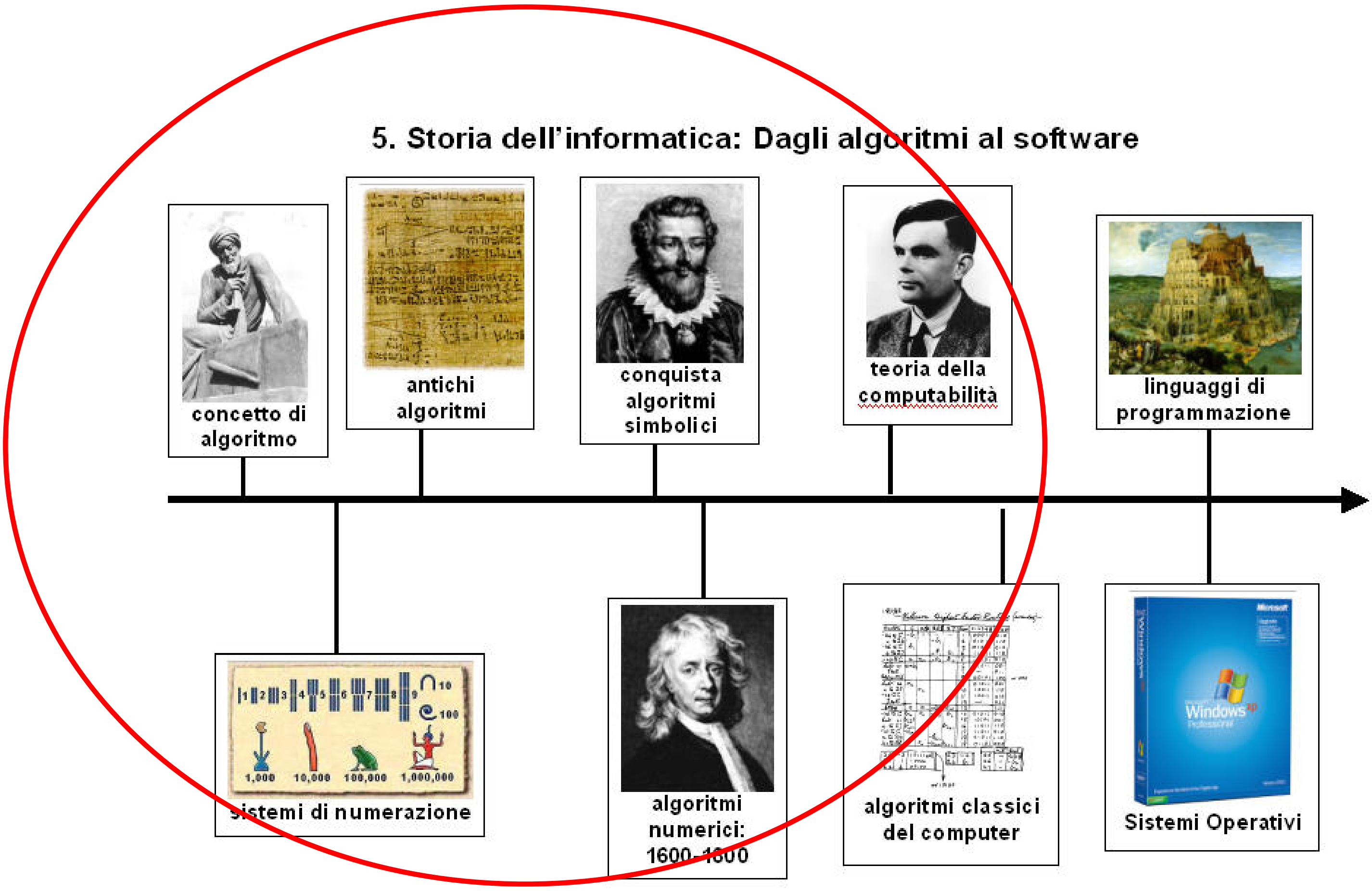
Dagli antichi algoritmi alle macchine di Turing

Paolo Giangrandi
paolo.giangrandi@dimi.uniud.it

Università degli Studi di Udine

13/05/2008

Sommario


5. Storia dell'informatica: Dagli algoritmi al software
concetto di algoritmo
antichi algoritmi
conquista algoritmi simbolici
teoria della computabilità
linguaggi di programmazione
sistemi di numerazione
algoritmi numerici: 1600-1800
algoritmi classici del computer
Sistemi Operativi

1. Introduzione agli algoritmi

La storia dell’informatica non riguarda solo lo sviluppo degli strumenti di calcolo e del moderno computer, ma include anche lo studio dei **procedimenti di calcolo** per risolvere problemi (sia quelli eseguiti dall’uomo che quelli eseguiti automaticamente dagli strumenti di calcolo).

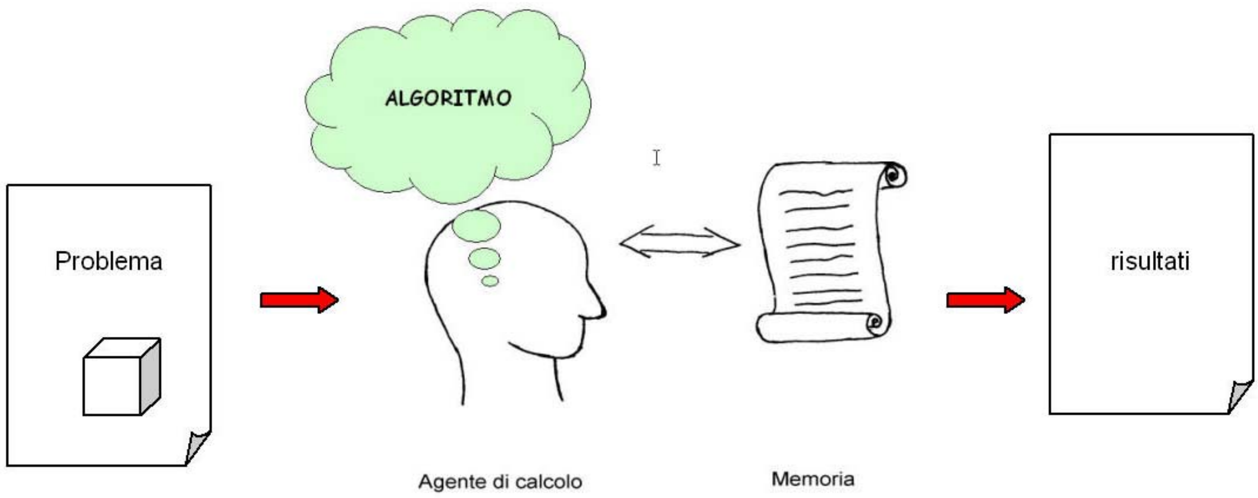
In informatica, i procedimenti di calcolo vengono comunemente denominati **algoritmi**.

> *Un **algoritmo** è una procedura di calcolo descritta in modo sufficientemente preciso atta a risolvere un determinato problema.*

Nel corso dei secoli la concezione e il modo di descrivere gli algoritmi è cambiato in modo significativo e oggi è possibile scrivere algoritmi che possono essere eseguiti automaticamente su una macchina.

Dal problema all'algoritmo

Nella risoluzione di un problema troviamo diversi elementi caratteristici come è illustrato nella seguente figura:



- Il ***problema***, come sappiamo, è costituito da una richiesta di informazione che deve essere soddisfatta a partire da un insieme di dati/informazioni note.
- L'***algoritmo*** è un procedimento risolutivo costituito da un insieme finito di istruzioni che, eseguite in ordine e in modo preciso, permettono di determinare i risultati del problema a partire dalle informazioni disponibili. Ogni istruzione deve essere elementare, non ambigua e descritta in modo sufficientemente preciso e completo per poter essere eseguita "meccanicamente".
- L'***agente di calcolo*** rappresenta colui che esegue materialmente le operazioni specificate nell'algoritmo al fine di risolvere il problema; può es-

sere rappresentato da una persona, oppure da un sistema automatico.

- La ***memoria*** rappresenta il supporto dove vengono conservate le informazioni non solo iniziali ma anche quelle che vengono prodotte man mano che si esegue l'algoritmo.
- I ***risultati***, infine, rappresentano le informazioni desiderate e possono essere formate semplicemente da un singolo dato o da una risposta si/no, oppure possono essere costituite da un insieme strutturato e ampio di informazioni come ad esempio la dimostrazione di un teorema.

Un algoritmo è una sequenza finita di istruzioni per manipolare simboli secondo regole sintattiche precise.

Ogni regola di manipolazione deve essere "meccanica", deve prescindere dal significato dei simboli e deve essere deterministica, cioè non deve essere legata ad aspetti probabilitistici o di altra natura. Le regole di manipolazioni che possiamo utilizzare per manipolare i simboli iniziali devono appartenere ad un insieme prestabilito, discreto e finito di operazioni.

Ogni algoritmo è legato ad un particolare modello di calcolo a secondo del tipo di oggetti manipolati e a seconda delle operazioni ad essi applicate: possiamo operare con numeri, con stringhe composte da lettere, con equazioni, con figure, ecc.

L'insieme iniziale dei simboli manipolati deve essere finito e deve appartenere ad un alfabeto discreto e finito.

Nel corso dei secoli sono stati introdotti diversi modelli computazionali a partire dai quali sono stati realizzati un gran numero di algoritmi. Questi modelli di calcolo sono stati essi stessi oggetto di studio e i matematici hanno saputo metterne in rilievo caratteristiche e limiti.

Oggi gli studi teorici di informatica hanno permesso di capire che non tutti i modelli di calcolo a cui storicamente si è fatto ricorso sono equivalenti e hanno i requisiti per essere considerati dei buoni modelli di calcolo.

Per molti secoli il **termine algoritmo ha assunto le connotazioni di procedimento risolutivo per un problema a prescindere dal fatto che esso sia "effettivo"**, cioè solo se opera su una rappresentazione finita con regole meccaniche secondo le caratteristiche appena elencate.

Vedremo quindi algoritmi effettivi come il metodo di moltiplicazione indiana per i numeri naturali rappresentati in forma posizionale e il crivello di Eratostene, ma anche procedimenti che non rientrano nella moderna definizione di algoritmo come le procedure con riga e compasso dei Greci, o i procedimenti di risoluzione di equazioni di 2° grado applicati dai babilonesi che richiedono l'estrazione di radice quadrata, operazione che non sempre può essere svolta in forma esatta.

Il fatto che dal punto di vista algoritmico questi procedimenti non siano effettivi non implica che non siano esatti: si tratta comunque di oggetti matematici ben definiti su cui possiamo "ragionare" non algoritmicamente ma per altra via.

Nella storia della matematica (e dell'informatica) non si osserva fino agli anni '30 alcuna particolare distinzione tra procedimenti effettivi e non effettivi perché solo nel secolo scorso il concetto moderno di algoritmo viene messo a fuoco in modo rigoroso.

D'altra non è possibile comprendere la storia degli algoritmi senza esaminare anche quelle procedure che per secoli hanno affiancato ciò che noi oggi riguardiamo come algoritmi.

1.1. Il concetto di algoritmo

Un “buon” algoritmo deve soddisfare deve caratteristiche:

Caratteristiche generali degli algoritmi
1. un algoritmo deve essere composto da un insieme finito di istruzioni; **2. ci deve essere un agente di calcolo capace di eseguire le istruzioni dell’algoritmo;** **3. non ci deve essere ambiguità sul significato di ogni operazione elementare specificata nell'algoritmo;** **4. le istruzioni dell'algoritmo vengono eseguite con passi deterministici senza ricorrere a metodi casuali;** **5. le operazioni descritte nell'algoritmo devono essere eseguite per passi discreti senza l'uso di metodi 'continui' o di dispositivi analogici;** **6. l'agente di calcolo può utilizzare una memoria in cui tenere i risultati intermedi per poi utilizzarli nelle fasi successive;** **7. i dati elaborati nell’algoritmo devono essere rappresentabili con un alfabeto finito di simboli e devono essere di lunghezza finita;** **8. l'insieme delle istruzioni di base che l’agente di calcolo è in grado di svolgere è finito;** **9. non c'è alcun limite al numero di istruzioni che possono essere svolte durante l'esecuzione di un algoritmo; qualora l'esecuzione dell'algoritmo non abbia termine, non sarà possibile conoscere i risultati finali prodotti nell'esecuzione dell'algoritmo;** 10. **non c'è alcun limite alla quantità di memoria che può essere utilizzata durante l'esecuzione dell'algoritmo.**

1.2. L’origine del termine “algoritmo”

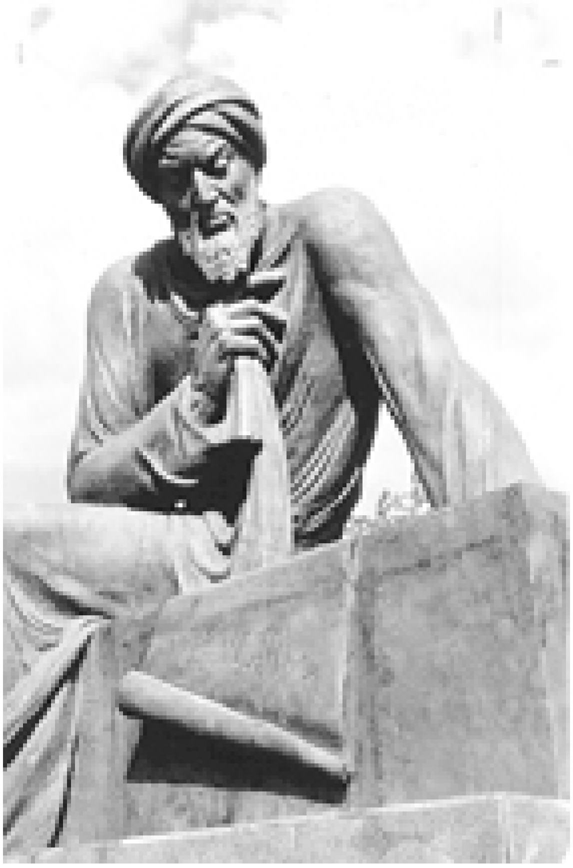


Fig. Statua di al-Khwarizmi.	**Fig. Page from al-Khwarizmi's Kitab al-Jabr wal-Muqabala, the oldest Arabic work on algebra.**

La parola "algoritmo" ha origine in Medio Oriente e proviene dal nome latinizzato del matematico persiano al-Khwarizmi.

Al-Khwarizmi scrisse diversi trattati e tra questi il trattato più famoso è “*al-Kitāb al-Mukhtasar fi Hisab al-Jabr wa l-Muqabala*” (Compendio del calcolo per mezzo della restaurazione e del confronto), contenente le **prime regole elementari del calcolo algebrico** per risolvere equazioni.

La sua opera “Kitab al-Jam'a wal-Tafreeq bil Hisab al-Hindi”, in cui veniva descritto il sistema posizionale decimale inventato dagli indiani, venne tradotta in latino attorno al 1120 con il titolo “***Algoritmi de Numero indorum***”. La traduzione latina iniziava così: “*Dixit Algoritmi….*

A poco a poco, la parola latina “**algorismus**” (o “**algorithmus**”) cominciò ad essere usata per indicare i procedimenti di calcolo per **eseguire le quattro operazioni aritmetiche nel sistema decimale** in contrapposizione al sistema di numerazione romano e all’uso dell’abaco e tale uso portò quasi a dimenticare il collegamento tra il termine “algorismus” e il matematico arabo, collegamento che venne riscoperto solo nella metà del XIX secolo, quando le opere del matematico arabo vennero ritrovate dopo un lungo oblio.

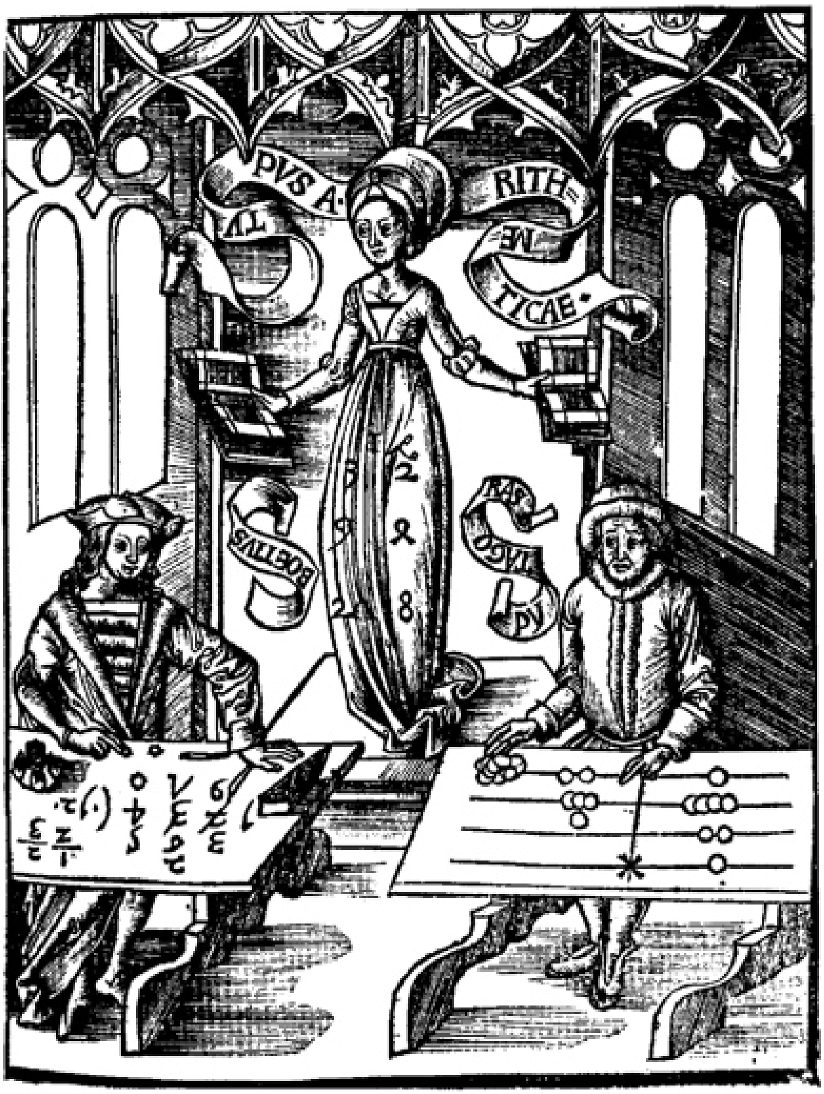


Fig. Un abacista (che utilizza una tavola per contare) in competizione con un algorista (che utilizza il sistema decimale posizionale).

Nei secoli XII e XIII gli “**algoristi**” erano coloro che adottavano i nuovi metodi per eseguire le operazioni aritmetiche esposti nel trattato di al-Khwarizmi.

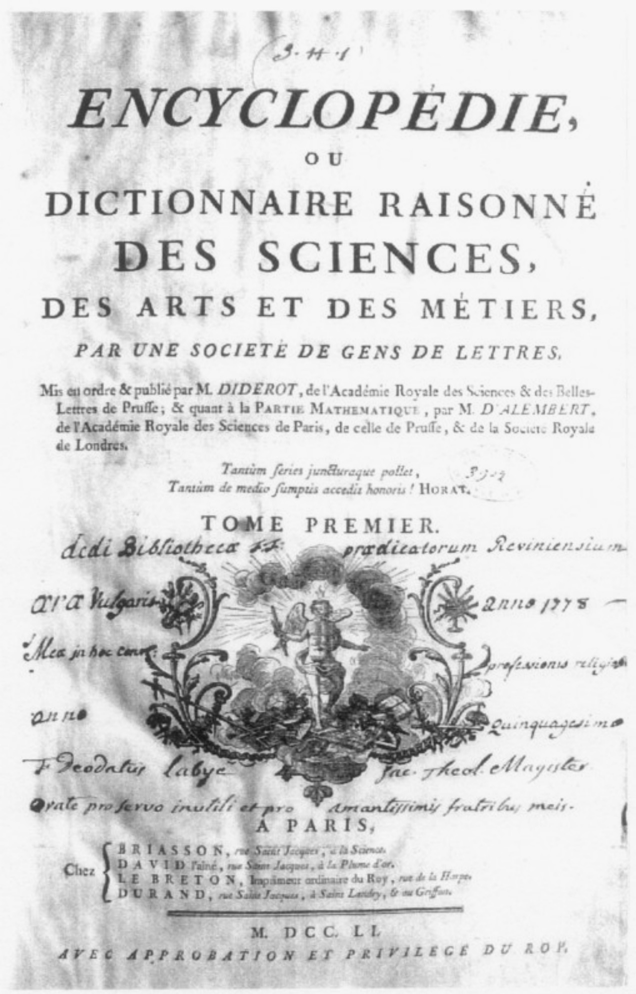
Questi algoristi erano in “competizione” con gli abachisti, che per eseguire le operazioni adottavano ancora l’abaco.

Così **Tartaglia** nel 1500 spiega all'inizio del secondo libro del General Trattato il significato del termine:

> *La Pratica Aritmetica, come afferma Giovan de Sacrobusto, fu data compendiosa in luce da un Philosopho detto Algo, e per questa causa fu detta Algoritmo, over Algorithmo. Le specie del qual Algoritmo, over Algoritmo, secondo Giovan de Sacrobusto, Perdocimo de Beldemandis, e Michel Scotto sono nove.*

Il "**Philosopho Algo**" rappresenta ovviamente al-Khwarizmi.

Successivamente, il termine algoritmo finì per indicare non solo i metodi per eseguire le quattro operazioni aritmetiche, ma un qualunque procedimento di calcolo atto a risolvere un problema di calcolo.



ENCYCLOPÉDIE,
OU
DICTIONNAIRE RAISONNÉ
DES SCIENCES,
DES ARTS ET DES MÉTIERS,
PAR UNE SOCIETÉ DE GENS DE LETTRES.

Mis en ordre & publié par M. DIDEROT, de l'Académie Royale des Sciences & des Belles-Lettres de Pruſſe; & quant à la PARTIE MATHÉMATIQUE, par M. D'ALEMBERT, de l'Académie Royale des Sciences de Paris, de celle de Pruſſe, & de la Société Royale de Londres.

Tantùm series juncturaque pollet,
Tantùm de medio ſumptis accedit honoris! HORAT.

TOME PREMIER.

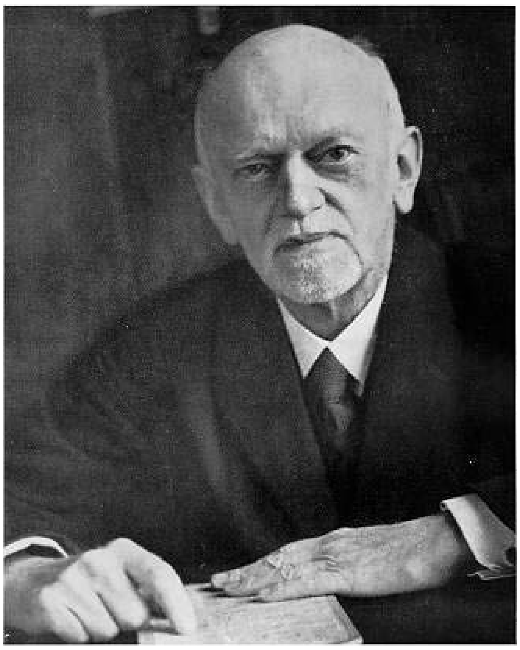
A PARIS,

Chez BRIASSON, rue Saint Jacques, à la Science.
DAVID l'aîné, rue Saint Jacques, à la Plume d'or.
LE BRETON, Imprimeur ordinaire du Roy, rue de la Harpe.
DURAND, rue Saint Jacques, à Saint Landry, & au Griffon.

M. DCC. LI.
AVEC APPROBATION ET PRIVILEGE DU ROY.

Fig. Frontespizio dell'Enciclopedie di Diderot e D'Alembert (1751-1772).

D'Alembert definisce in questo modo il termine algoritmo: "**Termine arabo, usato da molti autori, e particolarmente dagli spagnoli per indicare la pratica dell'algebra. Può anche indicare l'aritmetica delle cifre… La stessa parola può in generale significare il metodo e la notazione per tutti i tipi di calcolo. In questo senso, parliamo di algoritmo del calcolo integrale, di algoritmo del calcolo esponenziale, di algoritmo dei seni, ecc.**"



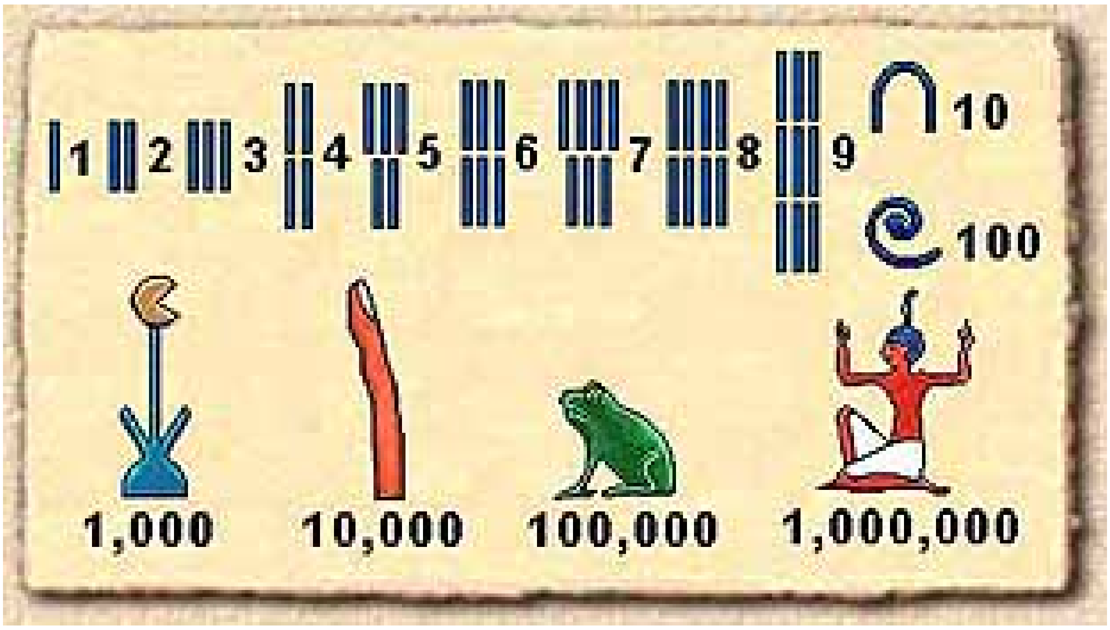
Per molto tempo non si è sentita l'esigenza di dare una definizione più chiara e precisa del concetto di algoritmo.

Nel '900 il termine assumerà un significato più preciso nell'ambito dello studio dei fondamenti stessi della matematica, grazie soprattutto al **programma di ricerca** lanciato dal grande matematico tedesco **David Hilbert**.

I problemi posti da Hilbert porteranno i matematici a precisare meglio gli aspetti caratterizzanti gli algoritmi. Nel 1935-37 appariranno finalmente i lavori di **Alonzo Church** e **Alan Turing**, che gettano le basi della moderna definizione di algoritmo.

2. Sistemi di numerazione

Paolo Giangrandi
paolo.giangrandi@dimi.uniud.it



Università degli Studi di Udine

13/05/2008

2.1. La scrittura dei numeri

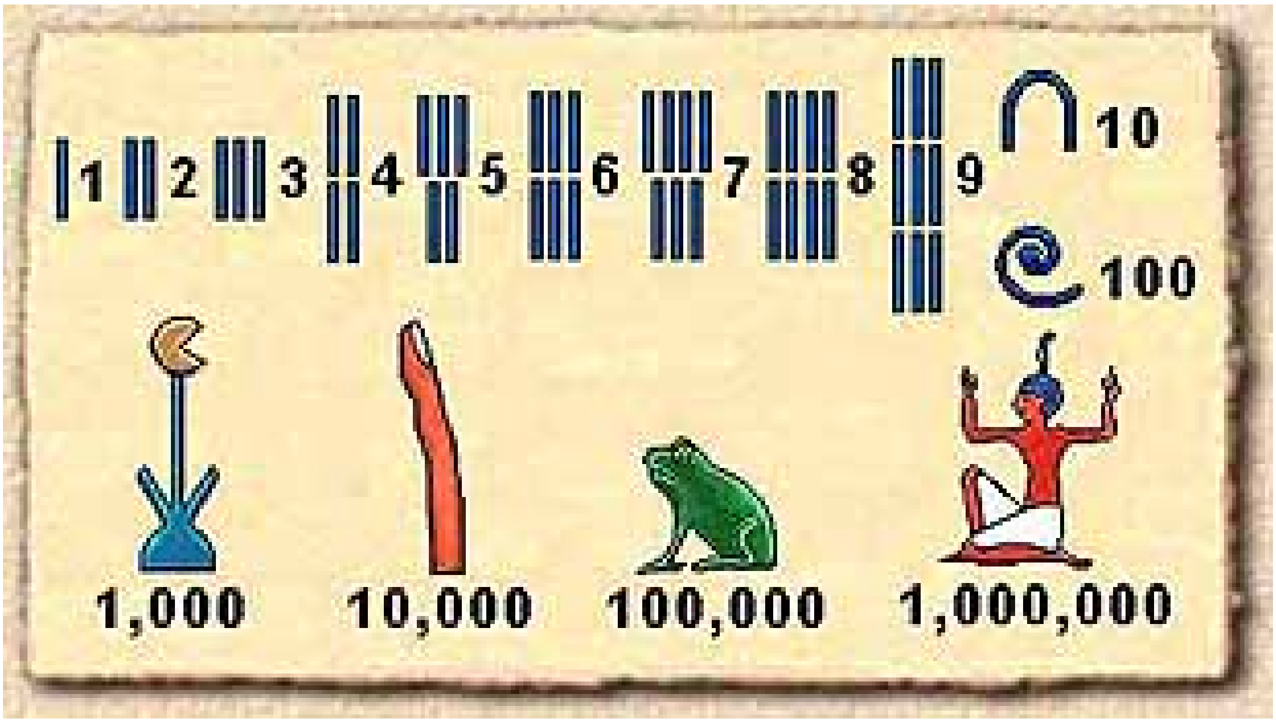


Fig. Sistema di numerazione egizio.

La scrittura dei numeri pone il problema di trovare una rappresentazione efficace che consenta di operare su di essi in modo efficace.

In termini informatici il problema è quello di trovare una struttura dati che consenta di rappresentare efficacemente i numeri facilitandone le operazioni aritmetiche.

Nel corso dei secoli il modo di rappresentare i numeri è cambiato non solo in termini di simboli usati, ma anche come principio di funzionamento.

Due sono gli aspetti più importanti che hanno caratterizzato la scrittura dei numeri:

- il **concetto di base** e
- la presenza o meno del ***sistema posizionale***.

Mentre nelle civiltà più antiche prevalsero sistemi di numerazione additivi, a partire dal IV-V sec. d.C. in India si diffuse quel sistema posizionale che caratterizza la scrittura moderna dei numeri.

Quali sono le caratteristiche di un buon sistema di numerazione?

