Rudi Mathematici

Rivista fondata nell'altro millennio

Numero 129 – Ottobre 2009 – Anno Undicesimo

Rudi Mathematici
Rivista fondata nell'altro millennio da
Rudy d'Alembert (A.d.S., G.C., B.S)
rudy.dalembert@rudimathematici.com
Piotr Rezierovic Silverbrahms (Doc)
piotr.silverbrahms@rudimathematici.com
Alice Riddle (Treccia)
alice.riddle@rudimathematici.com

www.rudimathematici.com

RM128 ha diffuso 2429 copie e il 30/09/2009 per Google eravamo in 9'280 pagine.

Siamo sicuri appartenga all'infanzia di tutti voi la frase "*Non si sommano mele con pere!*". Ora, se in un afflato di fantasia qualcuno volesse cambiare la frase, abbiamo un ottimo suggerimento. E, se qualcuno la trova su *GoogleMaps*, chiediamo la residenza.

1. Piccole storie nascoste

…ha fondato a Palermo una società matematica internazionale e una delle riviste matematiche più diffuse nel mondo intero
(Henri Poincaré, su "Le Temps", 1908)

La ragazza ha lo sguardo assorto, probabilmente già preso dagli impegni del lunedì mattina. Cammina veloce e senza guardarsi attorno, disegnando una linea perfettamente rettilinea nella sua traiettoria sotto il portico della via cittadina. È ancora estate, ma la meteorologia sembra esserselo scordato: una pioggia persistente, noiosa, lava le strade da quasi una settimana. Se non è ancora autunno, è un gran bell'anticipo.

Le persone che incrociano la ragazza la guardano con un po' di curiosità e un'ombra di fastidio: sono costrette a passarle un po' più distante di quel che farebbero normalmente, a causa dell'ombrello. Perché la ragazza, concentrata e assorta, tiene l'ombrello aperto di lato, come tenesse il guinzaglio d'un cane, e quindi ha un ingombro insolito nel viavai del mattino feriale. In effetti, il comportamento della fanciulla, pur senza essere particolarmente curioso o misterioso, merita un minimo di considerazione: gli ombrelli si tengono aperti sopra la testa o chiusi in borsa, o in mano aderenti al corpo. Che senso ha portarli così, a mezz'altezza, aperti ma non sopra la testa? C'è davvero l'intenzione di rendere complicata la vita agli altri passanti?

Basta osservare per un po', o pensarci ancora meno, e si vede che il comportamento è tutt'altro che insolito. Ci sono diverse persone che fanno lo stesso: non è un fare intelligente, ma sembra abbastanza istintivo: il fatto è che piove, ma sotto il portico non piove; quel portico, però, è abbastanza breve e termina dopo qualche decina di metri, dopodiché ricomincia il triste marciapiede non protetto. E per questo arriva l'atroce quesito, registrato soprattutto dai cervelli che sono in tutt'altre faccende affaccendati, entro i quali si svolgeranno presumibilmente i seguenti passi logici: 1) Piove: devo tenere l'ombrello aperto sopra la testa. 2) Sto entrando sotto un portico, non piove più: dovrei chiudere l'ombrello. 3) Il portico finisce presto, dovrei riaprire quasi subito l'ombrello. Questa sequenza, se esaminata con sufficiente attenzione, dovrebbe condurre a due soli possibili esiti: se il soggetto decide che il portico è troppo corto, farà finta che il portico non esista per niente, continuando a tenere l'ombrello aperto sopra la testa. Se invece giudicherà il portico abbastanza lungo, non volendo fare la figura dello sciocco che tiene l'ombrello aperto dove non piove, finirà col chiudere l'ombrello per riaprirlo di nuovo quando sarà il momento.

Verosimilmente, nella testa della ragazza distratta i tre passi logici vengono eseguiti, ma in una sorta di elaborazione in background, e la scelta viene sospesa. Il risultato è quindi quello di una mezza-scelta inerziale che persegue il principio di minima azione (e infatti non si fa l'azione di chiudere l'ombrello), ma che però si preoccupa del rischio di fare la figura della sciocca, e quindi allontana l'ombrello dalla testa come a dire agli altri: "*Non sono scema, lo so che qua sotto non piove…*". Il risultato finale è quanto di più illogico possibile, sia dal punto di vista del risparmio energetico che dell'immagine pubblica, perché tenere un ombrello aperto di lato costa più fatica che tenerlo normalmente aperto sulla testa, e inoltre dà molto più fastidio ai passanti.

La ricostruzione delle elucubrazioni mentali della fanciulla[1] può essere naturalmente sbagliata: in fondo, non siamo certo psicologi, e anche gli psicologi hanno le loro difficoltà a ricostruire gli schemi mentali che conducono a determinate azioni. Certo è che la giustificazione suona comunque convincente, tutto sommato lineare, concatenata. Questo è probabilmente dovuto al fatto che, pulsioni comportamentali e psicologiche a parte, sembra essere soddisfatto comunque il caro vecchio principio di causa-effetto, che è tanto caro all'umana ragione. Caro al punto che viene spesso usato anche per giustificare proposizioni non necessariamente vincolate a tale principio: il fatto che virtualmente ogni azione umana sia leggibile tramite il principio di causa-effetto non implica certo che il suddetto principio resti valido anche per fenomeni che umani non sono; ma resta il fatto che provare ad applicarlo, anche solo per gioco, nei contesti più leggeri è un metodo molto efficiente per scoprire delle curiosità divertenti, degli aneddoti, talvolta intere storie nascoste.

Prendete un caso qualunque, ad esempio un post di un blog letto in una tarda domenica sera. Commentando il mancato successo della Ferrari nell'ultimo gran premio di Formula Uno, l'autore del post commentava, più o meno "*… il mio disco C: e il mio Pentium piangono insieme a me per il disastro delle rosse: credevamo che quest'anno avrebbero inaugurato una nuova stagione di allori, e invece…*". E invece no, si direbbe. Ma a noi bastano queste righe, per cominciare la caccia alle storie: se davvero esiste una causa per ogni effetto, basta scavare dentro le parole per trovarle, le cause, e di causa in causa ricostruire una storia.

«*…il mio disco C: e…*» – Non serve essere troppo vecchi per saperlo, ma forse per qualcuno dei lettori più giovani la domanda non è peregrina. E di sicuro, prima o poi, fra qualche anno, ci sarà chi si chiederà perché mai l'hard-disk, il disco fisso primario di tutti i personal computer sia identificato proprio dalla lettera C. Gli altri device seguono poi in ordine alfabetico: D: per il CD, magari E: per la pen-drive che si infila nella USB, forse; e poi F:, G:, H: e così via, a seconda della quantità di periferiche che si decida di collegare[2].

1 *Olivetti M24 (con doppio floppy drive…)*

Non sarà difficile, per i ventenni curiosi, scoprire che A: e B: non sono lettere neglette, ma solo cadute in disuso, perché strettamente legate a strumenti che ormai non si usano più. I primi PC non avevano dischi fissi, ma lettori di floppy-disk. Ci voleva un floppy-disk con il sistema operativo nel drive primario (che infatti si chiamava A:) per vedere il PC svegliarsi alla vita elettronica, e sempre via floppy bisognava caricare programmi e applicazioni. Al punto che ben presto i PC si dotarono di un secondo lettore (indovinato? Sì, quello identificato dalla lettera B:) per velocizzare la lettura. In genere – ma non era obbligatorio – le applicazioni prevedevano di avere i programmi eseguibili su dischi da porre nel drive A:, i quali si appoggiavano a dati, ad archivi situati nel floppy-drive B:. Quando finalmente arrivarono gli hard-disk, furono subito visti come una manna, ma si riteneva sempre prioritario il *bootstrap* dal disco A; e comunque, anche solo per questioni di priorità storica, non potevano certo arrogarsi una lettera già assegnata ai floppy-drive. Così, dopo A e B, agli hard-disk toccò

[1] Prima di essere accusati di violazione delle politiche di genere, precisiamo che la protagonista dell'aneddoto è una ragazza solo perché, effettivamente, il primo esemplare umano osservato con tale comportamento – quello che insomma ha reso palese la cosa agli occhi di chi scrive – era effettivamente giovane e di sesso femminile. Ma questo non deve essere preso a modello: pochi minuti di osservazione hanno mostrato che il comportamento suddetto è del tutto indipendente dal sesso e dall'età, bambini a parte. I bambini, di far vedere agli altri che "sanno che sotto i portici non piove" se ne fregano altamente, e continuano a giocare con l'ombrello esattamente come fuori dai portici.

[2] Già sentiamo urla e stridor di denti. I molti esperti di informatica noteranno certo la malnata approssimazione nel raccontare la storiella, e certo saprebbero meglio spiegare le relazioni tra lettere e strumentazione dei computer: ma qui non si vuole essere precisi, solo sollecitare un po' di curiosità.

la C:, che è la lettera che hanno tuttora (e che presumibilmente terranno per sempre, finché avranno ragione d'esistere).

«*…e il mio Pentium…*» – Come nel caso precedente, se non si è al di sotto dei trent'anni, probabilmente l'aneddoto non riveste nessun mistero. Però è già un po' meno noto delle lettere che identificano i drive del PC, e anche un po' più curioso, visto che c'entrano anche delle logiche commerciali. Un tempo, i microprocessori che identificano la CPU dei personal computer erano identificati solo da un numero. Numero che aveva certo un significato importante: ad esempio l'Intel 8086 – che pure non era certo il primo microprocessore – mostrava di essere derivato dalla famiglia 8080, ma il 6 finale stava a rappresentare che era interfacciato a 16 bit, a differenza del confratello 8088, che invece lo era solo a 8. In Italia, l'8086 era montato sul PC nazionale che era a suo tempo più diffuso, l'Olivetti M24, che in effetti superava in prestazioni il personal computer dell'IBM, che montava invece il citato 8088. In più, l'8086 ha il merito di aver iniziato una vera e propria architettura, che infatti si chiama x86: la sua prima evoluzione fu il processore 80286, con il 2 in mezzo che stava a mostrare di essere una sorta di seconda generazione del progenitore 8086. E dopo l'80286, vennero naturalmente l'80386, l'80486, che ormai venivano chiamati convenzionalmente con le sole ultime tre cifre, talvolta precedute dalla "i" di Intel: i286, i386, i486. Quando stava per giungere quello che tutti erano pronti a chiamare i586, la Intel si accorse di avere un patrimonio che non stava mettendo a frutto, ovvero il nome dei suoi prodotti. I numeri, grazie al cielo, non possono infatti essere brevettati; e se chiami "586" un tuo prodotto, non puoi impedire ai tuoi concorrenti di fare lo stesso: e siccome un nome brevettato di un prodotto di successo equivale ad un sacco di soldi, la Intel rinunciò alle tre cifre, e si affidò al greco per richiamare il concetto di "quinta generazione": da cinque a penta, da penta a Pentium; perché Pentium™ a differenza di 386, può – anzi deve – essere seguito dall'apice ™.

«*… per il disastro delle rosse…*» – Le rosse, se si parla di Formula Uno, sono le Ferrari. Non si può mica sbagliare: è il caso di scomodare perfino la nobile figura retorica dell'antonomasia, tanto è palese il modo di dire, che non è solo giornalistico. Eppure il fatto ha una sua curiosità, perché, anche se ormai legato a doppio filo con la casa di Maranello, il rosso colore della Formula Uno non è in realtà veramente proprietà della gloriosa scuderia. Basta entrare in un museo dell'automobile o ricercare qualche vecchio manifesto pubblicitario per accorgersene. L'Italia è terra ricca di motori, e molte case automobilistiche hanno prodotto vetture da corsa: Alfa Romeo, Fiat, Lancia, Maserati… e, guardando le vecchie immagini, salta agli occhi come quel colore che adesso viene spesso chiamato "rosso Ferrari" sembra in realtà essere patrimonio comune: tutte rosse, le macchine italiane, e tutte dello stesso tono. Infatti, se non esiste il "rosso Ferrari" esiste invece il "rosso corsa[3]", che era proprio il colore che dovevano vestire le automobili italiane che si presentavano al via delle gare internazionali. Inizialmente, infatti, i colori delle vetture non dovevamo identificare le scuderie, ma proprio la nazione d'appartenenza; all'Italia toccò il rosso, nonostante lo spirito sportivo

2 *Una (rossa) Fiat da corsa*

[3] L'identificazione è comunque legittima dal momento che il vincolo colore/nazione non è più valido, e visto che invece la Ferrari è rimasta fedele al colore tradizionale. Purtroppo, per ragioni di sponsor, anche la Ferrari ha poi dovuto modificare la tonalità vermiglia, passando dal "*rosso corsa*" al "*rosso Marlboro*".

nazional-popolare si identifichi quasi senza fallo col colore azzurro[4]. Il blu andò alle vetture francesi, il bianco alle tedesche (queste due in coerenza con i colori delle nazionali calcistiche, peraltro), e così via. Di certo è che potere individuare le "rosse" come Ferrari è lecito e possibile solo grazie ad una sorta di monopolio nazionale della Formula Uno.

«…*avrebbero inaugurato*…» – La maggior parte delle piccole storie sta nascosta dentro un normale dizionario etimologico. Ad ogni pagina si viene facilmente proiettati nei meandri dell'indoeuropeo, senza appigli mnemonici storici; o, se si è più fortunati, nel greco di Atene e Sparta. O, se va davvero di lusso, nel bel mezzo dell'antica Roma. E si scopre magari che, per i primi pastori latini e romani, il *templum* era inizialmente solo uno spazio sacro, ben delimitato ma non necessariamente decorato da costruzioni, come gli edifici che ormai siamo soliti immaginare quando sentiamo parlare di templi. Nello spazio sacro potevano e dovevano entrare solo i sacerdoti, e da lì cercare di leggere il volere degli dei. Si poteva entrare solo da una certa direzione (in genere da Nord), e da lì osservare il cielo, e contare gli uccelli che sorvolano quel *tempio*. E dal loro numero, e dal loro procedere da destra a sinistra o viceversa, i sacerdoti capivano se gli dei erano favorevoli o no. Ed è probabilmente proprio dal latino *avis*, uccello, che prendono il nome quei sacerdoti che dovevano leggere il destino nei voli: gli *auguri*. Sempre da *avis* discende la parola *auspici*, che sono i segni divini che il cielo manda attraverso il volo degli uccelli: e infatti l'augure, osservando gli uccelli, traeva gli auspici, e sulla base di questi si intraprendevano o meno le grandi avventure come le battaglie, le decisioni politiche, le costruzioni di opere pubbliche. Quindi, il momento iniziale di ogni impresa è proprio quello, quando gli *auguri entrano* nel tempio: *in+augure*, inaugurare.

