Hanc Marginis Exiguitas Non Caperet

Rudi Mathematici

Rivista fondata nell'altro millennio

Numero 193 – Febbraio 2015 – Anno Diciassettesimo

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
RM190 ha diffuso 3'161 copie e il 01/02/2015 per Google eravamo in 11'300 pagine.

Walter Benjamin e il passaggio dall'affresco al *poster* ci avevano abituato alla riproducibilità delle opere d'arte, ma il lavoro del gruppo ***Deskriptiv*** (www.deskriptiv.de) ci pare un ulteriore passo avanti: le opere vengono progettate al computer e quindi realizzate con una stampante 3D. E sul sito potete comprarle per meno di cento euro (se non sapete il tedesco, fatevi aiutare da Treccia).

1. La face l'École Militaire, #16

"Questo è il privilegio del genio: percepire, vedere relazioni dove occhi comuni vedono solo fatti isolati."

"Nelle scienze sperimentali, i periodi dei successi più brillanti sono quasi sempre divisi da lunghi intervalli di quiete quasi assoluta."

"Il calcolo delle probabilità, quando confinato nei giusti limiti, dovrebbe interessare in egual misura il teorico, lo sperimentatore e l'uomo di stato."

"Mi sono spesso avvilito vedendo uomini che si disputavano un pezzo di pane al pari degli animali. I miei sentimenti a riguardo sono cambiati molto da quando ho provato personalmente i morsi della fame. Ho infatti scoperto che un uomo, qualunque fossero la sua origine, la sua educazione e le sue abitudini, sotto certe circostanze è governato molto più dal suo stomaco che dal suo cervello e dal suo cuore."

Il termine "Seconda Repubblica" è andato molto di moda, negli ultimi decenni, al punto di essere entrato senza dubbio nel lessico abituale degli italiani. Abbastanza recentemente è tornato alla ribalta, e non tanto perché l'ipotetica Seconda Repubblica goda di particolare salute o benevolenza, ma proprio per la causa opposta: molti giornalisti e operatori mediatici ritengono piuttosto che i cambiamenti in atto nel sistema politico italiano siano ormai tali da giustificare la celebrazione del funerale della Seconda Repubblica, in modo che questa possa finalmente far posto alla Terza.

1 *Nasce la repubblica – la Prima*

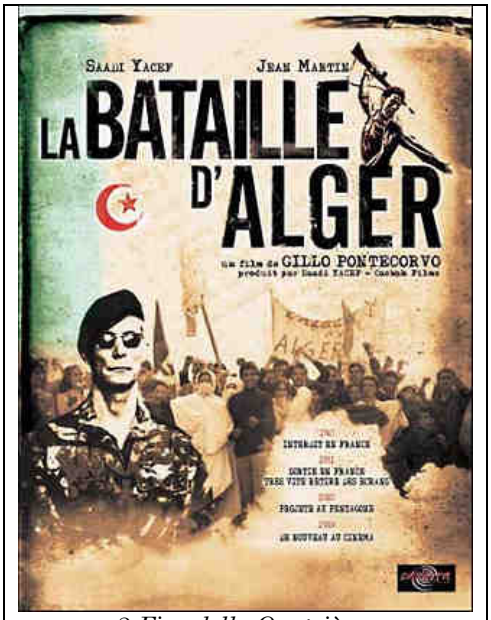
L'espressione prese piede all'inizio degli anni Novanta, quando gli sconvolgimenti nati soprattutto sull'onda degli scandali di "Tangentopoli" e dell'inchiesta "Mani Pulite" condussero effettivamente ad una profonda rivoluzione delle forze politiche: i partiti che per quasi mezzo secolo erano stati ininterrottamente i protagonisti del Parlamento scomparirono quasi simultaneamente – seppur in modi e misure diverse – e vennero sostituiti da forze politiche nuove, quantomeno nel nome e in parte nei programmi.

La cesura nel mondo politico insomma ci fu, anche se probabilmente sono molti coloro che si appelleranno alla celebre sentenza di Tomasi di Lampedusa, nel Gattopardo, e sosterranno che cambiò tutto per far in modo che non cambiasse nulla.

Giudizi di così alta levatura politica sono comunque al di fuori del piccolo perimetro d'una modesta e scherzosa e-zine di matematica ricreativa, e fuori resteranno. Si può comunque affermare che, almeno dal punto di vista formale, il concetto di Seconda Repubblica è davvero improprio. È verosimile che gli operatori dell'informazione, per rimarcare l'importanza delle mutazioni in atto, lo abbiano costruito sul calco delle denominazioni francesi. I cugini transalpini sono infatti ben più avanti nel numero d'ordine: quella che abitano in quest'inizio di terzo millennio è già la loro Quinta, ed è possibile che un parziale di 5 a 1 sia considerato un bilancio troppo severo nei nostri confronti.

Resta però il fatto indiscutibile che un numero d'ordine da affiancare alla forma dello stato è storicamente giustificabile solo a valle d'una mutazione radicale, costitutiva, mentre la Costituzione della Repubblica Italiana in vigore è sostanzialmente la stessa che ha ratificato la nostra forma di stato decisa nel 1946.

Per noi, insomma, "seconda repubblica" è solo un comodo modo di dire, che nessun costituzionalista e nessuno storico si sentirebbe di avallare in via ufficiale. A Parigi, invece, la storiografia ufficiale non si discosta da quella colloquiale: la *Cinquième République* nasce ufficialmente il 5 ottobre 1958, sull'onda di un referendum celebratosi poco prima, il 28 settembre, con il quale i francesi cambiano la loro costituzione trasformando la Francia da repubblica parlamentare a repubblica presidenziale[1]. Il padre fondatore dell'attuale forma repubblicana è stato il generale Charles De Gaulle, che propugnò la radicale trasformazione istituzionale per risolvere il pantano politico in cui era finita la Quarta Repubblica, soprattutto dopo la crisi d'Algeria[2].



2 *Fine della Quatrième*

La repubblica numero quattro era invece, in buona sostanza, la continuazione di quella sopravvissuta alla seconda Guerra Mondiale: ufficializzata da un'apposita costituzione repubblicana nell'ottobre del 1946, non ebbe mai vita facile. Puramente parlamentare, soffriva dei mali caratteristici di questa forma istituzionale quando non esiste un partito dominante: tra il 1946 e il 1958 tre partiti politici, grosso modo della stessa forza elettorale, partorirono ventidue governi diversi.

Come si è detto, di fatto la *Quatrième République* altro non era che la continuazione della *Troisième*, che però ebbe vita più lunga, pur non essendo affatto indenne dai medesimi mali della sorella più giovane. La Terza Repubblica Francese cessò di esistere nel giugno del 1940, quando l'invasione tedesca della Francia condusse alla frammentazione dello stato, lasciandolo nominalmente governato dal regime collaborazionista di Vichy. Abbastanza curiosamente, la causa non solo della morte, ma anche della nascita della repubblica scaturiva da una sconfitta inflitta ai francesi dalla Germania: dopo il disastro di Sedan, nella guerra franco-prussiana del 1870, il Secondo Impero francese di Napoleone III si scioglie come neve al sole e i cugini transalpini provano per la terza volta della loro storia ad organizzarsi in forma repubblicana. Pur con gli alti e bassi di ogni nazione europea, la Terza Repubblica dura quindi per settant'anni, e mette definitivamente fine alle forme monarchiche che per secoli avevano regnato a Parigi.

Niente più regno o impero francese: del resto, l'impronta più decisa e profonda che la Francia lascia nella storia d'Europa e del mondo è tuttora quella che ha impresso nella sabbia della Bastiglia il 14 luglio 1789: la Rivoluzione Francese è stata ben di più che un quieto passaggio da una forma di governo ad un'altra, ma non di meno è opportuno ricordare che la capostipite delle cinque repubbliche francesi, la Prima Repubblica, è proprio quella che nacque senza ordinale, in un'epoca e in un continente in cui la sola parola "repubblica" suonava – letteralmente – rivoluzionaria.

[1] Il termine esatto, a dire il vero, è "semipresidenziale". Il Presidente della Repubblica Francese è eletto a suffragio universale, non è sfiduciabile dal Parlamento ed è responsabile del potere esecutivo, che esercita nominando il Primo Ministro: quest'ultimo però deve godere della fiducia del Parlamento.

[2] Crisi d'Algeria che non ci metteremo certo a ricordare qui. Comunque, un paio d'ore passate a guardare uno dei film più famosi della storia del cinema, "La battaglia di Algeri" di Gillo Pontecorvo, sono tempo sicuramente ben speso.

A metter fine alla Prima Repubblica Francese sarà il figlio più famoso della rivoluzione: il Consolato prima, l'Impero poi, trasformeranno la repubblica rivoluzionaria in un impero continentale e strettissimamente legato ai voleri d'un solo uomo, Napoleone Bonaparte. *Après lui le déluge*, con buona pace di Luigi XV, che è l'autore della celebre frase.

Al pari di quella italiana, mal definita e ufficialmente ancora inesistente, la meno nota tra le repubbliche francesi è forse proprio la Seconda. Di certo, è stata la più breve, sopravvivendo solo i quattro anni che vanno dal 1848 al 1852; ma non si può dire che fossero anni tranquilli. Dopo il periodo della Restaurazione e la successiva Monarchia di Luglio, la Francia si ritrova nel bel mezzo dei moti del 1848; il re, Luigi Filippo, abdica in favore del nipote, che però non salirà mai al trono: un governo repubblicano, richiesto a furor di popolo, prende le redini della Francia il 22 febbraio, proprio sotto la colonna che ancora oggi marca il luogo dove sorgeva la Bastiglia.


3 *Napoleone III*

A vederla da più di un secolo e mezzo di distanza, la Seconda Repubblica Francese suscita uno strano misto di depressione e tenerezza. Le bastano pochi mesi, poco più di cento giorni, per finire in mezzo ad una crisi istituzionale: già nel giugno del 1848 è costretta ad affidare poteri di dittatore ad un solo uomo, Louis Eugène Cavaignac, per reprimere i violenti moti popolari di protesta causati dalla crisi economica e dalla mancanza di lavoro; e prima della fine del suo movimentassimo anno di nascita (del resto, non si dice "*è successo un quarantotto*" per niente), quando riesce finalmente ad eleggere il suo primo "Presidente della Repubblica", finirà col mettere sul suo scranno più alto proprio colui che, nel giro di poco tempo, metterà fine alla sua esistenza.

È una repubblica che si sente davvero la sorellina minore della più celebre primogenita del 1789: non solo ha voluto nascere anch'essa in piazza della Bastiglia, ma ha anche preteso la Marsigliese come suo inno. Per continuare sulle somiglianze: nascono entrambe dopo una monarchia, entrambe finiscono per far posto ad un impero, e sia il Primo, sia il Secondo Impero portano ad imperatori che fanno Bonaparte di cognome, ed entrambi i Bonaparte possono a buon diritto chiamarsi figli della repubblica che hanno ucciso.

Ma soprattutto entrambe avevano uno spirito nobile, coniugato però attraverso divisioni e frammentazioni che sfociavano assai facilmente in violenza e disordini. Prima dell'elezione a presidente di Carlo Luigi Napoleone Bonaparte[3], il 20 dicembre 1848, la giovane repubblica ha già attraversato delle crisi profonde e moti di piazza violenti. Quelli più significativi sono quelli che infiammano Parigi il 24, 25 e 26 giugno.