- compattezza,
- facilità di calcolo,
- facilità di memorizzazione dei simboli,
- possibilità di trattare numeri arbitrariamente grandi,
- generalizzazione a numeri non interi, …

2.2. Sistemi di numerazione non posizionali

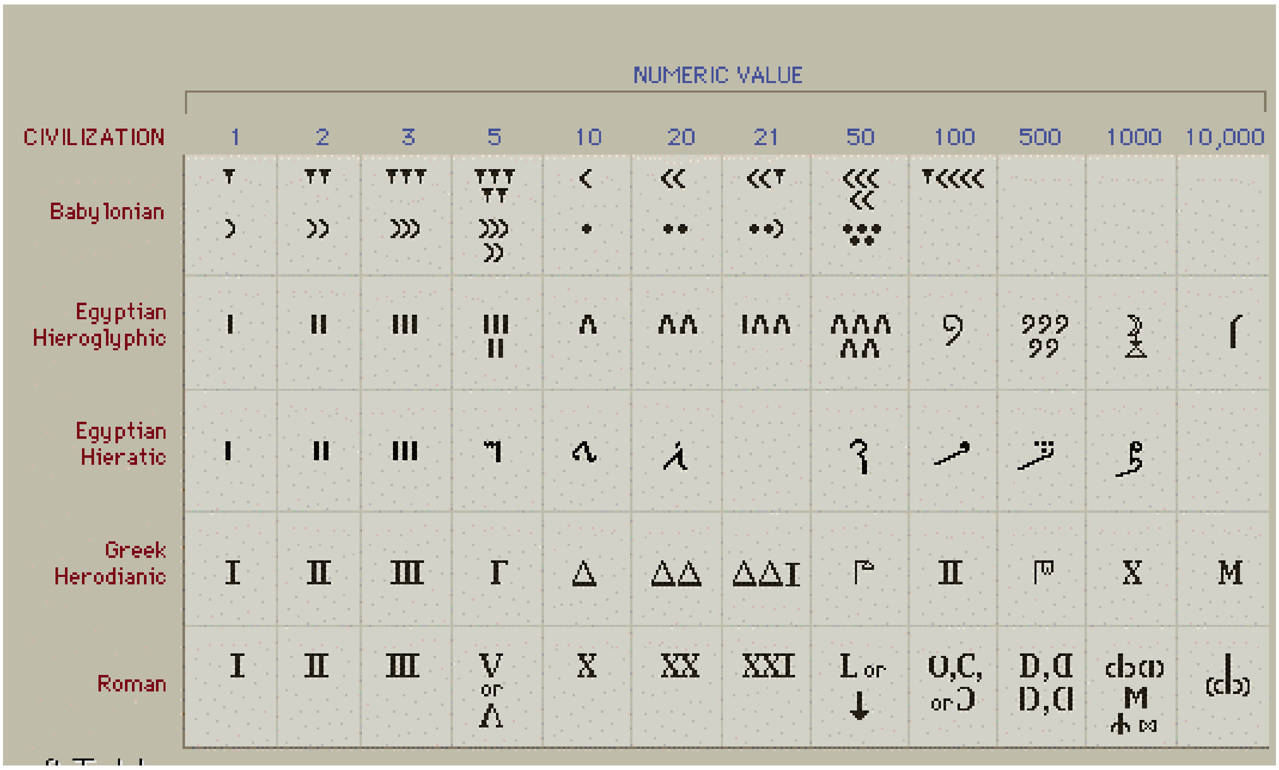


Fig. Alcuni sistemi di numerazione antichi.

Probabilmente il primo sistema di numerazione è stato quello ***unario***: ad ogni unità corrispondeva un segno o un'incisione su qualche tipo di supporto.

La maggior parte delle civiltà antiche ha utilizzato come base il numero 10, legato ovviamente al numero dita delle mani. Questo perché le dita della mano hanno rappresentato sicuramente il primo strumento di calcolo usato dall'uomo.

Non mancano comunque esempi di sistemi di numerazione con base diversa. **Il più noto è il sistema sessagesimale dei babilonesi a base 60**.

A questo proposito, occorre osservare che ancora oggi **conserviamo traccia di questo sistema nella misurazione del tempo** (cioè, per i minuti e per secondi) e nella misurazione degli angoli (frazioni di grado).

I primi sistemi di numerazione furono per lo più *di tipo additivo* fondati sull'uso di una base numerica. In questi sistemi, ad ogni simbolo di un dato tipo è associato un valore numerico prefissato, e il sistema si dice additivo perché il valore complessivo del numero rappresentato si ottiene sommando i valori numerici dei singoli simboli che compongono il numero.

Ad esempio, nella **numerazione romana antica**, il numero

XXXVII

viene interpretato sommando:

10 + 10 + 10 + 5 + 2 = 37.

In un sistema additivo, il valore di un numero non ha niente a che vedere con la posizione dei simboli che si trovano nella sequenza che rappresenta il numero.

In generale, **i sistemi additivi consentono una facile esecuzione delle operazioni di addizione e sottrazione, ma le altre operazioni sono difficili**. In passato, queste operazioni venivano svolte con metodi diversi da quelli che noi oggi utilizziamo.

Il sistema di numerazione egiziano

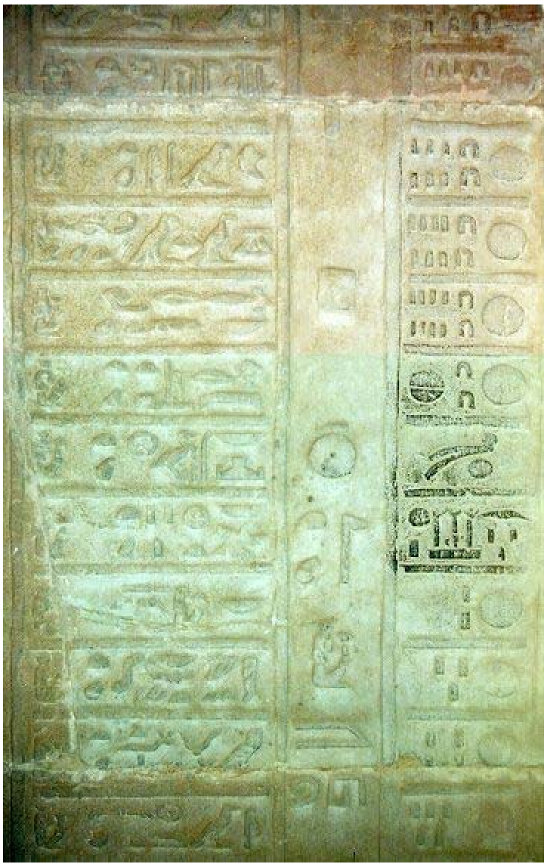


Fig. Egyptian Numerals.

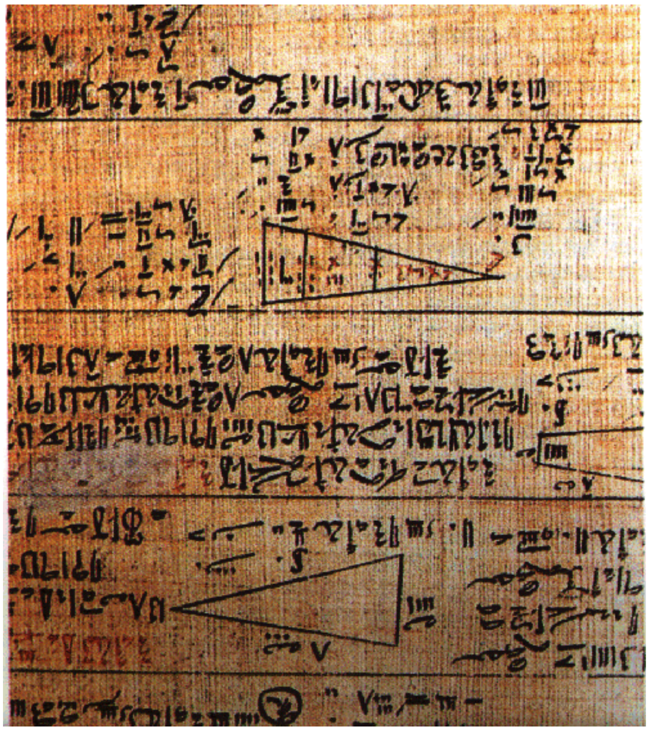


Fig. Frammento del papiro di Ahmes, circa 1600-1900 a.C.

Gli egiziani utilizzavano un sistema di scrittura basato sull'uso dei geroglifici che risale ad oltre 3000 anni prima di Cristo. Il sistema di numerazione egiziano impiegava dieci simboli base:

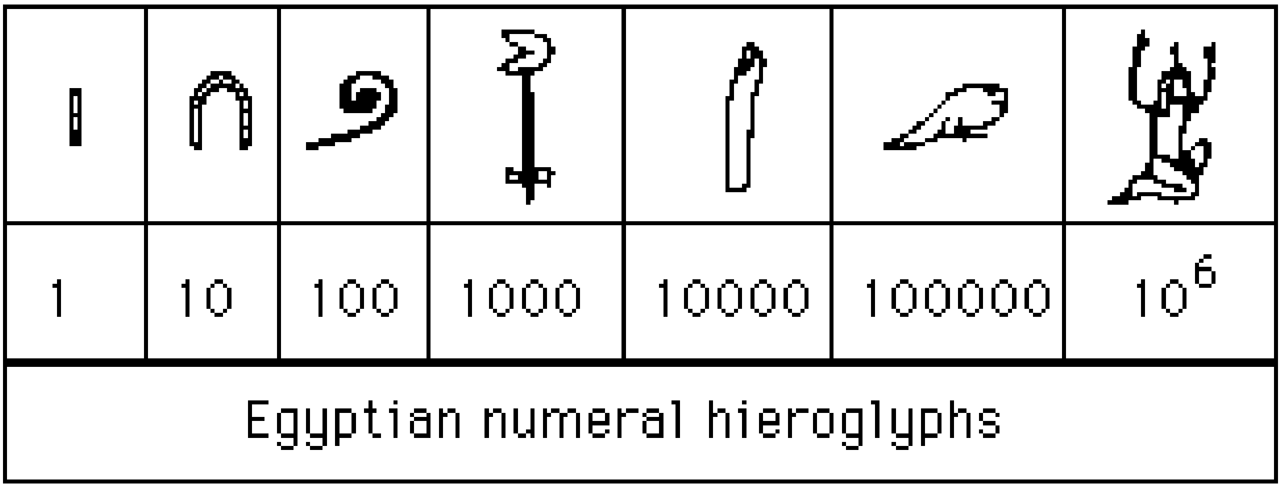


Fig. Here are the numeral hieroglyphs.

Il sistema era di tipo additivo. I numeri venivano scritti semplicemente giustapponendo i simboli e il numero rappresentato era dato dalla somma dei numeri corrispondenti a ciascun simbolo:

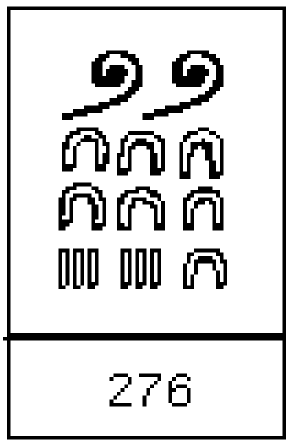
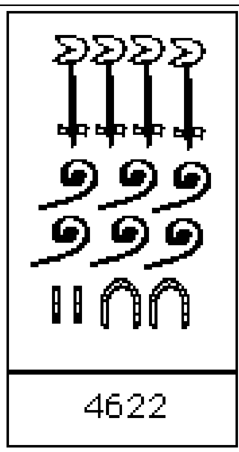
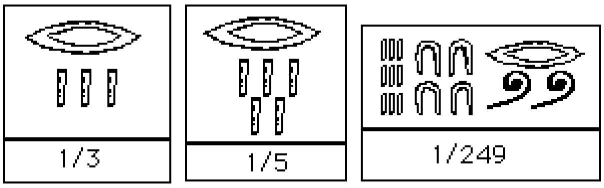
	

Fig. 276 in hieroglyphs.	**Fig. 4622 in hieroglyphs.**

Le frazioni venivano scritte come somma di frazioni unitarie, cioè con il numeratore uguale a uno (tranne per le frazioni $^{2}/_{3}$ e $^{3}/_{4}$). Alcuni esempi sono illustrati qui di seguito:



Nel corso dei millenni, il sistema di numerazione egiziano è cambiato. Ad esempio, la **scrittura ieratica** permetteva di scrivere i numeri in una forma più compatta:

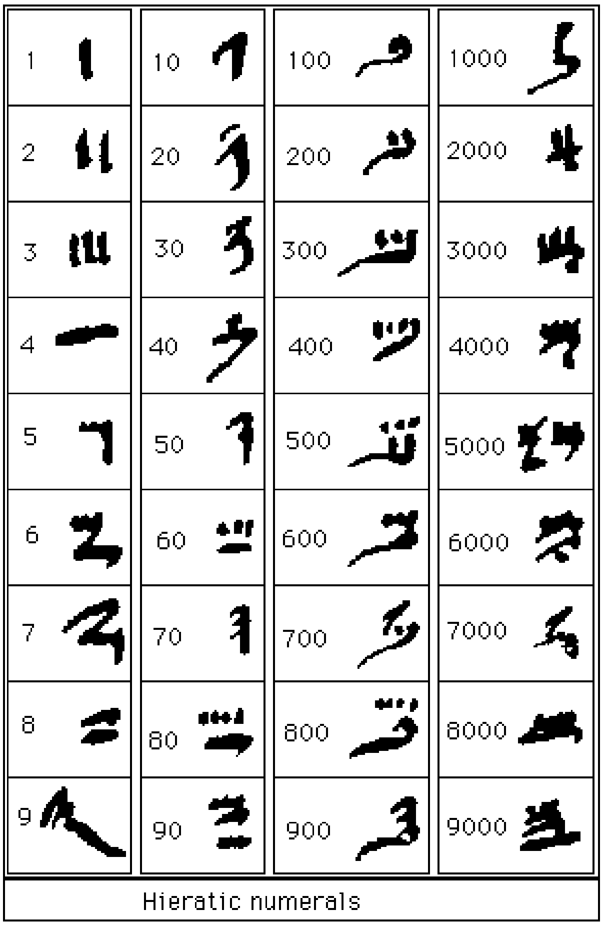


Fig. Here are versions of the hieratic numerals

La moltiplicazione degli antichi egizi

Nell'antico Egitto le **operazioni di moltiplicazione e divisione** venivano svolte secondo una tecnica diversa da quella attuale. **Entrambe le operazioni si basavano sull'operazione di duplicazione (cioè di raddoppiamento)**.

Si supponga di dover moltiplicare 41 per 59 utilizzando la tecnica dei raddoppiamenti. Si costruisce preliminarmente una tabella con i prodotti di 59 per le potenze successive di 2. Si procede fino alla potenza di 2 immediatamente più piccola di 41 (ossia, fino a 32).

41	**59**	
1	**59**	✓
2	**118**	
4	**236**	
8	**472**	✓
16	**944**	
32	**1888**	✓

A questo punto, è necessario scomporre 41 nella somma di potenze di 2 elencate nella prima colonna:

41 = 32 + 8 +1.

Sfruttando la proprietà distributiva possiamo scrivere:

$$\begin{aligned} \mathbf{41 \cdot 59} &\mathbf{= (1 + 8 + 32) \cdot 59 =} \\ &\mathbf{= 1 \cdot 59 + 8 \cdot 59 + 32 \cdot 59 =} \\ &\mathbf{= 59 + 472 + 1888 =} \\ &\mathbf{= 2419} \end{aligned}$$

Il sistema di numerazione babilonese

Il sistema di **numerazione babilonese aveva base 60 ed era un sistema posizionale**. Di fatto, tutti i numeri venivano rappresentati utilizzando in forma additiva due soli simboli, uno per le unità e uno per le decine.

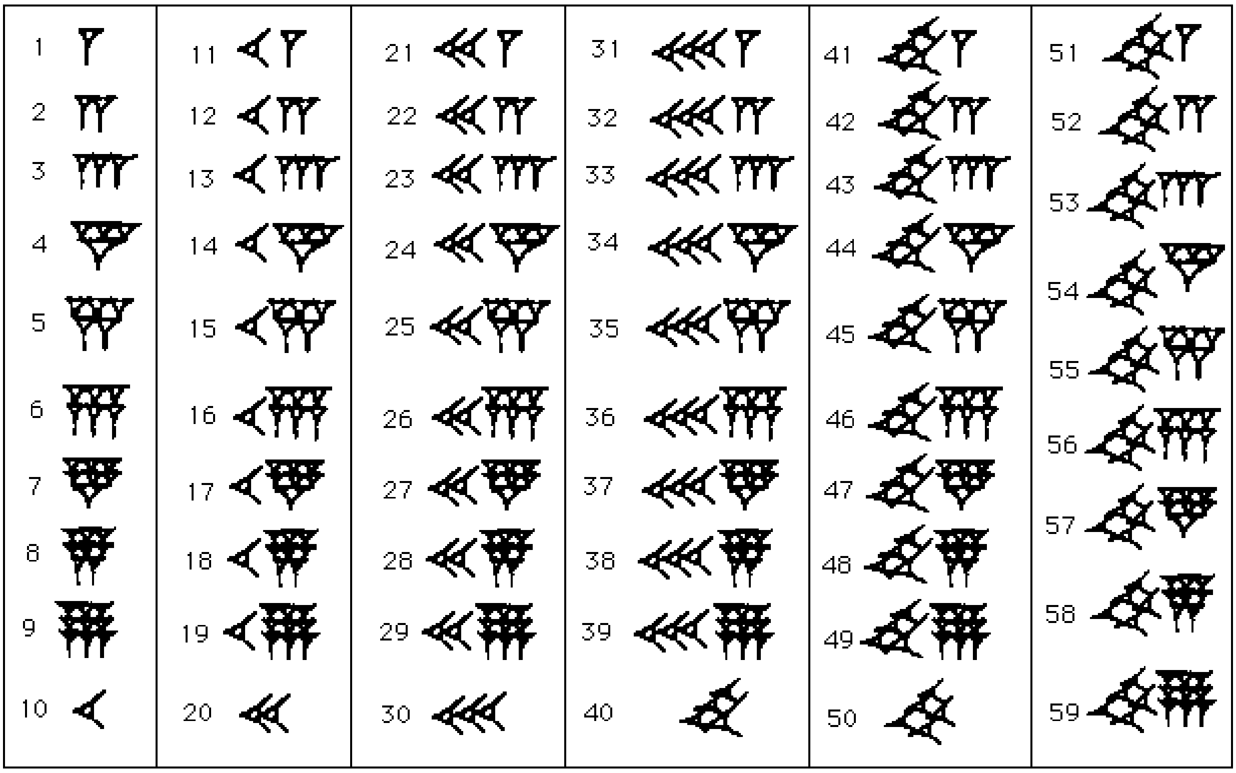


Fig. Here are the 59 symbols built from these two symbols

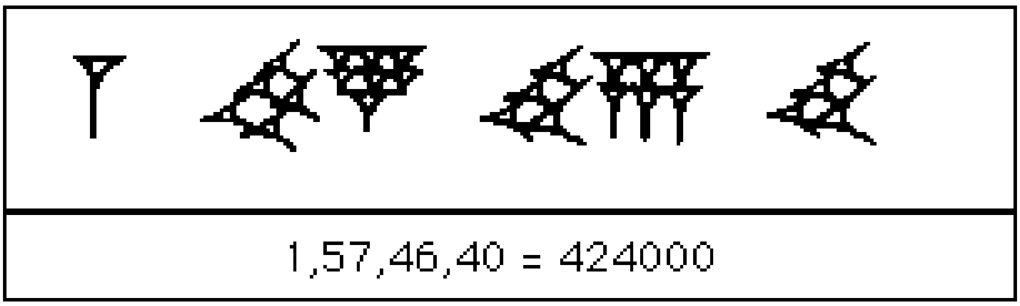


Fig. Here is 1,57,46,40 in Babylonian numerals

Se I babilonesi avessero introdotto anche lo zero, avrebbero anticipato il moderno sistema di numerazione posizionale.

2.3. L’india e il sistema di numerazione posizionale

Le **civiltà babilonese e cinese** furono capaci di anticipare l’idea del sistema posizionale, ma **non riuscirono a comprendere il ruolo e l’importanza dello zero**, per cui non riuscirono di fatto a sviluppare un sistema veramente efficace e funzionale.

La civiltà a cui va il merito di aver elaborato un sistema posizionale veramente completo è quella indiana attorno al V o VI d.C.

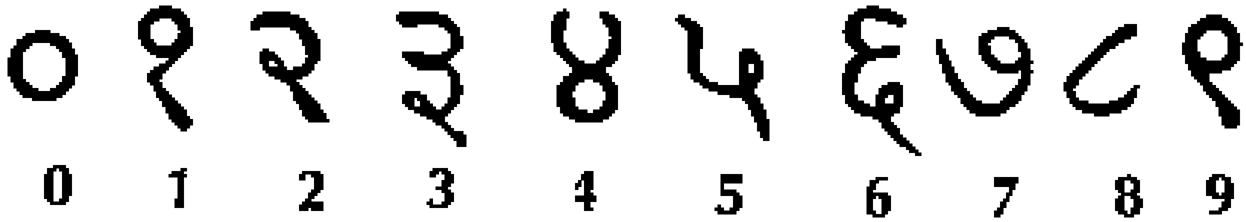
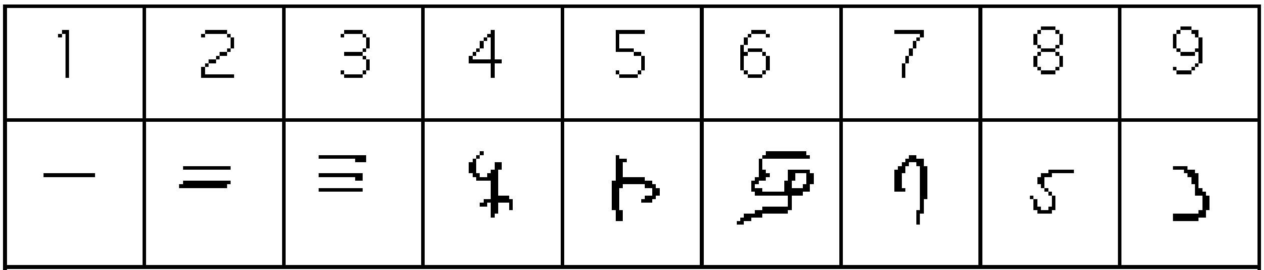


Fig. Sanskrit numerals.

Fu probabilmente l'abaco a suggerire agli indiani il sistema posizionale e probabilmente anche l’uso dello zero. Volendo trascrivere il contenuto di ciascuna riga dell’abaco, come indicare le righe vuote? Per indicare tali righe, gli indiani pensarono di usare un puntino; a poco a poco questo puntino divenne un piccolo ovale così come noi oggi usiamo lo zero.



Gupta numerals around 4th century A.D.

Cosa importante da sottolineare è che **per la prima volta lo zero**, che in qualche era già comparso qua e là in civiltà precedenti, **venne considerato un vero e proprio numero** e non soltanto un segno di mancanza di cifre nella scrittura dei numeri: se è vero che i diversi ingredienti del sistema posizionale erano già stati usati in precedenza presso varie civiltà, furono gli indiani a combinare il tutto facendone un sistema veramente funzionale!

Il sistema indiano grazie all’uso dello zero (per il quale introdussero la parola sunya, che significa ‘posto vuoto’) e di altre nove cifre divenne il sistema di gran lunga più semplice ed efficace di quelli elaborati da altre civiltà.

Il sistema di numerazione indiano è un sistema di tipo posizionale in quanto il valore numerico associato ad ogni cifra varia secondo la posizione che essa occupa nella scrittura del numero. Gli indiani furono inoltre capaci di sfruttare i vantaggi del sistema posizionale nell'esecuzione delle operazioni, cosa che invece non era stata compresa dai Babilonesi e dai Cinesi.

Nel corso dei secoli la forma delle cifre è cambiata più volte. I primi simboli usati per le cifre sono quelli di tipo bramini risalenti al IV d.C., ritrovati su monete di Poona, Bombay, e Uttar Pradesh. L'origine di questi simboli non è nota.

Il più antico documento datato in cui compare il sistema posizionale indiano è un documento di tipo legale che contiene la data del 594 d.C., ma alcuni studiosi ritengono che questa data sia stata aggiunta successivamente.

1	2	3	4	5	6	7	8	9	0
१	२	३	४	५	६	७	८	९	०

Nagari numerals around 11th century A.D.

L’antico **manoscritto di Bakhshali** contiene numeri con il sistema posizionale, ma non è chiara la data di realizzazione di questo manoscritto.

Per quanto riguarda l’uso dello zero il primo documento datato che testimonia direttamente l’uso dello zero risale al 876 d.C., sebbene già da almeno due secoli fosse usato dagli indiani.

 LINK

http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Indian_numerals.html

http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Zero.html

I numeri: dall'India all'Europa attraverso gli Arabi

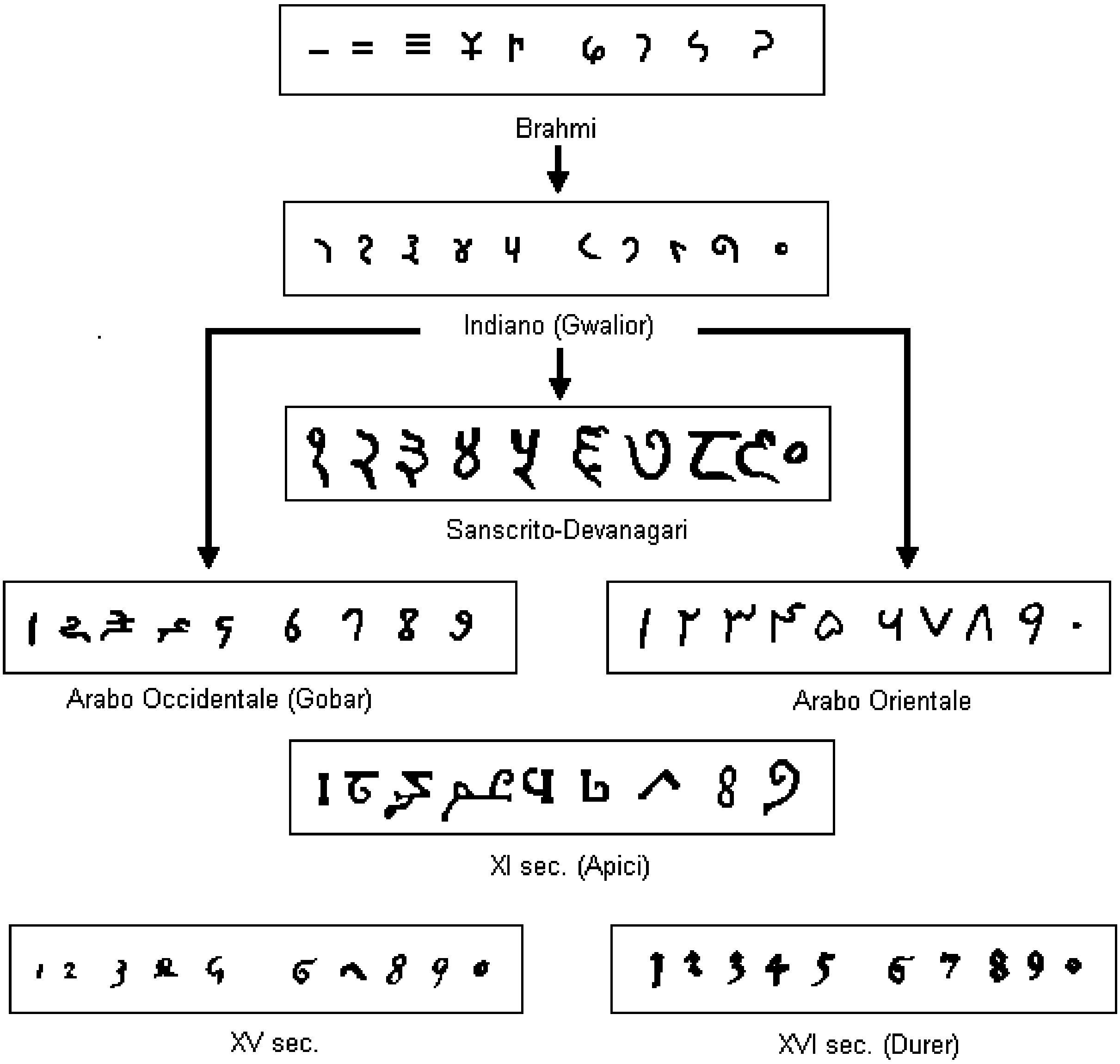


Fig. Evoluzione delle cifre arabe, secondo Karl Menninger.

I contatti tra il mondo arabo e quello indiano portarono ben presto la diffusione del sistema di numerazione indiano nella cultura araba. Abbiamo un documento arabo del 662 d.C. che cita i sistema indiano.

Tra i personaggi arabi che si ritiene abbiano contribuito a diffondere il sistema posizionale c'è lo stesso **Al-Khwarizmi** (circa 780-850), che abbiamo incontrato parlando proprio dell'origine del termine "algoritmo".

Attorno all'820 egli scrisse un testo dedicato al sistema di numerazione posizionale. Il testo evidenzia il ruolo importante dello zero, caratterizzante i sistemi di numerazione posizionale. Oltre alle dieci cifre, un po' diverse per forma da quelle odierne, sono presenti i metodi per eseguire le operazioni aritmetiche, compreso il calcolo della radice quadrata.

Gli arabi rielaborarono i metodi indiani per eseguire le operazioni introducendo varianti comunque concettualmente equivalenti a quelli indiani. In particolare **il matematico al-Uqlidisi (circa 920 – 980) contribuì a trasformare le tecniche di calcolo indiane ideate per lavagne a sabbia nei metodi adatti a carta e penna**. Infatti, fino ad allora in India e nel mondo arabo era pratica fare i calcoli aritmetici scrivendo sulla sabbia o sulla polvere, cancellando i passaggi intermedi mentre si procedeva.

Bisogna aspettare ancora circa tre secoli perché il sistema di numerazione indo-arabo giunga anche in Europa, dove era in uso essenzialmente il metodo di numerazione romano.

Il primo documento europeo contenente le cifre arabe risale al 976 d.C., il ***Codex Vigilanus***. Dal momento che Europa medioevale acquisì il sistema di numerazione non direttamente dagli indiani, ma dagli arabi, nella cultura occidentale le cifre numeriche vengono dette anche ***cifre arabe***. Per molto tempo i numeri indiani furono comunque usati a fianco dei numeri romani.

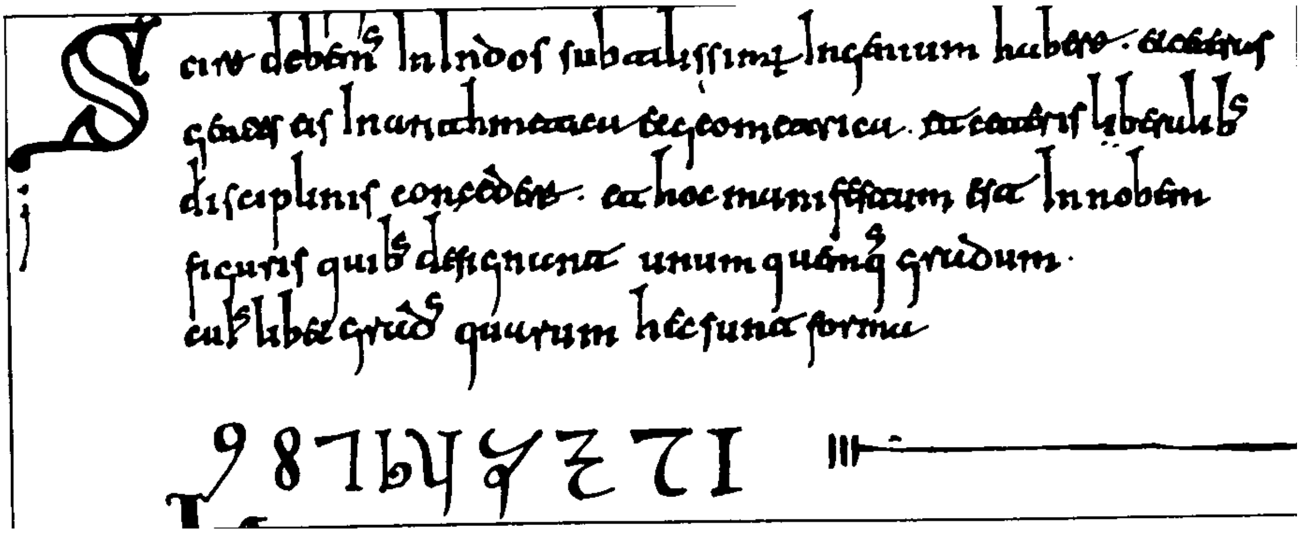


Fig. Codex Vigilanus: la più antica indicazione trovata in Europa delle nostre cifre decimali (976 d.C.).

La diffusione in Europa avvenne prevalentemente per opera di matematici legati ad ambienti culturali diversi: quello delle scuole ecclesiastiche e delle università e quello dei mercanti.

