

Miriam Di Ianni

IL SENTIERO DEI PROBLEMI IMPOSSIBILI

Da Euclide al problema da un milione di dollari

scienza **FA**



FrancoAngeli

scienza **FA**

Una collana di saggi per il lettore non specialista:
per comprendere la realtà che ci circonda

Collana diretta da:
Renato Betti, Politecnico di Milano
Roberto Lucchetti, Politecnico di Milano
Giuseppe Rosolini, Università di Genova

Miriam Di Ianni

IL SENTIERO DEI PROBLEMI IMPOSSIBILI

Da Euclide al problema da un milione di dollari

scienza **FA**

FrancoAngeli

Progetto grafico di copertina: Géraldine D'Alessandris

1a edizione. Copyright © 2020 by FrancoAngeli srl, Milano, Italy

L'opera, comprese tutte le sue parti, è tutelata dalla legge sul diritto d'autore. L'Utente nel momento in cui effettua il download dell'opera accetta tutte le condizioni della licenza d'uso dell'opera previste e comunicate sul sito www.francoangeli.it.

Se sei aperto e umile, la matematica ti condurrà per mano. Molte e molte volte, quando ero in dubbio su come procedere, ho dovuto solo attendere finché questo è accaduto. Ciò mi ha portato lungo un sentiero inaspettato dove si sono aperte nuove prospettive, un sentiero che conduceva a un nuovo territorio, dove si poteva preparare una base operativa da cui esaminare il panorama presente e pianificare il progresso futuro.

Paul Dirac

Solo perché un problema non è ancora stato risolto non è detto che sia impossibile da risolvere.

Agatha Christie

Indice

Prologo	pag.	11
1. Che problema!	»	17
1.1. Il signor problema e le sue istanze	»	18
1.2. C'è istanza e istanza	»	20
1.3. Si fa presto a dir difficile	»	22
1.4. Unità di misura	»	25
2. Un mondo da descrivere	»	27
2.1. L'invenzione del metodo assiomatico	»	29
2.2. Oltre la geometria: la teoria degli insiemi	»	32
2.3. "Concordo con lei su tutte le cose essenziali"	»	38
2.4. Il falso e il vero	»	42
2.5. Bando alle intuizioni!	»	46
2.6. Un esempio eccellente	»	49
2.7. L'aritmetica di Peano*	»	52
2.8. Ma sarà vero quel che è vero?	»	55
3. La perfetta conoscenza	»	58
3.1. Sistemi assiomatici e metamatemica	»	59
3.2. La sfida di Hilbert: dobbiamo sapere, sapremo!	»	63
3.3. Ci sono più cose in cielo e in terra...	»	66
3.4. Questione di punti di vista	»	69
3.5. Un'occhiata al Teorema di Gödel*	»	70

3.6. Cosa resta del sogno	pag.	77
3.7. <i>L'Entscheidungsproblem</i> e Turing*	»	79
4. L'araba fenice	»	83
4.1. Mi capisci quando parlo?	»	84
4.2. Il passo elementare: un passo da gigante	»	86
4.3. Scelte obbligate	»	89
4.4. L'appetito vien mangiando	»	94
4.5. Una macchina? È una parola!...	»	97
4.6. Dalla macchina alla... metamacchina	»	99
4.7. La macchina di Turing Universale*	»	100
4.8. Una macchina dal potere... incalcolabile!	»	119
5. La forma e la sostanza	»	125
5.1. Universalità	»	126
5.2. Algoritmi e modelli di calcolo	»	129
5.3. Dal nastro ai registri	»	132
5.4. Registri e numeri interi	»	138
5.5. Macchine a registri	»	140
5.6. Macchina di Turing vs Macchina a Registri (e tutto il resto)	»	144
5.7. La macchina a Registri Universale*	»	146
5.8. L'architettura di Von Neumann – e tutto quel che segue	»	152
5.9. Appendice	»	157
6. Fugge il tempo	»	160
6.1. La Torre di Hanoi	»	161
6.2. Problema, ma quanto mi costi?	»	166
6.3. Algoritmo, ma quanto mi costi?	»	168
6.4. Ma, poi, che cos'è un algoritmo?	»	173
6.5. Modelli e complessità	»	175
6.6. La Teoria della Complessità Computazionale	»	179
6.7. Polinomiale è bello	»	180
6.8. P: la classe dei problemi risolvibili per davvero	»	187
6.9. Fuori da P! O forse no?	»	190

