Naviglio Piccolo

Giovedì 20 ottobre 2011 - ore 21.00

Stasera diamo i numeri

conversazione con

Pierluigi Boschetti

Gli appassionati che si occupano dello studio dei numeri, siano essi matematici o semplici cultori, che magari impiegano anni per trovare il numero primo che segue l'ultimo trovato nel proprio quest'anno ($2^{43112609}$ - 1 un numero di quasi 13 milioni di cifre, che solo per essere scritto richiede circa migliaia di pagine) sono forse pazzi? E' certo che lo studio dei numeri e dell'aritmetica presenta difficoltà tra le più grandi dell'intera matematica.
Vogliamo presentare una carrellata atipica sul mondo dei numeri visti con occhi stupiti sui loro misteri.
Esporremo le ipotesi sulla loro origine: sono stati inventati per contare i propri beni, campi, buoi, ...per necessità rituali o ancora per esigenze speculative? Con spirito curioso, ci intratterremo sui diversi insiemi numerici: gli interi, i razionali, gli irrazionali e gli immaginari, che già dal nome rivelano l'immagine che li circonda; così gli irrazionali sembrano un po' fuori dalla logica, gli immaginari un frutto della fantasia, etc. Ci soffermeremo su alcuni personaggi che hanno segnato lo sviluppo di questa parte della matematica, diffondendo sul nostro argomento niente più che un profumo.
Concluderemo con un'applicazione dei numeri primi che all'epoca della scoperta (1600 circa) era niente più che una bizzarria di uno di quei pazzi citati all'inizio, ma che oggi costituisce la base necessaria per navigare in internet in sicurezza.

Pierluigi Boschetti, laureato in Fisica Teorica …qualche anno fa (1969). Dopo un breve periodo di insegnamento e di ricerca all'Università, durante il quale ha pubblicato diversi articoli su giornali internazionali di Fisica, ha lavorato nell'informatica fino al 1994. Da piccolo aveva la passione della scultura; qualche anno dopo la laurea, in una giornata piovosa sul lago, per passare il tempo, ha ripreso l'antica passione e lasciata l'informatica si é dedicato nuovamente alla scultura e alla pittura, che ha poi praticato professionalmente. Da pensionato coltiva anche lo studio della musica suonando il flauto traverso e delle lingue antiche, greco ed ebraico biblico. Continua privatamente lo studio della matematica e della fisica.

Viale Monza 140 I Piano (M1 Gorla - Turro)

Quote di partecipazione ad ogni incontro:	
Normale	**€ 2,00.**
Soci di Naviglio Piccolo	**€ 1,00.**
Per chi si associa al momento	**gratuita**
Quota associativa a Naviglio Piccolo	**€ 15,00**

Informazioni: www.navigliopiccolo.it **email** naviglio.piccolo@navigliopiccolo.it

Si ringrazia:

Cooperativa Sociale
CIRCOLO FAMIGLIARE DI UNITA' PROLETARIA
VIALE MONZA, 140 - TEL.022574683 - 20127 MILANO

Stasera diamo i numeri

INTRODUZIONE

Metti una conversazione trai due vecchi amici, un matematico e un artista, e metti che il discorso tocchi una poesia di Omar Khayyam, poeta persiano del secolo XI°

O cuore, fa' conto di avere
tutte le cose del mondo
Fa' conto che tutto ti sia
giardino delizioso di verde
E tu su quell'erba verde
fa' conto d'esser rugiada
Gocciata colà nella notte,
e al sorgere dell'alba svanita

Matematico: conosco l'autore, anche perché è stato un grande matematico. So anche che il nome Khayyam letteralmente significa "fabbricatore di tende", dalla professione del padre.
Artista: mi fa piacere che tu lo conosca, io l'ho trovato molto interessante, però mi risulta che in occidente sia conosciuto quasi esclusivamente come poeta. Infatti, A. Bausani, nella prefazione alle "Quartine" di Khayyam (ed. Einaudi), cita solo di sfuggita l'attività di scienziato di Khayyam.

M: infatti, anch'io lo conosco come poeta, ma so che è stato anche un grande matematico del medioevo persiano.

Giacomo Balla "Numeri Innamorati"

A: oggi non è comune trovare una persona valente sia come poeta sia come scienziato, specialmente per noi italiani dopo l'idealismo di Croce e Gentile, che ha permeato la nostra educazione scolastica.
M: osservo che la commistione di arte e scienza nella stessa persona, non tocca solo la poesia; anche la pittura e la scultura hanno mostrato fenomeni analoghi.
A: la psicologia moderna ha trovato una differenziazione funzionale tra l'emisfero destro e sinistro del cervello dedicati rispettivamente all'attività creativa e a quella razionale, però abbiamo illustri esempi di personaggi in cui entrambi gli emisferi del cervelli funzionavano eccezionalmente bene, basti pensare a Leonardo da Vinci.
M: la matematica, come tutte le espressioni del pensiero, risente dell'ambiente sociale in cui il matematico si trova ad operare, oltre delle caratteristiche personali; così, ad esempio, i greci erano più interessati alla geometria e gli arabi all'algebra, mentre l'analisi ha avuto un forte impulso nella Francia dell'ottocento.
A: so che ogni argomento del sapere sviluppa un proprio linguaggio, ma il linguaggio della matematica mi sembra particolarmente ostico con

le sue tante parole astruse, come algebra e algoritmo. Riconosco che anche la poesia ha sviluppato i suoi termini, come ermetismo, metrica, endecasillabo.

M: Anche la matematica ha sviluppato un suo linguaggio. Ad esempio, la parola metrica si trova anche nella geometria e nella cosmologia, però ha un significato diverso rispetto a quello che assume nella poesia. Ma per venire alla tua questione, molte, moltissime parole derivano dall'arabo, perché gli arabi nel medioevo tradussero opere filosofiche e scientifiche dei greci e dei popoli del medio oriente. Così sono di derivazione araba tanti nomi di stelle Betelgeuse, Algol, Mizar, ... Ritornando al nostro argomento, il nome "algebra" deriva da "al-Jabr"che significa "aggiustamenti" e compare per la prima volta nel titolo di un libro (appunto di algebra) di al-Khwarizmi matematico persiano del 1000 d.c. mentre il nome algoritmo deriva proprio dal nome di questo matematico.

ORIGINI

M: I numeri esercitano una loro attrazione che talvolta raggiunge momenti che potremmo eufemisticamente definire strani; come quando James Ussher arcivescovo di Armagh a metà del XVII secolo calcolò che il mondo era stato creato il 22 ottobre 4004 a.C., ma, ... udite, udite, alle sei del pomeriggio!

A: cosa sappiamo sull'origine dei numeri?

M: in realtà non è un problema del tutto chiarito, stiamo parlando di eventi che si perdono nella notte dei tempi. Esistono diverse teorie.Potrebbero aver avuto lo scopo di "contare" i propri beni**.** Sembra che la prima forma di "conteggio" fosse la distinzione tra uno e molti e che la distinzione tra uno, due e molti venisse introdotta solo successivamente.

A: ah, come singolare, plurale e in alcune lingue anche duale, come nel greco e nell'ebraico antichi. Gli altri numeri invece?

M: forse per confrontare esattamente chi era il più ricco. Infatti dire: "Io ho molti buoi", non mi distingue da un altro che pure ha molti buoi. Ma la distinzione diventa evidente quando si dice:" io ho cento buoi", mentre l'altro ne ha duecento. Il conteggio degli oggetti non è l'unica ipotesi sulla nascita dei numeri, che potrebbe avere avuto un'origine rituale. Durante un rito sacro, il sacerdote dice ai suoi assistenti: prima entri tu con i fiori, poi entri tu portando l'incenso, ecc.

A: ho capito, significa: tu sei il primo, tu il secondo, ...

M: infine è possibile che l'uomo abbia sentito la necessità di utilizzare la sua logica a fini puramente speculativi. Questa ipotesi tuttavia, non sembra molto plausibile, perché la nascita del pensiero astratto dovrebbe essere stata piuttosto tarda nella vita dell'uomo.

A: mi sembra che sia comunque una strada da esplorare.

M: la logica ha raggiunto una delle sue punte più alte con la scoperta della dimostrazione. Il concetto di dimostrazione segna forse il vero inizio della matematica non più come semplice osservazione numerologica. Metaforicamente potremmo dire che l'alchimia della matematica cede il passo alla chimica matematica.

A: è veramente interessante questa metafora del passaggio alla certezza scientifica come transizione dall'alchimia alla chimica.

M: i greci furono i primi a comprendere che era possibile "dimostrare" che certi fatti rimangono veri per quanto lontano ci si spinga a contare, per quanti esempi si esaminino.

Una delle forme più raffinate della logica umana è la "dimostrazione per assurdo" una specie di rompicapo per molti studenti, che in fondo possono anche aver ragione. Tale metodo di dimostrazione si fa risalire a Ippocrate.
A: sai cosa mi piace molto in queste forme di ragionamento? Il fatto che la repubblica dei numeri è realmente democratica; nessun principio d'autorità, nessun verbo dominante, nessun potere sopra gli altri. La verità emerge all'ultimo rigo della dimostrazione, è lì che si può decidere della giustezza delle affermazioni fatte e non perché le ha dette qualcuno per importante che sia.