«…*stagione di allori*…» – Lo sport, anche se con una connotazione abbastanza diversa da come lo consideriamo oggi, viene fatto risalire alle Olimpiadi antiche. E il termine "alloro" come sinonimo di vittoria è tradizionale, associato al premio che veniva consegnato al vincitore delle gare di Olimpia. In realtà, l'associazione tradizionale di idee rischia di non essere molto precisa: gli antichi giochi greci erano diversi, non solo "olimpici", e i premi erano diversi: solo i giochi di Delfi, i giochi Pitici in onore di Apollo, prevedevano per i vincitori una corona di alloro. I giochi Panatenaici, poco prestigiosi dal punto di vista della fama, compensavano i vincitori con oggetti d'oro e d'argento, forse proprio per consolarli della scarsa notorietà; i giochi Istmici offrivano una corona di pino, mentre quelli Nemèi addirittura una di sedano. I giochi più famosi, quelli Panellenici che si tenevano nelle celebre Olimpia, consegnavano ai campioni sempre delle corone vegetali, ma non di alloro, bensì di olivo selvaggio. È insomma probabile che gli "allori" usati oggi come sinonimo di trionfi sportivi vengano invece dai trionfi romani, dove c'erano effettivamente corone d'alloro poste sulla testa del

3 *Trionfo di Tito e Vespasiano (Louvre)*

[4] Tra l'altro, anche nell'azzurro delle divise nazionali c'è una storia, o quantomeno una ragione, una causa: la maggior parte delle nazioni tendono a riportare nelle divise sportive i colori della bandiera, ma nel tricolore italiano non c'è traccia di azzurro. Fu per onorare i Savoia, il cui colore dinastico era l'azzurro, che fu scelto il colore attuale; la nazionale di calcio, inizialmente dotata di maglia bianca, nel 1911 dovette incontrare l'Ungheria, che aveva anch'essa divisa bianca. Per dovere d'ospitalità (che oggi non si rispetta più nemmeno per scherzo) gli italiani lasciarono il bianco agli ungheresi, e indossarono delle maglie azzurre per onorare la famiglia reale. Poi, a ben vedere, ci sarebbe una storia anche nell'azzurro sabaudo, perché lo stemma inizialmente era solo uno scudo rosso con una croce bianca; ma una particolare devozione alla Madonna fece sì che nello stemma venne poi inserito l'azzurro, che è il colore tradizionale del manto di Maria nelle immagini sacre. Che poi, a ben vedere, è anche questo frutto di una causa ben precisa: tutte le rappresentazioni dei santi usano un linguaggio ben preciso, in modo che i fedeli possano di volta in volta riconoscere il santo rappresentato; l'azzurra veste mariana è forse solo l'artificio più noto, perché la codifica iconografica prevede molte altre regole e… Ma è meglio smettere. Di causa in causa, si rischia di perdere ogni effetto.

trionfante *imperator*; niente di sportivo, insomma, ma solo di militare. E anche il senso della corona cambiava: non era segno di gloria o maestà, anzi, era invece una protezione, uno scudo. Il trionfo, del resto, meritava davvero certe cautele: non c'era niente che romano potesse desiderare di più, era davvero una parificazione momentanea agli dei, e tanta gloria era pericolosa. Il fortunato generale percorreva la via trionfale su una biga, diretto al tempio di Giove, dove si sarebbe sacrificato un toro[5] per ringraziare il dio supremo; aveva la faccia dipinta di rosso, proprio come erano rosse le statue degli dei, e non c'era quasi nulla che non potesse avere, in quel momento. Per questo, occorrevano prudenti accorgimenti: uno, contro il rischio di perdere la consapevolezza di non essere un dio, e all'uopo era accompagnato dallo schiavo che gli ripeteva il "*memento mori*", ricordati che devi morire, ricordati che sei un uomo. Un'altra cautela, invece, era diretta proprio verso gli dei, che forse potevano irritarsi per vedere un mortale adorato tanto quanto loro stessi. Il grande Giove, padre degli dei e padrone del Campidoglio e di tutta Roma, poteva forse infuriarsi, e come difendersi allora dalla sua punizione, da una saetta che avrebbe potuto scagliare per incenerire l'arrogante mortale? Ma proprio mettendo un piccolo scudo d'alloro, pianta sacra al dio e da lui amatissima, a protezione del capo del generale vincitore.

Un guaio, nell'inseguire le piccole storie nascoste dietro quasi ogni frase o parola, è che il gioco è virtualmente infinito, dipanandosi in una catena che passa da anello ad anello, da aneddoto ad aneddoto, senza speranza di trovare una fine. Era già possibile perdersi in una biblioteca, o in uno scaffale modesto, o perfino solo dentro un dizionario enciclopedico: adesso, con internet aperta ad ogni minima curiosità e tempi di ricerca prossimi a zero, la navigazione randagia in cerca di storie nascoste è davvero un viaggio senza ritorno. Un altro, è che il viaggio può essere consolatorio, ma solo fino ad un certo punto: se uno si mette in viaggio perché è triste perché le Ferrari hanno corso male la loro gara, non è che girando a caccia di storie la situazione cambierà. Se, da amanti della matematica, vi avventurate nell'albo d'oro delle quarantasette Medaglie[6] Fields[7] e vi rattristate perché compare un solo nome italiano, non è che navigando navigando troverete altri vincitori connazionali, oltre a Bombieri[8]. Le storie sono pur sempre pezzetti di Storia, e quella è bene che non cambi. Però, può capitare che la storia immutabile sia possibile guardarla con occhi nuovi.

La medaglia Fields viene consegnata durante i "Congressi Internazionali dei Matematici", International Congress of Mathematicians, ICM; massimi incontri del gotha matematico, che si svolgono ogni quattro anni. Il prossimo si inaugurerà il prossimo 19 Agosto 2010 a Hyderabad, in India, e in quell'occasione quattro matematici sotto i quarant'anni saranno insigniti del prestigioso riconoscimento. Il primo Congresso dei Matematici si tenne a Zurigo nel 1896; a quello fece seguito il celebre congresso di Parigi nel 1900, quello in cui Hilbert presentò i suoi famosissimi 23 problemi del secolo. Dopo Parigi, patria della maggiore scuola matematica dell'epoca, il Congresso nel 1904 emigrò a Heidelberg, in Germania, dove risiedeva l'altra grande scuola di matematica d'inizio Novecento. L'uso di premiare i matematici che avessero mostrato particolare talento arriva però solo nel 1936, proprio per merito di John Charles Fields che aveva fin da prima del 1924 fortemente propugnato una tale istituzione.

---

[5] Al giorno d'oggi, quando un artista esegue mirabilmente una performance, o quando un personaggio pubblico è meritevole di un particolare apprezzamento da parte degli astanti, riceve dai presenti una *standing ovation*, che è il massimo cui può ragionevolmente aspirare. Tutti in piedi, in segno di rispetto o apprezzamento, ad applaudire: il termine inglese – peraltro del tutto simile all'italiano – discende dalla celebrazione romana inferiore al trionfo, l'*ovazione* appunto, così detta perché, essendo meno importante, prevedeva il sacrificio non di un toro, ma di una pecora (*ovis*).

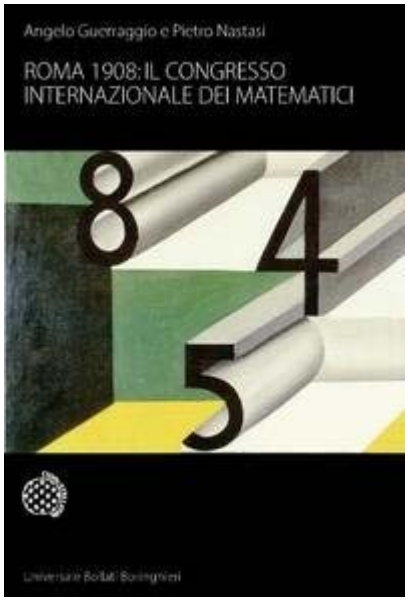
[6] http://www.mathunion.org/general/prizes/fields/prizewinners/, o più semplicemente in RM100.

[7] Sulla vita di Fields e sull'istituzione della Medaglia, trovate migliori informazioni sul compleanno a lui dedicato, "*Diventare padrone dell'universo*", appunto RM100, Maggio 2007.

[8] Enrico Bombieri vinse la Medaglia Fields nel 1974.

Fatto sta che il massimo riconoscimento matematico, che l'Italia ha ricevuto una sola volta, è una medaglia d'oro, riportante l'effigie di Archimede, assegnata ad un valente studioso durante gli ICM: e se è vero che scavare nelle pieghe delle cronache per trovare piccole storie nascoste non fa certo aumentare il numero delle medaglie Fields col nastrino tricolore, è anche vero che si può con meraviglia scoprire almeno un'altra medaglia al merito matematico, riportante l'effigie di Archimede, assegnata durante un ICM ufficiale, che finì sul petto orgoglioso d'un matematico italiano. Le piccole storie nascoste sono piene di coincidenze.

Dopo Zurigo, terra neutrale per eccellenza, Parigi e Heidelberg, il quarto Congresso Internazionale dei Matematici, quello del 1908, sarebbe dovuto finire nella terra della terza nazione matematicamente più in auge di quegli anni. Non era però così facile stabilire quale fosse questa nazione: gli inglesi, padroni del mondo – era quello ancora il periodo in cui *Britannia rules the waves* – erano convinti di meritare l'onore, ma dovettero aspettare ancora quattro anni, prima di organizzare il loro congresso a Cambridge, nel 1912. Perché il Congresso del 1908 si tenne a Roma, a dimostrazione che la scuola matematica italiana era davvero tra le maggiori del mondo.



4 *Il libro di A.Guerraggio e P.Nastasi*

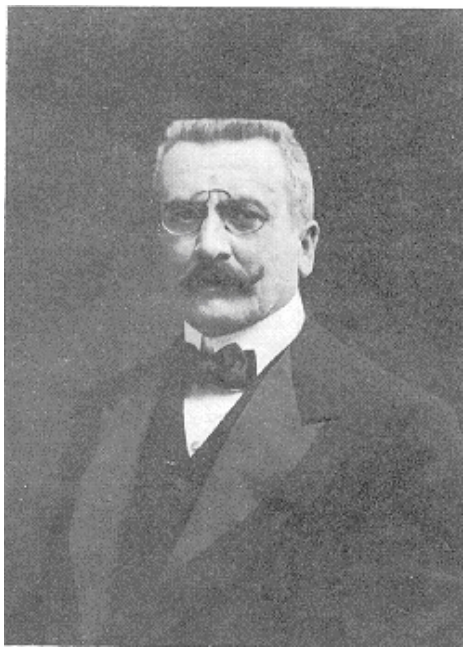
Sulla storia del grande congresso romano del 1908 si dovrebbe scrivere un libro, tanto furono interessanti, nello sviluppo della matematica italiana sia le fasi di preparazione che quelle di realizzazione. Per fortuna, a scrivere quel libro ci hanno già pensato le persone giuste: Angelo Guerraggio e Pietro Nastasi che, quasi a celebrare la ricorrenza, un secolo dopo la storica riunione hanno pubblicato per Bollati Boringhieri il libro "*Roma 1908: il Congresso Internazionale dei Matematici*[9]". Fatto sta che durante quel congresso si assegnò un premio – appunto una medaglia d'oro con il volto di Archimede – al matematico che un'apposita commissione giudicò particolarmente meritevole. La commissione non era certo composta da dilettanti: i tre matematici che ne facevano parte rappresentavano le già citate tre grandi scuole nazionali; c'erano Segre[10] per l'Italia, Noether[11] per la Germania e Poincaré per la Francia. Dopo le strabilianti somiglianze, è bene precisare che le differenze con la futura medaglia Fields erano comunque notevoli. Tanto per cominciare, il premio, che oltre alla medaglia in prevedeva anche la somma di tremila franchi in oro, aveva un tema fisso: quello previsto per il 1908 era la teoria delle curve gobbe algebriche, e in genere si immaginava che fosse sempre destinata a lavori di geometria. Inoltre, il meccanismo era simile a quello di un vero e proprio concorso: una volta noto il tema, i matematici che intendevano partecipare dovevano inviare le loro memorie, ma in forma assolutamente anonima, pena l'esclusione dal novero dei candidati. Infine, il premio era sostanzialmente un premio privato, non istituzionale: se la Fields viene infine istituita, nel 1936, grazie a degli "avanzi di bilancio", nel caso del premio italiano i costi erano a carico d'un solo benefattore, che non per nulla dava il nome alla medaglia stessa.

[9] Nella Universale Scientifica Boringhieri: 219 pagine, 17,00 Euro. Da qui vengono quasi tutte le notizie che seguono sugli eventi del 1908.

[10] Segre, Corrado, geometra: da non confondersi con Beniamino (altro geometra, parente ma non troppo prossimo) o con Emilio, fisico e "ragazzo" di via Panisperna.

[11] Max Noether, grande della geometria algebrica e papà di Emmy, che si è meritata uno dei primi compleanni di RM ("*Questione di attributi*", RM050, Marzo 2003).

Il vincitore della medaglia fu Francesco Severi, personaggio che divenne poi assai influente nella matematica italiana del primo Novecento; e il premio che ottenne aveva il nome di Medaglia Guccia.



5 *Giovanni Battista Guccia*

Giovanni Battista Guccia nacque a Palermo il 21 Ottobre 1855, da una famiglia ricca, nobile e famosa nell'isola. Ricevette un'educazione di prim'ordine e, forte del benessere familiare, passò una giovinezza serena dedicandosi anche ai cavalli e allo sport in generale. I suoi interessi matematici, comunque, non vennero mai meno: studiò dapprima a Roma, sotto la guida di Cremona; poi, poco prima di laurearsi, ebbe modo di recarsi a Reims per la sessione annuale della Associazione Francese per l'Avanzamento delle Scienze. Ed è probabilmente qui, incontrando personaggi come Sylvester, Cayley, Hermite, Darboux, che Guccia scopre la sua passione per l'ambiente della ricerca, e soprattutto per la ricerca internazionale, liberata dai confini di stato che imprigionano il libero fluire delle idee. Così, non appena discussa la sua tesi a Roma e ottenuta la laurea, Guccia ritorna nella sua Palermo, e si mette subito al lavoro per fondare un'istituzione per la ricerca internazionale in matematica. Giovanni non ha ancora compiuto ventinove anni quando, nel marzo del 1884, ventisette membri firmano lo statuto provvisorio del *Circolo Matematico di Palermo*. Il *Circolo* è la più antica società italiana di matematica, se non si contano le università, ed è in tutto e per tutto una creazione personale del giovane siciliano. È Guccia che fornisce gli spazi, la biblioteca, i fondi: virtualmente ogni aspetto organizzativo dell'associazione è sotto il suo compito e sotto il suo controllo. E infatti segue pedissequamente i desideri del fondatore: una norma dello statuto nel 1888 apre le iscrizioni al Circolo anche agli stranieri, e in brevissimo tempo il numero dei soci sale a duecento: tra questi, praticamente tutti i maggiori matematici del tempo.

