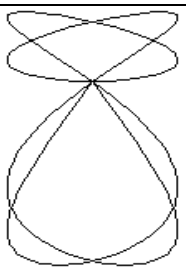
MatematicaMente

Pubblicazione mensile della sezione veronese della MATHESIS – Società Italiana di Scienze Matematiche e Fisiche – Fondata nel 1895 – Autorizzazione del Tribunale di Verona n. 1360 del 15 – 03 – 1999 – I diritti d'autore sono riservati. Direttore responsabile: Luciano Corso - Redazione: Luciano Corso, Luigi Marigo, Elisabetta Capotosto - Via IV Novembre, 11/b – 37126 Verona – tel e fax (045) 8344785 – lcorso@itisgmarconi.vr.it – Stampa in proprio - Numero 18 – giugno 1999



Particolari classi e operazioni tra classi

di Ruggero Ferro

Le nozioni sulle classi, che richiamiamo brevemente, sono molto note. Tuttavia vorrei spendere un po' di tempo a ricordarle per far vedere come esse siano già relative alla nozione di classe, senza far riferimento agli insiemi: infatti esse si basano sugli elementi appartenenti a delle classi.

Una classe, diciamola X, i cui elementi sono anche elementi di un'altra classe, diciamola Y, è detta sottoclasse dell'altra e si usa la scrittura $X \subseteq Y$. Cioè, $X \subseteq Y$ se per ogni elemento a se $a \in X$ allora $a \in Y$. Se X è una sottoclasse di Y si dirà anche che X è contenuto, o incluso, in Y, e che Y contiene, o include, X, e si userà pure la notazione $Y \supseteq X$. Si osservi che ogni classe è sottoclasse di se stessa.

Se una classa X è contenuta in una classe Y ed anche una classe Y è contenuta nella classe X, allora gli elementi della classe X sono esattamente gli elementi della classe Y e le due classi coincidono, X=Y.

Si dirà classe vuota una classe che non ha elementi, e la si indicherà con il simbolo ∅. Poiché una classe è determinata dai suoi elementi e due classi sono la stessa se hanno gli stessi elementi, la classe vuota è unica. Si osservi che la classe vuota è sottoclasse di ogni classe.

SI può anche fissare l'attenzione su un solo elemento. Si noti che un elemento e la classe che ha quell'elemento come unico elemento sono due cose ben distinte, e questa diversità viene ben rispecchiata dalla nozione: se a è il nome dell'elemento, la classe che ha per unico elemento a si indica con {a} (spesso chiamato singoletto di a) che non è a, la notazione dell'elemento.

A volte vogliamo considerare tutti gli elementi diversi da quelli appartenenti ad una certa classe X. Otteniamo così una nuova classe che viene chiamata complementare della classe X. Essa è la classe $\{x: x \notin X\}$. Indicheremo con –X (in letteratura si trovano anche altre notazioni) la classe complementare di X. Quella appena considerata è un'operazione tra classi, e precisamente quella che ad una classe associa la sua classe complementare.

Date le classi X e Y, la classe che si ottiene considerando gli elementi che appartengono sia alla classe X che alla classe Y è detta intersezione delle due classi, e si indica così: $X \cap Y$. Cioè $X \cap Y=\{x: x \in X \text{ e } x \in Y\}$. L'intersezione è commutativa ($X \cap Y=Y \cap X$). Quella considerata è un'altra operazione tra classi e precisamente quella che a due classi associa la loro intersezione. Si noti che $X \cap Y$ è una sottoclasse sia della classe X che della classe Y. Due classi la cui intersezione è la classe vuota si dicono disgiunte, cioè se $X \cap Y=\varnothing$ allora diremo che X e Y sono classi disgiunte.

L'operazione di intersezione tra classi può essere ripetuta un numero finito di volte, e, poiché questa operazione è associativa [cioè $(X \cap Y) \cap Z=X \cap (Y \cap Z)$], l'ordine in cui vengono eseguite le successive intersezioni è irrilevante per il risultato. Perciò, invece di $(X \cap Y) \cap Z$, possiamo scrivere $X \cap Y \cap Z$ senza cadere in ambiguità. Più in generale, se $X_1, X_2, \ldots, X_n$ sono n classi, è ben precisato cosa vuol dire considerare la classe $X_1 \cap X_2 \cap \ldots \cap X_n$ che è anche la classe $\{x: x \in X_1 \text{ e } x \in X_2 \text{ e } \ldots \text{ e } x \in X_n\}$.