7. <i>Deus et machina</i>	pag.	193
7.1. Questione di punti di vista	»	196
7.2. Problemi, aghi e pagliai	»	199
7.3. Le angustie di Cassandra – la questione delle istanze negative	»	202
7.4. Quando Cassandra ha importanza – la classe NP	»	206
7.5. (Meta)Problemi, indovine, e supermodelli	»	209
7.6. Un’idea di non determinismo	»	213
7.7. Il SuperModello e la classe NP	»	216
7.8. Appendice	»	219
8. Nel cuore del mistero	»	223
8.1. L’importanza di essere NP	»	224
8.2. Se si dimostrasse che $P \neq NP$	»	226
8.3. Se si dimostrasse che $P = NP$	»	228
8.4. Da problema a problema	»	230
8.5. Il padre di tutti i problemi	»	234
8.6. Lo zoccolo duro e la questione fondamentale	»	238
8.7. Una dimostrazione del Teorema di Cook-Levin*	»	241
9. Oltre	»	257
9.1. L’arte di accontentarsi	»	258
9.2. Un fiume in piena	»	262
9.3. Tante belle cose	»	265

Prologo

Al ristorante con un gruppo di amici, nel momento del conto, arriva la solita, immancabile, richiesta: “Calcoli tu il costo a persona? Sei un matematico!”. E lui, il matematico, facendo buon viso a cattivo gioco, sorridendo a denti stretti, esegue la divisione e pensa: “Eh, certo, la laurea in matematica l’ho presa giusto per imparare a fare le divisioni...”. Forse, in una situazione del genere ti sarai trovato anche tu, potenziale lettore, che stai sfogliando – più o meno distratamente – queste pagine per capire di che cosa si occupa il libro che ti è capitato fra le mani.

Se sei un matematico, non occorre certo spiegarti la frustrazione che si prova di fronte a siffatta richiesta. Se non sei un matematico, allora... prova a vederla così: pensare a un matematico come a qualcuno bravo a fare i conti è come pensare a Dante Alighieri come a uno che sapeva scrivere senza fare errori di ortografia!

E, comunque, se sei interessato alla questione, trovi in libreria una quantità di pubblicazioni che, affrontando molte delle sfumature possibili delle quali la matematica si adorna, declinate in tutti i livelli di dettaglio e complessità immaginabili (per lettori che spaziano dalla scuola elementare all’università, per intenderci), sono in grado di soddisfare ogni tua possibile curiosità.

Come il matematico al termine di ogni cena al ristorante, anche l’informatico è spesso oggetto di richieste, diciamo così, “ingenue” circa le sue competenze: “Tu che sei informatico, mi insegni a scaricare i film?” o “Visto che sei informatico, mi installi tale pacchet-

to?” o ancora “Il mio computer si è preso un virus, me lo sistemi tu, che sei informatico?”...

Richieste del tipo appena elencato andrebbero correttamente indirizzate a un *tecnico informatico*, ossia a un professionista che si occupa degli aspetti, per l'appunto, tecnici dell'informatica. Ma, nell'immaginario comune, se sei un informatico, se sei un laureato in informatica, le tue competenze sono esattamente quelle di un tecnico informatico – niente di meno, niente di più.

Nell'immaginario collettivo, appunto, l'informatica è una questione puramente tecnologica. Così, un informatico è uno che sa *usare* bene il calcolatore (o computer, se amate gli anglismi). Nulla di più falso. Chi *usa* il calcolatore non è l'informatico. L'informatico, il computer, lo costruisce. O, meglio, l'informatico insegna al computer a comportarsi come ci si aspetta che esso si comporti.

Per esempio, parte del bagaglio di competenze di un informatico è il “pensare algoritmico”, che significa affrontare la questione della risoluzione di un problema *progettando un procedimento risolutivo che possa essere insegnato a un calcolatore*. Questo richiede capacità di affrontare un'approfondita analisi critica del problema, capacità di decomporre il procedimento risolutivo in passi elementari di calcolo, capacità di descrizione del procedimento in un linguaggio comprensibile al calcolatore...

