

Quasi per caso: quando i computer danno i numeri

Paolo Caressa

A Davide Donati, che ci ha lasciati troppo presto.
In memoriam.

1. Introduzione

I computer, malgrado tutto, sono macchine deterministiche: questo vuol dire che eseguono (programmi che codificano) algoritmi deterministici, cioè che a parità di condizioni iniziali svolgono sempre lo stesso compito nello stesso modo.

In altri termini, un computer è prevedibile: per esempio, ogni volta che accendiamo il nostro portatile, il sistema operativo contenuto nel suo disco rigido viene attivato sempre nello stesso modo e con la stessa sequenza di passi: quando il computer è pronto per essere usato, ci presenta sempre la stessa schermata, per esempio lo spazio per introdurre nome utente e password, e quando introduciamo questi dati si comporta sempre allo stesso modo, vale a dire se il nome utente e/o la password sono sbagliate ci chiede di reinserirle, altrimenti carica le impostazioni del nostro profilo e rimane in attesa di istruzioni, che gli utenti gli impartiscono cliccando col mouse su qualche icona, inserendo dei comandi con la tastiera, etc.

Può anche accadere che il computer ci chieda di cambiare le nostre credenziali di accesso, il che è usualmente considerata una seccatura da parte degli utenti (che cambiano la password da “pippo1” a “pippo2” e simili), ma anche questo è un comportamento deterministico: il sistema operativo è programmato per contare da quante volte, o da quanto tempo, non si cambia la password e chiederla quando questa soglia è superata.

Questa caratteristica dei computer (o degli *smartphone* o di qualsiasi altro dispositivo che contenga una memoria e un processore) li rende macchine eminentemente non casuali, e in questo li differenzia da molti altri oggetti del mondo reale, a partire da noi umani.

Ma è proprio così? E, se sì, come è possibile che i computer siano utilizzati per svolgere simulazioni di eventi che invece costituiscono la quintessenza della casualità, come le previsioni meteorologiche, l'andamento delle borse, i fenomeni sismici, etc.? Per non parlare delle applicazioni dei giochi elettronici su *smartphone* e *playstation*, che sono computer anche molto potenti: come è possibile che un computer riesca a simulare un gioco nel quale l'imprevedibilità e il caso sono il principale elemento che un giocatore cerca per trarre reale divertimento dal gioco?

Banalmente, come è possibile anche soltanto simulare un lancio di dadi al computer se, come abbiamo detto, questo non è in grado di eseguire altro che algoritmi deterministici?

Per provare a rispondere a queste domande, e porne altre non meno interessanti, dobbiamo prima chiarire cosa si intenda con tutti questi termini: caso, casualità, determinismo, computer, algoritmo, etc., che è quello che cercheremo di fare in questa nota, cercando di mantenere la discussione al livello più elementare possibile, ma senza privarci del piacere di introdurre i concetti matematici di base che consentono di definire in modo preciso e soddisfacente tutte queste nozioni.

Se alla fine di queste note chi legge avrà capito il titolo che le corredata nella sua ironica precisione, lo scopo di questo breve testo sarà stato raggiunto¹.

2. Il comune senso della casualità

Il caso è una componente ineluttabile della nostra esistenza e, in generale, sembra pervadere il mondo che si presenta ai nostri sensi: già la parola contiene in sé una traccia di questa pervasività, dato che viene dal latino *casus* che vuol dire *caduta*: dunque il caso è ciò che (ac)cade, “*un avvenimento fortuito, accidentale e imprevisto*”, come recita il Dizionario Treccani².

Sebbene il caso sia un fedele compagno delle nostre vite, per la maggior parte delle volte la sua influenza è assolutamente trascurabile o controllabile: altre volte è una questione di vita o di morte, come nel caso dei passanti, coinvolti in atti terroristici o semplici catastrofi naturali, che si trovavano a passare di lì, appunto, per caso.

Limitandoci a fenomeni quantificabili, che possono cioè essere rappresentati con dei numeri, ciascuno di noi ha un concetto “intuitivo” di fenomeno casuale: l’esempio più banale sono i numeri estratti a una lotteria, ma anche le misurazioni della temperatura in una certa località, il valore di una azione, etc.

Ciascuno di questi fenomeni è riassumibile con un numero, e la rilevazione successiva del fenomeno dà quindi luogo a una successione numerica: il fenomeno è per noi casuale se, ogni volta che lo andiamo a misurare, non restituisce necessariamente lo stesso numero della volta precedente, né è chiaro in che modo l’ultima misurazione sia legata alle precedenti.

Ma come caratterizzare un fenomeno casuale? La risposta è meno ovvia di quel che sembri. Consideriamo per esempio le seguenti successioni numeriche:

1 1 1 1 1 1 1 1 1 1 ...
1 4 1 5 9 2 6 5 3 5 8 9 ...
640 231 100 91 1003 ...

La prima ci sembra tutto meno che casuale, eppure è stata ottenuta lanciando dodici volte di seguito un dado, mentre la seconda è data dalle prime cifre decimali del π greco, e la terza è la lista di

¹ Le slide della conferenza dalla quale queste note originano si trovano sul sito <http://www.caressa.it/quasipercaso/>

² Cfr. <http://www.treccani.it/vocabolario/caso/>

numeri che Leporello snocciola a donna Elvira nell'aria *Madamina, il catalogo è questo* del *Don Giovanni* di Mozart e Da Ponte.

Dunque solo il primo evento può realmente dirsi casuale, eppure è in grado di produrre successioni che non sembrano casuali: questo perché, nel sentire comune, “casualità” è sinonimo di “irregolarità” e “imprevedibilità”; una successione composta solo da 1 è regolare e prevedibile (anche se prima o poi il dado darà un altro risultato), mentre le altre due successioni non sembrano a priori seguire alcuna regola, sebbene la regola, sotto sotto, ci sia.

Questa definizione “intuitiva” di casualità è troppo soggettiva per poter essere utilizzata in modo coerente: infatti se identifichiamo la casualità con l'irregolarità dovremmo definire quest'ultima; ma, “irregolare” vuol dire “senza una regola”, ed è difficile stabilire con certezza che non ci sia una regola dietro un fenomeno (anzi, come vedremo, la storia della scienza è stata tutto un cercare regole in fenomeni che apparentemente non ne avevano).

Ma anche stabilire che una regola c'è non è affatto scontato: per esempio lanciando dodici volte un dado, e ottenendo sempre 1, potremmo dedurre che il dado è truccato e che quindi è soggetto alla regola “fai sempre uscire 1”: ma non potremo mai essere realmente sicuri che sia così se non lanciandolo infinite volte. Infatti nessuno ci garantisce che, prima o poi, non esca un altro numero.

L'unico modo per essere convinti che il dado sia truccato sarebbe analizzarlo e scoprire che un peso è stato posto in prossimità della faccia opposta a 1 (che è 6): ma anche allora potrebbe accadere che, per un certo lancio “maldestro”, il dado non si posizioni sull'1.

Naturalmente nessuno può lanciare infinite volte un dado, ma un numero molto alto di volte sì, e quello che ci aspettiamo è che, in media, più volte lo si lancia e più tutte le facce tenderanno ad uscire, e più o meno lo stesso numero di volte. Questa convinzione è lecita, e corrisponde all'idea che il lancio di un dado non truccato corrisponda a un evento “uniformemente distribuito”: vediamo di cosa si tratta.

Chiameremo *variabile aleatoria*³ un fenomeno (o evento) che, ogni volta che viene misurato, fornisce un numero, e supporremo sempre di conoscerne:

- l'insieme $\{x_1, x_2, \dots, x_N\}$ dei possibili valori che possono risultare dalla misurazione della variabile;
- la probabilità che ciascun valore ha di essere effettivamente misurato.

Per quanto riguarda il concetto di probabilità, una trattazione rigorosa ed esauriente ci porterebbe lontano, possiamo comunque darne una definizione operativa: se una variabile aleatoria X possiede N possibili valori $x_1, x_2, \dots, x_N$, la *distribuzione probabilistica* di X è una successione $(p_1, \dots, p_N)$ di N valori tali che

- Ciascun p_i è un numero strettamente compreso fra 0 e 1: $0 < p_i < 1$.
- La somma dei p_i vale 1: $p_1 + \dots + p_N = 1$.

Diciamo che ciascun p_i è la *probabilità* del valore x_i .

³ Termine derivato dal latino *alea* che vuol dire “dado”.

Per esempio: se X è il risultato del lancio di un dado, i valori possibili sono $x_1 = 1, x_2 = 2, \dots, x_6 = 6$, e le rispettive probabilità valgono tutte $1/6$: $p_1 = p_2 = \dots = p_6 = 1/6$.

Una variabile aleatoria X si dice *uniformemente distribuita* o semplicemente *uniforme* se per ciascuno dei suoi possibili N valori x si ha che la corrispondente probabilità è $p = 1/N$.

Vediamo un esempio di variabile aleatoria non uniforme: consideriamo X i cui valori sono la somma dei risultati nel lancio simultaneo di due dadi: $x_1 = 2, x_2 = 3, \dots, x_{11} = 12$. Calcoliamo le probabilità corrispondenti usando una definizione di probabilità basata sulle possibili frequenze di occorrenza dei singoli valori della variabile: la probabilità p_i è cioè il quoziente n/m fra il numero n di occorrenze del valore x_i , e m è il numero totale di occorrenze possibili di ciascuna variabile.