Un'altra operazione tra le classi è l'unione. Data una classe X e una classe Y, la classe unione delle classi X e Y è la classe i cui elementi sono o elementi della classe X o elementi della classe Y. Indicheremo l'unione delle due classi X e Y così: $X \cup Y$. Cioè $X \cup Y=\{x: x \in X \text{ oppure } x \in Y\}$. L'unione è commutativa ($X \cup Y=Y \cup X$). Si osservi che, qualunque sia X, l'unione della classe X con la classe –X, complementare di X, fa ottenere la particolare classe {x: x è un elemento} cui appartengono tutti gli elementi. Questa viene chiamata classe universale e la indichiamo con U. Brevemente si può scrivere $X \cup -X=U$. L'operazione di unione tra classi può essere ripetuta un numero finito di volte, e, poiché questa operazione è associativa [cioè $(X \cup Y) \cup Z=X \cup (Y \cup Z)$], l'ordine in cui vengono eseguite le successive unioni è irrilevante per il risultato. Perciò, invece di $(X \cup Y) \cup Z$, possiamo scrivere $X \cup Y \cup Z$ senza cadere in ambiguità. Più in generale, se $X_1, X_2, \ldots, X_n$ sono n classi, è ben precisato cosa vuol dire considerare la classe $X_1 \cup X_2 \cup \ldots \cup X_n$ che è anche la classe $\{x: x \in X_1 \text{ oppure } x \in X_2 \text{ oppure } \ldots \text{ oppure } x \in X_n\}$.

Una ulteriore operazione tra classi che considereremo è la differenza di classi. Date una classe X e una classe Y, la classe differenza X-Y è la classe i cui elementi appartengono a X ma non a Y: $X-Y=\{x: x \in X \text{ e } x \notin Y\}$. La classe X-Y è anche detta la classe complementare di Y in X. Osserviamo che gli elementi che appartengono ad una classe X e non appartengono ad una classe Y sono gli elementi che appartengono sia alla classe X che alla classe complementare della classe Y. Perciò, $X-Y=X \cap (-Y)$. Si noti che X-Y è una sottoclasse della classe X.

Dopo aver applicato una operazione ad alcune classi, è possibile applicare ancora la stessa operazione, o altre, alle classi risultato delle precedenti operazioni. A tale proposito osserviamo come certe combinazioni di operazioni diano lo stesso risultato di altre. In particolare:
$(X \cap Y) \cup Z=(X \cup Z) \cap (Y \cup Z)$ e $(X \cup Y) \cap Z=(X \cap Z) \cup (Y \cap Z)$.

La nozione di contenuto tra classi può essere caratterizzata mediante ciascuna delle operazioni di intersezione, unione o differenza tra insiemi. Infatti valgono le seguenti equivalenze: $X \subseteq Y$ se e solo se $X \cap Y=X$ se e solo se $X \cup Y=Y$ se e solo se $X-Y=\varnothing$.

Sulla chiusura di operazioni nel continuo

di Luciano Corso

Non sempre intersezioni di insiemi numerabili danno insiemi numerabili. Il seguente esempio, tratto da [B.1], dimostra proprio questo. Consideriamo l'intervallo $\Omega=(0;1]$ sulla retta reale. Prendiamo ora la seguente partizione dell'intervallo (0; 1]: considerando un generico numero razionale h prendiamo la partizione costituita dal sotto intervallo di sinistra (0;h), dal punto razionale [h;h] e dal sotto intervallo di destra (h;1]. Considerati tutti i razionali di Ω, si ha una infinità numerabile di partizioni - essendo numerabili i razionali di quell'intervallo. Formiamo ora il plurintervallo $P^h_{(0;1]}$ composto dai sotto intervalli di destra e di sinistra della generica partizione h, togliendo il razionale h. L'intersezione

$$\bigcap_{h=1}^{\infty} P^h_{(0;1]}$$

è l'intersezione dell'infinità numerabile dei plurintervalli cui sono stati tolti i razionali. Tale intersezione è l'insieme dei numeri irrazionali. Ma l'insieme degli irrazionali non è numerabile e forma un insieme che ha la potenza del continuo. Quindi non

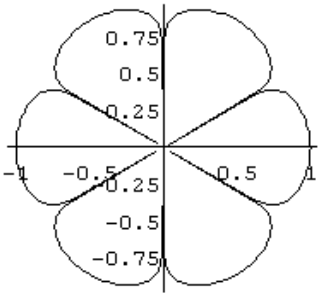
è vero che unioni e negazioni (o intersezioni) di plurintervalli numerabili danno insiemi numerabili. Questo esempio è molto importante per dimostrare che gli insiemi di Borel sono sotto classi della classe degli insiemi numerabili.