LA NUMERAZIONE – basi

M: un primo problema nell'organizzazione dei numeri deriva dalla necessità di utilizzare un opportuno elenco di simboli.
A: già, credo anch'io che non sia molto pratico avere un simbolo diverso per ogni numero; dopo i primi 10, al massimo 20 numeri saremmo in difficoltà.
M: hai colto il problema che ha portato a definire un insieme limitato di simboli (cifre), con cui costruire tutti gli altri numeri: Quest'insieme limitato di numeri è quello che chiamiamo una base, con ovvio riferimento al significato di base per la costruzione di tutta la numerazione. La scelta di quanti simboli utilizzare è ovviamente arbitraria. Solitamente noi contiamo in base 10, vale a dire con un insieme base di 10 cifre, ma nessuna proprietà dei numeri e delle operazioni dipende da questa scelta.
A: ho capito quello che dici, ma da cosa dipende la scelta di un base piuttosto dell'altra?
M: nella storia si pensa che la base 5 del romani dipendesse dal numero delle dita di una mano utilizzando il simbolo V come stilizzazione delle dita aperte di una mano, e il segno X come stilizzazione di due mani sovrapposte in maniera rovesciata. Si crede che anticamente i francesi contassero in base 20 di cui sarebbe un residuo l'espressione quatre-vingt per il nostro 80; lo stesso soixante-dix (70) come multiplo di 20 aumentato di 10 (3*20 + 10). I babilonesi contavano in base 60. La base10 invece dipenderebbe dalla possibilità di contare con le dita delle due mani, una specie di abaco naturale.
A: ma come sono stati introdotti e da chi le 10 cifre che sono la base per scrivere tutti i numeri (0, 1, 2, 3, ...)?
M: qui c'è un piccolo giallo, perché noi chiamiamo queste cifre numeri arabi, mentre in realtà sono state inventate dagli indiani. Il nome che gli abbiamo assegnato dipende dal fatto che, come abbiamo già osservato, sono state diffuse in Europa dalle opere di matematica araba del medioevo.
A: e gli arabi cosa ne pensano di questa "spogliazione" del merito della scoperta?
M: beh, certo ci devono essere rimasti male, come se gli avessero detto che il couscous è stato inventato dagli inglesi o dai norvegesi. Riprendiamo il nostro discorso sulla numerazione, e per semplicità ci atteniamo alla numerazione in base 10, con le cifre arabe. Ovviamente il valore numerico di una certa cifra dipende dalla sua posizione così ad esempio in 18, (naturalmente diamo qui per scontata la costruzione dell'insieme dei numeri interi), 1 non ha il valore di 1 unità, ma di 1 decina.
A: mi sembra che questo valore posizionale sia un pò come dire che un nano seduto sul gradino più alto è più alto di un gigante seduto sul gradino più basso. Nel numero 18 quindi l'1 nonostante sia un numero più piccolo vale più dell'8.
M: attenzione che c'è una difficoltà, abbiamo appena visto che la posizione occupata da una cifra ne specifica il valore di decine, di centinaia, etc., ma cosa succede se un 1 indica le centinaia, mancano le decine e 2 indica le unità? È stato introdotto un segno particolare per indicare questa mancanza, lo zero. Così in 102, 1 ha il valore di 1 centinaia, e questo significato

di 1 è stato reso possibile segnando con 0 l'assenza delle decine. Questo valore dello 0 è chiamato "posizionale".
A: con questo abbiamo risolto il problema di scrivere tutti i numeri con solo 9 cifre più lo 0.

LO ZERO

M: lo zero che hai appena citato, merita un'attenzione particolare.
A: perché, non è un numero come gli altri?
M: beh, sì, si comporta come tutti gli altri numeri, e quindi è un numero a tutti gli effetti, però, ...
A: però, ..., cosa?
M: pensando al numero per contare gli oggetti, lo zero crea qualche perplessità, ad esempio, una coda di zero persone non è, di fatto, una coda; zero banane è un concetto diverso da zero pesche, ma la realtà sottostante è la medesima, vale a dire un piatto vuoto. Ancora si dice zero di qualcosa come l'assenza di quel qualcosa, come dire che zero banane lo si dice pensando in qualche modo di eliminare da un insieme di banane una banana alla volta fino a restare senza banane; è ovvio che zero unicorni non è una frase dello stesso tipo, perché l'operazione di eliminazione in questo caso è un pensiero del tutto astratto, non esistono 1, 2, 3 unicorni per realizzare il processo di eliminazione.
A: è vero sembra anche a me che lo zero abbia caratteristiche peculiari.
M: queste particolarità, in effetti, hanno fatto sì che lo zero fosse l'ultimo numero introdotto
M: ora anche i numeri, come gli uomini, sono animali sociali, in altre parole un numero è tale, se "socializza" con gli altri o fuor di metafora se entra nelle operazioni con loro e se queste operazioni soddisfano le stesse determinate proprietà.
A: e allora lo zero, socializza o no con gli altri?
M: certamente e, infatti, è un numero, infatti ci si possono fare tutte le operazioni, manifestamente 3+0=3, 3+0+0=3 ecc, ancora 3-0=3, 3∗0=0, infatti nel suo significato 3∗0 significa 0+0+0 per 3 volte e quindi resta ancora zero, però ..., c'è un però, infatti oltre agli evidenziati problemi sul suo significato nel conteggio, anche nelle operazioni lo zero vuol mantenere una sua peculiarità, infatti vediamo subito che, diversamente dagli altri numeri, non si può fare una divisione per zero.

A: perché?
M: beh, ad esempio se fosse possibile la divisione per zero, tutti i numeri sarebbero uguali
A*:* ma va là, cosa dici, come è possibile?
M*:* certo e te lo dimostro. Sei d'accordo che poiché 6∗0=0 e 17∗0=0, allora 6∗0=17∗0. Quindi, se potessimo dividere entrambi i membri per 0, ne verrebbe che 6∗0:0=17∗0:0, poiché 0:0 dovrebbe essere 1 come qualsiasi numero diviso per se stesso, allora ne verrebbe 6∗1=17∗1 e in definitiva 6 =17. Davvero bizzarro il nostro zero e piuttosto superbo, non si vuole mescolare fino in fondo agli altri numeri. Questa peculiarità dello zero fa sì che si distinguano i numeri "naturali" usati per il conteggio degli oggetti (1, 2, 3,..). dai numeri "interi" che includono lo zero (0,1, 2, 3,..).
M: ricordi che abbiamo parlato all'inizio della dimostrazione per assurdo?

A: sicuro.
M: bene, senza parere, qui sopra l'abbiamo utilizzata: ipotizzando che si potesse dividere per zero ne è derivato l'assurdo dell'uguaglianza di tutti i numeri.
A: proseguendo nei nostri ragionamenti, una volta forniti di tutte le cifre da 1 a 9 e anche dello 0, la situazione dell'aritmetica naviga in acque più tranquille.
M: fino ad un certo punto. Verso le cifre arabe ("la pericolosa magia saracena" secondo Guglielmo di Malmsbury) ci fu in Europa una forte diffidenza per lungo tempo, e la colpa fu, per un certo verso, proprio dello zero. Infatti, fin troppo facilmente un disonesto poteva trasformare uno 0 in 6 o 9. Così a Firenze nel 1299 il Consiglio cittadino emanava un'ordinanza che dichiarava illegale l'uso delle cifre nelle scritture contabili: le somme dovevano essere indicate in lettere. All'Università di Padova i bibliotecari erano tenuti a indicare i prezzi dei libri "non per ciphras, sed per literas claras". Nel 1494 il sindaco di Francoforte diede istruzione ai contabili "di astenersi dal calcolare con le cifre". D'altronde ancora oggi il valore legale dell'assegno è dato dalla scrittura in lettere e non dalla scrittura in cifre. In Italia nel 1340 lo zero diventa una palpabile realtà economica nella partita doppia quando è 0 la differenza tra le attività e le passività, come elemento di pareggio del bilancio e quindi indice di attività sana.
Il tipico contabile mercantile calcolava con l'abaco (pallottoliere) e scriveva i risultati sul libro mastro sotto forma di numerali romani o parole. Solo molto lentamente le cifre arabe sostituirono questo armamentario.Ci fu scontro tra abachisti (tenaci sostenitori del calcolo meccanico con l'abaco) e algoristi (sostenitori della superiorità del fare operazioni con carta e matita, come facciamo oggi) senza bombe o spari, ma non per questo meno cruento sul piano verbale. Immagino che la parola algoristi ti si rivela chiara nelle pieghe del racconto svolto finora. Abbiamo già osservato che algoritmo deriva da Al-Khwaritzmi
A: questa polemica intellettuale mette in luce aspetti che sono nascosti come tra le pieghe di un velo.
M: certamente, ma c'era dell'altro in gioco, si trattava di catturare potenziali clienti, mostrando che il proprio metodo di calcolo era la scelta d'insegnamento più consono per la formazione dei figli. Infatti, troviamo in un libro sul calcolo di Adam Riese proprio un potenziale cliente che è dubbioso se mandare il figlio dall'abachista o dall'algorista. L'autore commenta: " Ho constatato, insegnando ai giovani,che quelli che imparano a fare i conti con le linee, (cioè con l'abaco o pallottoliere) diventano sempre più abili e più rapidi di quelli che adoperano le cifre e la penna,,,".
A: così nascosto tra le pieghe del velo... c'era un tornaconto economico, per trovare clienti a cui fare lezione di calcolo.
M: beh, non sarei così drastico. In effetti c'era anche la soddisfazione di riconoscere la supremazia del proprio metodo. Con le conoscenze di oggi possiamo affermare che il ricorso a uno strumento meccanico per il calcolo (l'abaco) è più veloce se ci si limita a fare le quattro operazioni, ma fallisce miseramente se si affronta anche solo un piccolo cenno di algebra. La teoria dei numeri è tra le cose più difficili della matematica. Infatti la sistemazione rigorosa della geometria è avvenuta sin dall'antichità; già nel 300 a.c. Euclide negli "Elementi", deriva le proprietà del piano e dello spazio come teoremi rigorosamente dimostrati a partire da alcuni principi considerati evidenti per sé stessi (assiomi). Per l'algebra e l'aritmetica, si deve invece attendere fino al XIX secolo (!) per avere una sistemazione assiomatica della teoria dei numeri, cioè una teoria dei numeri rigorosamente derivata da alcuni assiomi iniziali. E molte cose apparentemente semplici non sono ancora oggi note, come l'individuazione del successivo di un numero primo, un metodo efficace per la scomposizione di un numero nei suoi fattori primi, ecc.

