cioè del tipo $f : \mathbb{N} - \{0\} \ \rightarrow\ \mathbb{N} - \{0\}$

3.7.4 Funzione di Eulero

Si dice funzione φ di Eulero la funzione aritmetica che ad ogni numero naturale $m \geq 1$ associa il numero di naturali $0 < n < m$ che sono primi con m.
Cioè $\varphi(m) = |\{n \in \mathbb{N} :\ 0 < n < m,\ gcd(n, m) = 1\}|$.
Alcuni esempi:

- $\varphi(1) = 1$ perché 1 è primo con 1;
- $\varphi(2) = 1$ perché 1 è primo con 2;
- $\varphi(3) = 2$ perché 1,2 sono primi con 3;
- $\varphi(4) = 2$ perché 1,3 sono primi con 4;
- $\varphi(5) = 4$ perché 1,2,3,4 sono primi con 5;

Se $m = p$ è un numero primo, allora tutti i numeri tra 1 e $m-1$, non avendo divisori comuni con p, sono primi con p. Pertanto: $\varphi(p) = p - 1$.

Se $m = p^r$, con p primo, allora sono primi con m tutti i numeri compresi fra 1 e m che non sono multipli di p ovvero tutti ad eccezione di $1 \cdot p, 2 \cdot p, \ldots, p^{r-1} \cdot p$. Risulta pertanto $\varphi(m) = \varphi(p^r) = p^r - p^{r-1}$.

Esempi: $\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$
$\varphi(5^3) = 5^3 - 5^2 = 100$ Consideriamo l'anello $\mathbb{Z}_m$ delle classi di resto modulo m, con un numero naturale maggiore di uno.

Proposizione 3. Se $ac \equiv_m bc$ e $gcd(c, m) = 1$, allora $a \equiv_m b$.

Dimostrazione. Da $ac \equiv_m bc \;\Rightarrow\; ac - bc = km \;(k \in \mathbb{Z}) \;\Rightarrow\; (a-b)c = km$. E poiché $gcd(c, m) = 1$ segue che $a - b$ è multiplo di m. Dunque $a - b = hm$ $(h \in \mathbb{Z}); \Rightarrow\; a \equiv_m b$. □

Proposizione 4. Se $ac \equiv_m bc$, allora $a \equiv_{\frac{m}{d}} b$, dove $d = gcd(c, m)$.

Dimostrazione. Essendo $gcd(c, m) = d$, risulta $c = c'd$ e $m = m'd$ $(c', m' \in \mathbb{N})$. Da $ac \equiv_m bc \;\Rightarrow\; ac - bc = km \;(k \in \mathbb{Z})$. Ed ancora $(a-b)c = (a-b)c'd = km'd \;\Rightarrow\; (a-b)c' = km'$. Ma $gcd(c', m') = 1$ e quindi $a - b$ è multiplo di m', cioè $a - b = hm'$ $(h \in \mathbb{Z})$. Ciò significa che $a \equiv_{m'} b$ e dato che $m' = \dfrac{m}{d} \;\Rightarrow$ $a \equiv_{\frac{m}{d}} b$. □

A questo punto ci chiediamo: quanti dei rappresentanti delle classi appartenenti a $\mathbb{Z}_m$ cioè $1, 2, 3, \ldots, m$, hanno massimo comune divisore d con m, supposto $d \,|m$

Evidentemente tali numeri devono essere multipli di d, ossia sono del tipo: $d, 2d, 3d, \ldots, kd, \ldots, \left(\dfrac{m}{d}\right) d$. Supponiamo che sia kd, allora si ha: $gcd(kd, m) = d \;\Leftrightarrow\; gcd\left(k, \dfrac{m}{d}\right) = 1$, ovvero se e solo se k è primo con $\dfrac{m}{d}$ poiché i numeri primi con $\dfrac{m}{d}$ e minori di $\dfrac{m}{d}$ sono $\varphi\left(\dfrac{m}{d}\right)$, si conclude che il numero dei naturali rappresentanti le classi di $\mathbb{Z}_m$ e aventi massimo comune divisore d con m è $\varphi\left(\dfrac{m}{d}\right)$.

Teorema 25. Per ogni numero naturale $m \geq 1$ siano $d_0, d_1, \ldots, d_r = m$ i suoi divisori. Allora risulta $\displaystyle\sum_{i=0}^{r} \varphi(dv) = m$.

Dimostrazione. Ogni numero naturale minore o uguale ad m ha un certo massimo comune divisore con m che è uno di questi: $d_0 = 1, d_1, \ldots, d_r = m$. Quanti di questi numeri $1, 2, \ldots, m$, hanno con un massimo comune divisore uguale a

d_i $(0 \leq i \leq r)$? Sappiamo essere $\varphi\left(\frac{m}{d_i}\right)$. Pertanto $\sum_{i=0}^{r} \varphi\left(\frac{m}{d_i}\right) = m$. D'altra parte si verifica sempre la seguente uguaglianza: $d_i = d_{r-i} = m$ da qui segue che $d_{r-i} = \frac{m}{d_i}$. Quindi $\sum_{i=0}^{r} \varphi\left(\frac{m}{d_i}\right) = \sum_{i=0}^{r} \varphi\left(d_{r-i}\right) = \sum_{i=0}^{r} \varphi\left(d_i\right)$ □