Poiché le possibili combinazioni di valori di due dadi sono:

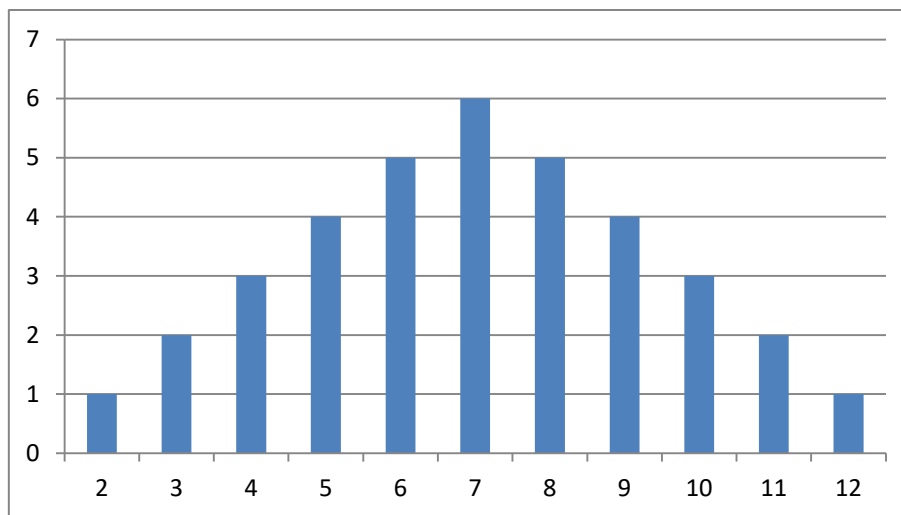
$$\begin{aligned}2 &= 1 + 1 \\3 &= 1 + 2 = 2 + 1 \\4 &= 1 + 3 = 2 + 2 = 3 + 1 \\5 &= 1 + 4 = 2 + 3 = 3 + 2 = 4 + 1 \\6 &= 1 + 5 = 2 + 4 = 3 + 3 = 4 + 2 = 5 + 1 \\7 &= 1 + 6 = 2 + 5 = 3 + 4 = 4 + 3 = 5 + 2 = 6 + 1 \\8 &= 2 + 6 = 3 + 5 = 4 + 4 = 5 + 3 = 6 + 2 \\9 &= 3 + 6 = 4 + 5 = 5 + 4 = 6 + 3 \\10 &= 4 + 6 = 5 + 5 = 6 + 4 \\11 &= 5 + 6 = 6 + 5 \\12 &= 6 + 6\end{aligned}$$

troviamo che i possibili valori sono $1 + 2 + 3 + 4 + 5 + 6 + 5 + 4 + 3 + 2 + 1 = 36$, e le singole probabilità sono: $p_1 = 1/36, p_2 = 2/36, p_3 = 3/36, p_4 = 4/36, p_5 = 5/36, p_6 = 6/36, p_7 = 5/36, p_8 = 4/36, p_9 = 3/36, p_{10} = 2/36, p_{11} = 1/36$.

Pertanto, ci aspettiamo che lanciando una coppia di dadi sia più facile che esca il 7 piuttosto che esca il 12, perché 7 si ottiene in sei modi diversi, 12 in un modo soltanto.

Possiamo rappresentare graficamente la distribuzione di una variabile aleatoria con un *istogramma*, cioè con un grafico in cui ciascuna colonnina, sopra un possibile valore della variabile, è alta proporzionalmente alla possibile frequenza di occorrenza di quel valore: nel caso dei due dadi l'istogramma è il seguente⁴:

⁴ Si noti come questa figura sia sostanzialmente la lista di equazioni precedenti ruotata di 90° .



Se invece lanciamo due volte di seguito uno stesso dado, e chiamiamo x il valore uscito la prima volta e y il valore uscito la seconda, la probabilità che, fra tutte le possibili coppie di numeri (n, m) compresi fra 1 e 6, sia uscita proprio la coppia (x, y) è pari al prodotto delle probabilità di x e di y , che sono entrambe $1/6$, e quindi pari a $1/36$. Infatti i due lanci sono indipendenti, uno non ha influenza sull'altro e viceversa, e la probabilità che si verifichino entrambi è il prodotto delle probabilità che si verifichino singolarmente, che come sappiamo per un dado non truccato sono $1/6$.

Dunque la distribuzione della variabile aleatoria che misura le coppie di valori nel lancio successivo di un dado è ancora uniforme: in generale, se lanciamo n volte uno stesso dado, annotando i valori successivi, ciascuna possibile combinazione di valori ha la medesima probabilità, pari a $1/6^n$ di occorrere.

Per esempio, lanciando dieci volte di seguito un dado non truccato potremmo ottenere le seguenti successioni:

```

1 1 1 1 1 1 1 1 1 1
5 3 1 5 6 3 4 1 7 2
6 1 4 3 1 5 6 2 4 3

```

E' poco intuitivo, ma, come abbiamo appena stabilito, tutte queste sequenze sono *equiprobabili*: ciascuna ha la medesima probabilità di comparire dell'altra. La prima sequenza ci sembra tuttavia "meno casuale" delle altre, perché riflette una ovvia regolarità, e ci pare poco probabile che tutti quegli 1 escano di seguito con altri 5 numeri a disposizione per ogni lancio.

Questo errore "psicologico" è legato a un'altra ben nota fallacia in cui il senso comune incorre quando si ha a che vedere con estrazioni di numeri a caso, tipicamente nelle lotterie: se un numero non viene estratto per un certo periodo si ritiene che la sua probabilità di estrazione aumenti col passare del tempo. Si tratta dei cosiddetti "numeri ritardatari" noti agli accaniti amanti del Lotto.

Ma questo concetto non ha senso: a meno che la lotteria non sia truccata, ogni volta che si estrae un numero, tutti i numeri nell'urna hanno la stessa probabilità di essere estratti, quindi ogni volta 1 ha

la stessa probabilità di essere estratto della volta precedente. In altri termini ogni estrazione è un evento a sé, indipendente dai precedenti, e quindi ogni estrazione “ignora” la storia delle estrazioni precedenti e quindi non può in alcun modo esserne influenzata: i numeri non hanno memoria!

Il fatto, intuitivo, che prima o poi il numero esca è piuttosto ancora conseguenza della proprietà di uniformità, in virtù della quale, al tendere del numero di estrazioni all’infinito, le frequenze di estrazione di ciascun numero possibile⁵ tendono a coincidere. Ma una proprietà “in grande” e che vale “in media” non può in alcun modo garantire quale sarà la prossima estrazione: un evento realmente casuale è in effetti imprevedibile, anche se la sua distribuzione è nota.

In questo senso, il calcolo delle probabilità non aiuta, in quanto non consente di dedurre nulla su una singola sequenza di numeri generata da un evento o fenomeno casuale: supponiamo per esempio che qualcuno ci abbia consegnato un dado asserendo che non è truccato; se lanciamo dieci volte il dado ed esce sempre 1, e replicassimo che quindi ci pare truccato, chi ce lo ha dato ci ricorderebbe che la sequenza di dieci 1 ha la stessa probabilità delle altre.

Soltanto lanciando il dado moltissime volte e applicando dei test statistici per verificare l’aleatorietà della sua distribuzione potremmo convincerci che non è truccato: ma analizzando una singola sequenza di lanci è impossibile farlo.

3. La guerra (persa) contro il caso

Tutto questo interesse per la probabilità e il caso sembra, fin qui, una mera curiosità legata nel migliore dei casi ai giochi di azzardo: in effetti, la teoria delle probabilità è nata proprio dallo studio dei giochi d’azzardo e dei giochi di carte, nel XVIII secolo. La sua applicazione e i suoi usi nella scienza e nella tecnologia moderne sono molto più recenti, e per una buona ragione: potremmo infatti dire che l’intera storia del pensiero scientifico, fino agli albori del ‘900, è stata infatti una “guerra” contro il caso.

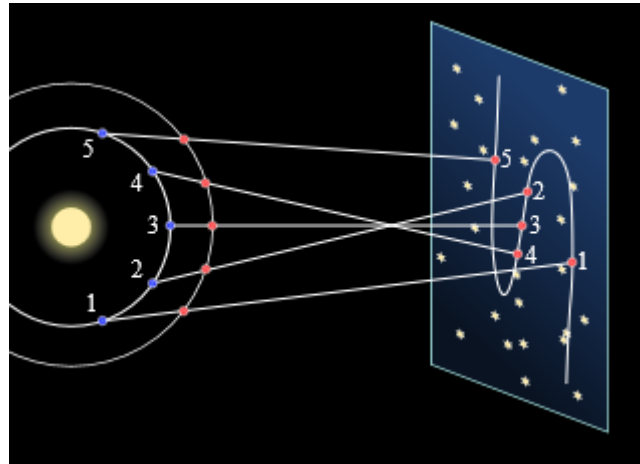
In effetti, fin dalla più remota antichità, l’Uomo ha cercato sempre degli schemi e delle regole per comprendere il mondo che lo circondava: in effetti molti fenomeni presentavano delle regolarità, come il giorno, le stagioni, le maree, etc. Era quindi importante capire queste regolarità per poter anticipare i fenomeni naturali e limitarne i danni, o sfruttarli a proprio vantaggio: probabilmente queste prime conoscenze empiriche hanno anche favorito lo sviluppo dell’agricoltura, circa 12.000 anni or sono, e quindi le città e le civiltà che conosciamo in tempi storici.

