# QUEL CHE RESTA DA SCOPRIRE IN MATEMATICA

## Con una nota sui “problemi del Millennio”.

**2. Edizione**

DE

La matematica non è come le altre scienze, e infatti certi puristi dubitano che sia una scienza.
Il matematico non ha bisogno di guardare fuori della finestra di casa sua. Non ha bisogno di microscopi o telescopi o acceleratori di particelle o strumenti per la risonanza magnetica nucleare o satelliti artificiali. In linea di principio ha bisogno soltanto del suo cervello. Poi si trova che carta e matita e magari una poltrona comoda possono aiutare.
In realtà, oggi può aiutare anche un buon calcolatore elettronico che possa fare in poco tempo le operazioni, anche formali, necessarie alla ricerca matematica. Esistono per questo diversi programmi o linguaggi, di varia potenza, taluni anche sotto forma di applicazioni da scaricare sul cellulare.

Ma di che cosa si occupa il matematico? O, se vogliamo, che cos’è la matematica? Ecco una domanda interessante, a cui si è risposto anche in vari illustri libri, tra cui il primo che viene in mente è “Che cosa è la matematica?” di R. Courant e H. Robbins, edizione Inglese del 1941.

Un matematico dell’Ottocento, L. Kronecker, disse: *“Il buon Dio fece i numeri interi; tutto il resto è opera dell'uomo”.* Anche lui aveva le sue fissazioni, ma qualche altro matematico aggiunse che l’Uomo si limitò a creare i numeri Razionali, mentre fu il Maligno ad inventare i numeri irrazionali (in tal caso, quale ancor più malefica potenza avrebbe inventato i numeri complessi?) Ma torniamo a noi: potremmo dunque dire che il matematico si occupa, da vicino o da lontano, dei numeri interi, cercando di ampliarne la famiglia e scoprire le loro proprietà, e non ne parliamo più. Però, non credo che possiamo accettare questa risposta senza pensarci un momento.

Se tutti i risultati della matematica oggi noti stanno in cento volumi, ciascuno di mille pagine, ogni neonato della specie umana parte dal frontespizio del primo volume; diversi miliardi di bipedi umani sono fermi a pagina dieci; lo studente che ha concluso le scuole medie è a pagina venti, il liceale (scientifico) ha studiato qualche capitolo del primo volume, uno studente che abbia concluso il biennio di una facoltà di scienze Italiana è da qualche parte nel secondo-quarto volume. Tolti allora i primi quattro volumi, che cosa è scritto nei successivi novantasei volumi? Si tratta in massima parte di dimostrazioni di teoremi che riguardano diversi campi della matematica, che hanno i nomi più astrusi. Tutti, avrebbe detto quel matematico, variazioni più o meno lontane dal tema dei numeri naturali.

E qui sorgono due domande.
***1) Veramente i numeri (almeno quelli naturali) esistono all'infuori dell'uomo o li abbiamo costruiti noi col nostro pensiero?*** Se non ci fossero uomini, i numeri naturali esisterebbero lo stesso, in attesa di una specie razionale, per esempio società di scarafaggi, che li voglia studiare? Per esempio, il contare sembra essere una necessità fondamentale degli esseri viventi. Sappiamo che, ad esempio, certe rane "contano" fino a 10, e i lupi pare che contino meglio dei cani (come se l'essere stati addomesticati ne avesse ridotto le capacità aritmetiche). Lo scimpanzé Ai in Giappone contava e usava un apposito PC. In quanto al pappagallo Alex contava fino a 6. Per un paragone, si noti che la lingua Tupì-Guarany aveva all'arrivo dei missionari bianchi nomi per i numeri solo fino a quattro...
Niente paura, alla domanda (1) , detta "questione ontologica", tanto per complicare le cose, si può rispondere sì o no, e ciascuna delle risposte ha un gran numero di seguaci che hanno passato la loro vita a studiare la risposta, senza ovviamente convincere nessuno del campo avverso. Grosso modo, in maggioranza i filosofi (che hanno per la matematica in genere un amore platonico, cioè l'amano, ma non la studiano) dicono che i numeri li abbiamo fatti noi, mentre i matematici (quelli che sui numeri ci lavorano sul serio) in maggioranza dicono che i numeri esistono indipendentemente da noi. Avrebbero naturalmente un'esistenza speciale: i numeri sono evidentemente eterni, incorruttibili, sono in ogni luogo. Tutti possiamo fare contemporaneamente l'operazione 2 x 3, e non dobbiamo metterci in fila perché il vicino di banco ci sta usando il tre.