Esempi

1) Se $m = 10$, i divisori sono: $1, 2, 5, 10$, poiché $\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(5) = 4,\ \varphi(10) = 4 \Rightarrow \sum_{d_i|m} \varphi(d_i) = 1 + 1 + 4 + 4 = 10.$

2) Se $m = 20$, i divisori sono: $1, 2, 4, 5, 10, 20.$ $\varphi(1) = 1,\ \varphi(2) = 1,\ \varphi(5) = 4,\ \varphi(10) = 4,\ \varphi(20) = 8.$ $\sum_{d_i|m} \varphi(d_i) = 1 + 1 + 2 + 4 + 4 + 8 = 20.$

Teorema 26. Se la fattorizzazione di un numero naturale in prodotti di potenze di primi, tutti diversi fra loro, è $n = p_1^{r_1}, p_2^{r_2} \dots p_k^{r_k}$, allora si ha: $\varphi(n) = \varphi(p_1^{r_1}) \cdot \varphi(p_2^{r_2}) \cdot \dots \cdot \varphi(p_k^{r_k})$.

Dimostrazione. Chiamiamo peso del numero n il numero naturale $\rho = r_1 + r_2 + r_3 + \dots + r_k$ ossia la somma dei suoi esponenti.

Proviamo il teorema per induzione rispetto al peso in questo modo: se la tesi è vera per i numeri di peso 1 e se è altrettanto vera per i numeri di peso r, con $1 < r < \rho \quad \Rightarrow$ risulta vera per il numero n di peso ρ. Allora la formula è vera per ogni numero naturale di peso $\rho > 1$.

Se il peso è 1, si ha l'identità e quindi la tesi è vera (infatti: sia $r_1 = 1$, cioè $n = p_1^1 \quad \Leftrightarrow \varphi(n) = \varphi(p_1)$.

Supponiamo che la formula sia vera per tutti i numeri di peso r $(1 < r < \rho)$. Consideriamo dunque $n = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdot \dots \cdot p_{k-1}^{r_{k-1}} \cdot p_k^{r_k - 1} \cdot p_k$ e indicando con $n'' = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdot \dots \cdot p_{k-1}^{r_{k-1}}$ e $n' = n'' \cdot p_k^{r_k - 1}$. Contiamo ora i divisori di n: essi formano l'insieme $D = \{\text{divisori di } n'\} \cup \{\text{divisori di } n'' \neq n'' \text{moltiplicati per } p_k^{r_k}\} \cup \{n\}$. Gli insiemi indicati costituiscono una partizione dell'insieme D dei divisori di n.

Ricordando che $\sum_{d_i|n} \varphi(d_i) = n$ otteniamo:

$$\begin{aligned} n &= \sum_{d_i'|n'} \varphi(d_i') + \sum_{d_i''|n'' \ (\neq n'')} \varphi(d_i'' p_k^{r_k}) + \varphi(n) \\ &= n' + \underbrace{\sum_{d_i''|n'' \ (\neq n'')} \varphi(d_i'' p_k^{r_k})}_{\text{per ipotesi induttiva}} + \varphi(n) \end{aligned}$$

pertanto si ha:
$\varphi(n) = n - n' - [\varphi(p_k^{r_k})] \sum_{d_i''|n'' \ (\neq n'')} \varphi(d'') = n - n' - \left[p_k^{r_k} - p_k^{r_k - 1}\right] \sum_{d_i''|n'' \ (\neq n'')} \varphi(d'')$
poiché

$$\sum_{d_i'' | n''} \varphi(d'') = n'' - \varphi(n'') \Rightarrow$$

$$\begin{aligned}\varphi(n) &= n - n' - \left(p_k^{r_k} - p_k^{r_k-1}\right)(n'' - \varphi(n'')) \\ &= n - n' - p_k^{r_k} n'' + p_k^{r_k-1} n'' + p_k^{r_k}\varphi(n'') - p_k^{r_k-1} \cdot \varphi(n'') \\ &= n - n' - n + n' + \varphi(n'')\left[p_k^{r_k} - p_k^{r_k-1}\right] \\ &= \varphi(n'')\varphi(p_k^{r_k})\end{aligned}$$

Per l'ipotesi induttiva si ha $\varphi(n'') = \varphi(p_1^{r_1})\varphi(p_2^{r_2})\ldots\varphi(p_{k-1}^{r_{k-1}})$. Da cui $\varphi(n) = \varphi(p_1^{r_1})\varphi(p_2^{r_2})\ldots\varphi(p_{k-1}^{r_{k-1}})\varphi(p_k^{r_k})$ □

N.B. Nel caso in cui si ha $a, b \in \mathbb{N}$, $a \neq b$ e $gcd(a,b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$.