È anche un segno dei tempi; è infatti un buon periodo per la Sicilia, grande produttrice di zolfo: l'economia dell'isola è in fortissimo sviluppo e, come accade sempre, lo sviluppo economico genera anche sviluppo culturale e notorietà internazionale. Ben presto nasce l'esigenza di pubblicare i lavori dei membri, e si istituiscono così i *Rendiconti del Circolo Matematico di Palermo*, che diventeranno una delle riviste matematiche più autorevoli mai pubblicate. Il circolo raggiunse infatti i mille soci, e le sue pubblicazioni furono, tra il 1900 e il 1910, probabilmente il miglior prodotto matematico disponibile sul pianeta. È sufficiente dare uno sguardo agli indici[12] per rimanere stupefatti della quantità e qualità dei lavori prodotti.

Come capita spesso alle creazioni di una sola persona, il Circolo cominciò a decadere con la scomparsa del fondatore. Era del resto il 1914, anno fatale non solo per gli individui, ma anche per nazioni, imperi e stili di vita. Il Circolo sopravvisse, sotto certi aspetti sopravvive ancora oggi sotto l'egida dell'Università di Palermo, ma naturalmente non avvicina neppure i fasti d'inizio secolo. Era proprio nel 1914, nel trentesimo anniversario dalla fondazione, che Edmund Landau asseriva, durante le celebrazioni: "*Celebriamo il giubileo di una società che ha solo una minoranza dei suoi membri nella città dove risiede, ma che ha riunito quasi mille matematici in tutto il mondo e, tra questi, i più grandi e*

[12] http://math.unipa.it/~circmat/ricerca/INDICE.pdf

illustri studiosi d'Italia, di Germania, di Francia, degli Stati Uniti, di Ungheria e di tutte le nazioni dove si coltiva la nostra scienza. È l'unica organizzazione permanente che abbiamo; così noi consideriamo Palermo come il centro del mondo matematico"[13].

A differenza delle altre storie che abbiamo raccontato in quest'articolo, la storia del Circolo Matematico di Palermo non è stata affatto piccola né nascosta. È stata solo breve, purtroppo.

[13] Tutta la citazione di Landau è presa – anzi è copiata di sana pianta – dal libro citato di Guerraggio e Nastasi.

2. Problemi

	Rudy d'Alembert	**Alice Riddle**	**Piotr R. Silverbrahms**
Un vecchio PM, e un problema dell'anno scorso			
Quasi un Summer Contest			

2.1 Un vecchio PM, e un problema dell'anno scorso.

PM che nessuno si ricorda[14], siamo sicuri.

Questa volta la coloritura è decisamente più semplice: partiamo dall'idea che ogni *numero naturale* (lo evidenziamo perché di recente in merito ci abbiamo fatto l'ennesima figuraccia) è colorato di rosso o di giallo; sappiamo anche che **8** è il naturale più piccolo di colore giallo. Inoltre, sappiamo che la somma e il prodotto di due numeri di colore diverso sono, rispettivamente, di colore rosso e giallo.

Bene, liquidata la parte "vecchio PM", veniamo alla parte "problema dell'anno scorso": secondo voi, di che colore è il numero **2008**? Nel caso non vi piaccia fare i conti con i problemi riciclati, potreste verificare di che colore vengano gli altri anni da quelle parti, presente incluso…

Non ci ricordiamo se ve lo abbiamo detto, ma Rudy ha dei problemi incredibili con le date: per quanto riguarda gli anni in cui sono successe cose particolari, si ricorda la presa della Bastiglia (1789, facile, sette-otto-nove), lo sbarco sulla Luna (1969, al pensiero, sente ancora caldo alla guancia sinistra) e un'altra data, che è la seconda presentata qui di seguito.

Questa volta prendiamo i numeri relativi: li coloriamo in verde, in blu o in nero (un solo colore ciascuno); la somma di due numeri blu è verde e la somma di due numeri verdi è blu; l'opposto di un numero verde è blu e l'opposto di un numero blu è verde; sappiamo inoltre che **1009** è verde e **1492** è nero.

Come avrete intuito, l'altra data che Rudy ha memorizzato è la data della scoperta dell'America[15]; adesso, abbiamo due domande:

1. Cosa cavolo è successo nel 1009?
2. In quest'altra notazione, di che colore è 2008?

Per la seconda domanda, sempre valide le estensioni, chiaro.

[14] RM055, Agosto 2003: "I numeri colorati". Giusto per gli archeologi: anche perché Rudy odia colorare le cose, visto che va sempre fuori dai bordi: nel senso di *Hanc Marginis*… con quel che segue.

[15] In realtà, ricordando che l'annuncio al presidente degli Stati Uniti d'America del funzionamento della pila atomica costruita da Enrico Fermi fu "Il navigatore italiano è arrivato nel Nuovo Mondo; gli indigeni si sono mostrati amichevoli", Rudy si ricorda anche che basta invertire le due cifre centrali (1492→1942) per avere l'anno di inizio dell'Era Nucleare. E questo fa una data in più.

2.2 Quasi un Summer Contest

"Padre, *emergenza*!"

Il 97,354% della popolazione mondiale maschile con prole, alla ricezione di una telefonata di questo tenore scatterebbe probabilmente in piedi preoccupatissima; il restante due-e-qualcosa per cento, al quale appartiene Rudy, considererebbe che se fosse un'emergenza *vera*, Alberto avrebbe telefonato alla madre, e quindi si limiterebbe a rispondere un "Seeh…".

Come al solito, Rudy aveva pienamente ragione: vediamo il resto della conversazione.

"…devono trovare i nomi nelle scatole numerate e se uno non trova il suo perdiamo tutti…"

"Ferma, e ricomincia da capo. Di chi stai parlando, cosa stai facendo e chi deve fare cosa? Non necessariamente in quest'ordine."

"Sto facendo l'animatore, come al solito. Mi hanno rifilato *diciotto* mocciosi che il più sveglio sa contare fino a due se qualcuno suggerisce[16], e i miei colleghi sono nella stessa situazione, sia numerica che intellettuale. Hanno proposto un gioco a squadre, decisamente perfido…"

"Che gioco?"

"*Mi lasci parlare, che magari te lo spiego?* Sfruttando il fatto che all'interno di ogni gruppo i diciotto nomi dei mocciosi sono tutti diversi, a ogni squadra verrà presentata una fila di diciotto scatole numerate, ognuna delle quali conterrà il nome di uno dei ragazzini della squadra stessa. Naturalmente, nessun ragazzino conoscerà il contenuto delle scatole. Il gioco consiste nel fatto che ogni pischello, a turno, dovrà aprire nove scatole, e sperare di trovare in una di queste nove il proprio nome. Se è fortunato e lo trova, bene, torna tra i suoi compagni e un altro dei diciotto si cimenterà subito dopo nella stessa impresa, e così via. Se invece non trova il suo nome nelle nove scatole che apre, amen, gioco finito: tutta la sua squadra ha perso. Evidentemente, possiamo parlare tra di noi prima del gioco, ma quando si comincia silenzio totale ed è vietato lasciare segni sulle scatole o sui biglietti".

"Hai ragione, è perfido. Se procedete a caso…"

"…la probabilità che tutti i diciotto mocciosi trovino il loro nome e la squadra sopravviva alla prova è infima, lo so: viene compresa tra una su centomila e una su un milione. Non ho la calcolatrice, ma se due alla decima fa circa dieci alla terza, dovrebbe essere un po' maggiore di uno su dieci alla sesta".

"Figliuolo, ci sono rari momenti in cui penso che non ho sprecato il mio tempo, con te: questa è già la seconda volta in un anno che lo penso, e la cosa è preoccupante"

"Quand'era la prima?"

"Mi rifiuto di rispondere".

"Allora sentiti abbastanza in colpa da darmi una mano: esiste un metodo per aumentare le nostre probabilità? Non pretendo la certezza, ma almeno un qualcosa meglio di una su un milione…"

"Beh, si può fare. Ad esempio…"

E qui, per non annoiarvi, tronchiamo l'aneddoto.

E come al solito, adesso tocca a voi. Riuscite a trovare un qualche modo con una probabilità meno fetente di riuscita? Non pretendiamo la certezza e neanche l'"uno su

[16] Questa è una delle solite iperboli di Alberto: i ragazzini sanno far di conto, se gli si spiega cosa fare.

due", ma almeno qualcosa che permetta ad Alberto di avere qualche speranza: maggiore di una su quattro sarebbe già un buon risultato.

3. Bungee Jumpers

Provate che:

$$\sin\varphi+\sin(\varphi+\alpha)+\sin(\varphi+2\alpha)+\ldots+\sin(\varphi+n\alpha)=\frac{\sin\frac{(n+1)\alpha}{2}\sin\left(\varphi+\frac{n\alpha}{2}\right)}{\sin\frac{\alpha}{2}}$$

e che

$$\cos\varphi+\cos(\varphi+\alpha)+\cos(\varphi+2\alpha)+\ldots+\cos(\varphi+n\alpha)=\frac{\cos\frac{(n+1)\alpha}{2}\cos\left(\varphi+\frac{n\alpha}{2}\right)}{\cos\frac{\alpha}{2}}.$$

Conservate il risultato: ci servirà il mese prossimo.

La soluzione, a "Pagina 46"

4. Soluzioni e Note

Il rientro dalle vacanze in Redazione è stato molto turbolento, per cui ve lo diciamo, non sappiamo ancora come affrontare questo autunno. Tra errori, sviste, pasticci, imprecisioni, ci siamo ormai fatti un nome in rete e tra i nostri lettori, ma con il numero di settembre ne abbiamo collezionati a bizzeffe: perfino la newsletter aveva un link sbagliato (per fortuna amiamo l'abbondanza e la ridondanza, ed i link erano due, di cui uno giusto), e degli altri errori leggerete probabilmente tra queste pagine.

Comunque siamo ancora qui, e proviamo ad andare avanti. Prima di tutto con le promesse ancora aperte: c'è un lavoro che stiamo cercando di preparare sul Bookshelf del sito, per poter contenere i numerosi contributi che abbiamo ricevuto recentemente… abbiate ancora un po' di pazienza e andate a controllare ogni tanto, di sicuro sarete premiati: si tratta di contributi di matematici veri, non come noi...

Poi, per quanto riguarda gli eventi di ottobre, abbiamo una segnalazione dell'ultimo minuto, da parte di ***Mario***:

> Domenica 4 ottobre alle 17.30 il prof. John Nash della Princeton University terrà una conferenza sui Giochi cooperativi, nell'ambito delle manifestazioni di Bergamo Scienza. La relazione sarà preceduta da una introduzione alla Teoria dei Giochi del prof. Gianfranco Gambarelli, professore ordinario di Matematica, Teoria dei Giochi e delle Decisioni nella Facoltà di Economia dell'Università degli Studi di Bergamo (http://dinamico.unibg.it/dmsia/staff/gambar.html). La partecipazione è gratuita. Essendo previsto un notevole afflusso di pubblico, conviene iscriversi alla voce "prenotazioni" sul sito www.bergamoscienza.it

Potrebbe essere tardi per segnalarla, ma noi proviamo lo stesso. Se qualcuno ci va, accettiamo volentieri anche resoconti e foto.

Inoltre vi segnaliamo le conferenze della Mathesis di Ivrea, che ci coinvolgono in modo particolare, soprattutto quella del 7 ottobre: il programma dovrebbe trovarsi qui: http://www.subalpinamathesis.unito.it/ivrea.php, ma scriveteci se siete interessati.

Massimo ci segnala il suo studio del gioco dell'Hex, http://www.massimodacasto.net/, e cerca qualcuno con cui discutere i suoi risultati.

Le cronache settembrine si sono riempite anche di dichiarazioni in merito al Premio Peano, istituzione alla quale siamo visceralmente affezionati per aver vinto, l'anno scorso, la "Segnalazione Speciale della Giuria" per i libri di matematica editi nel 2007. Il tumulto nasce dal fatto che Piergiorgio Odifreddi, vincitore del premio nel 2002, intende restituirlo per manifestare il suo disaccordo all'assegnazione del premio di quest'anno (relativo al 2008) a Giorgio Israel. Noi, lungi dal prendere una qualsivoglia posizione in merito alla diatriba – siamo matematici troppo piccoli per entrare nelle discussioni dei grandi – ci limitiamo a dire che sappiamo benissimo che il nostro premiuccio è immeritato, ma non abbiamo nessunissima intenzione di restituire alcunché. Siamo pronti ad appellarci anche al sacro istituto dell'usucapione, se necessario!

Ed ora, finalmente, andiamo a vedere come sono andati i problemi.

4.1 [126] – Summer Contest

La più grande sorpresa dell'anno è che il Summer Contest non ha avuto molto seguito. L'unico che ha avuto voglia di mettere alcune delle soluzioni in bella copia è stato ***Gnugnu***, e per questo lo ringraziamo con tutto il cuore e pubblichiamo le sue soluzioni senza indentarle. Buon divertimento!

4.1.1 Zensyoji 1, Prefettura di Nagano

Costruzione con riga e compasso: ***XY*** = retta per ***X*** e ***Y***; ***(XY)*** = circonferenza di centro ***X***, passante per ***Y*** . Dati i punti ***A*** e ***B***; nella prima parte si individua ***C***, nella seconda si completa la costruzione.

$AB \bigcap (AB) \to D, B$

$(DB) \bigcap (BD) \to E, E'$

$EA \bigcap (AB) \to F, F'$

$(DF) \bigcap AB \to G, G'$

$(GA) \bigcap AB \to H, A$

$(HA) \bigcap AB \to C, B$

$\overline{CA} = \overline{BA} \cdot \left(4\sqrt{2} - 5\right)$

$(CA) \bigcap AB \to I, A$

$(IC) \bigcap AB \to J, C$

$(JC) \bigcap (CJ) \to K, K'$

$KK' \bigcap (IC) \to L, L'$

$LJ \bigcap (JI) \to M, M'$

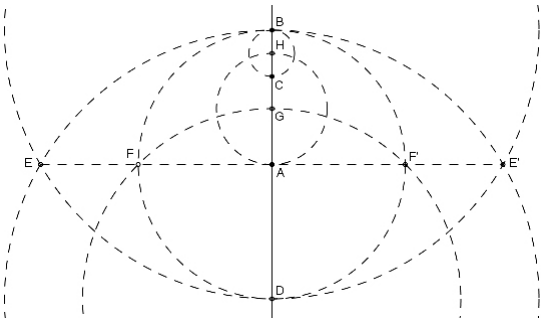
$L'J \bigcap (JI) \to N, N'$

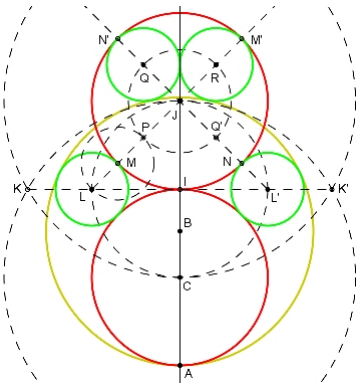
$(ML) \bigcap LJ \to P, L$

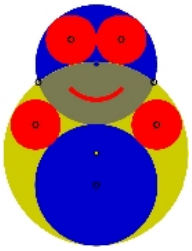
$(JP) \bigcap L'J \to Q, Q'$

$(JP) \bigcap LJ \to R, P$

$\overline{CA} = \overline{JI} = \overline{QN'} \cdot \left(1 + \sqrt{2}\right)$

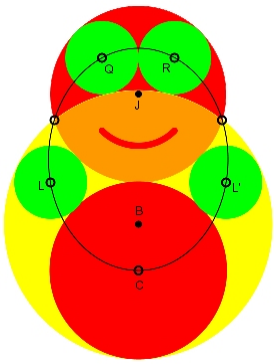






$$\overline{LM} = \overline{L'N} = \overline{RM'} = \overline{QN'} =$$
$$= \overline{CA} \cdot \left(\sqrt{2} - 1\right) = \overline{BA} \cdot \left(13 - 9\sqrt{2}\right).$$

I centri di tutti i cerchi sono legati da un'unica ellisse, avente per fuochi ***B*** e ***J***, passante per i restanti cinque e per le intersezioni delle due circonferenze con centro nei fuochi.



