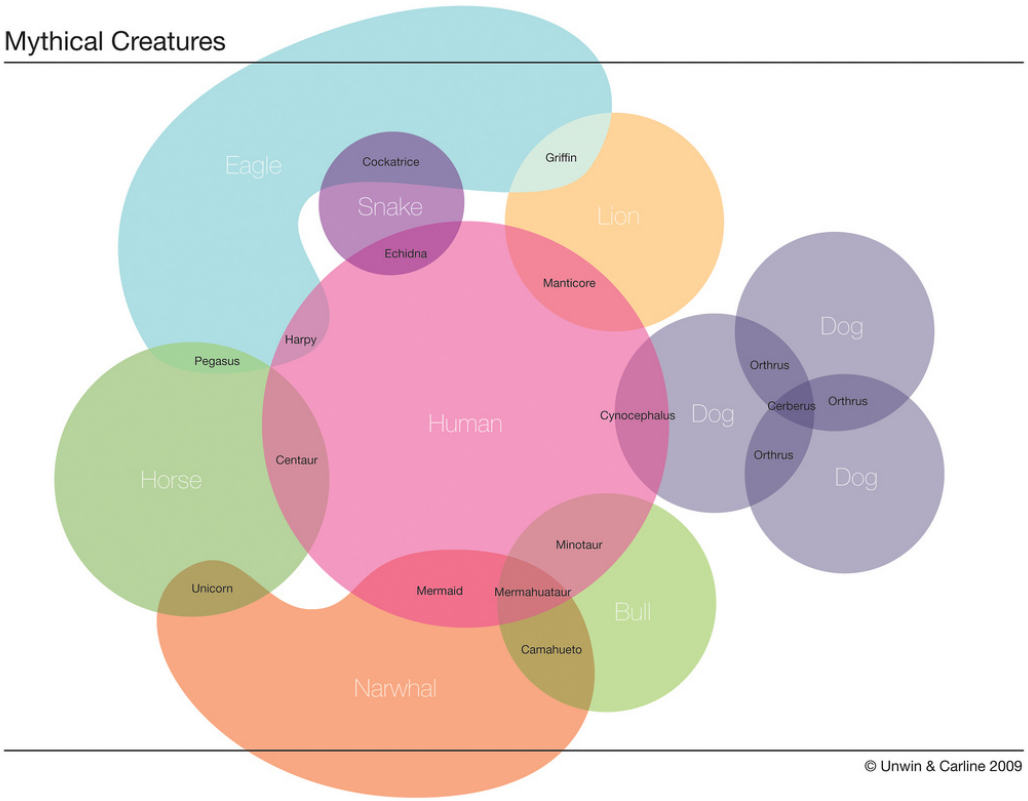
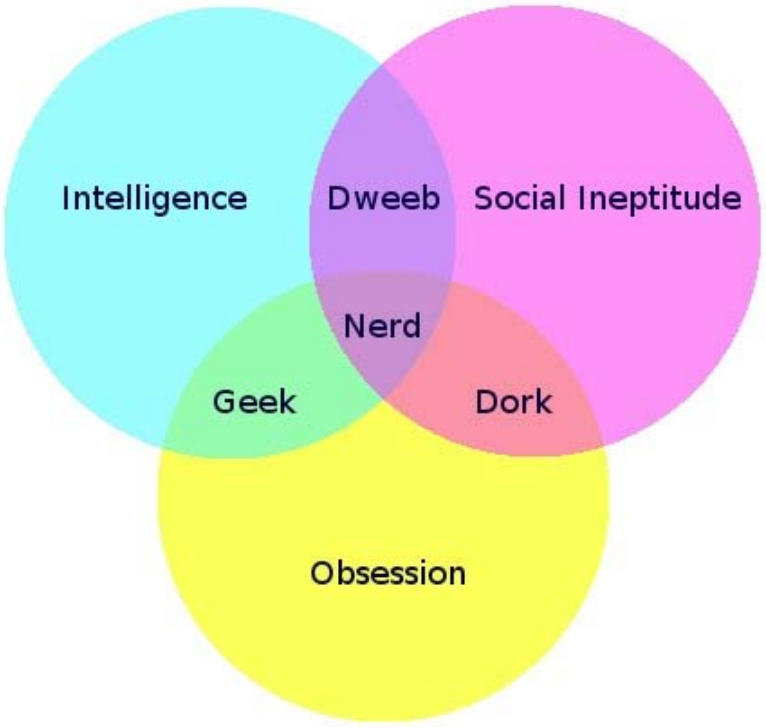
Rudi Mathematici

Rivista fondata nell'altro millennio

Numero 130 – Novembre 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

RM129 ha diffuso 2453 copie e il 03/11/2009 per Google eravamo in 9'380 pagine.

Abbiamo già detto che i diagrammi "di Venn" sono antipatici in quanto non sono di Venn, bensì di Eulero. Riteniamo però questi due piuttosto interessanti, anche se sul primo non siamo completamente convinti della posizione della Manticora (dovrebbe avere i denti da squalo, se ben ricordiamo) e, per quanto riguarda il secondo, vorremmo sapere dove siamo finiti.

1. Pari opportunità

Oh! squarciatemi il velo, e l'inumana
storia m'aprite di que' vili astuti;
date agli occhi di pianto una fontana!
La voce alzate, o secoli caduti!
Gridi l'Africa all'Asia, e l'innocente
ombra d'Ipazia il grido orrendo aiuti.
Gridi irata l'Aurora all'Occidente,
narri le stragi dall'altare uscite;
e l'Occaso risponda all'Oriente.
*(*V. Monti, *Poesie,* Il fanatismo*)*

Vediamo se vi ricordate questi nomi.

In rigoroso ordine alfabetico: Elizabeth Blackburn, Carol Greider, Herta Müller, Elinor Ostrom, Ada Yonath. Vi dicono niente? È sperabile che vi suonino un po' familiari, almeno di questi tempi, in quest'autunno inoltrato del 2009: anche se la consegna ufficiale avviene sempre il 10 Dicembre, anniversario della morte di Alfred, i nomi dei vincitori dei premi Nobel si conoscono già a Ottobre, e i cinque nomi sopra ricordati appartengono ad altrettanti *laureati*[1] di quest'anno. E, come non è difficile notare dai nomi di battesimo, si tratta di cinque donne.

1 *Cinque premi Nobel 2009 – Blackburn, Greider, Müller, Ostrom, Yonath*

Non è un particolare trascurabile. A voler giocare con le percentuali, è del tutto sorprendente che ben quattro premi su sei (67%) vedano quest'anno un nome femminile nel loro albo d'oro. Certo, a voler essere un po' più pignoli, si può diluire l'entusiasmo femminino e femminista notando che solo 2,5 dei 6 premi totali sono andati al gentil sesso, ridimensionando così la percentuale ad un più modesto 42%. I premi possono, infatti, essere condivisi: in parti uguali, come ad esempio nel caso di Elinor Ostrom e Oliver Williamson che si sono equamente spartiti il premio per l'Economia, o anche in rapporti diversi, come è successo quest'anno per la Fisica: metà premio è andato a Charles Kao, mentre gli altri due vincitori, Willard Boyle e George Smith hanno dovuto accontentarsi di un quarto di premio a testa. Facendo i conti in questa maniera, si vede che se Herta Müller ha conquistato il premio indiviso per la Letteratura, Elizabeth Blackburn e Carol Greider hanno invece ottenuto un terzo a testa del premio per la Medicina e Fisiologia; aggiungendo allora il terzo vinto da Ada Yonath per la Chimica e il già citato mezzo premio della Ostrom, si raggiunge appunto la quota di 2,5 su 6.

Si possono fare conti ancora più pessimistici. Alla fin fine, anche se ben cinque sono le donne premiate, sono sempre in netta minoranza rispetto ai colleghi di sesso maschile: ai tre fisici e all'economista già citati bisogna infatti aggiungere Jack Szostak (Medicina e

[1] Contrariamente a quanto normalmente si dice, non esistono "vincitori" del Premio Nobel, perché, come asserisce un po' pomposamente il sito ufficiale, *"l'attribuzione dei premi Nobel non è una competizione né una lotteria, e di conseguenza non ci sono vincitori né vinti. I laureati del Nobel ricevono il premio in riconoscimento delle loro conquiste in fisica, chimica, fisiologia o medicina, letteratura, pace".*

Fisiologia), Venkatraman Ramakrishnan e Thomas Steitz per la Chimica, e Barack Obama per la Pace. Totale, otto maschietti contro cinque femminucce, cosa che abbassa la quota rosa al 38%. Prima di stracciarsi le vesti per il vistoso crollo della percentuale (e in parte anche per rendersi pienamente conto del perché Rita Levi Montalcini si è detta assai felice del numero di donne premiate quest'anno), si può andare a spulciare negli archivi della Fondazione Nobel[2] e scoprire con raccapriccio che, dalla sua istituzione, il premio è stato assegnato per 829 volte; togliendo le associazioni e normalizzando i pochi premi andati più volte alla stessa persona, sono 802 gli individui che hanno ottenuto il premio. Le donne, in tutto sono solo 40: meno del cinque per cento.

Lo squilibrio tra la quota di popolazione femminile (che ci prendiamo la libertà di presumere molto vicina al 50%) e quella delle Nobel-laureate al femminile è ampiamente al di fuori di ogni possibile naturale fluttuazione statistica. Che lo si voglia o meno, il gap che separa dal punto di vista del genere la formazione d'eccellenza è ancora alto, persino nel ricco Occidente. Anche se non è molto corretto prendere come campione statistico una base dati che affonda le sue radici nel lontano 1901, quando anche solo l'idea di far frequentare una scuola alle ragazze era da considerarsi temeraria, è altrettanto palese che, seppur più vicine, le pari opportunità nella formazione, nel lavoro e nella ricerca sono ancora lontane dall'essere raggiunte in quasi tutti i paesi del mondo (con differenze macroscopiche tra paese e paese, comunque).

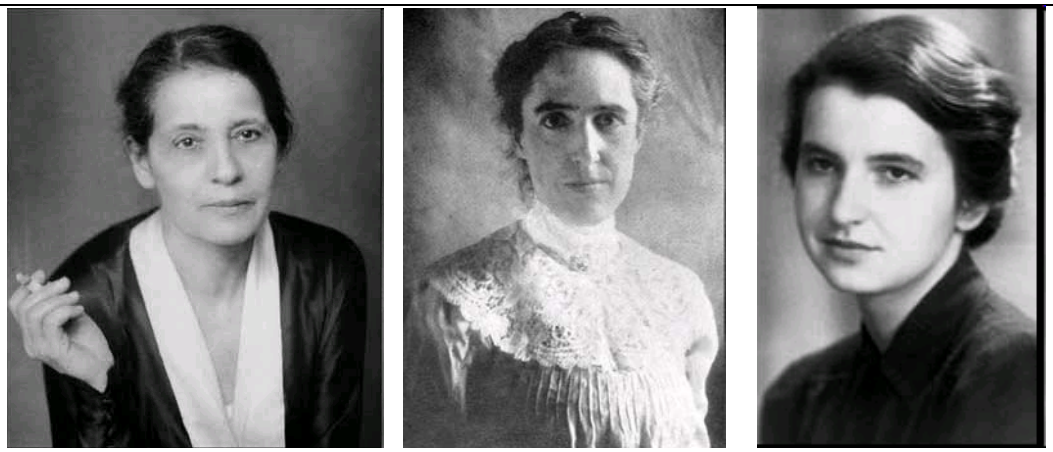
Una delle maniere più semplici per rendersene conto è la banale enumerazione: ogni qual volta si cerca di recuperare nelle pieghe della storia i nomi delle donne famose non in quanto femmine – e quindi come mogli, madri, figlie, amanti, e per estensione vergini, regine, prostitute – ma semplicemente in quanto esseri umani, si deve sempre andare a caccia di eccezioni. Eccezioni certo presenti, in ogni campo, ma pur sempre eccezioni: sono esistite (ma erano poche), le pittrici, le scultrici; ci sono state (un po' più numerose) le scrittrici e le poetesse, ma sempre in forte minoranza; e ci sono state (pochissime) le scienziate.

Si finisce sempre per parlare di Maria Skłodowska, moglie, madre e suocera di premi Nobel[3], che per non sfigurare in famiglia di premi ne ha vinti due essa stessa, uno per la Fisica e uno per Chimica; ma questo è quasi un guaio, perché l'astro brillante di Marie Curie rischia più che altro di interrompere la discussione, anziché farla procedere nell'indagine delle cause dello squilibrio di genere nella storia della scienza. Anche perché, per una Madame Curie ci sono chissà quante donne letteralmente defraudate: è quasi inspiegabile come sia possibile che la grandissima Lise Meitner non figuri nell'elenco dei premiati a Stoccolma, e lo stesso si può forse dire di Henrietta Swan Leavitt[4]. In compenso, che Rosalind Franklin sia stata certamente scippata del Nobel che avrebbe dovuto quantomeno condividere con Williamson e Crick per la scoperta del DNA è sostanzialmente acclarato.

[2] http://nobelprize.org/index.html

[3] Maria Skłodowska Curie: moglie di Pierre, con il quale condivise il Nobel 1903 per la Fisica (tra moglie e marito si infilò, quell'anno, anche Becquerel), ma poi decise di vincere da sola il premio per la Chimica nel 1911. Marie e Pierre ebbero una figlia di nome Irene, che seguì le loro orme. Irene finì poi con lo sposare Frédéric Joliot, e moglie e marito vinsero insieme il Nobel per la Chimica nel 1935.

[4] Astronoma di prima grandezza d'inizio secolo, che rivoluzionò l'astrofisica e in parte la cosmologia con il suo studio sulle Cefeidi, e venne grosso modo trattata sempre alla stregua di un'impiegatuccia, o quasi. Quattro anni dopo la sua morte, Mittag-Leffler la propose per il Nobel, ma il premio postumo non venne ritenuto opportuno. Del resto, i rapporti tra Mittag-Leffler e Nobel (sia premio che persona) sono sempre stati ammantati di leggenda, di screzi e di mistero: ma qui ci vorrebbe una nota a piè di pagina per la nota a piè di pagina, quindi è meglio sorvolare.



2 *Tre Nobel inspiegabilmente mancati: Lise Meitner, Henrietta Swan Leavitt e Rosalind Franklin*

La matematica ha le sue eroine. La maggior parte nel Novecento, ma con qualche affascinante e intrigante eccezione anche nei secoli precedenti. Da Emmy Noether a Julia Robinson, da Sophie Germain alla Kovalevskaya, dalla Stott alla Scott, risalendo fino alla Agnesi, e ancora prima[5]. E, a proposito di "prima", parlando di donne e matematica è davvero impossibile non parlare – anzi non iniziare – proprio da lei, da Ipazia[6] di Alessandria.

3 *Ipazia*

Ipazia, figlia di Teone, nasce nel 1123 AUC, Ab Urbe Condita, ovvero nel dodicesimo secolo, a voler contare gli anni come probabilmente li contava lei, dalla fondazione di Roma. Secondo il nostro computo, correva allora il 370 d.C., più o meno. In realtà, gli storici più prudenti si limitano a dire che nacque nella seconda metà del IV Secolo dell'Era Corrente, ad Alessandria d'Egitto. Suo padre era forse il maggiore matematico del suo tempo (almeno finché non fu superato dalla figlia), ed è virtualmente certo che fu proprio da Teone che Ipazia venne iniziata ai misteri della matematica. Prima di lei, nessuna: almeno, per quanto ci è dato conoscere, non esiste nessun nome di donna che compaia nella storia della matematica prima del suo. Ma il suo c'entra di prepotenza, e in maniera sorprendente: Teone era non solo matematico, ma anche filosofo, capo della scuola Neoplatonica: ebbene, all'inizio del V secolo sarà proprio Ipazia a succedergli

[5] A questo proposito, potremmo guardare nel nostro orticello e fare due conti. I "compleanni" esistono da RM48, quindi, questo compreso, dovrebbero essere state pubblicate 83 celebrazioni di matematici. Alcuni compleanni sono però dedicati a più di un matematico (Hardy & Littlewood, Babbage & Lovelace, etc.). In prima (e probabilmente imprecisa) approssimazione dovrebbero essere stati protagonisti di Compleanni 102 individui. Tra questi, in forma di protagoniste, co-protagoniste o quasi-protagoniste troviamo solo sei signore: in ordine cronologico sono Emmy Noether (RM50), Ada Lovelace (RM58), Florence Nightingale (RM104), Elizabeth Scott (RM106), Maria Gaetana Agnesi (RM112) e appunto Ipazia in questo RM130. Meno del 6%, e se non ci avesse messo una pezza Alice, sponsorizzando almeno la metà dei sei tributi, saremmo messi probabilmente molto peggio delle Commissioni di Stoccolma.