Esempio: $\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = \varphi(2^3)\varphi(3)\varphi(5^2) = (2^3 - 2^2)\cdot 2 \cdot (5^2 - 5) = 160$

Osservazione: sia $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{r_1})\varphi(p_2^{r_2})\ldots\varphi(p_k^{r_k}) \\ &= \left(p_1^{r_1} - p_1^{r_1-1}\right)\left(p_2^{r_2} - p_2^{r_2-1}\right)\ldots\left(p_k^{r_k} - p_k^{r_k-1}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)\end{aligned}$$

Teorema 27 (di Fermat)**.** Siano a, m numeri naturali primi fra loro ($gcd(a,m) = 1$). Allora:

$$a^{\varphi(m)} \equiv_m 1$$

Dimostrazione. Consideriamo i numeri minori di m e primi con m; li indichiamo con: $k_1(=1), k_2, k_3, \ldots, k_{\varphi(m)}$. Ora li moltiplichiamo tutti per a. Poiché $gcd(a,m) = 1$ e $gcd(k_i, m) = 1$ $(1 \leq i \leq \varphi(m))$, si ha $gcd(ak_i, m) = 1$. Osserviamo che nessuna coppia dei numeri $ak_1, ak_2, ak_3, \ldots, ak_{\varphi(m)}$ può risultare congrua modulo m. Infatti, se fosse $ak_s \equiv_m ak_r \Rightarrow ak_s - ak_r = a(k_s - k_r)$ sarebbe multiplo di m. Ma ciò non può verificarsi. Infatti m è divisore di $a(k_s - k_r)$, ma non lo è né di a $(gcd(m,a) = 1)$ né di $k_s - k_r$ (essendo $k_s - k_r < m$).

In modo del tutto analogo si prova che nessuno di questi numeri è congruo zero modulo m. Pertanto i prodotti ak_i sono rispettivamente congrui ai numeri $k_1, k_2, k_3, \ldots, k_{\varphi(n)}$ considerati in un certo ordine.

Ne segue che: $ak_1 \cdot ak_2, k_3 \cdot \ldots, ak_{\varphi(m)} = k_1 k_2 k_3 \ldots k_{\varphi(m)} \cdot a^{\varphi(m)} \equiv_m k_1 k_2 k_3 \ldots k_{\varphi(m)}$ posto $k_1 k_2 k_3 \ldots k_{\varphi(m)} \cdot a^{\varphi(m)} = k a^{\varphi(m)} \equiv_m k \Rightarrow k\left(a^{\varphi(m)} - 1\right) \equiv_m 0$. Ricordando che $gcd(k_i, m) = 1$, anche il prodotto di tali numeri con m sarà primo con m, $gcd(k,m) = 1$. Quindi $m \,|\, k\left(a^{\varphi(m)} - 1\right)$ e $gcd(m,k) = 1 \Rightarrow m \,|\, \left(a^{\varphi(m)} - 1\right) \Rightarrow \left(a^{\varphi(m)} - 1\right) \equiv_m 0$ □

Osservazione Consideriamo l'anello $\mathbb{Z}_m$ delle classi dei resti modulo m. se a è un numero primo con m allora $[a]$ ammette classe reciproca $[x]$ in $\mathbb{Z}_m$.

Sia, infatti, $[a] \cdot [x] = [1]$. Ma $a^{\varphi(m)} \equiv_m 1 \Rightarrow x = \dfrac{a^{\varphi(m)}}{a} = a^{\varphi(m)-1}$

Pertanto la classe reciproca di $[a]$ e $\left[a^{\varphi(m)-1}\right]$.

Problema 3. Trovare in $\mathbb{Z}_{100}$ la classe reciproca di [31]

Soluzione. Posto $a = 31$ ed essendo $gcd(31, 100) = 1$ si ha $a^{\varphi(100)} \equiv_{100} 1$ quindi $\left[31^{\varphi(100)-1}\right]$ è la classe reciproca di $[31]$. Ora $100 = 2^2 5^2$ da cui $\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = 2 \cdot 20 = 40$. Allora la classe reciproca di $[31]$ è $\left[31^{39}\right]$.

Scriviamo così:

$$\begin{aligned}
31^{39} &= \left(31^2\right)^{19} \cdot 31 \\
&= (961)^{19} \cdot 31 \equiv_{100} (61)^{19} \cdot 31 \\
&= \left(61^2\right)^9 \cdot 61 \cdot 31 \\
&= (3721)^9 \cdot 61 \cdot 31 \equiv_{100} (21)^9 \cdot 61 \cdot 31 \\
&= \left(21^3\right)^3 \cdot 61 \cdot 31 \\
&= (9261)^3 \cdot 61 \cdot 31 \\
&\equiv_{100} 61^3 \cdot 61 \cdot 31 \\
&= (3721)^2 \cdot 31 \equiv_{100} 41 \cdot 31 \\
&= 1271 \equiv_{100} 71
\end{aligned}$$

Pertanto la classe reciproca è $[71]$. □

Problema 4. Qual è nel sistema di numerazione decimale l'ultima cifra del numero $(3427)^{91}$?

Soluzione. Osserviamo che la cifra delle unità corrisponde al resto della divisione del numero per 10. Innanzitutto $3427 \equiv_{10} 7$, quindi si cerca il resto di 7^{91}. Essendo $7^{\varphi(10)} = 7^4 \equiv_{10} 1 \Rightarrow 7^{91} = (7^4)^{22} \cdot 7^3 \equiv_{10} 1^{22} \cdot 7^3 = 343 \equiv_{10} 3$. La cifra delle unità di $(3427)^{91}$ è pertanto 3. □

Problema 5. Determinare le ultime due cifre decimali, del numero 9^{1964}

Soluzione. Le ultime due cifre decimali corrispondono al resto della divisione per 100. $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) = (2^2 - 2)(5^2 - 5) = 40$ da cui $9^{\varphi(100)} = 9^{40} \equiv_{100} 1$. inoltre $1964 = 40 \cdot 49 + 4$ e pertanto $9^{1964} = \left(9^{40}\right)^{49} \cdot 9^4 \equiv_{100} 1^{49} \cdot 9^4 = 6561 \equiv_{100} 61$. Le due ultime due cifre finali sono quindi 61. □

Definizione 11. Si definisce congruenza di primo grado nell'incognita x ogni equazione della forma

$$ax \equiv_m b$$

con $a, b \in \mathbb{Z},\ m \in \mathbb{N}$.