Bibliografia: [B.1] Luciano Daboni, Calcolo delle probabilità ed elementi di statistica, UTET, Torino, 1980

Un fiore a 6 petali

Le rose di G. Grandi (1671-1742) possono dare numerosi spunti a chi si interessa di grafica. Qui viene presentato un fiore particolare, le cui coordinate parametriche sono:

$$\begin{cases} \{0 \le t \le 2\cdot\pi\} \\ r(t) = Exp\left[ln\left| cos\left(\frac{6\cdot t}{2} \right) \right|^{\frac{1}{12}} \right] \\ x(t) = r(t)\cdot cos(t) \\ y(t) = r(t)\cdot sen(t) \end{cases}$$



L'elaborazione è una mia variante di una proposta a 5 petali, in TurboPascal, di Arnaldo. Vicentini (L.C.)

Una equazione diofantea con una lunga storia

di Piero Plazzi *

1. A séguito dell'intervento su queste pagine del prof. Vicentini, mi sono incuriosito sul conto dell'equazione $y^2=x^3+30$, ed ho trovato - con una certa sorpresa, visto che non sono un esperto di teoria dei numeri - che questa equazione ha una lunga storia ed una teoria ricca e profonda. Riferisco qui di alcuni risultati di cui sono venuto a conoscenza.

Una equazione della forma

(B_k) $y^2=x^3+k$, k intero

di cui si cerchino soluzioni intere (ci riferiremo al caso I di (B_k)), o razionali (caso II di (B_k)) è nota come equazione di Bachet, o di Mordell; essa è un'equazione diofantea molto interessante. Nonostante la sua apparenza elementare, essa ha un comportamento assai difficile da determinare ed a tutt'oggi presenta molti problemi aperti: perfino per risolverla in casi particolari sono necessari risultati e conoscenze assai profonde sui numeri interi e sulle curve piane algebriche.

2. Dopo un accenno assai fugace in Diofanto [D] al caso k=-2, con soluzioni intere, ("Trovare un quadrato che, aumentato di 2, dia un cubo"), la prima osservazione non banale nota è dovuta a C. G. Bachet (1621) che notò come, sempre per k=-2, a partire da x=3, y=±5, altre infinite soluzioni (razionali) potessero essere trovate col metodo "delle tangenti". Esso si basa su un'osservazione che, con linguaggio moderno, si esprimerebbe in questo modo: *dato un punto semplice razionale su una cubica a coefficienti razionali, la tangente nel punto incontra la curva in un altro punto razionale*. Il procedimento del resto è puramente algebrico: si sostituiscano x, y con u+3 e v+5 in (B_{-2}); si impone che i termini di primo grado si elidano, il che dà u=10v/27 e si risolve in v scartando due soluzioni v=0. È abbastanza facile programmare ad es. DERIVE™ per ottenere iterativamente, da soluzioni razionali date, molte altre soluzioni, anche nel caso k=30 (partendo dalla soluzione $(19, \pm 83)$): dimostrare però che in questo modo se ne ottengono infinite distinte tuttavia non è immediato. La prima dimostrazione dell'esistenza di infinite soluzioni razionali (ma solo per certi k) è dovuta a Fueter (1930): questa dimostrazione copre i casi k=-2 e k=30 [M].

3. Fermat lesse il testo di Diofanto commentato da Bachet: su di esso scrisse anche il famoso enunciato del suo "ultimo teorema", ma si occupò anche della nostra equazione; egli osservava [F] che provare che le uniche soluzioni intere di (B_{-2}) sono date da x=3 era "questione…difficile da indagare" ma che egli aveva trovato una "dimostrazione che non lascia dubbi". Asseriva che il problema del caso I non era stato finora esaminato da nessuno, nemmeno da Bachet [F]. Come sempre, egli non pubblicò mai nulla al proposito: egli però pose ai matematici inglesi, tra gli altri, proprio il problema di provare che le uniche soluzioni si trovano, nel caso I di (B_{-2}), per x=3. Solo molti anni dopo Eulero pubblicò una dimostrazione (peraltro insufficiente) di questo fatto, che venne provato compiutamente solo circa un altro secolo dopo. Solo Mordell nel 1918 dimostrò che il caso I ha sempre al più un numero finito di soluzioni (eventualmente zero). Non esistono a mia conoscenza altri risultati così generali al proposito.