Spesso si confonde, nell'immaginario collettivo, il pensare algoritmico con l'utilizzare un algoritmo progettato da altri. Ma, fra i due approcci la distanza è immensa: progettare un algoritmo è, in qualche modo, costruire un calcolatore, eseguire un algoritmo (progettato da altri) è scimmiettare (comportarsi come) un calcolatore. E, purtroppo, confondere i due piani è alla base del grande fraintendimento che, mediamente, si incontra quando si parla di informatica.

Ecco, in siffatto garbuglio di idee poco chiare, si colloca questo libro. L'obiettivo, con esso, è quello di convincere il lettore che l'Informatica è una Scienza – con la “S” maiuscola, al pari di altre Scienze quali la matematica, la fisica, la chimica. Una Scienza, l'informatica, che utilizza, per crescere, gli stessi strumenti utilizzati dalle altre scienze: modellazione, progettazione, deduzione, verifica.

E questo obiettivo sarà perseguito attraverso un racconto che evidenzierà l'inestricabile intreccio che aggroviglia l'informatica

a quella, fra le discipline scientifiche, che merita l'appellativo di "scienza esatta": la matematica.

A questo scopo, seguiremo insieme un percorso il cui punto di partenza è rappresentato dalle origini dell'informatica e il cui punto di arrivo è l'aspetto, forse, più famoso dell'informatica teorica: la congettura, il teorema mai dimostrato, sulla cui dimostrazione è stata messa una taglia da un milione di dollari – un percorso costellato, appunto, di problemi "impossibili". E ci sarà tempo e modo di chiarire il senso del termine "impossibile".

Perché questa scelta? Partiamo dal punto di arrivo: il problema da un milione di dollari. Un problema che si domanda se due insiemi, **P** e **NP**, sono uguali. Due insiemi, entità decisamente matematiche, il cui significato è, però, di natura squisitamente informatica – due insiemi che non si riesce a mostrare se sono uguali oppure no. Un problema, dunque, a cavallo fra le due discipline. E che ha attirato l'attenzione dell'industria cinematografica – è stato trattato in più di una serie televisiva e anche in qualche film. Naturalmente, l'approccio mediatico è lungi dal poter essere considerato accurato sia rispetto al significato del problema sia rispetto alla portata della sua (eventuale) soluzione. Tuttavia, esso ha avuto l'indubbio merito di aver acceso l'attenzione su un "problema informatico". Anzi, un "problema informatico impossibile" (almeno per il momento).

Così, perché non partire proprio dal problema da un milione di dollari? O, meglio, perché non *arrivare* al problema da un milione di dollari? Sì, perché per comprendere bene, a fondo, il problema da un milione di dollari è necessario partire dall'inizio, proprio dal punto in cui l'informatica ha avuto origine. E quel punto, in qualche modo inaspettatamente, coincide con il punto in cui è entrato in crisi il tentativo di individuare i fondamenti ultimi della matematica. Perciò, per arrivare a parlare del problema da un milione di dollari non si potrà fare a meno di parlare di matematica e di mettere in luce il forte legame fra tale disciplina e l'informatica.

Il carattere di questo libro è divulgativo, con l'obiettivo dichiarato di renderlo fruibile anche ai non addetti ai lavori (che abbiano un minimo di formazione matematica), a tutti gli interessati alle questioni scientifiche. E con l'obiettivo segreto (e ambizioso) di avvicini-

nare alle scienze informatiche anche coloro i quali all'informatica-scienza guardano con diffidenza.

Il tono sarà, spesso, scanzonato – gli illustri eroi di questa storia saranno, talvolta, tirati in ballo in modo, diciamo così, “poco ortodosso”, ponendo loro, per esempio, domande che da sempre qualunque studente avrebbe voluto porre... o, comunque, giocando un po' con loro.

Il tono scanzonato non potrà che accostarsi a uno stile colloquiale e a un livello di descrizione quasi sempre informale e intuitivo. Scelte, queste, che hanno portato, necessariamente, a rinunciare in più di una situazione ai livelli di precisione, formalità e accuratezza che sarebbero doverosi in una trattazione scientifica¹ – rinuncia fatta a tutto vantaggio della (auspicabile) leggibilità della trattazione.