Il teorema di Fermat ci permette di risolvere una congruenza di questo tipo, nell'ipotesi che $gcd(a, m) = 1$. Una soluzione è $x_0 = b \cdot a^{\varphi(m)-1}$. Infatti $a \cdot b \cdot a^{\varphi(m)-1} = a \cdot a^{\varphi(m)-1} \cdot b \equiv_m b$ poiché $a^{\varphi(m)} \equiv_m 1$. Tutte le altre soluzioni sono del tipo $a^{\varphi(m)-1} \cdot b + km$ $(k \in \mathbb{Z})$, sono cioè congrue fra loro modulo m.

3.8 Analisi indeterminata

Siano $a, b, c \in \mathbb{Z}$. Un'equazione diofantea lineare è un equazione della forma

$$ax - by = c \tag{3.1}$$

Risolvere questa equazione significa trovare tutte le coppie (x, y) di numeri interi che la soddisfano.

Teorema 28. Condizione necessaria e sufficiente affinché l'equazione 3.1 ammetta soluzioni è che il termine noto c sia multiplo di $d = gcd(a, b)$.

Dimostrazione. Necessità: se la $ax - by = c$ ha soluzione (x, y), allora c deve essere multiplo di d. Infatti d dividendo a e b, divide anche tutto il primo membro dell'equazione e quindi anche c.

Sufficienza: sia c multiplo di d, supponiamo $c = qd$. Allora per il teorema di Bezout esistono due interi h, k tali che $ak - bh = d$. Si ha $a(kq) - b(hq) = dq = c$. Quindi $kq, hq)$ è una soluzione particolare della (3.1). □

N.B. Se $c = d$, la $ax - by = c$ ha la soluzione particolare (k, h).

Il ragionamento sopra esposto ci dice come trovare una soluzione della (3.1): se $d = gcd(a, b)$ ed è verificata la condizione necessaria e sufficiente per l'esistenza di soluzioni, cioè $c = dq$, si determinano con l'algoritmo euclideo i numeri k, h e quindi la soluzione $x_0 = kq$, $y_0 = hq$.

Presentiamo ora un procedimento equivalente per calcolare una soluzione particolare della (3.1). Supposto $gcd(a, b) = 1$ (è lecito fare questa ipotesi poiché, dividendo a e b per $gcd(a, b)$, si trova proprio questa condizione), consideriamo la congruenza lineare $ax \equiv_b c$, che ha la soluzione particolare $x_0 = a^{\varphi(b)-1} \cdot c$. Scriviamo l'equazione (3.1) nella forma $ax - c = by$ ossia $ax \equiv_b c$. si ha quindi la soluzione $x_0 = a^{\varphi(b)-1} \cdot c$. Pertanto $ax_0 - c = by_0 \Rightarrow y_0 = \dfrac{ax_0 - c}{b}$. La coppia (x_0, y_0) soddisfa l'equazione ed è pertanto una sua soluzione.

Teorema 29. Se l'equazione (3.1) ammette una soluzione (x_0, y_0), allora le altre infinite soluzioni sono tutte e sole quelle del tipo $(x_0 + kb, y_0 + ka)$ con $k \in \mathbb{Z}$.

Dimostrazione. Proviamo che le coppie $(x_0 + kb, y_0 + ka)$ sono soluzioni. Sostituendo, si ottiene $a(x_0 + kb) - b(y_0 + ka) = ax_0 + kab - by_0 - kab = ax_0 - by_0 = c$.

All'infuori di questo tipo di soluzioni non ce ne sono altre. Supponiamo che (x_1, y_1) sia una soluzione della (3.1) allora $ax_1 - by_1 = c = ax_0 - by_0 \Rightarrow a(x_1 - x_0) = b(y_1 - y_0)$. Osserviamo che il primo membro di questa uguaglianza è divisibile per b, ma poiché a è primo con b, allora $x_1 - x_0 = kb$. Analogamente $y_1 - y_0 = ha$. Pertanto: $x_1 = x_0 + kb$, $y_1 = y_0 + ha$. Sostituendo la soluzione $x_1, y_1)$ nella (3.1) si ha: $a(x_0+kb)-b(y_0+ha) = c \Rightarrow ax_0+kab-by_0-hab = c \Rightarrow kab - hab + (ax_0 - by_0 - c) = 0 \Rightarrow kab - hab = 0 \Leftrightarrow k = h$. Quindi la soluzione $(x_1, y_1) = (x_0 + kb, y_0 + ka)$. □

N.B. Se l'equazione diofantea è $ax + by = c$ $(gcd(a, b) = 1)$ una sua soluzione particolare è: $x_0 = a^{\varphi(b)-1} \cdot c, y_0 = \dfrac{c - ax_0}{b}$.