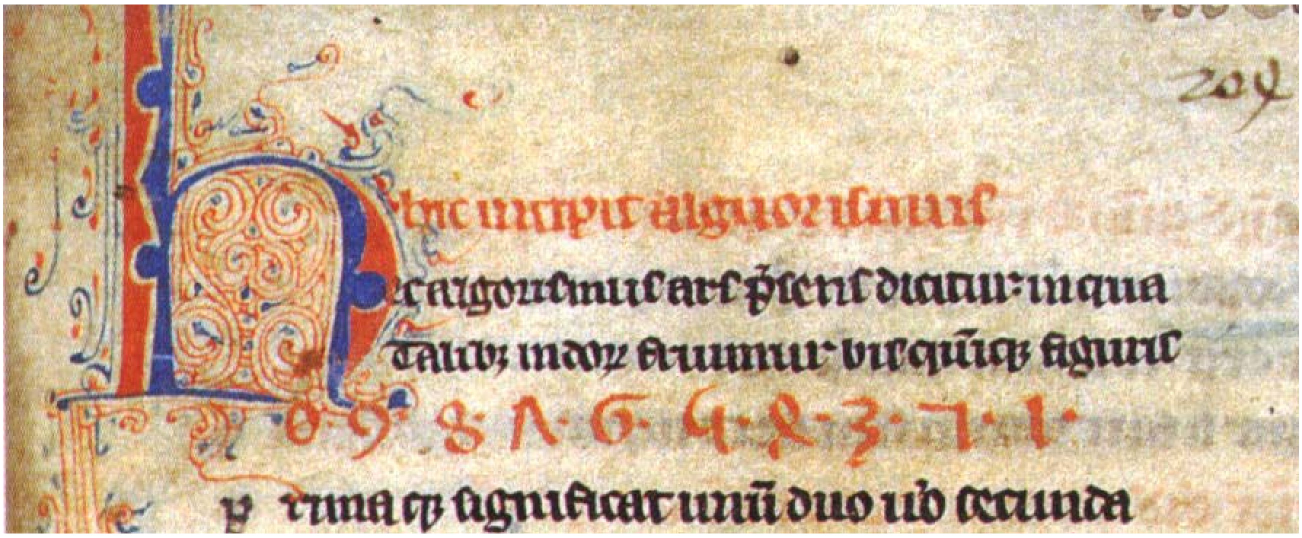


Fig. Incipit del Carmen de Algoritmo, poema latino del XIII sec. di Francois Alexandre de Villedieu.

Tra i personaggi che maggiormente contribuirono ad introdurre il nuovo sistema di numerazione decimale in Europa attorno al XIII sec. d.C. va sicuramente menzionato **Leonardo Pisano (1170-1250), detto Fibonacci con il suo *Liber Abaci* (1202)**.

Fig. Leonardo Pisano, detto Fibonacci.

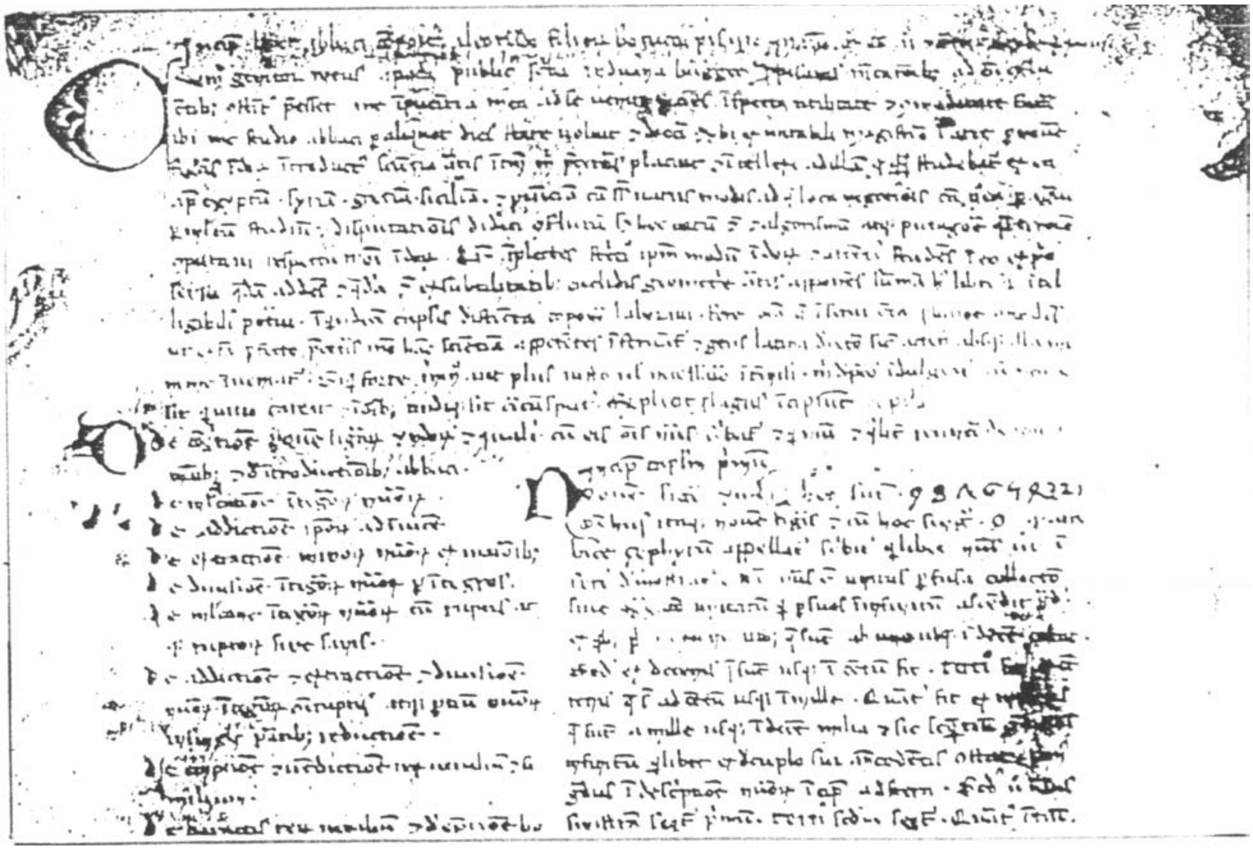


Fig. Pagina iniziale del Liber abaci.

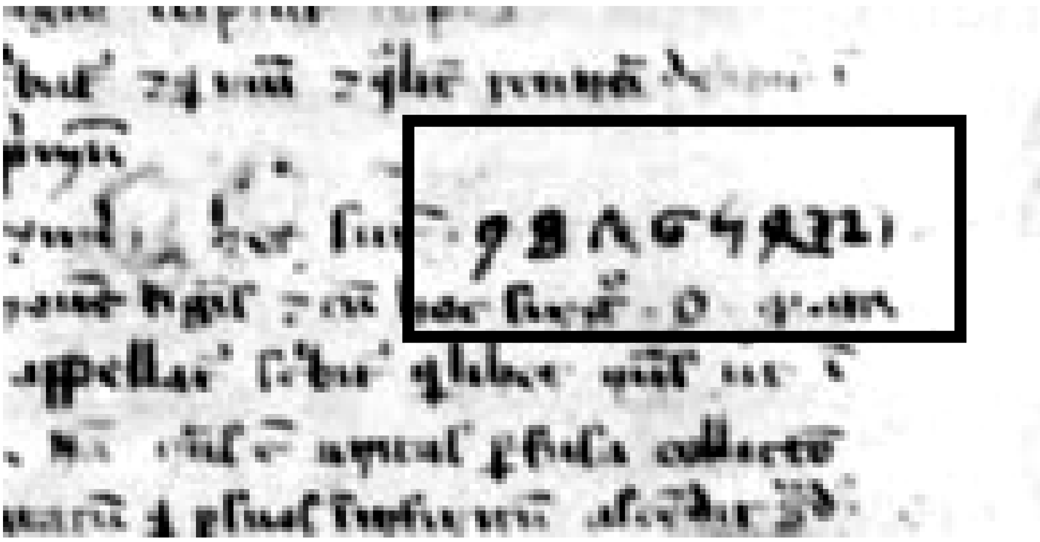


Fig. Dettaglio delle cifre arabe descritte nel Liber abaci.

La numerazione posizionale comportò non solo l'introduzione di un nuovo sistema di scrittura dei numeri, ma determinò parallelamente l'introduzione delle regole di calcolo che noi oggi utilizziamo.

```
  2594 ×
    27 =
------------
 18158
 5188
------------
 70038
```

MMDXCIIII × XXVII = ?

Fig. La moltiplicazione nel sistema decimale e nel sistema romano presentano una notevole differenza come difficoltà.

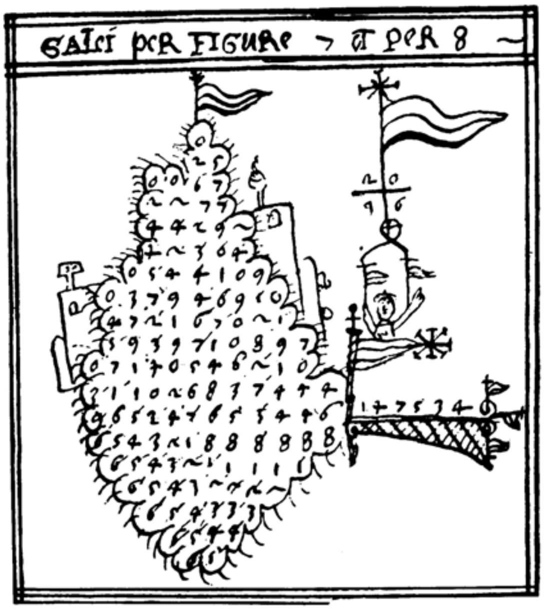


Fig. La divisione secondo il metodo "per galera", derivata da quella con l'abaco (utilizzata fino a secolo XV).

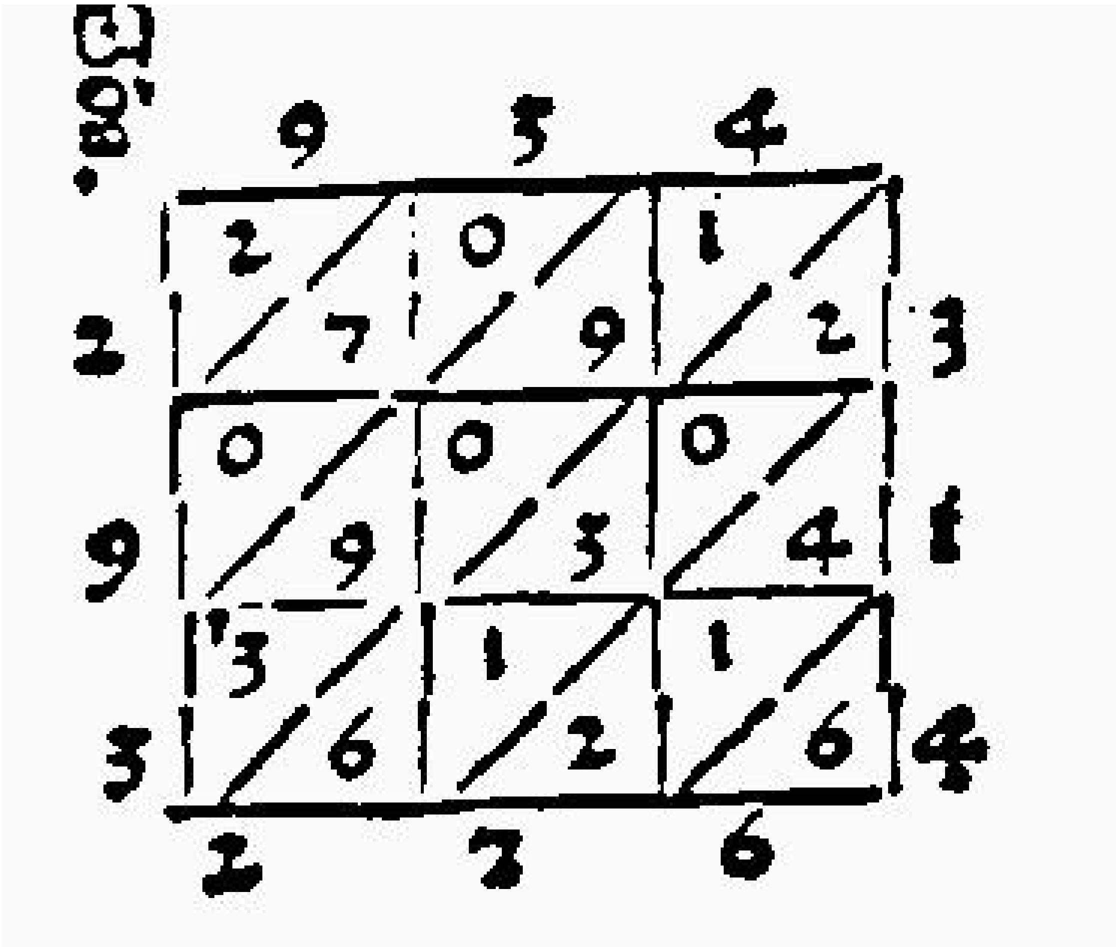
Gli algoritmi della moltiplicazione posizionale in Europa

L'introduzione del sistema decimale si può considerare un'autentica rivoluzione, per certi versi confrontabile all'attuale introduzione del computer. Noi oggi siamo così abituati a questo sistema da non renderci conto della sua immensa importanza nel facilitare le operazioni.

La moltiplicazione nel sistema decimale posizionale è l'operazione per la quale troviamo la maggior varietà di metodi, che anche graficamente assumono aspetti molto diversi tra loro e ai quali gli algoristi assegnarono nomi fantasiosi.

Fibonacci illustra nel *Liber abaci* vari metodi per eseguire le operazioni aritmetiche.

Un algoritmo che riduce al minimo le possibilità di errori perché i possibili riporti si hanno solo in sede di addizioni che seguono una serie di semplici moltiplicazioni a una cifra è quello detto in Italia come *a **gelosia***, oppure *a caselle* o *a reticolo* (già noto comunque agli indiani e agli arabi). Ecco uno schema di moltiplicazione a gelosia, tratto dall'***Aritmetica di Treviso***.



Un metodo di moltiplicazione molto rapido è il metodo per crocetta presentato nel testo *Scala grimaldelli* (libro I) del 1560 di Francesco Feliciano, matematico del XVI sec.[1]

Moltiplicar per Crocetta, o Casella, si puol moltiplicar, e far di quante figure tu vorrai, ma bisogna tenere il capo a bottega per gli incrociamenti che gli vanno, e per questa causa pochi lo adopera da due figure in suso. E fassi in questo modo, pono che habbi a moltiplicare 86 fia 59; acconcia le tue figure come vedi qui da canto, e comincia dalla prima figura da man destra, e di’ 6 fia 9 fa 54 e metti 4 e tieni 5, e poi di’ 8 fia 9 fa 72 e serva, poi di’ 5 fia 6 in croce fa 30, hor summa 5 che tenesti e 72 che servasti con 30, fa 107, e metti 7 e tieni 10, e poi di’ 5 fia 8 fa 40, e 10 che tenesti fa 50, metti 50 in bina con 74, starà così 5074 e tanto fa 59 fia 86, e così puoi far tutte le simili, e la prova farai come alle antedette, fatta.

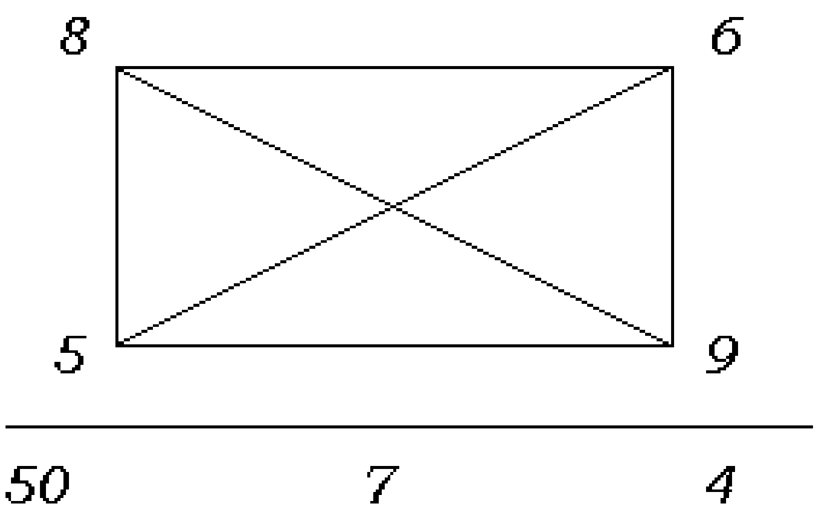
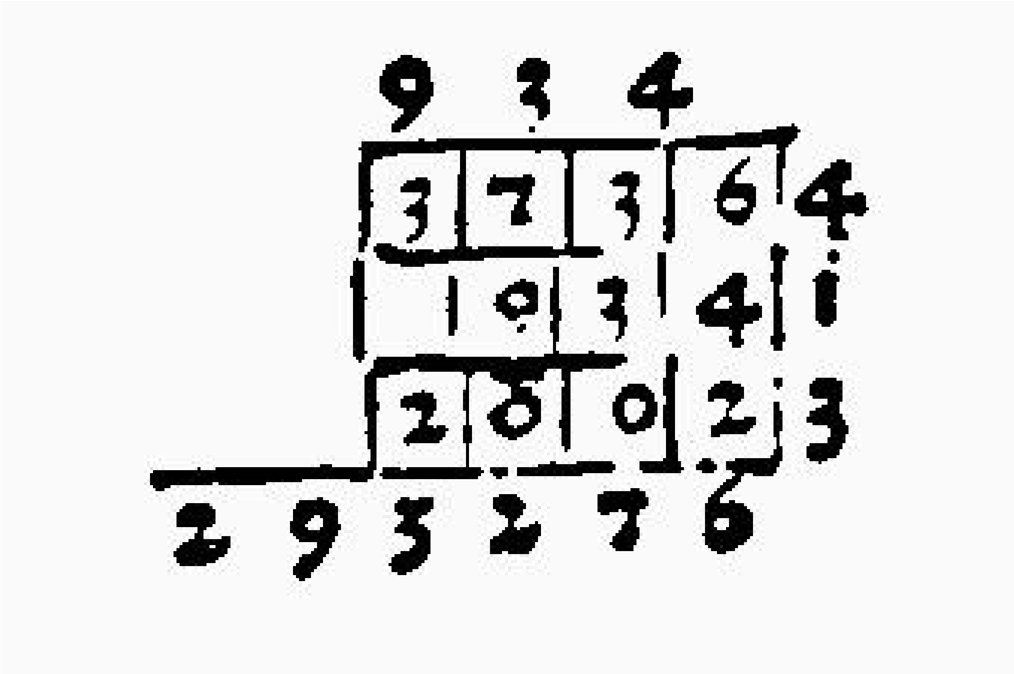


Fig. Il metodo di moltiplicazione a crocetta.

[1] Bottazzini, U., Freguglia, P., Toti Rigatelli, L., Fonti per la storia della matematica, Sansoni, pag 24.

Il ***quadrilatero*** era un altro metodo molto comune, esposto anche nel *Liber abaci*. Questo è lo schema relativo alla stessa moltiplicazione precedente, tratto sempre dall'*Aritmetica di Treviso*:



L'attuale metodo veniva detto in Toscana *per* ***biricucolo*** e lo stesso metodo veniva invece indicato come *per schacchiere* a Venezia e *per organetto* a Verona.

Nel 1478 esce ***Larte de labbacho*** (noto anche come ***Aritmetica di Treviso***), il primo manuale di aritmetica stampato (di autore anonimo) orientato alla matematica necessaria per le arti mercantili e nel 1494 esce la ***Summa de aritmetica, geometria, proporzioni et proporzionalità***, che racchiude tutto il sapere matematico elaborato nel periodo buio del medioevo. Questi testi e altri segnano di fatto l'avvento definito del sistema posizionale decimale.

LINK

http://www2.math.unifi.it/~archimede/archimede/note_storia/numeri/numeri1/node8.html#moltiplicazione

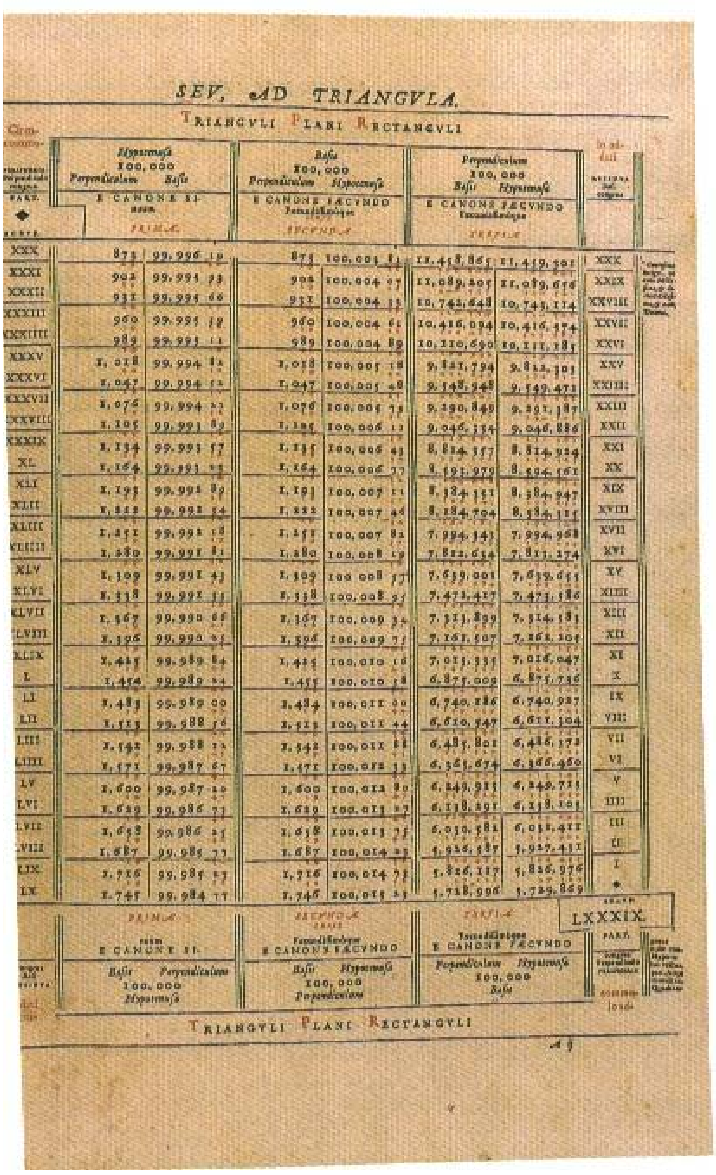
http://www.dm.uniba.it/ipertesto/indice.doc

http://www2.math.unifi.it/~archimede/archimede/fibonacci/immagini_mostra/virtuale.php

Dalle frazioni decimali ai numeri decimali con la virgola

Contrariamente a quanto si può pensare, l'uso della virgola nella rappresentazione dei numeri non interi non è contemporaneo all'introduzione del sistema posizionale decimale.

Fibonacci, che tanto contribuì all'introduzione del sistema decimale in Europa, non si rese conto della possibilità di descrivere quantità frazionarie mediante l'uso della virgola e di ulteriori cifre decimali. L’uso sistematico della virgola fu invece introdotto solo tre secoli più tardi.



SEV, AD TRIANGVLA.

TRIANGVLI PLANI RECTANGVLI

	Hypotenusa 100,000 Perpendiculum	Basis	Basis 100,000 Perpendiculum	Hypotenusa	Perpendiculum 100,000 Basis	Hypotenusa	
	E CANONE SInuum PRIMÆ		E CANONE FÆCVNDO SECVNDÆ		E CANONE FÆCVNDO TERTIÆ		
XXX	873	99.996 19	873	100,003 81	11,458,865	11,459,301	XXX
XXXI	902	99.995 93	902	100,004 07	11,089,205	11,089,656	XXIX
XXXII	931	99.995 66	931	100,004 35	10,742,648	10,743,114	XXVIII
XXXIII	960	99.995 39	960	100,004 61	10,416,094	10,416,574	XXVII
XXXIIII	989	99.995 11	989	100,004 89	10,110,690	10,111,185	XXVI
XXXV	1,018	99.994 82	1,018	100,005 18	9,821,794	9,822,303	XXV
XXXVI	1,047	99.994 52	1,047	100,005 48	9,548,948	9,549,471	XXIIII
XXXVII	1,076	99.994 21	1,076	100,005 79	9,290,849	9,291,387	XXIII
XXXVIII	1,105	99.993 89	1,105	100,006 11	9,046,334	9,046,886	XXII
XXXIX	1,134	99.993 57	1,135	100,006 43	8,814,357	8,814,924	XXI
XL	1,164	99.993 23	1,164	100,006 77	8,593,979	8,594,561	XX
XLI	1,193	99.992 89	1,193	100,007 11	8,384,351	8,384,947	XIX
XLII	1,222	99.992 54	1,222	100,007 46	8,184,704	8,185,315	XVIII
XLIII	1,251	99.992 18	1,251	100,007 82	7,994,341	7,994,968	XVII
XLIIII	1,280	99.991 81	1,280	100,008 19	7,812,634	7,813,274	XVI
XLV	1,309	99.991 43	1,309	100 008 57	7,639,001	7,639,655	XV
XLVI	1,338	99.991 05	1,338	100,008 95	7,472,417	7,473,086	XIIII
XLVII	1,367	99.990 66	1,367	100,009 34	7,313,899	7,314,583	XIII
XLVIII	1,396	99.990 25	1,396	100,009 75	7,161,507	7,162,205	XII
XLIX	1,425	99.989 84	1,425	100,010 16	7,015,335	7,016,047	XI
L	1,454	99.989 42	1,455	100,010 58	6,875,009	6,875,736	X
LI	1,483	99.989 00	1,484	100,011 00	6,740,186	6,740,927	IX
LII	1,513	99.988 56	1,513	100,011 44	6,610,547	6,611,304	VIII
LIII	1,542	99.988 12	1,542	100,011 88	6,485,801	6,486,572	VII
LIIII	1,571	99.987 67	1,571	100,012 33	6,365,674	6,366,460	VI
LV	1,600	99.987 20	1,600	100,012 80	6,249,915	6,249,715	V
LVI	1,629	99.986 73	1,629	100,013 27	6,138,191	6,138,105	IIII
LVII	1,658	99.986 25	1,658	100,013 75	6,030,582	6,031,411	III
LVIII	1,687	99.985 77	1,687	100,014 23	5,926,587	5,927,431	II
LIX	1,716	99.985 27	1,716	100,014 73	5,826,117	5,826,976	I
LX	1,745	99.984 77	1,746	100,015 23	5,728,996	5,729,869	◆
	PRIMÆ E CANONE SI-nuum		SECVNDÆ E CANONE FÆCVNDO		TERTIÆ E CANONE FÆCVNDO		LXXXIX
	Basis Perpendiculum 100,000 Hypotenusa		Basis Hypotenusa 100,000 Perpendiculum		Perpendiculum Hypotenusa 100,000 Basis		

TRIANGVLI PLANI RECTANGVLI

Fig. ???Una pagina del *Canon mathematicus* di Viete con le frazioni decimali, 1571. (da http://euler.us.es/~libros/aritmetica.html)

L’uso della virgola viene anticipato dall’uso delle ***frazioni decimali***, in contrapposizione a quelle sessagesimali, e si riscontra nei testi di alcuni matematici del 1500, come Stevin e Viete. Il loro uso era stato comunque anticipato cinque secoli prima dal matematico arabo Abu'l Hasan Ahmad ibn Ibrahim al-Uqlidisi (c. 920-c. 980).

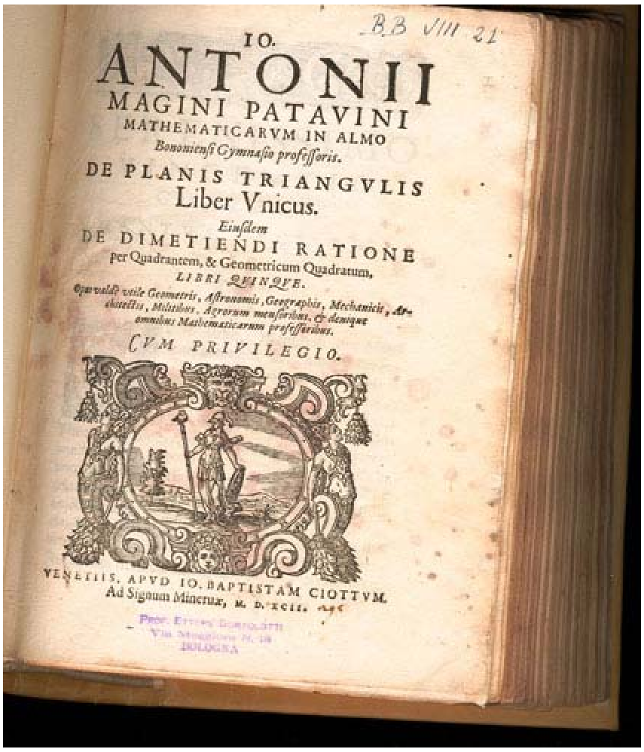


Fig. Frontespizio dell'opera *De planis triangulis* di Magini. (da http://www.dm.unibo.it/libradm/document/500ant/500.html#magini)

Carl Boyer attribuisce il primo uso della virgola al matematico italiano Giovanni Antonio Magini (1555-1617), un astronomo amico di Keplero e concorrente con Galileo alla cattedra di matematica a Bologna.

Nel suo libro *De planis triangulis* del 1592 sono presenti i primi numeri con la virgola.

La virgola (nel continente europeo) o il punto decimale (nei paesi anglosassoni) diventarono di uso comune soltanto venti anni più tardi, quando le tavole logaritmiche, inventate dal matematico scozzese Nepero, furono introdotte per velocizzare i calcoli matematici.

La rappresentazione mediante la virgola permise di rendere omogenei gli algoritmi usati con i numeri interi con quelli usati per gestire la parte non intera.

```
     4253 ×
     7689 =
------------------
     38277
    34024
   25518
  29771
------------------
  32701317
------------------------------------------
     42,53 ×
     7,689 =
-------------------
     38277
    34024
   25518
  29771
--------------------
  327,01317
```

Fig. La virgola facilita le operazioni con i numeri non interi. La moltiplicazione di 42,53 e 7,689 non è essenzialmente più difficile della moltipli-

cazione dei numeri interi 4253 e 7689, poiché, a parte la gestione della virgola, vengono utilizzati i medesimi procedimenti di calcolo.

Questa notazione si dimostrò poi di particolare importanza anche per i settori scientifici e tecnologici che proprio in quegli anni stavano movendo i primi passi.