Quando nasce, a febbraio, la Repubblica si dà naturalmente un Governo Provvisorio, il cui intento principale è quello di ribadire la natura repubblicana dello stato e indire immediate elezioni: elezioni che, per quanto limitate al solo elettorato maschile, saranno

[3] Carlo Luigi Napoleone Bonaparte è nipote del più celebre zio, in quanto figlio terzogenito di Luigi, fratello del più famoso dei figli di Corsica, e da questi piazzato sul trono d'Olanda. Nei sussidiari di scuola elementare lo si trovava spesso, coi suoi baffi lunghi e sottili e la barbetta da moschettiere, ma sempre con la sintetica didascalia "Napoleone III", visto il ruolo cruciale che ha giocato nel Risorgimento Italiano quando rivestiva ormai i panni d'imperatore. Potremmo fare un sacco di pettegolezzi su come abbia preteso in cambio dell'aiuto Nizza e la Savoia, o di come quella volpe di Cavour lo abbia circuito grazie ai bersaglieri sulla Cernaia e soprattutto "grazie alle grazie" di Virginia Oldoini, Contessa di Castiglione; ma questa è una Prestigiosa Rivista di Matematica Ricreativa, mica un Raccapezzato Fogliaccio di Gossip Pseudostorico, diamine.

le prime lezioni a suffragio universale della storia. Si tengono il 23 Aprile: sulle basi del risultato della consultazione prende forma la Commissione Esecutiva, ovvero un governo che, almeno nelle intenzioni, dovrebbe essere assai meno provvisorio. Tutti i membri che compongono la commissione assumono congiuntamente, e in modo egualitario, il titolo di "capo di stato"; anche se ad uno solo di essi – segnatamente al Presidente della Commissione – sarà dato il titolo di capo di stato in maniera formale.

Nella primavera del 1848, Parigi è in fermento come pochi altri luoghi, e come lo è stata poche altre volte nella sua pur tormentata storia. La crisi economica, il cambio di regime istituzionale, la consapevolezza e la necessità di dover lottare per ottenere non solo diritti e privilegi, ma anche, più drammaticamente, il necessario per non morire di fame, portano alla costituzione di molti partiti, associazioni, raggruppamenti. È tutto un fiorire di società, di "club", di diversa matrice politica. Tra i principali, di natura socialista: la *Société Fraternelle Centrale*, il *Club des Amis du Peuple*, il *Club de la Révolution*, il *Club Lycée des Prolétaires*, il *Club des Travailleurs Libres*, il *Club de la Société Républicaine Centrale*. Quelli più radicali: il *Club de la Sorbonne*, il *Club de la Montagne*, il *Comité Central Républicain*, il *Club Républicain*, il *Club des Francs Républicains*. Persino alcuni solo femminili, come il *Club Fraternel des Lingères* e la *Société de la Voix des Femmes*. Tutti nati nel 1848.


4 *Auguste Blanqui*

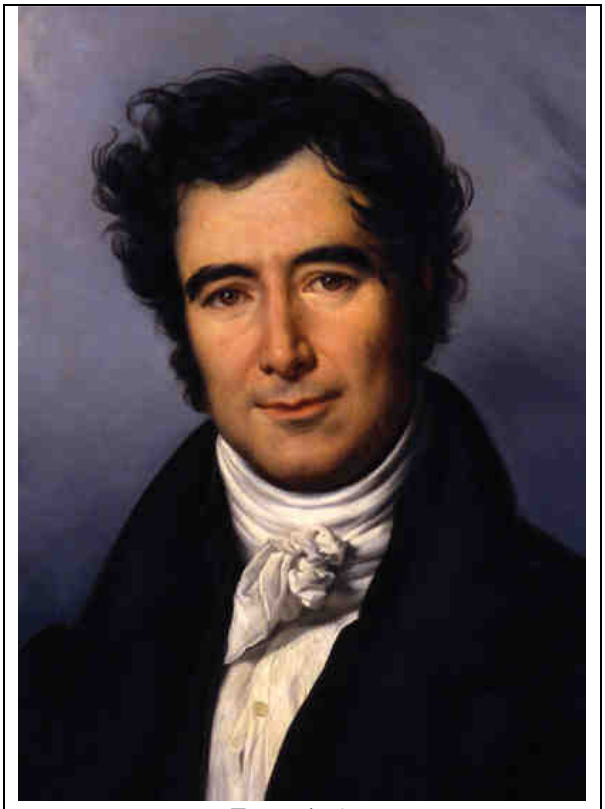
E i fondatori erano personaggi notevoli: la *Société Républicaine Centrale*, che ebbe un ruolo cruciale nei moti di piazza di giugno, quelli che misero in crisi la Commissione Esecutiva e in un certo qual modo tutta la Seconda Repubblica, era stata fondata da Auguste Blanqui, un personaggio che sembra davvero uscito dalla penna di un romanziere. Basta forse il suo soprannome a definirlo: *l'Enfermé*, che si potrebbe tradurre come "il Prigioniero", il "Galeotto", o forse, più semplicemente e correttamente, come "l'Arrestato". Blanqui subisce infatti arresti per tutta la vita, vita che in gran parte è costretto a passare in prigione. Nasce nel febbraio del 1805, da una famiglia di origini italiane, e già a diciassette anni comincia la sua attività di eterno ribelle. A diciannove anni è carbonaro, a ventidue è ferito per tre volte in una manifestazione studentesca, a ventitré progetta una spedizione in Grecia per aiutare gli insorti ellenici.

Naturalmente partecipa con un ruolo di primo piano alla rivoluzione del 1830, e nel 1831 viene arrestato per la prima volta. Da quel momento in avanti, tutta la sua vita sarà scandita da rivoluzioni, arresti, soggiorni in galera; per poi ricominciare con rivoluzioni, arresti, e così via. Subirà anche una condanna a morte nel 1840, che riuscirà ad evitare – paradossalmente – perché il suo stato di salute lo fa trasferire in una prigione ospedale fino al 1847; poi, appunto, ci sarà il '48.

È l'autore del più famoso dei motti anarchici, quel "*Ni Dieu ni maitre*"[4] che è ancora talvolta ricordato dalle sinistre radicali di tutto il mondo. La sua avventura ideologica e politica (e inevitabilmente, anche carceraria) non terminerà con la Seconda Repubblica; proseguirà contro il Secondo Impero di Napoleone III, anche qui con arresti, evasioni e complotti antigovernativi; e la sua influenza si sentirà molto anche durante la Comune di Parigi del 1871, con molti degli insorti che si riconoscevano nella sua ideologia e inneggiavano al suo nome.

[4] "Né Dio, né padroni": era anche il titolo di un giornale da lui fondato.

In quel fatale giugno del 1848, la giovane Seconda Repubblica di Francia doveva fronteggiare sia i pericoli provenienti dalle forze conservatrici monarchiche, sia i partiti più radicalmente rivoluzionari come quelli di Blanqui. Un compito davvero improbo, per una commissione dei repubblicani moderati appena saliti al potere: ed è facile figurarsi i componenti di quella commissione come posati intellettuali borghesi abituati più ad una vita tra libri e scartoffie che tra barricate e cannonate. Ma erano quelli tempi davvero tempestosi, tempi che necessariamente forgiavano uomini eccezionali: se la vita di Blanqui sembra uscita da un romanzo, quella del Presidente della Commissione Esecutiva non era da meno. Colui che a quel tempo poteva, con maggior diritto di chiunque altro, chiamarsi "Presidente della Repubblica" era un uomo che da bambino aveva tentato di uccidere un soldato spagnolo con una lancia. Uno che a diciotto anni confessava agli amici di star progettando un attentato contro Napoleone. Uno che era riuscito ad irritare così tanto un arcivescovo al punto tale che il sant'uomo finì col rifilargli un pugno in faccia. Uno che, appena diciannovenne, fu fatto prigioniero di guerra, nonostante non fosse in territorio nemico né come soldato né come spia. Uno che riuscì a convincere il comandante della sua prigione a farlo fuggire, e nella fuga arrivò fino ad Algeri, e qui ricatturato. Uno che fugge ancora, su una barca che è un guscio di noce, e finisce in una tempesta che lo riporta sulle rive algerine per essere di nuovo catturato da tribù di beduini; e qui liberato sotto la promessa di conversione all'Islam, ma comunque ancora imprigionato, poco dopo, da uno scettico bey di Algeri, che lo condanna ai lavori forzati in una colonia penale, che evita per miracolo grazie a manovre diplomatiche dell'ambasciatore di Francia. Uno insomma che nel 1848 ha ormai quasi sessant'anni, ma un'intensa vita alle spalle e un cumulo d'avventure da raccontare ai nipotini. Un curriculum che è certo quello di un fragile intellettuale travolto dalle tempeste politiche. E tutta la sua statura politica, tutte le sue esperienze di guerra, se le era costruite quasi per sbaglio, nei ritagli di tempo; perché il Presidente della Seconda Repubblica francese ha ben altro da fare: lui è, prima di tutto, uno scienziato.



5 *François Arago*

Dominique François Jean Arago nasce a Estagel, nei Pirenei orientali, il 26 febbraio 1786. Già il luogo e la sua data di nascita dice molto: per quanto venuto al mondo in un famiglia ragionevolmente benestante che gli consentirebbe un'infanzia e una giovinezza relativamente tranquilla, François ha appena tre anni quando scoppia la Rivoluzione Francese, e la Francia rivoluzionaria si trova ben presto in mezzo alle guerre che le monarchie di mezza Europa le dichiarano contro. La Spagna è tra le prime nazioni che si muove contro i rivoluzionari, e i francesi dei Pirenei si ritrovano subito in prima linea.

Il 17 settembre 1793 ci fu lo scontro di Peyrestortes, in cui le truppe catalane ebbero la peggio contro le armate francesi. François Arago, che i genitori dovevano abitualmente trattenere a forza in casa per evitare che si aggregasse ai soldati che andavano al fronte, si imbatte in cinque soldati spagnoli che stanno cercando di rientrare in suolo spagnolo. Si intrufola in fretta nel magazzino dove si trovano le armi che gli abitanti del paese

usano per la guerriglia, afferra una lancia e corre a tirarla contro il capopattuglia. Non gli fa davvero gran danno, ma lo spagnolo sguaina la sciabola e si prepara a rendergli pan per focaccia; si salva solo grazie all'accorrere di abitanti del paese armati di zappe e forconi, che mettono definitivamente in fuga i cinque spagnoli. L'intrepido guerrigliero ha sette anni e mezzo.

6 *La guerra franco-spagnola, vista dal Goya*

Il conflitto con la Spagna, in un modo o nell'altro, segna tutta la prima parte della vita di Arago: è mentre passeggia sui bastioni della sua città che incontra un ufficiale del genio che sta studiando come intervenire per eseguire le riparazioni necessarie alle mura. Affascinato, scopre che per poter fare quel lavoro deve andare al Politecnico, e che per entrare in quella scuola occorre superare dei difficili esami di matematica. Da quel giorno, il giovane François dedica gran parte del suo tempo a studiare le opere dei maggiori matematici e fisici del suo tempo.

