I Numeri Primi e la Crittografia

Progetto **Teatro in Matematica** a cura di **Maria Eugenia D'Aquino**
con **Maria Eugenia D'Aquino**, **Vladimir Todisco Grande**
con la partecipazione di **Massimo Loreto**
drammaturgia a cura di **Riccardo Mini**
consulenza matematica del prof.**Alberto Colorni** del Politecnico di Milano
regia di **Valentina Colorni**
video **Ino Lucia**
produzione **PACTA . dei Teatri**

La maggior parte di noi sa che cosa siano i numeri primi, pochi però conoscono la loro storia, le loro applicazioni e soprattutto il loro lato enigmatico. Nello spettacolo vengono mostrati gli aspetti più affascinanti e curiosi di questa famiglia di numeri (considerati a ragione come i mattoni su cui si costruisce tutta la matematica) e le molteplici implicazioni che hanno nella vita di tutti i giorni.

Siamo su un treno speciale, il *Trans Eulero Express*, in un Paese in guerra, le stazioni hanno nomi che sono numeri e solo quelle con numeri primi sono un rifugio sicuro per i passeggeri. Il fatto che non si sappia come siano distribuite le stazioni (come i numeri primi) le rende difficili da trovare da parte degli inseguitori. Questo dà un connotato perfino positivo e salvifico a quella che in realtà è una spina nel fianco di ogni matematico che si occupi di teoria dei numeri.
Un controllore ci accompagna nel viaggio notturno, e un viaggiatore misterioso non vuole rivelare che cosa contenga la valigia dalla quale non si separa mai. I vagoni del treno sono altrettanti momenti di storia della matematica e della crittografia, dalla cifratura di Cesare al metodo RSA (quello che regola il nostro bancomat), basato proprio sull'enigma dei numeri primi.
Fino a quando l'enigma non verrà risolto il treno continuerà a viaggiare nella notte custodendo il segreto, ma forse quel momento non è poi così lontano.
Alla scena del vagone del treno si alterna la scena di un accampamento del nemico, in cui due sentinelle che attendono il passaggio del treno si intrattengono giocando con i numeri primi e approdano a interessanti scoperte, che però le distraggono dalla loro missione: avvertire al passaggio del treno.

Al termine dello spettacolo è previsto un incontro con il pubblico, in cui i protagonisti dello spettacolo e del progetto raccontano e approfondiscono i parallelismi tra linguaggio scientifico e linguaggio teatrale sotto tutti gli aspetti.
Durata 60 min circa.

.
Riassunto degli argomenti matematici dell'incontro → **I Numeri Primi in 8 mosse**

1. *Numeri primi e fattori primi di un numero*
2. *Differenza tra congetture e teoremi*
3. *Le "belle" dimostrazioni (la bellezza in matematica)*
4. *La dimostrazione "per assurdo" : il teorema di Euclide*
5. *Operazioni dirette e operazioni inverse*
6. *Le soluzioni per tentativi ("brute force")*
7. *Crittografia e crittoanalisi*
8. *Chiave pubblica e chiave privata*

.... Nello spettacolo vengono sfiorati tutti quelli che sono gli aspetti più affascinanti e curiosi di questa famiglia di numeri particolari considerati a ragione come i mattoni su cui si costruisce tutta la matematica. Ogni numero naturale (1, 2, 3,...) è infatti esprimibile come prodotto di potenze di numeri primi e questa fattorizzazione è unica e caratteristica solo di quel numero, un po' come la combinazione degli elementi in chimica che può dare origine, una volta fissati elementi e proporzioni, a una e una sola sostanza. I numeri naturali poi, a loro volta, servono a costruire i numeri razionali che servono a costruire i numeri reali, che a loro volta sono alla base dei numeri complessi (per spingerci, volendo, anche ai quaternioni). Da questi numeri si può partire per costruire tutta (o quasi) la matematica.

Che i numeri primi siano infiniti lo sappiamo da tempo. Lo dimostrò già Euclide circa nel 300 a.C. con un procedimento semplice e elegante, tanto semplice da poter essere raccontato nel corso dello spettacolo. Quello che ancora non sappiamo è come sono distribuiti, in pratica come trovare un numero primo successivo a un numero primo dato. Bella l'idea di associarli a delle stazioni ferroviarie nelle quali alcuni fuggiaschi possono rifugiarsi e trovare la salvezza da chi li sta perseguitando. Il fatto che non si sappia come sono distribuite (le stazioni come i numeri primi) le rende difficili da trovare da parte degli inseguitori e questo dà un connotato perfino positivo e salvifico a quella che in realtà è una spina nel fianco di ogni matematico che si occupi di teoria dei numeri.
Se non si conosce la distribuzione dei numeri primi, almeno si sa che questo problema è strettamente legato alla dimostrazione di un'importante congettura, detta Ipotesi di Riemann. Tale ipotesi, formulata per la prima volta dal matematico tedesco nel 1859, ipotizza una proprietà degli zeri (i valori per cui una funzione si annulla) di una funzione speciale, detta appunto di Riemann". Chi riuscisse a dimostrare tale ipotesi guadagnerebbe il milione di dollari messi in palio dal Clay Mathematics Institue di Cambridge, un'associazione no-profit che si dedica all'incremento e alla diffusione delle conoscenze matematiche nel mondo.