LE OPERAZIONI

M: entriamo adesso nel cuore della matematica dei numeri, evidenziandone i concetti fondamentali. Nei verdi anni delle scuole elementari si comincia dapprima familiarizzando con la successione dei numeri naturali, poi con le tabelline, poi con i primi esercizi sulle operazioni,..
A: nelle tabelline qualcuno a volte ci mette un pò d'inventiva.

M: beh, posso dire che non sempre i libri di testo e gli esercizi hanno avuto una forma così.. come dire,.. arida, come si può considerare quella di oggi.
A: certo l'allenamento richiesto è molto noioso, ma mi è capitato di trovare una curiosa formulazione di un problema sulle operazioni in un libro di testo di Bhaskara, matematico indiano del XII secolo, "Lilavati" (Graziosa fanciulla) dedicata appunto all'apprendimento delle operazioni:

> Deliziosa fanciulla bella e cara, i cui occhi assomigliano a quelli di una divinità campestre, se sei versata nella moltiplicazione, dimmi quanto fa 135 volte 12?

M: sono davvero poetiche queste formulazioni, tanto più se si pensa ad un libro di testo di matematica come quello che mi hai citato di Bhaskara.
A: sai, ripensando agli anni di scuola, mi sembra che la matematica sia sempre esistita così come la conosciamo, con le sue operazioni, i suoi teoremi, ciascuno dotato di un'etichetta sempre quella, così si parlava del teorema di Pitagora, del teorema di Euclide, ecc.
M: ovviamente non è così, anche la matematica ha avuto la sua evoluzione, anche nella sua notazione. Consideriamo ad esempio, un'equazione come la scriveva Luca Pacioli nel XV e fino a tutto il XVI secolo:

censo de censo e censo equale a nu.o

la tabella che segue spiega il passaggio dalla questa notazione a quella moderna ben più compatta e significante:

1500	***significato***	***Nel 1800***
nu.o	*numero noto*	
cosa	*incognita*	x
censo	*seconda potenza della cosa*	x^2
Cubo	*terza potenza della cosa*	x^3
censo de censo	*quarta potenza della cosa*	x^4
e	*addizione*	+
equale	*uguaglianza*	=

la stessa equazione in termini moderni quindi si scrive $x^4 + x^2 = a$

A: certo c'è una notevole compattazione della notazione, ma il linguaggio non è diventato troppo specialistico?
M: sicuramente, ma la capacità di esprimere situazioni sempre più complesse che si ottiene, compensa ampiamente la difficoltà iniziale. Spendiamo qualche parola in più sulla lunga strada che ha permesso di passare dalla notazione di Luca Pacioli a quella odierna. Il segno + (più) e il

segno – (meno) sono stati introdotti nel 1489, quando un signore di nome Widmann li usò per sue necessità commerciali. Precisamente, alcune sue casse di merci dovevano pesare 4 ***c**entner*[1] l'una, ma alcune erano più leggere e pesavano ad esempio 5 Libbre in meno, allora Widmann sulla cassa stampigliava 4c – 5L, ad indicare che mancavano 5 libbre ai 4 centner prestabiliti, viceversa se erano più pesanti e pesavano 5 Libbre in più, sulla cassa segnava 4c + 5L. Quindi il segno – indicava una differenza in meno nella quantità contenuta nella casa e il segno + invece un eccesso di quantità. Quella notazione si rivelò così espressiva che passò presto dalle casse di merci ai fogli contabili e successivamente dal commercio all'algebra. Il segno di uguale ha avuto un'altra storia, correva l'anno 1557 e ci si poneva il problema di sostituire la parola *aequalis* che abbiamo visto utilizzata ancora nell'equazione di Luca Pacioli, e Robert Recorde inventò quel segnetto così semplice che usiamo oggi (=). Qualche tempo dopo, quando il segno da lui inventato circolava già nel mondo matematico, richiesto del perché di quella scelta, rispose: perché sono due linee gemelle e niente è più uguale di due gemelli.

A: un'immagine poetica. Uno sguardo accattivante sulle operazioni è anche quello di Schulz, l'autore di Charlie Brown:

LE OPERAZIONI INVERSE

M: ma vorrei riprendere il nostro discorso sulle operazioni, per fare una interessante osservazione ricca di conseguenze. Le operazioni inverse sono più complicate delle operazioni dirette e talvolta non hanno risultato nell'insieme dei numeri già noti.

A: vediamo se ho capito. *L'operazione inversa della addizione è la sottrazione:* se io eseguo la sottrazione disponendo solo dei numeri naturali e dello 0, - cioè 0,1,2,3,.. - l'operazione 5-3 deve dare un numero che aggiunto a 3 dà 5, e questo é 2. Quindi, l'operazione 2-3 deve dare come risultato quel numero che aggiunto a 3 dà 2, che non esiste tra i numeri interi che conosco. Mi sembra un'impasse insuperabile.

M: hai capito benissimo, ma la soluzione al problema esiste ed è "di ampliare l'insieme numerico di partenza", cioè l'insieme dei numeri noti, introducendo nuovi numeri che si possono considerare "risultato di sottrazioni" . È un punto cardine del discorso.. L'insieme di questi nuovi numeri, che estende l'insieme dei numeri e rende sempre possibile la sottrazione, lo chiamiamo insieme dei numeri interi (senza nessuna altra specificazione).

A: mi richiedi uno sforzo per comprendere questioni difficili. Io ho capito che i "numeri risultato di sottrazioni" sia del tipo 5-3 (fattibile anche con i "vecchi" numeri), che del tipo 2-3 (non fattibile con i "vecchi" numeri), sono concettualmente uguali perché sono costruiti esattamente nello stesso modo.

M: certo, e quelli che sono il risultato di operazioni come 2-3 li chiamiamo numeri interi negativi e convenzionalmente poniamo il nuovo numero 2-3 = –(3-2) = –1, cioè premettiamo il segno (-) al risultato della sottrazione "contraria", mentre quelli che sono il risultato di operazioni come 5-3 li chiamiamo numeri interi positivi e convenzionalmente premettiamo al risultato il segno (+), così scriveremo 5-3=+2 .

[1] quanto vale un *centner* è inessenziale in questo discorso

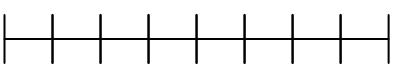
A: bene, ma tu stesso mi avevi fatto notare che per essere numeri devono socializzare tra di loro.
M: qui mi hai proprio preceduto. E' un punto di capitale importanza. L'introduzione di nuovi numeri come quella che abbiamo appena visto richiede che le operazioni definite per i nuovi numeri soddisfino le stesse proprietà e che se i nuovi numeri sono il risultato di operazioni possibili anche per i vecchi, essi devono comportarsi esattamente nello stesso modo.
A: ma questi numeri hanno anche un'utilità pratica o sono solo astruse speculazioni?
M: ma no, sono subito utili, certamente legati a convenzioni, come quella di definire le temperature sotto lo zero, i debiti e i crediti, ecc.

I NUMERI RAZIONALI

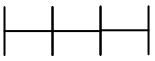
A: è interessante la capacità dell'uomo di inventare soluzioni ai problemi che via via sorgono, come quello che abbiamo visto di superare l'impossibilità di certe operazioni attraverso il procedimento di estensione dell'insieme dei numeri. Presumo che l'estensione dei numeri che abbiamo usato per le sottrazioni, sia possibile anche per le divisioni, dato che non sempre la divisione è possibile nell'insieme dei numeri interi, così ad esempio non è possibile trovare un numero intero che sia il risultato di 2:3.
M: anche qui il tuo ragionamento è veramente penetrante. Poiché abbiamo capito come estendere l'insieme dei numeri naturali per rendere illimitatamente possibile l'operazione di sottrazione, abbiamo una traccia per estendere la divisione. Visto che nell'insieme dei numeri interi la divisione 2:3 non ha risultato, consideriamo il simbolo 2:3 un nuovo tipo di numero, un numero razionale.