LINK

http://members.aol.com/jeff570/fractions.html

http://www.iesmurgi.org/matematicas/materiales/numeros/node7.html

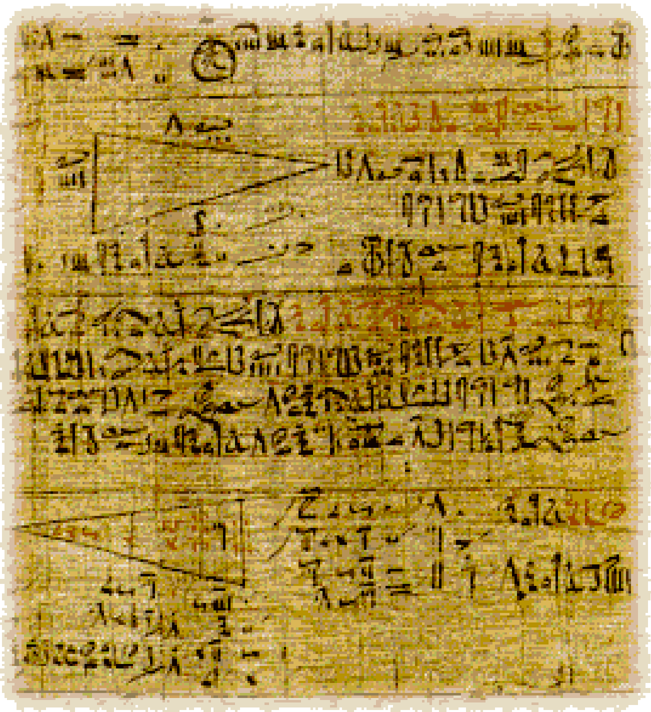
http://members.aol.com/jeff570/fractions.html

http://www.maths.uwa.edu.au/~schultz/3M3/L9AlUqlidisi.html

http://www.maths.uwa.edu.au/~schultz/3M3/L11Stevin.html

3. Antichi algoritmi

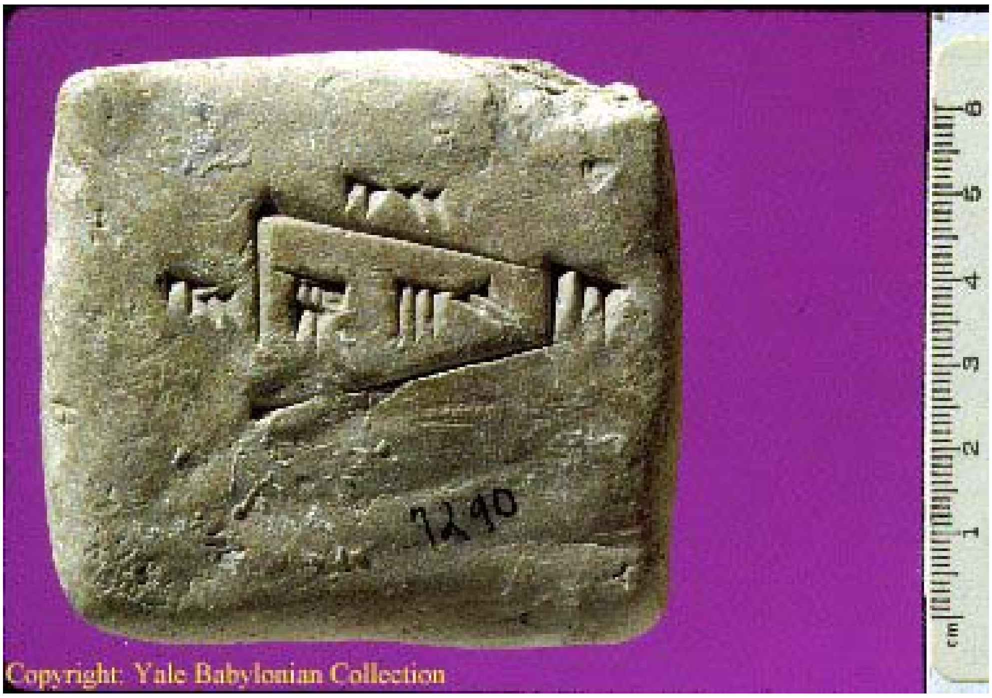
Paolo Giangrandi
paolo.giangrandi@dimi.uniud.it



Università degli Studi di Udine

13/05/2008

3.1. I primi algoritmi



Sebbene l'idea di algoritmo sia un concetto formalmente studiato solo di recente, numerosi algoritmi sono stati prodotti fin dall'antichità in forma di procedimenti matematici.

Troviamo algoritmi nella matematica dell'antico Egitto, in Mesopotamia, nell'antica Cina, in India, ecc.

La descrizione delle procedure risolutive non veniva però data in forma generale (poiché non esisteva ancora il calcolo letterale), ma era fornita mediante esempi numerici particolari spesso senza alcuna parola di commento.

Algoritmi nell'antico Egitto

La matematica dell'antico Egitto è documentata da pochi papiri. Il documento più importante e più noto che descrive la matematica ai tempi dei faraoni è rappresentato dal papiro di Ahmes (papiro di Rhind), scritto dallo scriba Ahmes attorno al 1650 a.C. e copia di uno scritto più vecchio di un paio di secoli precedenti.

Qui vediamo come esempio il problema 63 tratto dal papiro di Ahmes:

Problema 63.

700 razioni di pane devono essere divise tra quattro persone nel seguente rapporto:

$$\frac{2}{3} : \frac{1}{2} : \frac{1}{3} : \frac{1}{4}$$

Algoritmo.

Sommare

$$\frac{2}{3} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{7}{4}.$$

$$\begin{aligned}\frac{700}{7/4} &= 700\cdot\frac{4}{7}\\ &= 700\left(\frac{2}{7}+\frac{2}{7}\right)\\ &= 700\left(\frac{1}{4}+\frac{1}{28}+\frac{1}{4}+\frac{1}{28}\right)\\ &= 700\left(\frac{1}{2}+\frac{1}{14}\right)\\ &= 350+50\\ &= 400\end{aligned}$$

Il numero che si ottiene 400 è il numero base. Ora si tratta di moltiplicare ogni frazione per 400 per ottenere le razioni per ciascuna persona.

Questo algoritmo non fa comprendere immediatamente la spiegazione del procedimento seguito.

Riesaminando il problema nel linguaggio moderno possiamo scrivere:

$$\frac{x_1}{x_2}=\frac{\frac{2}{3}}{\frac{1}{2}},\quad \frac{x_2}{x_3}=\frac{\frac{1}{2}}{\frac{1}{3}},$$

ecc., dove x_1, x_2, x_3, x_4 sono le razioni incognite spettanti alle quattro persone. Da queste uguaglianze possiamo dire che esiste un numero *a* tale che:

$$x_1 = \frac{2}{3}a$$
$$x_2 = \frac{1}{2}a$$
$$x_3 = \frac{1}{3}a$$
$$x_4 = \frac{1}{4}a$$

allora sommando le incognite possiamo scrivere,

$$x_1 + x_2 + x_3 + x_4 = (\frac{2}{3} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4})a = 700$$

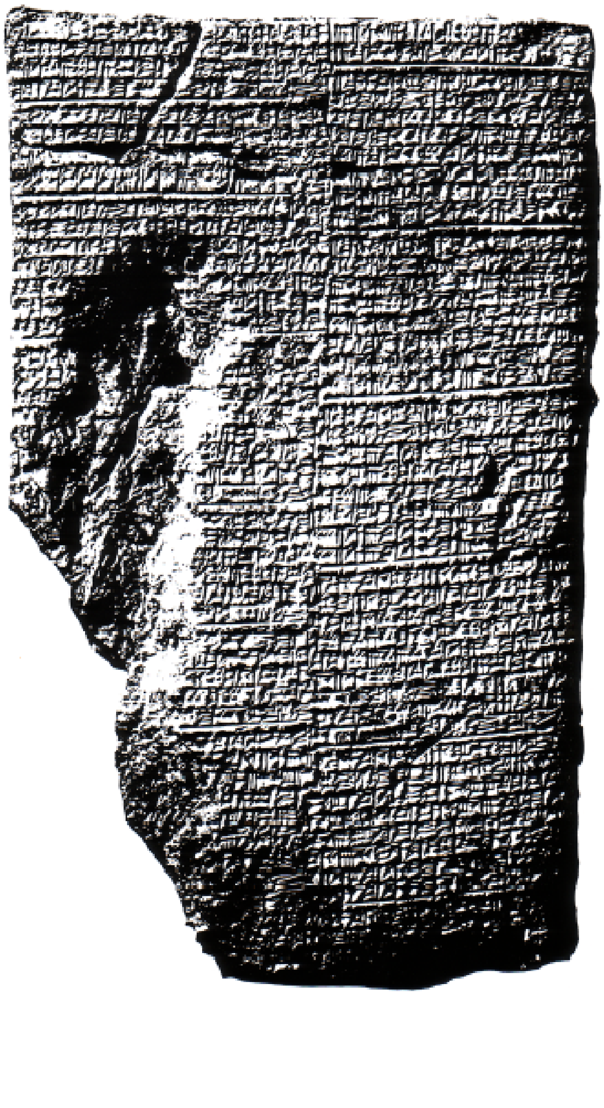
Sommando le frazioni al secondo membro si ottiene 7/4. Infine, moltiplicando il reciproco di questa frazione per 700 si ricava:

$$a = 400.$$

che permettere di calcolare x_1, x_2, x_3, x_4.

Algoritmi nell'antica Mesopotamia

La matematica babilonese è documentata dal ritrovamento di numerose tavolette cuneiformi. I Babilonesi erano in grado di risolvere problemi algebrici di primo e secondo grado e disponevano di tecniche per risolvere svariati problemi geometrici.



Qui vedremo come esempio, il metodo babilonese per risolvere le equazioni di secondo grado. Questo è essenzialmente basato sul completamento del quadrato.

L'esempio che consideriamo è tratto dalla tavoletta BM 13901 scritta tra il 2000 e il 1500 a.C. e recita:

Problema 1, BM 13901.

> ***Ho sommato la superficie [e il lato] del quadrato: fa ¾.***

L'equazione data in forma retorica corrisponde alla forma simbolica:

$$x^2 + 1x = \frac{3}{4}$$

Algoritmo.

- ***a) Prendi il coefficiente 1 [numero dei lati considerato].***
- ***b) Dividilo a metà. Tu hai ½.***
- ***c) Moltiplica ½ con ½*** **[fa ¼]).**
- ***d) Congiungi ¼ con ¾ e*** **(fa)** ***1 che ha 1 come radice quadrata.***
- ***e) ½ che tu hai moltiplicato*** **[per se stesso]*, sottrai da 1* e (fa)** ***½***
- ***f)*** **(che) è (il lato del)** ***quadrato.***

La descrizione corrisponde al seguente algoritmo:

$$x = \sqrt{(1/2)^2 + \frac{3}{4}} \quad - \quad \frac{1}{2}$$

Non è chiaro il modo con cui i Babilonesi sia pervenuti a questa formula, ma diversi studiosi avanzano l'ipotesi che sia derivata da un procedimento di tipo geometrico.

LINK

http://www.malhatlantica.pt/mathis/Babilonia/BM13901.htm http://it.stlawu.edu/%7Edmelvill/mesomath/Rectangular.html

Algoritmi senza dimostrazione

Le civiltà più antiche, come quelle babilonese, egizia e cinese, ci hanno lasciato numerosi ed importanti contributi matematici, ma nelle tante tavolette e papiri a noi pervenuti **manca del tutto una giustificazione** (**dimostrazione**) dei procedimenti risolutivi.

Sulla base delle testimonianze disponibili, gli studiosi sono concordi nel ritenere che in Egitto, in Mesopotamia, in Cina e in India mancasse del tutto un sistema logico-deduttivo analogo al nostro. Consideriamo ad esempio il ***problema 14*** tratto dal ***Papiro di Mosca***.

Fig. Il problema 14 del Papiro di Mosca per trovare il volume di un tronco di piramide.

Il problema è quello di trovare il volume di un tronco di piramide di base quadrata alto 6 unità e con gli spigoli della base superiore e di quella inferiore rispettivamente di 2 e 4 unità.

Versione letterale	Traduzione moderna
"Se ti si dice: una piramide tronca di 6 per l'altezza verticale, di 4 sulla base, di 2 sulla cima. Tu devi quadrare questo 4, risultato 16. Tu devi quadrare 2, risultato 4. Tu devi moltiplicare 4 e 2, risultato 8. Tu devi sommare il 16, l'8 e il 4, risultato 28. Tu devi prendere un terzo di 6, risultato 2. Tu devi prendere 28 due volte, risultato 56. Vedi, è 56. Troverai che è corretto."	Sia h l'altezza verticale, a e b i lati dei due quadrati che stanno alla base e alla sommità, e V il volume del solido. Trovate l'area del quadrato di base: a^2. Trovate l'area del quadrato alla sommità: b^2. Trovate il prodotto di a e b: ab. Trovate $a^2 + ab + b^2$. Trovate 1/3 dell'altezza: h/3. $(a^2 + ab + b^2)h/3$. $V = (a^2 + ab + b^2)h/3$

Nel papiro manca una qualunque indicazione sul perché questa "ricetta" fornisce la risposta corretta: bisogna accontentarsi del "***Troverai che è corretto***".

Non sappiamo attraverso quale strada gli Egizi siano pervenuti a questo procedimento: forse il volume del tronco di piramide è stato ricavato come differenza tra due piramidi, oppure deriva da qualche osservazione empirica, ma nulla viene suggerito in tal senso nel testo.

La stessa mancanza di spiegazione si riscontra in tutti gli altri documenti a noi pervenuti.

Alcuni studiosi ritengono che questo visione dogmatica della matematica rifletta in qualche modo il tipo di **struttura sociale caratterizzante queste civiltà**, basata essenzialmente su un potere di carattere autoritario e su una suddivisione rigida della società in caste.

In che modo allora gli antichi hanno prodotto tanti risultati che sono in molti casi esatti? L'ipotesi più probabile che **le conoscenze matematiche fossero prodotte principalmente per via sperimentale**: da un lato procedendo per tentativi ed errori e dall'altro lato applicando un processo di induzione a partire da tante osservazioni di situazioni concrete. Nei documenti a nostra disposizione comunque non compare alcun riferimento ad una qualunque attività sperimentale.

Naturalmente le conseguenze di questa mancanza di una qualunque spiegazione era quella di ostacolare non poco il progresso delle conoscenze scientifiche.

LINK

http://www.math.buffalo.edu/mad/Ancient-Africa/mad_ancient_egypt.html

http://www.dipmat.unipg.it/~bartocci/PIRAM.htm

http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Egyptian_papyri.html

3.2. I Greci e gli algoritmi con dimostrazioni

Come abbiamo detto, gli Egizi, i Babilonesi e le altre civiltà antiche non distinguevano tra risultati esatti e risultati approssimati e nei loro contributi alla matematica non troviamo alcun riferimento ad una giustificazione della correttezza dei procedimenti utilizzati.

Il merito di aver compreso l'importanza di questo aspetto va principalmente agli antichi matematici greci: nessuna civiltà precedente o contemporanea comprese così bene l'importanza di fondare i risultati della matematica su una giustificazione logica rigorosa.

I Greci compresero che la ragione e non i sensi, dovevano costituire il fondamento metodologico per la matematica.

I Greci furono i grandi inventori del metodo ipotetico-deduttivo che ancora oggi utilizziamo e possiamo dire che tale scoperta costituisce una sorta di spartiacque tra la matematica pre-greca e quella successiva.

Non è del tutto chiaro come mai furono proprio i Greci (tra il VI e il V sec.) ad introdurre la moderna dimostrazione matematica, ma gli studiosi evidenziano alcuni motivi fondamentali che contribuirono ad indirizzare i Greci su tale strada:

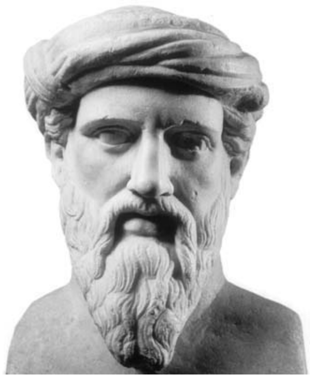
- un ***motivo di natura euristica***, legato alle necessità pratiche di discernere fra procedimenti corretti e quelli errati;
- un ***motivo di natura filosofica,*** legato alla spinta che manifestarono i grandi filosofi greci nella ricerca del "vero" e nella ricerca dei "principi primi";
- un ***motivo pedagogico***, legato alla necessità di trasmettere ad altri il sapere;
- un ***motivo di natura ideologica***, correlato alla forte differenza politica fra la democrazia greca e il totalitarismo caratterizzante altre civiltà.

Il sistema assiomatico-deduttivo elaborato nell’età ellenistica appare per la prima volta in tutta la sua forza e compiutezza nell’opera di Euclide, gli ***Elementi***, composti attorno al 300 a.C.

Comunque **nelle opere filosofiche di Aristotele** (384-322 a.C.), che cronologicamente precedono di poco quelle di Euclide (circa 325-265 a.C.), **si trovano già descritte le linee guida** a cui il grande matematico alessandrino si atterrà per elaborare la sua opera immortale.

3.3. Sui numeri computabili con le quattro operazioni

Che cosa si può calcolare con le quattro operazioni?

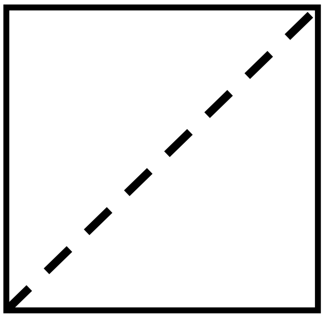


Il sistema della quattro operazioni con i numeri razionali (assoluti) ad essi legato appariva ai Pitagorici sufficiente a trattare ogni questione pratica, ma anche teorica della matematica.

Sappiamo che i numeri nella **Scuola Pitagorica** non solo costituirono l'oggetto delle prime teorie matematiche, ma, nell'ambito delle ricerche filosofiche sul problema dell'*archè* (ossia del principio di tutte le cose), rappresentarono di fatto la base di una teoria con cui interpretare il mondo. "***Tutto è numero***" è il motto famoso che sintetizza lo spirito filosofico della Scuola Pitagorica.

Pitagora credeva che tutte le relazioni caratterizzanti il mondo reale potessero essere interpretate in termini di relazioni tra numeri e in un certo senso possiamo dire che la sua teoria fu il primo tentativo per cercare un'interpretazione su base razionale del cosmo: questa idea verrà ripresa duemila anni più tardi da Galileo e costituirà il punto di partenza della moderna rivoluzione scientifica!

Incommensurabilità della diagonale

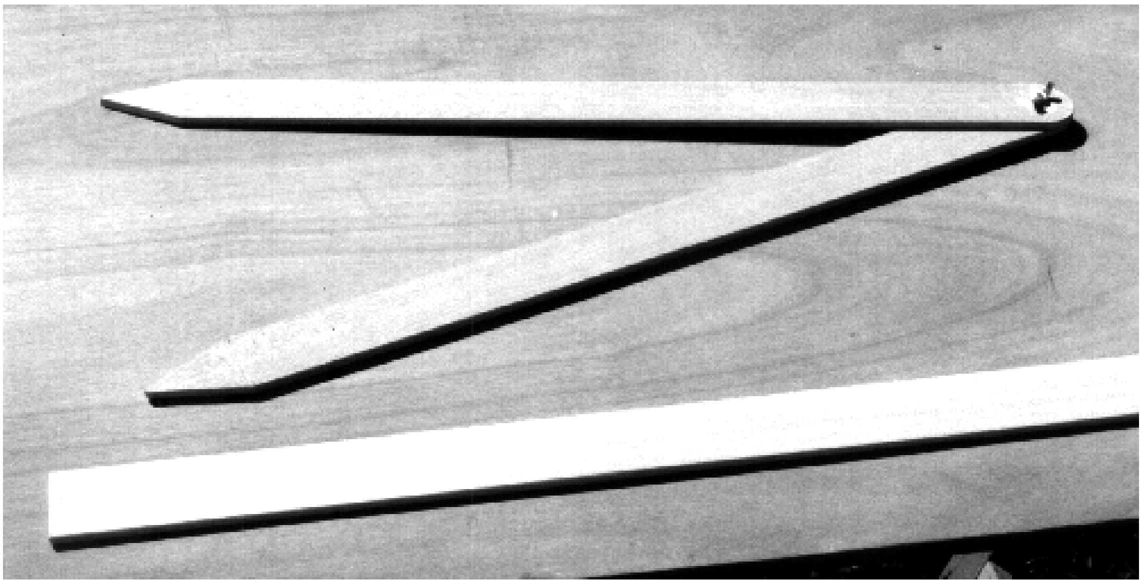


Nessun numero razionale p/q permette di “misurare” la diagonale del quadrato → numeri irrazionali

In termini computazionali: le quattro operazioni applicate ai numeri razionali non permettono di calcolare la diagonale del quadrato.

L’incommensurabilità della diagonale determinò una crisi profonda nei confronti dei sistemi numerici: i matematici cominciano a fondare la matematica su un sistema geometrico.

Euclide, negli Elementi, tratta le grandezze numeriche mediante segmenti.



La riga e il compasso sembravano più potenti delle quattro operazioni aritmetiche.

Algoritmi con riga e compasso

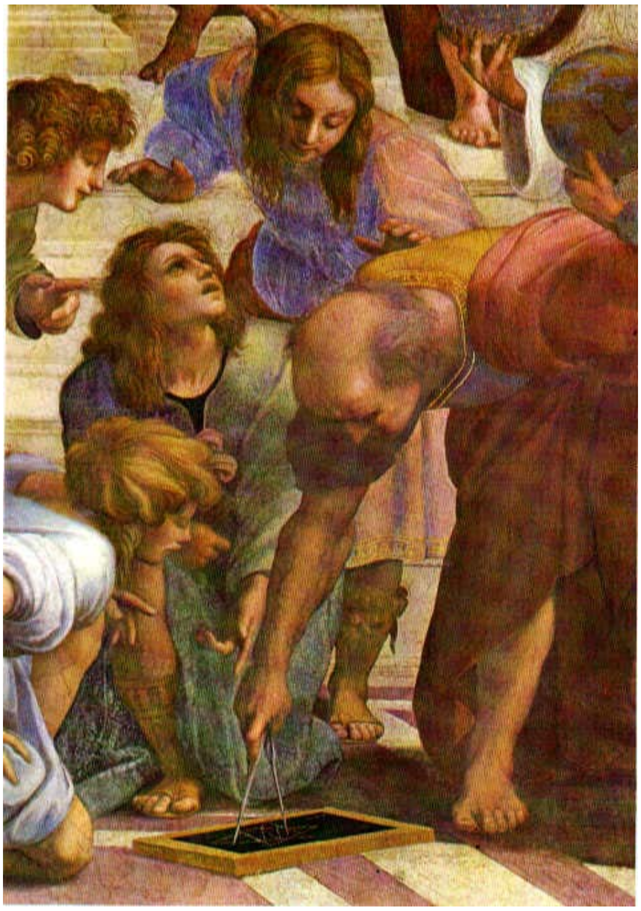


Fig. Euclide, particolare della Scuola di Atene di Raffaello.

Sebbene quando si parla di algoritmi si tenda a pensare a procedure per manipolare numeri (in forma numerica o in forma simbolica), nella storia degli algoritmi hanno avuto un ruolo importante le costruzioni geometriche con riga e compasso.

Molte delle costruzioni geometriche realizzate con la riga e il compasso possono essere interpretate anche in senso algebrico. Infatti, gli antichi Greci erano in grado di risolvere equazioni di 1° e 2° grado mediante opportune costruzioni geometriche.

Gli algoritmi con riga e compasso rappresentarono per molti secoli uno dei punti più alti raggiunti dai matematici.

Dal punto di vista dell'informatica, la restrizione all'uso della sola riga e compasso e l'impianto assiomatico ad esso collegato rappresentarono un modello di rigore non solo per la matematica ma anche per il concetto di procedura algoritmica.

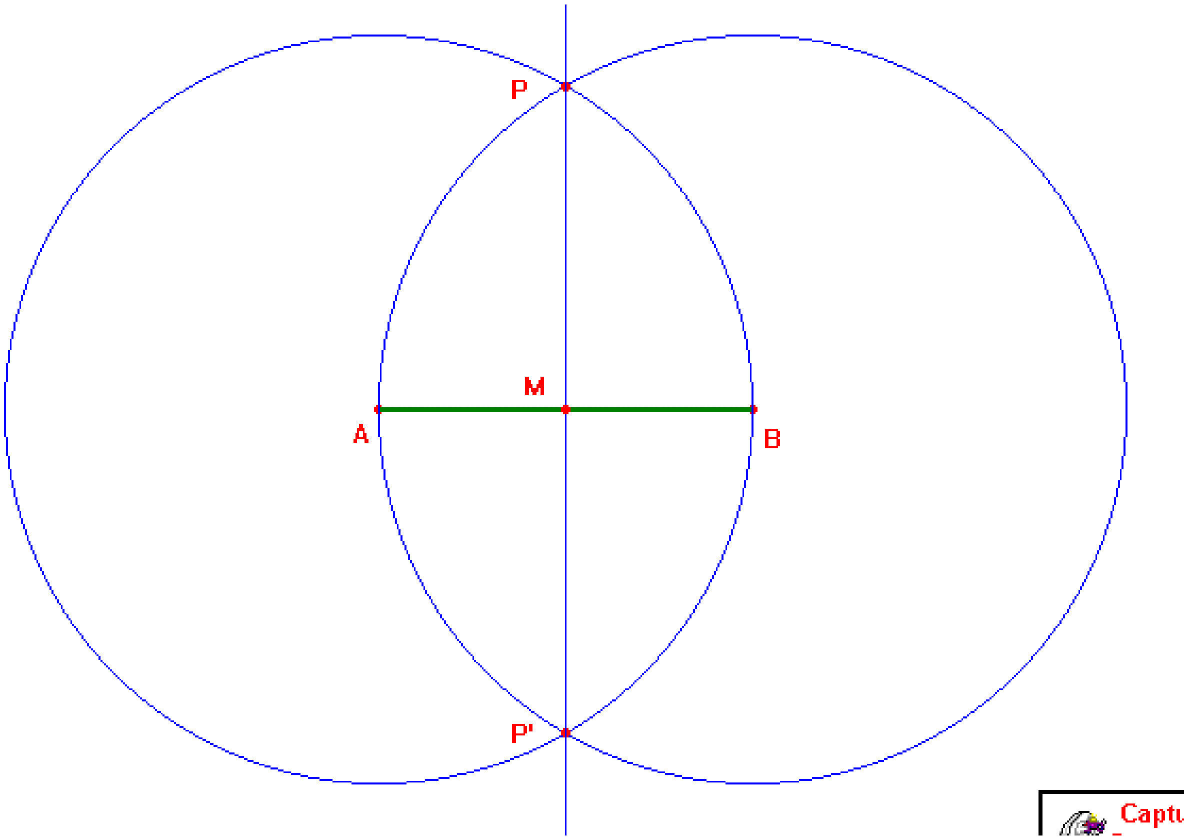
I Greci e le costruzioni con riga e compasso

Fig. Due pagine del testo di Euclide, in una delle versioni più antiche (Biblioteca Vaticana)

Una costruzione geometrica è considerata valida quando **ogni oggetto geometrico viene costruito con riga e compasso e non è scelto ad occhio o mediante misurazione**. Più precisamente, le costruzioni con riga e compasso vengono realizzate attraverso alcune operazioni elementari che sono:

a) disegno di una retta (libera, passante per un punto, o per due punti,
b) disegno di una circonferenza (libera, di dato centro, o di dato centro e di dato raggio),
c) intersezione di due rette,
d) intersezione di una circonferenza con una retta,
e) intersezione di due circonferenze.

Ognuna di queste operazioni consente di individuare nuovi punti con cui procedere per realizzare la figura desiderata. Ogni **costruzione geometrica** parte da alcuni dati, che sono gli oggetti geometrici di partenza (rette, segmenti, circonferenze, ecc.) e tramite un numero finito di passi costituiti dalle operazioni elementari *a), b)* e *c)* e permette di realizzare un nuovo oggetto.



Algoritmo di Euclide

L'algoritmo di Euclide rappresenta un esempio classico di algoritmo per calcolare il M.C.D. di due numeri naturali e si trova descritto negli ***Elementi* di Euclide** (circa 300 a.C.). Non sappiamo se l'algoritmo sia stato scoperto per primo da Euclide, oppure fosse già noto in precedenza.

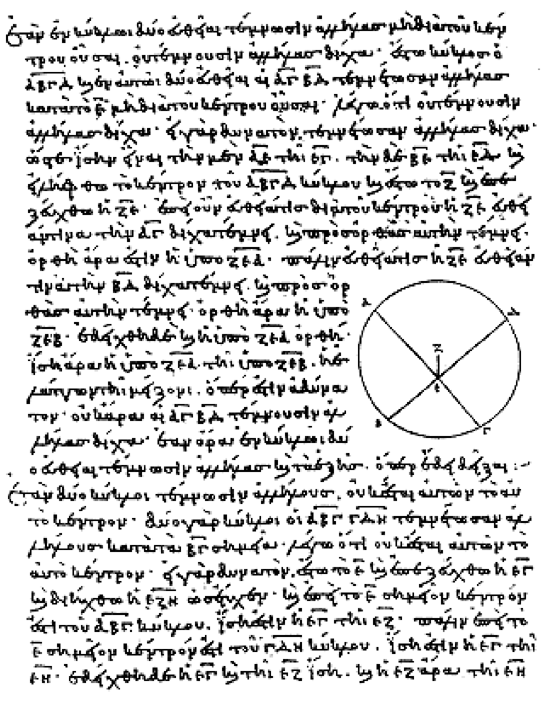
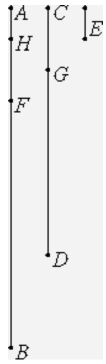


Fig. Questa è una pagina presa da un'edizione medioevale degli Elementi (888 d.C.).

Negli *Elementi* **il procedimento per la ricerca del massimo comun divisore (M.C.D.) è dato in forma geometrica**, poiché i greci non possedevano ancora un formalismo algebrico come quello dai oggi utilizzato.

Dagli Elementi di Euclide: Libro VII



Proposizione 2

Svolgimento. Siano AB, CD i due numeri dati che non sono primi fra loro. Si deve comunque trovare il massimo comun divisore di AB, CD.

Supponiamo dapprima che CD divida AB; ma esso, d'altra parte, divide anche sé medesimo per cui CD [in tal caso] è divisore comune di CD, AB. Ed è evidente che è anche il massimo; infatti nessun numero maggiore di CD può dividere CD.

Se invece CD non divide AB, ed a partire da AB, CD si continua a sottrarre di volta in volta il numero minore dal maggiore, la differenza dal minore, e così via, rimarrà un numero che dividerà quello immediatamente precedente. Infatti non si avrà come ultimo resto l'unità; in caso contrario, AB, CD sarebbero primi fra loro, il che non è per ipotesi. Si avrà quindi un numero, come ultimo resto, che dividerà quello immediatamente precedente. E allora CD, dividendo BE, lasci il resto EA minore di CD, mentre EA, dividendo DF, lasci il resto CF minore di EA, e si supponga che CF divida AE. Poiché dunque CF divide AE, ed AE divide DF, si ha che CF dividerà pure DF, ma divide anche se stesso, per cui dividerà anche tutta quanta la somma CD. Ma CD divide BE; quindi anche CF divide BE; ma divide pure EA, per cui dividerà anche tutta quanta la somma BA; ma esso divide pure CD, quindi CF è divisore comune di AB, CD. Dico ora che è anche il massimo. Infatti, se CF non fosse il massimo comun divisore di AB, CD, un altro numero, che fosse maggiore di CF, dividerebbe i numeri AB, CD. Li divida, e sia esso G. E poiché G divide CD, ma CD divide BE, anche G divide BE; ma esso divide pure tutta quanta la somma BA, per cui dividerà anche la differenza AE. Ma AE divide DF; quindi anche G dividerà DF; ma esso divide pure tutta quanta la somma CD, per cui dividerà anche la differenza CF, cioè un numero maggiore dividerebbe un numero minore – il che è impossibile; non può quindi un altro numero, che sia maggiore di CF, dividere i numeri AB, CD; dunque CF è il massimo comun divisore di AB, CD.

Fig. L'algoritmo di Euclide nella versione geometrica data negli *Elementi*.

Nella descrizione di Euclide, vengono dati solo i primi passi in modo che il lettore possa comprendere come deve procedere in generale. All'epoca di Euclide, infatti, non esisteva ancora un formalismo algebrico per descrivere in modo generale i procedimenti iterativi.

Algoritmo di Euclide (versione algebrica):

Sia $a > 0$, $b \geq 0$ e $a \geq b$

```
inizio
mentre a ≠ b esegui la seguente istruzione
    se a > b allora  a ← a – b
        altrimenti  b ← b – a
scrivi "Il M.C.D. è ", valore di a
fine
```

Fig. Versione moderna dell'algoritmo di Euclide per il calcolo del massimo comun divisore.

I problemi classici non risolubili con riga e compasso

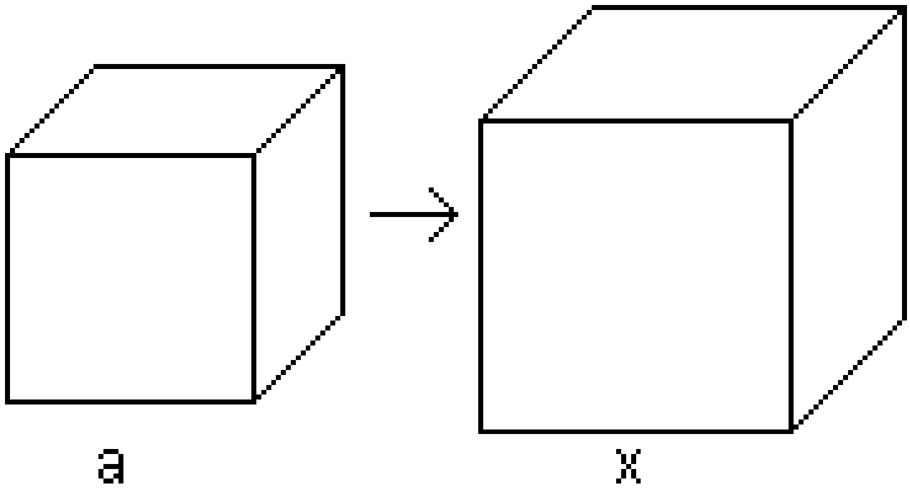


Fig. Problema della duplicazione del cubo.