E infatti riesce ad entrare al Politecnico, dopo un severo esame che sostiene di fronte a Monge[5], che peraltro in quell'occasione era particolarmente irritato, perché il compagno di Arago, che aveva sostenuto l'esame appena prima di lui, si era guadagnato una disonorevole bocciatura.

Gli anni di studio al Politecnico sono anche anni di tormento politico: Napoleone è salito al potere, la patria è perennemente in guerra, e ciò nonostante i fermenti scientifici accesi dai sogni del 1789 sono ancora in corso. Nel 1806 Arago non ha ancora vent'anni, ma Delambre e Méchain hanno già iniziato l'avventura della misura del Meridiano[6], che dovrà infine concludersi con la nascita della nuova unità di misura universale per le lunghezze, il metro. Mentre Delambre prende le misure a nord di Parigi, fino a Dunkerque, Mechain è incaricato di scendere a sud, fino a Barcellona. Il compito della sezione meridionale viene successivamente esteso, con la richiesta di giungere fino a Formentera, nelle Baleari. Mechain non riuscirà a completare il lavoro, perché muore di febbre gialla nel 1804: a sostituirlo, il *Bureau des Longitudes,* nelle persone di due mostri

[5] Gaspard Monge, matematico francese, inventore della geometria descrittiva. Tanto per capirci, un signore che ci vergogniamo di non aver ancora celebrato con un compleanno…

[6] Sulla storia della misura del Meridiano si potrebbero scrivere interi romanzi, e infatti se ne trovano diversi in libreria. Denis Guedj, diventato famoso con "Il teorema del pappagallo", ce ne ha scritti sopra ben due, "La misura del Mondo" e "Il Meridiano", nel nostro piccolo noi abbiamo scritto un compleanno, in RM075.

sacri come Laplace e Poisson, chiamano il trentenne Jean-Baptiste Biot[7], e uno dei più promettenti studenti del Politecnico, che era già buon amico di Poisson: Arago, appunto. François inizialmente tentenna (il suo sogno è quello di comandare le artiglierie francesi, non quello di fare triangolazioni da un campanile all'altro), ma alla fine accetta, e si ritrova in breve a far misurazioni in condizioni e luoghi così insoliti e pericolosi che, con ogni probabilità, gli rendono la vita assai più avventurosa di quanto lo sarebbe stata quella dell'artigliere: è infatti svettando da un'altura all'altra armati di stranissimi marchingegni che entrambi finiscono per insospettire la popolazione e l'esercito spagnolo, e finiscono in carcere, e poi a fare il giro del Mediterraneo in catene, come accennato[8].

Ritornato finalmente a Parigi, Arago viene giustamente accolto come un eroe: diventa subito professore del Politecnico ed eletto membro dell'Accademia delle Scienze. Soprattutto, comincia a lavorare all'Osservatorio di Parigi, che resterà il suo luogo di lavoro per il resto della vita (a parte le sinecure politiche).

I suoi risultati scientifici sono davvero molti, e variati: fu il primo ad ipotizzare che la velocità della luce dovrebbe subire delle variazioni dovute alla rotazione terrestre, e progettò degli esperimenti per determinare tale variazione: rimase molto interdetto, e verosimilmente assai deluso, nel constatare di non riuscire a trovare alcuna differenza nella velocità della luce. Saranno Michelson e Morley, diversi decenni più tardi, a mostrare con rigorosa precisione che la luce continua invariata la sua corsa, dando così il "la" alla Teoria Speciale della Relatività.

L'ottica restò sempre il suo campo di indagine preferito: in parte a causa della sua professione, visto che alla fin fine era diventato il Direttore dell'Osservatorio Astronomico di Parigi; in parte per la stretta collaborazione che iniziò con Augustine Fresnel, probabilmente il maggiore teorico di ottica del suo tempo. Insieme a questi elaborò teorie e produsse esperimenti sulla polarizzazione della luce e sui principi della rifrazione. Pochi anni dopo, Fizeau e Foucault confermarono le sue ipotesi con degli esperimenti passati alla storia.

Come professore al Politecnico, doveva anche indirizzare gli studi dei suoi studenti. Fu lui ad incaricare ad un brillante giovanotto di nome Le Verrier di indagare sulle perturbazioni del moto di Urano. Il compitino dello studente si risolse nella scoperta di Nettuno. A dimostrazione della sua onestà intellettuale, non solo non tentò di appropriarsi della scoperta del suo discepolo, ma entrò ferocemente in disputa con Adams per difendere la priorità della scoperta del suo pupillo, e combatté una battaglia – che finì per perdere – al fine di far chiamare "Le Verrier" il nuovo pianeta appena scoperto.

Quando Carlo Luigi Napoleone Bonaparte, ormai impaziente, decide di diventare Napoleone III è il 2 dicembre 1852. Assume la carica di imperatore esattamente un anno dopo aver portato a termine il colpo di stato che ha del tutto esautorato la Seconda Repubblica, il 2 dicembre1851. Anche in questo rincorrersi delle date, il novello imperatore cerca di imitare lo zio, che si era incoronato Imperatore dei Francesi il 2 dicembre 1804. Da quel momento in avanti, tutto in Francia diventa "imperiale": le grandi "N" circondate da allori che ancora si vedono a Parigi fioriscono in questo periodo, non certo durante il Primo Impero. Persino l'Osservatorio Astronomico diventa "Imperiale Osservatorio"; persino l'Accademia delle Scienze diventa "Imperiale Accademia della Scienze". E naturalmente, tutti coloro che hanno qualcosa a che fare con l'osservatorio o con l'accademia sono chiamati a giurare fedeltà all'imperatore.

Arago dovrebbe giurare per ben due volte, come Segretario dell'Accademia e come Direttore dell'Osservatorio. Ma François Arago, vecchio e indomito repubblicano,

[7] Nome che si incontra nei libri di scuola inevitabilmente legato a quello di Felix Savart, nelle prime pagine dei capitoli sull'elettromagnetismo, grazie alle legge che prende il nome di entrambi.

[8] Così avventurosa che non si può far molto più che accennarla, come abbiamo già fatto poco sopra. C'è di buona che l'autobiografia del giovane Arago è reperibile integralmente in rete (in inglese) a questo link (davvero lungo, siate pazienti), dove rimandiamo tutti coloro che sono ancora convinti che fare gli scienziati sia un mestiere noioso: http://books.google.it/books?id=78MUAAAAQAAJ&pg=PA1&dq=arago+biography&hl=en&sa=X&ei=-McUT6ubNcXLtgfG-tymAg&redir_esc=y#v=onepage&q=arago%20biography&f=false

presidente della Commissione esecutiva della Repubblica, non giura affatto. Il novello imperatore non avrà il suo nome da esporre tra i fedeli dell'impero.

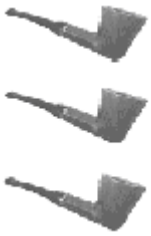
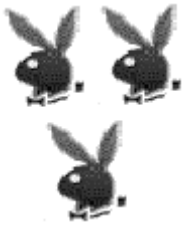
7 *Tour Eiffel – dettaglio della facciata del lato della Scuola Militare*

Eppure, il nome di Arago abbellirà la più orgogliosa creatura di Francia. Appena trentatré anni dopo la sua morte, che avvenne il 2 ottobre 1853, la Francia è nuovamente repubblicana, e comincia ad erigere il suo monumento più dirompente. Dopo tre anni di lavori, nel 1889, la torre Eiffel sovrasta tutta Parigi. Con i suoi trecento metri d'altezza e la sua struttura leggera e ancora moderna ipnotizza lo sguardo del turista, ed è assai probabile che, la prima volta che la si osserva, non si faccia caso ai nomi che la circondano e la decorano. Giusto sotto la prima e più grande terrazza.

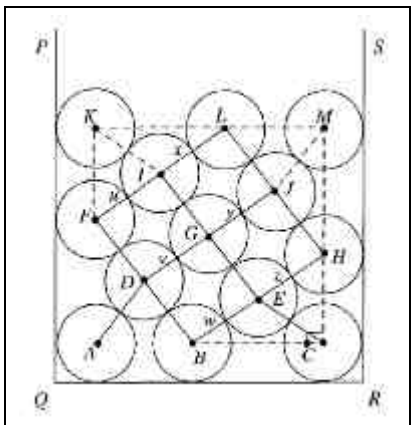
Sono settantadue nomi di scienziati che hanno onorato la Francia[9]. Diciotto per ogni facciata. Le facciate sono chiamate "Trocadero", "Grenelle", "Scuola Militare", e "La Bourdonnais", dai nomi delle parti della città verso cui le facciate sono esposte. Il sedicesimo nome sulla facciata della Scuola Militare è quello riservato ad Arago. Che placidamente segue Thenard (chimico) e precede Poisson e Monge (matematici); in quella compagnia, essere stato Presidente della Repubblica è un merito solamente accessorio, e certo non l'onore più grande.

[9] Tutti nati in Francia, o in territori che al tempo erano parte integrante dello stato francese, salvo uno. Uno che certo ha vissuto quasi sempre a Parigi, e ha reso grande la Francia, ma che francese non era. Si trova alla posizione numero sei della facciata Trocadero, ed è il protagonista del primo compleanno di RM, nel gennaio 2003. Non dovrebbe essere difficile indovinarne il nome…

2. Problemi

	Rudy d'Alembert	**Alice Riddle**	**Piotr R. Silverbrahms**
Ancora bottiglie!			
Si gioca con il robottino!			

2.1 Ancora bottiglie!



1 *Il problema dell'altra volta.*

Sembrate aver apprezzato il problema delle bottiglie nella scatola: siccome siete stati bravi, vi regaliamo il disegno della soluzione originale, dalla quale (oltre alla soluzione) si possono ricavare alcune interessanti caratteristiche della disposizione (a parte il fatto che siamo terribilmente disordinati, quando ci mettiamo d'impegno...).

Bene, adesso generalizziamo il concetto al periodo dopo le feste: la famiglia d'Alembert, come al solito, si è ritrovata ad organizzare una pletora di mangiate in casa con parenti e amici vari, il che *["...non vorrai mica portare in tavola una bottiglia* già aperta*???" Citazione Paulette d'Alembert]* ha fatto sì che si accumulasse un notevole numero di bottiglie *mezze piene* (siamo sempre stati ottimisti): il Vostro Umile Narratore, nel periodo postfestivo, ha quindi preso su di sé il gravoso incarico di svuotarle, ma nel mentre si è posto un problema che, nella vostra perversione, potreste anche giudicare interessante (nel senso della maledizione cinese, "*Che tu possa vivere in tempi interessanti*").

In questo caso, le bottiglie erano tutte diverse: per semplicità, assumeremo i loro raggi (di base, approssimandole a cilindri) siano pari a 1, 2, 3, ..., n: man mano che venivano consumate, venivano posate sul balcone (verandato, quindi nessun rischio per chi passava al di sotto) in modo tale da poggiare tutte sul pavimento piegate su un fianco (per capirci: come A, B e C nella figura, non come le altre: ma, come abbiamo detto, sono tutte di raggio diverso e intero 1, 2, ..., n).

