Infinito completato vs. incompleto in aritmetica

Edward Nelson

Dipartimento di matematica, Università di Princeton

I *numeri* sono 0, 1, 2, 3, ... I numeri costituiscono l'infinito più semplice, e dunque se vogliamo capire l'infinito ci conviene di tentare di capire i numeri.

Invece di usare i simboli 1, 2, ecc. di origine indiana, usiamo la notazione della logica matematica: i numeri sono 0, S0, SS0, SSS0, ... dove si può leggere S come "successore". Questa notazione esprime chiaramente l'idea che i numeri si ottengono da un processo di contare, l'uno dopo l'altro.

Ci sono almeno due modi diversi da pensare ai numeri: come un infinito completato oppure come un infinito incompleto. Non faremo un errore grave se chiamiamo questi il modo *platonico* (P) e il modo *aristotelico* (A).

Ora, ho già fatto un grande errore in questa conferenza a causa di una trappola di linguaggio. Ho parlato di P e A come due modi di pensare a "i numeri". Ma vedremo che P e A danno due sistemi di numeri *diversi*, non due modi di pensare allo stesso sistema.

Cominciamo con P, che è il punto di vista della matematica contemporanea. I numeri costituiscono un infinito completato notato $\mathbb{N}$. S'intende che i variabili x, y, e così via, sono elementi di $\mathbb{N}$. La proprietà fondamentale di $\mathbb{N}$ è *l'induzione*:

Ipotesi:
  0 ha la proprietà p;
  se x ha la proprietà p, allora Sx ha la proprietà p.
Conclusione:
  per ogni x, x ha la proprietà p.

La prima ipotesi è la *base* e la seconda è il *passo induttivo*. Per un numero specifico, ad esempio SSS0, non è necessario assumere l'induzione per dimostrare la conclusione dalle ipotesi. Infatti, supponiamo $p(0)$. Allora, usando successivamente il passo induttivo, otteniamo $p(\mathrm{S0})$, $p(\mathrm{SS0})$, e infine $p(\mathrm{SSS0})$. Cionondimeno, l'induzione è un assioma potente e molte proprietà dei numeri sono dimostrabili soltanto tramite l'induzione. Ecco un esempio.

Sia p la proprietà di x seguente: esiste un numero y non zero divisibile da ogni numero z non zero tale che $z \leq x$. Sostengo che ogni numero x ha la proprietà p. Certo che 0 ha la proprietà p (sia $y = \mathrm{S}0$). Supponiamo che x abbia la proprietà p, e dunque che esiste un numero y' non zero divisibile da ogni numero z non zero tale che $z \leq x$. Per induzione, ci resta soltanto di dimostrare il passo induttivo, che $\mathrm{S}x$ ha la proprietà p; cioè, che esiste un numero y non zero divisibile da ogni numero z non zero tale che $z \leq \mathrm{S}x$. Ma è vero: sia $y = y' \cdot \mathrm{S}x$ e consideriamo qualunque numero z non zero con $z \leq \mathrm{S}x$. Allora o $z \leq x$, nel qual caso esso divide y' e dunque divide $y = y' \cdot \mathrm{S}x$, oppure $z = \mathrm{S}x$, nel qual caso pure esso divide y, ciò che conclude la dimostrazione.

Nei primi anni del novecento, Bertrand Russell e Henri Poincaré scambiarono polemiche sopra la natura dell'induzione. Secondo Poincaré, l'induzione è un principio logico, una specie di sillogismo infinito. Russell sostenne che l'induzione è soltanto una definizione verbale—i numeri sono *definiti* come quegli oggetti che ubbidiscono all'induzione. Né l'uno né l'altro chiamò in questione la legitimità dell'induzione.