Abbiamo allora un’altra domanda.
2) Tutte le scienze naturali sono, per così dire, finite, ***esauribili***. Possiamo pensare che nel giro di un *milione* di anni avremo catalogato tutte le specie viventi, tutti i genomi, tutti i composti chimici, tutte le stelle dell’universo e probabilmente tutte le particelle subnucleari.
Ma prima che il Sole diventi una gigante rossa devono passare cinque o sei *miliardi* di anni. Che faranno gli scienziati in quei miliardi di anni? Abbandoneranno la scienza? Guarderanno la 1 678 456 349 edizione della coppa del mondo, o la 2 347 685 301 puntata di “Tempesta d’Amore”?
Esiste un libro intitolato “Quello che resta da scoprire”, che cerca di divinare quello che resta da scoprire nelle varie scienze. Interessante.

A noi però interessa la matematica: ***“Quale può essere il futuro della matematica?”*** Adesso propongo i termini del problema e chi ci si vuol cimentare darà la risposta. Ma bisogna anzitutto ricordare che, lasciando da parte i primordi semi-umani indicati, la matematica è con noi da forse cinquemila anni, i Greci hanno dato un grande contributo 2000 anni fa, i matematici Italiani del ‘500 un altro, ma la maggior parte delle scoperte è stata fatta negli ultimi 250 anni.

E qui abbiamo una sorpresa: nel 1931 Kurt Gödel propose due teoremi (teoremi di incompletezza) che da allora dominano la logica matematica o, se vogliamo, i fondamenti della matematica. Incidentalmente, Gödel dimostrò strada facendo che l'aritmetica è lungi dall'essere il campo più umile della matematica. Ben più umile la geometria. Al contrario, (quasi) ogni teorema della matematica più astrusa può esser trasformato in un teorema di aritmetica, e gli si possono applicare le conclusioni di Godel. Si veda in **Appendice I** un esempio di come un assioma o teorema possa essere aritmetizzato, cioè trasformato in un numero intero.

**Enunciato e pochi commenti sui teoremi di Gödel**
*(Lettura sconsigliata a chi non è in cerca di forti emozioni)*

Ora enuncio in modo formale (tratto da Wikipedia, a cui rinvio volentieri) i due teoremi di Gödel e poi li commento, entro i miei modesti limiti, non tanto i teoremi, che non sono in grado di dimostrare, quanto alcune delle loro (abbastanza controverse) conseguenze.

***Primo teorema:***

*1) In ogni Teoria matematica sufficientemente espressiva da contenere l'aritmetica, esiste una formula F tale che, se la teoria è coerente, allora né F né la sua negazione Non-F sono dimostrabili nell'ambito della Teoria.*

Qui Gödel dimostrò strada facendo che l'aritmetica è lungi dall'essere il campo più umile della matematica. Ben più umile la geometria. Al contrario, (quasi) ogni teorema della matematica più astrusa può esser trasformato in un teorema di aritmetica, e gli si possono applicare le conclusioni di Godel. Si veda in **Appendice I** un esempio di come un assioma o teorema possa essere aritmetizzato.

Il primo teorema dunque ci dice che in una teoria che risponde a date (non molto restrittive) condizioni, prima o poi ci si imbatte in una proposizione di cui non si può dire se sia vera o sia falsa, cioè una proposizione ***indecidibile.***

Una costruzione assiomatica non può soddisfare contemporaneamente le proprietà di coerenza e completezza. Per ***"coerenza"*** si intende qui che la stessa teoria non può dimostrare come vere un'affermazione e la sua contraria (anche una sola). Per "***completezza"*** si intende che la teoria non contiene verità non dimostrabili.

***Secondo teorema:***

2) *Sia* **T** *una teoria matematica sufficientemente espressiva da contenere l'aritmetica: se* **T** *è coerente, non è possibile provare la coerenza di* **T** *all'interno di* **T**.

O anche: *Nessun sistema, che sia abbastanza espressivo da contenere l'aritmetica, e coerente, può essere utilizzato per dimostrare la sua stessa coerenza.*

Il risultato dei due teoremi di Gödel fu una serie interminabile di discussioni, di interpretazioni, di fraintendimenti, ciascuno dei quali ha i suoi sostenitori. Per cui, quello che sto per scrivere troverà senz'altro chi non è d'accordo, e sperabilmente anche che è almeno parzialmente d'accordo.