4. Cercherò di descrivere brevemente le tecniche principali di studio, con riguardo ai casi particolari più elementari (se non più semplici).

a- Il metodo più immediato di studio è fornito da congruenze: con esse è spesso possibile provare che non vi sono soluzioni intere.

Sono di particolare importanza i risultati relativi alle soluzioni di $x^2 \equiv m \pmod p$, vale a dire i cosiddetti residui quadratici; in questo modo si possono risolvere, tra molti, i casi

k=23 [AG]: si esaminano le possibilità per x mod 4, e per eliminare il caso difficile $x \equiv 1 \pmod 4$ si usa il fatto che -1 è un residuo quadratico mod p (p primo dispari) se e solo se $p \equiv 1 \pmod 4$;

k = -73 [AG]: sempre usando residui quadratici, si può mostrare che neanche in questo caso c'è soluzione;

k = 45 [AG]: la risoluzione è elementare perché si può scrivere $45=2\cdot6^2-3^3=2\cdot3^2+3^3$;

$k = (4n-1)^3-4m^2$ con n intero e m privo di fattori primi $\equiv 3 \pmod 4$ [AG]: un caso del genere si ha con k= -19 = 81-100. Più in generale ancora, si possono trattare così casi in cui k è della forma $am^2+ bn^3$ con a, b, m, n interi soggetti a varie restrizioni (casi particolari k= -17, 42, -82, 11): vedi [M], [AG].

5. Come si vede, i risultati sono molto frammentari; ma anche utilizzando tecniche molto più avanzate non si sono ancora ottenuti risultati conclusivi. Accenno brevemente ad altre tecniche di analisi assai più complesse:

b- Uso dei campi quadratici, con trasformazione della (B_k) in equazioni ausiliarie. Tra i risultati provabili in questo modo:

k= -2 ha solo le soluzioni intere previste da Fermat (x=3); simile il caso

k= -13; le sole soluzioni sono per x=17.

Se k=7, 34, 58, 70, 159 non esistono soluzioni.

c- Uso delle forme cubiche. Questo strumento ha permesso a Mordell di provare l'esistenza soltanto di un numero finito di soluzioni [M]. In [H] sono descritte tutte le soluzioni dei casi I con $0< k \le 100$, tra cui finalmente il risultato per k=30: vi è, nel caso I, solo la coppia di soluzioni già menzionata.

d- Uso di algoritmi: il fatto che vi sia soltanto un numero finito di soluzioni in interi parrebbe permettere, almeno nei casi più semplici, una ricerca esaustiva di queste, se non altro per prova ed errore. Tuttavia, a quanto ne so, non vi sono algoritmi generali per la ricerca di soluzioni che siano utilizzabili in pratica, soprattutto per il fatto che la limitazione trovata per le soluzioni (nel caso I) è astronomica: Baker (1968) ha provato che |x| ed |y| si maggiorano con $\exp(10^{10}|k|^{1000})$!

A quasi quattro secoli di distanza, l'equazione di Bachet non smette di porre problemi sulla natura dei numeri interi.

Bibliografia: [AG] Adams-Goldstein, Introduction to Number Theory, Prentice Hall 1976. [D] Dickson, History of the theory of Numbers vol.II: Diophantine Analysis, Stechert 1934. [F] Fermat, Osservazioni su Diofanto, trad. it. Boringhieri 1959. [H] Hemer, 'Notes on the Diofantine Equation $y^2-k=x^3$', Arch. för Mat. 3 (1958), 67-77. [M] Mordell, Diofantine Equations, Academic Press 1969.

* Università degli Studi di Bologna

Ai lettori

Se non siete soci Mathesis di Verona, vi invitiamo a versare 12.000 lire per 12 numeri mediante vaglia postale o assegno bancario non trasferibile intestato a Corso Luciano c/o Mathesis Verona - Via IV Novembre, 11 b – 37126 Verona – specificando bene indirizzo con cap di chi effettua il versamento. Altrimenti potreste non ricevere più il presente foglio.