Questa agile struttura, in equilibrio *indifferente* (lo sottolineiamo in quanto di recente abbiamo avuto, in merito, alcune polemiche) occupa un certo spazio e, data la limitata capacità del balcone, vorremmo che questo spazio sa *minimo*. Per Natale, Capodanno, Epifania ci siamo limitati a una dozzina di bottiglie, ma come sapete stiamo entrando in un periodo nel quale RM ha in programma svariati festeggiamenti (e gli altri due festaioli hanno capacità bibitorie pari a quelle di Rudy): quindi, poteste portarvi avanti con i lavori e, supponendo il Satrapo di casa d'Alembert non ci costringa con le cattive a sgomberare

prima il balcone, vedere come "va a finire" con venti bottiglie, o con cinquanta. Tutte appoggiate per terra e di raggio intero e diverso, chiaro. Altrimenti non è divertente.

Svelti, che abbiamo sete.

2.2 Si gioca con il robottino!

Nel senso che abbiamo ritirato fuori il gioco preferito di Virgilio: vi ricordate, vero, che tempo fa avevamo comprato uno di quegli aspirapolvere che fanno tutto da soli e vanno dritti sin quando non trovano un ostacolo? Ve ne avevamo già parlato, e vi avevamo detto che Virgilio aveva imparato a dargli zampate sui sensori per farlo girare come un matto: Rudy, intendendo unire l'utile al dilettevole, ha deciso di verificare sperimentalmente[10] un risultato che lo aveva sempre lasciato perplesso.

Il vostro ha piazzato alcuni dei suoi gloriosi puntatori laser su due lati perpendicolari della stanza, ponendo nella posizione opposta dei sensori ottici recuperati dal robivecchi: tutti i raggi laser erano perpendicolari al lato della sala dalla quale originavano e centravano il loro sensore.

A questo punto, appiccicata al suddetto robottino un'opportuna asticella in grado di interrompere (quando lo avesse incontrato) un fascio laser, nella stanza sono stati liberati Virgilio e l'aspirapolvere, mentre Rudy teneva accuratamente il conto.

A gatto esausto (e pile scariche: più la seconda che la prima), Rudy si è accorto che il robottino aveva percorso in totale una distanza pari a $2n$ (misurato in "lati di stanza unitaria").

E si è anche accorto che, tra i vari fasci, ne esisteva sempre almeno uno che aveva almeno un certo numero di attraversamenti. Che, volendo potreste calcolare.

In pratica, esiste un raggio che viene attraversato almeno un certo numero di volte… Non è il minimo (facile, trovare un raggio attraversato zero volte), non è il massimo (potete ottenere qualsiasi valore, con delle traiettorie ben studiate), ma uno con almeno quel valore deve esserci, per qualsiasi traiettoria.

Ragazzi, la stanza sembra uno specchio. Quei due sono una squadra.

3. Oldies & Goldies

Nel vano quanto eroico tentativo di mettere ordine negli Archivi di una Prestigiosa Rivista di Matematica Ricreativa, Alice si è imbattuta in alcuni problemi per cui *non abbiamo ricevuto alcuna soluzione*: quindi, senza alcun intento di riciclo di materiale noto (lo sarebbe se lo mettessimo nei *Problemi*), proviamo a riproporveli (anche per vedere se andate oltre le prime pagine della rivista…).

Per questo, che ci serviva a fare bieca pubblicità ad uno spreco di preziose risorse cartacee, potreste anche essere giustificati: in tutti questi anni, Rudy non ha ancora trovato la soluzione (non che si sia sforzato molto a pensarla, ma *a volte ritorna*).

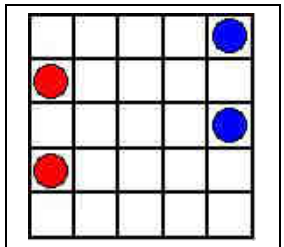
3.1 [RM157, Febbraio 2012] – Tre per due

...nel senso che a noi non costa niente, neanche leggere la soluzione che *non abbiamo*. Qualcuno probabilmente lo conosce, ma non ci risultano pubblicate analisi (e noi non l'abbiamo fatta, quindi ve lo diamo gratis).

La premessa è che saremmo felici se riusciste a dimostrare l'equivalenza con qualche gioco analizzato, ma anche se fate tutto da zero, per divertirvi, va bene lo stesso: ve lo descriviamo in modo stringato, che questa rubrica sta già usando troppe pagine ("Metà di una" sono già troppe, secondo Rudy).

[10] Sappiamo benissimo, come diceva Rabelais, che *enumeratio non fecit scientia*, e avevamo la dimostrazione teorica. Semplicemente, le cose ci diverte vederle anche "sul campo".

Materiale: Una scacchiera (quadrata), 2 gettoni blu grandi, 2 blu piccoli, 2 gettoni rossi grandi, 2 rossi piccoli.

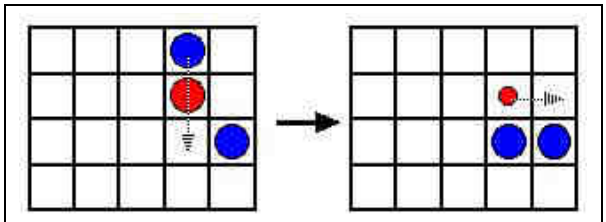

2 *Partenza della gara.*

Inizio: Decidere la dimensione della scacchiera e la sistemazione delle pedine grandi. Ad esempio, con la posizione in figura, decidete che muove per primo il blu, verso sinistra, poi il rosso, verso destra.

Mosse: a scelta, una tra queste:

- Spostare una pedina di almeno uno spazio nella direzione consentita.
- Saltare una pedina avversaria atterrando nella casella libera immediatamente oltre; una pedina saltata non può più saltare altre pedine, e questo si indica sostituendo la pedina grande con una piccola.

Trovate un esempio di salto nella figura a fianco: prima la mossa del blu, poi quella del rosso. Quando una pedina esce dalla scacchiera (come la rossa piccola alla prossima mossa dell'ultimo diagramma, ad esempio) non rientra e non può più muovere.


3 *Saltare!*

Scopo del gioco: Vincere, mi pare chiaro. Perde chi non ha mosse valide, quindi le pedine devono restare in campo più tempo possibile.

Un "grazie" (per aver comprato il libro) a quelli che lo conoscono. E adesso datevi da fare, che ci serve la soluzione per la seconda edizione.

4. Bungee Jumpers

Un multiplo di 17 viene espresso in base 2, e contiene esattamente tre 1.

Provate che deve contenere almeno sei 0 e che, se contenesse esattamente sette 0, uno di questi sarebbe la cifra meno significativa.

La soluzione, a "Pagina 46"

5. Soluzioni e Note

Febbraio!

Mese tradizionalmente breve, per molti motivi importante nella vita di RM, perché contiene San Valentino e il compleanno della Prestigiosa Rivista di Matematica Ricreativa, in ordine qualsiasi. Per festeggiare, cerchiamo sempre di organizzare qualcosa, e anche quest'anno siamo candidati per il Carnevale della Matematica sul nostro ormai ancora più Prestigioso Blog.

Quest'anno cominciamo con l'organizzare di uscire con RM, poi vediamo.

5.1 [190]

5.1.1 Questa è dura

Durissimo problema che si può riassumere così:

> *Doc sta studiando una decorazione del campo di tiro (*20x20*, bordi inclusi): fermo restando che il fondo resta a prato inglese, intende mettere un certo numero* $k = \{6, 5, 8, 7\}$ *di alberelli, e poi considerare tutti i triangoli costruibili con vertici in questi punti; di questi, sceglierà quello con l'area minore, e l'intero triangolo scelto verrà piantumato ad erica. Il vostro scopo è quello di posizionare i punti (nel numero dato) in modo tale che il triangolo minore abbia l'area massima possibile. In funzione del numero* k *di punti, quante piantine di erica, ciascuna coprente area unitaria, deve comprare Doc?*

Il mese scorso abbiamo pubblicato la soluzione di ***Lorenz***, ***Sawdust*** e ***Gnugnu***, e proprio quella di quest'ultimo ha ispirato il nostro ***trentatre***:

> Ho seguito la soluzione di ***Gnugnu*** al problema 190 2.1 *Questa è dura*, pubblicata in RM192. Parto dai suoi risultati per aggiungere qualche contributo. In fig. 1 riporto (salvo orientamento e nome dei punti) le soluzioni *buone* di ***Gnugnu***.

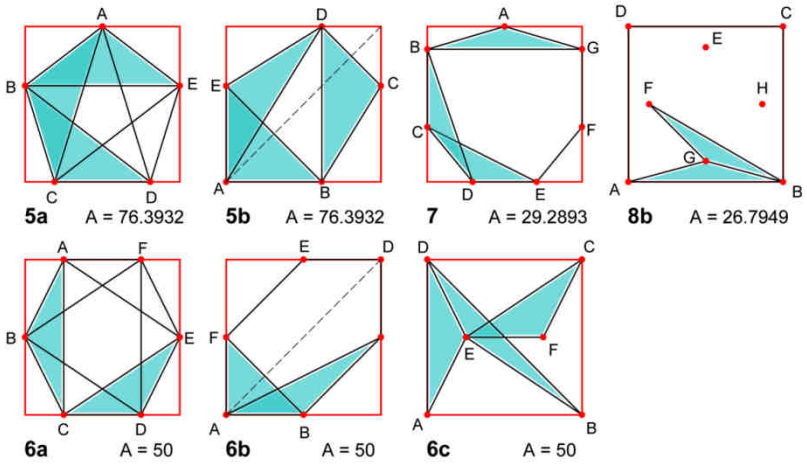


fig. 1

Abbrevio con Q il quadrato, T il triangolo minimo e A la sua area; k è il numero di punti. Rimando alla fine i calcoli espliciti e qualche nota.

Nelle soluzioni i punti sono disposti su un poligono senza punti interni, salvo **6c** e **8b**, che ne hanno rispettivamente 2 e 4. Mi occupo soltanto del primo caso, che è il più semplice; in presenza di punti interni è difficile individuare schemi generali.

Le **5a**, **5b**, **6a**, **6b**, **7** si ottengono da un poligono regolare inscritto in Q con opportune deformazioni. Questo si può fare in due modi.

<u>modo I</u>. Il poligono regolare è posto con un lato sulla base e di dimensione tale da toccare i lati sinistro e destro di Q, applicando poi una dilatazione verticale che porta i vertici superiori sul lato alto.

Per (5) e (6) si ottengono esattamente le **5a**, **6a**.

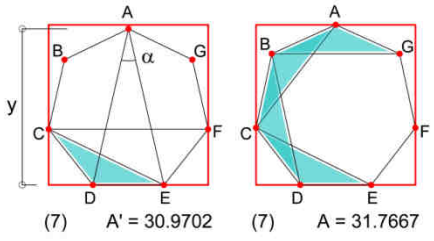


fig. 2

Per (7) si ha la soluzione di fig. 2, che migliora la **7**. A sinistra la dimostrazione; nell'ettagono <u>regolare</u> i sette triangoli simili a CDE sono tutti uguali, minori di ogni altro e di area $A'=400(1-\cos\alpha)\sin 2\alpha=30.9702$ con $\alpha=\pi/7$; il punto A non è su Q, ma poiché AD=CF=20 si ha y=20cos(α/2); con una dilatazione verticale dalla base di Q di modulo m=1/cos(α/2) il punto A finisce su Q e ci sono ancora 7 triangoli di forma lievemente diversa fra di loro ma di area comune $A=mA'=31.7667$.

