Un passeig aleatori a l'aritmètica*

Gregory Chaitin**

Déu no juga als daus només en la física, sino també en les matemàtiques pures. La veritat matemática de vegades no es més que un perfecte llançament de moneda.

El concepte d'aleatorietat obsessiona els físics d'avui dia. Fins a quin punt es pot predir el futur? Depèn de les nostres limitacions, o és que predir-lo és impossible per principi? La qüestió de la predictibilitat en física ve d'antic. A principis del segle XIX, les lleis deterministes clàssiques de Newton van fer creure a Pierre Simon de Laplace que el futur de l'univers es por determinar d'un cop per sempre.

Aleshores va aparèixer la mecànica quàntica, la teoria que és ara fonamental per la nostra comprensió de la natura de la matèria. Descriu objectes molt petits, com ara electrons i altres partícules fonamentals. Una de les característiques més polèmiques de la mecànica quàntica era la introducció de la probabilitat i l'aleatorietat en física a un nivell molt bàsic. Això no li agradava al gran físic Albert Einstein, que va dir que Déu no juga als daus.

Després l'estudi modern de la dinàmica no lineal ens ha ensenyat que fins i tot la física clàssica de Newton té l'aleatorietat i la impredictibilitat a la seva base. La teoria del caos, que una sèrie d'articles del *New Scientist* l'any passat descrivia, ens ha fet veure que el concepte d'aleatorietat i impredictibilitat comença a semblar un principi unificador.

Segons sembla, aquest principi es pot aplicar fins i tot a les matemàtiques. Puc fer veure que hi han teoremes relacionats amb la teoria de nombres que no es poden demostrar, perquè quan fem les preguntes adequades, els resultats que obtenim són equivalents a un llançament de moneda.

Els meus resultats haurien sorprès molts matemàtics del segle passat, car creien que les veritats matemàtiques sempre poden demostrar-se. Per exemple, el 1900, el matemàtic David Hilbert va donar una cèlebre conferència en la qual proposà una llista de 23 problemes com un desafiament al nou segle. El sisè problema tenia relació amb establir els axiomes, o veritats bàsiques universals, de la física. Un dels apar-

* Aquest article és la traducció, autoritzada per l'autor, del que va apareixer al *New Scientist* **125** (1990).

** **Gregory Chaitin** és membre del grup de física teòrica del Thomas J. Watson Research Center de Yorktown Heights, New York, que és part de la divisió d'investigació de la IBM.

tats d'aquesta pregunta tocava a la teoria de probabilitat. Per Hilbert, la probabilitat no era més que una eina pràctica, procedent de la física, que ajuda a descriure el món real quan només tenim accés a una quantitat limitada d'informació.

Una altra qüestió que va discutir era el seu 10è problema, que tenia relació amb la resolució de les equacions dites «diofàntiques», així anomenades en honor del matemàtic grec Diofant. Es tracta d'equacions algebraiques en què només hi intervenen nombres sencers. Hilbert demanava: Hi ha alguna manera de saber si una equació algebraica té o no solucions senceres?

Poc s'imaginava Hilbert que aquestes dues preguntes són subtilment relacionades. Això es devia a què ell pressuposava una cosa que era tan bàsica pel seu pensament que ni tan sols la va formular com a pregunta. Es tracta de la idea que tot problema matemàtic té una solució. Potser no som prou llestos o no hem treballat prou el problema, però, en principi, hauria d'ésser possible solucionar-lo. Almenys, això creia ell. Era una situació de blanc o negre.

Ara sembla que Hilbert no tocava gaire de peus a terra. De fet, hi ha una connexió entre el seu sisè problema sobre l'estadística i el desè sobre les solucions de les equacions algebraiques que porta a un resultat força sorprendent, que és: hi ha aleatorietat al cor d'una de les branques más tradicional de les matemàtiques pures, la teoria de nombres.

Les preguntes matemàtiques clares i simples no sempre tenen respostes clares. En teoria de nombres elemental, algunes preguntes sobre equacions diofàntiques tenen respostes completament aleatòries, que semblen més aviat grises que no pas blanques o negres. La resposta és aleatòria perquè l'única manera de demostrar-la és postular cada resposta com un axioma independent addicional. Einstein s'horroritzaria de saber que Déu no juga als daus només en física quàntica i física clàssica, sinó també en la matemàtica pura.