Le costruzioni geometriche realizzate con riga e compasso dagli antichi matematici Greci sono numerose, ma alcuni problemi sfidarono le capacità e la creatività dei grandi geometri. Tra questi problemi quelli che passarono alla storia perché su di essi si affannarono per secoli i matematici dell'antica Grecia e moltissimi altri matematici furono tre.

- Il problema della quadratura del cerchio.
- Il problema della trisezione di un angolo.
- Il problema della duplicazione del cubo.

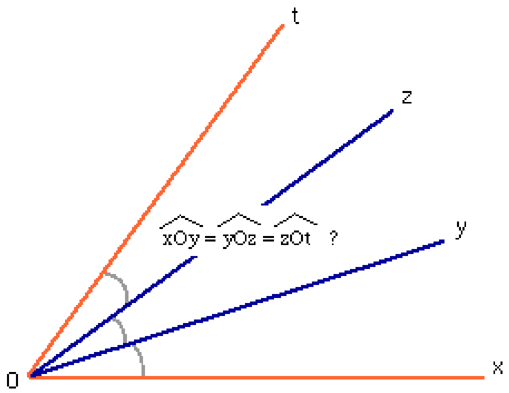


Fig. Problema della trisezione di un angolo.

Per due millenni i migliori matematici del mondo tentarono invano di risolvere questi problemi, fino a quando nel 1800, lo studio sistematico della matematica che sta dietro alle costruzioni matematica mise in evidenza l'impossibilità di trovare una soluzione a questi tre problemi mediante i soli strumenti di riga e compasso.

L'impossibilità di risolvere sia il problema della duplicazione del cubo che il problema della trisezione dell'angolo con il solo uso di riga e compasso venne provata algebricamente dal matematico francese Pierre Laurent Wantzel nel 1837.

Infine, non fu che nel 1882 che Ferdinand von Lindemann provò rigorosamente l'impossibilità della quadratura del cerchio dimostrando la trascendenza di π.

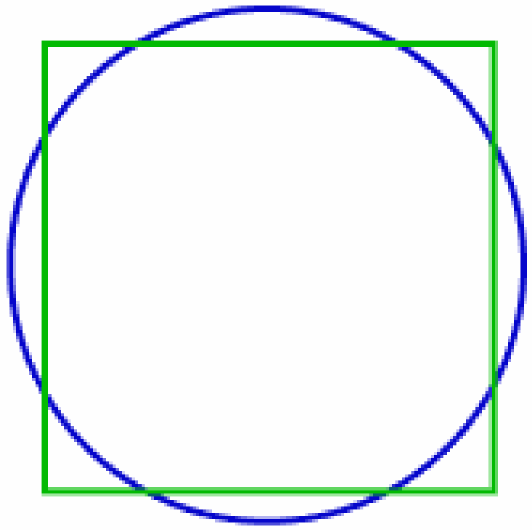


Fig. Problema della quadratura del cerchio.

3.4. Due famosi esempi di antichi algoritmi

Il crivello di Eratostene

Fig. Eratostene di Cirene (276 a.C. – 194 a.C.)

I numeri primi hanno da sempre costituito un tema di interesse per i matematici e la loro ricerca con metodi efficienti ha attirato tanti studiosi.

I numeri primi assumono un ruolo molto importante nella teoria dei numeri e oggi, hanno assunto un'importanza ancor più grande per quanto riguarda i metodi crittografici.

Uno dei metodi più antichi e anche più efficiente per individuare numeri primi è dovuto al matematico greco **Eratostene di Cirene**. Eratostene (circa 284 a.C. – 192 a.C.), nato a Cirene (nell'attuale Libia), oltre che matematico fu astronomo e direttore della famosa Biblioteca di Alessandria d'Egitto.

Per gli astronomi e cartografi, Eratostene è rimasto famoso anche per la prima misurazione scientifica della terra.

Il **crivello di Eratostene**, come descritto nel libro di Nicomaco, identifica tutti i numeri primi minori di un dato numero *n* mediante il seguente procedimento:

a) scriviamo in ordine crescente tutti i numeri dispari da 3 a n; non ha senso considerare i numeri pari perché tranne 2 non possono essere primi;
b) eliminiamo tutti i numeri multipli di 3 (ad esclusione del 3); nella lista, questi numeri si trovano distanziati l'uno dall'altro di tre posizioni;
c) cerchiamo nella lista il primo numero più grande di 3 non eliminato: questo numero è 5;
d) eliminiamo tutti i numeri multipli di 5 (ad esclusione del 5); nella lista, questi numeri si trovano distanziati l'uno dall'altro di cinque posizioni;
e) passiamo al numero successivo a 5 non eliminato, cioè 7 e ripetiamo la medesima operazione di eliminazione dei multipli;
f) procediamo in questo modo fino a n;
g) i numeri non cancellati dalla lista rappresentano i numeri primi fino ad n.

(possiamo osservare che dalla lista manca il numero 2). Un aspetto importante di questo metodo è rappresentato dal fatto che utilizza solo operazioni di moltiplicazione e non di divisione.

Esempio. Consideriamo tutti i numeri fino a 40:

3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39

cancelliamo i multipli di 3:

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 25 ~~27~~ 29 31 ~~33~~ 35 37 ~~39~~

cancelliamo i multipli di 5:

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 ~~25~~ ~~27~~ 29 31 ~~33~~ ~~35~~ 37 ~~39~~

Passando a 7, 11, ecc, nessun altro numero può essere cancellato, pertanto i numeri rimasti sono numeri primi:

3 5 7 ~~9~~ 11 13 ~~15~~ 17 19 ~~21~~ 23 ~~25~~ ~~27~~ 29 31 ~~33~~ ~~35~~ 37 ~~39~~

Fig. Esempio di applicazione del crivello di Eratostene per i numeri fino a 40.

Il matematico arabo Ibn al-Banna (XIII sec.) osservò poi che nel procedimento di Eratostene non serviva ripetere il processo fino ad n (come indicato nel passo f), ma era sufficiente procedere nel processo di eliminazione fino ad un numero pari a $\sqrt{n}$.

Metodo di Erone per estrarre la radice quadrata

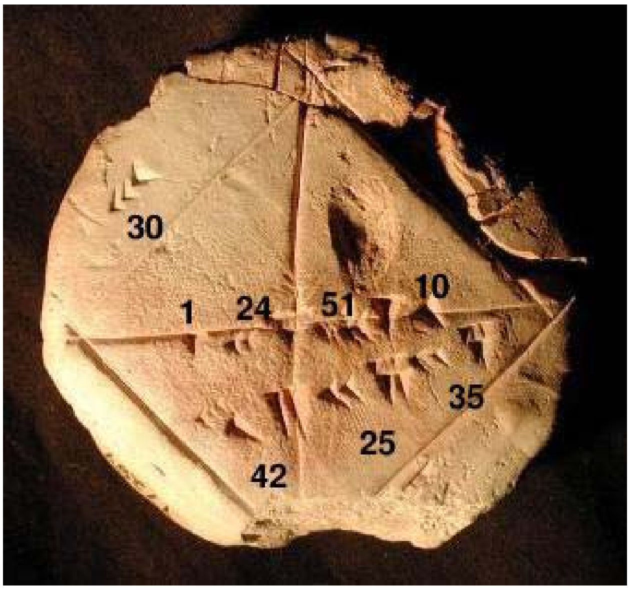


Fig. Tavoletta Babilonese con la radice quadrata di 2.

Fig. Erone di Alessandria, da una traduzione tedesca del 1688 del libro *Pneumatica* di Erone.

Il primo esempio di metodo per estrarre la radice quadrata di cui siamo a conoscenza è quello del matematico alessandrino Erone, vissuto nel I sec. a.C..

Il suo metodo è di tipo iterativo e ad ogni iterazione viene migliorato il valore precedente disponibile.

Dal momento che 720 *non ha come radice quadrata un numero razionale, possiamo ottenere un'approssimazione molto buona nel seguente modo. Poiché il quadrato più grande e più vicino a* 720 *è* 729*, la cui radice quadrata è* 27*, dividiamo* 720 *per* 27*. Il risultato è* $26\ ^{2}/_{3}$ *. Aggiungendo ad esso* 27*, si ottiene* $53\ ^{2}/_{3}$ *e dividendo per* 2 *si ottiene* $26\ ^{5}/_{6}$ *. Pertanto la radice quadrata di* 720 *è molto vicina a* $26\ ^{5}/_{6}$ *. Infatti, moltiplicando* $26\ ^{5}/_{6}$ *per se stesso, il prodotto dà* $720\ ^{1}/_{36}$ *, perciò la differenza è* $^{1}/_{36}$ *. Se desideriamo rendere la differenza ancora più piccola di* $^{1}/_{36}$ *, prenderemo* $720\ ^{1}/_{36}$ *invece di 729 (o piuttosto* $26\ ^{5}/_{6}$ *invece di 27), e procedendo nello stesso modo troveremo una differenza ancora più piccola di* $^{1}/_{36}$ *.*

Fig. Esempio dato da Erone nel libro *Metrica* per calcolare la radice quadrata in modo approssimato.

Nel libro *Metrica*, Erone descrive (mediante un esempio) il metodo per calcolare la radice quadrata di un numero a partire da un'approssimazione iniziale.

I passi fondamentali del metodo di Erone sono i seguenti:

- supponiamo di voler calcolare la radice quadrata di N.
- all'inizio si sceglie un valore di partenza X_0 scelto arbitrariamente, che utilizzeremo per calcolare un valore X_1 migliore utilizzando la seguente formula:

$$X_1 = (X_0 + N/X_0)/2$$

- a questo punto, utilizziamo X_1 per ricavare un'approssimazione X_2 migliore:

$$X_2 = (X_1 + N/X_1)/2$$

- da X_2 ricaviamo X_3 e così via fino ad ottenere approssimazione sempre migliori.

Ad esempio, volendo determinare la radice quadrata di 5, consideriamo come prima approssimazione il valore non corretto $x_0 = 1$. Da questa ricaviamo:

$$x_1 = (1 + 5/1)/2 = 3$$

Al secondo passo ricaviamo:

$$x_2 = (3 + 5/3)/2 = 2.333...$$

Al passo successivo si ottiene

$$x_3 = (2.333... + 5/2.333...)/2 = 2.2381...$$

e così via. Considerando, che il valore corretto di radice quadrata di 5 con cinque cifre significative è 2.2361, possiamo osservare con quale rapidità il metodo converge verso la soluzione esatta.

L’estrazione di radice quadrata pone due problemi:

- dato un numero qualunque, l’algoritmo di Erone termina con un numero finito di passi fornendo un valore esatto, oppure procede all’infinito?
- con altri algoritmi si presenta lo stesso problema, oppure possono avere termine fornendo una risposta esatta?

Come oggi ben sappiamo, l’algoritmo non può avere termine ogni qual volta in cui non siamo di fronte ad un quadrato perfetto e questa difficoltà non deriva dal particolare algoritmo utilizzato, ma è connessa alla natura stessa del problema affrontato.

Per quello che ne sappiamo, i primi a fare chiarezza su questo aspetto furono i matematici pitagorici, anche se il problema non fu posto esattamente in questi termini.

La dimostrazione della non terminazione dell'algoritmo è infatti indirettamente associata alla "terribile" scoperta delle grandezze incommensurabili, di cui ci siamo già occupati nel precedente capitolo.

Se l'algoritmo babilonese di estrazione della radice quadrata avesse termine poniamo per il numero 2, vorrebbe dire che $\sqrt{2}$ è rappresentabile con un numero razionale dal momento che l'algoritmo comprende solo somme e divisione di numeri razionali e componendo in numero finito queste operazioni si ha sempre come risultato un numero razionale.

Il fatto che le grandezze incommensurabili portassero ad algoritmi che non terminano è bene presente nella matematica greca, tant'è aspetto della non terminazione viene ripreso in Euclide quando, nel libro X sulla classificazione degli incommensurabili, egli definisce (proposizione 2) come incommensurabili tra loro due grandezze per le quali il ben noto algoritmo euclideo non termina.

4. La difficile conquista degli algoritmi simbolici

Paolo Giangrandi
paolo.giangrandi@dimi.uniud.it

Università degli Studi di Udine

13/05/2008

4.1. Introduzione

Nella stesura degli algoritmi assume un ruolo importante la notazione con cui vengono scritti. Il linguaggio algoritmico infatti non rappresenta semplicemente uno mezzo di comunicazione, ma rappresenta uno strumento essenziale per riflettere sui problemi: un linguaggio algoritmico "ricco" ed "espressivo" può aprire strade praticamente precluse ad un linguaggio povero di astrazioni.

Lo sviluppo dei linguaggi algoritmici si interseca per certi versi con la storia dell'algebra e delle notazioni algebriche. A questo proposito, seguendo la classificazione data dallo storico G.H.F. Nesselmann, si distinguono tre fasi principali:

- l'***algebra retorica***, nella quale i procedimenti algebrici vengono interamente espressi mediante l'uso del linguaggio naturale;
- l'***algebra sincopata***, nella quale alcuni termini vengono indicati mediante abbreviazioni,
- *l'**algebra simbolica***, nella quale i termini vengono sistematicamente rappresentati da simboli "puri", come nella moderna algebra.

Sebbene oggi molti studiosi ritengano superata la rigida sequenzialità cronologica di queste tre fasi, questa ripartizione è ancora utile anche per classificare i linguaggi algoritmici utilizzati nel corso della storia della matematica.

La conquista del linguaggio simbolico non ha significato semplicemente il raggiungimento di una notazione più comoda e compatta delle precedenti, ma ha rappresentato soprattutto una sorta di "meccanizzazione" del calcolo stesso.

Il linguaggio naturale (*algebra retorica*), con il significato associato a ciascuna parola, maschera il processo di meccanizzazione del calcolo così evidente nel calcolo letterale. Ad esempio, a prescindere dal significato specifico dei simboli, è possibile sostituire $(a + b)^2$ con $a^2 + 2ab + b^2$ e viceversa indipendentemente dai valori attribuiti ad a e b.

Senza la "meccanizzazione" formale delle regole algebriche sarebbe stato probabilmente impossibile giungere ai moderni linguaggi algoritmici basati sulla manipolazione sintattica dei simboli.

4.2. Algoritmi in linguaggio retorico

Nelle primi documenti di carattere matematico mancano perfino le descrizioni degli algoritmi e i procedimenti vengono dati semplicemente mediante esempi numerici.

Nei documenti più antichi (ad esempio relativi alla matematica egizia più antica o a quella sumera) spesso i risultati dei problemi vengono riportati senza neppure indicare la sequenza delle operazioni svolte, per cui risulta difficile ricostruire i procedimenti seguiti.

Solo lentamente si è passati ad una descrizione algoritmica mediante il linguaggio naturale.

Il linguaggio algoritmico basato su esempi numerici

Anche le civiltà più antiche furono capaci di elaborare algoritmi matematici abbastanza complessi e **numerosi documenti testimoniano le capacità matematiche di queste civiltà nel formulare algoritmi** risolutivi in vari campi del sapere contabilità, aritmetica, astronomia, geometria, ecc..

In che modo venivano formulati i procedimenti di calcolo? Qui di seguito vediamo un esempio di problema aritmetico, tratto dal papiro di Mosca.

Problema 6 del papiro di Mosca

"Modo di operare per un rett[ango]lo.
Quando si dà a te un r[ettang]olo di 12 in superficie e ½ + ¼ [cioè ¾] della lunghezza per la larghezza.
Fa tu. Opera su ½ + ¼ per trovare 1 [cioè calcola il numero che moltiplicato per ½ + ¼ dà 1]. Viene 1+1/3.
Opera sul 12, questo che è nella superficie 1+1/3 volte, viene 16.
Fa tu. Calcola la radice quadrata di esso. Ne viene 4 per la lunghezza, 1/2 +1/4 di esso, cioè 3 per la larghezza."

Il problema richiede di calcolare i lati di un rettangolo sapendo che l'area è 12 e che un lato è ¾ (cioè 1/ + ¼) dell'altro.

Nel linguaggio moderno il problema si riduce al sistema

$$\begin{cases} y = (3/4)\, x \\ xy = 12 \end{cases}$$

Il procedimento qui illustrato ci rivela alcuni aspetti tipici di numerosi algoritmi della matematica più antica: **la descrizione del procedimento viene data mediante un esempio numerico operando sulle quantità del problema e limitando al minimo la descrizione testuale del procedimento seguito**. Da notare l'uso esplicito dell'operazione di radice quadrata e l'introduzione di un simbolo apposito per essa.

La mancanza di una notazione simbolica non significa che i procedimenti non vadano intesi comunque come schemi generali, come sottolinea lo stesso Neugebauer,

> ***“Dagli esempi effettivamente calcolati appare evidente che si attribuiva importanza al procedimento generale, e non al risultato numerico.*** **[…]** ***I numeri che accompagnano questi esempi non hanno altra funzione che quella di offrire una guida conveniente per illustrare il processo generale che sta alla base di tutti questi calcoli. E’ dunque erroneo negare all’algebra babilonese l’uso di una “formula generale.”***

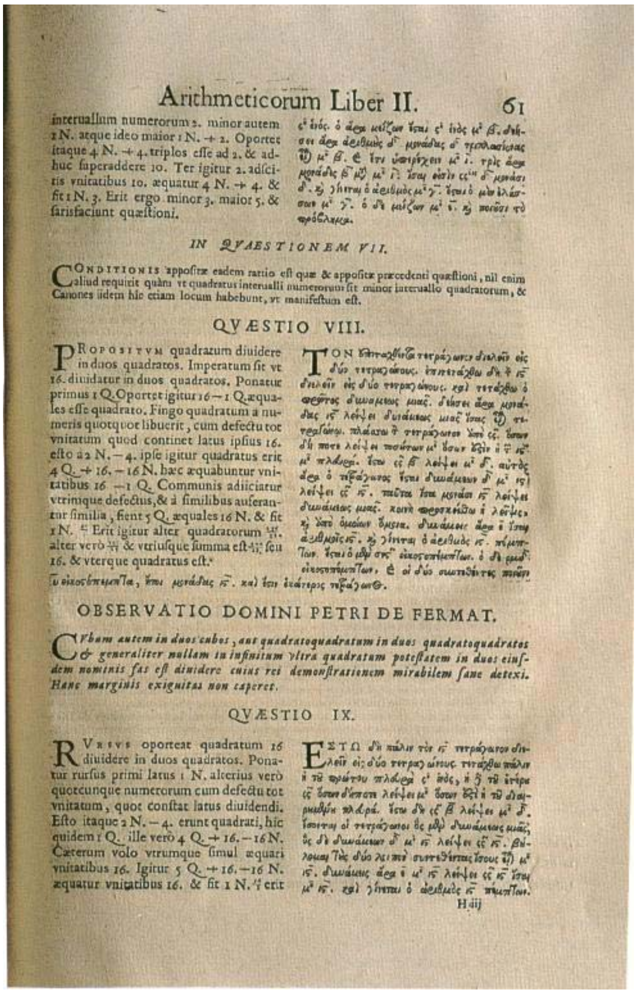
LINK

http://www.math.buffalo.edu/mad/Ancient-Africa/mad_ancient_egypt.html

http://www.dipmat.unipg.it/~bartocci/PIRAM.htm

http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Egyptian_papyri.html

Il linguaggio algoritmico di Diofanto


Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

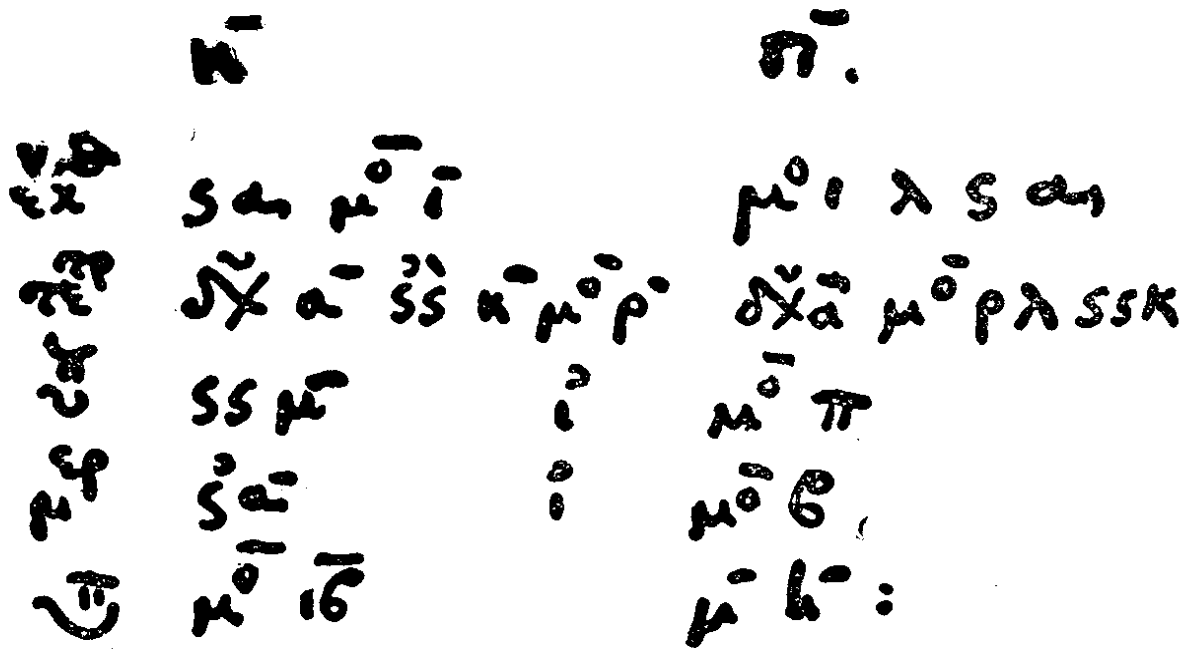
H iij

Fig. Traduzione di Pierre de Fermat dell’opera di Diofanto. (da http://euler.us.es/~libros/griegos.html)

Gran parte della matematica greca di livello più elevato riguarda la geometria mentre manca una trattazione altrettanto sistematica dell’algebra.

Tra i matematici greci che invece si occuparono di problemi di tipo algebrico e tentarono di introdurre un linguaggio più efficace per descrivere problemi algebrici va segnalato il matematico greco Diofanto, vissuto circa tra il 200 d.C. e il 284 d.C.

La sua opera più famosa è l'***Arithmetica***, di cui c'è arrivata solo una parte (10 capitoli su tredici). L'opera non si presenta come una trattazione sistematica dell'algebra, ma presenta una collezione di 150 problemi riguardanti principalmente la risoluzione esatta di equazioni determinate e indeterminate.



Un problema algebrico di Diofanto: Da un manoscritto del sec. XIV. Si tratta di trovare due numeri tali che la loro somma sia = 20, e la differenza dei loro quadrati = 80. I passaggi sono i seguenti:

Siano	$x + 10$	$10 - x$
Quadrati	$x^2 + 20\,x + 100$	$x^2 - 20\,x + 100$
Diff. dei quadrati	$40\,x$	$= 80$
Divisione	x	$= 2$
da cui	$x + 10 = 12$	$10 - x = 8$

Fig. Esempio di scrittura algebrica di Diofanto. (da http://www.dm.uniba.it/ipertesto/indice.doc)

La scrittura di Diofanto, secondo una classificazione dallo storico Nesselmann, costituisce un esempio di ***algebra sincopata***.

Questa notazione, pur essendo prevalentemente basata sull'uso di parole intere, spesso introduce alcune **abbreviazioni**, e singole lettere per denotare le quantità incognite.

Non si tratta ancora di un simbolismo di tipo moderno, ma rappresenta un importante passo in avanti rispetto alla matematica antica, interamente verbale (chiamata pertanto ***algebra retorica***).

Oggi sappiamo anche che non si tratta di un'invenzione completamente nuova di Diofanto dal momento che in un papiro antecedente di un secolo (il ***papiro di Michigan***) sono presenti forme di simbolismo simili a quelle di Diofanto.

All'inizio dell'***Arithmetica*** Diofanto introduce diverse abbreviazioni. Ad esempio, indica l'**incognita** con un simbolo molto simile alla **lettera greca** ζ (stigma o digamma), lettera arcaica addizionale precedente a quella dell'Età classica, forse ad indicare la lettera finale della parola αριθμ**ό**ζ, che significa "numero".

Ecco inoltre come rappresenta le potenze dell'incognita:

x	αριθμόζ ("numero")	ζ
x^2	δύναμις (cioè "potenza")	Δ^Y
x^3	χύβος ("cubo")	K^Y
x^4	δυναμοδύναμις ("potenza-potenza")	$\Delta\,\Delta^Y$
x^5	δυναμόχυβος, ("potenza-cubo")	$\Delta\, K^Y$
x^6	χυβόχυβος	$K\, K^Y$

Altri simboli usati nell'Arithmetica sono:

- **M°**, questo simbolo seguito da un numero indica il termine noto di un'equazione; questa notazione è formata dalle prime due lettere della parola *"monade",* che significa *unità*.
- ↑ è il segno usato per indicare la sottrazione;
- **í$^{\sigma}$** è usato per indicare il segno uguale;
- **έν** indica spesso l'operazione di divisione.

Nessun segno viene usato per l'addizione: la somma di due o più termini viene indicata scrivendo di seguito gli addendi.

Così l'espressione $2x^2 + 3x$, per Diofanto sarebbe stato $\Delta^{Y}\beta\zeta\gamma$ nella quale non viene utilizzato nessun simbolo per l'addizione e i numeri 2 e 3 sono rappresentati rispettivamente da β, γ e seguono il termine letterale.

Un altro esempio di scrittura usata da Diofanto è il seguente:

$\Delta^{Y}\,\bar{\xi}\,\mathring{M}\,\overline{,\beta\phi\kappa}$ ἐν μορίῳ $\Delta^{Y}\Delta\,\bar{\alpha}\,\mathring{M}$ ϡ ⋔ $\Delta^{Y}\,\bar{\xi}$

la cui traduzione nel nostro simbolismo è:

$$(60\,x^2 + 2520) / (x^2 + 900 - 60\,x^2)$$

Fig. Un esempio di quoziente di polinomi, tratto dal Problema XIV del Libro VI dell'Arithmetica di Diofanto.

Vediamo ora come Diofanto descrive il procedimento per risolvere il sistema lineare:

$$\begin{cases} x + y = 100 \\ y - x = 40 \end{cases}$$

Problema:

Che il numero dato sia 100 e che la differenza sia 40 unità. Trovare i numeri.

Soluzione:
Poniamo uguale ad un'incognita il più piccolo numero [x]; il più grande sarà pertanto l'incognita più 40 unità [x + 40]. Ora questa somma sono le 100 unità date, dunque 100 unità sono uguali a due incognite più 40 unità [2x + 40. Sottraiamo le quantità simili dai simili, cioè 40 unità da 100 e, inoltre, 40 unità da 2 incognite più 40 unità. Le due incognite rimaste sono uguali a 60 unità e ciascuna incognita è 30 unità.
Ritorniamo a quello che avevamo posto: il più piccolo numero sarà 30 unità, cosicché il più grande sarà 70 unità e la prova è evidente.

I problemi non sono ancora formulati in modo del tutto generale, ma fanno ancora riferimento a esempi numerici specifici, secondo una pratica che verrà seguita ancora per parecchi secoli.

Non c'è alcun tentativo di sfruttare la notazione sincopata per costruire una teoria organica delle equazioni.

Tra l'altro Diofanto non si preoccupa di fornire tutte le possibili soluzioni dei suoi problemi, ma ne considera sempre una sola.

L'opera e in particolare la notazione di Diofanto rimasero comunque a lungo dimenticati e solo nel 1500-1600 con la riscoperta dei testi classici i matematici europei (tra questi va ricordato Pierre de Fermat) approfondirono e compresero l'importanza del lavoro del grande matematico.

LINK

http://www.math.rutgers.edu/courses/436/436-s00/Papers2000/kirschm.html

http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Diophantus.html

Il linguaggio algoritmico di Brahmagupta

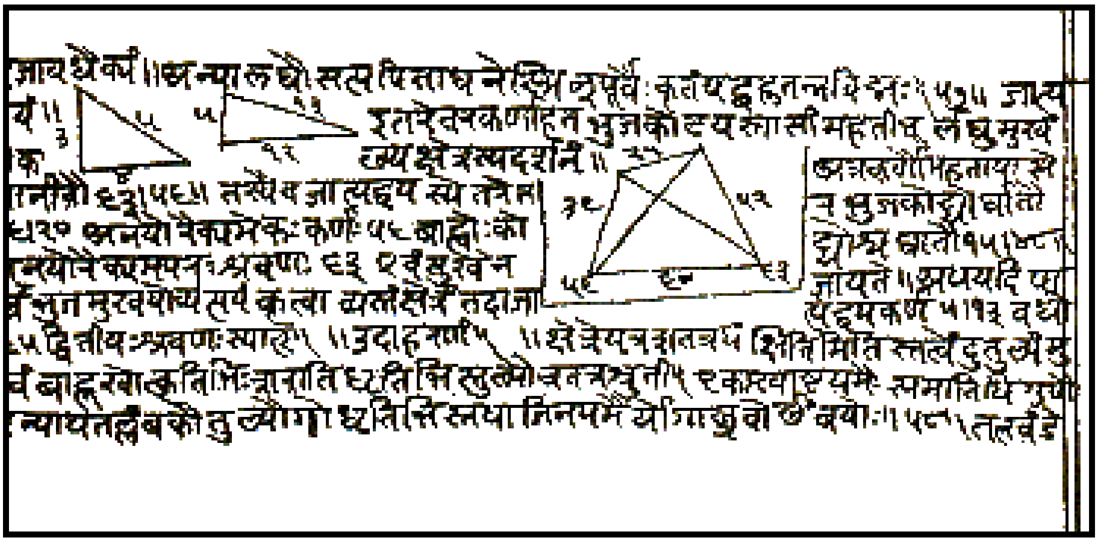


Fig. Frammento di uno scritto di Brahamagupta sulla formula per i quadrilateri ciclici.

Dopo gli enormi progressi della civiltà greca nella matematica, l’Europa visse un lungo periodo di decadenza e il primato delle ricerche matematiche più interessanti si spostò presso altre civiltà.

In particolare, in **India** diversi matematici contribuirono ad introdurre nuove idee matematiche particolarmente interessanti.

Due caratteristiche significative della matematica indiana antica che la distinguono da quella greca furono una **notevole indipendenza dell’algebra dalla geometria** e l’**uso dei simboli**, quali punti (nel manoscritto di Bakhshali) o lettere dell’alfabeto, **per indicare quantità incognite**.

I matematici indiani furono probabilmente i primi a fare un uso sistematico di questo metodo di rappresentazione delle incognite.

Brahmagupta (circa 598-670), una delle figure più importanti della matematica indiana, introdusse i numeri relativi dando le regole corrette per operare con essi. In questa sezione vogliamo vedere in che modo Brahmagupta descrive il procedimento per risolvere un'equazione di 1° grado:

> "***Se quattro volte la dodicesima parte della somma tra uno e l'incognita, aumentato di otto è uguale all'incognita aumentata di uno, dimmi il valore dell'incognita***".