Il fatto che per alcuni fenomeni naturali fosse possibile individuare delle regolarità ha generato alla lunga l’idea che ogni evento naturale fosse regolato da regole e leggi: lo studio di queste leggi poteva essere non semplice ma doveva sicuramente essere possibile. Basterà pensare allo sviluppo dell’astronomia presso antiche civiltà, come Babilonesi, Egizi e Maya, che riuscivano a prevedere fenomeni astronomici e il moto dei corpi celesti.

Persino fenomeni apparentemente irregolari, come il moto retrogrado del pianeta Marte, trovarono una spiegazione nel sistema tolemaico, che, sebbene ponesse la Terra al centro del Cosmo, riusciva

⁵ Per esempio nel caso del Lotto i numeri possibili sono 90.

a dare conto molto bene del moto degli astri, per quanto lo si potesse apprezzare con gli strumenti dell'età ellenistica: in particolare si riuscivano a prevedere le traiettorie di numerosi astri, utili (all'epoca) anche per formulare oroscopi e per altri scopi divinatori.



Il moto (apparentemente) retrogrado di Marte causato dal suo essere su un'orbita più esterna di quella della Terra (fonte: Brian Brondel - Opera propria, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=1652425>).

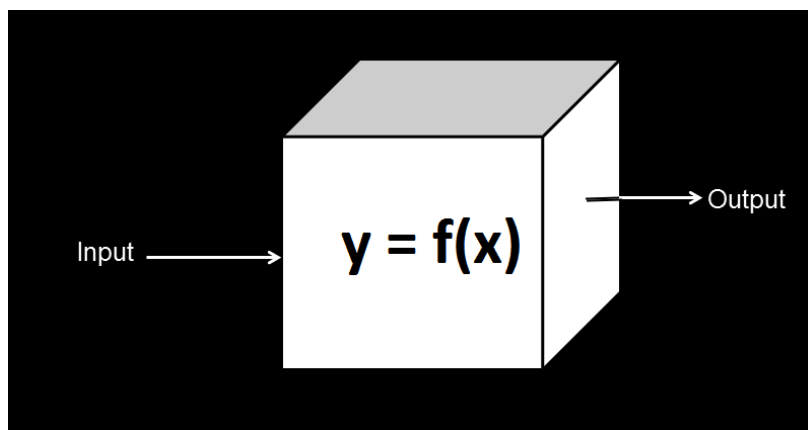
La scienza moderna, nata nel '600 in Europa grazie all'opera di studiosi come Giovanni Keplero, Galileo Galilei e Isaac Newton, riuscì a dare una spiegazione ancor più convincente dei fenomeni astronomici, culminando nella *teoria del mondo* di Newton, che con pochissime e semplici leggi spiegava tutti i fenomeni di gravitazione allora conosciuti.

Le leggi fisiche, da Newton in poi, si esprimono per mezzo di strumenti matematici chiamati *equazioni differenziali*, le cui incognite non sono numeri, come nel caso delle equazioni algebriche, ma traiettorie di oggetti (cioè curve) come particelle, pianeti e corpi dotati di massa.

Il concetto che fu sviluppato, da Newton e Leibniz (poggiando sulle ricerche di loro predecessori, come Pierre de Fermat e Isaac Barrow), per descrivere le traiettorie degli oggetti soggetti alle leggi naturali è uno di quelli centrali nella matematica: il concetto di *funzione*.

Nel caso più semplice possiamo pensare a una funzione come a un processo che dato un numero x in input restituisce un numero y in output in modo che uno stesso input non possa dar luogo a due output diversi. Scriviamo usualmente $y = f(x)$ dove f è il nome della funzione: racchiudere l'argomento della funzione fra parentesi suggerisce che al variare di x si ottengono tutti i possibili valori di y .

Una funzione può essere immaginata come una scatola nera nella quale si immette un numero e che ne restituisce un altro, in modo che lo stesso numero immesso dia sempre luogo allo stesso numero emesso.



Una funzione è quindi un oggetto *deterministico*: l'input determina univocamente l'output. In quanto tale una funzione è un oggetto assolutamente non casuale.

Ecco alcuni esempi di funzioni:

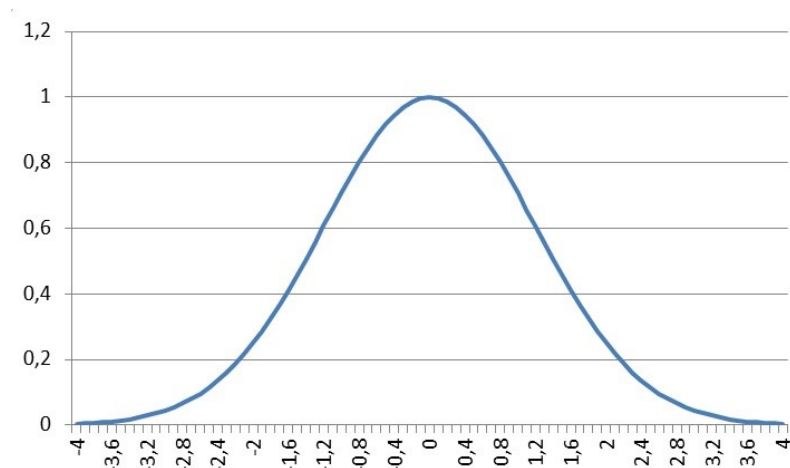
- $y = 4x(x - 1)$
- $y = \cos x$
- $y = \text{area del cerchio di raggio } x$

I seguenti invece *non* sono esempi di funzioni

- $y = \text{il numero il cui quadrato è } x$ (per esempio sia $+1$ che -1 hanno come quadrato 1).
- $y = \text{il numero il cui coseno è } x$ (poiché il coseno è periodico: $\cos x = \cos(x + 2\pi)$).
- $y = \text{il numero di lati di un poligono di area } x$ (per esempio il quadrato di lato 1 e un triangolo di base 2 e altezza 1 hanno la stessa area 1).

Una funzione si può rappresentare in diversi modi, che dipendono da cosa sappiamo della funzione stessa: in alcuni casi abbiamo una formula che lega la x alla y , e quindi possiamo dare una definizione esatta della funzione, come nel caso delle prime due funzioni precedenti. Possiamo poi conoscere una lista di coppie (x, y) per una funzione e quindi tabularne alcuni valori, oppure avere una idea qualitativa di come y varia in termini di x e riuscire a tracciarne il *grafico*.

x	$f(x)$
-4,00	0,00
-3,00	0,04
-2,00	0,25
-1,00	0,71
0,00	1,00
1,00	0,71
2,00	0,25
3,00	0,04
4,00	0,00



Le funzioni stanno alla fisica newtoniana come i numeri stanno all'algebra: le si usa per esprimere soluzioni di equazioni, che poi sono le leggi del moto dei corpi. Per esempio, la celeberrima equazione newtoniana $F = ma$ esprime la forza di un corpo come il prodotto della sua massa per l'accelerazione cui è sottoposta: nella fisica newtoniana, l'accelerazione è legata alla traiettoria del corpo da una legge "differenziale", che nel caso più semplice (accelerazione costante) è la seguente:

$$x(t) = x_0 + v_0 t + \frac{1}{2} a t^2$$

Cioè x è funzione del tempo t , e dipende anche da due parametri x_0 e v_0 che sono la posizione iniziale e la velocità iniziale del corpo (per semplicità stiamo supponendo un moto in una sola dimensione, quella dell'asse delle x appunto): si chiamano *condizioni iniziali* dell'equazione differenziale di cui la funzione $x(t)$ fornisce una soluzione, cioè una traiettoria.

I due fatti cruciali che rendono la teoria newtoniana così perfetta rispetto agli strumenti di misurazione disponibili nel '600 e '700 sono i seguenti

- *Esistenza e unicità delle traiettorie*: note le condizioni iniziali esiste sempre un'unica soluzione delle equazioni differenziali, come quelle che forniscono le leggi del moto: come a dire, ogni moto, fissate le condizioni iniziali, ha un'unica traiettoria che lo definisce⁶.
- *Linearità delle traiettorie*: al variare con continuità delle condizioni iniziali, varia con continuità la traiettoria che esse individuano: precisamente, *a piccole variazioni delle condizioni iniziali corrispondono piccole variazioni nella traiettoria del moto*.

Queste due proprietà rendono la fisica newtoniana una teoria deterministica, che non lascia spazio alcuno al caso.

Fra la seconda metà del '700 e la prima metà dell'800 la fisica newtoniana fu portata a compimento da studiosi come Leonhard Euler, Giuseppe Luigi Lagrange, Pierre Simon de Laplace e William Rowan Hamilton, che ne generalizzarono i principi e fondarono quella che oggi si chiama *meccanica analitica*. In particolare, Laplace, che si occupò anche di teoria analitica della probabilità, formulò all'inizio dell'800 nel modo più maturo e spregiudicato il principio di determinismo che all'epoca si credeva consentisse di spiegare qualsiasi fenomeno naturale:

Una intelligenza che, a un dato istante, conosca tutte le forze che animano la natura, la posizione rispettiva degli enti che la compongono, se fosse così vasta da sottoporre questi dati all'analisi [matematica], abbraccerebbe nella medesima formula i movimenti dei più grandi corpi dell'universo, e quelli dei più effimeri atomi. Nulla sarebbe incerto per essa, e sia l'avvenire sia il passato sarebbero presente ai suoi occhi.