A: siamo alle solite, tali simboli si possono chiamare numeri?
M: certamente, ti risparmio i dettagli, ma questi simboli possono entrare nelle operazioni con gli altri tipi di numeri e queste operazioni soddisfano tutte le proprietà delle operazioni ordinarie dei numeri naturali e cosa importante, questi simboli quando vengono considerati il risultato di una divisione per 1, sono assolutamente simili ai numeri naturali, sottolineo simili e non uguali, e comunque, per dirla come sopra, si comportano nello stesso modo. Quindi da un punto di vista pratico, con la richiesta che si comportino esattamente nello stesso modo nelle operazioni, nei calcoli non c'è nessuna differenza. I numeri che si possono pensare come risultato di divisioni li chiamiamo numeri razionali.
Questi numeri che abbiamo costruito come estensione dei numeri interi per rendere sempre possibile la divisione, si possono considerare da un altro punto di vista. Fissata un'unità di misura, la misura di un segmento è espressa come un numero razionale.
A: interessante passare dall'aritmetica alla geometria cambiando il punto di vista.
M: allora, vediamo qui sotto un esempio grafico:

 unità di misura.

 il segmento qui a lato misura 8 volte l'unità di misura.

Però io potrei utilizzare un'unità di misura che sia 3 volte più grande della precedente, come nel grafico che segue:

 nuova unità di misura.

Se il segmento che prima misurava 8 volte l'unità di misura, viene misurato con questa nuova unità, esso evidentemente misura 8 volte 1/3 dell'unità di misura, cioè misura 8/3.
A: mi sembra chiaro.
M: questo esempio, pensato al contrario, fa vedere che dal punto di vista della misura i numeri razionali non sono strettamente necessari. Un segmento misura 8/3, ma se scelgo un'unità di misura opportunamente più piccola misura 8, quindi la sua misura può sempre essere espressa da numeri interi.
A: anche questo mi sembra chiaro.
M: abbiamo precedentemente osservato che i greci erano particolarmente interessati alla geometria. Con l'eccezione di una grande personalità: Pitagora. Aveva diciotto anni quando partecipò alle Olimpiadi vincendo le gare di pugilato. Dopo la vittoria decise di viaggiare; nella Jonia passò due anni con Talete e il suo allievo Anassimandro. Poi in Siria soggiornò presso i saggi fenici, che lo iniziarono ai misteri di Byblo. Si imbarcò poi per l'Egitto dove rimase per ventidue anni ed ebbe tutto il tempo di acquisire il saper dei sacerdoti nei templi sulle rive del Nilo. Quando i persiani invasero il paese, venne fatto prigioniero e condotto a Babilonia. Pur nella precaria situazione, nei dodici anni che trascorse nella capitale mesopotamica, riuscì ad acquisire l'enorme patrimonio di conoscenze degli scribi e dei magi babilonesi. Carico di esperienza e del sapere che aveva carpito mettendo a frutto ogni occasione, tornò a Samo che aveva lasciato quarant'anni prima. Ivi regnava il tiranno Policrate e Pitagora che odiava i tiranni, come del resto la maggioranza dei greci, fuggì nella Magna Grecia. Sbarcò a Sibari e si stabilì nella vicina Crotone. Sappiamo che qui fondò una setta, una società segreta sul tipo dei misteri dionisiaci, con la differenza che la sua società era fondata sulla matematica e sulla filosofia.
A: una personalità davvero interessante, ma dimmi come entra nello studio dei numeri.
M: innanzi tutto la sua posizione filosofica recitava *Tutto è numero.* Anche Galileo, molti anni dopo, nel "Nuncius Sidereus" sostiene che la natura è scritta in simboli matematici. Pitagora, pur senza la visione scientifica di Galileo, ebbe la grande intuizione della razionalità dell'universo. Inventò le stesse parole matematica e filosofia: Filosofia significa amore del sapere, mentre matematica deriva da μαθημα (mathema) che significa conoscenza, apprendimento. Da qui deriva l'aggettivo μαθηματικη (mathematichè) che, con il soggetto τεχνη (techne) cioè arte, sottinteso, assume il significato che la matematica è l'arte dell'apprendimento. La matematica, infatti, era patrimonio comune delle persone colte, atteggiamento culturale che indubbiamente favorì lo sviluppo della disciplina.
A: grande! ... prosegui.
M: Pitagora era particolarmente interessato ai numeri al contrario di quello che poi successe ai greci che si orientarono più verso la geometria.
A: sempre più intrigante la visione di Pitagora.
M: ma Pitagora aveva un'altra valida ragione che sosteneva la sua visione dell'universo dove "tutto è numero". Precisamente essa era la scoperta dell'esistenza di rapporti intervallari tra le frequenze delle note musicali espressi da numeri razionali. Così l'intervallo di quinta giusta è espresso dal rapporto 2/3, mentre quello di quarta giusta da ¾ e quello di terza maggiore da 4/5 ecc.
A: è molto interessante, ma dimmi più estesamente.
M: conducendo esperimenti sul monocordo, probabilmente inventato da lui stesso, (una corda fissata ai due estremi, con un ponticello mobile che poteva essere fermato in tutte le posizioni

desiderate) Pitagora aveva notato, che riducendo la lunghezza della corda vibrante secondo i rapporti razionali 1, 1/2, 2/3, 3/4, otteneva successivamente la tonica, l'ottava (do), la quinta (sol), la quarta (fa) ecc.

A: comincio a pensare che Pitagora avesse proprio ragione a dire "tutto è numero" ed anche se non è proprio così, certo aveva molte frecce al suo arco per sostenere questa idea. Mi sembra già sufficiente questo anche senza entrare nel sistema di accordatura Pitagorica.

IRRAZIONALI

M: concordo con te, procediamo allora ad analizzare un'altra grande scoperta attribuita ai Pitagorici che è la scoperta dei numeri irrazionali. Il grande scandalo nella comunità intellettuale greca è stata la scoperta che non esisteva una unità di misura tale che il lato e la diagonale del quadrato avessero un rapporto tra le loro misure espresso da un numero razionale. In quel linguaggio matematico che trovi un po' ostico, si afferma che il lato e la diagonale del quadrato sono incommensurabili.

A: una volta di più mi confermi che i linguaggi specialistici sono di digestione difficile.

M: anche se il lato e la diagonale del quadrato appaiono ai nostri occhi con lo stesso grado di realtà, i pitagorici capirono che non c'erano i numeri per misurarle contemporaneamente. Ecco perché indicarono i nuovi numeri necessari alla bisogna come αλογοι, "inesprimibili". Conformemente alle norme della setta, lo "scandalo logico" dell'esistenza dei numeri inesprimibili", doveva rimanere segreto. Tuttavia, Ippaso di Metaponto, compiendo un terribile tradimento agli occhi della setta lo divulgò. I pitagorici letteralmente si infuriarono per questo e per punirlo del tradimento, gli edificarono una tomba, mentre lui era ancora vivo, per decretarlo metaforicamente morto.

A: tremendi e allo stesso tempo sagaci nella loro vendetta questi Pitagorici.

M: possiamo vedere l'origine degli irrazionali da un altro punto di vista. Abbiamo introdotto il concetto di estensione di un campo numerico per estendere la possibilità di effettuare operazioni, diventa quasi d'obbligo porsi il problema di estrarre la radice quadrata di tutti i numeri razionali. Ma, ad esempio, nel campo razionale non esiste nessun numero il cui quadrato sia 2. I numeri che estendono la possibilità di estrarre radici quadrate dei numeri razionali, li chiameremo irrazionali. Ci accontentiamo di questa estensione di operazioni per introdurre i numeri irrazionali anche se è una grossolana approssimazione e una forte limitazione, per non entrare in sofisticati problemi che hanno dato filo da torcere a più di uno studente nei primi anni del liceo. Non ci diffondiamo ulteriormente neanche sul problema se tali numeri "socializzino" con gli altri, dando per scontata la risposta positiva. La differenza pratica tra i numeri razionali e gli irrazionali è che questi ultimi non si possono rappresentare né sotto forma di frazione, né con un numero finito di decimali, così ad esempio $\sqrt{2}$ = 1,1415... e la successione dei decimali non ha fine.

A: è incredibile come lo spirito dell'uomo abbia sempre spinto sempre più in là le sue capacità speculative.

IMMAGINARI

M: ma i limiti alla possibilità di fare operazioni non sono ancora eliminati del tutto, infatti, neanche con i numeri irrazionali è possibile estrarre la radice quadrata dei numeri negativi, perché per definizione la radice quadrata di un numero è quel numero che moltiplicato per se stesso mi dà il numero dato, e tutti i numeri, positivi o negativi, moltiplicati per se stessi danno un risultato positivo e mai negativo. Per rendere possibile questa operazione, bisogna fare una nuova estensione del campo dei numeri.