Problema 6. Abbiamo n caramelle da spartire in sacchetti. Se le mettiamo in sacchetti da 16 ne avanzano 3, se le mettiamo in sacchetti da 25 ne avanzano 7. Determinare n sapendo che $1000 < n < 1500$

Soluzione. Indichiamo con x il numero di sacchetti da 16 e con y il numero di sacchetti da 25. Risulta: $n = 16x + 3 = 25y + 7 \Rightarrow 16x - 25y = 4$, essendo $gcd(16, 25) = 1$, consideriamo l'equazione $16x \equiv_{25} 4$ una soluzione è $x_0 = 16^{\varphi(25)-1} \cdot 4 = 16^{19} \cdot 4 \equiv_{25} 19$, $y_0 = \dfrac{16 \cdot 19 - 4}{25} = 12$. Le infinite soluzioni

dell'equazione sono del tipo $(19+25k, 12+16k)$ pertanto $n = 16(19+25k)+3 = 307+25\cdot 16k$. Dato che $1000 < n < 1500$ prendiamo $k = 2$ e quindi $n = 1107$ □

Problema 7 (di Fibonacci)**.** Giunta al mercato, una contadinella ricontrolla le sue uova, e si accorge che se le conta a due a due, oppure a tre a tre, oppure a quattro a quattro o anche a sei a sei, in tutti questi casi gliene rimane sempre una; se le conta inoltre a sette a sette, non ne avanza alcuna.

È possibile stabilire con quante uova la contadinella è andata al mercato?

Soluzione. Poiché $lcd(2,3,4,5,6) = 60$; il numero delle uova può essere scritto come un multiplo di 60 più 1 $\Rightarrow$ $60y+1$. Inoltre il numero delle uova è multiplo di 7, l'equazione che risolve il problema è $7x - 60y = 1$ essendo $gcd(7,60) = 1$, una soluzione dell'equazione $7x \equiv_{60} 1$ è $x_0 = 7^{\varphi(60)-1} = 7^{15} \equiv_{60} 43$, $y_0 = \dfrac{7\cdot 43 - 1}{60} = 5$. Le soluzioni sono $(43 + 60k, 5 + 7k)$. pertanto il numero delle uova è $7(43+60k)$ oppure $60(5+7k)+1$, cioè $301+420k$. Questo numero, come si vede, può essere 301, ma anche 301 più un multiplo intero di 420. □

Problema 8. Un treno parte da Pisa. Al momento della partenza il macchinista controlla il cronometro e nota che la lancetta dei secondi è sullo zero. Dopo aver percorso 8 km, il macchinista controlla di nuovo il cronometro e nota che la lancetta dei minuti copre esattamente quella delle ore. La velocità media del treno per gli 8 km percorsi è di 33 $\frac{km}{h}$. A che ora è partito il treno da Pisa?

Soluzione. Supponiamo che il treno sia partito x minuti dopo la mezzanotte, con $1 \le x \le 60 \cdot 12$. Esso impiega $\dfrac{8}{\frac{33}{60}} = \dfrac{160}{11}$ minuti per percorrere 8 km. Quindi quando il macchinista controlla di nuovo il cronometro, sono passati $x+\dfrac{160}{11}$ minuti dopo la mezzanotte. Inoltre , la lancetta dei minuti si sovrappone esattamente su quella delle ore undici volte fino a mezzogiorno, pertanto una volta ogni $\dfrac{720}{11}$ minuti, quindi, sono trascorsi $\dfrac{720}{11}y$ minuti dopo mezzanotte, con $1 \le y \le 11$. L'equazione che risolve il problema è $x + \dfrac{160}{11} = \dfrac{720}{11}y$, ossia $720y - 11x = 160$. Essendo $gcd(11, 720) = 1$ una soluzione dell'equazione $720y \equiv_{11} 160$ è $y_0 = 160 \cdot 720^{\varphi(11)-1}$ da cui $y_0 \equiv_{11} 10$; $x_0 = \dfrac{720\cdot 10 - 160}{11} =$ 640 il treno è partito alle 10:40. Se supponiamo che il treno sia partito dopo mezzogiorno otteniamo le 22:40. □

Appendice A

Logica matematica: le basi

A.1 Logica delle proposizioni

A.1.1 Connettivi logici

Nella lingua parlata gli elementi costitutivi sono le proposizioni (o affermazioni o enunciati); lo stesso avviene in matematica. Indichiamo gli enunciati tra virgolette, ad esempio sono enunciati:

- "Socrate è un uomo";
- "Pitagora mangia la mela";
- "$15 \cdot 2 = 30$";
- "2020 è un numero naturale";
- "$5 + 2 > 10$".

Caratteristica degli enunciati è che possiamo attribuire loro un valore di verità: vero (V) o falso (F). Ad esempio il terzo dei precedenti enunciati è vero mentre il quinto è falso.

Indicheremo gli enunciati con lettere come p, q, r ecc.

Data una proposizione p si può costruire la sua negazione che indichiamo con "$\overline{p}$" (si legge "non p"). Ovviamente, se p è vera, "$\overline{p}$" è falsa e viceversa. Ad esempio, se p è l'enunciato (falso): "3 è un numero naturale pari", allora "$\overline{p}$" è l'enunciato (vero): "3 non è un numero naturale pari".