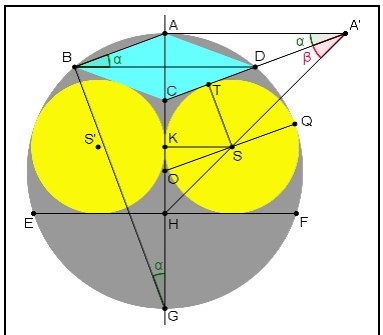
Non possono esistere altre soluzioni non degeneri.

4.1.2 Sangaku n. 3, prefettura di Nagano – Il gufo diplomato – Soluzione costruttiva.

Sia *AH* un segmento di lunghezza a appartenente ad *s* asse di simmetria della figura finale.

Si costruiscono successivamente:

- il triangolo *HAA'* isoscele e rettangolo in *A*;
- la circonferenza γ di raggio *r* ($2r < a$), con centro in $S \in HA'$, tangente ad *AH* in *K*;
- la tangente da *A'* a γ che interseca *AH* in *C* e tocca γ in *T*;
- *D*, punto medio di *A'C*;
- la circonferenza δ di raggio *R* con centro in $O \in s$, passante per *A* e *D*, *G* è l'altra intersezione con *s*;
- le corde *BD* ed *EF*, perpendicolari ad *s* e passanti rispettivamente per *D* ed *H*;
- la circonferenza γ' simmetrica di γ rispetto ad *s*.



6 *Il gufo diplomato.*

ABCD è un rombo di diagonale $\overline{BD} = \overline{AA'} = \overline{AH} = a$ e le circonferenze γ e γ' sono tangenti ad un lato del rombo, ad *AH* ed *EF*.

Indicati con α gli angoli congruenti $A\hat{G}B, D\hat{B}A \; e \; A\hat{A}'D$, con β l'angolo $C\hat{A}'H$ si ottiene:

dal triangolo *ABG* $\frac{a}{2} = \overline{BA}\cos\alpha = 2R\sin\alpha\cos\alpha = R\sin 2\alpha \rightarrow \quad \sin 2\alpha = \frac{a}{2R}$;

dal triangolo *A'TS* $\sin\beta = \frac{r}{\sqrt{2}(a-r)} \rightarrow \quad \cos 2\beta = 1 - 2\sin^2\beta = \frac{a^2 - 2ar}{(a-r)^2}$.

Essendo $\alpha + \beta = 45°$, gli angoli 2α e 2β sono complementari e perciò:

$$\sin 2\alpha = \cos 2\beta \rightarrow \frac{a}{2R} = \frac{a^2 - 2ar}{(a-r)^2} \rightarrow \quad R = \frac{(a-r)^2}{2(a-2r)}.$$

Da cui si ricava facilmente il richiesto valore, è infatti:

$$d = \overline{GH} = \overline{AG} - \overline{AH} = 2R - a = \frac{(a-r)^2}{a-2r} - a = \frac{a^2 - 2ar + r^2 - a^2 + 2ar}{a-2r} = \frac{r^2}{a-2r}.$$

Purtroppo occorre ancora dimostrare che la figura ottenuta soddisfa tutte le condizioni del sangaku. Le circonferenze γ e δ sono tangenti? Naturalmente la risposta è

affermativa, ma la dimostrazione risulta un po' articolata; occorre provare che è sempre $\overline{OS} = R - r$.

Dal triangolo *OKS* si ricava che $\overline{OS} = R - r$ equivale a

$$\overline{KO} = \sqrt{\overline{OS}^2 - \overline{KS}^2} = \sqrt{(R-r)^2 - r^2} = \sqrt{R(R-2r)} = \sqrt{\frac{(a-r)^2}{2(a-2r)} \cdot \left(\frac{(a-r)^2}{2(a-2r)} - 2r \right)} =$$

$$\sqrt{\frac{(a-r)^2}{2(a-2r)} \cdot \frac{a^2 - 6ar + 9r^2}{2(a-2r)}} = \frac{(a-r)|a-3r|}{2(a-2r)}.$$

Basta, a questo punto, verificare che la misura di *KO* ottenuta dalla costruzione coincide con questo valore.

Il punto *O* può appartenere ai segmenti *AK*, *KH* o *HG*. Il caso corrispondente alla figura, $O \in KH$, porta a:

$$\overline{KO} = \overline{KH} - \overline{OH} = r - (a - R) = r - a + \frac{(a-r)^2}{2(a-2r)} = \frac{2ar - 4r^2 - 2a^2 + 4ar + a^2 - 2ar + r^2}{2(a-2r} =$$

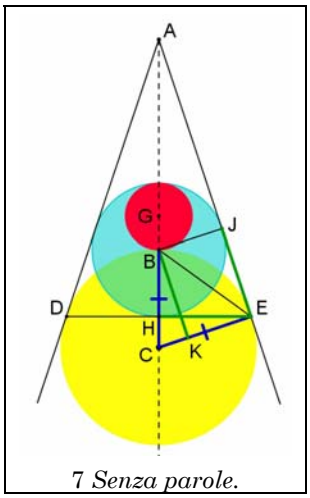
$$= \frac{-a^2 + 4ar - 3r^2}{2(a-2r)} = \frac{(a-r)(3r-a)}{2(a-2r)}.$$

Con $O \in AK$ si ottiene:

$$\overline{KO} = \overline{OH} - \overline{HK} = (a-R) - r = \frac{(a-r)(a-3r)}{2(a-2r)}.$$

Infine, con $O \in HG$:

$$\overline{KO} = \overline{KH} + \overline{HO} = r + (R-a) = \frac{(a-r)(3r-a)}{2(a-2r)} \text{ CVD}$$



7 *Senza parole.*

4.1.3 Sangaku n. 6, prefettura di Nagano – Soluzione senza parole

$BK \cong JE \cong HE \rightarrow \quad CB \cong CE$

$$r_2 = 2r_3.$$

4.2 [127]

4.2.1 "… 'tses tôrna si?"

Questo problema, il mese scorso, aveva avuto ben poco successo: solo una soluzione, da parte di ***Cid***. Dopo averla pubblicata in RM128, alcuni si sono fatti avanti per affermare di aver ottenuto gli stessi risultati, ma – non essendo totalmente soddisfatti dalle dimostrazioni – di non aver inviato nulla. Ma andiamo per ordine e ricordiamo il testo del problema:

> *Supponiamo di avere un certo numero (pari) di pietre in un giardino Zen, metà di un tipo e metà dell'altro, messe in modo tale che non ce ne siano mai tre collineari. Cercando le disposizioni "meno simmetriche" possibili, mi interesserebbe minimizzare (portando possibilmente a zero) le disposizioni per cui si possano*

trovare delle linee passanti per due pietre di tipo diverso tali che da ogni parte della linea ci siano tante pietre di un tipo quante dell'altro.

Attenzione: lo scopo sarebbe di trovare una disposizione in cui queste linee di divisione "non esistono", ma tanto per cominciare non ho posto limiti al numero di pietre, secondariamente se chiedo un "valore minimo" è abbastanza probabile che questo sia diverso da zero…

Ecco la critica di ***Franco57***, sostenuta anche da ***Gnugnu*** e ***Cid*** stesso:

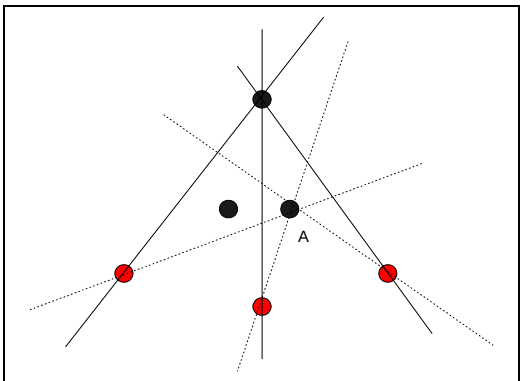
Nella soluzione pubblicata si cerca di provare che:

[Proposizione 1a] data comunque una pietra del primo tipo esiste sempre una pietra del secondo tipo tale che, se le congiungo, i due semipiani che trovo hanno la proprietà richiesta (chiamiamola P1), e cioè che in ciascuno di essi le pietre di un tipo sono numericamente uguali alle pietre dell'altro tipo. Le due pietre che stanno sulla retta non si contano in nessuno dei due semipiani.

Una volta dimostrata la [Proposizione 1a], abbiamo come conseguenza la

[Proposizione 1]: il numero totale delle rette con la proprietà P1 sia almeno N. Poi dato N si costruisce facilmente un insieme di N pietre di N pietre di un tipo e N dell'altro che abbia esattamente solo N delle rette con la proprietà P1.

Quello che ho descritto era anche almeno come pretendevo di averlo risolto io. Peccato che la [Proposizione 1a] è falsa. Ecco un controesempio con N = 3, nella figura a destra.



8 *Controesempio di* ***Franco57****.*

Fissata la pietra nera A non posso trovare una pietra rossa tale che la retta che le congiunge abbia la proprietà cercata.

Devo ammettere che invece il ragionamento alla base della [Proposizione 1a] è bellissimo e quando l'ho scoperto mi ha gratificato tantissimo. Esso può essere utilizzato per dimostrare un'altra bella proprietà e cioè che dato un punto non coincidente con nessuna retta e non allineato ad alcuna coppia di pietre esiste sempre una retta che passa per esso con la proprietà P1. Ma sulle rette che congiungono due pietre di colore diverso con perno su una pietra del primo tipo non funziona, perché ruotando la retta fino alla prossima pietra del secondo tipo possono passare in più o in meno nel semipiano più di una pietra del primo tipo .

La [Proposizione 1] invece secondo me è vera anche se non l'ho dimostrata. Lo dico perché ho fatto delle simulazioni con un programma generando con prove ripetute N punti di un tipo ed N dell'altro in un quadrato e contando le rette con la proprietà P1 che congiungono punti di tipo diverso. Ho scoperto che il numero di rette ha sempre la stessa parità di N e non scende mai sotto N. I valori che ottengo rendono il Lemma 1 una congettura estremamente credibile.

Ecco il risultato di una simulazione. Ho chiamato linee simmetriche le rette con la proprietà P1 e le pietre le ho immaginate rosse e nere:

numero prove = 5000

numero punti rossi = 10

numero punti neri = 10

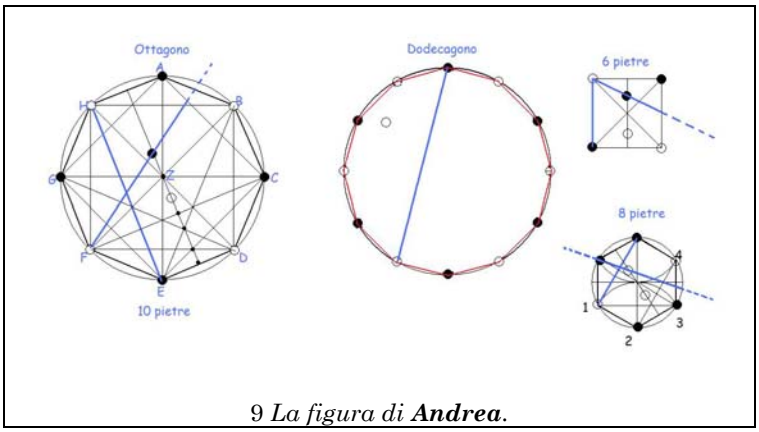
Il problema resta aperto per me.

linee simm	prove	%
10	175	3.50 %
12	310	6.20 %
14	349	6.98 %
16	432	8.64 %
18	460	9.20 %
20	464	9.28 %
22	442	8.84 %
24	402	8.04 %
26	389	7.78 %
28	350	7.00 %
30	322	6.44 %
32	232	4.64 %
34	222	4.44 %
36	132	2.64 %
38	113	2.26 %
40	80	1.60 %
42	57	1.14 %
44	35	0.70 %
46	14	0.28 %
48	6	0.12 %
50	6	0.12 %
52	6	0.12 %
54	2	0.04 %

Anche ***Andrea*** ci manda ancora qualche considerazione:

Ho letto la bella soluzione di Cid e credo anche di aver capito male il problema. Da come l'ho letto io mi sembrava che si chiedesse una disposizione delle pietre tale che ogni linea passante per due pietre di diverso colore dividesse le pietre restanti in maniera tale che sia da un lato che dal'altro della linea non ci sia mai un uguale numero di pietre dei 2 colori (facendo un esempio in modo tale che non ci siano mai X pietre nere e X pietre bianche da un solo lato della retta, e allo stesso modo X bianche e X nere dall'altro lato con tutte le X uguali tra loro). Nella soluzione di Cid si dice che per un numero di pietre pari a 2N ci siano N disposizioni possibili tali che da una parte e dall'altra della linea ci sia uno stesso numero di pietre dello stesso tipo mentre semplicemente disponendo le pietre sempre a poligono ma con una regola diversa a me queste disposizioni vengono 0 (per ora, poi se ho sbagliato si sistema tutto...).

In pratica il problema dice che bisogna avere un numero pari di pietre per il semplice fatto che se disponessimo un numero dispari di pietre in un poligono semi-regolare come detto da Cid si vedrebbe subito che qualsiasi retta passante per 2 vertici della figura la divide al massimo in 2 parti 2N+(2N+1) e quindi il numero delle disposizioni per cui si avrebbe lo stesso numero di pietre di colori diversi da ciascun lato della retta sarebbe chiaramente pari a zero. Di tutta la bella dimostrazione di Cid non capisco come mai alla fine scelga che "nei primi N vertici sistemo le pietre del primo tipo e nei successivi N vertici sistemo le pietre del secondo tipo". Intanto collocando le pietre a formare questo poligono semi-regolare (che da ora chiamo solo "poligono" che è più piccolo da scrivere) bisogna distinguere 2 casi principali per N=numero delle pietre e quindi dei lati, il primo in cui (N–2)/2=2n+1 e il secondo i cui (N–2)/2=2n per n=il numero che serve.