[6] Come capita quasi sempre per i matematici dell'antichità, la regola che vuole che il matematico protagonista del compleanno sia festeggiato nel suo mese di nascita viene meno per la banale ragione che non si conosce con esattezza la loro data di nascita. In questo caso, alcune fonti riportano Novembre come mese di morte di Ipazia, ma non sembra affatto una data sicura: più fonti dicono che Ipazia morì durante la Quaresima, e comunque in primavera. In ogni caso, ci sono altre ragioni per le quali ne parliamo proprio in questo periodo, e si capiranno leggendo il resto dell'articolo; e comunque, che questo fosse un compleanno anomalo lo si poteva capire già dal fatto che il nome del protagonista veniva citato prima ancora dell'inizio del testo, già nella citazione.

come capo della scuola filosofica alessandrina: sarà lei a tener lezione sulla base degli scritti dei padri fondatori del neoplatonismo, come Plotino e Giamblico.

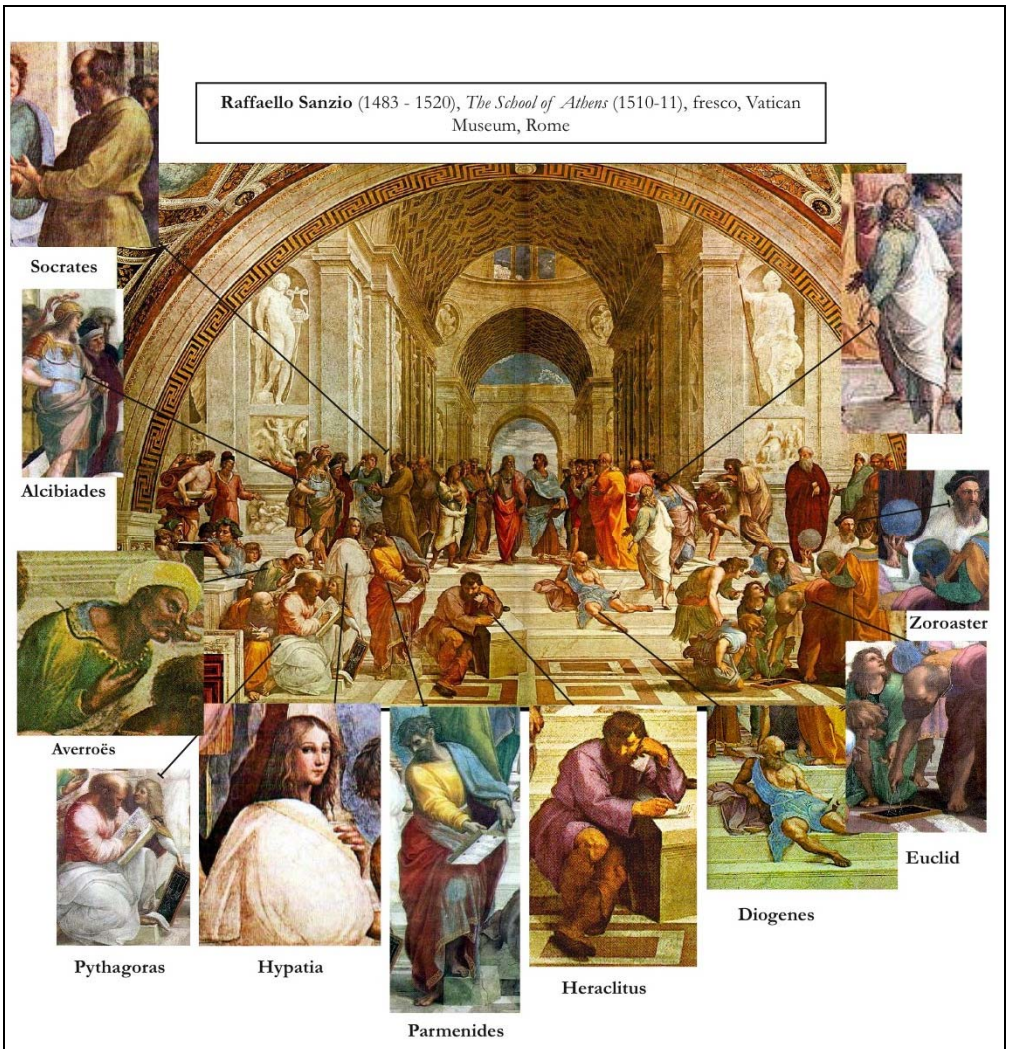
4 *Ipazia secondo Charles William Mitchell Laing Art Gallery, Newcastle upon Tyne*

Il neoplatonismo è una disciplina filosofica non banale, che presuppone livelli diversi di realtà e, in un certo senso, di conoscenza e consapevolezza. Si sposava pertanto benissimo con quello che oggi chiamiamo metodo scientifico, perché la continua ricerca aggiunge gradi di conoscenza senza necessariamente avere la pretesa di raggiungere la pienezza ultima, l'idea platonica di conoscenza. E Teone prima e Ipazia poi coniugavano perfettamente conoscenza, matematica e filosofia. Non si sa con certezza se Ipazia abbia effettivamente prodotto dei lavori originali in matematica, ma è certo che collaborò con le opere del padre: e alcune fonti non esitano a definirla "*più intelligente del genitore*". Così, è verosimile che gran parte delle opere di Teone siano ascrivibili anche a lei: tra queste, i commenti all'*Almagesto* di *Tolomeo* e la edizione arricchita e commentata degli *Elementi* di *Euclide*.

Da sola, senza la guida del padre, sembra poi che abbia compilato e commentato *l'Aritmetica* di *Diofanto*, le *Coniche* di *Apollonio*, e soprattutto che siano sue le realizzazioni di un originale astrolabio piano e di un idroscopio graduato in metallo. Questo in fondo la rende anche progenitrice delle ricercatrici di fisica, oltre che matematica e filosofa: e la sua capacità di riedizione dei classici la qualifica anche come prima divulgatrice scientifica e perfetta bibliotecaria (non per niente è stata il centro culturale della città con la biblioteca per antonomasia, Alessandria); ma in ultima analisi era nell'insegnamento e nella preparazione dei testi che trovava spazio il suo maggior talento. In un certo senso, Ipazia sembra essere davvero l'archetipo della professoressa di matematica. Anche se non sempre (o non tutte) le professoresse sono rappresentate come esempi di bellezza, nel caso di Ipazia la leggenda vuole invece che fosse anche assai graziosa, oltre che dotta; modesta e gentile, oltre che intelligente; e la leggenda ha preso evidentemente forma e luce, almeno nella rappresentazione che, verso la fine dell'Ottocento, ha fatto di Ipazia il preraffaellita inglese Charles Mitchell: l'ambientazione del quadro è drammatica, perché coglie l'eroina nei momenti sconvolgenti che precedono l'esplodere della violenza nei suoi confronti, cosa che giustifica la scelta di rappresentarla nuda, ma ciò non ha impedito all'artista di dipingerla bella come una top model, o forse anche di più.

Del resto, le rappresentazioni di Ipazia hanno sempre avuto vita difficile. Curiosamente, la più nota immagine di Ipazia, a parte quella *desnuda* del citato *preraffaellita*, è opera propria dello stesso *Raffaello* Sanzio. La figlia di Teone è infatti l'unica donna raffigurata nella mastodontica e celeberrima "Scuola di Atene", affresco della Stanza della Segnatura dei Palazzi Vaticani, dove i grandi nomi dell'antichità sono ritratti prendendo le sembianze di personaggi contemporanei dell'opera. Raffaello, oltre a mettere se stesso nella parte destra del dipinto a mo' di firma, usò infatti le fattezze di Michelangelo per

rappresentare Eraclito, quelle di Leonardo da Vinci per Platone, Bramante per dare il volto a Euclide, e così via.



5 *La Scuola di Atene di Raffaello, con i filosofi messi in evidenza*

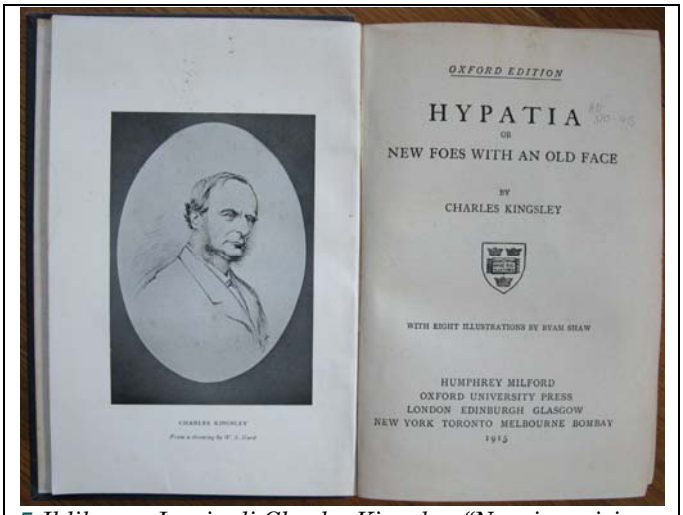
In questo affresco, la figura di Ipazia ha avuto una strana avventura. Raffaello, probabilmente affascinato dal personaggio o, più semplicemente, dalla sua unicità femminile, aveva in progetto di porlo al centro del quadro, nello "spazio vuoto" tra Parmenide e Diogene. Quando il cardinale responsabile dell'esecuzione notò la fanciulla nei primi bozzetti dell'affresco, interrogò Raffaello su chi fosse la donna rappresentata. "*Ipazia di Alessandria,*" rispose Raffaello: "*studiosa di matematica, filosofia, astronomia in Alessandria, e certamente uno dei maggiori pensatori di tutti i tempi.*" "*Toglietela*", sembra che abbia risposto il cardinale: "*la sua conoscenza va contro i principi della fede. Per il resto, il dipinto è accettabile.*"

Sembra che Raffaello fosse davvero dispiaciuto dall'ordine ricevuto. Nelle sue intenzioni, Ipazia doveva essere il vero baricentro del dipinto, anche perché avrebbe dovuto rappresentare il "centro di raccolta" del sapere che proveniva dai grandi dell'antichità che le stavano intorno e che lei, in qualità di vestale della conoscenza, avrebbe conservato e trasmesso ai posteri; da insegnante e commentatrice di testi qual'era stata, il ruolo le si addiceva perfettamente. Dispiaciuto, ma non al punto di poter disobbedire ad un ordine esplicito: alla fin fine, un'opera come quella è una commessa che vale una vita intera d'artista, e non ci si può incaponire più di tanto su questioni di principio.


6 *Bozzetto senza Ipazia*

Raffaello però escogitò una sorta di diplomatico compromesso: in una zona più defilata, dove inizialmente non era previsto che comparisse, inserì ugualmente l'immagine di Ipazia, ma usando una cautela particolare; come modello per Ipazia scelse infatti Francesco Maria della Rovere, amato nipote del papa Giulio II. Francesco aveva al tempo solo quindici anni, e poteva essere usato pertanto come modello per una figura femminile[7]. Era difficile ordinare di rimuovere una raffigurazione del nipote prediletto del papa, e così Ipazia riuscì a rientrare dalla finestra nell'affresco dalla quale era stata espulsa. Il bozzetto che mostra la zona dove poi ha preso posto la fanciulla ancora priva della sua presenza è ancora esistente.

In realtà, i rapporti tra la figura di Ipazia e la chiesa sono assai più burrascosi di quanto si potrebbe pensare leggendo solo queste righe a commento dell'affresco di Raffaello. Ma per capire quest'aspetto, occorre cercare di capire – per quanto possibile – come è finita la vita della prima matematica della storia.



7 *Il libro su Ipazia di Charles Kingsley: "Nuovi nemici con una vecchia faccia"*

Anche se la narrazione più celebre è quella romanzata da Charles Kingsley, "*New Foes with an Old Face*" la figura di Ipazia è indubbiamente storica. Ne parlano almeno tre fonti: le *Cronache* di Giovanni, vescovo di Nikiu, la *Storia Ecclesiastica* di Socrate Scolastico, e la *Vita di Isidoro* di Damascio.

Lasciamo quindi perdere i romanzi, e facciamo parlare Giovanni di Nikiu: *"…e allora una moltitudine di credenti in Dio si mostrò sotto la guida di Pietro il magistrato – questo Pietro era un perfetto credente in tutto ciò che riguardava Gesù Cristo – e si diressero a cercare la donna pagana che aveva ingannato il popolo della città e il prefetto con i suoi incantamenti. E quando vennero a sapere dove si trovava, andarono da lei e la trovarono che sedeva su un'alta sedia, e dopo averla fatta scendere la trascinarono alla grande chiesa, nel luogo che chiamavano Cesarione. Questo accadeva nei giorni del Digiuno. Poi le strapparono le vesti e la trascinarono lungo le strade della città finché morì. E la portarono in un posto chiamato Cinaron, e bruciarono col fuoco il suo corpo. E tutta la gente circondò il patriarca Cirillo e lo chiamò "nuovo Teofilo", perché aveva distrutto gli ultimi resti di idolatria nella città.*"[8]

[7] Come fanciulla ritratto da Raffaello, come uomo ritratto da Tiziano: è infatti celebre un suo ritratto del Vecellio del 1536.

[8] Se Vincenzo Monti (che religiosamente abbiamo riportato in apertura d'articolo) era dileggiato per essere "*il gran traduttor dei traduttor d'Omero*", noi siamo messi molto peggio. Le fonti citate sono riportate in traduzione inglese, e noi da queste traduciamo. Quindi si tratta di traduzione almeno doppia, con la finale fatta da noi, che non siamo certo professionisti nel campo. Prendete tutto con le molle.

Erano tempi davvero strani. Di certo è insolito pensare ai cristiani di allora non come vittime di persecuzioni religiose, ma piuttosto di persecutori. Ecco lo stesso episodio, secondo Socrate Scolastico, storico cristiano: *"C'era in Alessandria una donna chiamata Ipazia, figlia del filosofo Teone, che aveva fatto tali conquiste in scienza e letteratura da sorpassare tutti i filosofi del suo tempo. Essendo succeduta al padre nella guida della scuola di Platone e di Plotino, ella insegnava i principi della filosofia ai suoi discepoli, molti dei quali venivano da lontano per assistere alle sue lezioni. A dimostrazione della sua erudizione e delle sua abilità di conversazione, che aveva acquisito in seguito alla coltivazione della sua mente, appariva spesso in pubblico in presenza di magistrati, e non aveva vergogna di partecipare alle assemblee di uomini. Per questo gli uomini la ammiravano sempre più, per la sua straordinaria dignità e virtù. Eppure anch'essa cadde vittima della gelosia politica che a quel tempo prevaleva. Poiché ella aveva frequentazioni con Oreste, fu calunniosamente riportato tra i cristiani che era stata lei ad impedire che Oreste si riappacificasse con il vescovo. Allora alcuni di essi, il cui capo era un lettore chiamato Pietro, presi da uno zelo bigotto e ferino, la assalirono sulla via di casa e, trascinatala giù dal carro, la trascinarono alla chiesa chiamata Cesarèo dove la spogliarono completamente e la uccisero a colpi di tegola. Dopo aver fatto a pezzi il suo corpo, portarono le sue membra sanguinanti in un posto chiamato Cinaron, e lì le bruciarono. Questo episodio ha portato l'obbrobrio non solo su Cirillo, ma anche sull'intera chiesa di Alessandria. E di certo nulla può essere più lontano dallo spirito del cristianesimo che la giustificazione di massacri, battaglie, e cose di questo genere. Questo accadde nel mese di Marzo durante la Quaresima, nel quarto anno dell'episcopato di Cirillo, sotto il decimo consolato di Onorio e il sesto di Teodosio".* Secondo il nostro modo di contare gli anni, significa 415 dopo Cristo.