Messa in questo modo sembrerebbe che il determinismo altro non sia che la formulazione scientifica dell'onniscienza divina: tuttavia, quando Napoleone chiese a Laplace perché nel suo

⁶ Occorrerebbe rendere rigorosa questa affermazione precisando le ipotesi matematiche che garantiscono l'esistenza e l'unicità delle traiettorie: qualsiasi testo di analisi matematica o sistemi dinamici contiene enunciato e dimostrazione di questo importante teorema di esistenza e unicità per i sistemi di equazioni differenziali ordinarie.

celebre trattato *Esposizione del sistema del mondo* non vi avesse fatto menzione di Dio, Laplace rispose *non ho avuto bisogno di questa ipotesi...*

Ma fu proprio nel XIX secolo che la necessità di capire nuovi fenomeni, o di proporre nuove spiegazioni per fenomeni per i quali l'approccio newtoniano era impraticabile, come il comportamento dei gas, impose all'attenzione di fisici e matematici il caso e la statistica: la scienza scoprì che non solo non riusciva a spiegare tutto in modo deterministico, ma che non poteva fare a meno del caso!

Per esempio, la teoria di Charles Darwin, probabilmente il massimo traguardo della scienza ottocentesca, faceva intervenire il caso in modo essenziale nella variabilità genetica che consentiva il mutare, e quindi la selezione, delle specie. La teoria cinetica dei gas e la termodinamica statistica utilizzarono in modo essenziale i concetti probabilistici, come le distribuzioni e le variabili aleatorie, e, agli inizi del XX secolo, il determinismo non soltanto si trovò ridimensionato ma messo in discussione.

La celeberrima teoria quantistica, nell'impostazione datale da Werner Heisenberg, spazzò via definitivamente i principi newtoniani del determinismo: infatti, la teoria del moto di Heisenberg non va a delineare traiettorie ma descrive le particelle in termini di "ampiezze di probabilità", e si fonda sul *principio di indeterminazione*, che stabilisce l'impossibilità di poter conoscere posizione e velocità di una stessa particella a un dato istante: cioè le condizioni iniziali della teoria newtoniana sono inconoscibili, e l'onniscienza immaginata da Laplace del tutto illusoria!

Non a caso il grande fisico Stephen Hawking, che pure si è occupato principalmente di "massimi sistemi", cioè di cosmologia e della teoria einsteiniana della gravitazione (l'ultima teoria deterministica sopravvissuta al '900) ebbe a dire:

Quindi sembra che Einstein fosse doppiamente in errore quando diceva che Dio non gioca a dadi. Non soltanto Dio gioca sicuramente a dadi, ma spesso ci confonde lanciandoli dove non possiamo vedere [allude ai buchi neri].

Il caso è tornato di nuovo sul trono delle scienze naturali e sembra difficile che abdiccherà in tempi brevi al proprio dominio sulla Natura...

4. Calcolare a caso...

Come recita un celebre adagio: *se non puoi sconfiggerli, fatteli amici!* E' un po' quello che è successo con la scienza contemporanea, che non solo ha dovuto accettare la presenza del caso come componente intrinseca nella natura delle cose, ma che l'ha anche volto a proprio vantaggio e trasformato in uno strumento di conoscenza.

Due circostanze, accadute nello stesso periodo storico, hanno consentito alla casualità di divenire una componente importante della scienza moderna: lo sviluppo della teoria rigorosa delle probabilità (ad opera di studiosi come Andrei Markov, Paul Lévy e soprattutto Andrei Kolmogorov) e lo sviluppo dei calcolatori elettronici, che ha consentito di svolgere calcoli un tempo praticamente impossibili.

Un esempio è dato dal seguente metodo del calcolo del numero pi greco: come sappiamo questo numero è irrazionale, quindi il suo sviluppo decimale non è né finito né periodico, ma è possibile calcolarne delle approssimazioni finite da usare nei calcoli fisici e ingegneristici.

Un modo per calcolare il pi greco usando la definizione “frequentista” di probabilità è il seguente: ritagliamo un foglio quadrato di due metri di lato e inscriviamo in questo quadrato un cerchio; poi mettiamo il foglio steso in giardino e aspettiamo che piova: dopo averlo lasciato un po’ alla pioggia lo portiamo in casa e contiamo le gocce di pioggia cadute sul foglio.

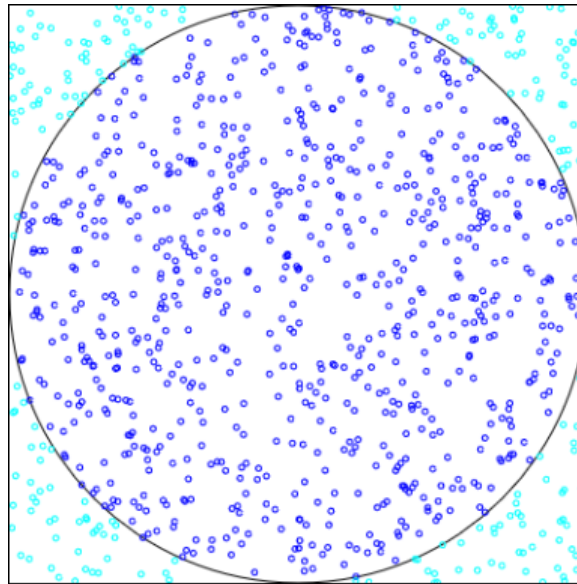
Se contiamo N gocce, delle quali N_C sono quelle cadute all’interno del cerchio, è abbastanza intuitivo che varrà (in modo approssimativo, e con approssimazione sempre migliore al crescere di N) la proporzione⁷

$$N:N_C = \text{Area del quadrato} : \text{Area del cerchio}$$

Ma, ricordando che il nostro cerchio ha raggio $r = 1$ e il quadrato ha lato $2r = 2$, l’area del quadrato è $(2r)^2 = 2^2 = 4$ mentre l’area del cerchio è $\pi r^2 = \pi$. Ne viene quindi che

$$N:N_C = 4 : \pi$$

il che vuol dire che $\pi = 4N_C/N$ (dove il segno “=” sta qui per “all’incirca uguale a”).



Calcolo del pi greco con 1000 gocce di pioggia: 785 ne sono cadute all’interno del cerchio quindi l’approssimazione per pi greco è $4 \times \frac{785}{1000} = 3,14$ (simulazione dell’autore on line alla pagina <http://www.caressa.it/quasipercaso/index.html#32>).

⁷ Supponendo che le gocce di pioggia cadano in modo uniformemente distribuito sul quadrato...

Non è certo questo il metodo più efficiente per calcolare il π greco⁸ ma l'idea è certamente notevole: in sostanza si riduce il calcolo di una quantità incognita (che tipicamente è il risultato di una operazione matematica chiamata “integrale”) al calcolo di una probabilità; quest'ultima si stima con l'approccio frequentista, cioè calcolando su un totale di casi la percentuale di casi che contribuiscono alla quantità che si vuole calcolare.

Naturalmente questo metodo, la cui idea si può far risalire alla prima metà del '700 all'opera di Georges-Louis Leclerc conte di Buffon, è molto difficile da applicare a mano, ma estremamente facile da applicare su un computer, e consiste essenzialmente nel primo esempio di una tecnica chiamata *Metodo di Montecarlo*, inventata durante la seconda guerra mondiale, precisamente nell'ambito del *Progetto Manhattan* il cui obiettivo era realizzare la bomba atomica, per opera di alcune delle più grandi menti del '900: Enrico Fermi, John von Neumann e Stanislaw Ulam.

Fra l'altro von Neumann (uno dei massimi scienziati del '900) è anche stato uno dei pionieri dei computer, tanto che l'architettura standard di un sistema di calcolo (non parallelo) si chiama *macchina di von Neumann*.

Ma cos'è esattamente una macchina di von Neumann, cioè un computer? Una risposta non precisa ma rapida è la seguente: si tratta di un dispositivo (solitamente elettronico) che consente di:

- Rappresentare numeri e altri dati con precisione finita e fissata e memorizzare sequenze di tali dati.
- Leggere e/o inviare dati da/a dispositivi esterni (tastiere, mouse, monitor, USB, etc.).
- Rappresentare codifiche di algoritmi che prendono in input i dati rappresentati e ne forniscono in output altri.
- Eseguire gli algoritmi codificati sui dati disponibili.

Un *algoritmo* altro non è che un particolare tipo di funzione, vale a dire una funzione “calcolabile”, cioè che si può esprimere con una procedura ripetibile che in un numero finito di passi consente di determinare il valore dell'output dato l'input⁹.

Dunque i computer sono sostanzialmente dispositivi in grado di calcolare funzioni, operando su numeri con un numero finito e fissato di cifre: ma l'idea che li rende così utili e generali è quella di rappresentare le stesse funzioni, e non solo i dati, con sequenze numeriche, in modo da poter memorizzare tutto nel computer e poter modificare o inserire nuove funzioni da calcolare ogni volta che si vuole (come si dice: “programmare” il computer).

A questo punto abbiamo però un problema: i computer, in quanto macchine che eseguono funzioni, sono assolutamente deterministici! Come possiamo svolgere una simulazione Montecarlo, che comporta l'estrazione di numeri casuali, su una macchina deterministica? Nel caso del calcolo del

⁸ Il lettore interessato, dopo una facile ricerca su Internet, potrà per esempio ammirare la formula di Ramanujan per il calcolo del π greco.