Nella matematica contemporanea, il punto di vista di Russell prevale. Oggi il solito fondamento della matematica è la teoria degli insiemi, teoria di Zermelo-Fraenkel con l'assioma di scelta (ZFC). Le proprietà sono reificate e diventano insiemi. Il numero 0 è definito come l'insieme vuoto, senza elementi. Per ogni insieme x, si definisce il suo successore $\mathrm{S}x$ come l'insieme i cui elementi sono gli elementi di x pure che l'insieme x stesso. Si dice che un insieme X è *induttivo* se 0 è un elemento di X e se ogni volta che x è un elemento di X, allora anche il suo successore $\mathrm{S}x$ è elemento di X. *L'assioma dell'infinito* di ZFC asserisce che esiste un insieme induttivo. Poi si dimostra che esiste un unico insieme induttivo minimale e si definisce $\mathbb{N}$, l'insieme di tutti i numeri, come questo insieme.

Detto verbalmente, tutto ciò riviene a questo: una proprietà è *induttiva* se e solo se sodisfa alla base e al passo induttivo; un oggetto è un *numero* se e solo se ha ogni proprietà induttiva. Così una proprietà che gli oggetti possono avere, quella di essere un numero, è definita tramite la collezione di tutte le proprietà che possono avere gli oggetti. Questa è una definizione impredicativa. L'impredicatività disturba profondamente alcuni pensatori; altri non vedono nessun problema. La matematica contemporanea è completamente impredicativa.

Quale fondamento per l'aritmetica, questa definizione non sodisfa. Certo che l'aritmetica, la teoria dei numeri, è la teoria matematica la più primitiva. Ma la si basa sulla teoria, ben più sofisticata, degli insiemi. Inoltre, il procedimento di reificare le proprietà come insiemi—rimpiazzando una proprietà, concetto intensionale, con l'insieme esten-

sionale di tutti gli oggetti che hanno la proprietà—conduce a contradizzioni ben note se non si prende cura, come Russell stesso scoprì nel suo paradosso famoso dell'insieme di tutti gli insiemi che non sono elementi di se stessi.

Strettamente legata all'induzione è la costruzione di numeri per mezzo della *ricorsione primitiva*. Questa si fa specificando prima il valore quando $y = 0$ (la *base*) e poi il valore per $\mathrm{S}y$ per mezzo del valore per y (il *passo ricorsivo*). Allora, per esempio, il valore per $y = \mathrm{SSS0}$ è determinato: il valore per $y = 0$ ci è dato, da questo otteniamo il valore per $y = \mathrm{S0}$, poi il valore per $y = \mathrm{SS0}$, e infine il valore per $y = \mathrm{SSS0}$. Introduciamo l'addizione $+$, la moltiplicazione $\cdot$, l'esponenziazione $\uparrow$, e la super-esponenziazione $\Uparrow$, e così via, come segue:

$$\begin{array}{ll} x + 0 = x, & x + \mathrm{S}y = \mathrm{S}(x + y); \\ x \cdot 0 = 0, & x \cdot \mathrm{S}y = x + (x \cdot y); \\ x \uparrow 0 = \mathrm{S0}, & x \uparrow \mathrm{S}y = x \cdot (x \uparrow y); \\ x \Uparrow 0 = \mathrm{S0}, & x \Uparrow \mathrm{S}y = x \uparrow (x \Uparrow y); \end{array}$$

e così via. Allora

$$\begin{array}{ll} x + y = \mathrm{S} \ldots \mathrm{S}x & \text{con } y \text{ occorrenze di S}, \\ x \cdot y = x + \ldots + x & \text{con } y \text{ occorrenze di } x, \\ x \uparrow y = x \cdot \ldots \cdot x & \text{con } y \text{ occorrenze di } x, \\ x \Uparrow y = x \uparrow \ldots \uparrow x & \text{con } y \text{ occorrenze di } x, \end{array}$$

e così via. Queste sono ricorsioni primitive. Ackermann dimostrò come andare inoltre alle ricorsioni primitive. Notiamo F_0, F_1, F_2, F_3, e così via, le funzioni $+$, $\cdot$, $\uparrow$, $\Uparrow$, e così via. Allora, una versione della funzione Ackermann è la funzione A il cui valore su y è $A(y) = y\,\mathrm{F}_y\,y$. Questa funzione è ricorsiva—per qualsiasi y abbiamo un procedimento meccanico per calcolare il valore $A(y)$—ma la funzione cresce ben più rapidamente di ogni funzione ricorsiva primitiva. Questa costruzione è un altro esempio del metodo diagonale di Cantor, metodo che Cantor usò per dimostrare che il continuo (i numeri reali) non è numerabile, un infinito più grande di $\mathbb{N}$, metodo che anche è alla base del paradosso di Russell e dei teoremi d'incompletezza di Gödel.