Nella scrittura moderna si tratta dell'equazione

$$4 \cdot \frac{x + 1}{12} + 8 = x + 1$$

Brahmagupta prima costruisce l’equazione che riflette le relazioni descritte nel testo del problema e poi mostra il procedimento risolutivo:

commento	**simbolismo di Brahmagupta**	**notazione moderna**
	ya1 ru1	**(x + 1)**
	ya1 ru1 **12**	**(x + 1)** **--------** **12**
e il quadruplo è	**ya1 ru1** **3**	**(x + 1)** **--------** **3**
aumentato con il numero assoluto otto, si ottiene	**ya1 ru25** **3**	**(x + 25)** **--------** **3**
Dopo aver indicato a parole il secondo membro dell’equazione (x + 1) e “*prendendo il triplo di entrambi*”, Brahmagupta scrive l’intera equazione ponendo i due membri uno sotto l’altro, cioè nella forma:	**ya1 ru25** **ya1 ru1**	**(x + 25 = 3x + 3)**
Riguardo alle incognite, semplificando si ha	**ya2**	**[(3x – x =) 2x]**
e per i termini	**22**	**[(25 – 3 =) 22]**
ottenendo infine il risultato	**11**	**[x = (25 – 3)/(3 – 1)]**

LINK

http://www-history.mcs.st-andrews.ac.uk/Biographies/Brahmagupta.html

Il linguaggio algoritmico di al-Khwarizmi

A partire dal 750 d.C. la civiltà araba diede importanti apporti nel campo della matematica raggiungendo forse il livello più alto a livello mondiale per alcuni secoli.

Di questi contributi forse il più importante riguarda lo **sviluppo dell'algebra** come disciplina autonoma. Il primo matematico a dare una svolta fondamentale a questo settore fu **al-Khwarizmi** (circa 780-850), la cui opera, scritta attorno al 830 d.C., oltre a dare il nome alla disciplina dalla parola '***al-jabr***', contiene la prima importante classificazione delle equazioni mai realizzato prima e di fatto fissa quei procedimenti risolutivi che ancora oggi adottiamo.

Per ricondurre le equazioni di vario tipo ai casi base al-Khwarizmi si serve di tre regole di trasformazione fondamentali che permettono di manipolare e semplificare la struttura dell'equazione:

- **operazione *al-jabr*:** l'equazione $2x^2 = 80x - 3x^2$ viene trasformata in $5x^2 = 80x$;
- **operazione *al-muqabala:*** l'equazione $40 + x^2 = 19 + 10x$ viene trasformata in $21 + x^2 = 10x$.
- **operazione *al-hatt***: l'equazione $42 + 2x^2 = 20x$ viene trasformata in $21 + x^2 = 10x$.

Il limite più importante del lavoro di al-Khwarizmi è costituito invece dalla mancanza di una notazione adeguata per rappresentare le equazioni stesse da manipolare dal momento che egli utilizza unicamente l'algebra retorica.

Qui possiamo vedere in che modo al-Khwarizmi descrive l'equazione e l'algoritmo risolutivo:

Ho diviso dieci in due parti, poi ho moltiplicato ogni parte per se stessa ed* [ho] *preso la somma delle due, che fa cinquattotto dirham*[2]*.	**descrizione problema**
Poni una delle due parti* [uguale] *una cosa e l'altra* [uguale a] *dieci meno una cosa. Moltiplica dieci meno una cosa per se stesso, fa cento più un censo meno 20 cose, poi* [moltiplica] *una cosa per una cosa, fa un censo. Poi addiziona entrambi* [i prodotti]*, fa cento più due censi meno 20 cose,* [il tutto] *equivalente a cinquattotto dirham.	**equazione:** $(10 - x)^2 + x^2 = 58$ $100 + x^2 - 20x + x^2 = 58$ $100 + 2x^2 - 20x = 58$
Restaura il cento più due censi con le venti cosa mancanti e portale ai cinquantotto* [dirham]*, fa allora cento più due censi equivalente a cinquattotto dirham più venti cose.	**operazione *al-jabr*** $100 + 2x^2 = 58 + 20x$
Riporta a un unico censo prendendo la metà di tutto* [ciò] *che hai. Fa cinquanta dirham più un censo equivalente a ventinove dirham più dieci cose.	**operazione *al-hatt*:** $50 + x^2 = 29 + 10x$
Diminuiscilo, cioè sottrai da cinquanta ventinove, rimane ventuno più un censo uguale a dieci cose.	**operazione *al-muqabala*:** $21 + x^2 = 10x$
Dimezza le radici, fa cinque, e moltiplicalo per se stesso, fa venticinque. Sottrai da questo il ventuno legato al censo, rimane quattro. Prendi la sua radice che fa due e sottrai questo dalla metà delle radici, cioè cinque. Rimane tre che è una delle due parti e l'altra è sette.	**formula risolutiva:** $x = 10/2 - \sqrt{[(10/2)^2 - 21]}$
Questo problema ti ha riferito uno dei sei casi, cioè censi più numeri equivalente a radici.	$x^2 + c = bx$

[2] Il dirham è una moneta araba.

Come possiamo vedere si tratta di una descrizione algoritmica puramente retorica non facile da seguire.

LINK

http://www-groups.dcs.st-and.ac.uk/~history/Indexes/Arabs.html

http://logica.rug.ac.be/albrecht/problems.php?code=KAA

Il linguaggio algoritmico di Fibonacci

Se il linguaggio retorico degli arabi del IX o X secolo per trattare problemi algebrici ci può sembrare ancora alquanto primitivo, non dobbiamo dimenticarci che altrove le cose non andavano meglio.

Anche nell'Europa medioevale di quattro secoli più tardi di al-Khwarizmi l'approccio algebrico non era molto diverso, come possiamo vedere esaminando l'opera matematica di Fibonacci, il più grande matematico europeo dell'età medioevale.

Fig. Problemi dal Liber Abaci: la falsa posizione

Per farci un'idea del modo con cui veniva organizzato nell'europa medioevale un algoritmo risolutivo vedremo come esempio un problema algebrico affrontato con il *metodo della falsa posizione,* descritto nel *Liber Abaci,* il testo più famoso di Fibonacci (e della matematica medioevale).

Questo metodo permette di risolvere equazioni di primo grado e non rappresenta una tecnica originale di Fibonacci essendo stato utilizzato fin dall'antichità prima.

Problema dell'albero
C'è un albero, di cui 1/3 e 1/4 stanno sotto terra. Il rimanente, che sta sopra la terra è 21 palmi. Si chiede quale sia la lunghezza dell'albero.

Risoluzione:
Poniamo che l'albero sia 12 palmi, da cui, tolti 1/3 e 1/4 , cioè 7, restano sopra la terra 5 palmi.
Dunque dirai: per 12 che ho posto, viene 5; cosa devo porre perché venga 21?
Moltiplica allora gli estremi, cioè 12 per 21, e dividi per il medio 5; verrà 50 e 2/5.

Fig. Un problema del Liber Abaci risolto mediante il metodo semplice della falsa posizione.

Come possiamo osservare tutta la descrizione del procedimento viene data in forma retorica e manca un qualunque formalismo simbolico per rappresentare in forma generale le quantità numeriche trattate.

Il metodo viene denominato della **falsa posizione** perché invece di tradurre il problema usando un'incognita e un'equazione come siamo abituati oggi, si procede con un valore ipotetico non corretto, scelto arbitrariamente, e si opera su di esso secondo le condizioni espresse nel problema e poi si corregge il valore iniziale mediante una proporzione (applicando, ad esempio, la regola del tre semplice).

Il vantaggio di questo metodo è quello di sopperire alla mancanza di formalismo simbolico che permette di costruire un'equazione su cui è possibile fare operazioni algoritmiche per risolvere il problema dato. Il metodo della falsa posizione è invece un algoritmo che manipola direttamente le quantità numeriche del problema.

A noi oggi le tecniche (trasformazioni) algebriche appaiono tanto semplici e naturali, ma bisogna osservare che in realtà le trasformazioni algebriche operate risultano semplici nella notazione simbolica e quando espresse nell'algebra retorica non sono più così immediate e semplici anche perché finiscono per alterare la struttura risolutiva associata al problema.

Questa difficoltà concettuale ha portato ad utilizzare la regola della falsa posizione in Europa per tutto il medioevo (e oltre) anche quando le tecniche algebriche arabe erano già note.

LINK

http://www2.math.unifi.it/~archimede/archimede/fibonacci/immagini_mostra/virtuale.php

http://it.wikipedia.org/wiki/Metodo_di_falsa_posizione_in_Fibonacci

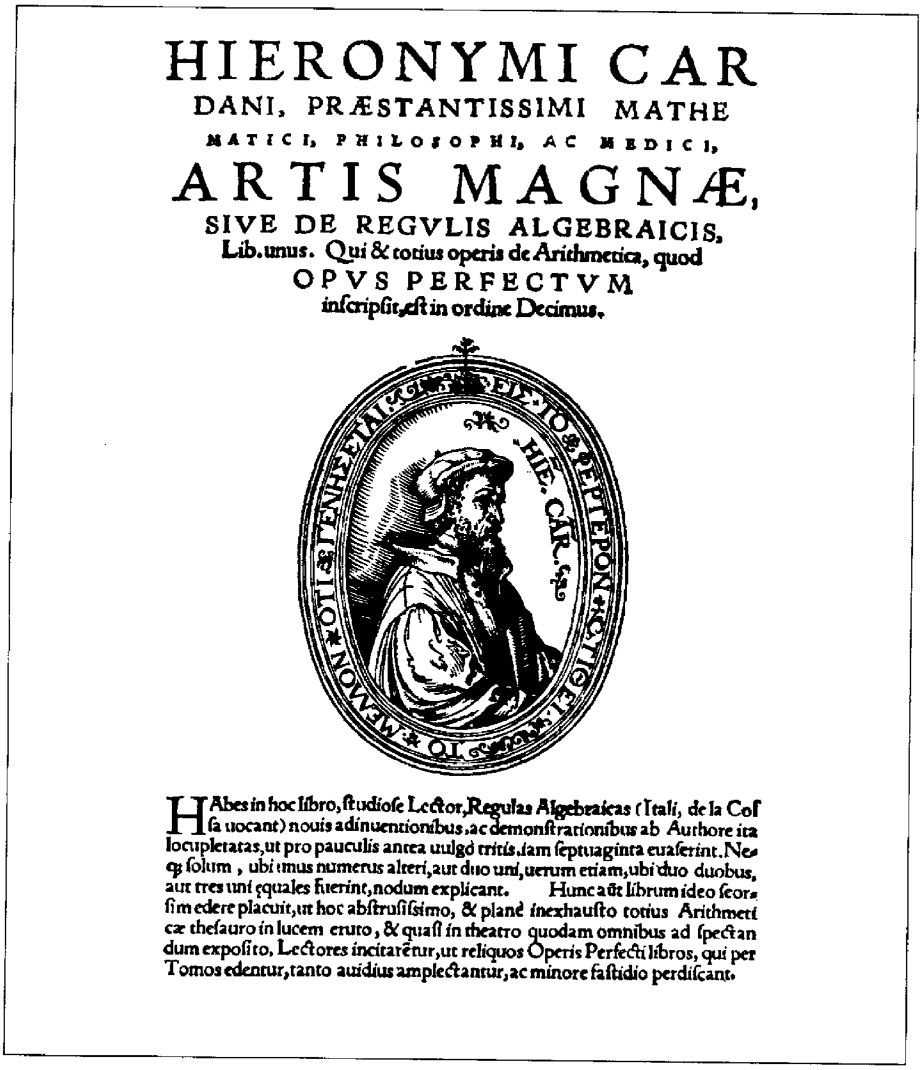
http://logica.rug.ac.be/albrecht/problems.php?code=FLA

Tartaglia e le equazioni di terzo grado

Fig. Niccolò Fontana, detto Tartaglia (1499-1557).

Per tutto il medioevo la matematica europea non fece particolare progressi rispetto a quanto erano riusciti a raggiungere gli antichi greci. **Il primo risultato importante arrivò solo nel 1500 con la risoluzione (generale) delle equazioni di 3° grado grazie agli algebristi italiani.** I principali nomi legati a questa scoperta sono Scipione Dal Ferro, Niccolò Fontana e Antonio Maria Fior, Gerolamo Cardano e Ludovico Ferrari.

Nel 1545 la formula dell'equazione di terzo grado (insieme a quella di quarto grado, ricavata nel frattempo da Ludovico Ferrari) divenne di pubblico dominio poiché venne presentata nel libro ***Ars magna* di Gerolamo Cardano**.



HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cossa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Neque solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aūt librum ideo seorsim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum exposito, Lectores incitarētur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

Fig. Frontespizio dell'Ars Magna di Gerolamo Cardano.

Descrizione di Tartaglia del metodo risolutivo:

Quando chel cubo con le cose appresso
Se agguaglia à qualche numero discreto
Trouan dui altri differenti in esso.
Dapoi terrai questo per consueto
Che'l lor produtto sempre sia eguale
Al terzo cubo delle cose neto,
El residuo poi suo generale
Delli lor lati cubi ben sottratti
Varra la tua cosa principale.
In el secondo de cotesti atti
Quando che'l cubo restasse lui solo
Tu osseruarai quest'altri contratti,
Del numer farai due tal part'à uolo
Che l'una in l'altra si produca schietto
El terzo cubo delle cose in stolo
Delle qual poi, per commun precetto
Torrai li lati cubi insieme gionti
Et cotal somma sara il tuo concetto.
El terzo poi de questi nostri conti
Se solue col secondo se ben guardi
Che per natura son quasi congionti.
Questi trouai, & non con passi tardi
Nel mille cinquecente, quatro e trenta
Con fondamenti ben sald'è gagliardi
Nella citta dal mar'intorno centa.

Fig. L'algoritmo di risoluzione dell'equazione di 3° grado in versi data da Tartaglia.

Nella notazione moderna:

per l’equazione $\boxed{y^3 + py + q = 0.}$

si ha la formula risolutiva

$$\boxed{y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},}$$

4.3. Il calcolo simbolico

La conquista del calcolo simbolico fu una tappa fondamentale non solo per la matematica ma anche per la storia degli algoritmi per varie ragioni:

- l'algebra simbolica consente di formulare i algoritmi in forma generale e non più legati ad esempi specifici;
- l'algebra simbolica permette di vedere più facilmente la similitudine tra problemi apparentemente lontani e diversi;
- l'algebra simbolica permette di evitare in certi casi problemi di ambiguità tipici del linguaggio naturale;
- l'algebra simbolica mette a disposizione uno strumento fondamentale per "astrarre" rispetto ai problemi concreti; ad esempio, storicamente si è passati dai problemi alle equazioni, dalle equazione numeriche alle equazioni parametriche e così via fino a percorrere strade sempre più astratte impensabili con i metodi più tradizionali;
- l'algebra simbolica permette di attribuire più facilmente particolari interpretazioni ad una struttura simbolica: si pensi alla geometria analitica in cui ad un'equazione (simbolica) viene associata una curva.
- l'algebra simbolica aiuta ad evidenziare regole sintattiche per manipolare i dati del problema indipendentemente dalla semantica specifica.

La conquista del moderno linguaggio simbolico avvenne tra il 1500 e il 1600 e rappresentò un passo formidabile per la storia della matematica e indirettamente per quella degli algoritmi.

E’ bene ricordare che alla diffusione di una moderna notazione matematica contribuì certamente l’**invenzione della stampa** (Gutenberg, 1455) che, oltre a diffondere sempre di più le opere in tutto il continente europeo, contribuì anche a standardizzare le notazioni.

Verso il calcolo simbolico

Probabilmente lo stimolo più importante per sviluppare il linguaggio simbolico fu lo studio sempre più sistematico delle equazioni e, successivamente, l’invenzione del calcolo infinitesimale: senza un’adeguata scrittura è difficile pensare che certi risultati sarebbero stati ottenuti.

Tra il 1500 e il 1600 in Europa avvenne il passaggio tra l’algebra retorica e quella simbolica passando attraverso l’algebra sincopata.

Nel suo testo più famoso del 1484, il *Triparty*, **Chuquet** scriveva ancora

8^3 multiplié par 7^{1m} monte 56^2

per indicare nel linguaggio algebrico moderno l’equazione

$$8x^3 \cdot 7x^{-1} = 56x^2$$

Inizia comunque il passaggio dall’algebra “retorica”, in cui le diverse operazioni sono descritte in linguaggio naturale, a quella “sincopata”, in cui i termini del linguaggio naturale appaiono abbreviati.

I frate e matematico Luca Pacioli nel suo testo più noto, *Summa de aritmetica, geometria, proporzioni et proporzionalità*, del 1494 scrive l'equazione $x + x^2 = 12$ in notazione sincopata

Trouame 1.n°. che gioto al suo qdrat° facia .12

Ancora nel 1545, nell'*Ars Magna* di Gerolamo Cardano l'equazione $x^2 = 4x + 32$ viene scritta in forma sincopata come

qdratu aeqtur 4 rebus p:32

Comunque nessuno di questi matematici capì in modo pieno e profondo l'importanza dell'algebra simbolica e l'uso di linguaggio rimase solo occasionale.

Il passo decisivo, questa volta consapevole delle potenzialità della notazione simbolica, venne invece compiuto dal matematico francese Francois Viete verso la fine del 1550.

 LINK

http://archimedes.mpiwg-berlin.mpg.de/cgi-bin/toc/toc.cgi?dir=pacio_summ2_X02_it_1494;step=thumb

I moderni simboli delle operazioni

Un passo intermedio importante verso il linguaggio simbolico dell’algebra è rappresentato dall’introduzione dei simboli per indicare le operazioni aritmetiche più comuni.

Questo processo avvenne tra la fine del 1400 e per tutto il 1500 e, precedette pertanto di poco l’introduzione dell’algebra simbolica stessa.

Per molto tempo l’**operazione di somma** è stata indicata con la parola latina ‘et’. Il simboli “più” (+) e “meno” (–) comparvero per la prima volta in nel testo *Behende und hüpsche Rechenung auff allen Kauffmanschafft*, di Johannes Widmann (nato c. 1460), pubblicato a Lipsia nel 1489.

I due simboli passarono poi dalla Germania a tutta l’Europa e nel corso del 1500 il loro uso divenne sempre più frequente nei testi dei matematici.

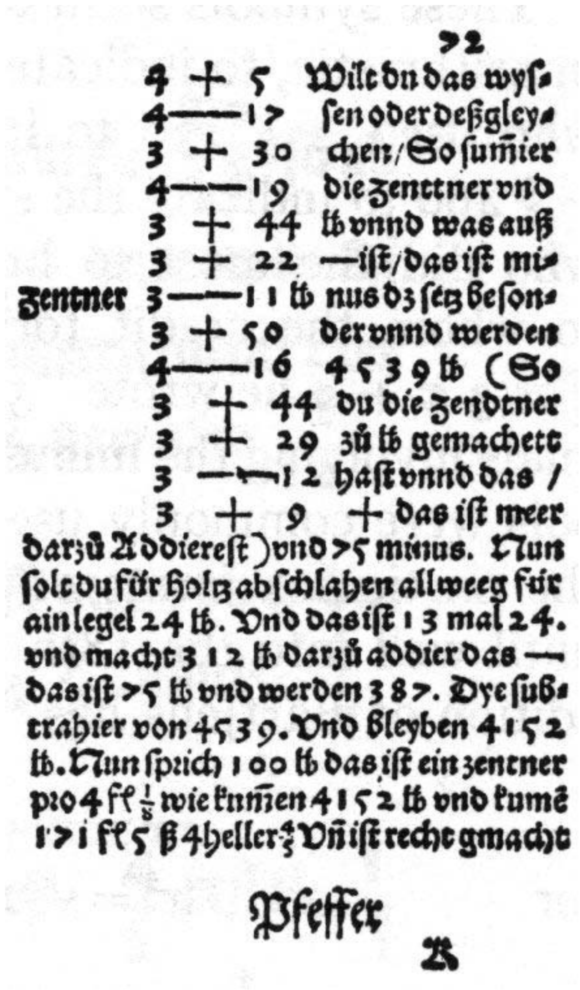

72
4 + 5 Wilt du das wys-
4 — 17 sen oder deßgley-
3 + 30 chen/So sumier
4 — 19 die zentner vnd
3 + 44 lb vnnd was auß
3 + 22 —ist/das ist mi-
zentner 3 — 11 lb nus dz setz beson-
3 + 50 der vnnd werden
4 — 16 4539 lb (So
3 + 44 du die zendtner
3 + 29 zů lb gemachett
3 — 12 hast vnnd das /
3 + 9 + das ist meer
darzů Addierest) vnd 75 minus. Nun
solt du für Holtz abschlahen allweeg für
ain legel 24 lb. Vnd das ist 13 mal 24.
vnd macht 312 lb darzů addier das —
das ist 75 lb vnd werden 387. Dye sub-
trahier von 4539. Vnd bleyben 4152
lb. Nun sprich 100 lb das ist ein zentner
pro 4 fl $\frac{1}{8}$ wie kumen 4152 lb vnd kumē
171 fl 5 ß 4 heller Vñ ist recht gmacht
Pfeffer
R

Fig. Here is an image of the first use in print of the + and - signs, from Widman's *Behennde vnd hüpsche Rechnung.* This image is taken from the Augsburg edition of 1526.

Il **simbolo della moltiplicazione** nella forma ‘×’ fu utilizzato per primo da William Oughtred (1574-1660) nell’opera *Clavis Mathematicae*, pubblicata a Londra nel 1631.

Successivamente Leibniz (1646-1716) propose di sostituire il simbolo ‘×’ con il punto ‘ · ‘ per evitare ambiguità con l’incognita **x**.

Secondo alcuni studiosi, l'uso del punto era stato anticipato da Johann Bernoulli stesso in una precedente lettera del 1694.

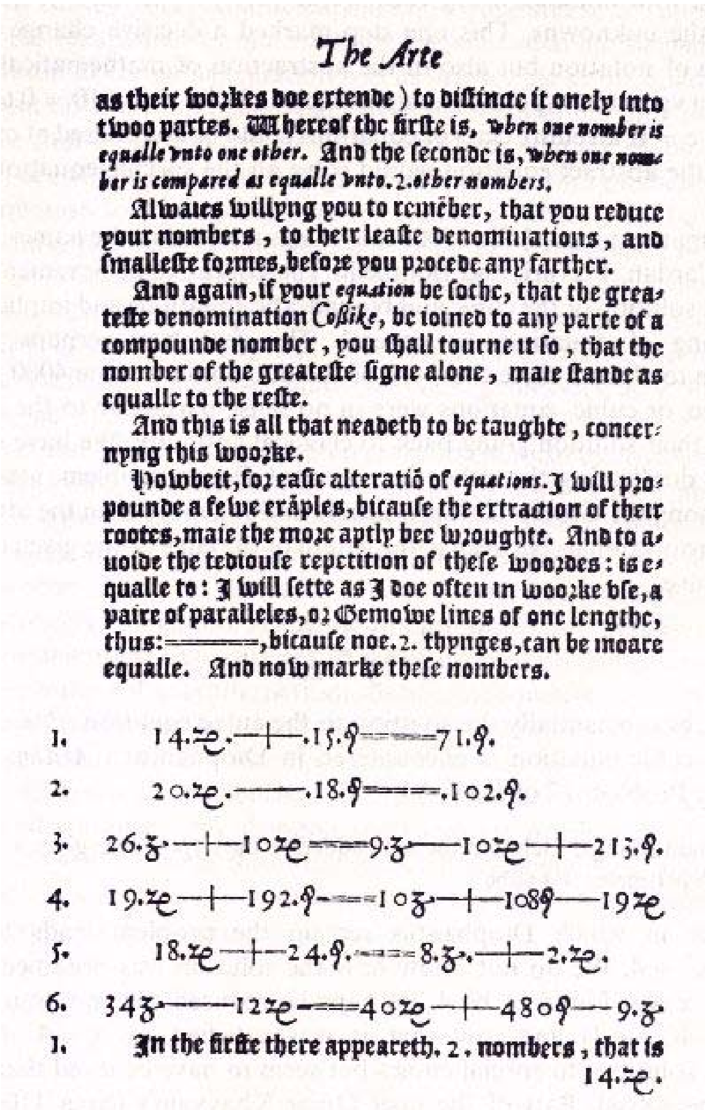
Per la **divisione il simbolo** '**:**' viene usato per la prima volta nel 1633 in un testo intitolato *Johnson Arithmetik; In two Bookes*, ma il simbolo veniva usato solo per le frazioni al posto dell'odierna linea di frazione. Gottfried Wilhelm Leibniz (1646-1716) utilizzò questo simbolo nel 1684 in *Acta eruditorum* per indicare sia le frazioni che la divisione.

Vediamo ora l'uso delle **potenze**. **Nicola Oresme** (c. 1323-1382) utilizzava i numeri per indicare le potenze, ma non nella forma attuale come apice. Nicolas Chuquet (1445?-1500?) utilizzò gli esponenti nella forma di apice nel suo testo *Le Triparty en la Science des Nombres* del 1484, la scrittura 12^3 significava $12x^3$. Cartesio scriveva *aaaa* per indicare a^4. Altri autori accennano a esponenti frazionari, ma questi furono usati sistematicamente solo a partire dai lavori di Isaac Newton (dopo il 1676).

Il simbolo di **radice quadrata** ℞ fu utilizzato da Fibonacci nel 1220 in *Practica geometriae*. Nel 1525 nel testo *Die Coss* di Christoff Rudolff (1499-1545) compare il simbolo di radice quadrata √; egli non utilizzò però gli indici per indicare altri radicali. L'uso dell'indice per indicare radici di vario genere fu suggerito nel 1629 da Albert Girard (1595-1632) nel testo *Invention nouvelle.*

Per molto tempo l’uguaglianza veniva indicata con parole come *est, aequales, aequantur, esgale, faciunt, ghelijck,* o *gleich, aeq*. Ancora nel 1500 l’uguaglianza 2 + 3 = 5 si scriveva ‘*2 plus 3 qequalis 5’*.

Il simbolo **uguale** ‘**=**’ fu usato per la prima volta[3] da Robert Recorde (c. 1510-1558) nel 1557 in *The Whetstone of Witte*.



The Arte

as their workes doe extende) to distincte it onely into twoo partes. Whereof the firste is, *when one nomber is equalle unto one other.* And the seconde is, *when one nomber is compared as equalle unto.2.other nombers.*

Alwaies willyng you to remẽber, that you reduce your nombers, to their leaste denominations, and smalleste formes, before you procede any farther.

And again, if your *equation* be soche, that the greateste denomination *Cosike*, be ioined to any parte of a compounde nomber, you shall tourne it so, that the nomber of the greateste signe alone, maie stande as equalle to the reste.

And this is all that neadeth to be taughte, concernyng this worke.

Howbeit, for easie alteratiõ of *equations*. I will propounde a fewe exãples, bicause the extraction of their rootes, maie the more aptly bee wroughte. And to auoide the tediouse repetition of these woordes: is equalle to: I will sette as I doe often in woorke use, a paire of paralleles, or Gemowe lines of one lengthe, thus: =====, bicause noe.2. thynges, can be moare equalle. And now marke these nombers.

1. 14.ze.—+—.15.℈=====71.℈.
2. 20.ze.———.18.℈=====.102.℈.
3. 26.ʒ.—+—10ze=====9.ʒ.——10ze—+—213.℈.
4. 19.ze—+—192.℈=====10ʒ.—+—108℈——19ze
5. 18.ze—+—24.℈.=====8.ʒ.—+—2.ze.
6. 34ʒ.———12ze=====40ze—+—480℈——9.ʒ.

1. In the firste there appeareth.2. nombers, that is 14.ze.

Fig. Here is an image of the page of *The Whetstone of Witte* on which the equal sign is introduced.

[3] Maracchia (pag 176) sottolinea che tale simbolo era stato già usato da Bombelli nel 1550.

Il simbolo si diffuse però solo grazie ai lavori dei matematici **Thomas Harriot** e **William Oughtred**.

Infine i simboli minore e maggiore ‘**<**’ e ‘**>**’ compaiono per la prima volta in *Artis Analyticae Praxis ad Aequationes Algebraicas Resolvendas* di **Thomas Harriot** (1560-1621), pubblicato postumo nel 1631.

LINK

http://members.aol.com/jeff570/operation.html

http://members.aol.com/jeff570/relation.html

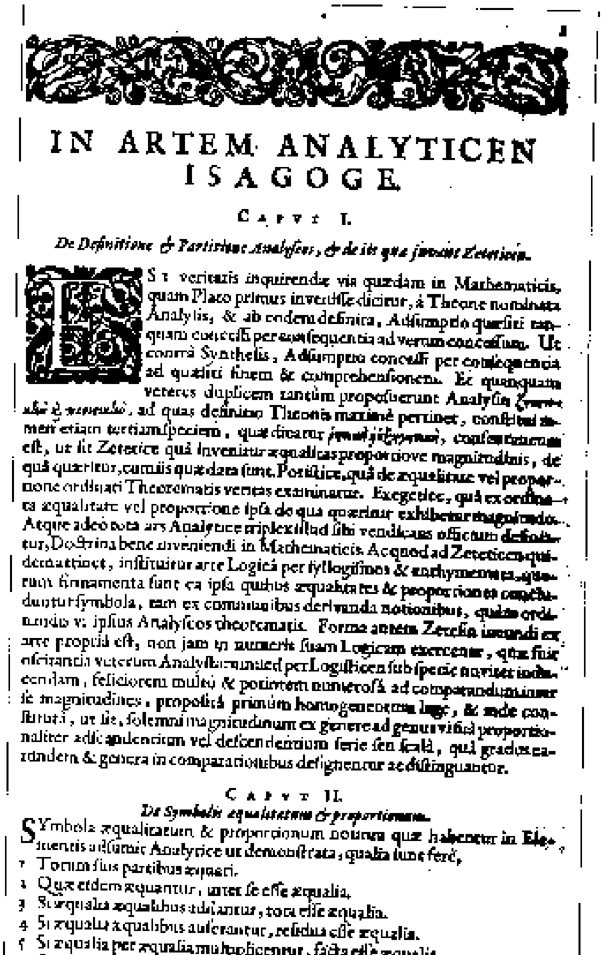
http://www.roma.unisa.edu.au/07305/symbols.htm

http://www.stephenwolfram.com/publications/talks/mathml/mathml2.html

http://math.unipa.it/~grim/mathnotation.pdf

Da Viete alla notazione simbolica moderna

Tra i personaggi che maggiormente contribuirono all'introduzione del linguaggio simbolico va ricordato il matematico francese **Francois Viete** (1540 - 1603), che introdusse una notazione innovativa per le equazione. In Viete le trasformazioni algebriche, che noi oggi adottiamo per trasformare e semplificare le equazioni diventano "una forma di ragionamento e non più un insieme di ingegnosi artifici, come l'aveva concepita Diofanto".



IN ARTEM ANALYTICEN ISAGOGE.

CAPVT I.

De Definitione & Partitione Analyseos, & de iis quæ juvant Zeteticen.

EST veritatis inquirendæ via quædam in Mathematicis, quam Plato primus invenisse dicitur, à Theone nominata Analysis, & ab eodem definita, Adsumptio quæsiti tanquam concessi per consequentia ad verum concessum. Ut contrà Synthesis, Adsumptio concessi per consequentia ad quæsiti finem & comprehensionem. Et quanquam veteres duplicem tantùm proposuerunt Analysin [illegible], ad quas definitio Theonis maximè pertinet, constitui tamen etiam tertiam speciem, quæ dicatur [illegible], consentaneum est, ut sit Zetetice quâ invenitur æqualitas proportiove magnitudinis, de quâ quæritur, cum iis quæ data sunt. Poristice, quâ de æqualitate vel proportione ordinati Theorematis veritas examinatur. Exegetice, quâ ex ordinata æqualitate vel proportione ipsa de qua quæritur exhibetur magnitudo. Atque adeò tota ars Analytice triplex illud sibi vendicans officium definiatur, Doctrina bene inveniendi in Mathematicis. Ac quod ad Zeteticen quidem attinet, instituitur arte Logicâ per syllogismos & enthymemata, quorum firmamenta sunt ea ipsa quibus æqualitates & proportiones concluduntur symbola, tam ex communibus derivanda notionibus, quàm ordinandis vi ipsius Analyseos theorematis. Forma autem Zetesin ineundi ex arte propria est, non jam in numeris suam Logicam exercente, quæ fuit oscitantia veterum Analystarum: sed per Logisticen sub specie noviter inducendam, feliciorem multò & potiorem numerosâ ad comparandum inter se magnitudines, propositâ primùm homogeneorum lege, & inde constitutâ, ut fit, solemni magnitudinum ex genere ad genus vi suâ proportionaliter adscendentium vel descendentium serie seu scalâ, quâ gradus earundem & genera in comparationibus designentur ac distinguantur.

CAPVT II.