Le posizioni dei punti derivano da quelle del poligono regolare (le y sono moltiplicate per m).

Per (8) si ottiene A'=24.2640; spostando i punti verso i vertici di Q, si arriva alla soluzione **8a** con A=25 (non disegnata e da scartare rispetto alla **8b**).

<u>modo II</u>. Il poligono è orientato con un vertice su una diagonale di Q, dimensionato in modo che almeno quattro punti tocchino il bordo. Si applicano poi due dilatazioni

assiali, lungo le diagonali di Q, per ottenere il massimo di A. Per (5), (6) si hanno esattamente le **5b**, **6b.**

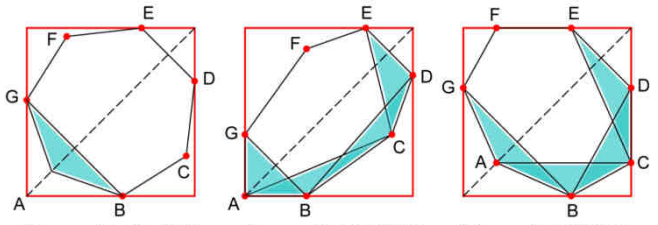


fig. 3

In fig. 3 i risultati per (7). Nel primo schema l'ettagono regolare con 4 punti su Q (anche questa è una soluzione); nel secondo T è vincolato a occupare un angolo di Q (è riportato solo per confronto con **5b**, **6b** e va scartato); nel terzo, applicate le dilatazioni, si ha la stessa A della soluzione I. L'equivalenza dei due modi vale per ogni k non multiplo di 4.

Sia I. che II. mantengono la proporzionalità delle aree e il parallelismo delle diagonali del poligono. Inoltre il numero di T è sempre uguale a k.

Tutti e due i modi si possono applicare ad ogni k e forniscono soluzioni utili, se non ottimali, salvo per i multipli di 4, che hanno tutte le simmetrie di Q (per questi casi conviene I.).

Per I. riporto alla fine le formule per l'area A per ogni k; non riporto invece quelle, più complicate, per II.

note

Ho cercato di capire quando una distribuzione dei punti P è una soluzione

a) non ci sono tre P allineati e almeno tre di essi, ma non più di otto, sono sul bordo di Q

* A è diversa da zero, e con solo due P su Q si può deformare la figura aumentando tutte le aree; su ogni lato possono stare solo due P

b) tutti i T sono connessi fra di loro

* esiste almeno un T ; un P non vertice di un T forma con i lati di questo triangoli maggiori di T, e si può spostare fino a formare un nuovo T, connesso al precedente

c) ognuno dei P è stabile, nel senso che un piccolo spostamento diminuisce l'area di un T

* se T diminuisce questo riduce l'area minima A, contro la assunzione che sia massima

d) ogni P è vertice di almeno un T, e di almeno tre se interno a Q

* per b) e c); un P interno che non sia vertice di almeno tre T non è stabile.

Esiste un'altra condizione e), che definisce una specie di "distanza " fra i punti. In fig. 4, ABC è un triangolo T e la figura è ottenuta tracciando righe parallele ai lati di T passanti per i vertici o contrapposte ad essi. All'interno della zona in colore (che si estende all'infinito), ad esclusione del contorno (in rosso) non possono esserci altri punti salvo A,B,C. Infatti ogni punto interno, p.es. nella fascia parallela ad AB, genera con AB un triangolo minore di T, il che è impossibile per T massimo. Gli eventuali P sul contorno (che ci sono certamente nelle soluzioni senza punti interni) producono altri triangoli T.

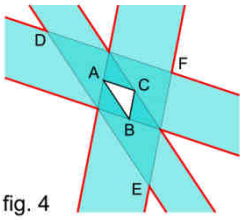


fig. 4

Le proprietà aiutano a riconoscere le soluzioni; p.es. la **7** di fig. 1 non è una soluzione: B e G non sono stabili e spostandoli si arriva alla (7) di fig. 2.

In mancanza di punti interni

- i k punti costituiscono un poligono convesso

- assumendo come limite un cerchio C anziché Q, la soluzione migliore - in realtà l'unica - è data dal poligono regolare, con i T formati da due lati adiacenti

- il passaggio da C a Q consente di aumentare A sfruttando lo spazio vicino ai vertici; ma questo non vale per (5), (6) e nemmeno per (7) (si dimostra a partire dalle coordinate dei punti "liberi" ed eguagliando l'area dei T)

- I. e II. danno gli stessi risultati, e le deformazioni diminuiscono al crescere di k.

Avanzo un congettura: senza punti interni e salvo per i multipli di 4, il valore dato da I. è il massimo possibile per ogni k.

- modo I. formule

- in un poligono regolare di k vertici e lato s, con $\alpha = \pi/k$, le lunghezze e le aree si possono esprimere tutte con questi soli parametri; il raggio circoscritto è $s/(2\sin\alpha)$; le diagonali poste in ordine di grandezza $d_1 \equiv s, d_2\ d_3, \ldots$ sono in rapporto $d_p / d_q = \sin p\alpha / \sin q\alpha$; l'area del triangolo composto da tre diagonali è $d_p\, d_q\, d_r \sin\alpha / (2s)$; l'area del poligono è $k\, s^2 / (4\tan\alpha)$

- da questo si ricavano i valori di A nel modo I.

$k = 4n, \qquad A = \tan\alpha \sin^2\alpha$

$k = 4n-2, \quad A = \sin^3\alpha$

$k : \text{dispari}, \quad A = 8\sin^3(\alpha/2)\cos\alpha$

- in particolare per k=5, 6, 7, 8 si hanno i valori già trovati

$k = 5,\ A = (3-\sqrt{5})/4$

$k = 6,\ A = 1/8 = 0.12500$

$k = 7,\ A = 0.07942$

$k = 8,\ A = 3\sqrt{2}/4 - 1 = 0.06066$.

NB. le formule valgono per un quadrato unitario; A va moltiplicato per 400.

Complimenti all'ispiratore e all'ispirato. Andiamo avanti.

5.2 [192]

Visto il ritardo con cui siamo usciti, è un miracolo aver ricevuto soluzioni, ma con i nostri lettori più affezionati non si scherza, e quelle che vedete più sotto ci sono ancora giunte nell'anno vecchio.

5.2.1 Un casino di Nim

Ecco un buon problema teorico multidimensionale, descritto dal Capo usando tutti i tempi verbali a disposizione. Vediamo se riesco a semplificare:

Un croupier (normale, umano e onesto) tira un dado, che indica un punteggio d. Poi si sposta alla tavola della roulette (normale, rotonda e onesta) per ottenere un certo valore r: a questo punto, metterà un gettone sul valore r del tappeto: e qui inizia la partita. Doc e Rudy, in quest'ordine, sono liberi di:

1. *Lasciare la posizione del dado invariata*
2. *Incrementare il valore del dado di* 1
3. *Decrementare il valore del dado di* 1

Se il dado segna 1*, possono solo lasciarlo invariato o incrementarlo, mentre se segna* 6 *possono solo lasciarlo invariato o decrementarlo (insomma, il dado non è ciclico); una volta compiuta questa operazione, il dado segnerà il valore x e, essendo al momento il gettone nella posizione k, verrà spostato alla posizione k – x : nel caso sia k < x, allora il giocatore che non può fare la mossa ha perso.*

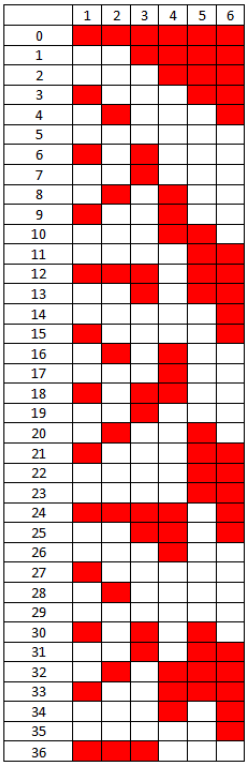
Esistono dei valori di r per cui Rudy è sicuro di vincere, qualsiasi sia il valore d del dado?

Per quali valori d del dado Doc ha almeno una probabilità su due di vincere?

Prima che cominci la partita, quali sono le probabilità di vittoria di Rudy?

Ah, purtroppo non il mio tipo preferito di problema, perdonatemi la brevità, vediamo subito la soluzione in due parti del nostro ***Alberto R.***:

Qualcuno (Wittgenstein?) ha detto che la filosofia è la lotta dell'uomo contro le ambiguità del linguaggio. Se è così i lettori di RM sono tutti filosofi. Anche questa volta il testo del problema è ambiguo. Mi spiego con un esempio. Supponiamo che il dado abbia dato 4 e Doc, avvalendosi della facoltà di incremento, sposta il gettone di 5 posizioni. Adesso tocca a Rudy. Può egli incrementare/decrementare l'originario 4 muovendo di 3, 4 o 5 passi, oppure deve fare riferimento al 5, nuova posizione del dado stabilita da Doc, muovendo di 4, 5 o 6 passi?



Naturalmente ho scelto la prima interpretazione che semplifica molto il problema.

Ciò premesso veniamo alla soluzione.

A seconda del numero *d* indicato dal dado, chiamiamo **rosse** (per tutti i valori leciti di n) le seguenti posizioni del gettone sul tappeto:

d = 1	3n
d = 2	4n
d = 3	6n 6n+1
d = 4	8n 8n+1 8n+2
d = 5	10n 10n+1 10n+2 10n+3
d = 6	11n 11n+1 11n+2 11n+3 11n+4

e **bianche** tutte le altre posizioni. Visivamente la situazione è la seguente.

La strategia vincente consiste nel muovere il gettone portandolo su una casella rossa. Se ciò non è possibile la partita è inevitabilmente persa (a meno, ovviamente, di sciocchi errori dell'avversario).

È facile, infatti, verificare che valgono le seguenti regole:

1. chi riceve il gettone su una casella bianca può sempre portarlo su una casella rossa
2. chi riceve il gettone su una casella rossa non può muoverlo su un'altra casella rossa, ma deve necessariamente portarlo su una casella bianca

3. un giocatore perde (perché non può più muovere) se e solo se il suo avversario nella sua ultima mossa ha posizionato il gettone su una casella rossa.
4. conseguenza immediata delle tre regole precedenti è che chi muove per primo ha una strategia vincente se il gioco comincia con il gettone su una casella bianca e chi muove per secondo se il gioco comincia con il gettone su una casella rossa.

Un esempio:

Il dado ha dato 3 e la rullette ha dato 15.