Sempre nell'ottica di stimolare quanto più possibile l'intuizione dei lettori, il linguaggio sarà, talvolta, grammaticalmente scorretto – ogni qualvolta lo sgrammaticato possa rivelarsi più incisivo del grammaticato². Ma tono giocoso, stile colloquiale e linguaggio sgrammaticato non traggano in inganno. Il materiale trattato è roba seria e seriamente trattata (tono, stile e linguaggio a parte). E si andranno a toccare argomenti delicati, dai sistemi assiomatici al Teorema di Gödel, dai modelli di calcolo al Teorema di Cook-Levin. Nel tentativo di renderli comprensibili a tutti.

Per bilanciare leggerezza del tono (utilizzata per coinvolgere i lettori meno esperti) e serietà dei contenuti (che possono essere apprezzati anche da lettori dotati di un maggiore bagaglio di competenze), l'approccio descrittivo sarà strutturato in due livelli:

- sezioni “normali”, auspicabilmente di semplice comprensione, nelle quali gli argomenti verranno introdotti in forma discorsiva, facendo ricorso all'intuizione e cercando di evitare le formalizzazioni;

1. Per fare un esempio, la Teoria della Complessità Computazionale è definita per problemi di decisione; d'altra parte, è probabile che la maggior parte dei lettori non abbia alcuna confidenza con i problemi di decisione (che potrebbero loro apparire poco significativi) e, dunque, per questa ragione, ho scelto di descrivere detta Teoria per problemi in cui viene richiesto il calcolo di una soluzione (in generale più consueti, immagino, per coloro i quali si avvicineranno a queste pagine).

2. E, con questa dichiarazione di intenti, mi sono anche parata le spalle a fronte degli errori che, inevitabilmente, avrò commesso...

- sezioni di approfondimento, più complesse, ove, invece, la formalizzazione non sarà bandita (pur rimanendo il più possibile “intuitivi”), dedicati ai lettori con una maggiore esperienza nella formalizzazione o, comunque, desiderosi di un maggiore livello di dettaglio – questi paragrafi saranno marcati con un asterisco (*).

Il libro è costruito in modo tale che le sezioni con asterisco possano essere saltate a pie’ pari senza che, per questo, venga compromessa la leggibilità del capitolo né la comprensione dell’argomento trattato.

I Capitoli 5 e 7, poi, contengono due Appendici nelle quali sono brevemente trattati dettagli o approfondimenti di taluni argomenti cui si accenna nei paragrafi del capitolo che costituiscono, in qualche modo, digressioni rispetto ai temi principali.

Pronti a partire, dunque. Ce n’è di strada da fare.

1

Che problema!

“Ma quanto è difficile questo problema!”, oppure “Questo problema è proprio impossibile da risolvere!”...

Fin dai tempi della nostra scuola elementare, quante volte abbiamo ascoltato (o pronunciato) queste frasi? Ma quand'è che possiamo affermare (senza tema di smentita) che un problema è davvero *difficile*?

Una prima risposta è quella egocentrica: se io non so risolvere il problema, allora, è ovvio, questo accade perché il problema è difficile. Solo che, a memoria d'uomo, un'argomentazione del genere non si è rivelata particolarmente utile per evitare un votaccio al compito di matematica. Ineccepibile, dal proprio punto di vista, per carità, ma un tantinello poco oggettiva.

Va bene. Allora, diciamo che un problema è difficile quando la metà degli studenti in una classe non sa risolverlo – o che è impossibile da risolvere quando proprio nessuno, in quella classe, sa risolverlo. Meglio, decisamente meglio. Ma se gli studenti di quella classe non avessero studiato a sufficienza? Potremmo ancora affermare che è colpa del problema se la classe non ha saputo risolverlo? O, ancora, se l'argomento non fosse stato spiegato con sufficiente chiarezza? Oppure, ancora, se quella classe fosse una terza elementare e il problema da risolvere fosse uno di quelli proposti all'esame di maturità scientifica? No, ancora non ci siamo: queste definizioni sono ancora troppo dipendenti dai fattori in gioco: le capacità della classe e del docente, il livello di difficoltà del problema rispetto al livello di conoscenza della classe, e via discorrendo.

In effetti, queste definizioni di difficoltà di un problema, che pure sono quelle alle quali immediatamente ci viene in mente di fare riferimento, soffrono di un inconveniente sostanziale: associano la difficoltà di un problema alle capacità di risolverlo degli individui che della sua risoluzione debbono occuparsi. Che, detto in altre parole, significa che, anziché misurare il livello di difficoltà di un problema, misurano il grado di adeguatezza a risolverlo di chi deve provvedere alla sua risoluzione. Ossia, queste definizioni di difficoltà fanno riferimento al risolutore più che a ciò che deve essere risolto.