A: ma queste estensioni non avranno mai fine?
M: procediamo con ordine e poi risponderò anche a questa tua domanda. I matematici cominciarono a riflettere sulle radici dei numeri negativi fin dai temi di Erone nel I secolo a.C. e di Diofanto. Ma quando si presentarono come soluzione di un'equazione erano dichiarate radici fittizie e l'equazione stessa insolubile. La comparsa di radici di numeri negativi iniziò a farsi più frequente nel XVI secolo quando furono scoperte le soluzioni delle equazioni di terzo grado.
A: vuoi dirmi che anche in questo caso nonostante già i greci avessero fatto qualche indagine su questo problema questi nuovi numeri sono comparsi sulla scena della scienza matematica solo nel XVI secolo con le ricerche dei matematici italiani sulle equazioni, ed anche allora guardati con sospetto?
M: sì, nell'impresa della risoluzione delle equazioni di terzo grado si erano cimentati i matematici greci ed arabi fin dai tempi di Archimede, ma essi erano arrivati a risolvere solo dei casi particolari, senza trovare un metodo generale. Ma prima di venire al contributo dei matematici italiani, vediamo il contesto storico in cui si trovarono ad operare.
A: il XVI° secolo è stato molto burrascoso per l'Italia, contesa tra Francia e Spagna e tuttavia molto prolifico per la matematica se, come mi dici, i matematici italiani di quel periodo hanno dato contributi decisivi alla risoluzione delle equazioni.
M: certamente, esemplare da questo punto di vista la storia di Nicolò Tartaglia (1500-1559). I vari staterelli italiani si schieravano alcuni con i francesi e altri con gli spagnoli nella contesa che aveva trasformato l'Italia in un campo di battaglia. Brescia, contro la volontà dei bresciani, era stata ceduta ai francesi; ma, di fronte a una sollevazione popolare che voleva restituire il controllo della città a Venezia (19 febbraio 1512), l'esercito francese con a capo Gastone di Foix intervenne per sedare la rivolta, mettendo a ferro e fuoco la città. Tartaglia, ragazzino di soli dodici anni, già orfano di padre, si rifugiò con la madre nel Duomo nella speranza di mettersi in salvo; ma i francesi continuarono la battaglia anche nella cattedrale. Tartaglia riportò una profonda ferita alla mandibola ed al palato che gli procurò una balbuzie che non lo lascerà più. Preso in giro dai coetanei con il soprannome di Tartaglia, mantenne questo soprannome anche quando raggiunse la fama. Detto per inciso, Gastone di Foix capo dei francesi e responsabile dello scempio della città, maledetto dai bresciani, morì poco dopo nella battaglia di Ravenna (11 aprile 1512).
A: certo che con questo clima è davvero straordinario che fosse trovato il tempo e la voglia di portare avanti gli studi di matematica.
M: facciamo una piccola digressione su quelli che erano gli studi di matematica di quel periodo. Intorno al 1500, Scipione Dal Ferro (1465-1526), professore di matematica a Bologna, riuscì a risolvere le equazioni cubiche del tipo $x^3+px=q$. Ma non considerava ancora ammissibili le radici complesse ("impossibili" soluzioni, le chiamava lui) che erano sempre in agguato nelle equazioni. Non pubblicò il suo metodo perché a quel tempo le scoperte erano spesso tenute nascoste per poi sfidare i rivali (colleghi) a risolvere lo stesso problema. Tale metodo fu rivelato dallo stesso Scipione Dal Ferro alla fine della sua vita ad un suo allievo, Antonio Maria Fior. Anche Tartaglia, aveva trovato indipendentemente un metodo per risolvere le equazioni di terzo grado del tipo $x^3+px=q$ e $x^3+px^2=q$ con p e q positivi. Nel 1535 fu organizzata una sfida tra Fior e Tartaglia. Ognuno dei due propose all'altro 30 problemi che l'avversario doveva risolvere. Tartaglia riuscì a risolvere tutti e trenta i problemi proposti da Fior, mentre quest'ultimo non riuscì a risolverne neanche uno. La notizia della vittoria di Tartaglia attirò l'attenzione di Girolamo Cardano (1501-1576), il quale, saputo che Tartaglia aveva trovato un metodo generale di risoluzione delle equazioni di 3° grado, dopo molte insistenze convinse Tartaglia a farsi rivelare il suo metodo, in cambio della solenne promessa di non rivelarlo. Ma la debolezza umana segnò ancora un punto a suo vantaggio. Nonostante la promessa, Cardano pubblicò nel 1545 il metodo di risoluzione delle equazioni di terzo grado nella sua opera Ars Magna. Certamente Cardano è uno scienziato molto particolare. Ha lavorato come medico e astrologo per alcuni dei più grandi uomini d'Europa, è stato professore di matematica a Milano, Pavia e

Bologna e fu circondato da ogni sorta di scandali. Esiliato dal mondo accademico, forse perché aveva affermato di aver fatto un oroscopo su Gesù Cristo, finì come astrologo in Vaticano. Nonostante le turbolenze della sua vita, Cardano riuscì ad avere una carriera matematica produttiva. Fu il primo matematico occidentale ad ammettere la possibilità di numeri negativi, e ha continuato a esplorare le loro radici quadrate. Nonostante l'evidenza emergente dai suoi calcoli sulle radici dei numeri negativi, non era ancora pronto a darle credito. Certamente è una ironia della sorte che da un matematico, astrologo e mago sia venuto un aiuto a sfatare le superstizioni della scienza.

A: mi sembra che spesso questa gente abbia aiutato la scienza.

M: procediamo ancora un po' nell'uso dei numeri immaginari. Le formule di Tartaglia evidenziavano come le radici dei numeri negativi fossero utili "formalmente" a trovare le soluzioni reali di un'equazione. Ad esempio, l'equazione $x^3-x=0$ ha evidentemente, le soluzioni x=0, +1, -1; invece la soluzione data dalla formula di Tartaglia è complicata e include $\left(\sqrt{-1}\right)^{\frac{1}{3}}$. Il punto importante è di osservare che, utilizzando il calcolo dei numeri immaginari nella formula, questa dà proprio lo stesso risultato. Magia dei numeri, la pericolosa magia saracena è ancora all'opera.

A: ma se questi numeri risultano così potenti, perché insistere a chiamarli "immaginari"?

M: il termine è un retaggio proprio della diffidenza con cui sono stati considerati dai matematici, da Scipione del Ferro fino a Cartesio che utilizzò per primo il termine "immaginario" ancora nel XVII secolo e ha ben rappresentato la titubanza dei matematici dell'epoca verso questi nuovi numeri che "non dovrebbero esistere". Nel XVII secolo i lavori di Abraham De Moivree di Eulero hanno iniziato a fornire ai numeri immaginari una base teorica cominciando a chiamarli "numeri complessi". Nei secoli successivi, il parere del mondo matematico ha oscillato tra lo scetticismo e il rifiuto, con inserita una sana dose di sconcerto. Gottfried Leibniz, rivale di Newton, nel 1702, chiamava il numero $\sqrt{-1}$ "una risorsa elegante e meravigliosa dell'intelletto divino, una nascita non naturale nel regno del pensiero, quasi un amphibium tra l'essere e non-essere". E così i numeri immaginari hanno fatto il loro ingresso nel mondo matematico. Certo, c'erano ancora gli scettici, come il grande matematico vittoriano Augustus De Morgan che espresse un disprezzo imperioso: "Abbiamo dimostrato il simbolo $\sqrt{-1}$ essere privo di significato in se stesso, contraddittorio e assurdo".

A: mi sei ancora debitore di una risposta.

M: ah, sì? E quale?

A: questa catena di estensioni dei campi numerici non avrà mai fine?

M: è vero; la risposta è che con l'introduzione dei numeri, diciamo pure con termine moderno, "complessi", la catena si interrompe. Dimostrare questa affermazione è abbastanza complicato. Possiamo tuttavia osservare che a questo punto tutte le operazioni elementari, cioè addizione, sottrazione, moltiplicazione, divisione, radici, potenze, sono sempre possibili, con l'eccezione..

A: lo so, della divisione per zero!

INFINITO

M: un simbolo molto importante in matematica è quello di infinito che si indica con un 8 che si è sentito male e che giace rovesciato su un fianco, così **∞.**

A: noto che non hai detto "numero, ma "simbolo", perché?

M: perché è un concetto molto particolare. Per immaginarlo bisogna pensare che dato un qualsiasi numero grande, ∞ è sempre più grande. Ad esempio io penso a un miliardo di miliardi, ma ∞ è più grande, ma anche se penso ad un miliardo di miliardi di miliardi, ∞ è ancora più grande. Per giunta, non socializza con gli altri numeri, non entra cioè nelle operazioni con le

stesse proprietà, infatti per la descrizione stessa che ne abbiamo appena dato, se viene sommato a qualsiasi numero da sempre se stesso, così ∞ + 2=∞ ma anche ∞ + 3=∞ e così ∞ + 5=∞ in queste condizioni è ovvio che il nostro ∞ non è un numero come tutti gli altri; e se fosse usato così ne deriverebbe 2=3=5, cioè tutti i numeri sarebbero uguali e uguali a zero.

A: a questo punto mi è chiaro, ma allora come entra nella matematica?