Poiché 15 non è di tipo $6n$ né di tipo $6n+1$, la casella 15 è bianca, quindi, in forza della regola 1, deve essere possibile portare il gettone sul rosso. Infatti Doc, che gioca per primo, fa avanzare il gettone di 3 posizioni portandolo sul 12 rosso. Per la regola 2 Rudy non può portare il gettone sul rosso, infatti a seconda che lo sposti di 2, 3, o 4 passi, lo porterà sulle caselle 10, 9, 8 che sono tutte bianche. Di lì Doc, muovendo rispettivamente di 4, 3, 2 passi, arriverà alla casella 6 rossa, da dove Rudy può andare solo su 4, su 3, o su 2 (bianchi), e qui si accorge di aver perso perché Doc può spostare il gettone sullo zero (che non per caso è rosso!).

E veniamo alle domande.

Esistono dei valori di r (quelli della roulette) per cui Rudy, che gioca per secondo, è sicuro di vincere, qualsiasi sia il valore d del dado? No, eccetto banalmente lo zero, ma in tal caso la partita finisce prima di cominciare. Infatti nessun'altra riga della tabella è interamente rossa. I numeri più fortunati per Rudy sono il 12 e il 24 con probabilità di vittoria di 5/6.

Per quali valori d del dado Doc, che gioca per primo, ha almeno una probabilità su due di vincere? Per tutti escluso $d = 6$. Basta contare il numero di bianchi su ciascuna colonna. Per $d = 1, 2, 3, 4, 5, 6$ le probabilità di vittoria di Doc sono rispettivamente 24/37, 27/37, 24/37, 22/17, 21/37, 17/37.

Complessivamente Doc è avvantaggiato: probabilità di vincita 60,8%.

Questo ci stupisce assai: un problema proposto dal Capo che non è a lui favorevole? Vediamo la seconda parte della soluzione di ***Alberto***:

Giorni fa ho proposto una soluzione del problema nell'ipotesi che ad ogni mossa il giocatore potesse incrementare/decrementare di una unità o lasciare inalterato l'originario valore del dado. Do ora la soluzione secondo l'altra interpretazione del testo e cioè che ad ogni mossa si faccia riferimento al valore del dado così come eventualmente modificato dalla precedente mossa dell'avversario.

	1	2	3	4	5	6
0	0	0	0	0	0	0
1			0	0	0	0
2				0	0	0
3	0				0	0
4						0
5	0	0				
6						
7						
8	0	0	0			
9			0	0		
10				0		
11	0				0	0
12					0	0
13	0	0				0
14						0
15				0	0	0
16	0	0	0			
17			0			
18				0		
19	0					
20						
21	0	0	0	0		
22						0
23				0	0	0
24	0				0	0
25						0
26	0	0	0	0	0	0
27						0
28						
29	0					
30						
31	0	0	0			
32			0	0		
33				0		
34	0				0	0
35					0	0
36	0	0				0

La tabella diventa la seguente, ma, per il resto, non cambia nulla. La strategia vincente consiste ancora nel muovere per giungere a una casella rossa. Infatti continuano a valere le tre regole:

1. chi riceve il gettone e il dado nella situazione individuata da una casella bianca può sempre portare il gioco su una casella rossa (qui indicata con un cerchietto rosso)
2. chi riceve il gettone e il dado nella situazione individuata da una casella rossa non può pervenire a un'altra casella rossa, ma deve necessariamente portare il gioco su una casella bianca
3. un giocatore perde (perché non può più

muovere) se e solo se il suo avversario nella sua ultima mossa ha raggiunto una casella rossa.

Conseguenza immediata delle tre regole precedenti è che chi muove per primo ha una strategia vincente se il gioco comincia su una casella bianca e chi muove per secondo se il gioco comincia su una casella rossa.

Cambiano, è ovvio, le risposte alle due domande.

- Esistono dei valori di r (quelli della roulette) per cui Rudy, che gioca per secondo, è sicuro di vincere, qualsiasi sia il valore d del dado? Si: lo zero e il 26, uniche righe tutte rosse.
- Per quali valori d del dado (si deve intendere il valore di partenza) Doc, che gioca per primo, ha almeno una probabilità su due di vincere? Per tutti i valori di d escluso il 6. Basta contare il numero delle caselle bianche di ogni colonna e rapportarlo a 37.

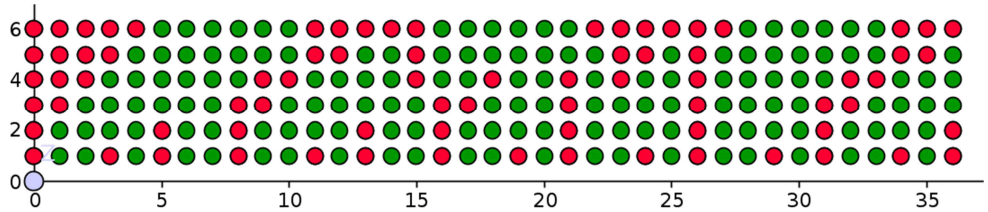
La tabella si può costruire in questo modo: La prima riga è – ovviamente – tutta rossa. Le caselle successive, dall'alto al basso, si colorano di rosso se e solo se non esiste alcuna mossa lecita che porti a un'altra casella rossa. Questa volta, però, mi sono fatto furbo e il lavoro di costruzione della tabella, lungo e noioso, l'ho lasciato al computer, e questo spiega perché le caselle "rosse" in effetti non sono colorate ma individuate da uno zero stampato in rosso!

Osservo infine che questa mia soluzione non ha nulla di intelligente, trattandosi sostanzialmente di una ricerca esaustiva, infatti la tabella non è altro che la descrizione compatta dell'albero di tutte le possibili evoluzioni del gioco.

Mah, l'ultima osservazione non ci pare completamente corretta, ma andiamo avanti, e facciamo un piccolo spazio a ***Gnugnu***, la cui tabella è orizzontale e più facile da sistemare in rivista – qualcuno che mi pensa…

Le possibili posizioni k del gettone segnaposto sono 37, i valori d del dado 6, si possono presentare quindi $37 \cdot 6 = 222$ stati diversi. Diciamo perdente uno stato che non consente alcuna mossa valida o permette solo mosse che portano ad uno stato vincente, viceversa uno stato sarà vincente se esiste almeno una mossa che porta in uno stato perdente.

GeoGebra, dopo aver inteso le regole del gioco, ha sfornato il disegno seguente, dove ogni punto del reticolo è colorato: in rosso, quando lo stato è perdente; altrimenti in verde. Conduce il gioco con notevole maestria!



Le risposte alle domande poste si possono leggere immediatamente sul disegno.

I valori r della roulette che garantiscono la vittoria a Rudy, indipendentemente dall'esito del dado, sono: 6, 7, 20, 28 e 30 (0 e 26 assegnano, viceversa, la vittoria a Doc) .

Il solo valore $d = 6$ del dado lascia a Doc almeno una possibilità su due di vincere, per l'esattezza 19 su 37 (per contro, il valore 2 ne lascia 9 su 37, meno di una su quattro).

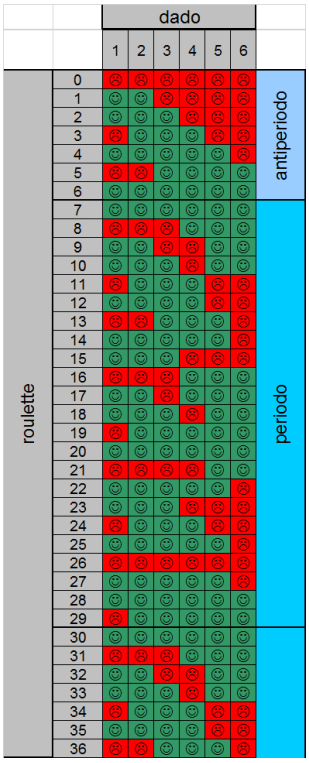
Prima che inizi la partita la probabilità di vittoria per Doc è 77/222, quella per Rudy 145/222.

Che il creativo autore di 'ti piace vincere facile?!' si sia ispirato a Rudy è più di un'ipotesi buttata lì, diciamola almeno una congettura, qualcuno però dovrebbe

spiegare perché il CG abbia voluto sottolineare, con tanto di *warning* in nota 14, che il problema fosse privo di un'analisi completa.

Osservando il disegno si nota che le colonne [30..36] sono identiche alle [7..13], ed allora, visto che i valori di una colonna possono dipendere solamente dalle sei precedenti (ad esser pignoli solo dalla *diagonale principale* di queste), l'ambaradan si ripete, con esclusione delle prime sette di assestamento, con periodo 23. Il tutto, spiace constatarlo, sempre a vantaggio del medesimo.

Eh, ecco, così ci sembra più normale, il Capo vince quasi sempre, è questo il suo modo di affrontare le probabilità. Ma aspettate, arriva ***Franco57***:



Dati i numeri r della roulette e d del dado, chiamo $S_{r,d}$ l'indicatore di vittoria sicura per Rudy (o in generale per il secondo giocatore) che vale 0 se perde, 1 se vince. Naturalmente si assume che Doc e Rudy, da bravi matematici ricreativi, giochino al meglio.

Banalmente vince solo colui che può muovere mettendo l'avversario in una situazione di perdita e il processo è ricorsivo. Cioè l'indicatore vale 0 se e solo se tra le situazioni raggiungibili ve ne è almeno una che vale 1, quindi posso calcolare:

$$S_{r,d} = \left(1 - S_{r-(d-1),d-1}\right) \cdot \left(1 - S_{r-d,d}\right) \cdot \left(1 - S_{r-(d+1),d+1}\right) \quad \text{per } r \geq 0 \text{ e } 1 \leq d \leq 6$$

$$S_{r,d} = 0 \text{ per } r < 0 \text{ opp } d < 1 \text{ opp } d > 6$$

dove per semplificare la formula ricorsiva di calcolo dell'indicatore ho esteso $S_{r,d} = 0$ fuori dai range ammissibili per rappresentare il caso che chi va in una situazione impossibile regala la partita all'avversario (equivalente a dire che perde chi non può muovere).

Bene adesso *calculemus!* o, molto più comodo, facciamo fare al foglio elettronico, che mi genera la figura dove ho messo la *facciacheride* o la *facciachepiange* di Doc (che è il primo giocatore).

Si nota che la mappa degli indicatori al crescere di r si comporta come la rappresentazione decimale di un numero razionale, con un antiperiodo e un periodo, cosa carina ma che non ci sorprende se pensiamo che un indicatore su r si basa al massimo sugli indicatori dei 6 precedenti valori di r.

Con il gioco completamente analizzato non è difficile rispondere alle domande finali:

1) a parte il caso banale che alla roulette esca lo 0, Rudy è sicuro di vincere indipendentemente dal dado anche se esce il 26;
2) le probabilità di vincere di Doc, riportate sotto, gli sono sfavorevoli solo se esce la faccia 6 del dado:

Dado					
1	2	3	4	5	6
22/37	28/37	27/37	25/37	25/37	18/37

3) A inizio partita le probabilità di vittoria di Rudy sono 77/222 quindi tra 34,68% e 34,69%.

Con lettori tanto bravi ci basta emettere frasi sibilline e poco comprensibili e loro partono e risolvono tre o quattro problemi diversi ispirati dalle nostre frasi bofonchiate. Siamo molto orgogliosi di noi stessi. ***Franco*** sembra d'accordo con ***Alberto***, ma in tema di probabilità io credo solo a quello che conosco e mi aspetto che il Capo abbia creato un problema in cui lui vince. Sarà una questione di interpretazione, ovvio.