9 *La figura di* ***Andrea***.

Nel primo caso si vede facilmente dalla figura che disponendo i tipi di pietra in maniera alterna (bianco, nero, bianco...) alla fine due vertici diametralmente opposti avranno lo stesso colore e quindi una qualsiasi linea passante per due pietre di colore diverso dividerà il numero delle pietre in due gruppi non aventi lo

stesso numero, e quindi con un numero di pietre corrispondenti al primo caso e con questa disposizione delle pietre non esiste nessuna linea passante per due pietre di colore diverso tale che da entrambi i lati della retta le pietre di tipi diversi si trovino ad essere nella stessa quantità (l'italiano non è granché ma credo di riuscire a farmi capire). Già nel primo caso quindi abbiamo che il numero dei disposizioni in cui il numero delle pietre di tipo diverso è uguale da entrambi i lati della retta è nullo mentre con il procedimento di Cid ci saremmo dovuti aspettare almeno N/2 configurazioni in cui ciò dovrebbe accadere e quindi almeno per la metà dei casi il ragionamento di Cid non dovrebbe funzionare (naturalmente non sto conteggiando le pietre che formano la linea e si ritengono le pietre come puntiformi per semplicità). Per il secondo caso arrivo alla stessa conclusione anche se in una maniera diversa. Per il secondo caso stavo provando a colorare dello stesso colore i vertici opposti dell'esagono e in pratica ne spuntavano sempre 4 di un colore e 2 dell'altro colore, allora ho pensato di aggiungerne 2 nelle altezze di due triangoli opposti al vertice in maniera tale che nessuna di queste due pietre fosse nell'intersezione tra l'altezza di questi 2 triangoli e le rette che nell'allegato sono le rette 2-4 e 1-3 dell'esagono. In questa maniera qualsiasi retta che passa per una di questa 2 pietre messe sulle altezze dei 2 triangoli opposti dividerà le pietre in maniera tale da avere un diverso numero di pietre indipendentemente dal colore da ciascun lato della retta e quindi si ripropone la situazione del primo caso arrivando allo stesso risultato di 0 disposizioni. Solo che per arrivare ad avere questo risultato ho dovuto aggiungere 2 pietre e quindi le pietre sono diventate 8. Partendo dal secondo caso quindi sono arrivato alla conclusione generale che qualsiasi numero pari di pietre può essere descritto come M+2 (con (M+2) che ora indica il numero totale delle pietre) e quindi qualsiasi numero pari si può rappresentare come un poligono di M lati più le due pietre sistemate nel suo interno nella maniera descritta prima (ad eccezione del quadrato che ha solo 4 vertici), e così in maniera generale per qualsiasi numero pari di pietre il numero minimo di disposizioni nelle quali il numero delle pietre di diverso tipo è uguale da ogni parte della retta è sempre pari a zero (per fare un esempio 6 pietre si possono mettere in un quadrato e 2 pietre al centro, 8 pietre=esagono+2 pietre, 10pietre=ottagono+2 pietre...). Ogni volta che si aggiungono le due pietre bisogna sempre fare attenzione che nessuna di queste si venga a trovare nell'intersezione tra l'altezza e tutti quei segmenti formati da 2 pietre che l'intersecano e alla fine il risultato per ogni figura dovrebbe essere simile all'ottagono con 2 pietre dell'allegato, anche se il numero di lati e tutto il resto cambia.

Non è una dimostrazione formale come quella di Cid, ma in ogni caso mi sembrano esagerati N/2 casi su N pietre di disposizioni con un numero uguale di pietre ai lati della retta. Questo è quello che mi è venuto fuori alla luce di quello che credo volesse chiedere il problema, la cosa che non mi piace è che pure questa soluzione è abbastanza simmetrica e non mi piace molto il fatto di allontanare di pochissimo le pietre dalla loro posizione nel poligono regolare, sarebbe meglio trovare un modo più elegante di disporre le pietre in maniera asimmetrica (dando anche la giusta definizione di simmetria).

Siete riusciti a prendere il fiato? Noi saremmo contenti se se ne parlasse ancora, per cui non aggiungiamo alcunché.

4.3 [128]

4.3.1 L'importante non è arrivare: è viaggiare

I titoli dei problemi del Capo sono sempre sibillini... In questo caso si trattava di passatempi da viaggio. Ecco in breve il testo del gioco proposto da Alberto:

"Fred, io penso un numero (naturale) minore o uguale a N (diciamo N=34, ma non perdiamo in generalità); tu hai a disposizione 7 punti, e puoi fare dei tentativi di

indovinarlo; ad ogni tentativo io ti dico se il numero da indovinare è maggiore o minore di quello che ho pensato; ad ogni domanda perdi un punto, ma attenzione: se il tuo tentativo è maggiore del numero che ho pensato, di punti ne perdi 2; vinci se indovini il numero senza avere un numero negativo di punti. Piace?"

"Mah, non so se fidarmi di te. Proviamo, ma poi cambiamo il numero dei punti e il valore massimo…"

Alberto è onestissimo nel gioco; secondo voi, esiste una strategia vincente? Logicamente, ci aspettiamo uno studio al variare del numero dei punti in funzione del valore massimo del numero pensabile…

Per buon peso, c'è anche una variante più cattiva:

"Fred, questa volta voglio essere generoso; ti do' 10 punti, di cui uno è un jolly; io penso un numero tra 1 e 50, e tu cerchi di indovinarlo come sopra, alle seguenti condizioni:

1. *Se hai zero punti, hai perso;*
2. *Se hai un numero di punti strettamente positivo, puoi fare un tentativo;*
3. *Se azzecchi il numero, hai vinto;*
4. *Se dici un numero minore del numero che ho pensato, perdi un punto;*
5. *Se dici un numero maggiore del numero che ho pensato, perdi il jolly; se lo dici maggiore senza avere jolly, hai perso."*

Qui, evidentemente Alberto sta facendo l'avvoltoio; esiste, per Fred, un metodo per almeno accrescere le sue possibilità di vittoria?

I solutori di cui abbiamo raccolto i contributi sono l'instancabile ***Cid***, ***Elena***, ***Millenium Bug***, ***Franco57*** e ***Ilaria***. Le soluzioni sono tutte belle, diamo la precedenza a quella di ***Ilaria***, che ci scrive per la prima volta ed è divertentissima.

Ricapitolando: c'è Alberto che pensa un numero tra uno e trentaquattro, che per comodità chiameremo Peppino (meglio della solita ics, perlomeno); io, che per l'occasione sono Fred, devo scovarlo in al più sette domande.

La prima considerazione banale che mi viene in mente è che ogni volta che sbaglio divido i numeri restanti in due gruppi, maggiori e minori del mio tentativo, e so in quale dei due si trova Peppino. A questo punto la domanda è: quanto devono essere grandi questi gruppi? Dopo un po' di tentativi a casaccio mi viene in mente che la soluzione più bilanciata potrebbe essere dire un numero che stia dalle parti di N terzi, nello specifico dodici: in questo modo se Peppino è più grande perdo un punto e riduco le possibilità a (circa) due terzi N; se è più piccolo di punti ne perdo il doppio, ma è doppio anche il restringimento del range (fosse stato un mezzo avrei *dimezzato*. Con un terzo cosa faccio, *diterzo*? *Sterzo*? Cosa? E con un quarto, è corretto dire che *squarto*? E perché *dissestare* significa tutt'altro? State cominciando a ringraziare il cielo che non vi abbia mai scritto? Eh?), il che sembra abbastanza equo. Insomma, in prima approssimazione provare ogni volta con un numero che stia ad altezza un terzo di quelli rimasti sembrerebbe una strategia vincente.

A questo punto vi risparmio il bellissimo albero degli eventi che avevo disegnato (*a ma-no*: non conosco altri sistemi) che prendeva in considerazione tutte le possibili scelte e tutti i possibili scenari che ne derivavano. Vi basti sapere che ci ho passato un pomeriggio, riuscendo a coprire col mio sistema al massimo trentatré numeri e ottenendo, come generalizzazione, un penoso (2/3)^m*(1/3)^(k–m)*N (dove m è il numero di volte in cui sbaglio per eccesso) che nel frattempo mi ero anche scordata cosa dovesse significare. Il tutto prima di rendermi conto che 1) è inutile fare calcoli troppo precisi dopo aver premesso che si trattava di una prima approssimazione, e

2) quella formuletta di prima coi numeri naturali non ci azzecca un gran bel tubo. Praticamente questo paragrafo ve l'ho messo solo perché l'ottica della lettera era di infamarmi un po' da sola.

Al che, sette camicie dopo, mi viene l'idea risolutiva: e se cominciassi dalla fine? Sembra una strada battibile. Dal momento che ogni domanda mi costa un punto anche se indovino, se ho un solo punto posso fare un solo tentativo. Se invece di punti ne ho due ho la certezza di indovinare solo se il range è ridotto a due numeri: provo con il minore, se sbaglio uso l'ultimo punto per dire l'altro. Ora, cosa succede se di punti ne ho tre? Se sbaglio per eccesso resto con un solo punto, quindi mi conviene che ci sia un solo numero minore di quello che ho detto; se sbaglio per difetto mi avanzano due punti, con cui come ho appena visto posso fare due tentativi. Per cui con tre punti copro quattro numeri: quello che dico, uno minore e due maggiori (ah, che limpidezza espositiva, ah). Ripeto il ragionamento per i successivi valori di k: con quattro punti copro quattro più due più uno uguale sette numeri; con cinque, sette più quattro più uno dodici; con sei venti (dodici più sette più uno); con sette, infine, trentatré. Toh! Allora non m'ero dimenticata niente, nel fare l'albero.

Generalizzazione: $N_k = N_{k-1} + N_{k-2} + 1$. Che sta a significare: il massimo N che posso coprire con k punti è uguale al massimo N che posso coprire con (k–1) punti più il massimo N che posso coprire con (k–2) punti, più uno. Sapendo che $N_1=1$ e $N_2=2$ posso sviluppare la successione un po' fin dove voglio, e questo è il massimo che sono in grado di fare. Lo "studio al variare del numero dei punti in funzione del valore massimo del numero pensabile" per me finisce qui, e se poi Alberto propone di concedermi ottocentosessanta punti per poter fissare N a dieci alla diecimila fattoriale io non protesto, può prendersi i miei punti, i miei soldi, una cornea, non mi oppongo.

Adesso passiamo all'altro caso, che apparentemente è una carognata bella e buona. Dieci punti di cui un jolly tradotto significa: nove possibilità di sbagliare per difetto, una sola di sbagliare per eccesso. Una buona politica è dire dieci in prima battuta: se Peppino è minore mi restano nove punti per dire tutti i numeri da uno a nove, in quest'ordine, con la certezza di stanarlo; se è maggiore ho ancora il jolly e posso applicare lo stesso sistema sui numeri che restano. Pertanto dico diciannove, e se perdo il jolly ho otto punti per provare con gli otto numeri tra undici e diciotto. La mia chiarezza nell'esprimermi è la stessa di prima, quindi lasciamo perdere l'analisi del resto della partita e passiamo subito alla generalizzazione: con queste nuove regole, il massimo N che posso coprire con k punti è la sommatoria dei numeri naturali tra uno e k. Nello specifico, con k=10, $N_{max}=55$. Ri-toh! Alberto si è messo nel sacchetto da solo, almeno prima un trentaquattresimo di probabilità di vittoria ce l'aveva.

La prossima soluzione che vi proponiamo è di ***Franco57***, che propone ulteriori estensioni.

Primo Gioco.

Invece di effettuare direttamente uno "*studio al variare del numero dei punti in funzione del valore massimo del numero pensabile…*" , ho trovato più conveniente chiedermi: disponendo di p punti, quale è il massimo range di numeri, chiamiamolo $N(p)$, che mi garantisce di indovinare il numero pensato con una opportuna strategia?

Da notare che, senza perdere in generalità, $N(p)$ rappresenta la dimensione di un range di numeri consecutivi, non necessariamente comincianti da 1, tra i quali c'è quello da indovinare.

Chiamo $X(p)$ il primo tentativo che devo fare per avere la sicurezza di indovinare il numero X pensato. Allora per $p \geq 2$ ci sono tre casi:

a) se $X(p) = X$, vinco;

b) se $X(p) > X$, perdo due punti e il nuovo range sarà $1 \div X(p)-1$ quindi di dimensione $X(p)-1$;

c) se $X(p) < X$, perdo un punto e il nuovo range sarà $X(p)+1 \div N(p)$ quindi di dimensione $N(p) - X(p)$.

Per massimizzare $N(p)$ devo ricorsivamente ottimizzare la dimensione dei due sotto-range dei casi (b) e (c), quindi ottengo rispettivamente:

1) $N(p-2) = X(p) - 1$

2) $N(p-1) = N(p) - X(p)$

e sostituendo la (1) nella (2) si ottiene una definizione simile ai numeri di Fibonacci:

3) $N(p) = N(p-1) + N(p-2) + 1$

Le condizioni iniziali sono:

N(0) = 1, che traduce il fatto che senza punti posso indovinare con certezza solo se c'è un unico numero possibile, e

N(1) = 2, che ci dice che con 1 punto posso indovinare fra 2 numeri ma non fra 3. Infatti:

1) con 2 numeri e 1 punto, vinco se provo inizialmente col minore e, se non è giusto, quello pensato è il maggiore che indovino quindi con 0 punti;

2) con 3 numeri e 1 punto, non si può indovinare, poiché se non tento subito col minore rischio di perdere 2 punti ed andare negativo, ma se esso non è quello cercato mi ritrovo con due numeri da indovinare e nessun punto.

Se con $F(n)$ rappresento la successione di Fibonacci [$F(0)=0$; $F(1)=1$; $F(n)= =F(n-1)+F(n-2)$], si può dimostrare per induzione che

4) $N(p) = F(p+3) - 1$

Infatti: per $p = 0$, abbiamo $F(p+3) - 1 = F(3) - 1 = 2 - 1 = 1 = N(0)$; per $p=1$, abbiamo $F(p+3) - 1 = F(4)-1 = 3 - 1 = 2 = N(1)$; supponiamo quindi che la relazione (3) sia valida per tutti i $p < q$, allora

$$\begin{aligned} N(q) &= N(q-1) + N(q-2) + 1 \\ &= (F(q+2) - 1) + (F(q+1) - 1) + 1 \text{ , per l'ipotesi induttiva} \\ &= F(q+3) - 1 \text{ , per la definizione dei numeri di Fibonacci} \end{aligned}$$

Dalla (1) otteniamo la strategia ottimale con p punti:

5) $X(p) = F(p+1)$.