M: possiamo farci un'idea più matematica del suo significato, rispetto a quanto abbiamo visto sopra, considerando la successione di divisioni
1:0,1; 1:0,01; 1:0,001; ... con la successione dei loro risultati 10; 100; 1000; ... si vede che quando il divisore diminuisce, il valore della frazione aumenta.

A: vuoi dire che se il denominatore è 0, il valore della frazione è ∞?

M: attenzione! Ti avevo anche detto che non si può dividere per 0.

A: è vero, me ne stavo dimenticando.

M: appunto il fatto che il denominatore non può mai essere 0 impedisce a questo nuovo simbolo di essere un numero. È tuttavia un simbolo molto utile. Voglio parlarti invece delle operazioni che si ripetono infinite volte.

A: ma esistono?

M: certo, tanto che il filosofo Zenone di Elea (VI–V secolo a.c.), fondatore della dialettica secondo Aristotele, avrebbe ideato quaranta paradossi – cioè argomenti logicamente validi – le cui conclusioni vanno contro (para=παρα) l'opinione comune o evidenza (doxa=δοξα) e servono per mettere in risalto difetti nella logica. Un bel tipo questo Zenone, di lui si racconta che abbia cercato di contrastare un tiranno con ogni mezzo, persino a prezzo della propria vita. Quando fu arrestato, secondo i racconti, fu sottoposto a tortura perché rivelasse i nomi dei suoi amici cospiratori. Subdolamente denunciò persone vicine al tiranno che furono così messe a morte. Subito dopo affermò di voler svelare un segreto all'orecchio del tiranno, e quando questi gli fu vicino, gli addentò un orecchio con grande forza nel tentativo di staccarglielo. Lasciò la presa solo quando le guardie ve lo costrinsero con la forza. Infine si mozzò la lingua con i suoi stessi denti, per evitare di parlare sotto tortura, e ne sputò la punta in faccia al tiranno stesso. È proprio un personaggio così che può creare paradossi. Il suo più famoso coinvolge infinite operazioni: è noto come il paradosso di Achille e la tartaruga. Questo afferma che se Achille (detto "pie' veloce") venisse sfidato da una tartaruga nella corsa e le concedesse un piede di vantaggio, egli non riuscirebbe più a raggiungerla, dato che Achille dovrebbe prima raggiungere la posizione occupata inizialmente dalla tartaruga che, nel frattempo, sarà avanzata raggiungendo una nuova posizione di vantaggio; quando poi Achille raggiungerà la nuova posizione, ancora la tartaruga sarà avanzata di un po', precedendolo ancora. Questo stesso discorso si può ripetere per tutte le posizioni successivamente occupate dalla tartaruga e così la distanza tra Achille e la lenta tartaruga, pur riducendosi sempre, non arriverà mai ad essere pari a zero. Quindi Achille non raggiungerà mai la tartaruga.

A: mi sembra di aver capito che il difetto logico in questo ragionamento consiste nel credere che, dopo un numero infinito di passi, continui a ripetersi ciò che succede in un numero comunque alto, ma finito di passi.

M: proprio così: si può ripetere cento volte, mille volte, un milione di volte i passaggi visti sopra ed effettivamente la tartaruga sarà sempre in vantaggio; ciò che Zenone non poteva sapere, cioè come trattare processi infiniti, è diventato possibile capirlo solamente con la scoperta dell'analisi infinitesimale da parte di Leibniz e Newton più di due millenni dopo.

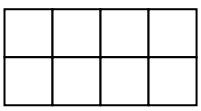
A: è veramente incredibile che sia trascorso così tanto tempo prima di scoprire questo punto sui processi infiniti.

M: aggiungo che oltre alle quattro operazioni dell'aritmetica ne esistono altre. Ad esempio i logaritmi, che hanno agevolato i calcoli dei matematici e degli astronomi, prima dell'introduzione dei calcolatori elettronici. Non mi addentro nel loro studio, mi basta citare che con i logaritmi le moltiplicazioni si riducono a addizioni e le divisioni a sottrazioni.

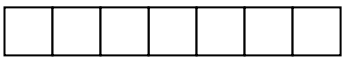
A: beh, mi sembra che in mancanza di ausili di calcolo, sia una bella cosa fare somme invece che moltiplicazioni, ma non è che si è semplicemente spostato il problema dalla esecuzione di moltiplicazioni a calcolare i logaritmi?
M: osservazione pertinente; perché ciò che dici sarebbe molto vero, anzi, calcolare il logaritmo sarebbe più difficile che eseguire moltiplicazioni, per complicate che siano. Il fatto è che i logaritmi dei numeri sono stati calcolati e messi a disposizione di tutti tramite tavole pubblicate.
A: ah, c'è il trucco allora.
M: certamente. Ma adesso mi voglio soffermare sulla figura del loro inventore Lord John Napier (Merchiston Castle, 1550 – Edimburgo, 4 aprile 1617) barone di Merchiston presso Edimburgo. Quando il suo castello non era sotto assedio e non era impegnato a combattere gli invasori in campo aperto o i vicini nelle corti di giustizia, si occupò di arti occulte, progettò congegni per navigare sotto l'acqua e un carro da guerra rotondo fatto di metallo a prova di doppio moschetto, ipnotizzò piccioni, cercò con la stregoneria tesori nascosti, dedusse – in 36 serrate proposizioni di "algebra apocalittica" che il Giudizio Universale sarebbe caduto tra il 1688 e il 1700; e inventò appunto i logaritmi. Nei primi del XVII secolo i suoi vicini sparsero la voce che fosse alleato con il demonio. Certo che l'abitudine di vestirsi di nero da capo a piedi, e l'aver scelto come fedele compagnia un gallo color dell'ebano, non contribuirono a dissipare simili voci. La diffusione del calcolo mediante logaritmi costituisce un fatto di grande importanza storica. Mediante i logaritmi Keplero riuscì a elaborare i dati astronomici fino alle considerazioni che gli consentirono di formulare le sue leggi, con le conseguenze sullo sviluppo dell'astronomia e della fisica che portarono alla formulazione di Newton delle leggi della meccanica. Come Nepero aveva previsto, i calcoli mediante i logaritmi hanno consentito di ridurre vistosamente i tempi dei calcoli, fino a far dire a Laplace che Nepero aveva "raddoppiato la vita degli astronomi". I calcoli mediante i logaritmi hanno contribuito allo sviluppo di una mentalità quantitativa anche nelle attività tecnologiche e finanziarie e hanno avuto un'influenza molto rilevante sullo sviluppo dei commerci e delle attività imprenditoriali e sulla nascita del mondo industriale a partire dalla seconda parte del XVII secolo.

NUMERI PRIMI

M: non vorrei lasciare l'impressione che le ricerche sui numeri siano divertimenti notturni di persone insonni. Ma a volte passa così tanto tempo tra la fase speculativa e un'eventuale applicazione da lasciar credere inutili questi studi; un interessante esempio di questa situazione sono le ricerche sui numeri primi di Fermat.
A: ho un vago ricordo, dai miei studi di ragazzo, della scomposizione dei numeri in fattori primi per la ricerca del minimo comune multiplo e massimo comun divisore. Continua.
M: i numeri primi sono quei numeri divisibili solo per se stessi e per l'unità, Così ad esempio 2 è primo, 3 è primo, 4 non è primo perché è divisibile per due, 14 non è primo perché è divisibile per 2 e per 7, etc. Un altro modo di visualizzare i numeri primi è di pensare che non possono essere l'area di un rettangolo o di un quadrato con i lati interi (e diversi da 1). Nel disegno qui sotto un rettangolo di area 8 può avere i lati 2 e 4 perché 8 non è primo e 2*4=8



Ma se l'area è 7, l'unica costruzione possibile è proprio il rettangolo di lati 1 e 7, così 7 risulta un numero primo



sembra semplice, no?

A: beh, certo, sono coinvolte solo operazioni semplici.

M: e invece sui numeri primi sappiamo pochissimo, ad esempio non sappiamo se esiste una legge in base alla quale si susseguono i numeri primi, dato che i numeri primi sono infiniti. Questa scoperta risale già a Euclide e non dovrebbe essere difficile da capire. E' una di quelle dimostrazioni per assurdo di cui abbiamo parlato inizialmente. Supponiamo che ci sia un numero finito p_1, p_2, p_3, ... e p_n di numeri primi. Consideriamo il loro prodotto $P=p_1*p_2*p_3*...p_n$ e il numero P+1. Esso non è divisibile per p_1, p_2, p_3, ..., p_n perché 1 non è divisibile per p_1, p_2, p_3, ..., p_n, quindi P+1 è primo contro l'ipotesi che i soli numeri primi fossero p_1, p_2, p_3, ..., p_n.

A: molto fine il ragionamento**, ipotizzare che solo** p_1, p_2, p_3, ..., p_n siano primi porta alla conseguenza assurda che **non solo loro sono primi**, ma che lo sia anche il loro prodotto P aumentato di 1. Mi pare che così abbiamo anche trovato un sistema per scoprire nuovi numeri primi, a partire dai pochi che io conosco (1,2,3,5,7)!

M: Bravo! Purtroppo il sistema non ci serve a trovare i numeri primi in successione, altrimenti avremmo sicuramente meritato il Premio Nobel. Ma proseguiamo il nostro discorso.