Basta così, vediamo l'altro problema.

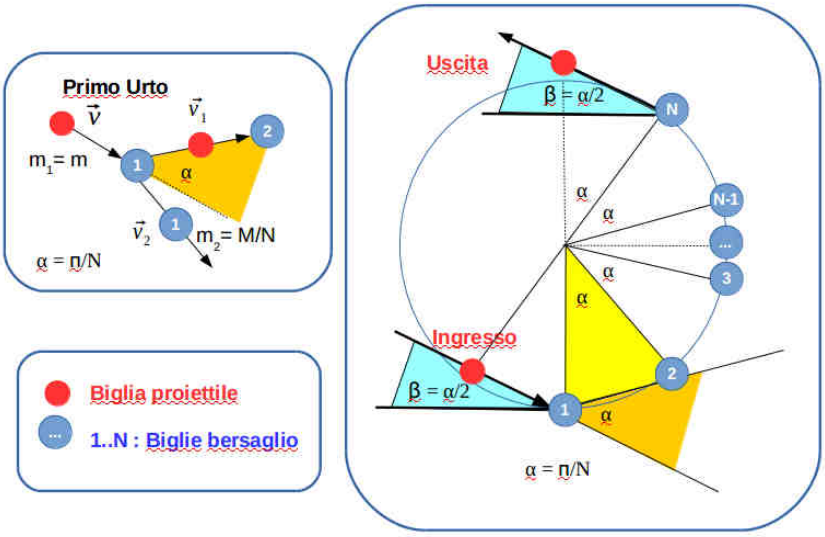
5.2.2 Biliardo Americano Quintessenziale

Senza fare troppi commenti iniziali vediamo prima di tutto di che cosa si trattava:

> *Dato un tavolo senza attrito e perfettamente in piano e N biglie identiche, ciascuna di massa M/N tra di loro equispaziate su una semicirconferenza con il lato "aperto" verso sinistra. A questo punto, prendiamo un'altra biglia di massa m e la lanciamo, da sinistra, con le ragionevoli condizioni iniziali per:*
>
> 1. *Urtare elasticamente la prima biglia e rimbalzare,*
> 2. *Urtare elasticamente la seconda biglia e rimbalzare,*
> 3. *...eccetera, eccetera, eccetera,*
> 4. *urtare elasticamente l'N-esima biglia, rimbalzare e uscire (dritta) sulla sinistra.*
>
> *A parte trovare le condizioni iniziali, supponiamo che N→∞, ossia che la massa di ogni pallina tenda a zero: qual è il minimo valore per M/N che permette alla palla lanciata di uscire dritta a sinistra? Per questo valore di M/N, qual è il rapporto tra la velocità iniziale e quella finale?*

Non è bellissimo? Un bel problema di fisica degli urti con principi di azione e reazione! Non poteva che ispirare il nostro ***Trekker***:

Con il significato dei termini come da figura



si può scrivere la seguente legge di conservazione della quantità di moto per l'urto fra la biglia proiettile e la prima biglia bersaglio, precisamente:

$$m_1\vec{v} = m_1\overrightarrow{v_1} + m_2\overrightarrow{v_2}$$

Da cui si può ricavare $\overrightarrow{v_2} = \frac{m_1}{m_2}(\vec{v} - \overrightarrow{v_1})$ e

$$v_2^2 = \overrightarrow{v_2}\cdot\overrightarrow{v_2} = \frac{m_1}{m_2}(\vec{v} - \overrightarrow{v_1})\cdot\frac{m_1}{m_2}(\vec{v} - \overrightarrow{v_1}) = \frac{m_1^2}{m_2^2}(v^2 - 2\vec{v}\cdot\overrightarrow{v_1} + v_1^2)$$

Il prodotto scalare fra i due vettori $\vec{v}$ e $\overrightarrow{v_1}$ si può esprimere come $\vec{v}\cdot\overrightarrow{v_1} = vv_1cos(\alpha)$, dove α è l'angolo fra i due vettori. Sostituendo si trova:

$$v_2^2 = \frac{m_1^2}{m_2^2}(v^2 - 2vv_1cos(\alpha) + v_1^2)$$

Trattandosi di urto elastico si conserva l'energia cinetica totale pertanto si può scrivere:

$$\frac{1}{2}m^2v^2 = \frac{1}{2}m_1^2v_1^2 + \frac{1}{2}m_2^2v_2^2$$

Sostituendo a v_2^2 quanto trovato prima ed elaborando un poco l'equazione della conservazione dell'energia cinetica si ottiene:

$$(m_1 + m_2)v_1^2 - 2m_1cos(\alpha)vv_1 + (m_1 - m_2)v^2 = 0$$

Posto $t = \frac{v_1}{v}$ riscriviamo l'equazione come:

$$(m_1 + m_2)t^2 - 2m_1cos(\alpha)t + (m_1 - m_2) = 0$$

La condizione affinché questa equazione di secondo grado abbia soluzioni reali è che il discriminante Δ sia ≥ 0, ovvero che $\frac{m_2}{m_1} \geq sin(\alpha)$.

Essendo $m_2 = \frac{M}{N}$ e $m_1 = m$ si ottiene perciò $\frac{M}{N} \geq m \cdot sin(\alpha)$

Affinché la biglia proiettile torni "indietro" dopo i corrispondenti N urti elastici con le biglie bersaglio "equispaziate" con un angolo α su una semicirconferenza bisogna che $\alpha = \frac{\pi}{N}$ ovvero:

$$\boldsymbol{\frac{M}{N} \geq m \cdot sin\left(\frac{\pi}{N}\right)}$$

Si noti che $M \geq m \cdot N \cdot sin\left(\frac{\pi}{N}\right)$ e che $lim_{N\to\infty}\, m \cdot N \cdot sin\left(\frac{\pi}{N}\right) = m \cdot \pi$

Se $m_2 = \frac{M}{N}$ assume il **valore minimo accettabile** $\boldsymbol{m \cdot sin\left(\frac{\pi}{N}\right)}$ affinchè la biglia proiettile torni "indietro" allora l'equazione di secondo grado in t ammette l'unica soluzione (corrispondente a Δ=0)

$$t = \frac{v_1}{v} = \frac{m_1 \cdot cos\left(\frac{\pi}{N}\right)}{m_1 + m_2} = \frac{m \cdot cos\left(\frac{\pi}{N}\right)}{m + m \cdot sin\left(\frac{\pi}{N}\right)} = \frac{cos\left(\frac{\pi}{N}\right)}{1 + sin\left(\frac{\pi}{N}\right)}$$

Dopo N urti elastici il rapporto $\frac{v_N}{v}$ fra la velocità di uscita e quello di ingresso della biglia proiettile vale:

$$\frac{v_N}{v} = t^N = \left(\frac{\boldsymbol{cos\left(\frac{\pi}{N}\right)}}{\boldsymbol{1+sin\left(\frac{\pi}{N}\right)}}\right)^{\boldsymbol{N}} \text{ e } lim_{N\to\infty}\frac{v_N}{v} = e^{-\pi} \approx 0.0432139.$$

Siamo arrivati al fondo. Alla prossima!

6. Quick & Dirty

A noi sono sempre piaciute le soluzioni "alternative": qui, ne abbiamo trovata una che ha trasformato un problema delle Olimpiadi Matematiche in un "Q&D". La domanda a cui non sappiamo rispondere è: "Ma qual era, la soluzione ortodossa?" Nel senso di quella noiosa che occupa un paio di pagine, e non poche righe appassionanti…

Dimostrate che se da una scacchiera $2^n \times 2^n$ viene rimossa una casella qualsiasi, la parte restante della scacchiera è ricopribile da tri(o)mini[11] a forma di "L".

7. Pagina 46

Se la rappresentazione binaria di $17k$ contiene esattamente tre 1, allora deve essere:

$$\exists a > b > c \geq 0\colon 17k = 2^a + 2^b + 2^c.$$

ossia:

[11] Ci pare di ricordare che la traduzione italiana dei libri di Martin GARDNER li chiamasse "trimini", ma abbiamo trovato anche la dizione "triomini". Non essendo intenzionati a scatenare guerre di religione, mettiamo la "o" tra parentesi.

$$17k = 2^c (2^{a-c} + 2^{b-c} + 1)$$

e quindi, considerato che 17 è primo, 2^c divide k.

Se $k = 2^c m$, allora

$$17m = 2^{a-c} + 2^{b-c} + 1),$$

il che significa che m deve essere dispari.

Se $17k$ contiene nove o più cifre (o, equivalentemente, se $a \geq 8$), allora almeno tre devono essere 1: per verificare che questo è sempre vero, procediamo per assurdo, supponendo $a \leq 7$.

In questo caso, avremmo $a - c \leq 7$, e a maggior ragione, visto che $b < a$, $b - c \leq 6$. Quindi dovrebbe essere:

$$17m \leq 2^7 + 2^6 + 1 = 193 \Rightarrow m \leq 193/17 \Rightarrow m \leq 11.$$

Il che ammette per m i valori 1, 3, 5, 7, 9, 11, ma nessuno di questi è possibile: quindi $17k$ contiene almeno nove cifre.

L'equazione

$$17m - 1 = 2^{a-c} + 2^{b-c}$$

mostra che $17m - 1$ è la somma di due diversi numeri dalla lista (2, 4, 8, 16, 32, 64, 128): ma al variare di m, $17m - 1$ assume i valori 16, 50, 84, 118, 152, 186, e nessuno di questi è la somma di due valori della lista precedente.

Per quanto riguarda la seconda parte della domanda, se la nostra rappresentazione binaria contenesse sette 0, allora $17k$ sarebbe un numero di dieci cifre formato da sette 0 e tre 1, e quindi avremmo $a = 9$ e

$$17m = 2^{9-c} + 2^{b-c} + 1.$$

Se $c = 0$, allora:

$$17m = 2^9 + 2^b + 1, \text{ con } 0 = c < b \leq 8.$$

Al variare di b, $17m$ varia nell'insieme {515, 517, 521, 529, 545, 577, 641, 769}, ma nessuno di questi è divisibile per 17. Quindi $c > 0$, e il numero dato termina per 0.

8. Paraphernalia Mathematica

8.1 Go, Alice, Go! [001]

Sorry, Treccia, non stiamo parlando di te. E neanche di Lewis Carroll.

Tutto nasce da una certa insoddisfazione di Rudy nel campo della crittografia, per la quale sono state adottate soluzioni secondo lui piuttosto estremiste: o dite "troppo", con degli agili libretti di quasi mille pagine[12], come l'ultimo che si è procurato Rudy, o dite "troppo poco", come ha fatto John Gordon nella meravigliosa "*La vera storia di Alice e Bob*[13]":

> *Against all odds, over a noisy telephone line, tapped by the tax authorities and the secret police, Alice will happily attempt, with someone she doesn't trust, whom she cannot hear clearly, and who is probably someone else, to fiddle her tax returns and to organise a coup d'etat, while at the same time minimising the cost of the phone call.*
>
> *A coding theorist is someone who doesn't think Alice is crazy.*

Ottima spiegazione[14], ma ammetterete che basta sì e no per costruire un titolo ad effetto, come abbiamo giustappunto fatto: adesso, cerchiamo di analizzare qualche caso e capire *come* Alice può farcela.