Da notare che poiché, come è noto, $F(p) / F(p+1)$ tende al rapporto aureo, questo fatto induce che lo stesso accade per

$$X(p) / (N(p) - X(p)) = F(p+1) / N(p-1) = F(p+1) / F(p+2) - 1 ,$$

cioè il primo tentativo da fare è (o meglio tende ad essere) quello che divide il range in due zone in rapporto aureo tra loro, con la più piccola ai numeri bassi.

Tornando al gioco tra Alberto e Fred, visto che $N(6) = 33$ e $N(7) = 54$, per indovinare uno fra i 34 numeri servono effettivamente 7 punti, ma con questi punti si può elevare il range fino a 54.

Secondo Gioco.

Per come ho capito le regole del gioco, sembra che Fred riesca con certezza a determinare il numero pensato da Alberto, quindi non sono andato ad indagare come massimizzare le sue possibilità di vittoria.

In generale con p punti, di cui uno è un jolly, Fred può arrivare a determinare con certezza un qualsiasi numero nel range $1 \div 1+2+3+ \ldots +p$, provando inizialmente con p:

a) se p è il numero da trovare Fred ha vinto;

b) se il numero da trovare è inferiore a p, Fred perde il jolly ma ha disposizione $p-1$ punti, beh gli bastano se non sballa mai, quindi comincia con 1, poi 2, etc. fino, al limite, a $p-1$;

c) se il numero da trovare è maggiore di p, Fred ha ancora il jolly, $p-1$ punti e deve indovinare il numero in un range di $1+2+3+ \ldots +(p-1)$, quindi è lo stesso problema con un p abbassato di 1.

Rimane solo da vedere che il meccanismo funziona con $p = 1$, ma è chiaro che non ci sono problemi a indovinare un unico numero con un unico tentativo.

Poiché $1+2+3+\ldots +10 = 55 > 50 > 1+2+3+ \ldots +9 = 45$, Fred può applicare la strategia per un range di 55 numeri. Il primo tentativo, ad esempio, sarebbe quindi 10.

Ho visto che il problema si può generalizzare con p punti di cui j sono jolly, sostituendo, in modo naturale, nella regola 5 "perdi *il* jolly" con "perdi *un* jolly" e nella regola 4 "perdi un punto" con "perdi un punto non jolly, se possibile, altrimenti perdi un punto jolly".

Analogamente al primo gioco, determiniamo ricorsivamente il massimo range $N(p,j)$ di numeri che consente con certezza di indovinare il numero da trovare.

Per $p>j>0$ abbiamo:

$$N(p, j) = 1 + N(p-1, j-1) + N(p-1, j)$$

in cui i tre addendi corrispondono ai casi (a), (b), (c) elencati sopra, rispettivamente numero azzeccato, numero per eccesso (perdo 1 jolly e 1 punto), numero per difetto (perdo 1 punto ma non jolly).

Per $p>0$ e $j=0$, abbiamo

$$N(p,0) = p$$

perché si può vincere con sicurezza senza jolly solo con p tentativi a partire dal numero più piccolo a salire.

Per $j=p>0$, cioè con soli punti jolly, abbiamo:

$$N(p, p) = 1 + N(p-1, p-1) + N(p-1, p-1) = 1 + 2 \cdot N(p-1, p-1)$$

poiché anche se il tentativo è per difetto perdo un numero jolly. Qui si pone convenzionalmente $N(0,0)=1$, in modo da ottenere la evidente $N(1,1)=1$.

Innanzitutto si vede che $N(p, p) = 2^p - 1$ e si dimostra per induzione poiché è vera per $p=1$ e se vale per $p=q-1$ allora vale anche per p=q:
$N(q,q) = 1 + 2 \cdot N(q-1, q-1) = 1 + 2 \cdot (2^{q-1} - 1) = 2^q - 1$

Più in generale vale la formula: $\boxed{N(p,j)=\sum_{1\le i\le j+1}\binom{p}{i}}$

fissato $q>j>0$ supponiamo la formula vera per ogni $p<q$, allora abbiamo

$$N(q-1,j-1)=\sum_{1\le i\le j}\binom{p-1}{i}\text{ e}$$

$$N(q-1,j)=\sum_{0\le i\le j}\binom{p-1}{i+1}=\binom{p-1}{1}+\sum_{1\le i\le j}\binom{p-1}{i+1}$$

e quindi si ricava la formula per $p=q$ con l'ipotesi induttiva

$$N(q,j)=1+N(q-1,j-1)+N(q-1,j)=1+\binom{q-1}{1}+\sum_{1\le i\le j}\left(\binom{q-1}{i}+\binom{q-1}{i+1}\right)=$$

$$=q+\sum_{1\le i\le j}\binom{q}{i+1}=\sum_{1\le k\le j+1}\binom{q}{k}$$

I casi limite sono pure verificati:

$$N(p,0)=p=\sum_{1\le k\le 1}\binom{p}{1}$$

$$N(p,p)=2^p-1=\sum_{0\le k\le p}\binom{p}{k}-1=\sum_{1\le k\le p}\binom{p}{k}=\sum_{1\le k\le p+1}\binom{p}{k}$$

Naturalmente complimenti anche a tutti gli altri, ma andiamo avanti… che c'è molto da dire sul secondo problema.

4.3.2 Trivial Poursuites

In molti si sono accorti del fatto che il problema era più complesso di quanto sembrasse: non per niente il numero di soluzioni giunte in redazione è stato veramente interessante e di vario formato. I solutori sono stati ***Alberto R.***, ***Zar***, ***Andrea***, ***Giampietro***, ***Franco57***, ***Cid***, ***Trentatre***, ***Ilaria***, ***Br1***. Vediamo il testo:

> *Rudy si è messo a studiare i mezzi di trasporto della Catalogna, scoprendo alcune interessanti caratteristiche:*
>
> *1. I mezzi di trasporto disponibili sono tre: aereo, bus e treno*
>
> *2. Due città sono legate da un unico mezzo di trasporto*
>
> *3. Non ci sono tre città legate tra di loro dallo stesso mezzo di trasporto*
>
> *Adesso vorremmo sapere, al massimo, quante città ci sono in Catalogna?*

Quando le soluzioni sono cominciate ad arrivare, il Capo ha dichiarato "*Ohibò*[17]*, direi che al punto (2) delle condizioni si è perso un "qualunque": "Due città qualunque"...*". Siamo caduti dalle nuvole: e adesso quali soluzioni pubblichiamo? E come lo diciamo ai nostri fustigatori? Così – per continuità, visto che è quello che facciamo sempre – abbiamo

[17] Esclamazione che, insieme alla famosa "porca pupattola" è diventata una delle preferite della Redazione.

concordato di non fare proprio nulla e semplicemente di pubblicare qualche soluzione a caso. Prendete quello che ci ha scritto ***Zar***:

> Naturalmente possono esserci alef_zero città, in Catalogna. Prendiamo la città numero 1, essa sarà connessa per via aerea (mettiamo) con la città numero 2, la quale a sua volta sarà connessa via treno alla 3, che sarà connessa alla 4 nuovamente per via aerea, e così via. In questo modo facciamo anche a meno del terzo mezzo di trasporto, e non ci sono tre città connesse con lo stesso mezzo.
>
> Quando ci troviamo di fronte a 2^(alef_zero) città, invece, le cose cambiano. Non possiamo passare da una città alla successiva, dato che non esiste una città "successiva" – a meno che non riteniamo valido il principio del buon ordinamento (riguardo a questa ipotesi, ricordo il famoso detto che afferma che l'assioma della scelta è ovviamente vero, il principio del buon ordinamento è ovviamente falso e, circa il lemma di Zorn, chi è capace di capirci qualcosa?). Ma anche in questo caso, ogni città avrebbe un successore ma non è detto che per ogni città esista un predecessore, e questo ci darebbe dei problemi qualora volessimo poi tornare indietro. Per non parlare poi dell'altro problema, quello dei nomi: ci risulterebbe un po' complicato nominare tutte le città, e quindi avremmo poi dei problemi ad acquistare i biglietti per il treno o l'aereo (e, se usiamo l'automobile, faremmo un po' fatica a trovare le indicazioni stradali).
>
> Direi quindi che esistono almeno alef_zero città, ma non 2^(alef_zero) città.
>
> Il fatto che l'esistenza di un numero maggiore di alef_zero ma minore di 2^(alef_zero) sia indipendente dalla scelta di assiomi che abbiamo fatto relativi alla Catalogna ci fa concludere che, se vogliamo, in Catalogna ci sono alef_zero città; se non vogliamo, ce ne sono un po' di più, ma non troppe.
>
> Come? Il quesito di Rudi intendeva un'altra cosa? Ho sempre pensato che Rudi non è molto chiaro quando propone i suoi quesiti...

E che dire della risposta di ***Ilaria*** (sì, la stessa del problema precedente)?

> Attenzione, castronerie in caduta libera.
>
> Dunque, cerchiamo di affrontare la questione da un lato abbordabile: che succederebbe se il mezzo di trasporto fosse uno solo? Non potrebbero esserci più di due città, perché altrimenti ci sarebbero giocoforza tre città collegate dallo stesso mezzo, quello lì, l'unico disponibile. E se i mezzi fossero due? Se i mezzi fossero due prendendo una città a caso, la città Gesualda, questa sarebbe collegata ad a città con un mezzo, diciamo l'aereo, e a b città con l'altro, diciamo il bus. Ora, le città collegate a Gesualda con l'aereo tra di loro devono essere collegate col bus, altrimenti avremmo già un triangolo di aerei; e non possono essere tre o più, altrimenti avremmo un triangolo di bus. Lo stesso discorso vale per le città b, il che mi porta a dire che due mezzi di trasporto permettono un massimo di cinque città. Per il momento so di stare sulla strada giusta uno perché l'ho disegnato e funziona, due perché mi ricorda molto da vicino il caso delle sei persone che si stavano simpatiche e antipatiche in un problema di millemila numeri fa.
>
> Adesso però arriva il treno e la faccenda si fa più oscura. Prendo sempre una città a caso, Gesualda. Gesualda è collegata ad a città con l'aereo, a b città col bus e a t città col treno, e fin qui. Per lo stesso discorso di prima, le città collegate a Gesualda con l'aereo non possono essere collegate tra loro con l'aereo: saranno collegate col treno o col bus, la qual cosa le fa ricadere nel caso "due mezzi di trasporto" e limita il loro numero a cinque. La stessa solfa è valida per b e per t, quindi io direi: in Catalogna, a queste condizioni, ci possono essere al più sedici città. Bene, dove sta la magagna? La magagna sta nel fatto che io non sono affatto sicura che collegando le città a alle b e alle t non venga fuori nessun triangolo. A occhio direi di no, basta che ognuna faccia cinque collegamenti per tipo, ma

andando a occhio la terra è piatta e il sole ci gira intorno. Dovrei dimostrarlo, cosa che, ho realizzato con orrore, *non so fare*.

Shame on me.

A fare il disegno ci ho rinunciato, alla decima linea è già un quadro di Balla. Al momento sono impegnata a costruire un solido con sedici vertici di pongo e i collegamenti di stecchini e cordicelle. L'importante non è risolvere: è impazzire nel tentativo.

Il quadro di Balla ci ha tenuti allegri per un paio di giorni. Il nostro ***Cid*** ha trovato il problema facile, e l'ha risolto come un Sudoku: senza di lui non sapremmo cosa fare, veramente.

Per risolvere questo problema, parto dall'analisi di un caso più semplice: Consideriamo che in una regione della Catalogna

1) I mezzi di trasporto siano solo due: (che chiamerò X e Y)
2) Due città siano legate da un unico mezzo di trasporto
3) Non ci siano tre città legate tra di loro dallo stesso mezzo di trasporto

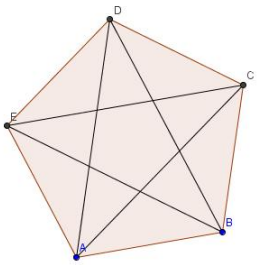
Quante città ci sono, al massimo, in questa regione?

Per rispondere a questa domanda basta considerare che da ogni città ci possono essere al massimo due città collegate ad essa con il mezzo di trasporto X e altre due città collegate ad essa con il mezzo di trasporto Y. Infatti, se ci fossero tre città collegate a questa città tramite lo stesso mezzo di trasporto, esse o sono tutte e tre collegate tra loro con l'altro mezzo di trasporto e quindi formano un triangolo di città legate tra di loro dallo stesso mezzo di trasporto, oppure vi sono almeno due di queste città collegate tra loro con lo stesso mezzo di trasporto che le collega alla prima città e quindi formano ugualmente un triangolo di città legate tra di loro dallo stesso mezzo di trasporto.

Quindi il numero massimo di città in questa regione è uguale a 5.

Un esempio di regione con 5 città può essere una regione in cui le città sono i vertici di un pentagono. I collegamenti di tipo X sono quelli che formano i lati del pentagono, e quelli di tipo Y sono quelli che formano le diagonali interne al pentagono.

In figura, ho chiamato le città con i nomi A, B, C, D, E ed ho disegnato con due colori distinti i collegamenti di tipo X e quelli di tipo Y.



10 *Esempio di* ***Cid***.

Torniamo ora al problema originale:

Quante città ci sono, al massimo, in Catalogna?

Per rispondere a questa domanda occorre considerare che da ogni città ci possono essere al massimo cinque città collegate ad essa con il mezzo di trasporto X (aereo), altre cinque città collegate ad essa con il mezzo di trasporto Y (treno) ed altre cinque con il mezzo di trasporto Z (bus).

Infatti, se ci fossero sei città collegate a questa città tramite lo stesso mezzo di trasporto, esse o sono tutte e sei collegate tra loro con gli altri due mezzi di trasporto e quindi contengono un triangolo di città legate tra di loro dallo stesso mezzo di trasporto in quanto abbiamo appena verificato che con solo due mezzi di trasporto non è possibile collegare più di cinque città senza formare un triangolo di città legate tra di loro dallo stesso mezzo di trasporto.

Oppure, vi sono almeno due di queste città collegate tra loro con lo stesso mezzo di trasporto che le collega alla prima città e quindi formano ugualmente un triangolo di città legate tra di loro dallo stesso mezzo di trasporto.

Quanto fatto finora ci dimostra che le città della Catalogna non possono essere più di 16 (Il numero 16 deriva da: 1 + 5 + 5 + 5), ma possono essere 16? La risposta è SÌ.

Il modo migliore per dimostrarlo è fornire un esempio. Siccome un disegno dei collegamenti tra 16 città sarebbe illeggibile, ho deciso di rappresentare con una tabella i collegamenti tra le varie città. Per una maggiore leggibilità della tabella, ho colorato le caselle della tabella nel seguente modo:

- se due città sono collegate tra loro con l'aereo, la casella è di colore azzurro,
- se due città sono collegate tra loro con il treno, la casella è di colore verde,
- se due città sono collegate tra loro con il bus, la casella è di colore giallo.