Diamo per scontata l'unicità della fattorizzazione, e cioè che valga il teorema fondamentale dell'aritmetica: per ogni numero naturale diverso da 1 esiste una ed una sola scomposizione in prodotto di numeri primi (fattorizzazione), salvo l'ordine dei fattori. E ciò fa dei numeri primi i mattoni costitutivi di tutti i numeri, un po' come gli atomi per la materia.

A: sì, recuperando nel cestino della mia memoria, mi risulta ad esempio che 76=4*19, e 54=2*3*3*3.


Pierre de Fermat

M: perfetto. Come nostra abitudine parliamo un pò dell'autore elle ricerche sui numeri primi, per illustrare un esempio di udi che sono stati utilizzati soltanto dopo secoli. Pierre de ermat nacque a Beaumont-de-Lomagne il 17 agosto1601 e orì a Castres il 12 gennaio 1665. Era avvocato al Parlamento Tolosa. Lavorava duramente e scrupolosamente ma onostante ciò nel tempo libero si occupava di letteratura ompose persino alcuni versi), e soprattutto di matematica. er questo Fermat è stato chiamato "Il principe dei dilettanti" … el 1648 divenne Consigliere del Re al Parlamento di Tolosa e antenne tale carica per i successivi 17 anni. Fermat è famoso er la sua congettura che afferma: non esistono soluzioni intere ositive all'equazione

$$x^n+y^n=z^n \text{ se } n > 2 .$$

ongettura nota anche come ultimo teorema di Fermat, e che è masta non dimostrata per più di 300 anni fino al 1994. E' facile v e c'è: è la terna pitagorica 3, 4, 5 ($3^2+4^2=5^2$). La dimostrazione g a Andrew Wiles nel 1994. Una piccola curiosità al riguardo è che Fermat era solito annotare le sue osservazioni a margine dei libri. In questo caso annotò: "ho dimostrato..., ma la dimostrazione non sta nel margine". La dimostrazione di Wiles però utilizza strumenti matematici moderni che Fermat non poteva assolutamente conoscere.

A: ma Fermat l'avrà dimostrata davvero?

M: chi lo può dire? Il campo in cui Fermat fu più attivo è sicuramente la teoria dei numeri; si può infatti considerare uno dei fondatori di questa disciplina. Espresse molte delle sue scoperte in forma di congettura, in altre parole senza fornire una dimostrazione, molte di queste furono trovate nel XVIII secolo da Eulero, mentre per altre (ad esempio quello abbiamo appena citato, noto come ultimo teorema di Fermat), si dovrà aspettare ancora oltre.

A: l'attenzione dedicata alla teoria dei numeri non è un po' sprecata, tanto più che hai già evidenziato che è uno dei campi più difficili della matematica?

M: quanto a questo non si può mai dire se una ricerca è utile o meno. Stavo appunto per raccontarti la circostanza che sono passati 3 secoli prima che le ricerche di Fermat,

dall'universo dei divertimenti puramente speculativi, trovassero utilizzazione pratica nel mondo dell'economia reale.

A: mi sembra che sia successo più di una volta nella storia della scienza che ricerche assolutamente teoriche si siano dimostrate molto utili in tempi più o meno lontani. Ho sentito dire che il mondo degli atomi è governato da teorie che si basano sui nostri numeri "immaginari", e così tutte le applicazioni che sono derivate da queste conoscenze, come i semiconduttori che si trovano in tutti gli apparati elettronici, i telefonini,... ecc.

M: è proprio così, come vedi non sono poi così "immaginari". Ritorniamo all'utilità delle ricerche di Fermat sui numeri primi. Cominciamo con una piccola magia. Seguimi bene che è un argomento più complicato di quanto abbiamo visto finora. Consideriamo l'orologio; sul suo quadrante ci sono 12 ore. Lo scorrere delle ore è contrassegnato dal fatto che completato il ciclo di 12 ore, con il 13 si ricomincia da 1, quindi 13 corrisponde a 1, 14 corrisponde a 2, 15 a 3 fino a che dopo 24 ore con il 25 si ritorna a contare da 1. In altre parole è come dividere per 12 l'ora segnata e considerare il resto. Infatti 1 è il resto della divisione di 13 per 12, ma anche di 25:12, mentre 2 è il resto di 14:12 ecc.. Semplifichiamo, pensando ad un orologio con 5 ore sul quadrante: analogamente questo implica che il 6 corrisponde a 1, 7 a 2 ecc. Questo ci permette di capire la piccola magia che mi appresto a fare. Consideriamo un orologio con 5 ore sul suo quadrante. La magia consiste in questo: se su questo orologio si prende un numero qualunque ad esempio 2 e lo si moltiplica per se stesso 5 volte, sul quadrante di questo orologio compare ancora 2. Possiamo evidenziare la successione di operazioni sul nostro orologio; il primo passo è ovvio, il secondo passo, 2x2=4 corrisponde ancora a 4; nel terzo passo, prendo il risultato del passo precedente, cioè 4, e lo moltiplico ancora per 2, il risultato 8, sull'orologio con 5 ore corrisponde a 3, lo prendo e di nuovo lo moltiplico per 2, il risultato sull'orologio è 1 e finalmente al quinto passo, ricompare magicamente 2

N° di moltiplicazioni		Risultato	Orologio di 5 ore
2	2	2	*2*
2x2	*2*x2	4	*4*
2x2x2	*4*x2	8	*3*
2x2x2x2	*3*x2	6	*1*
2x2x2x2x2	*1*x2	2	**2**

Fermat ha trovato un teorema, noto come Piccolo Teorema di Fermat che dà veste scientifica a questo fatto, e che ci fornisce la chiave per sapere se e quando questa magia funziona: preso un numero qualunque, se lo si moltiplica per se stesso **un numero primo p di volte**, su un orologio con p ore, come per magia all'ultimo passo si ritrova il numero di partenza. Più formalmente si direbbe che:

se p è un numero primo e a un numero intero qualunque, allora $a^p \equiv a \pmod p$.

A: cioè se io prendo 3 e lo moltiplico per se stesso 5 volte ottengo di nuovo 3 su un orologio con 5 ore?

M: esattamente.

A: vediamo!

N° di moltiplicazioni		Risultato	Orologio con 5 ore
3	3	3	*3*
3x3	*3*x3	9	*4*
3x3x3	*4*x3	12	*2*
3x3x3x3	*2*x3	6	*1*
3x3x3x3x3	*1*x3	3	**3**

Stupefacente e davvero magico il comportamento dei numeri primi. Ma tu volevi farmi un esempio in cui si vedeva l'utilità dei numeri primi, e questo cosa c'entra?

CODICI DI SICUREZZA PER LA NAVIGAZIONE IN INTERNET

M: eccoci al punto. Da sempre l'uomo ha sentito il bisogno di comunicare messaggi segreti, cioè destinati a essere letti solo da specifiche persone. **Le ricerche su questo comportamento degli orologi con un numero primo di ore hanno fornito il sistema crittografico che ha permesso l'enorme sviluppo delle transazioni commerciali su internet.** La crittografia (dal greco κρυπτω γραφη = nascondere scrittura) è la scrittura di un messaggio tramite una chiave, in modo che sia leggibile solo dal destinatario. Tradizionalmente la chiave per la codifica e la decodifica del messaggio era la stessa. Un esempio semplice è il codice di Cesare, in cui la chiave consisteva nel sostituire una lettera dell'alfabeto con quella che la seguiva di un numero fissato di posti. Ad esempio se la chiave crittografica era 5, la "a" diventava "f", la "b" diventava "g" ecc. pertanto il messaggio "lago" era trasmesso come "qfnt". Ovviamente questo tipo di crittografia richiede un accordo preventivo tra i corrispondenti sulla chiave da utilizzare; la possibilità che la chiave sia violata e le difficoltà logistiche aumentano con il numero dei corrispondenti. Così durante la seconda guerra mondiale i Tedeschi avevano messo a punto una macchina, dal nome espressivo di "Enigma", che richiedeva a Berlino di mandare numerosi agenti che consegnassero ai capitani degli U-Boot i libri con la descrizione dettagliata delle regolazioni da apportare giornalmente alla loro macchina per la codifica e la decodifica dei messaggi. È evidente che il problema logistico diventa insuperabile se lo scambio dei messaggi coinvolge i milioni di persone che fanno transazioni on line sul web. Nel 1976 un articolo di Diffie e Hellman, due matematici dell'Università di Stanford, suggeriva la possibilità teorica di usare due chiavi diverse per la codifica e la decodifica dei messaggi, come se si trattasse di una porta che si chiude con una chiave e si apre con un'altra. Il primo importante risultato sarebbe stato che l'intercettazione della chiave di codifica non avrebbe comunque consentito la lettura del messaggio. Ron Rivest del Dipartimento di Informatica del MIT, che stava facendo ricerche sulla crittografia, venuto a conoscenza dell'articolo di Diffie e Hellman, cominciò ad arrovellarsi sul tema. Parlando con due colleghi del Dipartimento di Matematica, Adi Shamir e Leonard Adleman, gli venne in mente il Piccolo Teorema di Fermat, già visto, nella versione riveduta di Eulero:

in un orologio con N di ore, dove N è il prodotto di due numeri primi N=p*q, un numero qualunque moltiplicato per se stesso (p-1)*(q-1)+1 volte è ancora il numero di partenza.