⁹ Anche questa definizione è lungi dall'essere rigorosa: ma, a dire il vero, non esiste una definizione rigorosa di algoritmo, piuttosto esistono numerose definizioni equivalenti di “calcolabilità” e l'ipotesi, detta “tesi di Church” (dal nome del logico statunitense Alonzo Church) secondo la quale un algoritmo ammette sempre una formulazione in ciascuna di queste definizioni equivalenti di calcolabilità.

pi greco precedente, si tratta per esempio di produrre N coppie di coordinate (x, y) dove $0 \leq x \leq 2$ e $0 \leq y \leq 2$ casuali e distribuite in modo uniforme. Come è possibile?

Una prima risposta è che è sicuramente impossibile produrre numeri a caso su un computer, proprio perché quest'ultimo è una macchina deterministica: come ha scritto efficacemente lo stesso von Neumann

Chiunque consideri metodi aritmetici per generare cifre a caso vive, naturalmente, nel peccato. Infatti, come è stato notato molte volte, non ci sono cose come i numeri a caso, ci sono solo metodi per produrre numeri a caso e una procedura rigorosamente aritmetica non è ovviamente un tale metodo.

Eppure, proprio in questo momento mentre leggete queste note, da qualche parte nel mondo un gruppo di scienziati sta svolgendo calcoli, esperimenti e simulazioni che comportano l'uso di metodi di Montecarlo (o loro varianti più sofisticate) tutti rigorosamente realizzati al computer, e numerosi computer stanno effettivamente svolgendo queste simulazioni per una quantità di applicazioni diverse.

Nel farlo, in realtà, non stanno realmente estraendo numeri a caso, ma generando numeri, secondo processi deterministici, che sembrano a caso, pur non essendolo: i *numeri pseudo-casuali*.

Per capire cosa siano e come sia possibile che vadano altrettanto bene dei numeri realmente casuali per esperimenti e simulazioni è necessario finalmente prendere di petto la domanda: ma cos'è esattamente una successione di numeri casuali?

5. Casualità, complessità e comprimibilità

Abbiamo in precedenza parlato di variabili aleatorie, e detto che una tale variabile, ogni volta che viene interrogata, fornisce un valore, fra un insieme di valori possibili, e con una certa probabilità. Misurare per un certo numero di volte la variabile vuol dire produrre una successione di tali valori, che potrebbe non essere sempre la stessa, ma che segue la distribuzione della variabile aleatoria.

Ma se invece della variabile aleatoria abbiamo solo una successione numerica? Che significa dire che è casuale?

In statistica esistono numerosi test per appurare il grado di casualità di una successione, che sostanzialmente si basano sul supporre che la successione sia un esempio prodotto da una variabile aleatoria con una qualche distribuzione. Questi test statistici consentono di valutare il carattere di aleatorietà della successione e quanto sia verosimile ascriverla a un certo fenomeno aleatorio. Ma non ci dicono cosa distingua una successione casuale da una che non lo sia: dobbiamo quindi cercare altrove una definizione di casualità di una successione data.

In effetti, definire in modo univoco cosa voglia dire che una successione di numeri sia casuale è compito arduo: tenteremo qui di riportare la definizione dovuta al genio di Andrei Kolmogorov, “l’Euclide della probabilità”¹⁰.

Un primo approccio alla definizione di successione casuale, senza implicare le variabili aleatorie, è stato dato dallo scienziato austriaco Richard von Mises che agli inizi del ‘900 ha tentato di definire cosa sia la casualità di una successione in termini di giochi d'azzardo: in sostanza, egli afferma, una successione numerica è casuale se non è possibile alterarne la statistica eliminandone una sottosuccessione.

Cioè scommettere “con un sistema” non migliora, nel lungo periodo, le possibilità di vincere in un gioco completamente casuale.

Facciamo un esempio: se abbiamo una successione di 0 e 1 che è casuale e uniformemente distribuita, se le togliamo tutti gli elementi di indice¹¹ pari non alteriamo in alcun modo la probabilità che sia estratto 0 o 1.

D’altra parte, se consideriamo la successione 0 1 0 1 0 1 ... in cui gli elementi di indice dispari sono 0 e quelli di indice pari sono 1, se togliamo la sottosuccessione degli elementi di indice pari rimaniamo con 0 0 0 ... che è una successione di soli 0 senza 1: abbiamo quindi cambiato la probabilità di estrazione di 0 e 1 (che è del 50% in entrambi i casi) rendendo la probabilità di estrarre 0 pari al 100% e quella di estrarre 1 pari allo 0%. Secondo la definizione di von Mises questa non è quindi una successione casuale.

Questa definizione è ingegnosa ma problematica: infatti andrebbero definite con esattezza come si possono definire le sottosuccessioni da estrarre, etc.

Invece una definizione di casualità che può essere resa completamente precisa è stata data proprio da Kolmogorov a metà degli anni ‘60 e indipendentemente anche dagli studiosi Ray Solomonoff e Grigory Chaitin.

L’idea è molto interessante e coinvolge proprio i computer: in sostanza, si considera come casuale una successione che non può essere prodotta da un programma per computer il quale sia sensibilmente più breve della successione stessa.

Per capire meglio la questione dobbiamo ricordare che un computer esegue algoritmi, cioè particolari funzioni, e che questi algoritmi sono codificati in sequenze di numeri memorizzati nella memoria del computer. La codifica di un algoritmo si chiama anche “programma”, e una tale codifica è una successione numerica, confrontabile quindi con l’output che è in grado di produrre quando il computer esegue il programma.

¹⁰ Fra le altre cose, Kolmogorov è stato il primo a fondare la probabilità su un approccio assiomatico, individuando un insieme di assiomi generali per una probabilità piuttosto che dire esplicitamente cosa sia una probabilità: in questo ha reso alla teoria lo stesso servizio che Euclide ha reso alla geometria piana e spaziale.

¹¹ Intendiamo con “indice” di un elemento di una successione ordinata il posto che occupa quell’elemento a partire dal primo: per esempio nella successione 3 8 5 7 2, 3 ha indice 1, 8 ha indice 2, 5 ha indice 3 e così via.

Per esempio, potremmo aver scritto un algoritmo per calcolare il massimo divisore fra due numeri: questo algoritmo, che normalmente è espresso in un linguaggio simbolico, viene poi tradotto in una sequenza di numeri che sono “codici” eseguibili dalla CPU del computer: infatti un computer non sa leggere testi, ma solo scandire sequenze di numeri e interpretarle come istruzioni da eseguire. Ciascun computer ha un proprio “linguaggio macchina”, cioè interpreta un certo numero, o una certa sequenza di numeri come una ben precisa istruzione che la sua CPU esegue. Dunque il programma che codifica l’algoritmo del massimo comune divisore è diverso, in quanto codifica numerica, da computer a computer ma esegue lo stesso algoritmo.

Supponiamo ora di avere una successione, per esempio un miliardo di numeri che sono alternativamente 0 e 1: 0 1 0 1 0 1...

Un programma per computer in grado di produrre questa successione di un miliardo di numeri, può essere codificato con qualche decina, centinaio al massimo di numeri: quindi possiamo generare la successione di $10^9 = 1.000.000.000$ numeri con un programma di lunghezza nell’ordine di $10^2 = 100$ numeri, il che vuol dire che la successione è completamente determinata e predicibile con una quantità di informazione che prende sette ordini di grandezza in meno della successione stessa.

Se, per esempio, volessimo comunicare a qualcuno questa successione, faremmo molto prima, e risparmieremmo molto più tempo, a inviare a questo qualcuno il programma che la genera. Pertanto, un altro modo di guardare a questo programma è come a una versione compressa della successione: la stessa informazione necessaria a replicare esattamente la successione può essere compattata in uno spazio di diversi ordini di grandezza inferiore.

Dunque, l’idea di Kolmogorov è che se riusciamo a scrivere un programma che genera una successione e che sia molto più breve della successione stessa, abbiamo definito la regolarità, lo schema, il *pattern* come spesso si usa dire, della successione, che quindi è completamente replicabile in modo deterministico. Abbiamo compresso in un programma tutta l’informazione contenuta nella successione: decomprimere l’informazione vuol dire eseguire il programma e quindi generare per mezzo di esso la successione.

Vale la pena di fare una osservazione esplicita: se trattiamo successioni finite, queste sono sempre “deterministiche”, nel senso che esiste sempre un algoritmo che le genera.

Per vederlo basterà considerare una successione $x_1, x_2, x_3, \dots, x_N$ anche per N molto grande: un algoritmo che la genera è il seguente (che scriviamo in italiano ma che è facile esprimere in un qualsiasi linguaggio di programmazione e quindi in un programma per computer):

1. stampa il numero x_1 ;
2. stampa il numero x_2 ;
3. stampa il numero x_3 ;
- ...
4. stampa il numero x_N .

Ma, chiaramente, questo algoritmo contiene esplicitamente i numeri che deve generare, quindi il programma corrispondente non potrà essere più corto della sequenza che vuole generare (anzi sarà più lungo perché contiene le istruzioni di stampa).

Se non è possibile generare una successione finita con un algoritmo più breve della successione stessa, si dice che la successione ha *complessità di Kolmogorov alta*: dal punto di vista informatico, questo vuol dire che la successione non è comprimibile (altrimenti esisterebbe un algoritmo di decompressione che la genererebbe).

Ma la teoria di Kolmogorov si estende alle successioni infinite ed è molto utile in questo caso: per esempio lo sviluppo decimale di un numero irrazionale, come il π greco o la radice di 2, è infinito e non periodico, quindi le cifre decimali dopo la virgola di questi numeri formano una successione infinita. In che senso queste successioni sono “casuali”?