		Barcelona	Città 1	Città 2	Città 3	Città 4	Città 5	Città 1	Città 2	Città 3	Città 4	Città 5	Città 1	Città 2	Città 3	Città 4	Città 5
			Zona 1					Zona 2					Zona 3				
Barcelona			X	X	X	X	X	Y	Y	Y	Y	Y	Z	Z	Z	Z	Z
Zona 1	Città 1	X		Z	Y	Y	Z	Y	Y	X	Z	X	X	Z	Y	Z	X
	Città 2	X	Z		Z	Y	Y	X	Y	Y	X	Z	X	X	Z	Y	Z
	Città 3	X	Y	Z		Z	Y	Z	X	Y	Y	X	Z	X	X	Z	Y
	Città 4	X	Y	Y	Z		Z	X	Z	X	Y	Y	Y	Z	X	X	Z
	Città 5	X	Z	Y	Y	Z		Y	X	Z	X	Y	Z	Y	Z	X	X
Zona 2	Città 1	Y	Y	X	Z	X	Y		X	Z	Z	X	Y	Z	Z	Y	X
	Città 2	Y	Y	Y	X	Z	X	X		X	Z	Z	X	Y	Z	Z	Y
	Città 3	Y	X	Y	Y	X	Z	Z	X		X	Z	Y	X	Y	Z	Z
	Città 4	Y	Z	X	Y	Y	X	Z	Z	X		X	Z	Y	X	Y	Z
	Città 5	Y	X	Z	X	Y	Y	X	Z	Z	X		Z	Z	Y	X	Y
Zona 3	Città 1	Z	X	X	Z	Y	Z	Y	X	Y	Z	Z		Y	X	X	Y
	Città 2	Z	Z	X	X	Z	Y	Z	Y	X	Y	Z	Y		Y	X	X
	Città 3	Z	Y	Z	X	X	Z	Z	Z	Y	X	Y	X	Y		Y	X
	Città 4	Z	Z	Y	Z	X	X	Y	Z	Z	Y	X	X	X	Y		Y
	Città 5	Z	X	Z	Y	Z	X	X	Y	Z	Z	Y	Y	X	X	Y	

Per aiutare a capire la costruzione della tabella ho diviso le 16 città in quattro gruppi, il primo gruppo è formato dalla sola capitale (Barcelona) e gli altri 3 gruppi da tre regioni (o zone) composte da 5 città ciascuna.

Per amore di completezza, dobbiamo dirvi che ***Zar*** ci ha scritto ancora:

Tornando al quesito "serio" relativo alle città della Catalogna, penso che meriterebbe qualche pipa, qualche birra e qualche coniglio in più.

Ho cercato qua e là ed ecco quello che ho trovato: Abbiamo un grafo completo di ordine N (cioè un poligono di N lati con tutte le possibili diagonali). Vogliamo colorarle con tre colori in modo tale che non vi siano triangoli coi lati tutti dello stesso colore. Questo si chiama *problema di Ramsey multicolore*

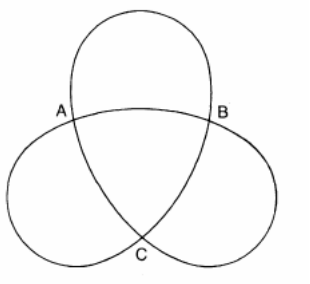
http://en.wikipedia.org/wiki/Ramsey%27s_theorem (il problema originale, o più famoso, era bicolore, noto anche come il problema delle strette di mano).

Poi ha provato a risolvere lui, ma queste S&N sono ormai talmente lunghe che dobbiamo fermarci qui. Ma continuate a scriverci, pubblicheremo il più possibile. Non ci resta che salutarvi e seguire il resto delle avvincenti proposte sui problemi di Ramsey!

5. Quick & Dirty

Essendo *quick* ed essendo *dirty*, una delle regole di questa rubrica è di non avere disegni, altrimenti è troppo facile capire cosa sta succedendo (e la parte *dirty* viene male); purtroppo, certe volte non se ne può fare a meno, visto che la spiegazione "suppergiù ad anelli borromei, ma con un filo unico" verrebbe decisamente male.

Di sicuro (visto che ne abbiamo già parlato) ricorderete che la definizione di nodo, in matematica, richiede non solo che ci sia un nodo nella corda, ma che i due estremi della corda siano poi uniti tra di loro; infatti, non deve essere possibile disfare il nodo.



Bene, avete una corda che forma la figura a fianco, ma non sapete se nei tre punti *A*, *B* e *C* la corda passa sopra o sotto se stessa. Quello che vorremmo sapere, è quale sia la probabilità che la corda sia effettivamente annodata.

6. Pagina 46

Consideriamo la somma:

$$\begin{aligned}&[\cos\varphi + i\sin\varphi] + [\cos(\varphi+\alpha) + i\sin(\varphi+\alpha)]\\ &+ [\cos(\varphi+2\alpha) + i\sin(\varphi+2\alpha)] + \ldots\\ &+ [\cos(\varphi+n\alpha) + i\sin(\varphi+n\alpha)].\end{aligned}$$

Calcoliamo i coefficienti per le parti immaginarie e reali della somma; indicando $\cos\varphi + i\sin t$ come a e $\cos\alpha + i\sin\alpha$ come x, se applichiamo la formula per la moltiplicazione dei numeri complessi e la formula di De Moivre, possiamo trasformare la formula mostrata sopra in:

$$\begin{aligned}
\sum_{i=0}^{n} ax^i &= \frac{ax^{n+1}-a}{x-1} \\
&= (\cos\varphi + i\sin\varphi)\frac{\cos(n+1)\alpha + i\sin(n+1)\alpha - 1}{\cos\alpha + i\sin\alpha - 1} \\
&= (\cos\varphi + i\sin\varphi)\frac{[\cos(n+1)\alpha - 1] + i[\sin(n+1\alpha)]}{(\cos\alpha - 1) + i\sin\alpha} \\
&= (\cos\varphi + i\sin\varphi)\frac{-2\sin^2\frac{n+1}{2}\alpha + 2i\sin\frac{n+1}{2}\alpha\cos\frac{n+1}{2}\alpha}{-2\sin^2\frac{\alpha}{2} + 2i\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}} \\
&= (\cos\varphi + i\sin\varphi)\frac{2i\sin\frac{n+1}{2}\alpha\left[\cos\frac{n+1}{2}\alpha + i\sin\frac{n+1}{2}\alpha\right]}{2i\sin\frac{\alpha}{2}\left[\cos\frac{\alpha}{2} + i\sin\frac{\alpha}{2}\right]} \\
&= \frac{\sin\frac{n+1}{2}\alpha}{\sin\frac{\alpha}{2}}(\cos\varphi + i\sin\varphi)\frac{\left(\cos\frac{n+1}{2}\alpha + i\sin\frac{n+1}{2}\alpha\right)\left(\cos\frac{\alpha}{2} - i\sin\frac{\alpha}{2}\right)}{\cos^2\frac{\alpha}{2} + \sin^2\frac{\alpha}{2}} \\
&= \frac{\sin\frac{n+1}{2}\alpha}{\sin\frac{\alpha}{2}}\left[\cos\left(\varphi + \frac{n}{2}\alpha\right) + i\sin\left(\varphi + \frac{n}{2}\alpha\right)\right].
\end{aligned}$$

Da cui segue immediatamente l'identità richiesta.

Come dicevamo, anche se una cosa del genere sembra interessare solo Alice, tenetela a tiro. Verrà utile, prima di Natale...

7. Paraphernalia Mathematica

7.1 Non ho capito… [001]: Dovremmo essere serî (ma non lo saremo)

A parte un paio di aneddoti, visto che Rudy molti anni fa su queste cose ci ha lavorato[18], il motivo principale di questo pezzo è rendere pubblica una cosa che avevamo trovato anni fa in rete e che, almeno dalle ricerche dell'anno scorso, sembra sparita; se volete la versione completa in inglese, chiedete e invieremo. Eccola.

> Quando uno specialista nell'argomento che vogliamo trattare ha bisogno di due variabili, non le chiama ***A*** e ***B***; per qualche oscura tradizione, le chiama Alice e Bob.
>
> Ora, sono stati scritti centinaia di articoli a proposito di Alice e Bob; nel corso degli anni, queste due persone hanno cercato di frodare le Compagnie di Assicurazione, hanno giocato a poker per posta con puntate altissime e si sono scambiate messaggi segreti attraverso telefoni sorvegliati.
>
> Se mettiamo assieme i piccoli dettagli che possiamo raccogliere qui e là da una marea di documenti, otteniamo un ritratto affascinante di quali siano le loro vite. Tanto per cominciare, vediamo che sovente Bob è impegnato nella vendita di azioni a speculatori; dalla quantità di azioni che vende, c'è da supporre che Bob sia un intermediatore di professione.
>
> Però, date le sue preoccupazioni nei confronti delle intercettazioni telefoniche, è molto probabile che sia anche coinvolto in qualche gruppo sovversivo; e dal numero di azioni che Alice compra da lui, possiamo facilmente dedurre che Alice sia uno speculatore.
>
> Inoltre, Alice vuole tenere nascosti a suo marito i suoi legami finanziari con Bob.
>
> Riassumendo, Bob è un intermediario sovversivo e Alice uno speculatore dalla doppia vita.
>
> Ma Alice ha una serie di problemi gravi.
>
> Lei e Bob parlano unicamente per telefono, e nel paese dove vivono le telefonate sono estremamente costose. E loro sono molto tirchi, quindi la prima cosa che Alice deve fare è minimizzare il costo delle telefonate.
>
> I telefoni sono anche molto disturbati; certe volte, i rumori di fondo sono tali che Alice e Bob possono a malapena sentirsi.
>
> Infine, Alice e Bob hanno una serie di nemici estremamente potenti, tra i quali l'Ufficio Imposte e la Polizia Segreta; questo è molto grave, in quanto i loro argomenti principali di conversazione sono la frode fiscale e come sovvertire il governo.
>
> Inoltre, questi nemici hanno anche risorse illimitate: possono ascoltare in qualsiasi momento le conversazioni tra Alice e Bob.
>
> E sono molto infidi. Uno dei loro trucchi favoriti è di telefonare ad Alice sostenendo di essere Bob. Capite quindi che Alice deve stare molto attenta, e penserete che debba riconoscere dalla voce se si tratta di Bob. No; Alice non ha mai incontrato Bob, e non ha la più pallida idea di quale sia la sua voce.

[18] Se, nei primissimi anni dell'ultimissimo decennio dell'altro millennio avete frequentato il Politecnico di Torino e avete usato la versione 2 delle "lavatrici", sappiate che tutto il software locale (con l'eccezione dei driver Ethernet, ma inclusa grafica, lettore badge e stampante) lo aveva scritto Rudy. E dentro c'era anche quello di cui parleremo.

> Come vedete, Alice deve affrontare un mucchio di problemi; dimenticavo, va anche detto che Alice non si fida di Bob; non sappiamo il motivo, ma probabilmente nel passato c'è stata qualche incomprensione.
>
> La maggior parte della gente, nelle condizioni di Alice, lascerebbe perdere tutto. Ma non Alice. Alice ha un coraggio grandioso.
>
> Contro tutti i problemi, attraverso linee telefoniche disturbate, intercettata dall'Ufficio Imposte e dalla Polizia Segreta, Alice cerca allegramente, con qualcuno di cui non si fida, che non si riesce a sentire bene e che molto probabilmente è qualcun altro, di frodare il fisco e di organizzare un colpo di stato, il tutto minimizzando le spese telefoniche.
>
> Un crittografo è una persona convinta che Alice ce la farà[19].

Carino, vero? Bene, adesso cominciamo, e la prendiamo da un punto di vista eminentemente pratico.

L'idea alla base di ogni algoritmo di crittografia è, detta in inglese, "Fast&Hard": veloce (nel senso di implementabile con facilità anche su una caffettiera con una manciata di byte di memoria) e robusto (nel senso che nessuno ci capisce un tubo); delle ultime novità nel campo ne parleremo un'altra volta[20], per adesso ci vorremmo limitare alla prima cosa seria nel campo.

"Seria" in un senso molto semplice; per alcuni millenni (la notizia di un testo cifrato compare già nella Bibbia) l'idea di base è sempre stata quella di tenere segreto il *metodo* di cifratura; se vi arriva nella mailbox una cosa che si intitola "TWFK OCVJGOCVKEK" probabilmente pensereste ad una prestigiosa rivista di elicicoltura edita ad Ulan Bator, ma se vi diciamo che è un codice a trasposizione (o *di Cesare*: proprio il Giulio, ve l'avevamo detto che è roba vecchia) di passo due, forse la cosa diventa più interessante.

Il guaio dei metodi che nascondono il metodo è che se qualcuno scopre il metodo, dovete usare un altro metodo; dall'enfasi che abbiamo messo sulla parola "metodo", dovreste aver capito che proprio lì sta il busillis.

Ci si avvia verso la soluzione al problema quando oltre al metodo si utilizza una qualche altra parte (la *chiave*) variabile e mantenuta segreta: ad esempio, uno dei primi cifrari di questo tipo prevedeva di scrivere il testo in chiaro (senza spazi) sotto la chiave, e poi di trasmettere il messaggio leggendo in verticale secondo l'ordine delle lettere dell'alfabeto della chiave (e inserendo degli spazi per facilitare la trasmissione); ad esempio, " KLEOC EOITN ETNAE RREAA IEEDO ROLSI IOLFT EBAAP LIESI TTMKK NIAQM ARKTP DTVRE KNRCN SAOET PNUPR EIRTE PSISP INTIO OELNS TSREE INEER REAEK IETNL", dovreste conoscerla, ma il procedere per tentativi può rivelarsi piuttosto noioso, anche se facile[21]; se però non sapete nulla della frase (o meglio, delle frasi: due) usate, vi conviene chiedere all'agente segreto con metodi poco gentili che si fa prima.

Cerchiamo di stabilire cosa serva ad un sistema di cifratura.

Tanto per cominciare, abbiamo il *Testo in Chiaro*, di solito indicato con la lettera **P** (da *Plain Text*), che possiamo assumere come una stringa di bit; da questo, vogliamo ottenere un'altra stringa **C** di *Testo Cifrato* attraverso un *Algoritmo Crittografico* (solitamente indicato con "$\oplus$", e molto sovente è proprio uno XOR) e una *Chiave* **K**.

---

[19] "*The Alice and Bob after-dinner speech*", di John Gordon; Seminario di Zurigo, aprile 1984. Va avanti per altre cinque o sei pagine, ma per capire le altre battute prima dovete studiare: se non lo trovate in rete, vi mandiamo la nostra copia.

[20] Come dovreste aver intuito dal titolo, abbiamo intenzione di tirarla per le lunghe.