Ma pensiamo bene alle conseguenze: se tutta la matematica potesse essere aritmetizzata, *allora potremmo pensare che sia possibile costruire una macchina che lavori sui numeri naturali e sia in grado di dimostrare tutti i teoremi di tutta la matematica.* Si inserisce un programma che contiene i postulati e le definizioni, si immettono i dati del teorema da dimostrare, si gira la manovella, e – a suo tempo – la macchina si arresta consegnandoci il suo editto: il teorema è vero oppure è falso.
***Turing dimostrò che invece questa è proprio una di quelle proposizioni indecidibili (cioè di cui non si può dimostrare se siano vere o false)***. La nostra macchina può essere posta davanti ad un problema che la constringe a non fermarsi mai, perché può non giungere mai ad una risposta ("problema dell'arresto").

Dunque un'interpretazione del primo teorema di Gödel è che **non esiste** un sistema completo di definizioni e regole (postulati o assiomi), che naturalmente siano compatibili le une con le altre, in base alle quali una macchina ideale possa dimostrare tutte le verità sui numeri interi, cioè tutte le verità dell'umile aritmetica. E nella stessa impossibilità si troverebbero la teoria degli insiemi e l'analisi matematica.
Cioè non si può costruire una macchina che dimostri tutti i teoremi della matematica, ma solo una macchina parziale che arriva prima o poi ad un teorema di cui non possiamo sapere se sia vero o falso.
Va notato che i teoremi e i loro cuginetti (lemmi e corollari), si devono dimostrare, mentre postulati e definizioni non si dimostrano: definiscono il mondo in cui ci muoviamo. Se non ci piacciono, ne scegliamo degli altri, purché, naturalmente, siano compatibili gli uni con gli altri.
Qui un uomo pratico direbbe: "Niente di male. Decidiamo noi per la macchina e aggiungiamo una regola o assioma che rende vero il teorema – in altre parole, trasformiamo il teorema in un assioma. Avremmo così costruito un nuovo sistema su cui la nostra macchina potrebbe riprendere a lavorare. Anzi, potremmo anche costruire un secondo sistema aggiungendo invece l'assioma opposto, che vale assumendo che il teorema sia falso. Avremo così due teorie matematiche al prezzo di una".
*Questo lo si è fatto in geometria con il famoso Quinto Postulato di Euclide, che afferma che per un punto esterno ad una retta passa una ed una sola retta parallela alla retta data.* Per qualche motivo, il Quinto **Postulato** (quindi non dimostrabile) fu per lunghi secoli considerato un teorema (quindi da dimostrare).
Nei primi anni dell'Ottocento si osservò che si potevano costruire tre tipi di

geometria: uno, secondo il quale per un punto passa una e una sola parallela (e questo è il caso studiato da sempre, della geometria euclidea); uno, secondo il quale per il punto non passa nessuna retta parallela alla retta data; uno, secondo il quale per il punto passano infinite parallele alla retta data. (Più tardi la geometria differenziale incorporò i tre casi in una trattazione più generale, basata sulle idee di Riemann).
Se i sistemi accresciuti da nuovi assiomi risulteranno abbastanza semplici, avranno un numero finito di teoremi, scriveremo l'ultimo teorema e chiuderemo il libro. E' questo il caso della Geometria Euclidea (quella in cui si è scelto come postulato l'unicità delle parallele per un punto esterno ad una retta). Se invece i nuovi sistemi risulteranno "abbastanza" complicati, aggiungendo un nuovo assioma sposteremmo soltanto il problema, anche i nuovi sistemi cadranno nelle grinfie del teorema di Gödel, e quindi prima o poi arriveremo ad un teorema di cui non si potrà dire se sia vero o falso. Aggiungeremo il teorema come postulato, ripeteremo il processo e via dicendo. Fino all'infinito.
Incidentalmente, si parla sempre del Quinto Postulato, ma esso non è l'unica proposizione indecidibile: altri animali logico-matematici più astrusi , quali l'"assioma della scelta", o la "ipotesi del continuo" o il "problema dell'arresto" (già citato) fanno parte della famigliola, che aumenta di anno in anno. Ma non ci si deve spaventare se la famiglia non aumenta abbastanza rapidamente: dopo tutto, per riconoscere e superare il problema costituito dal quinto postulato di Euclide ci vollero duemila anni.