De Symbolis æqualitatum & proportionum.

SYmbola æqualitatum & proportionum notiora quæ habentur in Elementis adsumit Analytice ut demonstrata, qualia sunt ferè,

1 Totum suis partibus æquari.
2 Quæ eidem æquantur, inter se esse æqualia.
3 Si æqualia æqualibus adiiciantur, tota esse æqualia.
4 Si æqualia æqualibus auferantur, residua esse æqualia.
5 Si æqualia per æqualia multiplicentur, facta esse æqualia.
6 Si æqualia per æqualia dividantur, orta esse æqualia.

A

Fig. Isagoge in Artem Analyticem di Viete.

Con la sua notazione simbolica, che compare per la prima volta nel trattato ***Isagoge in Artem Analyticem*** (pubblicato nel 1591), egli si propone di introdurre un linguaggio matematico generale indipendente dagli esempi numerici fino ad allora usati.

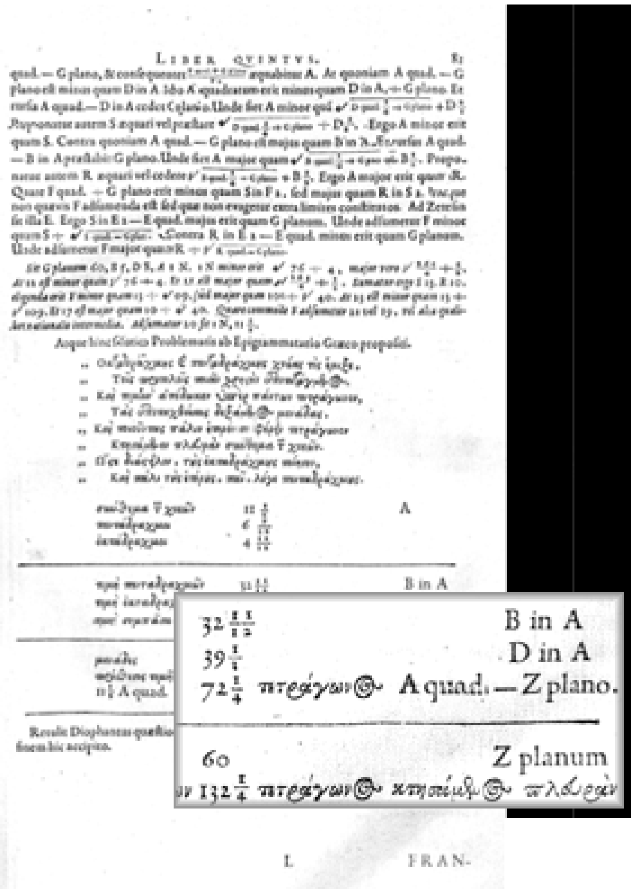
Egli chiamava la sua algebra simbolica *logistica speciosa* in contrapposizione con la *logistica numerosa*, che serviva per trattare i numeri.

Nella sua opera egli utilizzò sistematicamente lettere per indicare le incognite (in particolare le vocali), ma egli non si fermò solo a questo aspetto; infatti, procedette anche ad usare lettere (più precisamente, consonanti) per indicare parametri o coefficienti da considerarsi comunque quantità note.

Per le operazioni invece continuò ad usare le parole per non confonderle con le quantità note o incognite. Ad esempio, un'equazione a parametri come

B in A aequantur A quad. + Z quad.

significava $bx = x^2 + z^2$. Questo tipo di scrittura gli permise comunque di studiare in modo generale intere classi di equazioni.



LIBER QVINTVS.

32 $\frac{11}{12}$ B in A
39 $\frac{1}{4}$ D in A
72 $\frac{1}{4}$ πτεράγωνος A quad. — Z plano.

60 Z planum

Fig. La notazione algebrica di Viete. (da http://www.lindahall.org/events_exhib/exhibit/exhibits/y1k/numbers2.shtml)

A partire da Viete, le lettere furono sempre più di frequente utilizzate per indicare nella matematica.

Naturalmente, il passaggio ad una notazione simbolica non fu compiuto tutto da Viete.

Fig. Francois Viete. (da http://www-

Anche Cartesio diede importanti contributi all'algebra simbolica.

Nell'inventare notazioni si distinse molto di più **Leibniz**, il quale introdusse vari simboli ancora oggi in uso. Leibniz era infatti convinto che una buona notazione fosse fondamentale per fare progredire la matematica stessa. In questa direzione si spinse perfino ad immaginare un linguaggio logico universale con cui poter affrontare in modo inconfutabile tutti i ragionamenti. La sua notazione più famosa riguarda l'operatore integrale: dopo aver utilizzato il simbolo "*omn.*" probabilmente come contrazione della parola latina *omnium*, nel 1675 introdusse il simbolo ∫:

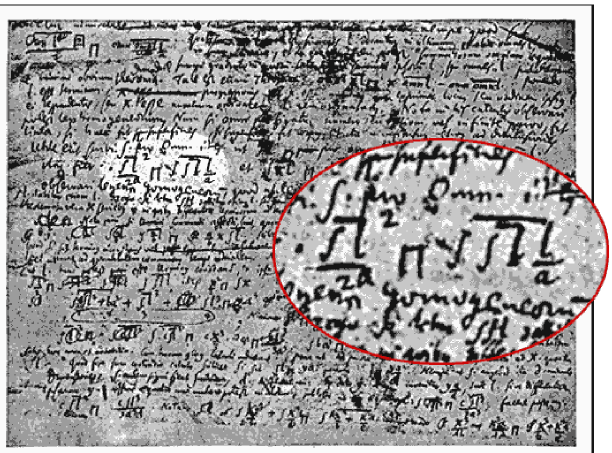


FIG. 124.—Facsimile of manuscript of Leibniz, dated Oct. 29, 1675, in which his sign of integration first appears. (Taken from C. I. Gerhardt's *Briefwechsel von G. W. Leibniz mit Mathematikern* [1899].)

Nel 1700, **Eulero**, seguendo le orme di Leibniz, innovò ulteriormente la notazione matematica. Egli cominciò ad utilizzare in modo sistematico le lettere romane e greche per le variabili e la notazione usata nei suoi testi ci appare molto vicino a quello in uso oggi.

forma generalis autem sumendo $m = 3n$ praebet

$$\frac{\int dx\left(l\frac{1}{x}\right)^{n-1}\cdot\int dx\left(l\frac{1}{x}\right)^{3n-1}}{\int dx\left(l\frac{1}{x}\right)^{4n-1}} = k\int\frac{x^{3nk-1}dx}{(1-x^k)^{1-n}},$$

quibus coniungendis adipiscimur

$$\frac{\left(\int dx\left(l\frac{1}{x}\right)^{n-1}\right)^4}{\int dx\left(l\frac{1}{x}\right)^{4n-1}} = k^3\int\frac{x^{nk-1}dx}{(1-x^k)^{1-n}}\cdot\int\frac{x^{2nk-1}dx}{(1-x^k)^{1-n}}\cdot\int\frac{x^{3nk-1}dx}{(1-x^k)^{1-n}}.$$

Sit nunc $n = \frac{i}{4}$ et sumatur $k = 4$ fietque

$$\frac{\int dx\left(l\frac{1}{x}\right)^{\frac{i}{4}-1}}{\sqrt[4]{1\cdot 2\cdot 3\cdots(i-1)}} = \sqrt[4]{4^3}\int\frac{x^{i-1}dx}{\sqrt[4]{(1-x^4)^{4-i}}}\cdot\int\frac{x^{2i-1}dx}{\sqrt[4]{(1-x^4)^{4-i}}}\cdot\int\frac{x^{3i-1}dx}{\sqrt[4]{(1-x^4)^{4-i}}}.$$

COROLLARIUM 1

35. Si igitur sit $i = 1$, habebimus

$$\int dx\sqrt[4]{\left(l\frac{1}{x}\right)^{-3}} = \sqrt[4]{4^3}\int\frac{dx}{\sqrt[4]{(1-x^4)^3}}\cdot\int\frac{xdx}{\sqrt[4]{(1-x^4)^3}}\cdot\int\frac{xxdx}{\sqrt[4]{(1-x^4)^3}};$$

quae expressio si littera P designetur, erit in genere

$$\int dx\sqrt[4]{\left(l\frac{1}{x}\right)^{4n-3}} = \frac{1}{4}\cdot\frac{5}{4}\cdot\frac{9}{4}\cdots\frac{4n-3}{4}P.$$

COROLLARIUM 2

36. Pro altero casu principali sumamus $i = 3$ eritque

$$\int dx\sqrt[4]{\left(l\frac{1}{x}\right)^{-1}} = \sqrt[4]{2\cdot 4^3}\int\frac{x^2dx}{\sqrt[4]{(1-x^4)}}\cdot\int\frac{x^5dx}{\sqrt[4]{(1-x^4)}}\cdot\int\frac{x^8dx}{\sqrt[4]{(1-x^4)}}$$

seu facta reductione ad simpliciores formas

$$\int dx\sqrt[4]{\left(l\frac{1}{x}\right)^{-1}} = \sqrt[4]{8}\int\frac{xxdx}{\sqrt[4]{(1-x^4)}}\cdot\int\frac{xdx}{\sqrt[4]{(1-x^4)}}\cdot\int\frac{dx}{\sqrt[4]{(1-x^4)}};$$

L'importanza e la notevole diffusione delle opere di Eulero contribuì a divulgare e a standardizzare la notazione matematica, ormai praticamente identica a quella oggi in uso. A questo punto le differenze tra la notazione del tempo e quella adottata oggi divennero sempre più piccole e le opere dei matematici ci appaiono molto simili a quelle moderne.

LINK

http://www.stephenwolfram.com/publications/talks/mathml/mathml2.html

5. Dai fondamenti della matematica alla teoria della computabilità

Paolo Giangrandi
paolo.giangrandi@dimi.uniud.it

Università degli Studi di Udine

13/05/2008

5.1. Introduzione

Per molti secoli, i calcolatori furono considerati solo come strumenti di calcolo e lo **studio** di queste macchine fu unicamente di tipo **tecnologico-ingegneristico**.

Contrariamente a quanto si può pensare, **le ragioni che portarono i matematici a studiare dal punto di vista teorico il concetto di "calcolo meccanico" e di algoritmo non scaturirono dal lavoro sperimentale sui calcolatori (meccanici), ma dallo studio della logica matematica**.

Questi studi teorici non ebbero inizio per puro caso, ma scaturirono da un trentennio di ricerche sui **fondamenti della matematica**, sul ruolo dell'infinito in matematica e sugli stessi processi logici da cui derivano nuove conoscenze matematiche.

Negli **anni '30** un piccolo gruppo di matematici cominciò a mettere a fuoco la natura matematica del processo di calcolo:

- **si può "meccanizzare" il ragionamento logico?**
- **cosa è una procedura di calcolo**?
- **si può realizzare uno strumento di calcolo universale**?
- **quali sono i limiti intrinseci di una macchina per calcolare**?

Queste e altre domande, fino ad allora ignorate, portarono alla definizione dei fondamenti teorici della computabilità.

Il maggiore pioniere di questo studio sul calcolo automatico fu probabilmente il matematico inglese **Alan Turing**.

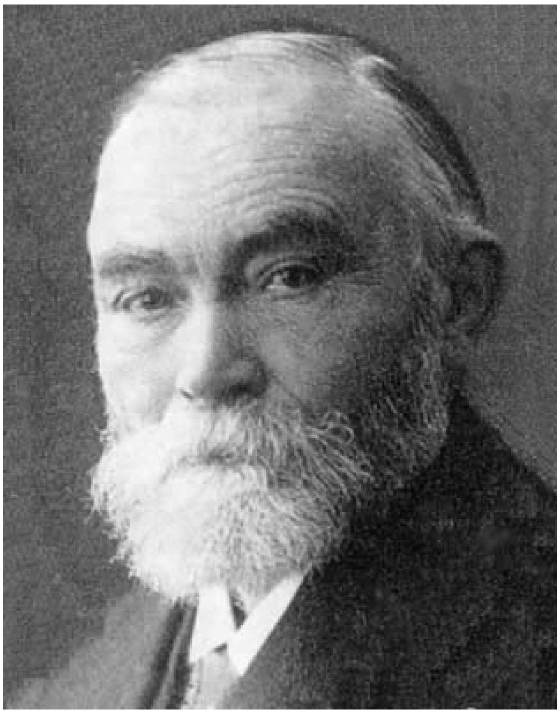
5.2. Alla ricerca dei fondamenti della matematica

Bernhard Bolzano (1781- 1848): Paradossi dell'Infinito

Karl Weierstrass (1815-1897): la nozione di limite

Richard Dedekind (1831-1916): i numeri reali

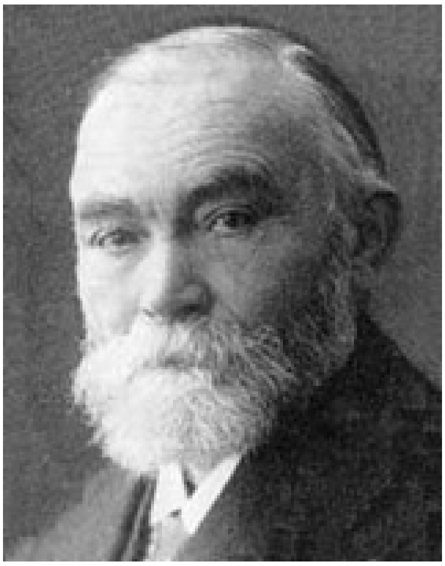
George Cantor (1845-1918): il primo studio rigoroso sugli infiniti



Gottlob Frege (1848-1925): la nascita della logica moderna

David Hilbert (1862-1943): programma di costruzione dei fondamenti della matematica

L'ideografia di Frege

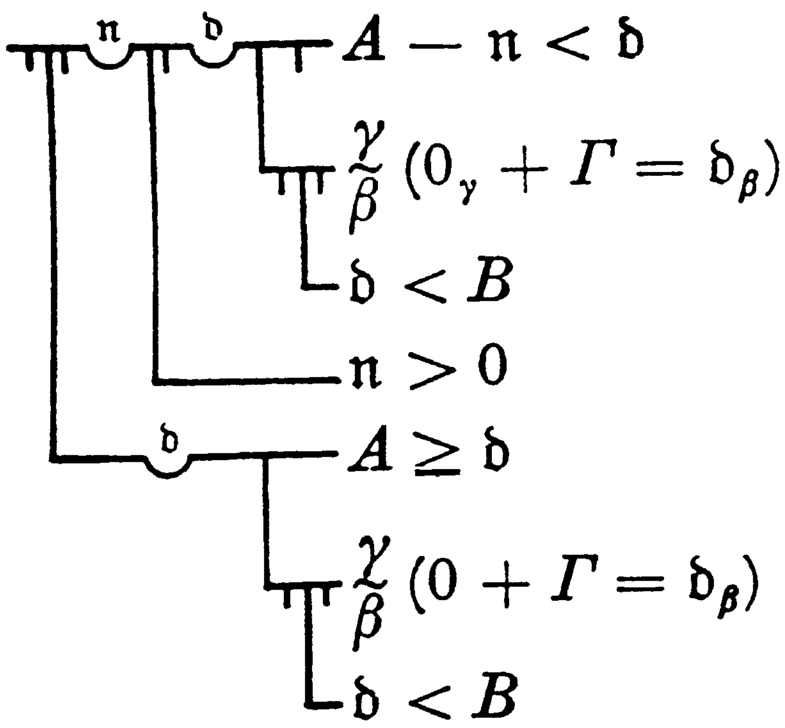


Gottlob Frege (1848 - 1925) è considerato il fondatore della logica matematica moderna.

Frege era rimasto affascinato dall'idea leibniziana di un **calculus philosophicus**, che il grande filosofo tedesco aveva descritto due secoli. E proprio seguendo il sogno leibniziano di un **linguaggio universale cercò di costruire un linguaggio rigoroso, «in formule di pensiero puro», che permettesse il «calcolo logico»** e che potesse costituirsi come fondamento di tutti i calcoli particolari e specifici delle varie scienze (aritmetici, geometrici, ecc).

Rispetto al lavoro di Boole, limitato allo studio calcolo proposizionale, egli raffinò ed estese il sistema considerando anche predicati, funzioni e quantificatori: di fatto introdusse quello che oggi è noto come **calcolo dei predicati del secondo ordine**.

Frege denominò il proprio sistema ***Ideografia*** (*Begriffsschrift)* e lo descrisse in un'opera pubblicata per la prima volta nel 1879.



Frege aveva creato quella **characteristica universalis**

- che sarebbe diventato un misto di formule algebriche e ideogrammi e, inoltre,
- mostrò che era possibile superare i confini della logica proposizionale e sillogistica, dai quali neppure Boole era uscito, sviluppando un sistema di assiomi e regole per la logica predicativa.

Nel 1884 Frege scrisse ***I Fondamenti dell'Aritmetica***, in cui forniva una prima formalizzazione dell'aritmetica.

I due volumi dei ***Principi dell'Aritmetica***, pubblicati nel 1893 e 1903, rappresentarono il primo serio tentativo di dare una formalizzazione assiomatica dell'aritmetica.

Dai tempi degli *Elementi* di Euclide, con cui aveva formalizzato la geometria, nessun altro matematico aveva osato tanto con un formalismo così rigoroso e puro.

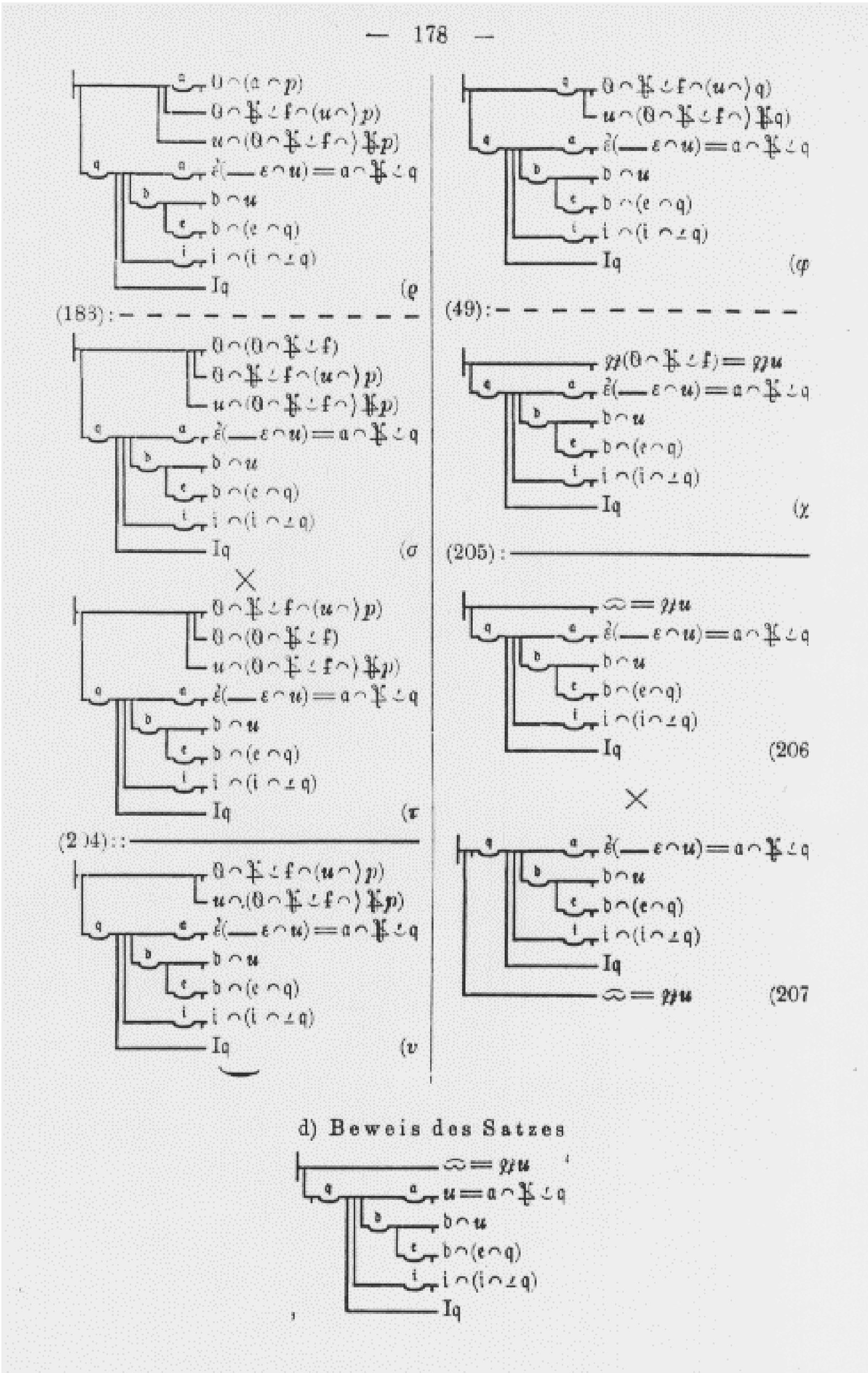
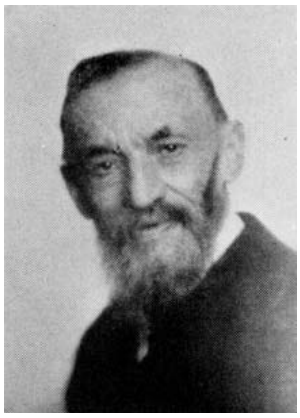


Fig. Friedrich Ludwig Gottlob Frege, Grundgesetze der Arithmetik, volume 2, H. Pohle, Jena, 1903, end of section 143 "Aufbau," page 178.

La notazione logica di Frege non era di facile di lettura, ma successivamente altri matematici, tra cui l’italiano **Giuseppe Peano**, ne migliorarono il sistema di scrittura fino a pervenire a quello attuale.



·1 $0 \varepsilon N_0$

·2 $a \varepsilon N_0 \,.\supset.\, a+ \,\varepsilon N_0$

·3 $s \varepsilon \mathrm{Cls} \,.\, 0 \varepsilon s : a \varepsilon s \,.\supset_a.\, a+ \,\varepsilon s \,:\supset.\, N_0 \supset s$ Induct

·4 $a, b \,\varepsilon N_0 \,.\, a+ = b+ \,.\supset.\, a = b$

·5 $a \varepsilon N_0 \,.\supset.\, a+ -= 0$

Paradossi e crisi dei fondamenti della matematica

Nella seconda metà dell’Ottocento diversi matematici si posero **il problema di dare solide fondamenta alla matematica** con maggiore cura di quanto non fosse stato fatto in precedenza, ma **diversi paradossi misero in difficoltà questo progetto evidenziando quanto fosse problematico il rigore matematico**.

In particolare, dopo che Cantor ebbe aperto la strada allo studio degli insiemi infiniti, diversi matematici cominciarono ad approfondire il tema dell’infinito da vari punti di vista e ben presto incontrarono alcune sorprese.

Uno dei primi paradossi fu quello di Cesare Burali-Forti, nel 1897, che dimostra che il processo di costruzione dell'insieme di tutti i numeri ordinali porta ad una contraddizione.

Paradosso di Russel, 1902.

Proprio mentre Frege si accingeva a scrivere il secondo volume della sua opera sui principi dell’aritmetica, Bertrand Russell, comunicò a Frege che il suo sistema permetteva di derivare una contraddizione.

L'insieme di tutti gli insiemi che non appartengono a se stessi, appartiene o no a se stesso?

- **Se si, allora è uno degli insiemi che non appartengono a se stessi, e quindi non può appartenere alla loro collezione, cioè a se stesso;**
- **se no, allora è uno degli insiemi che non appartengono a se stessi, e dunque appartiene alla loro collezione, cioè a se stesso**.

Questo paradosso viene spesso divulgato nella forma del **paradosso del barbiere**: "In un villaggio c'è un unico barbiere. Il barbiere rade tutti (e soli) gli uomini che non si radono da soli. Il barbiere rade se stesso?"

Un altro paradosso relativo alla definibilità dei numeri reali venne trovato da matematico francese Jules Antoine Richard è stato proposto dal Richard nel 1905.

… e ancora paradosso di Berry (1906), paradosso di Grelling (1908), …

5.3. Il programma di Hilbert

La **crisi dei fondamenti matematici**, innescata dalla scoperta di vari paradossi e dallo studio di funzioni matematiche “patologiche” ponevano la necessità non solo di ridefinire i concetti matematici portanti con un maggiore rigore ma esigevano anche di **capire meglio quelle forme di ragionamento** impiegate per millenni ma ora sotto accusa per i paradossi a cui davano origine.

Il famoso matematico tedesco David Hilbert (1862-1943) propose di costruire queste basi facendo ricorso

- alla **logica** studiata da Frege per costruire assiomatizzazioni dei vari settori della matematica
- alla **teoria degli insiemi (infiniti)** emersa dal lavoro di Cantor

L’assiomatizzazione della matematica

Agli inizi del 1900, David Hilbert lanciò come programma di ricerca l'**idea alquanto ambiziosa di formalizzare la matematica** individuando sistemi assiomatici da cui poter derivare in modo "meccanico" tutti i teoremi della matematica.

Un **sistema assiomatico** rappresenta una sorta di teoria che contiene tutti i principi primi da cui partire per effettuare ragionamenti in un dato settore della matematica.

La parola "**meccanico**" si riferisce al fatto che la derivazione dei teoremi non deve far riferimento a procedimenti intuitivi o all'intelligenza del matematico, ma deve seguire dall’applicazione di regole (dette *regole di inferenza*) semplici e prive di ambiguità come, ad esempio, le regole di gioco degli scacchi.

Un primo importante esempio di progetto di assiomatizzazione è costituito dalla “rivisitazione” degli Elementi di Euclide che portò ad un’assiomatizzazione completa della geometria euclidea nel famoso lavoro ***Grundlagen der Geometrie*** del 1899.

Secondo Hilbert, ogni problema (matematico) avrebbe potuto trovare una risposta (affermativa o negativa) a partire da un opportuno sistema assiomatico applicando le regole di inferenza:

> **"Ogni problema matematico deve essere necessariamente suscettibile di una chiarificazione esatta, o nella forma di una risposta effettiva alla domanda sollevata, o attraverso la dimostrazione dell'impossibilità della sua soluzione e quindi del necessario fallimento di tutti i tentativi… Per quanto inaccessibili possano sembrarci questi problemi e per quanto si possa rimanere scoraggiati di fronte a essi, abbiamo, nondimeno, la ferma convinzione che la loro soluzione deve conseguire da un numero finito di processi puramente logici …".**

Attorno al 1910 iniziarono i primi tentativi per dare una risposta al programma di Hilbert e nei primi anni '30 arrivarono le risposte più "interessanti" in merito al progetto di Hilbert.

I Principia Mathematica di Russell e Whitehead

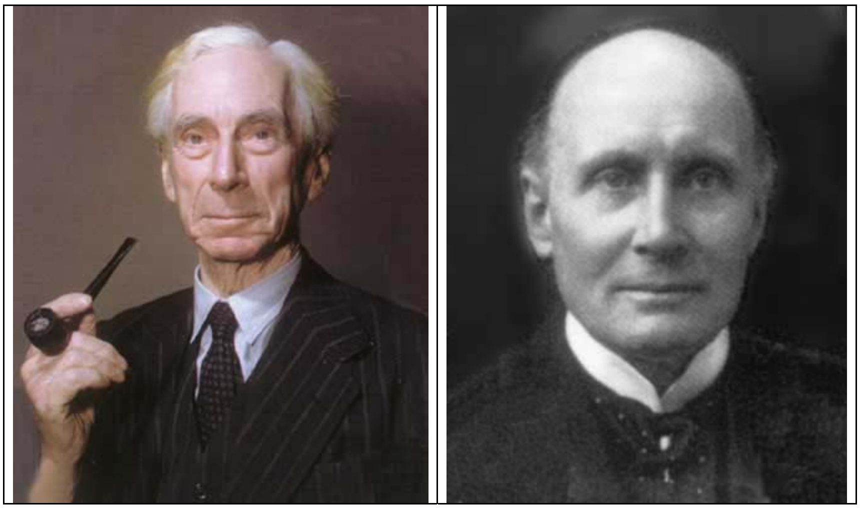
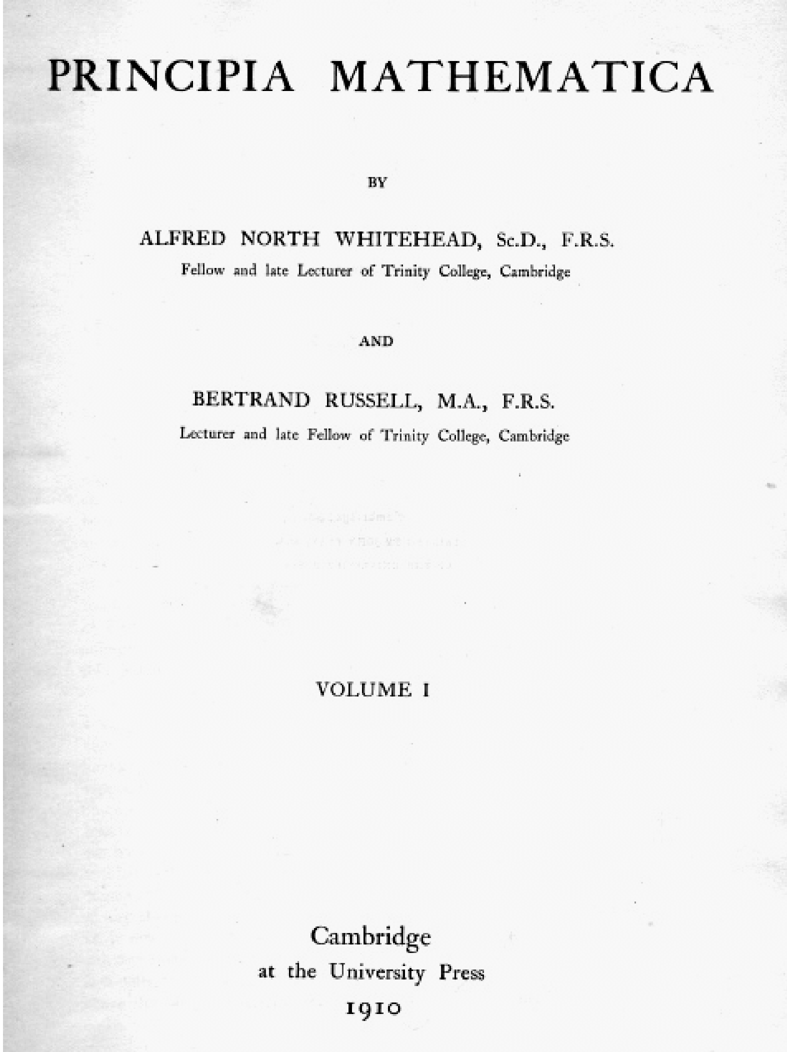


Fig. Bertrand Russel (a sinistra) e Alfred North Whitehead

Il programma di Hilbert per la realizzazione di un sistema logico formale da cui derivare tutti i teoremi della matematica produsse come uno dei risultati più importanti la pubblicazione (1910-13) dei ***Principia Mathematica*** da parte dei logici-matematici inglesi **Bertrand Russel e Alfred North Whitehead**.

L'opera di Russell e Whitehead partiva dal precedente lavoro del logico tedesco G. Frege in cui Russell stesso aveva trovato un aspetto contraddittorio. Questa opera rappresentò il più elaborato tentativo mai fatto prima di allora di sviluppare le nozioni fondamentali della matematica (aritmetica) a partire da un insieme ben definito di assiomi.



PRINCIPIA MATHEMATICA

BY

ALFRED NORTH WHITEHEAD, Sc.D., F.R.S.
Fellow and late Lecturer of Trinity College, Cambridge

AND

BERTRAND RUSSELL, M.A., F.R.S.
Lecturer and late Fellow of Trinity College, Cambridge

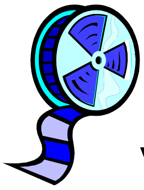
VOLUME I

Cambridge
at the University Press
1910

Fig. Copertina del libro di Russell e Whitehead.