Le proposizioni possono essere legate tra loro dando luogo a proposizioni più complesse. Nel linguaggio comune il collegamento viene effettuato per mezzo delle congiunzioni. In logica matematica i termini di collegamento si chiamano connettivi logici. Anche la negazione è considerata un connettivo.

Gli altri sono i seguenti: la congiunzione, che corrisponde alla congiunzione "e". Essa viene indicata col simbolo $\wedge$. La disgiunzione, che corrisponde alla congiunzione "o", nel senso del "vel" latino (contrapposto ad "aut"). Essa viene indicata col simbolo $\vee$. L'implicazione, che corrisponde alla locuzione "se ... allora"; viene indicata col simbolo $\Rightarrow$. La doppia implicazione, che corrisponde alla locuzione "se e solo se"; viene indicata col simbolo $\Leftrightarrow$.

Usando i connettivi logici e le parentesi possiamo formare enunciati composti come i seguenti: $p \Rightarrow (q \Rightarrow r)$, $(p \vee q) \Leftrightarrow r$, ecc.

Per evitare di sovraccaricare gli enunciati composti con troppe parentesi si conviene di introdurre tra i connettivi un ordine gerarchico esattamente come si fa in aritmetica per le quattro operazioni $(+, -, \cdot, :)$

Ad esempio la scrittura $(2 \cdot 3 + 5)$ significa $(2 \cdot 3) + 5$ e non $2 \cdot (3 + 5)$. Si suol dire che moltiplicazione e divisione "legano" più di addizione e sottrazione.

Analogamente, introduciamo tra i connettivi il seguente ordine dove ciascun connettivo "lega" più dei successivi: $\overline{()}, \wedge, \vee, \Rightarrow, \Leftrightarrow$. Con questa convenzione invece di scrivere $((\overline{p}) \Rightarrow (\overline{q})) \Leftrightarrow (p \vee (\overline{r}))$ potremo scrivere semplicemente $\overline{p} \Rightarrow \overline{q} \Leftrightarrow p \vee \overline{r}$.

A.1.2 Tavole di verità

Quando due proposizioni vengono legate insieme usando i connettivi logici, il valore di verità della proposizione che ne risulta dipende dal valore di verità delle proposizioni componenti, secondo le seguenti regole o tavole di verità: Per il simbolo $\overline{()}$:

p	$\overline{p}$
V	F
F	V

Per gli altri:

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
V	V	V	V	V	V
F	V	F	V	V	F
V	F	F	V	F	F
F	F	F	F	V	V

A parole: "$p \wedge q$" è vera se p e q sono entrambe vere; falsa negli altri casi
"$p \vee q$ è falsa se p e q sono entrambe false; vera negli altri casi
"$p \Rightarrow q$" è falsa se p è vera e q è falsa; vera negli altri casi
"$p \Leftrightarrow q$" è vera se p e q sono entrambe vere o entrambe false; falsa negli altri casi.

Si nota che l'uso del connettivo $\Rightarrow$ non corrisponde propriamente alla locuzione "se ... allora" del linguaggio comune. Infatti, quando noi usiamo tale locuzione, riteniamo che le due proposizioni componenti p e q abbiano una correlazione causale o qualche altro tipo di legame. Invece in matematica la verità della proposizione "$p \Rightarrow q$" dipende solo dai valori di verità di p e q, anche se tali proposizioni non sono correlate fra loro.

L'origine della tavola di verità di "$p \Rightarrow q$" può essere spiegata intuitivamente come segue.

Esaminiamo la frase "se c'è il sole faccio una passeggiata". Ciò è equivalente all'alternativa "non c'è il sole oppure faccio una passeggiata".

Si noti che il fatto che non ci sia il sole non implica alcuna decisione riguardo alla passeggiata.

Dunque, nel linguaggio comune, dire: "$p \Rightarrow q$" è equivalente a dire "$\overline{p} \vee q$" La tavola di verità di "$\overline{p} \vee q$" è la seguente:

p	q	$\overline{p}$	$\overline{p} \vee q$
V	V	F	V
F	V	V	V
V	F	F	F
F	F	V	V

Tale tavola coincide con quella di "$p \Rightarrow q$".

Dunque, se riteniamo "corretta" la tavola di verità per il connettivo $\vee$, dobbiamo ritenere corretta anche quella indicata per l'implicazione.

Osserviamo infine che l'implicazione "$p \Rightarrow q$" spesso si legge "p è condizione sufficiente perché valga q" oppure "q è condizione necessaria perché valga p". La doppia implicazione "$p \Leftrightarrow q$", che esprime l'equivalenza logica delle due proposizioni p e q, si legge: "condizione necessaria e sufficiente perché valga p è che valga q".

A.1.3 Tautologie e regole di deduzione

Nella dimostrazione di un teorema o in ogni tipo di argomentazione logica si fa uso continuo di regole di deduzione (o di inferenza), cioè di regole logiche che precisano il corretto modo di ragionare.

Esaminiamo un classico esempio di argomentazione valida.

1) Socrate è un uomo.

2) Se Socrate è un uomo allora Socrate è mortale.

3) (Allora) Socrate è mortale.

La sequenza 1), 2), 3) è una deduzione corretta dell'enunciato 3) dagli enunciati 1) e 2); cioè è una dimostrazione che Socrate è mortale.

Osserviamo subito che 3) non si può dedurre solo da 2). In termini più generali, da "$p \Rightarrow q$" non si può dedurre q.