Ora, l'accusa che si può rivolgere a tali mie rozze interpretazioni è che non ho compreso le condizioni sotto cui i teoremi valgono, e che le impossibilità previste dai teoremi di Gödel non si applicano a tutta la matematica e a tutta la logica. Ma importa realmente? Basta che ci sia un solo ramo della matematica o della logica a cui si applichino i teoremi di Gödel perché esso sia condannato ad imbattersi continuamente nella necessità di aggiungere nuovi assiomi se vuol progredire. Da cui segue che tra mille o duemila anni, chiarito tutto il resto, l'intera matematica e logica si concentreranno su quell'unico ramo e saranno obbligate ad uno sviluppo infinito.
D'altra parte, va ribadito che questi sono teoremi di logica, per di più del primo ordine, cioè, più semplicemente, tale che si possa costruire una macchina basata su assiomi , la quale dimostri i teoremi. Per cui non mancano matematici che affermano che vi sono verità matematiche non raggiungibili " a macchina", con dimostrazioni logiche (formali), il che, evidentemente, non semplifica il problema se la matematica sia destinata ad uno sviluppo infinito, almeno fino a

che non troveremo quest’altra via alla verità matematica. In effetti la capacità di proporre teoremi nuovi non coincide con la capacità di risolverli.

Dunque, in un modo o nell’altro, sembra che ci sia una certa concordia sul concetto che la matematica sia ***inesauribile***. *Se questo è vero, allora abbiamo una semplice risposta alla domanda "che cosa resta da scoprire in matematica?", e la risposta è: "**praticamente tutto**".* Per quanti teoremi la specie umana abbia già dimostrato, tanti da riempire quel centinaio di volumi negli scaffali delle nostre biblioteche, abbiamo appena incominciato: non si scherza con l'infinito. Il bello deve ancora venire.

Esisterebbe dunque un compito immane davanti alla specie umana, compito che non sarà mai concluso e che assicura infinito diletto per quelli che vorranno dedicarsi alla matematica.

**Ma ci sono due principali difficoltà.** La prima è che il cammino di avvicinamento alle trincee della matematica si allunga ogni giorno che passa. E ogni neonato deve sempre partire da zero.
Possiamo continuare con il nostro esempio dei volumi sullo scaffale della matematica: non c’è modo di far partire il neonato di cui si parlava dal secondo volume invece che dal primo, mentre le trincee della matematica sono negli ultimi volumi, e ogni giorno si aggiungono nuovi fascicoli che allontanano le trincee. Certo, si potrebbe pensare di modificare geneticamente i cervelli dei neonati destinati alla matematica: ma se questi poi non potranno trasmettere il metodo e il senso delle loro scoperte, non avremo fatto altro che creare nuovi tipi di computer.
Anche se i matematici cercano di consolidare il terreno trovando scorciatoie che ci conducono a uno dei "PNR" (Problemi Non Risolti), possiamo immaginare che magari fra cento anni, il *cammino di avvicinamento* verso uno qualunque dei PNR non possa essere percorso nel breve periodo di una vita umana. E' inutile dire che probabilmente si potranno sempre proporre problemi, come la cosiddetta ipotesi di Goldbach (che ogni numero pari può esser scritto come somma di due numeri primi), che un dilettante come Goldbach potè concepire verso il 1742, ed i più illustri matematici non hanno ancora completamente provato, ma è lecito sospettare che la maggioranza dei PNR finirà a poco a poco in una regione ormai troppo lontana dai rudimenti della matematica. E' quello che vedremo quando tenterò di dare un'idea di alcuni dei problemi proposti per il futuro.