Si vuole che l'idea generale di funzione ricorsiva esprima il concetto di algoritmo. La parola *algoritmo* viene dal nome, al'Khwarizmi, dell'autore del trattato altamente influente *Al-Jabr wa-al-Muqabilah* scritto circa nel 820 (e la parola *algebra* stessa proviene dal titolo del libro!). Ma passarono più di undici secoli prima che fosse ricercato il problema di definire il significato di algoritmo, di definire il concetto di funzione ricorsiva. Il procedimento di Ackermann dimostra l'impossibilità

di fare una definizione sintattica esplicita del concetto di funzione ricorsiva, perchè ciò permetterebbe di elencarle e poi la costruzione diagonale darebbe una nuova funzione ricorsiva.

Il problema è stato risolto in tre modi apparentemente diversi da Church, Gödel, e Turing (rispettivamente professore all'Università di Princeton, socio permanente dell'Istituto per lo Studio Avvanzato a Princeton, e studente all'Università di Princeton, noto con orgoglio di paese), e queste tre definizioni si rivellarono equivalenti. Gödel stesso ha detto che la definizione di Turing è la migliore. Il lavoro di Turing costruì i fondamenti dell'informatica e il suo articolo [6] del 1936 è interessante ancora oggi, ma bisgona stare attenti al fatto che in questo articolo "computer" significa "persona che calcola".

Si può descrivere la definizione di Turing come segue. Consideriamo un programma computer (questo è un oggetto sintattico concreto) che prende i numeri come argomenti. Allora è un *algoritmo* se e solo se per ogni argomento, prima o poi il calcolo termina con un numero come valore (questo è un concetto semantico astratto). Il problema di decidere se o no un programma termina per ogni argomento non è risolvibile algoritmicamente; ciò significa che per un programma generale non c'è nessun modo per determinare se sia un algoritmo oltre che cercare fra tutti gli infiniti argomenti possibili e per ognuno di essi aspettare pazientemente—per sempre, se necessario—a vedere se il calcolo termina con un valore. Ecco l'infinito completato senza scherzi! (In uno dei libri del paese di Oz, lo Spaventapasseri dice, "Può darsi che resteremo intrappolati quì per sempre!" La Ragazza Mosaica chiede, "Quanto dura il 'per sempre'?" e lo Spaventapasseri risponde, "È proprio questo che scopriremo subito.")

* * *

Ora facciamo una critica aristotelica (come la chiamo) di queste idee, considerando i numeri come un infinito incompleto. Si può notare che etimologicamente l'aggettivo nella locuzione "infinito incompleto" è superfluo, dato che la parola *infinito* significa non finito (nel senso di "no ho finito").

Come abbiamo visto, l'induzione e la ricorsione primitiva si basano sul concetto dei numeri come un infinito completato. Introduciamo il concetto di un *numero da contare*. Questo è un concetto primitivo dell'aritmetica-A, e piuttosto che tentare di definirlo, enumciamo gli assiomi che postuliamo per questo concetto. Questi assiomi sono la base dell'induzione e il passo induttivo, cioè

0 è un numero da contare;
se y è un numero da contare, lo è anche Sy.

Ecco tutto quello che supponiamo riguardante questo concetto, e in particolare non postuliamo che tutti i numeri siano numeri da contare.