Il primo problema con il quale si scontra qualunque sistema spionistico ha l'aria piuttosto banale: dovete, nella maggior parte dei casi, ***passare la chiave*** di cifratura. Supponiamo di aver trasformato la nostra chiave di lunghezza n in un numero (binario), e cominciamo a lavorarci sopra: consideriamo tutte le 2^n n-uple passibili di diventare una chiave.

Tutti questi oggetti sono rappresentabili come un *Campo di Galois*[15] $GF(2^n)$: ogni chiave $(a_1, a_2, \ldots, a_n)$ è rappresentabile come il polinomio di grado $n-1$:

$$\sum_{i=1}^{n} a_i x^{i-1} = a_1 + a_2 x + a_3 x^2 + \ldots a_n x^{n-1}$$

;

si noti che gli esponenti hanno un valore "di uno minore" rispetto ai pedici: inelegante, ma fa parte della definizione standard.

Per fare un esempio con valori trattabili (che evidenzia anche il fatto che "si conta al contrario": da sinistra verso destra), possiamo usare $GF(2^3)$, che ha elementi:

$100 = 0$ $\quad 100 = 1$ $\quad 010 = x$ $\quad 001 = x^2$

$110 = 1 + x$ $\quad 101 = 1 + x^2$ $\quad 011 = x + x^2$ $\quad 111 = 1 + x + x^2$.

Nei Campi di Galois, anche se l'addizione non è difficile (si procede "per componenti"), per la moltiplicazione possono nascere dei problemi: tanto per cominciare, va scelto un polinomio $f(x)$ *irriducibile* (ossia non scomponibile in prodotto di polinomi appartenenti allo stesso campo); a questo punto, il prodotto uv di due n-uple in $GF(2^n)$ viene definito come l'n-upla ottenuta dal prodotto delle due n-uple *modulo* il polinomio irriducibile: la cosa non è simpaticissima, vista l'aleatorietà della *scelta* del polinomio, ma funziona. Ad esempio, sempre restando nel nostro $GF(2^3)$, supponiamo di aver scelto il polinomio $f(x) = x^3 + x + 1$: se questo è il *modulo*, *sarà equivalente a zero*: quindi, uguagliandolo a zero, otteniamo $x^3 = -x - 1 = x + 1$ (in quanto $-1 \equiv +1 (\mathrm{mod}\, 2)$); quindi, effettuata la moltiplicazione dei polinomi "come al solito", sostituiamo ogni valore con $(x+1)$ e

[12] A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography. Ci si chiede che mani hanno, per tenere una cosa del genere.

[13] Ve ne avevamo già parlato, nei PM di RM129 e RM130, dal titolo suggestivo "Non ho capito…".

[14] Una traduzione più o meno a braccio potrebbe essere: "*Malgrado tutte le difficoltà, usando una linea telefonica rumorosa, controllata delle autorità fiscali e dalla polizia segreta, Alice tenterà allegramente di manipolare la sua dichiarazione d'imposta e di organizzare un colpo di stato con qualcuno di cui non si fida, che lei non può sentire in modo chiaro, e che probabilmente è qualcun altro, tentando allo stesso tempo di ridurre al minimo il costo della telefonata. Uno studioso di teoria dei codici è qualcuno che non pensa che Alice sia pazza.*"

[15] Ne abbiamo parlato... Oibò! Non l'abbiamo mai fatto? Male. Provvederemo appena possibile.

considerando che stiamo lavorando *modulo* 2 sui numeri (somma *per componenti!*), possiamo ridurre il prodotto a un qualcosa contenuto nel campo originale. Proviamo con un esempio?

$$\begin{aligned} 011\cdot 111 &= (x+x^2)(1+x+x^2) \\ &= x+2x^2+2x^3+x^4 \\ &= x+x\cdot x^3 \\ &= x+x\cdot(x+1) \\ &= x+x^2+x \\ &= x^2 \\ &= 001 \end{aligned}.$$

Visto, che è meno complicato di quanto sembra? L'importante è mettersi d'accordo sull'*irriducibile*.

Dato un campo $GF(r)$, con gli $r-1$ elementi diversi da zero possiamo costruire un *Gruppo Ciclico* rispetto ad un generatore g scelto (aridaje...) come base: ad esempio, nel nostro gruppo ciclico, se scegliamo come generatore $g = 010 = x$ (attenzione che in questo caso va bene, ma non è detto che negli altri casi funzioni ugualmente bene), otteniamo una nuova rappresentazione di $GF(2^3)$:

$$\begin{aligned} 000 &= 1 &&= x^0 \\ 010 &= x &&= x^1 \\ 001 &= x^2 &&= x^2 \\ 110 &= 1+x &&= x^3 \\ 101 &= 1+x^2 &&= x^6 \\ 011 &= x+x^2 &&= x^4 \\ 111 &= 1+x+x^2 &&= x^5 \\ & x^7 &&= 1 \\ & x^8 &&= x \\ & x^9 &&= x^2 \end{aligned}.$$

Ossia, se vogliamo metterla sul formale, *ogni elemento diverso da zero di ammette logaritmo discreto*, che poi non sarebbe altro che l'esponente.

Abbiamo fatto un esempio semplice, ma se prendete dei gruppi "un po' più complicati" (ad esempio $GF(2^{300})$), siete abbastanza sicuri che nessuno riuscirà a trovarne "al volo" i logaritmi: a questo punto, possiamo definire una procedura per passare un messaggio (o una chiave) senza essere ascoltati: il metodo ricorda un po' quello dello "spedire un regalo in un paese di ladri"; siccome il metodo è complicatino, inseriamo il possibile *crack* in nota: leggete tutto due volte, e non preoccupatevi se gli ultimi punti non sono chiari: li spacchetteremo dopo. L'ipotesi è che **A** debba mandare a **B** il messaggio M.

1. **A** genera un intero positivo casuale "grande" a e spedisce a **B** la 300-upla M^a.
2. **B** genera un intero positivo casuale "grande" b e rimanda ad **A** la 300-upla M^{ab}[16].
3. **A** rimuove il rumore che lui stesso ha generato dal messaggio calcolando $\sqrt[a]{M^{ab}}$, ossia elevando il messaggio alla potenza a^{-1}; in questo modo ottiene M^b, che reinvia a **B**.
4. B toglie la sua parte di rumore generato calcolando $\sqrt[b]{M^b}$, ottenendo M.

Avete notato che ciascuno di loro lavora con *cose che sa*? A lavora con a, B lavora con b.

Piccolo problema: quanto è facile, in un Campo di Galois, calcolare una radice a-esima o b-esima? Proviamo a pensarci un attimo, cominciando con un esempio facile.

[16] Se C che sta in ascolto fosse un drago con i logaritmi nei Campi di Galois, sapendo che $\log M^{ab} = b \log M^a$ riuscirebbe a spacchettare il messaggio M^a, come dicevamo, la cosa non è facile.

Supponiamo di voler estrarre la radice quinta di x^2 in $GF(2^3)$, ossia di cercare l'elemento x^k tale che $(x^k)^5 = x^2$: siccome dai calcoli precedenti sappiamo che $x^7 = 1$, allora il nostro problema si riduce al calcolo della congruenza: $5k \equiv 2 \pmod 7$, che si risolve facilmente come $k = 6$.

Tutto risolto, quindi? Mica tanto. Infatti, se provate con la radice cubica di g^8 in $GF(2^4)$, ottenete dei risultati piuttosto strani. Infatti, cerchiamo k per cui $(g^k)^3 = g^8$ e, noto che $g^{15} = 1$ in $GF(2^4)$, la congruenza risulta $3k \equiv 8 \pmod{15}$: che non ha soluzioni!

Generalizzando, la radice t-esima di g^s esiste in $GF(r)$ solo se esiste una soluzione k a $(g^k)^t = g^s$ che equivale, dato che $g^{r-1} = 1$, al cercare le soluzioni di

$$kt \equiv s \pmod{r-1},$$

che non ha soluzioni se s non condivide tutti i divisori comuni a t e $r-1$.

Per questo motivo, quando si usa questo sistema, la tendenza è di utilizzare $GF(2^n)$ tali per cui $2^n - 1$ sia un primo[17], che rende le estrazioni delle radici più semplici: l'alternativa sarebbe quella di eliminare tutti gli a e b che non sono primi rispetto a $2^n - 1$, non che questo sia un grosso guaio, visto che ci restano comunque $\Phi(2^n - 1)$ valori[18] con i quali giocare. Vediamo un esempio con numeri "facili"? Supponiamo A voglia inviare il messaggio $M = 011$ a B.

Passo 1: A sceglie un numero casuale $a = 13$ e calcola[19] $M^a = 011^{13} = 110$, che invia a B.

Passo 2: B, alla ricezione del messaggio, sceglie un numero casuale $b = 11$ e calcola $M^{ab} = 110^{11} = (x^3)^{11} = x^{33} = x^5 = 111$.

Passo 3: A calcola a^{-1} dall'espressione $13k \equiv 1 \pmod 7$ ottenendo $a^{-1} = 13^{-1} = 6$, ed è quindi in grado di determinare $M^b = (M^{ab})^{a^{-1}} = 111^6 = 001$, che viene inviato a B.

Passo 4: B calcola b^{-1} dall'espressione $11k \equiv 1 \pmod 7$, ricavando $b^{-1} = 11^{-1} = 6$ e quindi è in grado di calcolare $M = (M^b)^{b^{-1}} = 001^2 = 011$.

Fatto. B ha ottenuto il messaggio, pur non conoscendo la chiave di cifratura usata da A.

Ma cosa succede, se C ascolta lungo la strada?

Tutto quello che riesce a sentire è "110", "111", "001": non essendo in grado di calcolare al volo i logaritmi di queste triplette, non riuscirà mai[20] a scoprire il messaggio.

Insomma, Alice è riuscita in un secondo compito impossibile: mandare un messaggio senza chiave, e farlo capire all'altro lato senza farlo ascoltare in mezzo. Siamo in dubbio se sia più eroico questo o il primo, consistente nel fare uscire RM tutti i mesi.

Rudy d'Alembert
Alice Riddle
Piotr R. Silverbrahms

[17] Il che rende chiaro anche l'entusiasmo quando viene trovato un nuovo Primo di Mersenne.

[18] Φ è la *funzione toziente* di Eulero.

[19] …E siccome Alice è pigra, si calcolerà una tavola contenente M, M^2, M^4, …, perché $M^{13} = M\,M^4\,M^8$. Certo, scrittura binaria. Con cinque moltiplicazioni ve la cavate. Non solo, ma dallo "smontaggio" di $GF(2^3)$ che abbiamo fatto prima, $M = 011 = x^4 \Rightarrow M^{13} = (x^4)^{13} = x^{52} = x^3 = 110$, se ci ricordiamo che $x^7 = 1$.

[20] "mai" è, come sempre, parola grossa: $n = 128$ e $n = 512$ sono ormai alla portata di qualsiasi computerino: e qualcuno sta sollevando potenti dubbi sulla "sicurezza" di $n = 1024$. Capite quindi che più primi di Mersenne ci sono, più siamo contenti.