C'è (almeno) una seconda difficoltà. La dimostrazione dei PNR ogni tanto è basata su una felice intuizione e la dimostrazione può stare tutta comoda in una pagina. Ma questo caso è sempre più raro. La dimostrazione completa del famoso “ultimo teorema di Fermat” (Wiles, 1993-1994) occupa un libro di trecento pagine ed è il frutto di una vita di studi.
Ma ancora peggiore, per certi versi, è il caso del “teorema dei quattro colori”. Questo problema si occupa del numero minimo di colori necessari per colorare una mappa politica, in cui, ovviamente, due Paesi (senza territori staccati) che hanno un tratto di confine in comune devono avere colori diversi (se il contatto è in un solo punto, si ammette che il colore sia lo stesso). Da tempo è stato dimostrato che cinque colori sono sufficienti, ma nessuno è mai stato capace di disegnare una mappa che richieda più di quattro colori. Il teorema che quattro colori sono in effetti sufficienti è stato dimostrato per la prima volta solo nel 1976 da Appel e Haken. Ma per dimostrarlo essi dovettero servirsi di tre computer che lavorarono per un totale di circa 1200 ore. Oggi i computers sono più veloci e soprattutto sono stati fatti progressi sull'impostazione del problema, ma la dimostrazione a mano richiederebbe ancora un tempo al di là di una vita umana. In effetti, pur non avendo trovato valutazioni dei tempi di lavoro per un uomo per risolvere il problema, ho letto che i computer dovettero fare “miliardi di calcoli” per dimostrare il teorema. Ora, una vita di cento anni contiene circa 3 miliardi di secondi, il che sarebbe sì e no sufficiente a contare le operazioni, senza parlare del doverle effettuare, o di svolgere altre funzioni vitali, quali il mangiare e il dormire. Dunque possiamo immaginare che molti teoremi del futuro richiederanno in media un numero crescente di ore di lavoro per un computer superveloce, fino a sfuggire alle possibilità dei computer esistenti, essendosi già lasciati da tempo alle spalle le possibilità di un uomo che ci lavori tutta la vita.

Ora, il fatto che bastino quattro colori per colorare qualsiasi mappa su un piano non ha, si dice, alcuna utilità pratica. I cartografi hanno disegnato per secoli mappe con tre, quattro o cinque colori senza mai chiedersi se fosse possibile fare meglio. La ricerca della dimostrazione con mezzi umani, ha invece dato origine a interi nuovi campi della matematica. Ma il fatto che il teorema possa solo essere dimostrato per mezzo di computers ha creato una discussione infinita. Che cosa chiediamo da una prova? A che serve sapere che un certo risultato è corretto se non abbiamo, anzi, *se non possiamo avere*, idea di come ci si sia arrivati? Su questo si discute da un pezzo, ma quello che abbiamo detto sopra sembra affermare che avremo sempre nuovi teoremi di matematica tra un miliardo d’anni, ma non sapremo che cosa significano e non li sapremo dimostrare se non usando potentissimi computers, *senza sapere come faranno*. Potremo allora dire che la matematica sarà morta come le altre scienze o no? **Resta ancora un passo da fare,** ma prima è bene discutere un altro aspetto della matematica moderna.

**Della probabile infinità di problemi non risolti che ci fronteggia è interessante speculare su quali siano i primi che vanno risolti.** Sembra difficile e certo presuntuoso fare un elenco di questi problemi; è ancora più difficile convincere i colleghi matematici che quelli e non altri sono i problemi prioritari, tanto per l'interesse intrinseco (ad esempio quando si tratta di congetture che sono alla base di sviluppi già acquisiti) quanto per il fatto che i tempi sembrano maturi per la dimostrazione.

Il primo che si cimentò con questo esercizio con successo fu David Hilbert, che proprio nell’anno 1900 presentò i problemi che secondo lui si doveva sperare che fossero risolti nel secolo ventesimo.

Si trattava di **ventitré** problemi dei tipi più diversi: si accetta unanimemente che otto siano stati risolti (SÍ) e due (l'ottavo e il dodicesimo) siano ancora non risolti (NON ANCORA).
Almeno quattro dei rimanenti sono definiti come "enunciati in modo troppo vago" (BOH?). Otto o sono parzialmente risolti, o per essi è stata proposta una soluzione, che però non è universalmente accettata (NI). Uno solo è stato dimostrato insolubile (CERTO NO). Curiosamente, né l'ultimo teorema di Fermat, né il teorema dei quattro colori, le cui dimostrazioni, come abbiamo visto, sono state due glorie della matematica del XX secolo, erano inclusi nell'elenco di Hilbert.