Tocca adesso a Damascio, che è il meglio disposto verso Ipazia e, di conseguenza, quello meno disposto a giustificare Cirillo. Anzi. "*Così era Ipazia, eloquente e forbita nel parlare tanto quanto era prudente ed educata nei suoi comportamenti. L'intera città l'amava e venerava in modo straordinario, ma i governanti della città fin dall'inizio la invidiavano, cosa che era accaduta a suo tempo anche ad Atene. Per contro, anche se la filosofia stessa è ormai scomparsa, tuttavia il suo nome ancora sembra magnifico e venerabile agli uomini che esercitano il governo. Così accadde che Cirillo, vescovo della setta avversa, stava passando vicino alla casa di Ipazia e vide una grande folla di gente e cavalli di fronte alla sua porta. Alcuni arrivavano, altri partivano, altri rimanevano in piedi lì intorno. Quando chiese perché ci fosse tutta quella gente e quale fosse la ragione di un tale assembramento, gli fu risposto che quella era la casa di Ipazia la sapiente, e che ella stava per affacciarsi e salutarli. Quando seppe ciò, Cirillo fu così colpito da invidia che incominciò immediatamente a pianificarne l'assassinio, e nella peggiore forma. Così, quando Ipazia uscì dalla porta nel suo modo consueto, un'orda di uomini feroci e spietati che non temevano né il giudizio di Dio né la giustizia degli uomini la attaccarono e la uccisero, commettendo così un disgraziato e abominevole gesto contro la loro stessa patria. (…) Il ricordo di questi eventi ancora vive tra gli abitanti di Alessandria*".

È sempre difficile provare davvero a capire, con assoluta chiarezza e sicurezza, cosa può essere accaduto così tanto tempo fa. La verità è *figlia del tempo*, dice un proverbio inglese, ma è certo una figlia avara di certezze. Per la Chiesa Cattolica, Cirillo di Alessandria è santo, celebrato il 27 Giugno, dottor e padre della Chiesa: succedette allo zio Teofilo alla guida della chiesa di Alessandria, si adoperò per far primeggiare il cristianesimo combattendo contro ebrei, novaziani e pagani. Partecipò al Concilio di Efeso ove si affermò la sua tesi, contraria al nestorianesimo. La sua figura non è secondaria, se appena due anni fa, da piazza San Pietro, papa Benedetto XVI ha ribadito la sua perfetta aderenza al pensiero cristiano[9]. Per gli storici, il giudizio su Cirillo è più difficile, ed esistono quasi tutte le sfumature possibili: alcuni propendono per una visione

[9] "*Di Gesù Cristo, Verbo di Dio incarnato, san Cirillo di Alessandria è stato un instancabile e fermo testimone...*", udienza generale del 3 Ottobre 2007.

sostanzialmente coincidente con la cronaca di Damascio, e ricordano che in fondo Cirillo aveva davvero una sorta di esercito privato di fanatici, i *parabolani*, e che i suoi metodi contro gli oppositori religiosi, ebrei e pagani in primis, non erano davvero assimilabili alla francescana non-violenza. Altri ritengono invece che l'atmosfera di quei tempi fosse comunque devastante e difficile da controllare, resa malsana da mille intrighi politici, e pensano che il vescovo potrebbe non aver avuto un ruolo attivo nella pianificazione del massacro della matematica alessandrina, ma solo una sorta di ruolo passivo.

A noi pare improbabile che Cirillo, capo della comunità cristiana della città, potesse davvero essere totalmente esente da colpe: però non ci sembra particolarmente costruttivo mettersi a riaprire una puntuale caccia al colpevole in un delitto vecchio di sedici secoli. L*a figlia del tempo* invecchia e perde molti dettagli. Quel che è certo, senza ombra di dubbio, è che il fondamentalismo porta spesso al fanatismo, e non riusciamo a trovare nella storia un solo esempio in cui il fanatismo abbia prodotto qualcosa di buono. Per contro, esempi del contrario abbondano in ogni minima piega del tempo.

Certo è che ci piacerebbe davvero che di Ipazia si tornasse a parlare. È un personaggio dal fascino e dalla bellezza assoluti, non solo per i cultori della matematica e della scienza. È il simbolo della conoscenza e della propagazione della conoscenza, e come tale un simbolo profondamente femminile. È una martire, ma martire pagana, civile, oseremmo dire martire della ragione, e sicuramente martire della scienza. Anche se rinunciamo a prendercela con Sant'Agostino, per il quale "matematici" era un insulto, vorremmo però quantomeno avere la libertà di innamorarci di questa donna che viveva di libri e di scienza, di matematica e di filosofia.

8 *Rachel Weisz interpreta Ipazia in "Agorà" di Alejandro Amenabar*

Così, scoprire che la più grande produzione cinematografica che la Spagna abbia mai affrontato riguarda proprio la storia di Ipazia è stata davvero una bella notizia: il regista Alejandro Amenabar ha girato "*Agorà*", film basato sul già citato romanzo di Charles Kingsley. Ad interpretare Ipazia c'è la splendida Rachel Weisz, già premio Oscar.

Ma, e sembra quasi una maledizione, ad ogni buona notizia ne segue una brutta, o quantomeno incomprensibile: il film[10], già uscito in Spagna e pronto per giungere nelle sale americane, israeliane, francesi, europee, insomma in tutto il mondo o quasi, sembra che non giungerà in Italia.

C'è chi sostiene che questo dipenda anche dal fatto che la Chiesa in Italia è particolarmente potente, e che la Chiesa non vuole che questo film raggiunga le sale cinematografiche. Non vogliamo crederci: paradossalmente, sarebbe quasi una lusinga speciale, per il pubblico matematico italiano, quella di essere riusciti ad attrarre l'attenzione preoccupata del Vaticano. Temiamo che la ragione sia più banale, persino più triste: ovvero che i distributori del film pensino che distribuire *Agorà* in Italia sia semplicemente un cattivo affare, che non ne valga la pena.

[10] In rete, o più precisamente su YouTube, si trova facilmente il trailer, che rende abbastanza bene l'idea dell'investimento spagnolo. Sembra quasi un kolossal: http://www.youtube.com/watch?v=-WSU-hh2j2g

Adesso, tocca un po' a noi decidere quale sia l'alternativa peggiore: quella di essere privati della visione di un film per una sorta di censura religiosa e fondamentalista, o quella di non essere un mercato minimamente attraente per l'intrattenimento culturale. Non è una scelta facile.

Non sappiamo quale reale valore possano avere le petizioni online, ma ci pare comunque doveroso far presente, alla fine di questa celebrazione, che qualcuno si è almeno preso la briga di proporre una petizione perché il film di Amenabar venga distribuito in Italia. Quella che segue è la locandina che la pubblicizza, con tanto di link.

9

2. Problemi

	Rudy d'Alembert	**Alice Riddle**	**Piotr R. Silverbrahms**
A gentile richiesta	N/A	N/A	N/A
L'ultima avventura del TRE-mendo duo			

2.1 A gentile richiesta

Ragazzi, abbiamo un problema, relativamente ai problemi.

Alcuni lettori ci hanno fatto "gentilmente" notare che stiamo tirando alto, per quanto riguarda la difficoltà dei problemi; robe che un brillante dottorando in matematica ci pensa per almeno un paio di mesi di solito vengono liquidate con un paio di pipe o poco più. Bene, abbiamo deciso di cercare un problema "multivalore", come difficoltà; nel senso che siamo partiti da un problema ragionevolmente facile, ma poi ci sono venute una serie di idee, e francamente non abbiamo ben chiara la difficoltà del risultato; garantiamo, comunque, che le prime domande sono tranquillamente abbordabili da tutti, noi inclusi; le estensioni, in compenso, posso essere un buon "*food for thought"* per chiunque, altri inclusi. Quindi, se riuscite a rispondere solo alle prime parti, mandate ugualmente la soluzione.

Supponete di avere un dado (da sei, ma non perdiamo in generalità); è abbastanza evidente che si può definire un gioco *onesto* dicendo "da uno a tre vinci tu, da quattro a sei vinco io"; con qualche (non noioso, ma lunghetto) calcolo, dovreste riuscire a stabilire le regole per un gioco onesto con *due* dadi (se non l'avete mai fatto, fatelo).

Bene, adesso di dadi ne avete *tre*: solo che il terzo dado sopra non ha dei numeri, ma su tre facce ha il segno "+", sulle altre tre ha il segno "–". Regola vuole che se esce il segno "+" si sommano i valori dei restanti due dadi, mentre se esce il segno "–" si sottrae il minore dal maggiore; è possibile, con questa terna, costruire un gioco equo?

> Due idee che ci sono venute in mente in questo momento: …e se il terzo dado avesse anche il "per" o il "diviso"? Sempre equiprobabili, evidentemente (per questo abbiamo scritto "o": sei diviso quattro, raramente fa un intero). E se i dadi non fossero a sei facce (qui quattro segni potrebbero starci, equiprobabili)?

Non solo, ma… Qualche numero fa[11] vi avevamo fatto analizzare il "seven-eleven", altrimenti noto come "craps"; riuscite a trovare un modo per giocare un gioco del genere con i dadi di cui sopra (scegliete il caso che preferite: "+/–", "tre operazioni", "non necessariamente sei facce"…).

Ora, fermo restando che noi abbiamo a malapena analizzato il primo caso, se diciamo "Yahtzee" a qualcuno vengono delle idee? Rudy, per un bel gioco complicato, sarebbe disposto anche a sacrificare il suo set da Dungeons & Dragons.

OK, non abbiamo ben chiaro neanche noi quali siano le domande, ma ci pare un campo esplorabile, appena cominciano le brutte giornate…

[11] RM096.

2.2 L'ultima avventura del TRE-mendo duo

Nel senso che quando andiamo in giro a tenere conferenze, dovremmo essere in tre ma per evidenti criticità logistiche va sempre a finire che siamo in due.

All'ultimo evento (che ormai tutti dovreste sapere sono misurati sulla Scala Torino, quella dei disastri planetari), Rudy si è preso una grande soddisfazione, ma ha avuto una piccola delusione; la soddisfazione glie la lasciamo raccontare con il suo classico stile parlato in nota[12].

La (piccola) delusione è nata dal fatto che nessuno gli ha chiesto di disegnare una cicloide (probabilmente sapevano come era fatta); Rudy era pronto a sfoggiare il suo meraviglioso "frisbee da ufficio" (un cordino morbido incollato a un foglio rotondo di tela cerata) da utilizzare come cerchio rotante senza strisciare su una retta per disegnare la curva. Non essendoci stata richiesta, per dar sfogo alle necessità ludiche di Rudy nel week-end successivo si è organizzata una garetta di frisbee, coinvolgendo anche l'intero staff dei VAdLdRM (nel senso che oltre a Fred e Alberto era presente anche Paolo, il figlio di Doc) e la moglie di Rudy (Paola): l'idea era di avere tre persone ai vertici di un triangolo e le altre tre dentro al triangolo; mentre i tre vertici si scambiano il frisbee, i tre in mezzo devono riuscire a prenderlo. Per "evidenti ragioni di motilità" *[non abbiamo capito bene cosa intendessero, e stiamo cercando di capire se offenderci o no: comunque, in segno di protesta, per tutto il gioco non ci siamo mossi dalle posizioni assegnate (RdA, PRS & Paola)]*, Rudy, Doc e Paola sono stati piazzati dentro al triangolo (in realtà, sui lati, uno per lato), mentre i tre giovini erano nei vertici; per dare un'idea delle posizioni, la situazione era circa questa:

Rudy era a metà strada tra Fred e Paolo, Doc era a metà strada tra Alberto e Paolo e Paola era a metà strada tra Alberto e Fred; le distanze tra due qualunque dei tre giovani teppisti o tra due qualunque degli arzilli vecchietti era sempre un numero pari (così nessuno aveva problemi con la virgola nel dividere per due e trovare la propria posizione); non solo, ma la distanza tra Alberto e Fred era maggiore della distanza tra Alberto e Paolo che era maggiore della distanza tra Fred e Paolo, che cercavano di stare il più vicini possibile.

Allora, secondo voi, quanto erano distanti i tre teppisti tra di loro?

…E così, anche quest'anno l'ultima partita della stagione ha portato a un grazioso mal di testa. E neanche causato dal frisbee!

3. Bungee Jumpers

Prima Parte

Sia dato un punto M su un cerchio di raggio R che circoscrive un n–agono regolare. Provare che la somma dei quadrati delle distanze di questo punto da tutti i vertici del poligono è un numero indipendente dalla posizione del punto M sul cerchio e che questa somma vale $2nR^2$.

Seconda parte

Sia dato un punto M sul piano sul quale giace un n–agono regolare $A_1A_2\ldots A_n$. Provare che la somma dei quadrati delle distanze tra M e i vertici del poligono dipende solo dalla

[12] "No, dunque, siete davanti a trenta prof di mate delle superiori, e fate un problema, dicendo che ha una caratteristica particolare che lo rende particolarmente interessante. Mezz'ora dopo chiedete se qualcuno ci ha provato e ricevete la risposta '…Non ci sono riuscito…'; alla successiva richiesta di spiegare perché era particolarmente interessante, tutti dicono che non l'hanno capito. Segno che non hanno neanche provato, visto che anche i VAdLdRM ci sono arrivati in tre – dicesi tre – minuti, al "trucco". Secondo voi quanto era contento, per aver tirato il cazziatone a trenta prof di mate che non avevano neanche provato a fare il compito?

distanza l di M dal centro O del poligono ed è pari a $n\left(R^2+l^2\right)$, ove R è il raggio del cerchio circoscritto al poligono.

Terza parte

Provare che quanto detto nella Seconda Parte resta valido anche se M non giace sul piano del poligono.

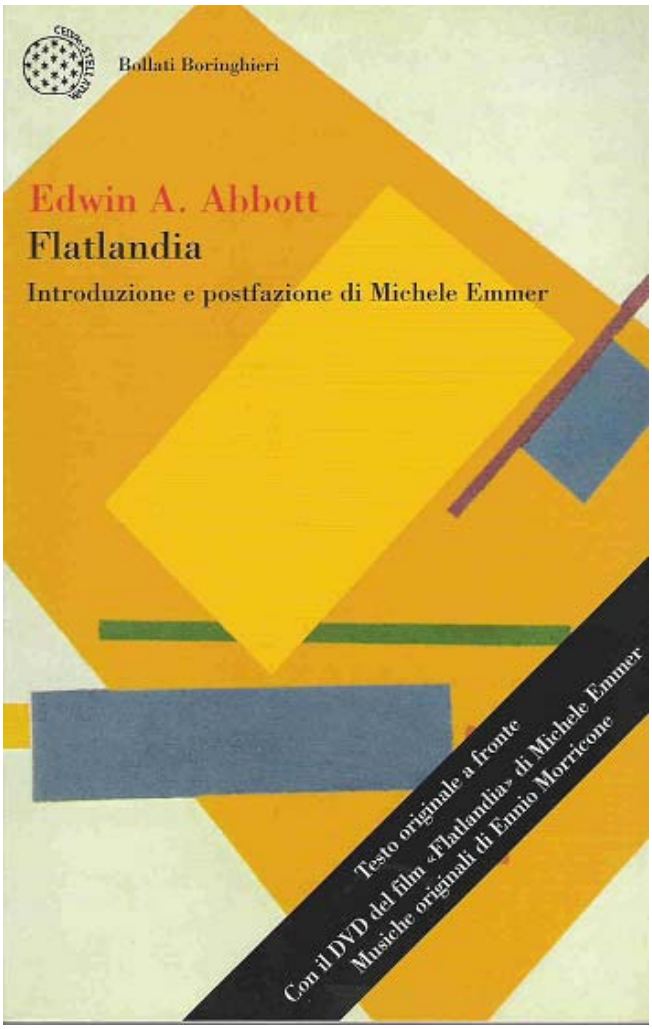
Tenete le risposte a portata: ci serviranno il mese prossimo.

La soluzione, a "Pagina 46"

4. Era Una Notte Buia e Tempestosa

Le regole che governano l'apparizione di questa rubrica su RM sono al tempo stesso assai rigide e ampiamente elastiche. Elastiche dal punto di vista cronologico delle sue apparizioni: è quasi un anno che non compariva su queste pagine, e la sua variabilità temporale è quindi decisamente confermata. Rigide, invece, lo sono per i criteri di apparizione: in questa rubrica si recensiscono opere in cui abbiano messo mano direttamente persone appartenenti alla comunità di RM, lettori, redattori, amici del giornalino, insomma. Questa volta parliamo di un'opera che ha visto il contributo di un grande amico di RM, anche se è del tutto evidente che, nello scambio d'amicizia, siamo noi a guadagnarci di gran lunga.

4.1 Flatlandia



È davvero possibile, per una rivista di matematica ricreativa, recensire *Flatland* di Edwin Abbott Abbot? Suona strano, quasi come insegnare l'alfabeto all'università: esistono delle conoscenze che si danno sempre per scontate, delle basi su cui costruire, che si presuppongono già nel discepolo e nel lettore. In fondo, se leggete una rivista scritta in italiano si dà per scontato che sappiate leggere e comprendere la lingua italiana; se leggete un giornale di matematica, si presuppone che conosciate, e siate in grado di comprendere i simboli della matematica, almeno quello essenziali; così, se vi ritrovate a leggere una rivista di matematica ricreativa, si suppone che conosciate alcuni testi sacri che affrontano la matematica da un punto di vista insolito, originale, giocoso: e quindi è lecito presupporre che conosciate già Flatlandia.