Ma, allora, quando è che possiamo dire che un problema è *davvero* difficile? O, meglio, che cosa caratterizza la difficoltà di un problema?

E, prima ancora, che cos'è un problema?!

1.1. Il signor problema e le sue istanze

Già, in definitiva, che cos'è un problema? Generalmente, siamo abituati a pensare che “*calcola l'area di un rettangolo la cui base e la cui altezza misurano, rispettivamente, 5 e 4*” sia un problema. Ebbene, in realtà la frase virgolettata e in corsivo è l'*istanza* di un problema.

Il problema corrispondente all'istanza appena enunciata è, propriamente, “*calcola l'area di un rettangolo date le dimensioni della sua base e della sua altezza*”. Ossia, il problema, di per sé, dichiara un certo insieme di entità – un rettangolo e le lunghezze di due segmenti – e le relazioni che intercorrono fra di esse – i due segmenti sono la base e l'altezza di quel rettangolo – specificando cosa di queste entità è conosciuto – le lunghezze dei due segmenti – e cosa, invece, deve essere calcolato – l'area del rettangolo.

L'esempio dell'area del rettangolo ci permette di indurre la definizione generale di problema che, tanto per andar sul sicuro, recuperiamo da un dizionario: “In matematica e in altre scienze, domanda con cui si chiede di trovare, sulla base di dati noti ed enunciati, dati non noti, o impliciti, che sono logicamente deducibili dai primi”. Ossia, un problema consiste in un elenco di dati espliciti (quelli che abbiamo bisogno di conoscere per risolvere il problema – due numeri positivi, nell'esempio) completato dalle relazioni che sussistono fra loro (il fatto che i due numeri sono le dimensioni della base

e dell'altezza di un rettangolo), e da una richiesta (la domanda del problema – l'area del rettangolo). Ogni qualvolta scegliamo i valori per tutti i dati espliciti otteniamo un'istanza di quel problema – cui corrisponde un insieme di valori per i dati impliciti che costituisce la soluzione per quella istanza.

È d'uopo fare qualche esempio. Sono problemi le seguenti richieste: “calcolare la radice quadrata di un (*generico*) intero n ”, oppure “calcolare quanto tempo impiega un corpo che si muove con accelerazione a e velocità iniziale v_0 a percorrere un spazio s ”, o anche, infine, “data una carta stradale e due città presenti sulla carta, calcolare il percorso più breve dall'una all'altra città”. A questi problemi corrispondono, sempre a titolo di esempio, rispettivamente le istanze seguenti: “calcolare la radice quadrata di 625”, “calcolare quanto tempo impiega un corpo che si muove con velocità iniziale 10m/s e accelerazione costante 3m/s^2 a percorrere 250 metri”, “data la carta stradale d'Italia, calcolare il percorso stradale più breve da Venezia a Siena”.

Questa distinzione fra problema e istanze di un problema gioca un ruolo importante... praticamente in tutto il resto di questo libro! Intanto, quando parliamo di soluzione per un'istanza di un problema ci riferiamo a un dato (o, più in generale, a un insieme di dati): così, la soluzione di “calcolare la radice quadrata di 625” è (il numero) 25, la soluzione di “calcolare quanto tempo impiega un corpo che si muove con velocità iniziale 10m/s e accelerazione costante 3m/s^2 a percorrere 250 metri” è 10 secondi, e la soluzione di “data la carta stradale d'Italia, calcolare il percorso stradale più breve da Venezia a Siena”... beh, è un tracciato segnato sulla carta stradale.

Quando, invece, parliamo di “risolvere un problema” ciò che intendiamo è che siamo interessati a individuare un *procedimento* che permetta di trovare la soluzione di *qualsiasi* istanza. Così, per farla facile, risolvere il problema “calcola l'area di un rettangolo date le dimensioni della sua base e della sua altezza” significa indicare il procedimento “moltiplica la dimensione della base con la dimensione dell'altezza”. In altri termini, sappiamo risolvere un problema quando sappiamo indicare una sequenza di passi che, a partire da certi dati specifici, ci permetta di ricavare il risultato – un po' come quando alle elementari ci hanno spiegato come aggiungere due