Usando le cifre arabiche (così chiamate benchè siano d'origine indiana e fossero trasmesse all'ovest principalmente dal persiano al'Khwarizmi), chiediamo se, dato un numero specifico y definito per mezzo di una ricorsione primitiva, ad esempio $y = 2 \Uparrow 5$ oppure $y = 2 \Uparrow 2 \Uparrow 5$, si può dimostrare che è un numero da contare. Ora, dire che c'è una dimostrazon ovvia di y passi è un ragionamento circolare, perchè i passi sono cose che si contano, e dunque i passi si possono contare solo se infatti y è un numero da contare. Si nota che $2 \Uparrow 5 = 2 \uparrow 2 \uparrow 2 \uparrow 2 \uparrow 2 = 2 \uparrow 65536$ è un numero super-astronomicamente grande, e che $2 \Uparrow 2 \Uparrow 5$ è uguale a $2 \uparrow \ldots \uparrow 2$ con quel numero, $2 \Uparrow 5$, di occorrenze di 2.

Facciamo le due definizioni seguenti:

1. x è un *numero additivo* se e solo se per ogni numero da contare y, anche $x + y$ è un numero da contare;
2. x è un *numero moltiplicativo* se e solo se per ogni numero additivo y, anche $x \cdot y$ è un numero additivo.

Allora abbiamo i teoremi seguenti:

3. Se x è un numero additivo, x è un numero da contare.
4. Se x è un numero moltiplicativo, x è un numero additivo.
5. Se x è un numero moltiplicativo, x è un numero da contare.
6. Se x e z sono numeri additivi, lo è anche $x + z$.
7. Se x e z sono numeri moltiplicativi, lo è anche $x + z$.
8. Se x e z sono numeri moltiplicativi, lo è anche $x \cdot z$.

Le dimostrazioni sono facili. Per 3, sia x un numero additivo. Applichiamo la definizione 1 a $y = 0$, che è un numero da contare. Allora $x + 0$ è un numero da contare, ma $x + 0 = x$.

Per 4, sia x un numero moltiplicativo. Applichiamo la definizione 2 a $y = 1$, che è un numero additivo, come facilmente si vede. Allora $x \cdot 1$ è un numero additivo, ma $x \cdot 1 = x$.

Notiamo che 5 è conseguenza di 3 e 4.

Per 6, siano x e y numeri additivi, e sia y un numero da contare qualunque. Secondo la definizione 1, dobbiamo dimostrare che $(x+z)+y$ è un numero da contare. Notiamo che $z + y$ è un numero da contare, secondo la definizione 1, e dunque $x + (z + y)$ è un numero da contare, sempre secondo la definizione 1. Ma $x + (z + y) = (x + z) + y$.

Per 7, siano x e z numeri moltiplicativi, e sia y un numero additivo qualunque. Secondo la definizione 2, dobbiamo dimostrare che $(x+z)\cdot y$ è un numero additivo. Notiamo che $z+y$ è un numero additivo, secondo la definizione 2, e che $x+y$ è un numero additivo, sempre secondo la definizione 2. Dunque $(x\cdot y)+(z\cdot y)$ è un numero additivo secondo il teorema 6. Ma $(x\cdot y)+(z\cdot y)=(x+z)\cdot y$.

Per 8, siano x e z numeri moltiplicativi, e sia y un numero additivo qualunque. Secondo la definizione 2, dobbiamo dimostrare che $(x\cdot z)\cdot y$ è un numero additivo. Notiamo che $z\cdot y$ è un numero additivo, secondo la definizione 2, e dunque $x\cdot(z\cdot y)$ è un numero additivo, sempre secondo la definizione 2. Ma $x\cdot(z\cdot y)=(x\cdot z)\cdot y$.

Ora possiamo dimostrare che $2\Uparrow 5$ è un numero da contare. Poniamo

$$\mathrm{a}_0 = 2,\ \mathrm{a}_1 = \mathrm{a}_0\cdot\mathrm{a}_0,\ \mathrm{a}_2 = \mathrm{a}_1\cdot\mathrm{a}_1,\ \ldots,\ \mathrm{a}_{16} = \mathrm{a}_{15}\cdot\mathrm{a}_{15}.$$

Allora $a_{16} = 2\Uparrow 5$. Si vede facilmente che 2 è un numero moltiplicativo. Applicando il teorema 8 seidici volte, vediamo che a_1, a_2, ..., e $\mathrm{a}_{16} = 2\Uparrow 5$ sono numeri moltiplicativi, e dunque $2\Uparrow 5$ è un numero da contare secondo il teorema 5, ciò che conclude la dimostrazione. Ma nessuno mai dimostrerà che $2\Uparrow 2\Uparrow 5$ è un numero da contare.