È un libro vecchio di 115 anni: narra le storie di un Quadrato e del suo mondo, piatto come è piatto il piano di Euclide. Curiosamente questa rubrica, che pure ha recensito solo pochissimi libri, ha

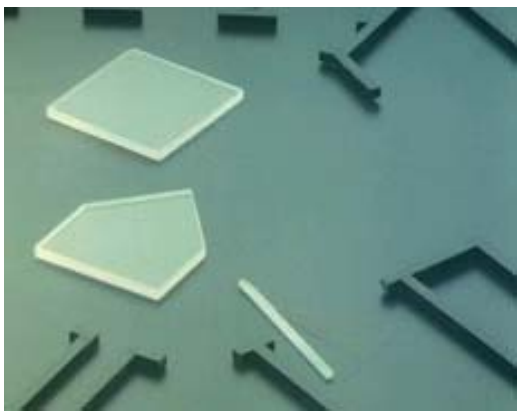
già trattato un testo succedaneo a questo capolavoro dell'Ottocento, il "*Flatterland*" di Ian Stewart, e in un certo senso questo è comunque indicativo della popolarità e della meritata fama dell'originale. In Italia è nota l'edizione per i tipi di Adelphi e per la traduzione di Masolino D'Amico: non abbiamo nessuna idea sussistano vincoli di parentela con la traduttrice di questa nuova edizione, Caterina D'Amico. Di certo, è comunque encomiabile il certosino lavoro di traduzione che una simile opera richiede: e, a maggior ragione, è encomiabile la scelta, in questa nuova edizione della Bollati Boringhieri, di riservare tutte le pagine di ordine pari al testo originale, in modo che la lettura in italiano delle pagine dispari possa essere agevolmente deviata, a richiesta, sul testo originale.

Però, se di un classico stiamo parlando, non è certo per raccontare la storia e l'importanza del classico medesimo: è qualcosa che si trova persino su Wikipedia[13], e

davvero non dovrebbe essere necessario aggiungere i nostri poveri commenti in merito. Se ne parliamo è per mettere in evidenza le caratteristiche particolari di questa edizione, e naturalmente per esaltare il ruolo di chi fa da anello di congiunzione tra il capolavoro e RM.

Il legame tra RM è Flatlandia è Michele Emmer. Michele è un nome assai importante della matematica italiana, e senza dubbio noi di RM commettiamo peccato di orgoglio, di alterigia, insomma ce la tiriamo un po', a voler annoverarlo tra i lettori di RM. Ma amico ci è davvero, se ha acconsentito a scrivere la prefazione al nostro "Rudi Ludi" – e senza ricevere in cambio nient'altro che la nostra riconoscenza – e quindi, se davvero stiamo commettendo peccato d'orgoglio, restiamo peccatori consci e soddisfatti.

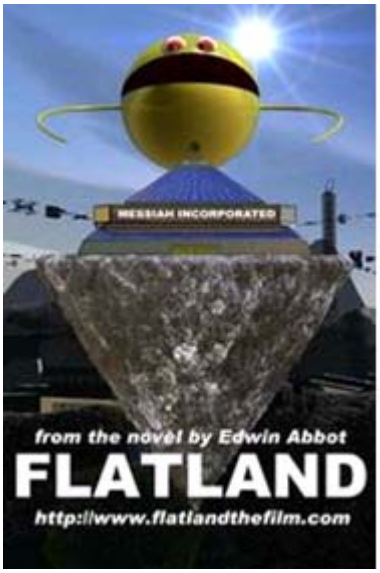
Emmer non è solo matematico: è anche regista (e in questo è figlio d'arte); ed è proprio questa sua seconda natura (sempre che sia lecito mettere in ordine, quasi in classifica, i molteplici interessi d'una persona) che più rende interessante la pubblicazione di Bollati Boringhieri: infatti, anche se Michele ha scritto sia un'introduzione che una prefazione che una postfazione al testo di Abbott, il suo contributo principale al libro resta il film che si trova allegato in DVD al libro stesso.

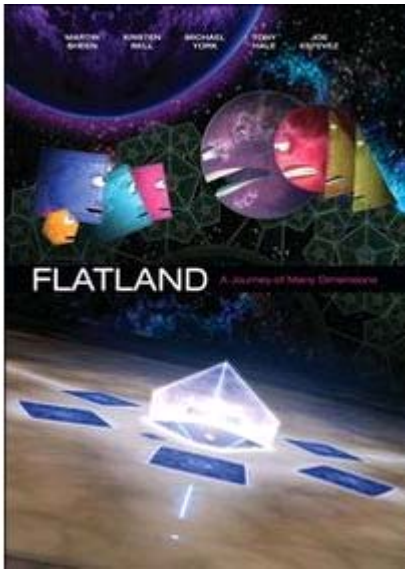


Fare un film animato è difficile. Fare un film animato con pochi mezzi è difficilissimo. Fare un film animato con pochi pezzi e con rigorosi vincoli scenografici e tecnici dovuti ad un'ambientazione del tutto spietata è quasi impossibile. Eppure il film Michele lo ha realizzato, e già dal 1982: questa edizione di Flatlandia è però la sua prima occasione di avere una distribuzione ufficiale per le canoniche vie editoriali. Per l'occasione, anche il film è stato rivisitato e arricchito: la postfazione di cui abbiamo già parlato racconta proprio il *making* del film, dai primi tentativi fino al completamento con un parte di computer grafica, nonché della colonna

[13] http://it.wikipedia.org/wiki/Flatlandia

sonora che contiene anche musiche originali di Ennio Morricone. È davvero affascinante scoprire come sia complesso e difficile superare le difficoltà tecniche che si presentano ad un progetto del genere: dalla scelta dei materiali più adatti agli artifici necessari per rendere visibili i protagonisti del film. Come dice lo stesso Emmer, occorreva un materiale trasparente, dai bordi riflettenti, e che fosse possibile ritagliare in forma di piccoli poligoni: e soprattutto è curioso come si sia dovuto ricorrere alla terza dimensione (quella dei bordi riflettenti, appunto, cui è delegata tra l'altro quasi per intero la funzione di "comunicazione" tra poligoni) per meglio rappresentare gli abitanti del mondo che di dimensioni ne ha solo due.





Negli Stati Uniti, e con i mezzi degli Stati Uniti, nel 2007 sono usciti ben due film su Flatland: uno di 34 minuti, diretto da Jeffrey Travis, e uno di 95 minuti, diretto da Ladd Ehlinger Jr.

Naturalmente, nessuno dei due film è mai giunto in Italia, e non possiamo darne un giudizio. Però, per una volta, possiamo almeno dire che esiste un film italiano che ha preceduto, di diversi anni, l'idea della messa su celluloide del romanzo di Abbott. E, grazie a questo libro con DVD, anche vedercelo a casa.

Titolo	Flatlandia
Titolo Originale	Flatland A Romance in Many Dimensions
Autore	Edwin Abbott Abbott
Traduzione	Caterina D'Amico
Introduzione, Postfazione, Realizzazione del film in DVD allegato	Michele Emmer
Editore	Bollati Boringhieri
Collana	Varianti
Data di Pubblicazione	2008
Prezzo	25,00 Euro
ISBN	978-88-339-1938-6
Pagine	255

5. Soluzioni e Note

Novembre. Come ogni mese cerchiamo di non dirvi quello che succede in Redazione, e poi ve lo diciamo lo stesso... ma almeno vediamo di cominciare con altro, e cioè con i vostri contributi.

Proprio il primo del mese scorso ***Ezio*** ci ha mandato una breve dimostrazione dell'esistenza di infiniti numeri primi, chiedendoci cosa ne pensavamo. Previa autorizzazione, abbiamo deciso di passare la domanda ai nostri lettori, che sono molto attenti, per cui ecco la dimostrazione: scriveteci, passeremo ad ***Ezio***.

Dal Teorema Fondamentale dell'Aritmetica possiamo scomporre ogni numero N come prodotto di potenze di numeri primi:

$$N = \prod_{i=1}^{k} p_i^{\alpha_i}$$

È altresì logico, ponendo $M=h\,N$ scrivere:

$$M = hN = \prod_{j=1}^{l} p_j^{\alpha_j} = h\prod_{i=1}^{k} p_i^{\alpha_i}$$

Da cui si deduce che $p_i \neq p_j$ e che al tendere di M all'infinito ($h\to\infty$) devono esistere infiniti numeri primi che soddisfano l'equazione. Per provarlo facciamo delle considerazioni su h:

1. h è un numero primo. Se nella sequenza dei valori $p_j^{\alpha_i}$ ho:

   $p_i=h$ per $i=z$ => $a_z=a_z+1$

   In tal situazione i numeri primi oggetto della scomposizione rimangono sostanzialmente gli stessi.

2. h non è un numero primo e pertanto possiamo reiterare il processo applicando ancora il Teorema Fondamentale dell'Aritmetica e scrivere:

   $$h = \prod_{m=1}^{z} p_m^{\alpha_m}$$

   si possono avere due sottocasi:

   a. $p_i=p_m$ cioè tutti i p_m esistono già nell'espressione di N e questo mi riporta sostanzialmente al caso discusso sopra.

   b. $p_i\neq p_m$ in almeno un caso e questo valida la tesi che esistono infiniti primi.

Ma il caso 2b è facilmente costruibile e questo porta a validare il teorema che esistono infiniti numeri primi. Arbitrariamente posso scegliere un valore di h tale che: $h=N+1$, cioè n ed h sono "relativamente primi" (hanno come unico MCD il valore 1). Questa equazione ci dice che h non è divisibile per gli stessi primi p_i che determinano N stesso e pertanto devono esistere dei primi $p_j\neq p_i$ (o almeno uno di questi). E la tesi è dimostrata.

Speriamo di averla riportata correttamente... Il prossimo contributo ci è piaciuto particolarmente perché coniuga matematica e poesia, come piace a noi. ***Loreto*** ci manda questo pezzo sulla media geometrica:

Se il cor tuo valutar anela
median geometrico tra due dati,
banal costruzione or ti svela

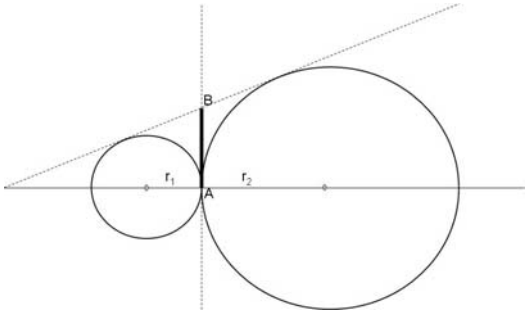
come lunghi, tediosi e complicati
manuensi calcoli puoi non far mai.
Con raggi pari a dati, sian tracciati

due cerchi, tangenti dove tu sai.
Indi la doppia comun tangente
dal detto tangente punto salpar fai.

Scegli ora, secondo il tuo cor piacente,
una retta che ambo i cerchi sfiori.
Alla fin ormai sei: sii gaudente!

Or dimostra, per guadagnar allori,
come pari sia il median desiato
a misura mera condotta fuori

dal tra cerchi di tocco punto dato
al comun tra rette: salpata pria
e tangente tra i cerchi afflato.



10 *La figura di* ***Loreto*** *per* $\overline{AB}=\sqrt{r_1 \cdot r_2}$.

Se digital macchina con te non sia,
bastevoli son compasso e righello
per fugar di quadre radici fobia.

Encomiastiche rime in stornello
per te or pensai che dimostrasti
tesi senza mai lamentar fardello.

Per te, allori, onori e fasti;
per me, che ahimè costruzion pensai,
sola speme per gli arcani vasti.

Non la trovate meravigliosa? Prima di procedere con qualsiasi altra cosa, vogliamo ringraziarvi per gli incredibili contributi riguardo a New Cuyama: ne sono arrivati talmente tanti che è difficile decidere quali link proporvi... ne mettiamo alcuni qui di seguito:

a. Grazie a ***.mau.***, http://en.wikipedia.org/wiki/New_Cuyama,_California e http://www.break.com/pictures/welcome-to-new-cuyama93291.html
b. ***Daniele*** ci scrive: *Gradevolmente allibito dal cartello riportato sulla copertina, ho cercato di raccogliere un po' di informazioni a riguardo. Ho troppa poca fiducia negli esseri umani per credere sia un "dotto" scherzo di qualche sindaco californiano, e l'assenza di siti che menzionino la storia del cartello ho paura suffraghi il mio punto di vista. Ad ogni modo, il cartello risiede effettivamente alle porte di New Cuyama, dopo un po' di sano bighellonaggio su Google Earth sono giunto alle seguenti coordinate: 34°56'54.07" N 119°41'30.57" W. Una volta inserite in G.E. tendenzialmente dovreste trovarvi davanti un incrocio tra due vie, una la statale californiana 166 e l'altra tale Perkins road. Proprio sull'incrocio dovreste anche vedere un benzinaio (con Burger Barn annesso), e appena alla sua destra un'iconcina di una macchina fotografica chiamata "Perkins Rd / CA-166". Doppio-clickando su questa si passa in modalità "street view" e ci si trova appunto con lo "sguardo" puntato al centro del rettangolo di navigazione, ovvero su questa stazione "MK GAS". A questo punto girando verso sinistra, superata la motrice di un camion, si vede il cartello incriminato, zoomabile a piacere e con una*

discreta nitidezza. Guardando questa Perkins road tra l'altro si dovrebbe vedere una colonnina di altre macchine fotografiche, un paio delle quali contengono altre visuali dello stesso cartello.

c. Un altro ***Daniele***, che si firma ***Tiggi***, deve aver seguito le istruzioni qui sopra, ma usando googlemaps... ci siamo divertiti molto a cliccare: http://maps.google.it/maps?f=q&source=s_q&hl=it&geocode=&q=34%C2%B056%E2%80%B253%E2%80%B3N+119%C2%B041%E2%80%B221%E2%80%B3W&sll=34.853256,-119.277191&sspn=0.602912,1.231842&ie=UTF8&ll=34.94885,-119.691753&spn=0.075277,0.15398&z=13&layer=c&cbll=34.948757,-119.691795&panoid=sZuDp_8lS4rPvR-GVJtpGA&cbp=12,177.67,,0,14.63

Ed ora passiamo alle novità. Se siete attenti, avrete già scoperto tutto, ma vi segnaliamo la versione aggiornata della sezione del nostro sito – il *Memento* (http://www.rudimathematici.com/memento.htm) – in cui tentiamo di segnalare tutti i prossimi eventi in ambito matematico di cui siamo a conoscenza. Abbiamo appena cominciato, ma contiamo di aggiornarlo spesso, compatibilmente con i nostri tempi, per cui continuate a seguirlo. Sempre sul sito, la pagina dei *Link* (http://www.rudimathematici.com/links.htm) è stata finalmente aggiornata, e abbiamo aggiunto una sottosezione del *Bookshelf* dedicata a un paio di nostri lettori matematici seri (http://www.rudimathematici.com/blocknotes.htm). Naturalmente noi li abbiamo già soprannominati ***R&M*** (***Rosario Turco*** e ***Maria Colonnese***), ma non fatevi trarre in inganno dal nostro modo di scherzare su tutto...

E adesso basta, che di sicuro abbiamo dimenticato parecchie cose importanti. Chiudiamo con una frase che ci ha inviato ***Ezio***, e la sua traduzione in termini matematici:

"*sembra incredibile come l'immaginazione alla massima potenza (dell'immaginazione) ci porti ad un esasperato, irrazionale realismo*", tradotto in matematica: $i^i = e^{-\left(\frac{\pi}{2}+2k\pi\right)}$.

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

5.1 [130]

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

Prima di parlarne, vediamo di riassumere il testo:

Ogni numero naturale 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. Di che colore è il numero 2008? Di che colore vengono gli altri anni da quelle parti, presente incluso?

Ora 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. Due domande:

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

I solutori di cui abbiamo raccolto i contributi sono ***Cid***, ***Alberto R.***, ***Silvano***, ***Mikhail***, ***Gnugnu*** e ***Franco57***. Come sempre tentiamo di dare la precedenza a chi ci scrive per la prima volta, e quindi partiamo con la versione di ***Mikhail***, che ha scelto un bell'allonimo: ***Miscellone***.