Per rendersi meglio conto di questo fatto consideriamo l'enunciato

"se 3 è un intero pari allora 4 è un intero dispari". Anche se tale enunciato è vero non possiamo certo dedurre che 4 è dispari.

Osserviamo inoltre che la validità della deduzione di 3) da 1) e 2) non dipende dal valore di verità di 1) e 2). Infatti, anche la seguente deduzione è corretta:

1) Socrate è un uomo.

2') Se Socrate è un uomo allora è immortale.

3') (Allora)Socrate è immortale.

Su che cosa è fondata la correttezza delle deduzioni precedenti?

Pensate di far eseguire la deduzione 1), 2), 3) da un elaboratore nella cui memoria siano inserite (come ipotesi) gli enunciati 1) e 2). Esso non sarà mai in grado di dedurre l'enunciato 3) a meno che non lo forniate della regola seguente: "se in memoria si trovano gli enunciati p e "$p \Rightarrow q$" allora si può inserire anche q.

Cerchiamo di capire l'origine di questa regola di deduzione.

Consideriamo l'enunciato seguente

$$p \wedge (p \Rightarrow q) \Rightarrow q \qquad \text{(MP)}$$

e la sua tavola di verità:

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	MP
V	V	V	V	V
F	V	V	F	V
V	F	F	F	V
F	F	V	F	V

Qualunque siano i valori di verità di p e q, il valore di verità di (MP) è sempre vero.

Essendo (MP) sempre vera, è naturale considerare q come conseguenza logica di p e "$p \Rightarrow q$" ovvero formulare la seguente regola di inferenza che si chiama modus ponens: da p e "$p \Rightarrow q$" si deduce q .

Dal punto di vista pratico il modus ponens opera così: se p è vera e si vuole mostrare che q è vera, si procede mostrando che "$p \Rightarrow q$" è vera.

Gli enunciati come (MP), veri qualunque sia il valore di verità delle proposizioni componenti, prendono il nome di tautologie.

Un'altra importante tautologia è la seguente, nota come principio di contrapposizione:

$$p \ \Rightarrow \ q \Leftrightarrow \ \overline{q} \ \Rightarrow \ \overline{p} \qquad \text{(PC)}$$

e la sua tavola di verità:

p	q	$\overline{p}$	$\overline{q}$	$p \Rightarrow q$	$\overline{q} \ \Rightarrow \ \overline{p}$	PC
V	V	F	F	V	V	V
F	V	F	V	V	V	V
V	F	V	F	F	F	V
F	F	V	V	V	V	V

Se fissiamo l'attenzione sulla prima implicazione "$p \Rightarrow q$" e la chiamiamo proposizione diretta, allora la seconda "$\overline{q} \ \Rightarrow \ \overline{p}$" è detta la contronominale; è detta invece inversa la "$q \ \Rightarrow \ p$" e contraria la "$\overline{p} \ \Rightarrow \ \overline{q}$".

La tautologia PC afferma l'equivalenza logica delle proposizioni diretta e contronominale. Da essa segue la regola di deduzione (di cui si fa uso larghissimo in matematica) detta di riduzione all'assurdo: nell'ipotesi che p sia vera, se si vuole dimostrare che q è vera si procede dimostrando che "$\overline{q} \ \Rightarrow \ \overline{p}$" è vera.

Altre tautologie, da verificare, per esercizio, sono le seguenti:

(TE) "$p \vee \overline{p}$"

(SI) "$(p \ \Rightarrow \ q) \wedge (q \ \Rightarrow \ r) \ (q \ \Rightarrow \ r)$"

(NC) "$\overline{p \wedge \overline{p}}$"

$(\text{DM})_1$ "$\overline{p \vee q} \ \Leftrightarrow \ \overline{p} \wedge \overline{q}$"

$(\text{DM})_2$ "$\overline{p \wedge q} \ \Leftrightarrow \ \overline{p} \vee \overline{q}$"

La (TE) è il principio del terzo escluso, la (NC) è quello di non contraddizione. La (SI) è nota come sillogismo ipotetico: la prima implicazione $(p \Rightarrow q)$ è detta premessa maggiore, la seconda $(q \ \Rightarrow \ r)$ premessa minore. Le ultime due sono note come leggi di De Morgan, utili quando si ha a che fare con la negazione di proposizioni composte.

E pure una tautologia la seguente: "$p \Rightarrow q \Leftrightarrow \overline{p} \vee q$" (infatti, come abbiamo già osservato, "$p \Rightarrow q$" e " $\overline{p} \vee q$" hanno la stessa tavola di verità). Dunque anche "$\overline{p \Rightarrow q} \Leftrightarrow \overline{\overline{p} \vee q}$" è una tautologia e infine, usando DM_2, anche "$\overline{p \Rightarrow q} \Leftrightarrow p \wedge \overline{q}$" lo è: ciò significa che negare "$p \Rightarrow q$" equivale all'enunciato: "$p \wedge \overline{q}$".

Siano: p: "oggi piove"
q: "non esco di casa"
r: "guardo la partita".
"$p \Rightarrow q$" significa: "se oggi piove non esco di casa"
"$p \wedge \overline{q}$" significa: "oggi piove ed esco di casa" (che è la precisa negazione dell'enunciato precedente).