Si noti che una successione infinita può essere generata da un algoritmo che non termina mai, come per esempio il seguente:

1. Stampa 1
2. Stampa 0
3. Vai al passo 1.

Questo semplice algoritmo genera la successione infinita 0 1 0 1 0 1 ... che, pur essendo infinita, è chiaramente non casuale in quanto generabile da un programma, per di più molto corto.

Kolmogorov definisce una successione infinita di numeri come casuale se la prima parte della successione è data da una successione finita di complessità alta: cioè una successione è casuale se una sottosuccessione finita con cui inizia non è comprimibile (in realtà questa definizione non è ben posta ed è stata resa rigorosa da Chaitin introducendo una particolare classe di algoritmi, che definire qui ci porterebbe troppo lontano: l'idea è tuttavia quella di considerare successioni i cui primi termini non siano esprimibili in modo più sintetico della successione stessa).

L'idea che una successione sia casuale se non la si può comprimere è in fondo riconducibile all'idea che se sappiamo descrivere in modo sintetico qualcosa allora lo abbiamo completamente determinato, e quindi non può essere considerato casuale. Invece, il carattere di imprevedibilità e irregolarità di una successione casuale è proprio legato al fatto di non saper trovare nessun modo più furbo di generare la successione se non enumerandone esplicitamente i termini.

C'è un modo empirico di verificare l'astuzia di questa teoria: basta prendere dei file e provare a comprimerli con un programma di compressione (come per esempio gzip o 7-zip): se proviamo a comprimere un file che contiene la sequenza 0 1 0 1 0 1 ... lunga un milione di caratteri, uno di questi programmi di compressione è in grado di comprimerlo a un file di qualche centinaio di caratteri.

Se invece produciamo un file di un milione di 0 e 1 a caso e proviamo a comprimerlo, la compressione non scenderà sotto i centomila caratteri, riuscendo quindi a comprimere solo di un ordine di grandezza il file.

Le successioni realmente casuali sono quindi proprio quelle che non si possono produrre con un algoritmo semplice, e, per di più, è possibile dimostrare che la misura della complessità di Kolmogorov di un algoritmo non è data da un algoritmo, cioè che la complessità di Kolmogorov non è calcolabile effettivamente. Cioè non è possibile dimostrare il grado di casualità di una successione perché non è possibile calcolare effettivamente la complessità di Kolmogorov: se però riusciamo a trovare un algoritmo che generi la successione, e quindi a comprimerla, avremo dimostrato che la sua complessità è bassa. Ma se non ci riusciamo non siamo sicuri se ciò non sia dovuto a non aver ancora scoperto un tale algoritmo, o al fatto che l'algoritmo non esista...

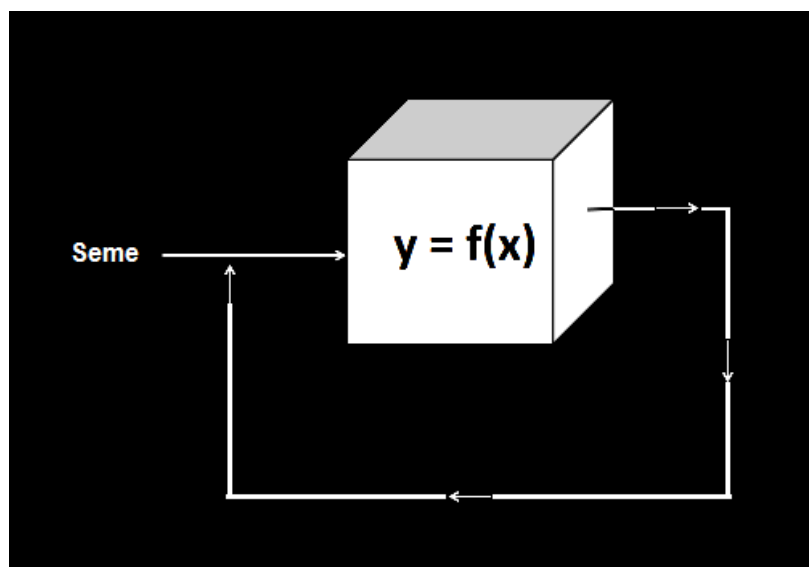
Quest'ultimo punto rende conto della sottigliezza della teoria e ci consiglia di volgere l'attenzione a questioni più concrete.

5. Simulare la casualità

La definizione di causalità come “incomprimibilità” che abbiamo discusso consente teoricamente di definire il concetto, ma non trova la possibilità di un effettivo riscontro pratico: tuttavia è possibile trovare delle misure approssimate per questo tipo di casualità, come per esempio i test statistici che si usano per appurare (entro certe approssimazioni) il carattere casuale di una certa sequenza finita di numeri, e offre degli spunti importanti per capire come definire degli algoritmi che simulino la casualità senza ovviamente ottenerla, i cosiddetti generatori di numeri pseudo-casuali.

Ma cos'è un generatore di numeri pseudo-casuali? E' un algoritmo il cui schema generale è molto semplice: si parte dal primo valore della sequenza pseudo-causale, che si chiama *seme* della sequenza, e, ogni volta che si deve generare un nuovo valore, si applica una stessa funzione al valore generato precedentemente.

In altri termini, un generatore pseudo-casuale si nutre del proprio stesso output: l'input della funzione al passo $n + 1$ è l'output della funzione al passo n .



Si noti che la funzione applicata è ogni volta la stessa. La successione pseudo-casuale generata da un tale algoritmo è la seguente, denotando con x_0 il seme:

$$x_1 = f(x_0)$$

$$x_2 = f(x_1)$$

$$x_3 = f(x_2)$$

...

$$x_n = f(x_{n-1})$$

...

Come è evidente, la successione $x_0, x_1, x_2, x_3, \dots, x_n, \dots$ è completamente determinata da x_0 e dalla funzione f . Questo tipo di algoritmo si chiama anche “mappa iterata” o “equazione alle differenze”.

Naturalmente, tutta la bontà del generatore di numeri pseudo-casuali nel produrre una sequenza che somigli effettivamente a una successione casuale è concentrata nella funzione f , che andrà scelta in modo che:

1. I valori x_n siano (o meglio somiglino a) valori uniformemente distribuiti in un certo intervallo: per esempio fra 0 e 1 se sono numeri decimali o fra 0 e un certo N fissato se sono interi.
2. I valori x_n siano (o meglio comportarsi come se fossero) mutuamente indipendenti.

La 2. non è realmente possibile soddisfarla: va quindi intesa nel senso che il *periodo* della successione pseudo-casuale deve essere il più grande possibile, dove il periodo è il minimo numero di passi dopo il quale la successione torna al valore x_0 e quindi si ripete, un po’ come nella teoria dell’Eterno Ritorno degli antichi Greci e di Nietzsche.

Che un generatore di numeri a caso abbia un periodo finito, cioè che i numeri a un certo punto inizino a ripetersi nello stesso ordine è chiaro per due motivi: poiché si tratta di un algoritmo eseguito da un computer, secondo la definizione che abbiamo dato sopra può trattare solo numeri con un numero finito di cifre, dunque un numero finito di numeri che vengono combinati in un numero finito di operazioni, il che vuol dire che prima o poi il valore di f o diverrà un *punto fisso*, cioè avremo incontrato un x_n tale che $f(x_n) = x_n$ e quindi la successione diventerà costante da quel punto in poi (il che non la rende un buon generatore di numeri pseudo-casuali), oppure il valore di f tornerà ad essere di nuovo x_0 ; essendo una funzione, e quindi deterministica, su x_0 la funzione torna sempre x_1 , su x_1 torna sempre x_2 e così via, quindi non appena il risultato è pari al seme, la successione generata si ripete in modo identico.

Vediamo un semplice esempio di generatore pseudo-casuale, che ha ormai solo un valore storico in quanto è quello inventato da von Neumann negli anni '40, che tuttavia non genera successioni che soddisfano le condizioni precedenti.

Questo generatore considera numeri interi con un numero fissato di cifre: supponiamo per esempio di lavorare con numero di 4 cifre, fra 0 e 9999. La funzione f associa al suo input x il numero di 4 cifre ottenuto prendendo il quadrato di x (che ha otto cifre) e tornandone le 4 cifre centrali¹².

Per esempio se $x = 8921$ allora $x^2 = 79584241$ e quindi $y = 5842$. Partendo dal seme $x_0 = 8921$ troviamo la successione: 8921, 5842, 1289, 6152, 8471, 7578, 4260, 1476, 7857, 7324, 6409, 0752, 5504, 2940, 4360, 0096, 0016, 0006, 0000; da questo punto in poi, dato che ovviamente $f(0) = 0$, la successione diviene costante e non produce più numeri diversi da 0.

Quindi dopo 20 estrazioni di numeri che sembrano in effetti casuali la successione si appiattisce sullo 0. Se andiamo a segnare i numeri estratti sulla retta dei punti fra 0 e 9999 vediamo che comunque sono tutt'altro che uniformemente distribuiti:



Un metodo che si impose nel dopoguerra, e che è stato usato fino a tempi sorprendentemente recenti è il metodo delle “congruenze lineari”.

Una *congruenza* è un’equazione che vale non soltanto se le due quantità eguagliate sono uguali ma anche se i loro resti diviso un certo numero sono uguali: precisamente, diciamo che x è congruo a y modulo n se i resti delle divisioni di x per n e di y per n coincidono, cioè se il resto della divisione di $y - x$ per n è zero. Scriviamo in tal caso

$$x \equiv y(\text{mod } n)$$

Per esempio tutti i numeri pari sono congrui modulo 2 così come tutti i numeri dispari sono congrui modulo 2 mentre un numero pari e un numero dispari non sono mai congrui modulo 2. Un altro esempio: l’aritmetica degli orologi analogici è modulo 24, infatti se sono le 23, fra 5 ore diciamo che sono le 4 proprio perché $4 \equiv 28(\text{mod } 24)$.