Per semplicità chiamiamo i numeri colorati in verde o blue semplicemente "colorati" e quelli colorati in nero "non colorati".

I. Immaginiamo che (a) sia il minimo numero positivo colorato (mettiamo in verde per determinatezza).

A questo punto:

(a) – colorato in verde

(2·a) – colorato in blu

(–a) – colorato in blu

(–2·a) – colorato in verde

II. Si nota facilmente che lo (0) non è colorato ((0) + (0) = (0)).

III. È importante il seguente fatto: se un numero (b) è colorato, il numero (b+3·a) ha per forza lo stesso colore. La dimostrazione è seguente: se (b) è verde, (b+a) è blu, ((b+a)+2·a) è di nuovo verde Se (b) è blu, (b+2 ·a) è verde, ((b+2·a)+a) è di nuovo blu. La stessa cosa vale ovviamente anche per il (b–3·a).

IV. Dimostriamo adesso che (a) e (2·a) sono gli unici numeri colorati nel intervallo ((0);(3·a))

Immaginiamo che esista un numero (b) colorato e tale che (0) < (b) < (3·a), e (b) è diverso da (a) e da (2·a)

1. Mettiamo che (b) sia colorato in verde. Siccome un numero positivo colorato non può essere minore di (a), abbiamo (a) < (b) < (3·a). Osserviamo numero (b–2·a) colorato in blu e tale che (–a) < (b–2·a) < (a), che contraddice al fatto che (a) sia il minor numero colorato.
2. Se invece, (b) è colorato in blu possiamo applicare al numero (3·a–b) la logica del punto IV.1

V. Mettendo insieme i punti III e IV si conclude facilmente che gli unici numeri colorati sono:

((2·k+1)·a) – colorati 'in verde

((2·k+2)·a) – colorati in blu

dove k=0, +/–1, +/–2, ...

VI. In conclusione si osserva che il numero 1009 (l'anno in cui è stata rasa al suolo la Chiesa del Santo Sepolcro a Gerusalemme) è un numero primo e quindi il prossimo colorato (in blu) sarà 2018 (chissà che cosa succederà ...).

Avete capito tutto? Proviamo a vedere che cosa ne dice ***Silvano***: troppe volte ci ha inviato i suoi contributi senza pubblicazione per meri problemi tecnici (usa una versione di editor che non piace molto ai nostri PC), questa volta vogliamo rimediare, anche se la sua soluzione è, come dire, giallorossa...

Problema ROMANISTA

[1] DEF: Numeri giallorossi $\forall n \in N \Rightarrow n \in R \text{ or } n \in G$

[2] DEF: Colorazione Unica $R \cap G = \emptyset$

[3] DEF: 8 è il primo giallo (Ma non era meglio il pupone con il N. 10 ?) $8 \in G, \forall n \in N \text{ ed } n < 8 \Rightarrow n \in R$

[4] DEF: Somma di Giallorossi $\forall r \in R, g \in G \Rightarrow r + g \in R$

[5] DEF: Prodotto di Giallorossi $\forall r \in R, g \in G \Rightarrow r \cdot g \in G$

[6] LEMMA: Intorno dei gialli $\forall g \in G \rightarrow (g+1), \ldots, (g+7) \in R$

DIM: I numeri 1,…,7 sono Rossi, quindi sto sommando un giallo ad un rosso che per [4] è rosso.

[7] LEMMA: $\forall g \in G \text{ ed } g \leq 8 n \Rightarrow g = 8 \cdot k \text{ con } k \in N \text{ ed } k < n$

DIM: Per induzione

n=1 → Vero per [3]

n=2 → $8 \in G$ per [3] $16 = 2 * 8 \in G$, inoltre per [6] 8 e 16 sono i soli numeri gialli

n=n → supposto vero per n–1 →8,16,….8(n–1) sono gli UNICI gialli

banalmente 8(n–1)+1,…8(n–1)+7 sono numeri Rossi per [6]

Devo dimostrare che 8n è giallo scomponendo n, posso avere 2 casi:

$n \neq 8^q k \text{ ed } k \text{ non multiplo di } 8 \Rightarrow n \in R$ per ipotesi di induzione, $8 \in G \rightarrow 8n \in G$

$n = 8^q k \text{ ed } k \text{ non multiplo di } 8 \rightarrow n \in G$ per ipotesi di induzione, ma allora:

$8n = 8^{q+1} k$ ma $8^{q+1} \in G, k \in R$ per ipotesi di induzione $\rightarrow 8n \in R$ per [5]

[8] LEMMA: gli unici gialli sono i multipli di 8 $\forall g \in G \rightarrow g = 8k \text{ con } k \in N$

DIM: Da [7] ponendo n arbitrariamente grande.

SOLUZIONE = 2008 = 8·251 è giallo, come lo sono 2000, 2008, 2016, ...

La seconda parte, sempre di ***Silvano***:

[1] DEF: Colorazione – Siano B è l'insieme dei numeri Blu, V dei Verdi ed $\bar{N}$ dei Neri allora: $\forall z \subset Z \Rightarrow z \subset B \text{ or } z \subset \bar{N} \text{ or } z \subset V$

[2] DEF/conseguenza: Disgiunzione (Colori non mischiati) $B \cap \bar{N} = \bar{N} \cap V = B \cap V = \emptyset$

[3] DEF: Somma di Blu $\forall b_1, b_2 \in B \Rightarrow b_1 + b_2 \in V$

[4] DEF: Somma dei Verdi $\forall v_1, v_2 \in V \Rightarrow v_1 + v_2 \in B$

[5] DEF: Opposto

[5a] $\forall v \in V \Rightarrow -v \in B$

[5b] $\forall b \in B \Rightarrow -b \in V$

[6] LEMMA: Opposto del nero è nero $\forall n \in \bar{N} \Rightarrow -n \in \bar{N}$

DIM: Per assurdo $Se -n \in B \Rightarrow -(-n) = n \in V$ assurdo per [5b],

$Se -n \in V \Rightarrow -(-n) = n \in B$ assurdo per [5a], quindi per [1] $-n \in \bar{N}$

[7] LEMMA: Zero è nero $0 \in \bar{N}$

DIM: Per assurdo $Se\ 0 \in B \Rightarrow -0 \in V$ assurdo per ipotesi

$Se\ 0 \in V \Rightarrow -0 \in B$ *assurdo per ipotesi* □

[8] LEMMA: Multipli di un numero colorato

$Se\ b_0 \in B \Rightarrow \begin{cases} (3k+1)b_0 \subset B \\ (3k+2)b_0 \in V \\ 3kb_0 \in \bar{N} \end{cases}$ □ ed anche similmente $Se\ v_0 \in V \Rightarrow \begin{cases} (3k+1)v_0 \subset V \\ (3k+2)v_0 \in B \\ 3kv_0 \in \bar{N} \end{cases}$ □

DIM:

$b_0 \in B \rightarrow b_0 + b_0 = 2b_0 \in V$ Quindi

$2b_0 + 2b_0 = 4b_0 \in B \rightarrow 4b_0 + b_0 = 5b_0 \in V$ Quindi

$4b_0 + 2b_0 = 7b_0 \in B \rightarrow 3b_0 + b_0 = 8b_0 \in V$

e cosi via si dimostrano i primi 2 enunciati, infatti: 1,4,7,10… sono i numeri Blu, mentre 2,5,8,11,.. sono i verdi; per i negativi basta considerare [5] si può costruire la sequenza blu: …, $(3k+1)$, –11, –8, –5, –2, 1, 4, 7, 10, …, $(3k+1)$, …

E similmente quella dei verdi è : …, $(3k+2)$, –10, –7, –4, –1, 2, 5, 8, 11, …, $(3k+2)$, …

Per quanto concerne $3kb_0 \in \bar{N}$ procedo per assurdo: se per assurdo

$3kb_0 \in B\ e\ b_0 \in B \rightarrow 3kb_0 + (3k+1)b_0 \in V, ma\ invece\ 3kb_0 + (3k+1)b_0 = b_0(3(2k)+1) \in B$

$3kb_0 \in V\ e\ b_0 \in B \rightarrow 3kb_0 + (3k+2)b_0 \in B, ma\ invece\ 3kb_0 + (3k+2)b_0 = b_0(3(2k)+2) \in V$

Quindi per [1] ottengo la tesi.

Le dimostrazioni della seconda parte sono simmetriche.

PARTE NUMERICA DEL PROBLEMA:

[9] LEMMA: 1 e –1 sono numeri Neri

DIM: Essendo $\pm 1492 = (3 \cdot 497 + 1) \cdot (\pm 1)$ se per assurdo 1 fosse Blu o Verde anche 1492 sarebbe dello stesso colore, il che non è possibile. Stesso dicasi per –1 con –1492.

[10] LEMMA: Numeri Verdi e Blu

$\forall z \in Z\ and\ z \in B \cup V \rightarrow z \in (3k+1)1008\ or\ z \in (3k+2)1008$

DIM: Visto che 1009 è primo, considero qualsiasi altro numero primo con 1009, ossia non un suo multiplo che so già per [8] come si comporta e lo chiamo x.

Senza perdita di generalità posso dire che X può essere scritto come $x = 3z + P$ potendo P assumere i valori 0,1,2:

$Come\ ad\ esempio \begin{cases} x = 3z \\ x = 3z+1 \\ x = 3z+2 \end{cases}$

Procedo per assurdo

Caso in cui fosse $x \in V$ si ha un assurdo, infatti dimostro che la somma di 2 verdi da Q= –1,0,1 che per [7] e [9] è certamente nera:

$1009 \cdot (3k+1) + x(3t+1) = Q$

$1009 \cdot 3k + 1009 + 3tx + x = Q$

$1009 \cdot 3k + 3tx = Q - 1009 - x$

Sostituisco al secondo membro soltanto, senza perdita di generalità, $x = 3z + P$:

$$1009 \cdot 3k + 3tx = Q - 1009 - 3z - P$$

Considero la tabella seguente per il fattore $Q - 1009 - P$:

	P=0	P=1	P=2
Q=1	1–1009–0= –1008 = –3·336	1–1009–1= –1009 NO	1–1009–2= –1010 NO
Q=0	0–1009–0= –1009 NO	0–1009–1= –1010 NO	0–1009–2= –1011= –3·337
Q= –1	–1–1009–0= –1010 NO	–1–1009–1= –1011= –3·337	–1–1009–2= –1012 NO

Insomma posso scegliere Q tra i neri ed ottengo sempre a destra un termine multiplo di 3, quindi semplificando:

$$1009 \cdot k + tx = -z + (336 \; oppure \; 337)$$ [***]

Essendo 1009 e X primi tra loro, posso scrivere che esistono k e t non nulli tali che:

$$1009 \cdot k + tx = 1$$

Moltiplicando ambo i membri per il termine noto della precedente equazione [***], non nullo (se è nullo stiamo considerando proprio –1009 come X), si dimostra la che su può ottenere un numero Nero come somma di numeri Verdi, assurdo.

N.B. $Q - 1009 - x = 0$ da cui $X = Q - 1009$ scegliendo Q come 0… dimostriamo il LEMMA.

Caso in cui fosse $x \in B$ si ha un assurdo, infatti dimostro che la somma di due numeri blu è pari a Q= –1,0,1 che per [7] e [9] è certamente nera:

$$-1009 \cdot (3k + 1) + x(3t + 1) = Q$$

$$-1009 \cdot 3k - 1009 + 3tx + x = Q$$

da cui considerando –k=k si ha

$$1009 \cdot 3k + 3tx = Q + 1009 - 3z - P$$

	P=0	P=1	P=2
Q=1	1+1009–0=1010 NO	1+1009–1=1009 NO	1+1009 –2 = 1008 = 3·336
Q=0	0+1009–0=1009 NO	0+1009–1 = 1008 = 3·336	0+1009–2=1007 NO
Q= –1	–1+1009–0 = 1008 = 3·336	–1+1009–1=1007 NO	–1+1009–2=1006 NO

Anche in questo caso posso trovare dei fattori k e t che, come prima, portano la somma di due numeri Blu pari a un numero nero con il teorema del MCD(1009,X)=1, assurdo. c.v.d

SOLUZIONE: essendo 2008 primo con 1009, 2008 è un anno NERO.

Ma non è vero! Chiedo la riformulazione del problema (o la ricolorazione), perché anche se non so cosa sia successo nel 1009, nel 2008 è nata mia figlia Sara e NON può essere un anno nero!

Beh, la motivazione ci sembra più che ragionevole! Del resto sul 1009 abbiamo avuto le risposte più diverse. ***Cid*** ci scrive:

> Cosa è successo nel 1009? Da Wikipedia qualche risposta la potrei trarre: Muore Papa Giovanni XIII e viene eletto Papa Sergio IV, muore San Bruno di Querfurt, il califfo egiziano Al Hakim fa radere al suolo la Chiesa del Santo Sepolcro a Gerusalemme, ecc... Ma credo che gli avvenimenti più importanti non siano quelli riportati sui libri di storia, bensì quelli che avvengono all'interno di ogni famiglia.

Non possiamo che essere d'accordo, e così infatti chiosa ***Gnugnu***:

> Volendo restare nell'ambito scientifico ed al calendario giuliano, gli avvenimenti importanti che riesco ad ipotizzare riguardano solo eventi epocali nella vita di numerosi antenati di Rudy.
>
> Trovo più interessante ricordare che, per il meno arbitrario calendario persiano, all'inizio del 1009, il sessantaseienne Galileo otteneva la prima approvazione del suo Dialogo e si accingeva, forse solo in parte cosciente dei rischi cui andava incontro, ad arrabattarsi per l'imprimatur.
>
> Otto mesi dopo moriva Keplero.
>
> L'almanacco di quell'anno è conservato nei locali del circolo 'Partigiani di Copernico'.

E ***Alberto R***.:

> La risposta è semplicissima. Poiché non si pongono limitazioni all'evento da citare, qualunque fatto accaduto in quell'anno risponde alla domanda. Allora vi dico che nell'anno 1009 il sole è sorto più di 100 volte.

Secondo noi il Capo non si sarebbe mai aspettato delle risposte così belle...

5.1.2 Quasi un Summer Contest

Il Capo l'ha fatto ancora una volta: il testo del problema era tanto criptico che ognuno l'ha interpretato a modo suo. Vorremmo farvi vedere tutte, ma proprio tutte le versioni che ci sono giunte, ma non ce la facciamo, siamo già in ritardo. Vi diamo però i nomi – o meglio gli allonimi – dei fantastici solutori: ***Br1***, ***FrancoZ***, ***Cid***, ***Millenium Bug***, ***Gnugnu***, ***Franco57*** e ***Diego***. Vediamo il testo:

> *Si tratta di un gioco a squadre, ogni squadra composta da diciotto ragazzini. Sfruttando il fatto che all'interno di ogni gruppo i diciotto nomi sono tutti diversi, a ogni squadra verrà presentata una fila di diciotto scatole numerate, ognuna delle quali conterrà il nome di uno dei componenti della squadra stessa. Naturalmente, nessuno 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 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, si può parlare prima del gioco, ma quando si comincia silenzio totale ed è vietato lasciare segni sulle scatole o sui biglietti.*
>
> *Riuscite a trovare una strategia di gioco con una probabilità decente di riuscita?*

Non abbiamo scuse, qui, sentite cosa scrive ***Br1***:

> Questo mese, se non ho mal interpretato, i due quesiti proposti prevedevano non tanto il risolverli, ma piuttosto nell'inventarsi il complemento del testo con le informazioni mancanti su RM129, Cap. 2…

Ciò ovviamente se non mi è sfuggito qualcosa di fondamentale; oppure forse il mio file 129.pdf è stato infestato da una versione informatica del verme disicio[14] o da qualche altro simile parassita.

Vediamo le scatole: per agevolare la descrizione, supponiamo che i ragazzini si chiamino **Uno**, **Due**, …, **Diciotto** (di cognome, neh…). Quando il primo di essi (**Uno**) si presenta davanti al tavolo con le scatole schierate, egli non ha nessunissima informazione sul loro contenuto per cui, qualunque sia il gruppo di 9 di esse che decide di aprire, e qualunque sia l'ordine di apertura, le sue probabilità di trovare il proprio (cog)nome non cambiano.

Se suddividiamo le scatole nei due sottoinsiemi *{scatole aperte da **Uno**}* e *{scatole non aperte da **Uno**}*, poiché gli elementi contenuti in essi sono 9 per entrambe, e siccome il biglietto col nome **Uno** non ha nessuna ragione preferenziale per trovarsi in uno particolare dei due sottoinsiemi, le probabilità che ha **Uno** di sopravvivere sono del 50%.