Perchè non si può continuare la serie di definizioni e teoremi? Supponiamo di definire

> 9. x è un *numero esponenziabile* se e solo se per ogni numero moltiplicativo y, $x\uparrow y$ è un numero moltiplicativo.

Ma allora non possiamo dimostrare

> 10. Se x e z sono numeri esponenziabili, lo è anche $x\uparrow z$.

La difficoltà è che l'esponenziazione non è associativa; cioè, in genere $x\uparrow(z\uparrow y)\neq(x\uparrow z)\uparrow y$, e abbiamo usato l'associatività dell'addizione e della moltiplicazione nei teoremi 6 e 8. Infatti, si può dimostrare il seguente: non esiste una proprietà p tale che si può dimostrare che se $p(x)$ allora x è un numero da contare e che se $p(x)$ e $p(z)$ allora $p(x\uparrow z)$. Questo teorema non è facile; la dimostrazione impiega il teorema profondo di Hilbert e Ackermann sull'eliminazione dei quantificatori. Vedi il capitolo 18 del libro dell'autore *Predicative Arithmetic* [4].

Insomma, da un punto di vista A, l'esponenziazione dei numeri non è un concetto ben definito. Per conseguenza, la matematica-A è *molto* più debole della matematica-P. Per esempio, il teorema sulla divisibilità che abbiamo dimostrato per l'induzione non può essere stabilito. Ciononostante, per alcune ragioni vale la pena di perseguire la matematica-A. Una ragione è che una quantità veramente sorprendente

della matematica avvanzata può essere sviluppata da questo punto di vista con grande simplificazione dei mezzi tecnici; vedi il libro dell'autore *Radically Elementary Probability Theory* [5].

Un'altra ragione per sviluppare la matematica-A è il suo legame coi problemi della complessità computazionale, campo molto attivo della matematica e dell'informatica teorica. Ora esaminiamo questo legame.

Turing, Church, e Gödel hanno risolto—a condizione che si accetti $\mathbb{N}$ come infinito completato—il problema "cos'è un algoritmo?". Con l'avvento dei computer si pone il problema, "cos'è un algoritmo *fattibile*?". È emerso un consenso fra gli studenti della complessità computazionale che la definizione giusta è una *funzione di tempo polinomiale*. Queste sono le funzioni tali che esistono una macchina di Turing (programma computer) e un polinomio π tali che per ogni numero y il calcolo termina e dà un valore dopo al massimo $\pi(\log y)$ passi. Questa è una definizione complicata che a prima vista sembra piuttosto arbitraria. Ma Bellantoni e Cook [1] [2], e anche Leivant [3], hanno dato una definizione equivalente che si può descrivere come segue.

Consideriamo di nuovo la ricorsione primitiva. Vogliamo definire $F(x, y)$, e a questo scopo specifichiamo un valore quando $y = 0$ e poi specifichiamo un valore per $F(x, \mathrm{S}y)$ in termini di x e del valore per $F(x, y)$:

$$F(x, 0) = G(x), \quad F(x, \mathrm{S}y) = H\big(x, F(x, y)\big).$$

Quì G e H sono date in termini di 0, S, e funzioni già definite. Allora abbiamo

$$\begin{aligned}
F(x, 0) &= G(x), \\
F(x, \mathrm{S0}) &= H\big(x, F(x, 0)\big) = H\big(x, G(x)\big), \\
F(x, \mathrm{SS0}) &= H\big(x, F(x, \mathrm{S0})\big) = H\big(x, H\big(x, G(x)\big)\big), \\
F(x, \mathrm{SSS0}) &= H\big(x, F(x, \mathrm{SS0})\big) = H\big(x, H\big(x, H\big(x, G(x)\big)\big)\big),
\end{aligned}$$

e così via fino al valore di $F(x, y)$.