Un generatore pseudo-casuale a congruenza lineare è tale che la sua funzione iterata è del tipo

$$f(x_n) = \text{resto della divisione di } ax_{n-1} + b \text{ per } m$$

dove a , b e m sono parametri da cui dipende la funzione, che non mutano durante l’esecuzione dell’algoritmo. Quindi esistono tanti generatori a congruenze lineari quante sono le scelte possibili dei numeri interi positivi a , b e m .

Il principale vantaggio dei generatori a congruenze lineari, ed il motivo della loro popolarità, è che facendo uso di un concetto della teoria dei numeri, quello di congruenza, studiato da oltre duecento anni, possiedono un apparato teorico che consente di definirne alcune importanti proprietà.

¹² La funzione $f(x)$ può descriversi aritmeticamente come: prendi il quadrato di x , dividilo per 100 e prendine il resto della divisione per 10000.

Per esempio si può dimostrare, applicando la teoria dei numeri, che:

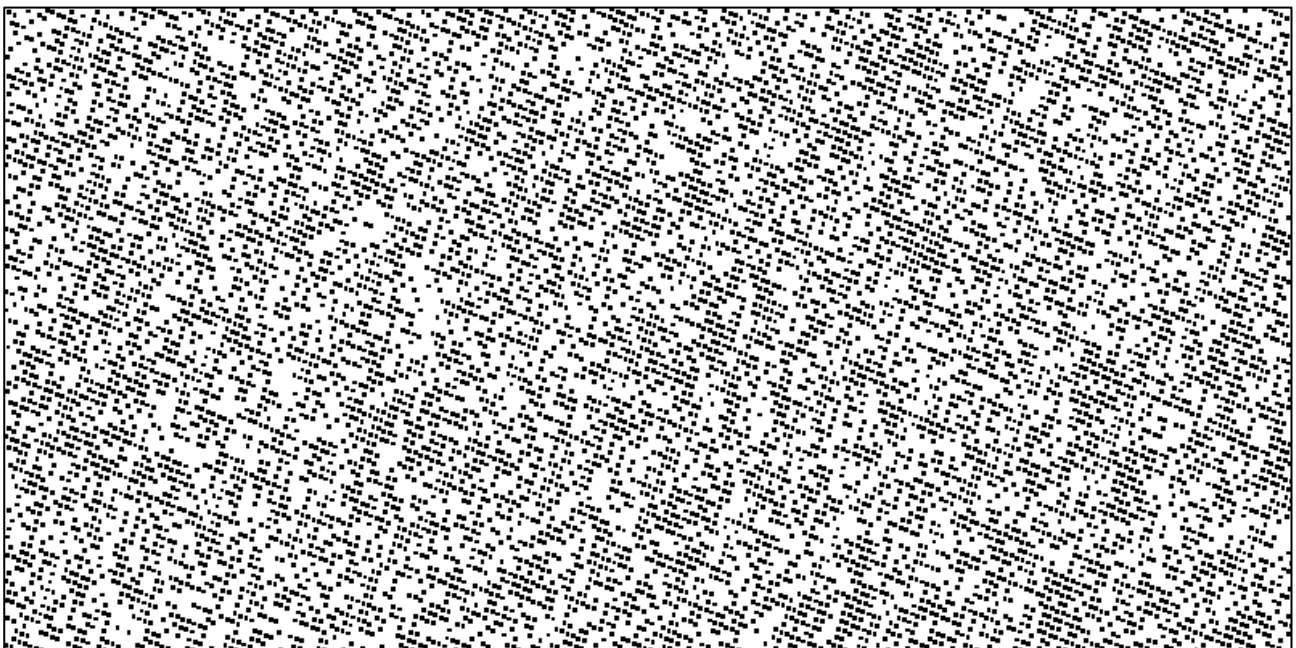
- Se $\text{MCD}(b, m) = 1$, ogni fattore primo p di m divide anche $a - 1$ e, se 4 divide m , allora divide anche $a - 1$ e il periodo del generatore è m .
- Se m è primo, $b = 0$, $x_0 \neq 0$, m divide $a^{m-1} - 1$ ma non divide $a^{k-1} - 1$ per $k = 1, 2, \dots, m - 2$, allora il periodo del generatore è il massimo possibile.

E' anche possibile caratterizzare i generatori di periodo massimo, cioè dire per quali classi di valori a , b , m un generatore ha valore massimo, avvalendosi della teoria delle radici primitive di Carl Friedrich Gauss, un capitolo classico e bellissimo della teoria algebrica dei numeri.

Tuttavia, alla fine degli anni '60, quando questi generatori erano stati utilizzati per simulazioni di ogni tipo, da quelle necessarie ai reattori atomici agli studi sulla popolazione, George Marsaglia scoprì che i numeri generati da questi algoritmi a congruenza lineare seguono uno schema, una regola, un *pattern*, molto stringente e quindi non possono realmente somigliare a una successione realmente casuale.

In particolare, usando i numeri generati da un tale algoritmo a congruenza lineare per formare coordinate di punti in uno spazio a n dimensioni, Marsaglia scoprì che questi punti non riempiono lo spazio in modo uniforme, come ci si aspetterebbe da coordinate "genuinamente" casuali, ma si dispongono su pochi piani, fra loro equidistanti.

Per esempio, considerando il generatore a congruenza lineare caratterizzato dai valori $a = 1103515245$, $b = 12345$, $m = 32768$ con seme $x_0 = 1$ e usando i numeri prodotti per formare le coordinate di punti del piano, andando a disegnare questi punti si ottiene la figura seguente:



Come si vede a occhio, i punti sembrano disporsi su rette diagonali che si dirigono, per intenderci, da Nord-Ovest a Sud-Est.

Un generatore soggetto a questo difetto, RANDU, è stato utilizzato sistematicamente fino agli anni '70 in quanto era il generatore della libreria standard del linguaggio Fortran, massivamente utilizzato nelle applicazioni scientifiche e ingegneristiche.

Lo stesso Marsaglia, e altri studiosi, hanno inventato nuove tecniche, solitamente basate sulla teoria dei numeri (ma non sulla teoria delle congruenze lineari!) per definire generatori più affidabili, dove il grado di affidabilità è legato a dei particolari test statistici che possono essere svolti sulle successioni generate.

Questi test statistici, basati sull'approccio "frequentista" alla probabilità che abbiamo discusso in precedenza, tendono a verificare alcune caratteristiche delle successioni numeriche prodotte da un generatore pseudo-casuale, come per esempio:

1. L'uniformità della distribuzione (se il generatore produce N valori possibili, questi devono comparire più o meno con la stessa frequenza nella sequenza generata).
2. Anche l'uniformità della distribuzione di coppie di valori viene testata in modo analogo.
3. Verificare se il generatore produce sequenze "non truccate" per particolari giochi, come per il poker.

Esiste poi una batteria di test, messa insieme da Marsaglia, il *Diehard Test* che include diverse misurazioni basate sulla statistica e la teoria delle probabilità, per valutare la bontà di un generatore di numeri a caso.

6. Alcune applicazioni

Le nozioni che abbiamo sommariamente riassunto fin qui e la storia della loro scoperta e del loro sviluppo sono di fondamentale importanza in tutti i campi dove si applicano i computer, e quindi praticamente ovunque nel mondo moderno: proveremo in quest'ultimo paragrafo a passare in rassegna alcune aree applicative dove i numeri pseudo-casuali e le tecniche di simulazione si sono rivelate essenziali e continuano a essere quotidianamente impiegate.

Applicazioni tecnico-scientifiche

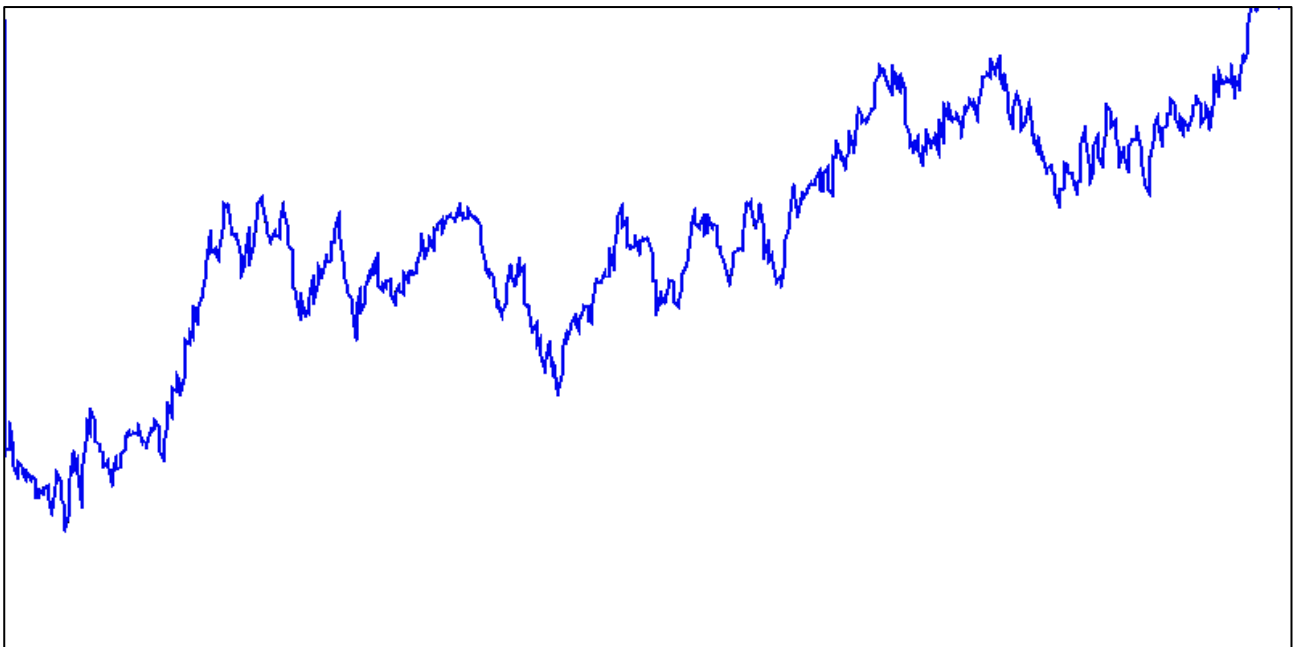
I generatori di numeri pseudo-casuali sono stati inventati insieme ai computer, durante la seconda guerra mondiale, sostanzialmente per poter svolgere simulazioni sia di dinamica dei fluidi che di fisica atomica (per esempio nel risolvere problemi di trasporto dei neutroni con la tecnica di Montecarlo, già usata da Fermi negli anni '30).