Quindi, inevitabilmente, qualunque sia la strategia adottata, in almeno la metà dei casi la squadra è destinata a soccombere… Vediamo cosa si può fare nell'altra metà; mi pare che l'unico modo di comunicare qualcosa ai compagni da parte di **Uno** e dei successivi contendenti sia l'ordine sequenziale con il quale le scatole vengono aperte, per cui è su questo che ci si baserà.

☺☻☺ Parte facoltativa ☻☺☻

Il problema mi sembra troppo facile… Ci deve essere qualche vincolo che mi è sfuggito, pur avendo letto e riletto 18 volte il testo del quesito… Immagino possa consistere nel fatto che i ragazzini siano obbligati a presentarsi al tavolo in un ordine prestabilito cioè che, dopo **Uno**, non possa andare **Undici**, bensì necessariamente **Due**, e poi **Tre**, **Quattro**… ordinatamente fino a **Diciotto**…

Se così non fosse (il testo del quesito non lo dice, almeno mi pare) si potrebbe ad esempio adottare la seguente strategia:

- **Uno** apre le scatole N°1 e N°2; almeno una di esse contiene necessariamente un nome diverso dal suo
- **Uno**, scegliendo il primo[15] di essi se entrambe i nomi sono diversi dal suo, identifica mentalmente due scatole che *codificano* quel nome, avendo ad esempio concordato coi compagni ciò che segue:

Scatole		Nome codificato	Scatole		Nome codificato	Scatole		Nome codificato
5	6	Due	6	8	Otto	8	5	Quattordici
5	7	Tre	6	9	Nove	8	6	Quindici
5	8	Quattro	7	5	Dieci	8	7	Sedici
5	9	Cinque	7	6	Undici	8	9	Diciassette
6	5	Sei	7	8	Dodici	9	5	Diciotto
6	7	Sette	7	9	Tredici			

[14] E qui ci viene segnalato un link esplicativo: http://www.scudit.net/mdverme.htm

[15] Consentire ad **Uno** di scegliere il secondo nome complicherebbe un po' le cose, potendo portare a casi particolari… Ma non è molto interessante…

- **Uno** poi apre, poniamo, in sequenza le scatole N°7 e N°6: ciò indica ad **Undici** (ed a tutti gli altri) che il suo nome è presente in una delle prime due scatole
- **Uno** apre quindi altre 5 scatole a casaccio, nemmeno guardando cosa contengano
- **Uno** va a sedersi, e **Undici** prende il suo posto al tavolo delle scatole
- **Undici** apre le prime due scatole, e trova il proprio nome; poi apre la terza, e memorizza la codifica del primo dei nomi diverso dal proprio contenuto nelle scatole N°2 e N°3, e procede poi come aveva fatto **Uno**, utilizzando stavolta le scatole dalla N°6 alla N°10 per la codifica…
- Gli altri procedono in sequenza, come sopra…

Ecco, visto che era facile? Se la sequenza con cui i partecipanti si succedono al tavolo fosse davvero libera, ci sarebbe addirittura una strategia tale da mantenere il 50% anche se ai 17 osservatori fosse consentito di assistere *esclusivamente* all'apertura delle ultime due scatole! Infatti **Uno** (e gli altri dopo di lui) potrebbe aprire le prime 7 scatole nascosto alla vista da una tenda, e quindi mostrare pubblicamente la sola apertura delle ultime due, che fornirebbero la *codifica* del nome del successivo partecipante…

☺☻☺ Fine della parte facoltativa ☻☺☻

Quindi, parrebbe che l'unico modo per rendere la vita veramente difficile ai ragazzini sia obbligarli a fornire, *prima* dell'inizio del gioco, la lista ordinata indicante in quale sequenza essi intendono presentarsi al tavolo…

Supponiamo allora che l'ordine di partecipazione prescelto (uno puramente a caso…) sia il seguente:

N	Partecipante	N	Partecipante	N	Partecipante
1°	Uno	7°	Sette	13°	Tredici
2°	Due	8°	Otto	14°	Quattordici
3°	Tre	9°	Nove	15°	Quindici
4°	Quattro	10°	Dieci	16°	Sedici
5°	Cinque	11°	Undici	17°	Diciassette
6°	Sei	12°	Dodici	18°	Diciotto

Ovviamente, **Uno** conserva ancora il 50% di probabilità di *sopravvivenza*… Se *sopravvive*, come può fare ad ottimizzare la strategia di gruppo per quelli che seguono? Facciamo una considerazione preliminare: se si agisce in modo che ad un certo punto del gioco sia noto a tutti l'elenco delle 9 scatole contenenti i nomi **pari** (e di conseguenza l'elenco complementare dei nomi **dispari** nelle rimanenti), anche non sapendo in quale scatola si trovi ogni specifico nome, tutti i concorrenti a partire da quel momento possono aprire le 9 scatole che contengono biglietti con la parità equivalente al loro nome, e condurre la squadra alla vittoria.

Come si vedrà, la strategia di seguito descritta garantisce che dal concorrente **Quattro** in poi le parità dei nomi nelle scatole siano note a tutti; affinché la squadra vinca, occorre allora massimizzare in qualche modo le probabilità di *sopravvivenza* di **Due** e di **Tre**, oltre naturalmente ricostruire gli elenchi di parità.

Quindi possiamo dire che **Uno**, nell'aprire le sue 9 scatole, deve porsi i seguenti obiettivi, in ordine di priorità decrescente:

1. Cercar di sopravvivere egli stesso

2. Fornire a **Due** il massimo di informazioni possibili per massimizzarne le probabilità di *sopravvivenza*
3. Fornire a **Tre** il massimo di informazioni possibili per massimizzarne le probabilità di *sopravvivenza*
4. Rendere nota a tutti la parità dei nomi via via estratti dalle scatole

Ribadendo che Uno non può in nessun modo migliorare il 50% relativo al primo obiettivo, la lista di regolette da seguire per conseguire i suoi altri obiettivi potrebbe essere la seguente.

Dopo aver aperto ciascuna scatola, inclusa la prima, **Uno** ne conosce il contenuto, che è un nome-numero; per selezionare la successiva scatola da aprire, **Uno** si comporta come segue (e come è noto a tutti gli altri 17 compagni che osservano in silenzio con attenzione estrema, e che prendono appunti scritti, se consentito, mentali altrimenti):

- Se il nome-numero estratto è **dispari** ma diverso da **Uno** e da **Tre**, viene selezionata la scatola immediatamente successiva come prossima da aprirsi
- Se il nome-numero estratto è **pari** ma diverso da **Due**, viene selezionata la scatola due posizioni in avanti come prossima da aprirsi
- Se il nome-numero estratto è **Tre**, viene selezionata la scatola **tre** posizioni in avanti come prossima da aprirsi
- Se il nome-numero estratto è **Due**, viene selezionata la scatola **quattro** posizioni in avanti come prossima da aprirsi
- Se il nome-numero estratto è **Uno**, viene selezionata la scatola **cinque** posizioni in avanti come prossima da aprirsi

Può capitare, quando **Uno** apre le sue ultime scatole, che il criterio di selezione della successiva porti oltre la diciottesima; in tal caso, Uno ricomincia dalla prima, *saltando* nel conteggio delle posizioni le scatole già aperte. È indifferente quale sia la prima scatola che **Uno** apre; per semplicità assumiamo che sia la N°1.

Come esempio del metodo, e supponendo che i nomi trovati via via da **Uno** nelle sue 9 scatole siano **Undici**, **Sei**, **Diciassette**, **Uno**, **Tre**, **Quattordici**, **Otto**, **Due** e **Dodici**, le scatole verranno scelte come dalle figure che seguono, dove con i numeri in **blu** sono indicate quelle via via aperte, in **rosso** quelle già considerate in precedenza e che vanno eventualmente saltate nei conteggi delle posizioni:

Manca, nelle figure qui sopra, quella relativa al **Dodici** finale, estratto da **Uno** nella scatola N°9… Uno non ha modo di informare i compagni circa la sua nona ed ultima estrazione, per cui questa potenziale segnalazione viene persa; *ma non sempre*, parlando adesso in generale e non più dell'esempio qui sopra. Poiché Uno segnala in modo esplicito (saltando 5 posizioni) il fatto di aver pescato il proprio nome-numero, se questa segnalazione non ha luogo nelle prime 8 aperture di scatole, e se ancora dopo la nona scatola **Uno** torna tutto felice e saltellante al suo posto per lasciare il turno a **Due**, allora ciò vuol dire che proprio all'ultima chance **Uno** si è salvato… E con sé la squadra… Quindi, in un caso su 9[16] di quelli in cui **Uno** sopravvive, **Due** (e tutti gli altri) sanno anche che la nona scatola aperta da **Uno** conteneva il suo nome-numero…

Nella metà dei casi in cui **Uno** *sopravvive*, che informazioni ha poi **Due** in base al comportamento di **Uno** descritto sopra? Vi sono più casi; vediamo quali:

1) **Uno** ha trovato il nome-numero **Due** in una delle sue prime 8 scatole
2) **Uno** *non* ha trovato il nome-numero **Due** in una delle sue prime 8 scatole; in questo caso, vi sono due sottocasi:
   a) **Uno** ha trovato il proprio nome-numero in una delle prime 8 scatole
   b) **Uno** ha trovato il proprio nome-numero nella nona ed ultima scatola

Nel caso 1), per **Due** la vita è facile; quando tocca a lui, apre la scatola indicata esplicitamente da **Uno** in cui è certo di trovare il proprio nome-numero, e poi ne apre altre 8, partendo da una a casaccio fra quelle non ispezionate da **Uno** e seguendo regole *simili* a quelle di **Uno**, per comunicare a **Tre** ed agli altri che seguono tutte le informazioni possibili sulla parità dei vari nomi-numeri contenuti nelle scatole (ed a **Tre** in particolare se casomai spunta fuori il suo nome). Nel

[16] Assunto che **Uno** trovi il proprio nome nelle sue 9 scatole, è statisticamente equivalente che lo peschi in una qualsiasi di esse; quindi la probabilità che lo becchi proprio nell'ultima è 1/9.

procedere, **Due** fa tesoro delle scatole aperte da **Uno**, e quindi salta nelle sue codifiche quelle già note.

Ma attenzione! **Due** non può usare esattamente le stesse regole di **Uno**… Verso la fine delle sue aperture di scatole, **Due** può infatti trovarsi in una situazione analoga a quella che segue:

In tal caso, o in casi simili, **Due** non può *codificare* univocamente il fatto di aver eventualmente trovato il proprio nome-numero nella scatola N°10 (come invece poteva sempre fare **Uno** in precedenza), il che comporterebbe l'aprire poi la scatola N°16 (cioè **quattro** posizioni dopo la 10, saltando le scatole con i numeri rossi, quindi N°16, N°17, N°18, N°16…). Anche l'aver eventualmente trovato un qualsiasi altro nome-numero **dispari** nella scatola N°10 porterebbe comunque alla scatola N°16, generando ambiguità… Allora le regole per **Due** sono un po' diverse da quelle di **Uno**: se e quando **Due** trova il proprio nome-numero, non lo codifica come avrebbe fatto **Uno** (quindi quattro posizioni più avanti), ma si limita ad indicare che il numero è pari, scegliendo la scatola due posizioni dopo per la successiva estrazione, cioè la scatola N°17 nell'esempio… In fondo, a **Tre** non interessa affatto dove sia precisamente la scatola di **Due**; le regole istituite per **Uno** servivano massimamente a garantire la *sopravvivenza* di **Due**; assunto che questi *sopravviva*, per **Tre** le regole di **Uno** relative a **Due** sono inessenziali… Inoltre, **Due** non ha la necessità di dover segnalare la estrazione del nome-numero **Uno**: quella scatola è già nota a tutti, e non vi è nessun bisogno di aprirla. Quindi le 5 regolette viste sopra per **Uno** si trasformano per **Due** nelle seguenti 3:

- Se il nome-numero estratto è **dispari** ma diverso da **Tre**, viene selezionata la scatola immediatamente successiva come prossima da aprirsi
- Se il nome-numero estratto è **pari**, viene selezionata la scatola **due** posizioni in avanti come prossima da aprirsi
- Se il nome-numero estratto è **Tre**, viene selezionata la scatola **tre** posizioni in avanti come prossima da aprirsi

La terza regola resta in vigore fin quando non restano almeno 4 scatole ancora incognite; dopo di ciò, **Due** può trovarsi in una situazione simile alla seguente:

In tal caso, **Due** non può discriminare l'estrazione del biglietto col nome-numero **Tre** da quella di un qualsiasi altro **dispari**, per cui si limiterà ad applicare le prime due regole.

Infine, se e quando mancano solo due scatole incognite, come qui sotto illustrato:

Due non può far altro che aprire l'ultima dopo la penultima, e non potrà quindi fornire nessuna informazione a **Tre** con le sue ultime mosse.

Nel sottocaso 2a), **Due** sa con certezza che il proprio nome non si trova nelle prime 8 scatole aperte da **Uno**; apre quindi 9 delle 10 rimanenti scatole, sperando di non essere particolarmente iellato, e sempre seguendo le stesse regole di cui sopra, per tenere ben informati Tre e gli altri.

Nel sottocaso 2b), **Due** sa con certezza che il proprio nome si trova in una delle 9 scatole non aperte da **Uno**; le apre allora tutte, ancora una volta trasferendo le debite informazioni agli altri nel solito modo.

Se anche **Due** sopravvive, **Tre** ha poi informazioni su almeno 15 scatole delle 18: o il suo nome è presente in una di esse (e lui sa esattamente quale sia), oppure esso si trova in una delle ultime tre. Apre la propria se nota, poi (o comunque) procede con quelle ancora incognite, fornendo così a **Quattro** ed agli altri le ultime informazioni di parità che mancavano… Nell'aprire la penultima delle scatole incognite, **Tre** ha davanti a sé una sola ulteriore scatola incognita: come può codificare la parità della penultima? Beh, ad esempio apre la scatola con il nome-numero **Uno** (che conosce con certezza) se dispari, e l'ultima scatola incognita se pari. L'ultima scatola incognita diventa contestualmente nota: delle altre 17 si sa ormai che sono 8 pari e 9 dispari, o viceversa…

Dopo di **Tre**, gli altri conoscono la parità di tutte le scatole, e la vittoria è certa…

In sintesi, una squadra che adottasse la strategia descritta vincerebbe se:

- (**Uno** *sopravvive*) AND (**Uno** *trova* il nome **Due** in una qualsiasi delle sue prime 8 scatole), OR:
- (**Uno** *sopravvive*) AND (**Uno** *non trova* il nome **Due** in nessuna delle sue prime 8 scatole) AND (**Due** *trova* il proprio nome in una qualsiasi delle sue 9 scatole)

Definiamo adesso le seguenti probabilità:

- P_1 = probabilità che sia vero che (**Uno** *sopravvive*)
- P_{1A} = probabilità che sia vero che (**Uno** *trova* il nome **Due** in una qualsiasi delle sue prime 8 scatole)
- P_{1B} = probabilità che sia vero che (**Uno** *non trova* il nome **Due** in nessuna delle sue prime 8 scatole)
- P_2 = probabilità che sia vero che (**Due** *trova* il proprio nome in una qualsiasi delle sue 9 scatole)

La probabilità complessiva di *vittoria* sarà allora:

$$1)\ P_{Tot} = P_1 \cdot \left(P_{1A} + P_{1B} \cdot P_2\right)$$

Sappiamo già che $P_1 = 1/2$; occorre calcolare le restanti tre probabilità…

Per P_{1A} e P_{1B}, possiamo immaginare di suddividere le scatole nei due sottoinsiemi *{prime 8 scatole aperte da **Uno**}* e *{le altre 10 scatole}*; il nome **Due** può trovarsi indifferentemente in una qualsiasi delle 18 scatole: questa si troverà in 8 casi su 18 nel primo sottoinsieme, nei restanti 10 nel secondo. Quindi:

$$2)\ P_{1A} = 8/18 = 4/9 \quad P_{1B} = 10/18 = 5/9$$

Con P_2 le cose sono un po' più complicate: prima cosa, il calcolo ha senso solo se **Uno** *non* ha trovato il nome **Due** nelle prime 8 scatole, per cui **Due** deve cercarselo nelle rimanenti. Le rimanenti possono essere 10, se **Uno** ha trovato il proprio nome in una delle prime 8 scatole (8 casi su 9), oppure 9, se **Uno** si è salvato in extremis con la sua ultima scatola (1 caso su 9). Nel primo caso, se suddividiamo le 10 scatole apribili da Due nei sottoinsiemi *{le 9 scatole che **Due** apre}* e *{l'ultima scatola, che **Due** non apre}*, il nome **Due** può trovarsi 9 volte su 10 nel primo sottoinsieme ed una sola volta su 10 nell'altro. Nel secondo caso, **Due** apre le 9 scatole non toccate da Uno, ed ha la certezza di trovarvi il proprio nome. Quindi:

$$3)\ P_2 = \frac{8}{9}\cdot\frac{9}{10} + \frac{1}{9} = \frac{4}{5} + \frac{1}{9} = \frac{41}{45}$$