Con un bagaglio di problemi di Hilbert non risolti o di incerta soluzione, entriamo ora nel XXI secolo e terzo millennio, in preparazione del quale vari matematici pensarono di proporre una nuova serie di problemi per il prossimo secolo, o addirittura millennio. Tra queste varie proposte, la più nota è probabilmente quella fatta dal ***Clay Mathematical Institute,*** fondato nel 1998, giusto in tempo per formulare i problemi, chiamati con enfasi americana "I problemi del millennio". Immagino volessero intendere "I problemi proposti all'inizio del terzo millennio", e non “i problemi che richiederanno mille anni per la loro soluzione”, o, peggio ancora, “i problemi più importanti da risolvere nei prossimi mille anni”. L'elenco è di soli sette problemi, e un premio di un milione di dollari è proposto per la soluzione di ciascuno di essi, tanto per invogliare i matematici. Ma evidentemente il businessman Landon T. Clay, dilettante in matematica e fondatore dell'istituto, non conosceva bene i suoi polli, come si vide ben presto. Così, verso il 2003 fu subito risolto uno dei sette problemi "del millennio". Dopo lunghe discussioni, poiché la soluzione non era stata pubblicata su un giornale “peer reviewed”, si decise comunque di assegnare il premio al matematico russo Grigorij Perel’man, il quale lo rifiutò, dicendo essenzialmente che ci sono cose che non si pagano coi soldi e che troppi soldi generano solo violenza.

Ecco i problemi:

1. P contro NP
2. Congettura di Hodge
3. Congettura di Poincaré (risolto)
4. Ipotesi di Riemann
5. Teoria quantistica di Yang-Mills
6. Equazioni di Navier-Stokes
7. Congettura di Birch e Swinnerton-Dyer

In questo elenco, i problemi sono stati enunciati in modo estremamente sommario, e probabilmente dicono poco. In realtà, se qualcuno dei miei improbabili lettori già possiede anche solo una vaga idea di cosa significhi l’enunciato di anche uno solo di questi problemi, probabilmente quanto ho scritto su questo soggetto è stato per lui noioso come la pioggia. E non parliamo di quello che sto per scrivere! Ma è consolante pensare che se invece di questi titoli abbreviati avessi scritto per esteso l’enunciato vero del problema, la loro comprensione non si sarebbe affatto semplificata.

Si tratta di provare in ogni caso se una ipotesi o congettura sia vera o falsa, oppure se determinate equazioni siano insolubili o abbiano una soluzione, nel qual caso si chiede la soluzione.

I problemi sono stati scelti in base alla loro “utilità” in matematica. Ma, naturalmente, l’utilità matematica di questi problemi non è lo stesso che l’utilità pratica. Circa sei miliardi di esseri umani vivono felici senza affatto sapere che questi sette problemi esistono, e della loro eventuale dimostrazione non sapranno mai probabilmente nulla, se non molto alla lunga e alla lontana. Ad ogni modo, la peculiarità di questi problemi è che molti di loro interessano diversi campi della matematica allo stesso tempo e l'influsso di una loro soluzione può diventare di comune interesse d'improvviso. Ad esempio, il 4° e il 7° problema hanno a che fare colla distribuzione dei numeri primi. Poiché molti sistemi di codificazione di informazioni riservate sono basati sui numeri primi, essi potrebbero essere messi in pericolo da una soluzione di una di queste due congetture, e degli hackers potrebbero mettere a rischio tutto, dai voli degli aerei ai nostri conti in banca. Francamente, io non credo a questa catastrofica ipotesi, e penso che per la sicurezza dei nostri dati esistano rischi, magari non matematici, assai più immediati.

Tempo fa mi proponevo di spiegare, innanzitutto a me stesso, in che cosa consistano i vari problemi. Con questo avrei anche dato qualche esempio di che cosa si occupino i matematici. Ma non ci si devono fare illusioni: solo per spiegare i vari enunciati dei problemi a persone non esperte di ciascuno di almeno sette campi della matematica (ho detto che alcuni problemi interessano diversi campi della matematica) occorrono conoscenze tecniche avanzate, e quindi dovrei dare delle spiegazioni da divulgatore TV, di quelle che spiegano e non spiegano, ma almeno fanno pensare per un quarto d'ora. Poi dimenticheremo tutto, ma almeno per un momento ci saremo affacciati su un mondo straordinario, quello della matematica. Con questo "caveat", è un progetto che non ho ancora abbandonato.

Capire in che cosa consistono questi problemi richiede comunque una certa attenzione ed un certo interesse. Qualcuno, venendo a sapere dell'esistenza dei problemi, potrebbe addirittura tentare di risolverne qualcuno. Si ricordi solo che, presentando i problemi, il Direttore dell'Istituto Clay disse: "Risolvere uno di questi problemi resta in ogni caso il modo più difficile di farsi un milione di dollari".
Buona fortuna.