Non stupisce quindi che le prime applicazioni dei numeri pseudo-casuali siano state le simulazioni svolte al computer di fenomeni fisici e naturali la cui complessità impediva la determinazione di soluzioni "esatte".

Le simulazioni continuano ad essere fondamentali nella scienza ma anche nell'industria moderna, perché consentono di svolgere calcoli su un oggetto, o su un processo, prima di metterlo effettivamente in piedi e quindi di studiare qualcosa che ancora non c'è con un notevole abbattimento dei costi.

Per esempio è possibile simulare i processi di attesa delle code, che seguono delle distribuzioni particolari, con una precisione che consente, tramite una simulazione Montecarlo, di tracciare gli scenari d'uso di un servizio e quindi di dimensionarne il costo, le tipologie di utenza, etc.

Le tecniche di simulazione sono oggi utilizzate anche in economia, finanza, informatica (per esempio per simulare il comportamento di utenti nel testare i programmi), biologia, ecologia, meteorologia (con tutti i problemi legati all'effetto farfalla e al caos) e in fisica, soprattutto nella fisica delle particelle elementari, ma non solo.



Simulazione di una traiettoria del moto browniano, un modello semplificato per i movimenti dei titoli in borsa per mezzo di numeri pseudo-casuali (simulazione on line dell'autore <http://www.caressa.it/quasipercaso/index.html#59>).

Applicazioni informatiche: intelligenza artificiale

Uno dei primi campi di ricerca nell'uso dei computer è stata l'intelligenza artificiale: questo termine un po' fuorviante indica una collezione di metodi e tecniche matematiche utili per simulare, o emulare, comportamenti "umani" da parte delle macchine.

In altri termini, un sistema di intelligenza artificiale può risolvere un problema apparentemente come lo risolve un umano, solo sfruttando la maggiore memoria e velocità dei computer: per esempio ci sono sistemi automatici di diagnosi medica che analizzano immagini mediche con una

precisione in alcuni casi superiore a quella di medici esperti, altri che formulano diagnosi complete, altri ancora che riescono ad analizzare la letteratura medica, che è sterminata, per corroborare ipotesi diagnostiche.

Tutti gli algoritmi di intelligenza artificiale che non si basano su deduzioni esatte utilizzano numeri casuali: per esempio le cosiddette “reti neurali”, gli “algoritmi genetici”, i metodi di “data mining”, etc.

Una *rete neurale* è un modello matematico iper-semplificato del cervello umano che può essere usato per calcolare funzioni molto complicate per le quali non si conosce nulla se non quanto valgono su un numero limitato di dati di input. Per farlo la rete “scopre” un algoritmo “nascosto” e questo avviene addestrando la rete su dati di prova proposti secondo combinazioni casuali: la casualità delle combinazioni dei dati di addestramento è una condizione cruciale per l’efficacia e l’efficienza della rete.

Un’altra classe di algoritmi di intelligenza artificiale, gli *algoritmi genetici*, offrono modelli matematici di calcolo ispirati alla teoria dell’evoluzione, in cui si cerca di risolvere un problema partendo da una soluzione casuale che viene fatta evolvere in modo da adattarsi al problema, e rimescolandone casualmente la struttura.

In sostanza si fa evolvere una soluzione adattandola a delle condizioni, che sono i vincoli del problema: anche in questo caso la possibilità di generare numeri pseudo-casuali è essenziale.

Questi e altri sistemi di intelligenza artificiale sono oggi impiegati quotidianamente per offrire servizi di vario tipo: per esempio il traduttore automatico di Google, i servizi di suggerimento di acquisti di Amazon, le pubblicità mostrate su Twitter e Facebook utilizzano questi strumenti sofisticati che dipendono tutti dalla possibilità di generare numeri (quasi) a caso.

Applicazioni informatiche: sicurezza su Internet

Un altro ambito di applicabilità degli algoritmi di generazione dei numeri pseudo-casuali è nell’accesso sicuro a sistemi informatici. Oltre ai soliti username e password, per autenticare un utente a un sistema informatico in modo più sicuro, è possibile assegnargli un dispositivo che generi una sequenza pseudo-casuale, o anche mettere il generatore in una *app* per smartphone.

Lo stesso algoritmo e il seme della sequenza sono noti anche al server del sistema sul quale l’utente si deve autenticare: dunque questo server può generare la stessa sequenza e verificare la password “usa e getta” inserita dall’utente che l’ha letta sul dispositivo. Questo metodo è usato per l’*home banking*: la banca dota i propri clienti di un dispositivo (spesso una chiavetta con un display) o di una *app* per cellulare che, quando c’è da compiere una transazione on line, l’utente accende per leggergli un numero, ogni volta diverso, in effetti l’ultimo numero generato della sequenza pseudo-casuale: poiché quest’ultima è deterministica, il server della banca (che ovviamente conosce sia il seme che la funzione del generatore di numeri pseudo-casuali) può ricostruire la sequenza e verificare se il numero immesso corrisponde a quello generato dal dispositivo in possesso dell’utente, e quindi autenticare o meno la transazione.

In questo modo la sicurezza delle credenziali non è legata solo a “ciò che si sa” (username e password) ma anche a “ciò che si ha” (il dispositivo OTP o una *app* su *smartphone* che generi la sequenza casuale associata dal server all’identità digitale dell’utente).

Ma i numeri pseudo-casuali sono anche fondamentali in altri campi che riguardano la sicurezza informatica e che sono indispensabili per il funzionamento delle transazioni su Internet e quindi per un uso della rete che non si limiti alla consultazione dei siti Web ma alla interazione sicura con essi.

Per esempio, tutte le nostre transazioni su Internet (bancarie, social, etc.) sono protette da sistemi di “crittografia a chiave pubblica”: quando sull’indirizzo del sito il prefisso “https” il server del sito e il nostro computer comunicano in modo “sicuro”, scambiandosi un “certificato digitale”. In sostanza, la crittografia a chiave pubblica consente a un utente di cifrare un messaggio avvalendosi di una chiave che solo lui conosce, ma consente anche a tutti gli altri utenti di decifrare il messaggio avvalendosi di una chiave pubblica, che può essere divulgata: il punto cruciale è che la conoscenza della chiave pubblica non consente di ricostruire la chiave privata.

Per ottenere questo, tutto il meccanismo si basa sulla difficoltà di fattorizzare numeri primi molto grandi, che sono utilizzati per produrre le chiavi pubbliche/private che garantiscono la segretezza dei dati.

In questi algoritmi e processi è spesso fondamentale poter generare numeri a caso, anche molto alti: senza questa possibilità non si potrebbero mettere in piedi le infrastrutture di sicurezza che reggono tutto il traffico economico di Internet!!!

Un altro impatto sulla vita quotidiana di ciascuno di noi, quando navighiamo su Internet, è legato alla sicurezza delle connessioni “TCP/IP” di rete, usate dai nostri dispositivi (computer, cellulari, tablet, etc.) per collegarsi a Internet si basa sulla non predicibilità di alcuni numeri con i quali sono etichettate le “transazioni” sulla rete: la sicurezza di una qualsiasi sessione Web è legata a questa imprevedibilità.

Un hacker che sappia in quale linguaggio di programmazione, o in quale infrastruttura, sia implementata una certa applicazione web, e che conosca l’algoritmo del generatore di numeri pseudo-casuali di quel linguaggio, potrebbe sfruttarne eventuali vulnerabilità (è successo con il linguaggio PHP diffuso per i siti Web).

Questi sono solo alcuni dei campi applicativi dove i numeri pseudo-casuali giocano un ruolo chiave, ma basterà pensare anche ai videogame, che generano un volume di affari notevole, dove chiaramente l’elemento di casualità e imprevedibilità rende il gioco interessante e che usano simulazioni e numeri pseudo-casuali per ottenere questi effetti, etc.

In definitiva, i computer e gli altri dispositivi “intelligenti” che ci circondano (e oggi lo sono televisori, lavatrici, automobili, etc.) per la maggior parte del tempo non fanno altro che dare i numeri, quasi per caso.