In definitiva:

4) $P_{Tot} = P_1 \cdot \left(P_{1A} + P_{1B} \cdot P_2\right) = \frac{1}{2} \cdot \left(\frac{4}{9} + \frac{5}{9} \cdot \frac{41}{45}\right) = \frac{1}{2} \cdot \frac{77}{81} = 0{,}4753+$

Quindi, l'imporre un ordine prestabilito di partecipazione ai ragazzini fa calare le probabilità complessive di successo, rispetto al caso di ordine sparso, appena del 5%… In sostanza, se **Uno** sopravvive è quasi fatta…

L'attento lettore si sarà accorto che nel calcolo delle probabilità non appare nulla di relativo a **Tre**… Eppure, sin da quando si sono elencati gli obiettivi di **Uno** (e di **Due**), **Tre** appariva in qualche modo in essi… La ragione sta nel fatto di aver introdotto la regola in base alla quale **Uno** e **Due** segnalano la posizione del nome-numero di **Tre** (se lo trovano); il farlo (o anche il non farlo) garantisce a **Tre** di avere la certezza di *sopravvivere*, cosa che potrebbe non avvenire se **Uno** e **Due** non agissero in tal modo. Supponendo infatti che **Uno** e **Due** non debbano indicare il fatto di aver trovato **Tre** in una scatola qualsiasi, potrebbe capitare il caso che segue: **Uno** e **Due**, nel complesso, producono informazioni su 16 scatole, di cui 8 pari ed 8 dispari. **Tre** si troverebbe davanti ad 8 scatole sicuramente dispari, più 2 incognite… Vi sarebbe per lui una probabilità su 10 di fallire… Invece, il segnalare esplicitamente la presenza del **Tre** nelle scatole aperte da **Uno** e **Due** rimuove il problema, ed essendo certo che **Tre** *sopravvive* (ammesso che ciò capiti per **Uno** e **Due**), rende inutile far calcoli probabilistici su di esso.

FrancoZ decide di poter muovere le scatole:

Come al solito le spiegazioni sono lacunose ma, sfruttando le lacune, non è poi così difficile trovare una strategia che consenta di raggiungere una probabilità di vittoria "dignitosa".

In particolare non ho trovato scritto da nessuna parte che le scatole con i foglietti dei nomi non possano essere spostate e quindi approfitterò senza ritegno di quest'opportunità.

Intanto stabiliamo che i bambini giochino in ordine alfabetico e facciamo cominciare il primo (Antonio).

Antonio apre le prime 9 scatole della fila. Se trova quella col suo nome la mette in fondo alla fila, le restanti 8 le lascia ai primi otto posti della fila ma mettendo al primo posto (se l'ha trovata) la scatola con il nome del prossimo giocatore.

Ammesso che Antonio non sia già uscito sconfitto (nel qual caso è inutile continuare a perdere tempo con questo stupido gioco), tocca adesso alla seconda della lista (Beatrice) che apre la prima scatola della fila e poi altre 8 a partire dalla nona.

Le sue probabilità di successo sono elevate in quanto è sicuro che il suo nome non possa essere nelle scatole fra la seconda e l'ottava posizione (già "cernite" da Antonio) e neppure può essere in diciottesima posizione (c'è la scatola col nome Antonio).

L'unica possibilità di insuccesso è che il foglietto col nome Beatrice si trovi nella diciassettesima posizione.

Comunque, se Beatrice non perde, mette la scatola col suo nome in fondo alla fila (quella col nome Antonio "scala" una posizione indietro") e le altre 8 che ha aperto le sistema nelle prime 8 posizioni della fila riservando il primo posto a quella (se l'ha trovata) contenente il nome del successivo giocatore.

La mano passa quindi a Chiara che apre anche lei la prima scatola e poi altre 8 a partire dalla nona.

Sicuramente troverà quella con il suo nome in quanto non è possibile che sia in quelle fra la seconda e l'ottava posizione (cernite da Beatrice) ed neanche nella diciassettesima o diciottesima (che contengono i foglietti con i nomi Antonio e Beatrice).

Anche Chiara mette la scatola col suo nome in fondo alla fila (quelle di Antonio e Beatrice scalano una posizione indietro) e le altre 8 nelle prime 8 posizioni riservando la prima posizione a quella contenente il nome del successivo giocatore (se l'ha trovata).

Tutti i giocatori successivi giocano allo stesso modo, aprendo la prima scatola ed altre otto a partire dal fondo della fila (saltando quelle che sicuramente contengono i nomi dei compagni che hanno già giocato) e poi risistemandole come spiegato precedentemente.

Vediamo quindi da calcolare che probabilità di vittoria ha in tutto la squadra sulla base delle posizioni di partenza delle scatole: la squadra perde se la scatola contenente il nome Antonio è in una posizione fra la 10 e la 18 – OR – la squadra perde se la scatola contenente il nome Beatrice è in posizione 18. È facile calcolare che la probabilità di vittoria è (9·16)/(17·18) = 144/306 = 47,06% circa. È maggiore di uno su quattro e quindi, almeno per me, è già un buon risultato.

Diego, amico di ***Franco57***, propone una soluzione "furbacchiotta".

Visto che nel testo del quesito non è scritto esplicitamente che le scatole non possano essere ricollocate nella fila, ma solo che i ragazzi non possono né parlare né scrivere, a parte il primo ragazzo che ha il 50% di probabilità di trovare il proprio nome, tutti gli altri potrebbero sapere quale insieme di 9 scatole guardare, con la sicurezza di trovare il proprio nome. Ecco come.

I ragazzi stabiliscono un ordine tra loro, ad esempio quello alfabetico del nome. Il primo apre le prime 9 scatole, quindi se ha trovato il proprio nome sa con sicurezza se il secondo ragazzo si trova nel primo insieme di 9 scatole o nel secondo. Per comunicarlo al secondo ragazzo, senza variare i due insiemi, basta ad esempio che permuti eventualmente le prime due scatole: se i numeri sono in ordine sarà il segnale che il secondo deve cercare nel primo insieme, altrimenti dovrà cercare nel secondo. Lo stesso farà il secondo ragazzo per informare il terzo e così via.

La soluzione che invece avevo tentato io non prevede alcun passaggio di informazione, ma non sono riuscito a trovare un metodo dimostrato ottimale per il gruppo, solo un metodo che minimizza ogni volta la probabilità di perdere (e c'è una bella differenza!).

Comunque il metodo prevede anche in questo caso di dividere le scatole in due gruppi e di far scegliere ai ragazzi dispari sempre il primo gruppo e ai pari sempre il secondo gruppo. In realtà si può vedere l'ordine di scelta dell'insieme di scatole non cambia mai la probabilità per il gruppo, probabilità che però sarebbe un tantino lontana dall'obiettivo di una su quattro, infatti varrebbe 1 / C(18,9) = 1 / 46620. Anche per questo non ho inviato i dettagli.

Non resistiamo a pubblicare anche l'*incipit* di ***Gnugnu***:

L'impressione ad una prima lettura è quella di un problema fuori posto, copiato da un test di ingresso ad un partito politico.

Se le regole del gioco vengono rigorosamente rispettate (non sarebbe difficile, basterebbe, ad esempio, lasciare i fanciulli al loro posto e far aprire dal giudice di gara le scatole indicate), la probabilità di vittoria, è molto piccola poco più di 2^(–18), visto che, dal secondo giocatore in poi, è possibile usare l'informazione aggiunta: 'tutti quelli che mi hanno preceduto hanno trovato il loro nome'. Anche nel caso in cui l'organizzazione, per aumentare le possibilità di vittoria, rendesse

> noto il numero della scatola in cui si trova il nome scovato, la probabilità non salirebbe sopra ad 1 su 45.
>
> Chi ha aperto le scatole ha una informazione sufficiente per far scegliere a tutti i suoi compagni un gruppo vincente, ma non può passarla agli altri. Gli basterebbe un bit per dire a chi lo segue se fra i biglietti che ha visto v'era, o meno, il suo nome, ma voglio sperare che 'silenzio totale' voglia dire 'nessun tipo di comunicazione', altrimenti sarebbe il paradiso per i giocatori di tressette delle osterie di fuori porta; quelli che in cambio di un litro di rosso, sapevano, fra una partita e l'altra, cantarti in un coro assolutamente silenzioso, l'ultimo successo del Quartetto Cetra.
>
> Devo supporre, allora, che l'apritore di scatole debba usare, nell'interesse della squadra, ma in proprio, l'informazione acquisita. (...)

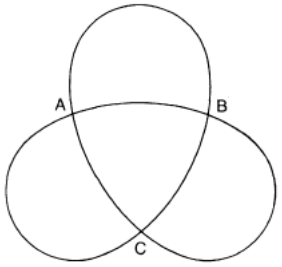
Poi procede a far ordinare i biglietti nelle scatole ai ragazzini, ottenendo anche lui una probabilità di vittoria superiore al 47%.

Qui dobbiamo fermarci, purtroppo. Nel ringraziarvi per i contributi, vi ricordiamo che vi aspettiamo il mese prossimo, continuate a seguirci!

6. 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.

> *Ci sono* **8** *possibili combinazioni, e solo due danno origine a nodi; quindi la probabilità che sia annodata è pari a* $1/4$.

7. Pagina 46

> *Vi avevamo chiesto di tenere la soluzione di ottobre (RM_129). Bene, tenetela a tiro.*

Prima Parte

Assumiamo che il punto M sia sull'arco A_1A_n del cerchio, e indichiamo l'arco MA_1 con α; valgono le uguaglianze:

$$\begin{aligned} MA_2 &= \alpha + \frac{2\pi}{n}, \\ MA_3 &= \alpha + \frac{4\pi}{n}, \\ &\dots, \\ MA_n &= \alpha + \frac{2(n-1)\pi}{n}. \end{aligned}$$

Ma la lunghezza della corda *AB* di un cerchio di raggio *R* è pari a $2R\sin\frac{AB}{2}$, e quindi la somma che vogliamo valutare vale:

$$4R^2\left[\sin^2\frac{a}{2}+\sin^2\left(\frac{a}{2}+\frac{\pi}{n}\right)+\sin^2\left(\frac{a}{2}+\frac{2\pi}{n}\right)+\ldots+\sin^2\left(\frac{a}{2}+\frac{(n-1)\pi}{n}\right)\right].$$

Ricordando che $\sin^2 x=\frac{1-\cos 2x}{2}$, l'espressione tra parentesi quadre diventa:

$$S=\frac{n}{2}-\left[\cos a+\cos\left(a+\frac{2\pi}{n}\right)+\cos\left(a+\frac{4\pi}{n}\right)+\ldots+\cos\left(a+\frac{2(n-1)\pi}{n}\right)\right].$$

Ma, dall'identità vista il mese scorso[17], abbiamo:

$$\cos a+\cos\left(a+\frac{2\pi}{n}\right)+\ldots+\cos\left[a+\frac{2(n-1)\pi}{n}\right]n=\frac{\sin\pi\cos\left[a+\frac{(n-1)\pi}{n}\right]}{\sin\frac{\pi}{n}}=0.$$

Quindi $S=\frac{n}{2}$, da cui segue l'asserzione del problema.

[17] Come dicevamo, RM129, Ottobre 2009: Bungee Jumper (e Pagina 46).

8. Paraphernalia Mathematica

8.1 Non ho capito… [002]: Il "Club delle Due Chiavi"

Bene, vogliamo sperare che dato il pezzo del mese scorso, abbiate ormai prosciugato il conto corrente del vostro capo. Pensiamo ora a come tenerci quei soldi, magari facendoli fruttare.

Come diceva il Gordon, uno dei problemi di Alice (ossia di chi parla) è che deve spiegare come decifrare il messaggio, ossia deve riuscire a trasmettere la chiave: questo, nei secoli, è sempre stato un guaio, tanto da dare origine ad un famoso problema irresolubile[18].

La soluzione è il classico Uovo di Colombo: un qualchecosa, fornito dal ricevente, in grado di *cifrare* il messaggio, ma che sia completamente inutile per *decifrarlo*: cerchiamo di cavarcela con un esempio, usando i soliti Alice, Bob e Eva[19]. Alice manda il messaggio a Bob, e Eva ascolta (non autorizzata).

Il trucco sta nel fatto che Alice e Bob (complichiamoci la vita: anche Eva) fanno parte del "*Club delle Due Chiavi*": ogni membro di questo club ha, giustappunto, due chiavi (numeriche): una è strillata ai quattro venti (nel senso che la conoscono tutti gli altri membri del club), l'altra è tenuta rigorosamente segreta dal socio del club: scopo di questo pezzo è il dimostrare che due qualsiasi membri del Club possono risolvere *tutti* i problemi che nascono quando si mandano messaggi cifrati; per dimostrarlo, vi chiediamo (contrariamente alla Regina Bianca di Carroll, in grado di credere sei cose impossibili prima di colazione) di credere all'esistenza delle *funzioni trappola*; tranquilli, prima della fine ne vedremo almeno due.

Una *funzione trappola* è una funzione:

1. facile da calcolare se avete le variabili di ingresso,
2. facile da calcolare all'inverso se avete una particolare variabile,
3. praticamente impossibile negli altri casi.

Pessima definizione. Caviamocela con qualche definizione cabalistica, usando le Due Chiavi del Club: in sostanza, nota (a tutto il mondo) la funzione, se cifrate con la *Chiave_1*, potete decifrare *solo con la corrispondente Chiave_2*, e la conoscenza della chiave di cifratura (la *Chiave_1*) non vi aiuta nella decifrazione, per quella è necessaria la

---

[18] Due comandanti hanno portato le loro truppe rispettivamente ad est e ad ovest del comune nemico; se attaccano separatamente saranno sconfitti, se attaccheranno in contemporanea vinceranno. Il comandante ad Est manda un messaggio con una staffetta al comandante ad Ovest: "Attaccheremo all'alba, se mi confermate la ricezione del messaggio". Il comandante ad Ovest riceve il messaggio e rimanda indietro la staffetta con il seguente messaggio: "Confermo la ricezione del messaggio di attacco. Confermate la ricezione di questo messaggio per essere sicuro che attaccherete contemporaneamente a me". E, quando questo secondo messaggio arriva al comandante ad Est, questo scrive… E avanti così. Irresolubile.

Ha risposta, invece, un aneddoto simile attribuito a Coxeter: Richiesto di scrivere un articolo per una rivista francese (evidentemente in francese), chiude l'articolo con la seguente sequenza di note:

1. Sono debitore al Professor Bourbaki per la traduzione dell'articolo.
2. Sono debitore al professor Bourbaki per la traduzione della nota precedente
3. Sono debitore al professor Bourbaki per la traduzione della nota precedente

Secondo voi, per quante note è andata avanti la cosa?

Risposta di Coxeter: "Bourbaki ha tradotto sino alla seconda nota inclusa: non conosco il francese, ma so *copiarlo*, e la terza nota l'ho scritta io copiando la seconda".

[19] Non ci ricordiamo se ne abbiamo parlato, ma è la cattiva della crittografia: il nome (inglese, quindi "Eve") deriva da "EaVErsdropper". Insomma, è quella persona che ascolta e cerca di capire cosa si dicono Alice e Bob.

Chiave_2. Non solo, ma la cosa è reversibile: se cifrate con la *Chiave_2*, potete decifrare solo usando la *Chiave_1*.

Siamo sicuri che a questo punto non capite più niente, quindi proviamo a mettere un po' di casi a titolo di esempio: abbiamo tre soci del Cd2C, Alice, Bob e Eva: trovate in tabella i simboli che useremo per le loro chiavi: la prima colonna (*Chiave Pubblica*), come si dice volgarmente la conoscono cani e porci, e tutti sanno a chi appartiene.