Su (SI) è fondata la deduzione seguente: se oggi piove non esco di casa; se non esco di casa guardo la partita; allora, se piove guardo la partita.

$(\mathrm{DM})_1$ indica: "non è vero che: oggi piove, oppure non esco di casa, equivale ad affermare che: non piove ed esco di casa".

$(\mathrm{DM})_2$ ...

A.2 Logica dei predicati

A.2.1 Quantificatori

Una logica basata solo sugli enunciati è insufficiente per i nostri scopi. Occorre introdurre il concetto di predicato: una proposizione contenente una o più variabili (o argomenti). Un predicato si dice unario se riguarda solo una variabile e si indicherà con una scrittura del tipo $p(x)$. Ad esempio: $p(x)$: "x è una donna", $p(x)$: " x è un numero reale > 3" sono predicati unari. Analogamente, un predicato si dirà binario, ternario, ecc. Se riguarda 2, 3 o più argomenti.

Se fissiamo tutte le variabili, il predicato diventa una proposizione che può essere vera o falsa. Ad esempio, sostituendo nel predicato: "$x \geq y$" ad x il numero 2 ad y il numero 3, si ottiene l'enunciato falso: "$2 \geq 3$".

A partire da predicati noti si possono costruire nuovi predicati usando le parentesi ed i connettivi logici. Un'altra maniera per produrre nuovi predicati è l'applicazione dei cosiddetti quantificatori: universale ed esistenziale. Il quantificatore universale è indicato col simbolo $\forall$ e significa: per ogni.

Il quantificatore esistenziale è indicato col simbolo $\exists$ e significa: esiste.

Per esempio, se $p(x)$ è un predicato (unario) allora: "$\forall x : p(x)$" e "$\exists x : p(x)$" sono predicati che significano, rispettivamente: "per ogni x è vera $p(x)$", "esiste almeno un x per il quale è vera $p(x)$".

Nei predicati contenenti più variabili si possono impiegare più quantificatori; bisogna allora fare attenzione all'ordine in cui questi vengono applicati, poiché il significato della proposizione risultante può essere completamente diverso nei diversi casi.

Esempio. Sia $p(x, y)$: "un uomo x osserva la stella y".
$\exists x : p(x, y)$ significa: "esiste un uomo che osserva la stella y"
$\forall x : p(x, y)$ significa: "tutti gli uomini osservano la stella y"
$\forall y, \exists x : p(x, y)$ significa: "per ogni stella esiste un uomo che la osserva"
$\exists x, \forall y : p(x, y)$ significa: "esiste un uomo che osserva ogni stella"
$\exists y, \forall x : p(x, y)$ significa: "esiste una stella osservata da tutti gli uomini"

Se una variabile in un predicato non è quantificata (cioè soggetta all'azione di un quantificatore) si dice libera. Così, considerando i vari predicati dell'esempio precedente, nei primi due la variabile y è libera; negli altri entrambe le variabili x e y sono quantificate; il predicato non dipende più effettivamente dalle variabili x e y, che pertanto si dicono mute. Il valore di verità di un predicato dipende dalle sue variabili libere. Se un predicato non ha variabili libere è un enunciato.

Osserviamo una importante relazione tra i due quantificatori $\exists$ e $\forall$. Si consideri, ad esempio, il predicato: "non tutte le mucche sono bianche". Se vogliamo formalizzarlo, possiamo introdurre i due predicati semplici:

$p(x)$: "x è una mucca"

$q(x)$: "x è bianco" .

Allora il nostro predicato può formalizzarsi nel modo seguente: "$\overline{\forall x : p(x) \ \Rightarrow \ q(x)}$"

Esso è equivalente a dire: "esiste una mucca non bianca".

Quest'ultimo enunciato può formalizzarsi così: "$\exists x \ : \ p(x) \wedge \overline{q(x)}$" ovvero "$\exists x : \overline{p(x) \ \Rightarrow \ q(x)}$" poiché, come abbiamo già osservato, la proposizione "$p \wedge \overline{q}$" è equivalente alla negazione della proposizione "$p \ \Rightarrow \ q$". Siamo dunque condotti a formulare la seguente proposizione, che è sempre vera: se $a(x)$ è un predicato, in cui x è variabile libera, allora

"$\overline{\forall x : a(x)} \ \Leftrightarrow \ \exists x : \overline{a(x)}$"

Analogamente abbiamo

"$\overline{\exists x : a(x)} \ \Leftrightarrow \ \forall x : \overline{a(x)}$"

Quanto sopra indica come operare col simbolo di negazione e i quantificatori: la negazione può essere scambiata con un quantificatore, pur di mutare questo nell'altro, negando il predicato quantificato. L'equivalenza espressa nelle regole precedenti mette in luce il ruolo dei controesempi nel dimostrare che un teorema è falso.

Si voglia ad esempio mostrare che un teorema del tipo "$\forall x : p(x) \ \Rightarrow \ q(x)$", è falso e cioè che "$\overline{\forall x : p(x) \ \Rightarrow \ q(x)}$" è vero. Per quanto visto è sufficiente esibire un particolare x (il controesempio) tale che $p(x)$ sia vera e $q(x)$ sia falsa.

Per esempio, per mostrare che l'enunciato: "ogni equazione di secondo grado ha una radice reale" è falso, basterà considerare la sola equazione: $x^2 + 1 = 0$.