[21] La cosa si complica ulteriormente se prendete questo aggeggio e lo rimettete nel calcolo; per quanto ne sappiamo, il "doppio passaggio" avente come chiave una frase di un libro (diverso per ogni agente) era usato dal Servizio Segreto inglese durante la prima guerra mondiale.

Si intuisce facilmente che un buon sistema crittografico deve originare un **C** contenente il massimo disordine, ossia il nostro algoritmo deve produrre una cosa il più possibile simile al caos.

Il più semplice degli algoritmi di cifratura è, come accennavamo, l'uso dell'*or esclusivo* tra **P** e **K**; il sistema funziona ragionevolmente bene sin quando avete una chiave **K** lunga quanto il messaggio da cifrare e *la usate una sola volta*; questo punto è particolarmente critico in quanto l'avere due messaggi cifrati sicuramente con la stessa chiave permette di decrittare con relativa facilità i messaggi, studiando le ricorrenze dei gruppi di simboli; ai tempi della Guerra Fredda, è stato proprio il riuso di una chiave a permettere la decifratura di un codice utilizzato dagli agenti sovietici.

Già nel diciannovesimo secolo, ***Kerckhoff*** ha dimostrato che la conoscenza dell'algoritmo, anche con i metodi più semplici, ha una scarsissima importanza se non si conosce la chiave; oggi, quando si progetta un algoritmo di crittografia, si tendono ad analizzare sostanzialmente tre casi:

- **Solo Cifrato**: il decrittatore ha a disposizione il solo testo cifrato, e deve ricavare tutto quanto.
- **Testo Chiaro Noto**: il decrittatore ha a disposizione il testo cifrato e almeno parti del testo in chiaro.
- **Testo Scelto**: Questo è complicato, in quanto ha tre sottocasi:
    - **Testo Chiaro Scelto** vero e proprio, in cui il decrittatore sceglie il messaggio che deve essere cifrato;
    - **Testo Cifrato Scelto**, in cui il decifratore sceglie quale testo cifrato debba essere decifrato;
    - **Testo Chiaro Scelto in Modo Adattativo**, in cui il decifratore sceglie il testo chiaro da cifrare in funzione dei testi cifrati trasmessi precedentemente.

Speriamo a questo punto sia tutto quanto abbastanza cifrato… Bene, cominciamo ad utilizzare qualche numero, almeno per misurare la sicurezza dell'algoritmo.

Prendiamo un algoritmo di cifratura con una chiave formata da k bit, e supponiamo di avere un metodo per decrittarlo; la domanda chiave è: quante chiavi dobbiamo tentare, per decrittare l'algoritmo? Questo numero indica la sicurezza dell'algoritmo e, evidentemente, più è vicino a 2^k, più l'algoritmo è sicuro; in questo linguaggio, un algoritmo perfetto viene quindi definito 2^k-sicuro.

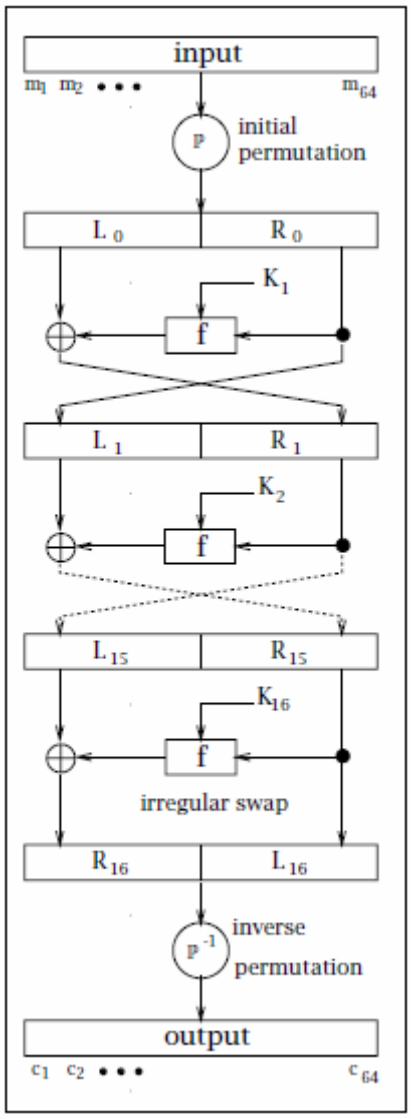
La cosa quasi incredibile è che con i tre rozzi strumenti che abbiamo a disposizione, ossia la trasposizione, la sostituzione e l'OR esclusivo, è possibile fare delle cose in grado di generare corposi mal di testa agli *eavesdroppers*[22]. Prima, però, un po' di storia.

Tutto comincia nel 1965, quando per "computer" si intendevano quegli aggeggi che ne servivano quattro per tutto il Regno Unito (forse ne avrebbero comprati cinque perché la Scozia ne voleva uno tutto suo), e il concetto di "World Wide Web" apparteneva più alla fantascienza con grossi ragni che all'informatica; in quei giorni, il Congresso degli Stati Uniti affidò al National Bureau of Standards l'incarico di definire delle linee guida per l'utilizzo civile[23] dei computer. Dopo appena cinque anni di pensate (quindi arriviamo al 1970), ci si rende conto che anche i civili hanno bisogno di rendere sicuri alcuni dati

[22] Qualcuno conosce una traduzione buona quanto l'originale di questo termine? "Ascoltatore non autorizzato" è corretta, ma fa schifo…

[23] Nel senso che non li usavano più solo i militari; all'altro significato di "uso civile del computer" purtroppo non ci siamo ancora arrivati adesso.

sensibili, e quindi l'NBS lancia un concorso per lo sviluppo di un sistema di cifratura pubblico ragionevolmente sicuro[24].



Al concorso non partecipano moltissimi, ma comunque il migliore viene considerato quello proposto dall'IBM: un cifrario di Feistel[25] a sedici giri con chiave a cinquantasei bit[26] e prende il nome di **DES**, *Data Encryption Standard*; cerchiamo di capire come funziona, aiutandoci con il disegno a fianco (rubato alle specifiche, quindi ve lo beccate in inglese).

Per prima cosa dividete il messaggio da cifrare in blocchi di 64 bit; basta seguire il percorso di uno solo di questi blocchi, tanto fanno tutti la stessa strada.

Indi, restiamo nel semplice: applicate una permutazione ***P***; dal punto di vista crittografico serve a pochino (tant'è che nelle analisi non la si usa quasi mai), ma l'algoritmo ufficiale la prevede… senza, non potete chiamarlo DES.

Poi arrivano i sedici cicli di cui dicevamo sopra. Ne descriviamo uno solo.

Inizio Ciclo:

Tanto per cominciare, dovete scegliere quarantotto bit dalla chiave di cinquantasei[27]: per sceglierli, dividete in due parti la chiave (questa divisione con la successiva rotazione sono alla base dei cosiddetti *Codici di Feistel*) e ruotate ognuna delle due metà di uno o due bit[28]: di un bit ai giri 1, 2, 9 e 16, di due agli altri. Rimettete assieme le due metà e scegliete i quarantotto bit rimescolandoli secondo la seguente tabella:

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Speriamo sia chiaro: in settima posizione (seconda riga, prima colonna) ci va il terzo bit, e avanti in questo modo, la rotazione di uno o due di cui sopra assicura la variabilità della chiave ad ogni giro.

Il passo successivo serve a "spalmare" l'informazione di ogni bit su più bit: prendete la metà destra dei dati (32 bit) e portatela a 48 bit, prendendo la sequenza dalla fine e

[24] Se, a questo punto, vi state ponendo delle domande da complottisti, resistete sino alla sezione "domande paranoiche".

[25] Due motivi, per il nome: il primo è che Horst Feistel lavorava all'IBM, il secondo ve lo spieghiamo dopo.

[26] Secondo complotto.

[27] Terzo complotto.

[28] Quarto complotto.

ripetendo (scambiando inoltre tra di loro le ripetizioni) ogni quarto e quinto bit (ottengo quindi quinto-quarto-quinto-quarto): se vi preoccupa il fatto che ad ogni ciclo usate sempre la metà destra dei bit, tranquilli; alla fine di ogni ciclo, destra e sinistra si scambiano e quindi al prossimo giro spalmate l'altra parte.

Adesso prendete i 48 bit della sottochiave e fate uno *XOR* con il mezzo messaggio spalmato di cui sopra: il risultato lo passate alla cosiddetta *S-Box*, che vi ritrasformerà i 48 bit di input di nuovo in 48 bit di output: questa la guardiamo un attimo bene, perché sta proprio qui dentro la complessità del DES.

Una *S-Box* è una matrice con quattro righe e sedici colonne. Tanto per cominciare, prendete blocchi di *sei* bit; il primo e l'ultimo, se li mettete assieme, vi danno un valore compreso tra zero e tre, che userete come indice di riga; gli altri due un valore tra zero e quindici, che userete come indice di colonna: come risultato tenete il valore che trovate all'intersezione.

Tutto chiaro? Bene. La *S-Box* cambia ad ognuno dei sedici giri. Se le volete tutte trovatevi le specifiche, qui vi diamo solo quella del quinto giro[29].

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	11	14	2	13	6	15	0	9	10	4	5	3

La caratteristica della *S-Box* è che ogni possibile valore tra zero e quindici compare una e una sola volta in ogni riga: ricordatevelo per dopo le paranoie.

Fine Ciclo.

…E meno male, che ormai i nostri bit hanno un mal di testa che te lo raccomando. Ah, ricordatevi ancora di fare l'inverso della permutazione ***P*** dell'inizio, per rimettere a posto le cose.

Poi mandate tutto in linea, ragionevolmente tranquilli.

Come dicevamo, una mente paranoica potrebbe a questo punto essersi posta delle domande. Vediamole, nell'ordine nel quale le abbiamo incontrate:

1) **Perché l'NBS e non l'NSA?** Perché c'era la paura che la decrittazione di un algoritmo pubblico dell'NSA (National Security Agency) avrebbe aiutato a capire la "filosofia" dei sistemi non-pubblici.

2) **Perché chiave a 56 e non a 54 bit?** Perché gli altri otto servivano per il controllo di parità.

3) **Perché solo 48 e non tutta la chiave? Non rischio di semplificare l'algoritmo, così?** No, perché ogni volta prendete dei bit diversi: in realtà, in questo modo lo complicate.

4) **Perché solo di uno o due? Non posso ruotarla di più?** Qui forse un po' di ragione l'avete: limitarsi a uno o due è stata una richiesta dell'NSA, in origine gli shift erano da uno a cinque bit.

5) **Il fatto che in quattordicesima colonna siano tutti numeri "piccoli", non è una debolezza?** No, anzi, il fatto che i numeri di qualche colonna "si somiglino" fa sì che sia molto più difficile trovare quali siano i due bit di riga.

Siete più tranquilli, adesso, a proposito del vostro conto corrente o dei vostri voti d'esame? Beh, non avete *proprio* tanta ragione di esserlo.

[29] Quattordicesima colonna: quinto complotto

Infatti, nonostante le obiezioni viste sopra siano piuttosto semplici, qualche specialista nel ramo ha dei grossi dubbi: ***Diffie*** e ***Hellmann*** (prima o poi riparleremo di questi due tizi), ad esempio, sostennero anni fa che con la modica spesa di venti milioni di dollari era possibile costruire un computer in grado di decrittare qualsiasi messaggio codificato DES in meno di un giorno; non solo ma, usando versioni semplificate del DES (al massimo sette cicli anziché sedici), si è dimostrato che è soltanto 2^{45}-sicuro: in pratica, vi basta provare **un milionesimo** delle chiavi possibili per decrittarlo. Tranquilli, oltre il settimo giro il metodo non funziona, e siete "costretti" (metodo di Shamir) a provare almeno un decimillesimo delle $2^{56} \approx 10^{19}$ possibili chiavi (vi ricordate, che di sessantaquattro bit ne usate solo cinquantasei?); il metodo, noto anche come **criptanalisi differenziale**, si basa proprio sulle *S-Box*. Vediamolo almeno a grandi linee.

Se prendiamo una *S-Box*, non è molto difficile calcolare tutti i sedici possibili output rispetto ai sessantaquattro input; in questo modo, posso costruire una tabella che mi indichi, per una data differenza tra due input, quale sia la differenza tra i due output: se le *S-Box* fossero lineari, ossia se per due input nella scatola fosse $DES(X \oplus X^*) = DES(X) \oplus DES(X^*)$, potrei decrittare il tutto anche a mano; il fatto che non lo siano aiuta, ma Shamir ha scoperto che con alta probabilità ogni differenza tra due testi genera una *caratteristica* ben specifica, e quindi, anche se la redistribuzione di un singolo testo somiglia molto al disordine completo (ossia distribuzione uniforme, probabilisticamente parlando), quando si vanno a considerare le differenze tra due testi si trovano dei punti di accumulazione; non solo, ma queste caratteristiche sono anche *iterative*, ossia sopravvivono (anche se con probabilità piuttosto bassa) alle sedici iterazioni.

Come ultimo punto sulle debolezze del sistema, va detto che in certi casi gli algoritmi proprio se li cercano, i guai: esistono infatti delle chiavi particolarmente facili da decrittare: sono le cosiddette "chiavi deboli" (che semplicemente non cifrano, sono quattro, per il DES), le "chiavi semideboli" (sei, queste cifrano solo dei pezzi) e le "chiavi probabilmente deboli (quarantotto, hanno accumulazioni evidenti). Inutile dire che sono note e che tutti i cifratori le fuggono come la peste.

Un'idea, a questo punto, potrebbe essere quella di usare il metodo degli inglesi nella prima guerra mondiale, ovverossia far girare due volte tutta la baracca; è interessante notare che questa procedura in realtà *indebolisce* il DES, esponendolo ad attacchi del tipo "meet in the middle", di avvicinamento ciclico alla soluzione, con tempi dell'ordine della decrittazione del DES singolo; ancora più stranamente, il far girare la macchina *tre* volte (con tre chiavi diverse), rende la cosa decisamente più sicura, tant'è che a questo punto si fida anche la vostra banca: attenzione però che se riciclate al terzo passaggio la prima chiave il vostro sistema diventa solo 2^{56}-sicuro (ossia equivalente a un DES singolo perfetto), contro un'aspettativa di 2^{108}; probabilmente è una leggenda metropolitana, ma si narra che, anni fa, quando vennero cambiati i codici di accesso bancomat passando da quattro a cinque cifre, fosse proprio perché la versione precedente riciclava la prima chiave. Nessuno ce lo ha mai confermato, quindi la notizia ve la vendiamo allo stesso prezzo alla quale l'abbiamo acquistata noi.

Quindi, non preoccupatevi del fatto che qualcuno sia in ascolto sulla linea: preoccupatevi di più dello *shoulder surfer* in coda dietro di voi.

La prossima volta, non ci limitiamo a bazzecole come qualche migliaio di euro sul vostro conto corrente: cifriamo *la lista della spesa*!

Rudy d'Alembert
Alice Riddle
Piotr R. Silverbrahms