	Chiave Pubblica	Chiave Privata
Alice	*Pub_A*	*Pri_A*
Bob	*Pub_B*	*Pri_B*
Eva	*Pub_E*	*Pri_E*

Cominciamo con il caso più semplice: Alice vuole scrivere a Bob senza che Eva capisca cosa si dicono. In questo caso prende *Pub_B*, la usa come chiave nella funzione trappola per cifrare il messaggio e manda il tutto a Bob: quest'ultimo decifra facilmente il tutto usando *Pri_B*; non solo, ma Eva non capisce niente, in quanto le sue chiavi non servono assolutamente a nulla per decifrare il messaggio di Alice.

Ora, continuate a credere all'esistenza della funzione trappola: questo aggeggio risolve un mucchio di problemi, quindi vale la pena. Prima, però, inventiamoci qualche notazione.

$$F(K,T)=C$$
$$F\left(K^{-1}C\right)=T$$

Questi aggeggi significano semplicemente che ho una funzione F (uguale in entrambi i casi) che grazie a una chiave K è in grado di trasformare il testo in chiaro T in un testo cifrato C e che esiste una chiave K^{-1} che utilizza la stessa funzione per trasformare il testo cifrato C nel testo chiaro K. Ossia, secondo la nostra pittoresca descrizione del Club, K e K^{-1} sono le due chiavi del socio; vediamo come usarle in qualche caso particolare.

Possiamo, come abbiamo visto, inviare un messaggio decrittabile solo dal destinatario: Alice cifra secondo la chiave pubblica di Bob il suo messaggio e lo rende pubblico (complichiamoci la vita, senza dire a nessuno che il messaggio è per Bob)

$$F(Pub_B,T_A)=C$$

Quando Bob e Eva ricevono il messaggio, ciascuno dei due cerca di tradurlo con la propria chiave privata:

$$F(Pri_B,C)=T_A$$
$$F(Pri_E,C)=????$$

Insomma, *solo la chiave privata di Bob riesce a dare un senso al messaggio*.

Se avete capito tutto, a questo punto dovreste ricordarvi che, come diceva Gordon, una delle attività preferite della Polizia Segreta e dell'Ufficio delle Imposte "*… è di telefonare ad Alice sostenendo di essere Bob*". E qui rischia di cascare l'asino: se *chiunque* può cifrare con Pub_A, Alice non avrà mai la certezza che a scrivere sia stato Bob; potrebbe, tranquillamente, essere stata Eva (che, in questo momento, fa da ufficiale di collegamento tra la Polizia Segreta e l'Ufficio delle Imposte).

In realtà la soluzione è semplicissima, tant'è che ve la passiamo in simboli con un minimo di spiegazione: per prima cosa, però, statuiamo il problema per rendere le transazioni comprensibili.

> Bob vuole scrivere ad Alice dimostrando di essere Bob senza che Eva riesca a capire né chi ha scritto né cosa c'è scritto nel messaggio.

1. Bob cifra la propria firma *secondo la propria chiave privata* e la appende al messaggio in chiaro.

2. Bob cifra l'intero messaggio secondo la chiave pubblica di Alice

Insomma, in simboli, se S è la firma:

$$T' = T + F(Pri_B, S)$$
$$C = F(Pub_A, T') = F[Pub_A, T + F(Pri_B, S)]$$

Quando Alice riceve il messaggio, lo decifra con la propria chiave *privata,* ottenendo un testo in chiaro (il messaggio vero e proprio) e una serie di caratteri senza senso al fondo:

$$T' = F(Pri_A, C) = T + F(Pri_B, S).$$

A questo punto, prova a decifrare la parte incomprensibile con *tutte le chiavi pubbliche che conosce*: solo la chiave pubblica di Bob funzionerà, permettendo di leggere la firma in chiaro S, in quanto

$$S' = F(Pub_B, F(Pri_B, S)).$$

Non solo, ma Eva, oltre a non capire il messaggio, *non riuscirà neanche a capire chi lo ha inviato*, in quanto la firma di Bob, anche se leggibile con la chiave pubblica di Bob, fornirà un risultato sensato solo dopo essere passata dalla chiave privata di Alice.

A questo punto potete inventarvi voi i casi più balordi di trasmissione di messaggi[20], e provare a risolverli con giochini sulle chiavi pubbliche/private dei partecipanti.

Se, a questo punto, siete sull'orlo del turpiloquio per quanto riguarda il chiedere come **** siano fatte le funzioni trappola, avete perfettamente ragione. Bene vediamone qualcuna.

La definizione comunemente accettata è quella di una funzione facile da calcolare in un verso, ma *molto* difficile da calcolare nel verso opposto; se ci pensate un attimo, vi accorgete subito che questa definizione è strettamente operativa, e infatti non esistono definizioni *teoriche* soddisfacenti di funzione trappola; non solo, ma non esiste neanche un metodo per dimostrare che una data funzione è una FT; sono stai proposti dei *candidati* e, come diremo, qualcuno ha decisamente mancato il bersaglio. La prima che vedremo (e che funziona) ci è particolarmente simpatica, visto che è nota come *Funzione Trappola di Eulero*.

Tanto per cominciare, dovete trasformare il vostro messaggio in un numero M, e vi servono altri due numeri r e s; la richiesta base è che sia:

$$1 < M < r;$$
$$MCD(M, r) = 1.$$

L'idea di base è di elevare M ad una potenza s e poi prendere il resto modulo r, trasmettendolo come messaggio cifrato; prima, però, ripassiamo un concetto, quello della *funzione toziente* di Eulero.

> Si definisce funzione toziente di un numero naturale x il numero $\phi(x)$ dei naturali minori di x che *non* dividono x[21].

Dicevamo che il nostro messaggio cifrato E si ottiene come:

---

[20] Compreso quello che Rudy chiama "Il problema di Aldo": mandate un messaggio attraverso canale sicuro e *in futuro* vorrete provare di essere stato proprio voi ad inviarlo, anche se adesso non volete farlo sapere.

Soluzione: messaggio in chiaro con firma criptata con la vostra chiave pubblica; solo la vostra chiave privata può rendere leggibile la firma. E se vi interessa sapere perché Rudy lo chiama così, il messaggio mandato da Radio Londra (canale sicuro) per l'insurrezione di Torino era "*Aldo dice ventinove più uno*". Non si conosce il nome dello speaker che lo ha pronunciato, ma c'erano tre o quattro persone che sostenevano di averlo detto loro.

[21] Ne abbiamo parlato nel PM di RM067, agosto 2004.

$$E \equiv M^s \pmod{r},\ 1 < E < r. \qquad \texttt{[8.1]}$$

Ora, per capire il metodo, usiamo un numero "sbagliato", ossia prendiamo *r* primo; come vedremo, il trucco sta proprio nello scegliere un *r* che "sembri primo" ma non lo sia, con dei fattori decisamente grossi. Il metodo di decifrazione comunque è lo stesso, semplicemente usando un valore primo si semplificano i conti.

Per prima cosa, troviamo l'inverso *t* modulo $r-1$ dell'esponente di cifratura *s*; questo si ottiene risolvendo in *t* la congruenza:

$$st \equiv 1 \pmod{r-1}. \qquad \texttt{[8.2]}$$

Perché abbia soluzione, occorre che $MCD(s, r-1) = 1$, ossia che *s* e $r-1$ siano primi tra loro. Ricavare *t* è possibile attraverso il Teorema di Eulero: infatti se *s* e $r-1$ sono primi tra loro, vale la relazione (ed ecco che entra in scena il toziente):

$$st \equiv s^{\phi(r-1)} \equiv 1 \pmod{r-1}$$

e, dividendo per *s* entrambi i membri otteniamo

$$t \equiv s^{\phi(r-1)-1} \equiv 1 \pmod{r-1}.$$

Ora, riprendiamo il nostro messaggio cifrato; elevando nella **[8.1]** entrambi i membri alla potenza *t* appena ottenuta, abbiamo:

$$E^t \equiv M^{st} \pmod{r}.$$

Ma abbiamo visto poco sopra che $st \equiv 1 \pmod{r-1}$, quindi si ha che

$$\exists k \in N : st = (r-1)k + 1$$
$$\Rightarrow E^t \equiv M^{(r-1)k+1} \pmod{r}$$

Riutilizzando il teorema di Eulero[22], abbiamo: $M^{r-1} \equiv 1 \pmod{r}$ (sempre per l'assunto che *M* e *r* siano primi tra loro).

E quindi si ricava $E^t \equiv 1^k M^1 = M \pmod{r}$, e il nostro messaggio è stato agilmente decifrato.

Facciamo un esempietto? sia *s*=3 e *r*=17; in questo caso, abbiamo $\phi(r-1) = \phi(16) = 8$, e vediamo che è $MCD(s, \phi(r)) = MCD(3,16) = 1$ (ricordate che il toziente di un primo è pari allo stesso primo decrementato di uno); si vede che in questo caso *t*=11, infatti $st = 3 \cdot 11 = 33 \equiv 1 \pmod{16}$.

Se supponiamo ora *M*=4, otteniamo che il messaggio cifrato vale 13, in quanto:

$$E \equiv M^s = 4^3 = 64 \equiv 13 \pmod{17}.$$

E riotteniamo il messaggio in chiaro elevando *E* all'esponente *t*:

$$E^t = 13^{11} = 13^{10} \cdot 13 = (371 \cdot 293)^2 \cdot 13 \equiv 13^2 \cdot 13 \equiv 4 \pmod{17},$$

che è esattamente il nostro messaggio cifrato.

Insomma, in questo modo non funziona.

[22] In realtà sin quando *r* è primo basterebbe il Teorema di Fermat, ma siccome dopo useremo un *r* composto, tanto vale usarlo sin da subito.

L'errore consiste come dicevamo nell'aver utilizzato per r un valore *primo*; se prendiamo però $r = pq$ (dove p e q sono primi decisamente "grossi") e il nostro esponente di cifratura s è tale che $MCD(s,\phi(r)) = 1$, la cosa funziona decisamente bene.

Infatti, a questo punto Alice pubblica s e r (tenendo ben segreti p e q) e Bob, quando vuole inviarle il messaggio M, non fa altro che elevarlo alla potenza s e spedire il risultato modulo r.

Quando Alice vuole decifrare il messaggio, ha come prima bisogno dell'esponente t, dato dalla

$$st \equiv 1 (\mathrm{mod}\, \phi(r)),$$

che è esattamente la stessa cosa che abbiamo detto in **[8.2]**, solo che qui, non essendo r primo, il toziente dobbiamo esplicitarlo.

Ma Alice conosce il toziente di r! Infatti, se $r = pq$, con p e q primi, si ha:

$$\phi(r) = (p-1)(q-1).$$

A questo punto, il giro è esattamente lo stesso, anche se le formule sembrano più complicate: infatti, da $MCD(s,\phi(r)) = 1$ si ricava $ts \equiv s^{\phi(\phi(r))} \equiv 1 (\mathrm{mod}\, \phi(r))$ e quindi si ha

$$t \equiv s^{\phi(\phi(r))-1} (\mathrm{mod}\, \phi(r))$$

Riepilogando, ad Alice arriva il messaggio $E \equiv M^s (\mathrm{mod}\, r)$: calcoliamo $E^t \equiv M^{st} = M^{\phi(r)k+1} (\mathrm{mod}\, r)$ e, ricordandoci che $M^{\phi(r)} \equiv 1 (\mathrm{mod}\, r)$, abbiamo $E^t \equiv M (\mathrm{mod}\, r)$[23].

Il giochino della firma autenticata ve lo dimostrate da soli, tanto è perfettamente uguale: semplicemente, Alice cifra secondo la propria t e Bob (dopo aver decifrato il messaggio con la propria chiave) decifra la parte incomprensibile usando la chiave pubblica di Alice. Funziona!

Insomma, l'elevamento a potenza in modulo è una buona *Funzione Trappola*. Visto che valeva la pena di crederci? Vi avevamo comunque promesso che ve ne avremmo spiegato qualcuna che *non* funziona: la cosa è piuttosto triste, in quanto il metodo era decisamente semplice: infatti, utilizzava la moltiplicazione (sempre in modulo) al posto dell'elevamento a potenza, il che la rendeva decisamente semplice.

Qui, come Funzione Trappola si utilizzava un vecchio problema, quello dello zaino; tant'è che il metodo è detto dello *Zaino Cifrato*; cominciamo dal problema, versione semplice.

> Avete uno zaino del peso di 23 kilogrammi; contato che avete messo dentro una serie di oggetti scelti da un insieme di sei di pesi 1, 2, 4, 8, 16 e 32 kilogrammi (gli altri li porta il vostro socio), che oggetti state portando?

Problemi di questo tipo sono sempre risolubili con facilità se, mettendo i pesi in successione, ognuno è più grande della somma dei pesi precedenti di almeno una unità: sappiamo che vi piacciono i paroloni, quindi se volete stupire gli amici vi diciamo che questi aggeggi si chiamano *successioni supercrescenti* (a noi sembra più carino di "esponenziale", ma non stiamo a formalizzarci).

[23] Ai più pessimisti tra di voi potrebbe essere venuto il dubbio che in alcuni casi la cosa non funzioni, in particolare se M non è primo rispetto a r; tranquilli, la probabilità che questo si verifichi è dell'ordine di una su 10^n, dove n è il numero delle cifre del più piccolo fattore di r.

Bene, come funziona una cifratura con il problema dello zaino? Tanto per cominciare, supponiamo che il messaggio da cifrare sia *53*, o, in binario, 110101; lo trovate, nella tabella che segue, scritto sulla sinistra dal basso verso l'alto.

Nella zona centrale abbiamo messo la nostra successione supercrescente circondata da un po' di cifre per rendere più complicata la cosa (questi diventano i "pesi" che possiamo mettere nel nostro zaino), e la composizione dello zaino si trova sulla destra; se sommate tutti i valori, ottenete il messaggio "cifrato" che avete al fondo sotto la riga di somma; come vedete, la nostra successione supercrescente dà origine al valore 53 all'interno del messaggio (mal) cifrato.

Messaggio Originale	Zaino (Facile)							Messaggio Cifrato						
1	8	3	0	1	0	5	1	8	3	0	1	0	5	1
0		2	0	2	0	6	1							
1	7	8	0	4	0	9	0	7	8	0	4	0	9	0
0	3	5	0	8	0	4	9							
1	2	4	1	6	0	1	3	2	4	1	6	0	1	3
1	3	3	3	2	0	7	8	3	3	3	2	0	7	8
								2	1	8	5	3	2	3	2

Il primo pensiero è che un oggetto del genere non serve a nulla, dal punto di vista della cifratura; diventa più interessante e "complichiamo" lo zaino, ossia se prendiamo i pesi (con i numeri aggiunti a caso) dello zaino facile e li moltiplichiamo per poi prendere un modulo; se, ad esempio, moltiplicate per $s = 324358647$ e riducete modulo $r = 786053315$, il vostro messaggio cifrato diventa 1832885704, e il messaggio originale è completamente sparito.

Formalizziamo il metodo.

Per prima cosa, prendiamo una successione di pesi a_i; la condizione di supercrescenza si definisce come:

$$a_{i+1} > \sum_{k=1}^{i} a_k \ .$$

Poi prendiamo un modulo *r* e un fattore *s* tale che $MCD(r,s) = 1$. Calcoliamo ora lo zaino difficile b_k e *pubblichiamo i* b_k:

$$b_k \equiv s a_k \pmod{r}.$$

Calcoliamo il *fattore di decifrazione t* tale che

$$st \equiv 1 \pmod{r},$$

e *teniamolo segreto*.

Se il messaggio in binario è $M = \sum_{k=0} m_k 2^k$, lo cifriamo con lo zaino difficile e lo inviamo:

$$E = \sum_{k=0} m_k b_k$$

Il destinatario, che conosce *t*,calcola

$$tE = \sum_{k} m_k t b_k \ .$$

ricordandosi che $tb_k \equiv tsa_k \equiv a_k \pmod{r}$, il Nostro ottiene

$$tE = \sum_k m_k a_k \ ,$$

ossia il messaggio risulta cifrato secondo uno zaino *facile* e si decifra al volo.

Molto carino ma, come dicevamo, purtroppo non funziona, e *proprio per colpa della moltiplicazione*; infatti, il problema dello zaino può essere risolto in modo "veloce" (virgolette d'obbligo: si intende in tempo polinomiale), e quindi il nostro zaino è piuttosto sforacchiato.

Per finire con una nota positiva, tranquilli: quello delle potenze sono trent'anni che cercano di smontarlo, ma nessuno ci è ancora riuscito. Ora, se volete passarci i dati della vostra carta di credito…

Rudy d'Alembert
Alice Riddle
Piotr R. Silverbrahms