A: una forma leggermente più complicata di quello che abbiamo visto prima.

M: E qui intervenne il miracolo dell'utilizzo pratico dei divertimenti notturni sui numeri di Fermat; il teorema di Fermat infatti è della metà del 1600, ma la sua utilizzazione è arrivata solo nel 1977 con queste ricerche di Rivest (più di 300 anni dopo). La crittografia che ne è derivata, è nota come algoritmo RSA, acronimo dei nomi degli inventori (brevettato), Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman. Rivest capì che poteva utilizzare il teorema di Fermat-Eulero per far sparire il messaggio segreto e per farlo riapparire come per magia. Cifrare un numero di carta di credito è come un trucco con le carte. In questo caso il mazzo ha un numero enorme di carte, così grande che sono necessarie più di cento cifre per scriverlo, un numero superiore a tutti gli atomi dell'universo che è dell'ordine di 80 cifre (10^{80}). Il numero della carta di credito è una carta del mazzo. Il cliente pone la sua carta di credito in cima al mazzo, il web mescola il mazzo e l'ubicazione della carta del cliente sembra andare completamente perduta. Un hacker si trova ad affrontare il compito impossibile di estrarre quella singola carta dal mazzo. Il sito web tuttavia conosce un trucco ingegnoso. Grazie al piccolo teorema di Fermat, è in grado di far riapparire la carta sulla cima del mazzo, dopo un'altra rimescolata. Questa seconda sequenza di scozzate è la chiave segreta nota soltanto all'azienda a cui appartiene il sito. Quando il cliente piazza un

ordine, l'azienda gli comunica il numero N di ore del calcolatore a orologio da usare. Per questo l'azienda prende due grandi numeri primi p e q dell'ordine di 60 cifre ciascuno e li moltiplica ottenendo N=p*q dell'ordine di 120 cifre. Il numero N è pubblico, mentre i due numeri p e q sono segreti; questi numeri sono gli ingredienti della chiave che è utilizzata per decodificare il numero della carta di credito del cliente. Poi il cliente riceve un secondo numero E, pure pubblico e invia sul web il numero della sua carta di credito elevato a E, operazione ovviamente da farsi sul calcolatore di N cifre. Con questo passaggio il numero della carta di credito è scomparso, ma Rivest sapeva che il teorema di Fermat garantiva l'esistenza di un numero magico di decodifica, D. L'azienda moltiplica il numero cifrato della carta di credito per se stesso D volte e magicamente il numero della carta di credito riappare. L'essenza del metodo è che il numero D si ricava a partire da p e q che, ricordo, sono segreti mentre N ed E sono pubblici. Quindi un hacker che volesse violare il numero della carta di credito, dovrebbe trovare p e q che sono i fattori primi di N. La sicurezza del sistema dipende dalla mancanza di un algoritmo per trovare i fattori primi di un numero in tempi accettabili. L'algoritmo RSA rappresenta un grande successo dell'aritmetica: paradossale, tuttavia, che la segretezza che l'algoritmo RSA promette (e mantiene) sia garantita proprio da una sconfitta della matematica: il non saper fattorizzare in tempi ragionevoli un numero che è il prodotto di due grandi numeri primi. Per dimostrare la sicurezza del loro algoritmo (e sotto sotto per farne pubblicità), Rivest, Shamir, Adleman offrirono un premio di 100 dollari a chi avesse trovato i fattori primi di un numero di 129 cifre, noto ormai come RSA 129, costruito da loro stessi come prodotto di due numeri primi. Più tardi la commercializzazione di RSA li fece diventare ricchi e offrirono premi ben più consistenti per la fattorizzazione di numeri di 155, poi di 174 cifre. Ci vollero 17 anni perché fossero trovati i fattori primi di RSA 129, tempo sufficiente in ogni modo per la scadenza della carta di credito crittografata. Oggi la società RSA raccomanda N di almeno 230 cifre, ma le agenzie governative utilizzano anche orologi con più di 600 cifre. L'algoritmo RSA non è l'unico metodo di crittografia, ce ne sono altri come l'algoritmo DES o altri ancora, che hanno l'obiettivo di ridurre l'oneroso impegno di calcolo dell'algoritmo RSA, che però resta l'algoritmo più sicuro. Un difetto di RSA, se così si può dire, è la mole dei calcoli aritmetici necessari, che per numeri grandi si traduce in una lentezza della operatività; poiché la codifica e la decodifica consistono essenzialmente in un elevamento a potenza in un'aritmetica finita, diventa essenziale disporre di algoritmi veloci per il calcolo delle potenze sugli orologi con N ore. RSA resta perciò un metodo di cifratura molto più lento (circa mille volte!) degli altri algoritmi; per questo motivo RSA è di solito utilizzato solo per trasmettere la chiave segreta di un DES (o altro cifrario simmetrico) e il messaggio vero e proprio è trasmesso appunto con il DES.

CONCLUSIONE

A: quanto mi hai fin qui raccontato, pur nella sua logica razionalità, ha tuttavia una sua suggestiva poeticità. Questi ragionamenti sui numeri, mi fanno sorgere in mente dei quesiti: il numero nasce per le esigenze dell'uomo - è per così dire una creatura dell'uomo - o si deve considerare un ente che ci deriva dall'esterno? La matematica allora è un'attività creativa o di scoperta? Ha funzione conoscitiva, o piuttosto "economica", per classificare gli oggetti nella maniera più conveniente? Per dirla con Croce, sono veri concetti o pseudoconcetti?
M: ti dirò che spesso la riflessione dei matematici ha oscillato tra le due alternative.
L. Kronecker (1823 -1891) indicava il terreno sicuro per la costruzione dell'intero edificio della matematica, distinguendo tra l'opera dell'uomo e quella di un ente superiore esterno con queste parole:
...*Dio creò i numeri naturali; tutto il resto è opera dell'uomo...*
Un grande matematico inglese del primo novecento, G. H. Hardy, espresse perfettamente questa tensione fra creazione e scoperta, affermando: " ritengo che la realtà matematica si situi

al di fuori di noi, e che la nostra funzione sia di scoprirla o di osservarla, e che i teoremi che dimostriamo e descriviamo con magniloquenza come nostre "creazioni" non siano altro che le note delle nostre osservazioni". Ma in altri momenti fa una descrizione più artistica del processo di fare matematica. Scrisse in *Apologia di un matematico* "La matematica non è una disciplina contemplativa, ma creativa". Merita osservare che Graham Greene ha posto questo libro accanto ai taccuini dello scrittore inglese Henry James - l'autore di "Ritratto di Signora, I Bostoniani, ecc. - come la migliore descrizione di cosa significhi essere un artista creativo.

APPENDICE

Qui sotto riporto una piccola spiegazione di come si generano le chiavi di codifica e decodifica per chi volesse provare

- si scelgono due numeri primi "p" e "q" molto grandi
- p ≠ q (p diverso da q)
- N = p*q
- f(N) = (p-1)*(q-1)
- si sceglie un numero intero naturale "E" minore di f(N)e primo con f(N)
- si calcola "D" l'inverso di "E", lo si ricava da E*D=1 mod(f(N), cioè su un orologio di (p-1)*(q-1) ore
con questi elementi si cifra il testo "t" ottenendo C = t^E mod N e si decifra con "D" t = C^D mod N

Esempio
siano
p=5, q=11
N=pq=5∗11=55
f(N)=(p-1)(q-1)=40
Si calcola il più piccolo intero **E** che sia primo con f(N) cioè con 40 (non abbia divisori in comune, in altre parole MCD(E, f(N)) = 1). Il numero **E** è la seconda chiave pubblica.
E=3 infatti MCD(2,40)=2, mentre MCD(3,40)=1
Si deve ora trovare **D** tale che **E**∗**D=**1 sull'orologio di 40 ore; gli algoritmi per questo calcolo non sono molto efficienti, e sono il motivo della lentezza del metodo RSA, diamo qui direttamente il risultato **D**=27.
Potete provare a calcolarlo voi per tentativi, ponendo E = 3 e D = 1,2,3,…fino al valore che fornisce E ∗D = 1 (mod 40).
Allora, per trasmettere il messaggio t=**7**, si calcola C = t^E (mod N) = 7^3 (mod 55) = 343 (mod 55) = 13; il numero da trasmettere è quindi **13**. Sul web quindi passa il numero 13 che non ha nessuna parentela con il messaggio reale **7**, per la decodifica si usa la chiave di decifrazione **D**, segreta, che permette di recuperare t grazie alla formula t = c^D (mod N); nel nostro caso t = c^D (mod N) = 13^{27} (mod 55) = **7** che è miracolosamente riapparso.
Già con questo esempio con numeri piccoli (!), si vede come i calcoli coinvolti siano piuttosto pesanti, anche se solo elevamenti a potenza. Immaginate cosa possono diventare se i numeri sono di 100 o 200 cifre e fino a 600 cifre. Se un hacker volesse scoprire t, numero della carta di credito, dovrebbe trovare i fattori primi di **N**, cioè p e q, cosa impossibile in tempi ragionevoli, con gli strumenti tecnici e matematici attuali.