Vorrei dare ora un'idea della difficoltà della spiegazione e comprensione degli enunciati dei sette problemi. Purtroppo posso solo farlo riferendomi ai tempi in cui studiavo io, e so bene che i programmi di matematica sono largamente cambiati nelle scuole italiane.

1) Prima di tutto, le buone notizie:  la comprensione di cosa sia il  problema 1 (**P contro NP**, anno 1956)  è accessibile a pedoni matematici, cioè che abbiano un'educazione matematica elementare (per intenderci a livello maturità scientifica).  Difatti, si pensa che  chi lo dimostrerà sarà un giovane matematico, forse giovanissimo. Perché? Perché non ci vuol molto a capire in cosa consiste il problema, e l'intuizione matematica diminuisce rapidamente con l'età.

2 e 7) La comprensione del significato del secondo (**Congettura di Hodge**, anni 1930-40 ) e  settimo problema (**Congettura di Birch e Swinnerton-Dyer**, anni 1960-65) è ai limiti delle mie possibilità esplicative, e nell'anno che mi sono dato per tenere aperto questo sito potrei non trovare un modo comprensibile di avere e trasmettere un'idea seppur assai vaga del problema. (Problema da quarto anno di Matematica dei miei tempi)

3) Raggiungere una vaga idea dell'enunciato del terzo problema (**Congettura di Poincaré**, anno 1904, comunque risolto) è al limite tra pedoni e ciclisti matematici. (Problema da Secondo anno di Matematica dei miei tempi). *Incidentamente, è questo il problema la cui soluzione è attribuita al russo Perel'man (2003), a cui ho accennato poc'anzi.*

4) Per il quarto problema (**Ipotesi di Riemann**, anno 1859), ci sono diversi livelli di comprensione dell'enunciato. Solo un matematico ciclista (e con una buona bicicletta) può però capire di che cosa stiamo parlando.  Ma un'idea magari un po' vaga, la si può raggiungere anche a un livello inferiore. Per capirne l'enunciato in modo da eventualmente incomincare a lavorarci, ai miei tempi avremmo dovuto essere circa a metà del terzo anno di Matematica. Una breve spiegazione di che cosa significhi la congettura di Riemann è già pronta e la metterò prima o poi  in linea.

5) Il sesto  problema (**Equazioni di Navier** (1822)-**Stokes** (1842-1850)) può essere compreso di schianto da un matematico ciclista, dicendogli: "si vuole la soluzione (o la dimostrazione della non esistenza della medesima) delle seguenti equazioni differenziali non lineari  alle derivate parziali sotto determinate condizioni". Seguono le equazioni, note, perché da due secoli sono alla base della meccanica dei fluidi, pur essendo risolte solo in casi particolarissimi. Il

problema, come è inteso dal Clay Institute, è squisitamente matematico. Ai matematici, in linea di principio, non importa nulla del moto dei fluidi, problema “da ingegneri”. E quindi al matematico dovrebbe bastare quanto ho detto.
Se poi vogliamo sapere da dove e come saltano fuori le equazioni di Navier-Stokes, il problema della spiegazione è più complicato, ma non va molto più lontano di una trascrizione della seconda legge di Newton***, F = ma***, in termini adatti. Cognizioni da secondo anno di un corso di Fisica Sperimentale dei miei tempi.

6) Il quinto problema (**Teoria quantistica di Yang-Mills**, anno 1954 ) proviene dalla Fisica delle particelle elementari. Anche qui me la potrei cavare dicendo: “si vuole la soluzione (o la dimostrazione della non esistenza della medesima) delle seguenti equazioni differenziali alle derivate parziali sotto determinate condizioni. La soluzione deve anche prevedere l’esistenza di particelle di massa non nulla e positiva”. Ma intanto le equazioni sono un ordine di grandezza più *numerose e complicate* delle equazioni di Navier Stokes. In quanto poi allo spiegare da dove e come saltino fuori le equazioni di Yang e Mills, be’ questo è un problema da tesi in fisica delle particelle elementari, diciamo inizio del quarto anno di Fisica dei miei tempi.