AUDIO

Audio 1: voce di Bertrand Russell in occasione del conferimento del Premio Nobel: Desire [da http://setis.library.usyd.edu.au/stanford/archives/win2002/entries/russell/russell-soundclips.html]

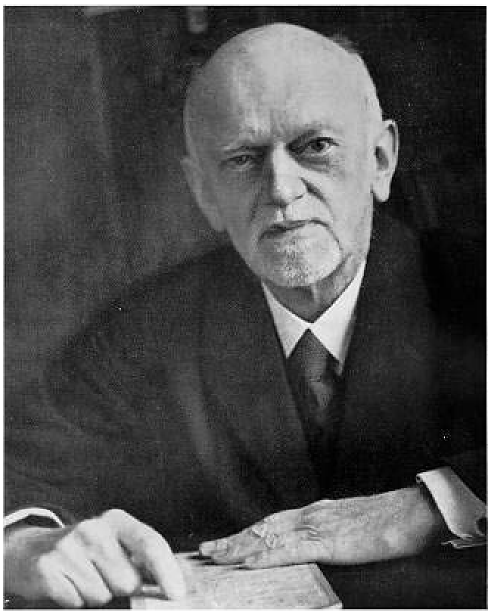
 VIDEO

Video 1: Bertrand Russel. [da http://www.britannica.com/nobel/ind_av.html]

 LINK

http://plato.stanford.edu/entries/principia-mathematica/

Le domande di Hilbert



Per poter "certificare" in modo indiscutibile il valore del lavoro di Russell e Whitehead era però necessario provarne la consistenza e la completezza.

Pertanto Hilbert, di fronte a questo lavoro, pose come ulteriore obiettivo quello di provarne la completezza e la non contraddittorietà.

Questo lavoro fu affrontato dai migliori logici matematici degli anni ’20 e portò nel 1931 a conclusioni molto diverse da quelle che Hilbert si aspettava.

Altre critiche di metodo poste da matematici come **Brouwer** richiedevano di capire quali forme di ragionamento potessero essere legittimamente impiegate nelle dimostrazioni matematiche: ad esempio **Brouwer metteva in discussione le dimostrazioni esistenziali impiegate nel corso di tutto l'Ottocento e metteva in dubbio la validità di principi logici come ad esempio il principio del terzo escluso**.

Le critiche sollevate da Brouwer spingevano inoltre i matematici a trovare per i problemi matematici soluzioni costruttive che potessero essere realizzate concretamente in un numero finito passi.

Tra l'inizio del 1900 e la fine degli anni '20 Hilbert pose diverse questioni logiche al fine di evitare quei paradossi logici che erano emersi proprio in quegli anni e per frenare le critiche ai metodi della matematica di Brouwer.

Nel 1928, al Congresso Internazionale dei Matematici, a Bologna pose in modo molto chiaro **tre questioni**:

- **La matematica dei *Principia Mathematica* è completa**? cioè ogni enunciato che produce può essere dimostrato a partire dagli assiomi iniziali mediante opportune regole di inferenza?

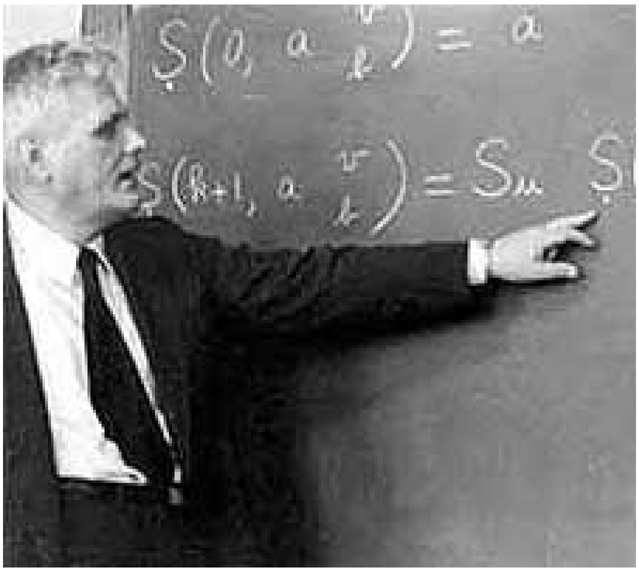
- **La matematica dei *Principia Mathematica* è consistente (coerente)**? cioè è possibile dimostrare che, ad esempio, l'enunciato 2 + 2 = 5 non può e non potrà mai essere dimostrato attraverso una procedura valida?

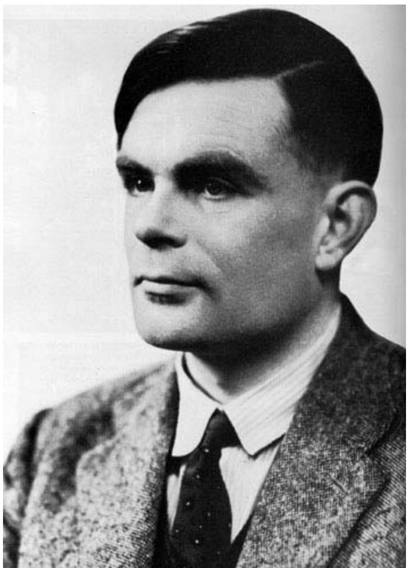
- **La matematica dei *Principia Mathematica* è decidibile**? cioè dato un sistema assiomatico e una proposizione scelta arbitrariamente, esiste una procedura che consenta di determinare se tale proposizione sia vera o falsa all'interno del sistema (questo problema venne denominato **Entscheidungsproblem – problema della decisione**)?

In cuor suo Hilbert era convinto che la risposta a tutte tre le domande fosse affermativa e che fosse solo questione di studiare bene le tre questioni per trovare la loro soluzione.

5.4. Il fallimento del programma di Hilbert


Kurt Godel


Alonzo Church


Alan Turing

Il teorema di Gödel

Diversi furono i matematici e logici che si cimentarono sui problemi posti da Hilbert riguardo la consistenza e completezza del sistema logico-formale realizzato da Russel e Whitehead.

La risposta alle prime due domande giunse nel 1931 grazie al geniale lavoro del logico austriaco **Kurt Gödel** (1906-1978) con il suo ***teorema di incompletezza***.

Gödel affrontando il problema in termini puramente logici dimostrò

- non solo che **il sistema di Russell-Whitehead era incompleto**, nel senso che esistevano proposizioni per le quali non era possibile dimostrare né la verità né la falsità,
- ma che **qualunque altro sistema formale sarebbe risultato parimenti incompleto** a causa di un'incompletezza di fondo caratterizzante qualunque sistema formale logico.

Questo era il prezzo da pagare a meno che non si volesse ammettere che il sistema logico era inconsistente.

Gödel riuscì a mostrare anche che nel sistema dell'aritmetica non è possibile formulare un enunciato logico che esprima la correttezza del sistema, conclusione che costituisce il **secondo teorema di Gödel**:

- **Nessun sistema coerente può essere utilizzato per dimostrare la sua stessa coerenza.**

Questo risultato risponde negativamente alla seconda questione posta da Hilbert al Congresso di Bologna: per riuscire a dimostrare la coerenza dell'aritmetica sono necessari metodi più potenti che non quelli semplicemente finitistici, ipotizzati da Hilbert.

Per giungere a questo risultato Gödel sfruttò in modo alquanto sofisticato un vecchio paradosso, noto come **paradosso del mentitore**: “Questa frase è falsa”.

Egli modificò questo paradosso nella forma “**Questo teorema non è dimostrabile**” e mostrò che era possibile codificare opportunamente questa espressione in una formula di un sistema logico formale (purché sufficientemente espressivo) dando luogo all’incompletezza del sistema stesso.

Il lavoro di Gödel mostrò che in matematica la derivazione di nuovi teoremi non è meccanizzabile se non in modo incompleto, non importa quanto sofisticato e complesso sia il sistema (logico) progettato.

Nonostante i risultati negativi rispetto alle speranze di Hilbert, il lavoro di Gödel e di altri studiosi fu comunque essenziale per tutto il settore della logica matematica e dei fondamenti stessi della matematica… inoltre, indirettamente diede inizio alla teoria della computabilità.


LINK

http://www-groups.dcs.st-and.ac.uk/~history/index.html

http://www.edinformatics.com/great_thinkers/godel.htm

L’Entscheidungsproblem

La terza domanda posta da Hilbert al Congresso di Bologna del 1928 era l’“***Entscheidungsproblem***” (in tedesco “problema della decisione”) e suonava così:

> **trovare un algoritmo (“procedura meccanica”) che sia in grado di decidere per una proposizione logica del primo ordine se questa è sempre vera (a prescindere da qualunque interpretazione semantica)**.

In qualche modo, si può dire che questo problema traeva origine addirittura dai tempi di Gottfried Leibniz, il quale immaginava di poter realizzare una macchina capace di manipolare simboli matematici in modo da poter stabilire la verità delle proposizioni matematiche. Egli mise in evidenza che il primo passo importante per fare una cosa del genere richiedeva di inventare un opportuno formalismo logico.

I lavori successivi nel campo della logica, portarono in effetti ad introdurre un linguaggio logico sufficiente preciso e potente grazie ai lavori di Boole e, come abbiamo visto, soprattutto di Frege.

1936: due risposte per lo stesso problema

A metà degli anni ’30, lo statunitense Alonzo Church e l’inglese Alan Turing affrontarono in modo indipendentemente il terzo problema di Hilbert (l’*Entscheidungsproblem*).

Nel 1936, la conclusione a cui giunsero entrambi quasi contemporaneamente (Church precedette Turing di pochi mesi) fu che era impossibile realizzare un algoritmo capace di decidere se una qualunque proposizione dell’aritmetica era vera o falsa.

Per poter rispondere al problema in modo rigoroso, ovviamente era necessario precisare in modo formale il concetto stesso di “algoritmo”.

- Alonzo Church, con il contributo di Stephen Kleene, propose un formalismo noto come ***lambda calcolo***,
- mentre Alan Turing propose delle macchine astratte (oggi note come **macchine di Turing**).

Tutte due i lavori sfruttavano la tecnica di enumerazione introdotte da Kurt Gödel pochi anni prima (derivata a sua volta da Cantor).

Nonostante i risultati negativi, il lavoro di Church e in particolar modo quello di Turing (descritto nel famoso articolo ***On computable numbers, with an application to the Entscheidungsproblem***, 1937) ebbero conseguenze importantissime per la storia dell'informatica e diedero il via alla teoria della computabilità.

Il lambda calcolo di Church e Kleene

Fig. Alonzo Church

Nell'articolo An Unsolvable Problem of Elementary Number Theory Church introduceva il lambda calcolo un particolare formalismo per esprimere in modo rigoroso funzioni matematiche:

$(\lambda\, x\, y.\ y\, x)\ (\lambda\, x.\ y)$	$(\lambda\, f.\ f\, 3)(\lambda\, x.\ x + 2)$	$\lambda\, f\, x.\ f\,(f\,(f\, x))$

Fig. Espressioni nel lambda calcolo.

Nel lavoro Church affermava poi che ogni espressione del lambda calcolo corrispondeva ad un procedimento di calcolo ben definito (algoritmo) dando così una definizione rigorosa di effettiva calcolabilità (funzione computabile) secondo quanto richiesto dal Hilbert.

Ogni poteva essere valutata (calcolata, eseguita) seguendo alcune regole ben precise.

Mediante il lambda calcolo Church mostrava che le proposizioni dell'aritmetica potevano essere tradotte in questo formalismo.

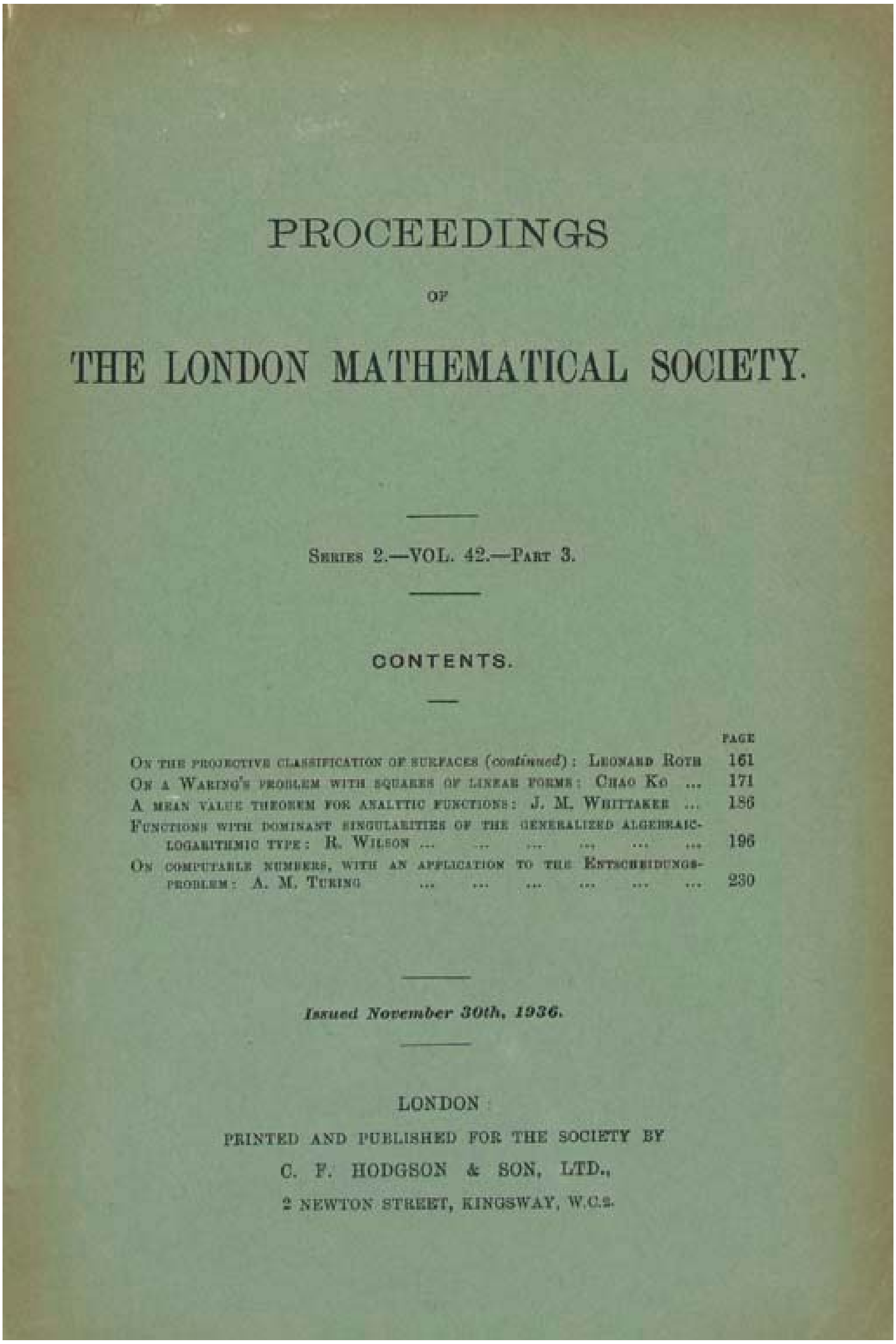
Infine, Church faceva vedere che non era possibile trovare una funzione computabile (espressa nel lambda calcolo stesso) che per due date espressioni del lambda calcolo potesse decidere se queste erano equivalenti oppure no. Proprio questa indecidibilità determinava la risposta negativa alla terza domanda di Hilbert.

LINK

http://www-groups.dcs.st-and.ac.uk/~history/index.html

http://en.wikipedia.org/wiki/Lambda_calculus

5.5. Il moderno concetto di algoritmo



PROCEEDINGS

OF

THE LONDON MATHEMATICAL SOCIETY.

SERIES 2.—VOL. 42.—PART 3.

CONTENTS.

Issued November 30th, 1936.

LONDON:
PRINTED AND PUBLISHED FOR THE SOCIETY BY
C. F. HODGSON & SON, LTD.,
2 NEWTON STREET, KINGSWAY, W.C.2.

Fig. Prima pagina degli atti che contengono il famoso articolo di Turing del 1936.

La macchina di Turing

Alan Turing cominciò a lavorare alle questioni proposte da Hilbert nei primi anni '30 e, diversamente da Gödel e da Church, **non utilizzò un approccio puramente di tipo logico**.

Ricercando una definizione il più possibile precisa e generale del concetto di "procedura di calcolo", Turing iniziò ad analizzare tutto ciò che un essere umano faceva durante l'esecuzione di un processo di calcolo cercando di individuare gli elementi essenziali e scartando tutti quelli irrilevanti.

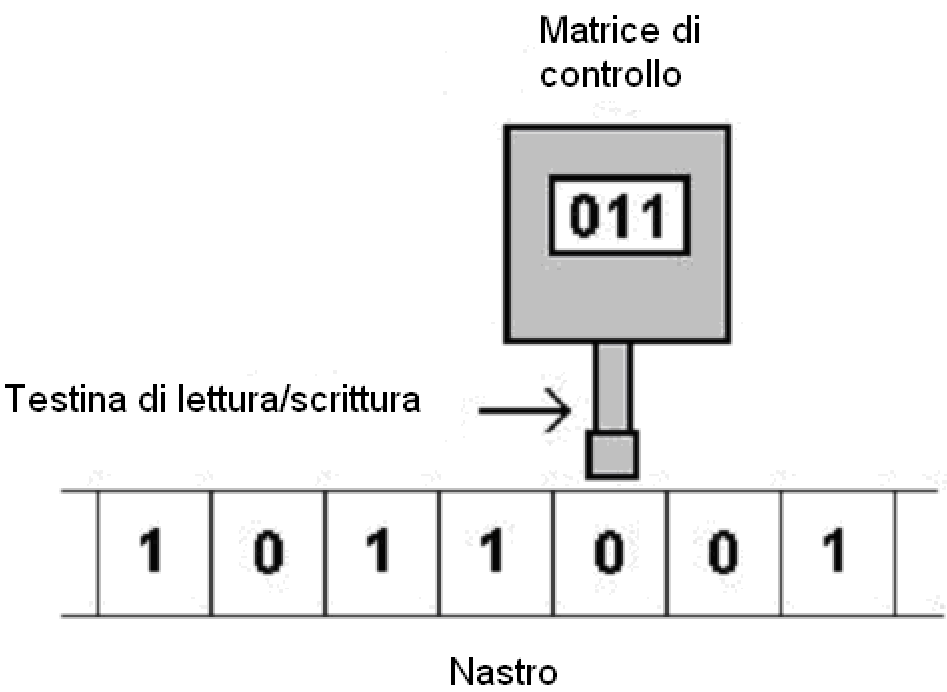
- la persona utilizza fogli di carta come memoria;
- la persona legge dati sul foglio di carta;
- la persona scrive dati a partire da altri dati, eventualmente cancellando dati precedenti;
- la persona decide cosa scrivere in base a ciò che è presente sul foglio e al proprio stato mentale.

In questo modo, egli inventò la cosiddetta **macchina di Turing** (che egli chiamava **A-machine**), che costituisce un modello di calcolatore molto semplice ma al tempo stesso sufficientemente potente per studiare le proprietà matematiche di ciò che è calcolabile.

Turing concepì **questo dispositivo come modello ideale di calcolatore** per studiarne le caratteristiche in termini teorici e non lo costruì fisicamente con dei dispositivi fisici. Si rese però conto che le azioni dell'uomo potevano essere facilmente sostituito da un meccanismo fisico.

La macchina di Turing (MT) è costituita

- da un **nastro**, che gioca il ruolo del dispositivo di memoria e viene supposto illimitato in entrambe le direzioni; il nastro è suddiviso in celle tutte uguali e ognuna di esse può contenere un simbolo.
- una **testina** che permette di leggere e scrivere sulle celle del nastro; in particolare la testina esplora una cella alla volta, quella cioè che a un dato istante viene a trovarsi in sua corrispondenza. **Il simbolo letto dalla testina può essere cancellato e sostituito con un nuovo simbolo**.
- un **dispositivo di controllo** che regola il movimento della testina rispetto al nastro, spostandola ogni volta di una cella verso sinistra o verso destra secondo i casi. **Il dispositivo di controllo è dotato di una memoria interna costituita da un certo numero finito di stati**.



Il comportamento della MT dipende
- dal simbolo letto sul nastro mediante la testina, e
- dallo stato interno in cui si trova il dispositivo di controllo in un dato momento.

Le informazioni che si trovano sul nastro all'inizio della computazione costituiscono i dati in ingresso, mentre quelle presenti sul nastro all'arresto della macchina costituiscono il risultato della computazione.

Il comportamento specifico della MT è descritto da una matrice di controllo che indica per ogni stato in cui si può trovare la MT e per ogni simbolo che può essere letto dalla MT il passo successivo da compiere.

Un passo consiste nello scrivere un nuovo simbolo nella cella correntemente letta dalla testina, nel portarsi in un dato stato e nello spostarsi a destra o a sinistra.

Qui di seguito possiamo vedere un esempio di macchina di Turing che esegue la differenza tra due numeri espressi in forma unaria: ad esempio il numero 6 viene rappresentato mediante una stringa di 6 “1”. All’inizio sul nastro sono presenti i dati di ingresso nella forma "x-y=", dove x rappresenta il minuendo e y il sottraendo (ad esempio 6-3 viene rappresentato come "111111-111=".

I simboli che possono essere usati sul nastro sono:

"1", " " (bianco), "-" (meno), e "=".

La macchina impiega complessivamente 5 stati, di cui uno è solo per indicare l’arresto della macchina. Qui vediamo la matrice di controllo:

	“ “	1	-	=
a	(a , " ", des)	(a , "1", des)	(a , "-", des)	(b , " ", sin)
b		(c , "=", sin)	(Halt, " ", sin)	
c		(c , "1", sin)	(d , "-", sin)	
d	(d , " ", sin)	(a , " ", des)		
Halt				

Fig. Esempio di matrice di controllo di una macchina di Turing.

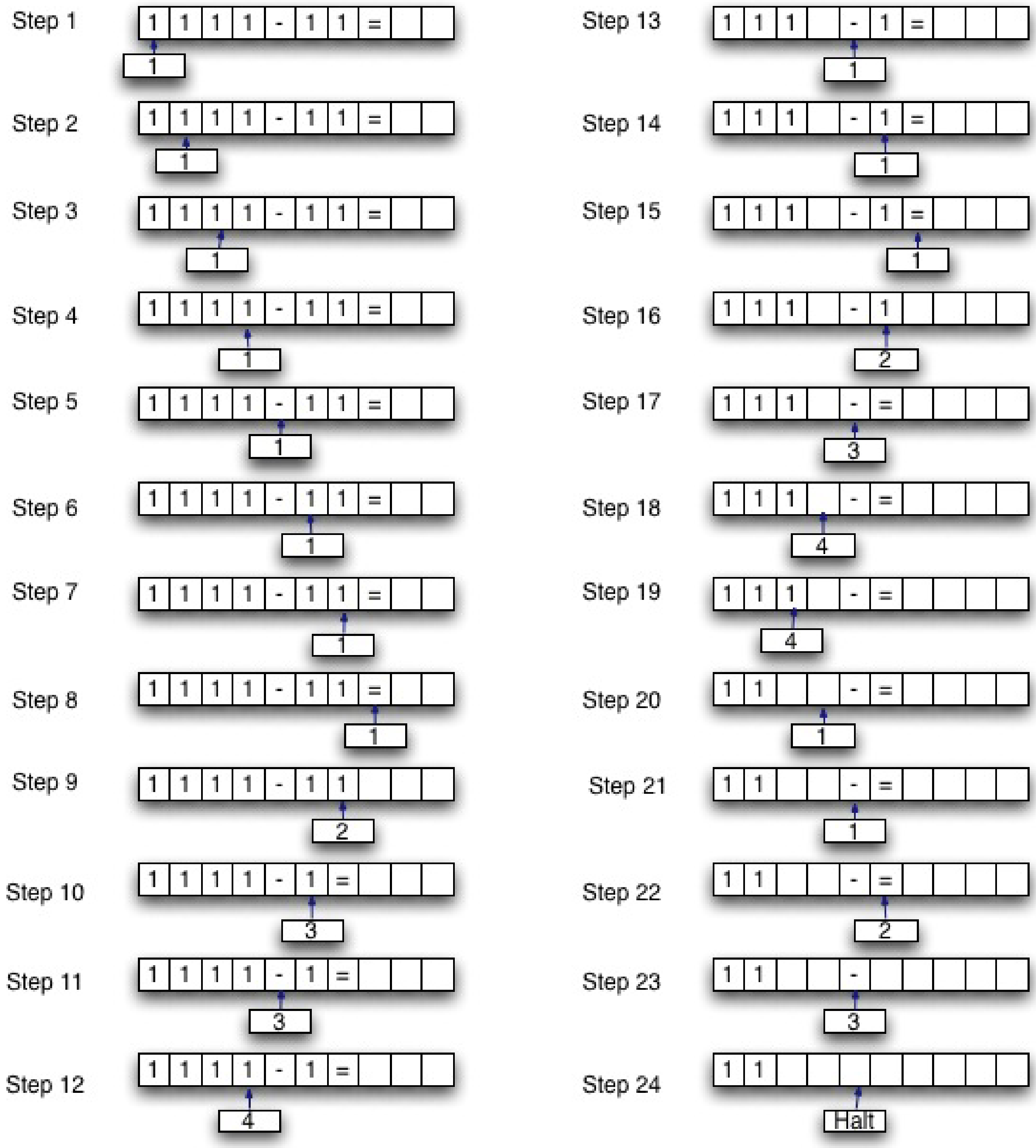


Fig. Esempio di computazione di una macchina di Turing.

LINK

http://www.cs.umass.edu/~immerman/cs601/turingRef erence.html

http://www.alanturing.net/turing_archive/archive/index/archiveindex.html

http://www-groups.dcs.st-and.ac.uk/~history/index.html

http://www.turing.org.uk/turing/

http://www.cs.swarthmore.edu/~dylan/Turing.html

http://www.alanturing.net/turing_archive/index.html

La macchina di Turing universale

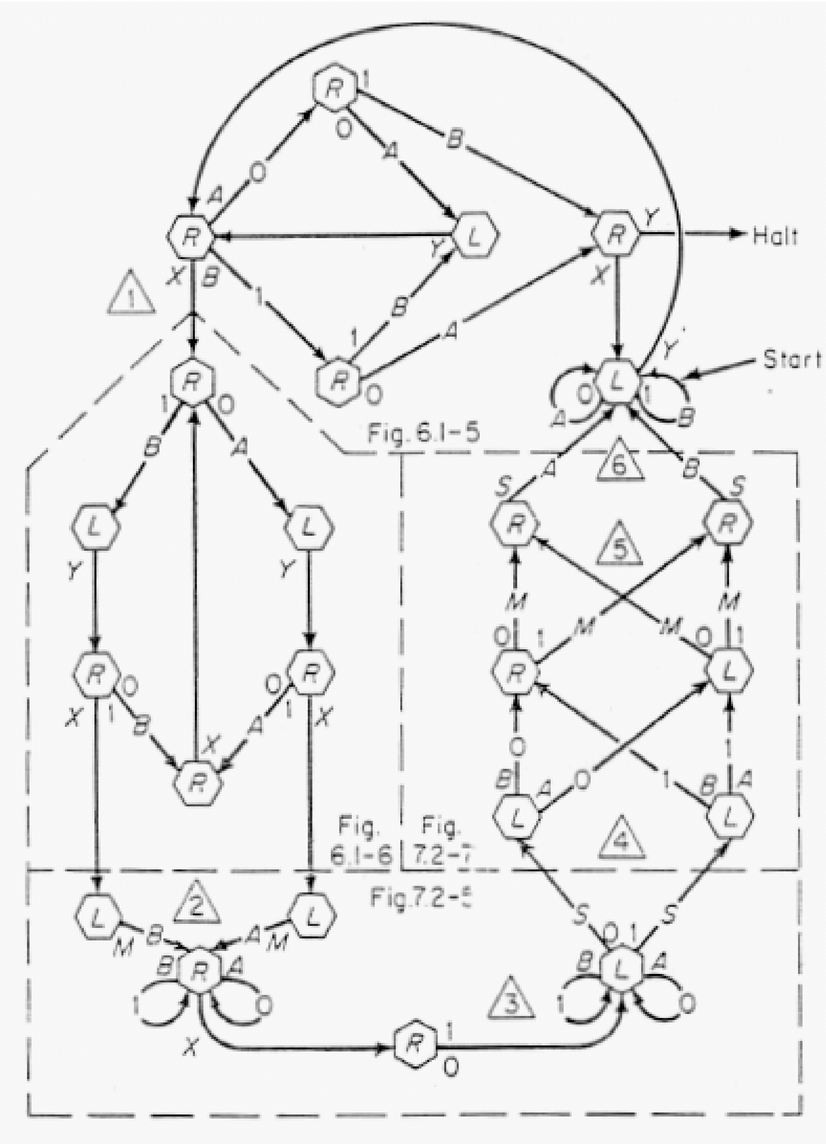


Fig. Il grafico di transizione di una macchina di Turing universale.

Turing non si limitò ad introdurre le cosiddette macchine di Turing, ma andò oltre e fece vedere che tra le diverse macchine di Turing era possibile trovarne una in grado di “simulare” tutte le altre macchine di Turing.

In altre, era possibile costruire una particolare macchina, denominata in seguito *macchina di Turing universale*, capace di prendere ingresso la descrizione di una qualunque macchina di Turing (opportunamente codificata) e i dati da elaborare e di calcolare il risultato secondo simulando la macchina fornita in ingresso.

Dal momento che una macchina di Turing è completamente definita dalla sua matrice di controllo, Turing mostrò che era possibile codificare la matrice di controllo come una sequenza di simboli del tutto analoga a quella utilizzata per i dati di ingresso. Tale descrizione poteva quindi essere scritta sul nastro della macchina di Turing insieme ai dati.

	1'	0'	*'	1	0	*
A				f	f	e0
B				C	C	e1
fC			c	b*	a*	C
c	=	C	E'	'	'	
a	b'	C	E'	'	'	'
b		a'	D	'	'	'
d	'	'	D	'	'	
D			e'	d'	–	
E	'	'	e'	=	–	'
e	B	A	=	'	'	'

The transition table at the right defines a small (11 states + 6 symbols) TM U by Ikeno which can simulate any other TM M over $\in \{0,1\}$ tape alphabet with the following stipulations (which still allow M simulate any other TMs): The direction of head shift is the function of the new post-transition state (lower case - left, upper case - right). And so is, for M only, the digit typed. The tape is infinite to the right only: the left states in the leftmost cell remain there. For M only, the new state is the tape bit read plus a function of the old state. In the U table the states and tape digits are shown only when changed; except that the prime is always shown. The halt and external input/output commands are special states for M; for U they are shown as =.

Fig. Una delle più semplici versioni della Macchina universale di Turing. La macchina è descritta da una tabella di transizione.

Una macchina di questo tipo costituisce un calcolatore generale programmabile nello stesso senso definito da Babbage con la Macchina Analitica.

Cento anni dopo il lavoro di Babbage, un altro inglese aveva riscoperto, questa volta in termini puramente teorici, il concetto di calcolatore universale.

Fu proprio con questa macchina che Turing riuscì a rispondere negativamente al problema posto da Hilbert (*Entscheidungsproblem*) trovando un problema algoritmicamente insolubile.

Turing, studiando il cosiddetto ***problema dell'arresto***, scoprì infatti nessuna macchina di Turing può essere costruita con lo scopo di riconoscere distinguere in modo infallibile le macchine di Turing che si fermano per un certo ingresso da quelle che non si fermano (*On computable numbers, with an application to the Entscheidungsproblem*, del 1936).

La strategia con cui veniva raggiunto questo risultato, fra l'altro, ricalcava molto da vicino le idee applicate da Gödel nel suo grande teorema del '31.

Tesi di Turing-Church

Negli stessi anni in cui Turing introduceva le sue macchine e negli anni successivi, **altri matematici introdussero formalismi atti a descrivere procedure di calcolo in modo altrettanto rigoroso ed astratto**: Godel (1931), Post (sistemi di riscrittura, 1936), Church (lambda-calcolo, 1936), …

L'analisi di questi formalismi portò alla conclusione:

> **Nessuna macchina può calcolare più di quello che fa la macchina universale di Turing: questi diversi modelli di calcolatore possono essere più efficienti, più veloci, più user-friendly della macchina di Turing, ma non possono calcolare funzioni che non siano calcolabili anche dalla macchina universale di Turing**.