Ma non è questa l'unica congettura legata ai numeri primi che si sia meritata un premio milionario. La stessa quantità di denaro era stata promessa a chi fosse in grado di dimostrare la congettura di Goldbach, anch'essa citata più volte nel corso dello spettacolo, molto più semplice nella sua formulazione: ogni numero pari maggiore di 2 è somma di due numeri primi. Tale congettura fu formulata per la prima volta nel 1742 in una lettera scritta da Christian Goldbach al grande matematico svizzero Leonard Euler: da allora generazioni di matematici sognano di trovarne una dimostrazione. Tra gli altri anche il personaggio immaginario del divertente romanzo di Apostolos Doxiadis "Lo zio Petros". La congettura di Goldbach fu definito da John Nash "un affascinante rappresentazione della trappola mentale nella quale può cadere un matematico, quando è troppo preso da un problema difficile".

Era stata proprio la casa editrice americana del libro di Doxiadis a offrire un milione di dollari a chi avesse dimostrato la congettura di Goldbach entro due anni dalla fine di marzo del 2000, data di pubblicazione del libro. Si contava su una ventina di persone al mondo in grado di vincere il premio, ma il tempo è ormai scaduto e la casa editrice ha, purtroppo per la scienza, risparmiato i suoi soldi. Esistono vari premi, sempre dell'ordine di centinaia di migliaia di dollari, per chi riuscisse a trovare un numero primo con 10 milioni, 100 milioni o un miliardo di cifre. E qui si apre l'affascinante capitolo della caccia ai numeri primi sempre più grandi. Esistono infatti migliaia di persone, molte delle quali non professionisti nel campo, che sognano di trovare il numero primo più grande tra quelli conosciuti. Ma come è possibile farlo ?

Innanzi tutto due parole sui numeri detti di Mersenne, ovvero i numeri della forma

$$M_n=2^n-1$$

con n numero naturale. Sono così chiamati dal monaco francese Marin Mersenne che nel secolo XVII dichiarò che tutti i numeri della forma erano primi per certi valori di n e sicuramente non erano primi per tutti gli altri valori di n minori di 257. Anche se la sua congettura risultò più tardi non del tutto vera, resta impressionante pensare che ci fosse arrivato senza avere a disposizione nemmeno una macchina calcolatrice. Ma i veri protagonisti della storia sono i numeri di Mersenne con n numero primo.
I numeri primi più grandi di cui siamo a conoscenza sono quasi tutti di questa forma. Esiste infatti un metodo particolarmente semplice per stabilire se un numero di Mersenne sia un numero primo oppure no e nello stesso tempo si è sicuri che se n non è un numero primo allora sicuramente anche M_n non lo è.

Nel 1995, grazie a un programmatore di nome George Woltman, nasce a Orlando in Florida un progetto mondiale chiamato GIMPS (The Great Internet Mersenne Prime Search) che conta a tutt'oggi più di quattromila volontari in tutto il mondo. A ogni partecipante vengono assegnati certi numeri di Mersenne con il compito di verificare se sono primi. Per poter partecipare al progetto basta scaricare su un computer di classe Pentium il programma che si trova sul sito del GIMPS ed essere disposti a farlo girare praticamente notte e giorno. A queste condizioni, occorre infatti almeno un mese per completare un singolo test di primalità.

Ma il fascino dei numeri primi non si ferma qui. Ci sono molte altre congetture meno famose in attesa di essere dimostrate, ci sono nuovi sistemi operativi che aspettano di essere testati proprio attraverso i calcoli che permettono di stabilire se un numero è o non è primo e ci sono metodi crittografici come l'RSA (quello che regola il Bancomat) che si basano sulla relativa facilità di trovare numeri primi grandi opposta all'enorme difficoltà di scomporre in fattori primi numeri interi opportunamente scelti.

CONTATTI:
Maria Eugenia D'Aquino e **Valentina Colorni**
teatroinmatematica@pacta.org
www.pacta.org