## Il futuro della matematica rivisitato

Dunque, per capire anche solo l’enunciato di tutti i teoremi del millennio, l’infante che sta imparando a contare sulle dita, deve studiare almeno quindici - diciassette anni. E qui ci viene un brivido freddo per la schiena, se notiamo che per formulare questi problemi sono bastati pochi secoli di ricerche matematiche da parte degli intelletti più fini dell’umanità. Se la matematica procede, se può procedere indefinitamente, come – ripeto, secondo certe interpretazioni - promette Gödel, è immediato ipotizzare che entro il prossimo millennio non solo avremo risolto i problemi pomposamente battezzati “problemi del millennio”, ma ci troveremo a fronteggiare altri teoremi ben più complessi, per capire l’*enunciato* dei quali non basterà una vita umana. Ohimé! E chi li enuncerà? Evidentemente non degli esseri umani, ma dei computer. E chi li dimostrerà? Già l’ho detto, saranno dimostrati, se mai lo saranno, non già da esseri umani, ma da computer. E chi programmerà tali computer? Non c’è speranza, saranno altri computer. La matematica, cioè, diventerà un gioco riservato ai Computer,

ed avremo dei centri di ricerca, da cui ogni tanto un computer lancerà nel suo linguaggio un “EUREKA!!”, avendo dimostrato in modo per noi inconoscibile, un teorema per noi incomprensibile. Presto, cioè, raggiungeremo il confine al di là del quale sta il vero infinito, l’infinito dei Problemi Non Risolti, anzi, dei Problemi Non Enunciabili in modo da noi comprensibile.
Ma poi, un brutto giorno, il sole diventerà una gigante rossa e il nostro computer svanirà, con l’angoscia in cuore (ma hanno un cuore i computer?) che *tutto* resta ancora da fare.

Temo proprio che il futuro della matematica sia questo.

## APPENDICE 1 – ARITEMETIZZAZIONE DELL'ARITMETICA

Mentre i punti del piano euclideo sono anonimi, i numeri interi non lo sono. Mi spiego. Un punto può ricevere un nome dalle due coordinate (x,y) che gli sono attribuite in un sistema di coordinate qualsiasi, ma mutando il sistema di coordinate, anche il nome del punto cambia. Invece, un numero intero porta con sè , per così dire, il suo codice fiscale, che è la sua scomposizione in fattori primi, che è *unica* ed *esclusiva*. Vale a dire, è *unica*, perché un numero naturale ha una sola scomposizione in fattori primi (e qui si vede perché il numero 1 non può essere considerato numro primo), ed è *esclusiva*, perché non esistono due numeri naturali che hanno la stessa scomposizione in fattori primi. E' questo il contenuto del "*Teorema fondamentale dell'aritmetica*", dimostrato nelle sue due parti, esistenza e unicità, per primo da Gauss prima del 1798, mentre l'*unicità* era già data per vera fin dai tempi di Euclide. Si noti che questa scomposizione non dipende dalla base adottata per scrivere i nostri numeri. Ad esempio, passando a base binaria, il numero 15 sarà scritto 1111, ma la sua unica scomposizione 11 x 101 ( 3 x 5) non avrà battuto ciglio.

Supponiamo ora di aver stabilito un dizionario che faccia corrispondere tutti i simboli matematici mai usati ad un numero intero: ce ne sono infiniti a disposizione. Per semplicità, potremmo trovarci che "A" sia 10 e "=" sia 2. Supponiamo ora di voler aritmetizzare uno degli assiomi fondamentali dell'aritmetica, cioè "A=A". Sfruttiamo ora il fatto che i numeri primi si susseguono in ordine crescente ben noto. Possiamo dunque usare la traduzione numerica dei nostri tre (anzi due) simboli, come esponenti dei primi tre numeri primi successivi (2,3,5), ottenendo così un numero intero unico, la traduzione del nostro assioma in un numero intero:

$$\text{A=A} \rightarrow 2^{10}3^{2}5^{10} = 90000000000$$

Ne risulta un numero assai grande ( il fatto che sia una cifra tonda è un caso), ma poco importa. Ciò che è importante è che scomponendo il numero 90000000000 si ritrovano in ordine i nostri tre esponenti e quindi la nostra formula di partenza. Ogni assioma, ogni teorema, ogni affermazione matematica può quindi essere ridotta ad un singolo numero intero magari enorme, fatto che ha implicazioni notevoli nella dimostrazione di Gödel, e che, per quanto ci riguarda, dimostra quanto poco umile sia l'aritmetica, che permette di usare operazioni aritmetiche su numeri interi per discutere l'aritmetica stessa (e molte altre teorie matematiche superiori).