Affinchè questo abbia senso, bisogna che y sia un numero da contare, perchè la definizione è una costruzione passo-a-passo da 0 a S0, a SS0, ..., e infine a y, ma anche se y è un numero da contare *non sappiamo che il valore* $F(x, y)$ *è un numero da contare* (a meno che non facciamo il postulato platonico che tutti i numeri sono numeri da contare). Una *ricorsione predicativa* è una ricorsione primitiva tale che tutte le ricursioni sono solamente sopra i numeri da contare.

Vediamo come funziona questo. Non c'è problema per l'addizione:

$$x + 0 = x, \quad x + \mathrm{S}y = \mathrm{S}(x + y).$$

Questo ha senso per ogni numero x e ogni numero da contare y. Adesso supponiamo che ambo i numeri x e y sono numeri da contare. Allora non c'è problema con la moltiplicazione:

$$x \cdot 0 = 0, \quad x \cdot \mathrm{S}y = (x \cdot y) + x$$

dato che abbiamo definito predicativamente la somma di un numero qualunque, come $x \cdot y$, con un numero da contare, come x. Questi sono esempi della ricorsione predicativa. Ma l'esponenziazione è impredicativa. Nella costruzione

$$x \uparrow 0 = \mathrm{S}0, \quad x \uparrow \mathrm{S}y = x \cdot (x \uparrow y)$$

non si sa che il numero $x \uparrow y$ è un numero da contare—ma la ricorsione predicativa per la moltiplicazione è predicativamente definita soltanto se il secondo argomento è un numero da contare. E infatti, l'esponenziazione è infattibile.

Bellantoni e Cook, e Leivant, hanno dimostrato che una funzione è una funzione di tempo polinomiale (algoritmo fattibile) se e solo se è costruita da una ricorsione predicativa. Questa è una caratterizzazione semplice e bella: non c'è niente che riguardi le macchine di Turing o i polinomi in questa descrizione, ma è equivalente alla definizione complicata già data.

* * *

Per concludere, il pensare ai numeri come un infinito incompleto è un alternativo viabile e interessante al pensare ai numeri come un infinito completato, alternativo che conduce a grandi simplificazioni in alcune aree della matematica e che ha legami forti con la teoria della complessità computazionale.

I due modi, P e A, di pensare ai numeri conducono a sistemi di numeri diversi. Quello che è un numero finito per P non è necessariamente numero finito per A. Nella matematica contemporanea, il concetto del finito viene definito tramite l'infinito completato $\mathbb{N}$. Non esiste un concetto chiaro del finito in termini del quale si può definire l'infinito come il non-finito. Nella matematica contemporanea, platonica, si va nel senso opposto e si definisce il finito come il non-infinito.

Forse dovremmo avere un congresso interdisciplinare sul finito. Come ha detto Orazio, "Ci sono meno cose in cielo e in terra, Amleto, di quante la tua filosofia abbia sognato."

Bibliografia

[1] Stephen Bellantoni and Stephen Cook, "A new recursion-theoretic characterization of the poly-time functions", *Computational Complexity*, 2:97–110, 1992.

[2] Stephen Bellantoni, *Predicative Recursion and Computational Complexity*, Ph.D. Thesis, University of Toronto, 1992.
ftp://ftp.cs.toronto.edu/pub/reports/theory/cs-92-264.ps.Z

[3] Daniel Leivant, "Ramified recurrence and computational complexity I: Word recurrence and poly-time", in Peter Cole and Jeffrey Remmel, editors, *Feasible Mathematics II*, Perspectives in Computer Science, pages 320-343, Birkhauser-Boston, New York, 1994.

[4] Edward Nelson, *Predicative Arithmetic*, Mathematical Notes #32, Princeton University Press, Princeton, New Jersey, 1986.
http://www.math.princeton.edu/~nelson/books/pa.pdf

[5] —, *Radically Elementary Probability Theory*, Annals of Mathematics Studies, Number 117, Princeton University Press, Princeton, New Jersey, 1987.
http://www.math.princeton.edu/~nelson/books/rept.pdf

[6] A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem", Proceedings of the London Mathematical Society, Series 2, 42, pp. 230–265, 1936. Errata in 43, pp. 544–546, 1937.
http://www.abelard.org/turpap2/tp2-ie.asp