D'on surt aquesta conclusió sorprenent? Hem de tornar a Hilbert. Ell va deixar dit que, quan es fa un sistema formal d'axiomes, hi hauria d'haver un procediment mecànic de decidir si una demostració matemàtica és correcta o no, i el sistema hauria de ser consistent i complet. Consistent vol dir que sigui impossible demostrar un resultat i la seva negació. Complet vol dir que donada qualsevol afirmació, o ella o la seva negació sigui demostrable. En una situació així, un procediment mecànic pot decidir la veritat o falsedat de qualsevol proposició matemàtica.

Hi ha una manera pintoresca d'explicar com funciona aquest procediment mecànic: l'anomenat «algorisme del British Museum». El que es fa —no es pot fer en la práctica perquè no s'acabaria mai— és fer servir el sistema d'axiomes, escrit en el llenguatge formal de les matemàtiques, per verificar totes les demostracions possibles, ordenades de més curta a més llarga i alfabèticament. Es comprova quines segueixen les regles i s'accepten. En principi, si el sistema d'axiomes és consistent i complet, donat qualsevol teorema es pot esbrinar si és cert o fals. L'existència d'un procediment així implica que un matemàtic ja no necessita ser enginyós ni tenir inspiració per demostrar teoremes. Les matemàtiques esdevenen mecàniques.

Evidentment, les matemàtiques no són així. Kurt Gödel, un lógic austríac, i Alan Turing, el pare de l'ordinador, van demostrar que és impossible obtenir una teoria

axiomàtica de les matemàtiques consistent i completa i que no existeix cap procediment mecànic per decidir si una proposició matemàtica arbitrària és certa o falsa, ni per decidir si és demostrable o no.

Gödel va ser el primer que va demostrar, mitjançant la teoria de nombres, l'anomenat «teorema d'incompletitud» (vegi's «The incompleteness of arithmetic», *New Scientist,* 5 november 1987). Però crec que la versió de Turing del teorema és més elemental i més fàcil d'entendre. Turing fa servir el llenguatge de l'ordinador: les instruccions, o programa, que un ordinador necessita per solucionar els problemes. Va demostrar que no hi ha cap procediment mecànic per decidir si un programa arbitrari acabarà algun cop de calcular o no.

Per veure que aquest «problema d'aturada» (*halting problem*) és irresoluble, executem el programa en una màquina de Turing, que és una idealització matemàtica d'un ordinador sense limitacions de temps. (El programa ha de tenir totes les dades dins seu.) Aleshores ens preguntem: «es quedarà calculant per sempre, o acabarà per deturar-se?».

En Turing va demostrar que no hi ha cap conjunt d'instruccions que es pugui donar a l'ordinador, cap algorisme, que pugui determinar si un programa mai es deturarà. El teorema d'incompletitud de Gödel n'és un corol·lari, perquè si no hi ha cap procediment mecànic així, aleshores el sistema d'axiomes no és pas complet. Si ho fos, hi hauria una manera mecànica de repasar totes les demostracions possibles per veure si els programes es paren o no; encara que trigaria molt de temps a fer-ho, és clar.

Per obtenir el meu resultat sobre l'aleatorietat en matemàtiques, tinc prou amb prendre el de Turing i expressar-lo amb altres paraules. El que en trec és una espècie de joc de paraules matemàtic. Encara que el problema d'aturada és irresoluble, podem preguntar-nos per la probabilitat que un programa escollit a l'atzar es deturi. Comencem per fer un experiment imaginari amb un ordinador que, si li donem prou temps, por fer la feina de qualsevol altre ordinador: la màquina de Turing universal.

En comptes de preguntar si un programa concret es detura, considerem el conjunt de tots els programes d'ordinador possibles. Assignem a cadascun una probabilitat de què l'escullin. Cada bit d'informació en el programa aleatori s'escull a cara o creu, una tirada independent per cada bit, de manera que un programa que contingui certa quantitat de bits d'informació, diguem N bits, tindrà una probabilitat de 2^{-N}. Podem preguntar ara quina és la probabilitat que aquests programes es deturin. Aquesta probabilitat d'aturada, diem-li Ω, ens dóna la resposa a la pregunta de Turing de si un programa pararà o no com un nombre entre 0 i 1. Si el programa no para mai, Ω és 0; si sempre para, Ω és 1.

De la mateixa manera que els ordinadors representen els nombres en notació binària, podem descriure Ω com a una tirallonga de zeros i uns. Podem determinar si el seu N-èssim bit és un zero o un u? Altrament dit, podem calcular Ω? No. De fet, puc demostrar que aquesta successió de zeros i uns és aleatòria fent servir la teoria algorísmica de la informació. Aquesta teoria assigna un «grau d'ordre» a cada conjunt d'informacions o dades segons existeixi o no un algorisme que pugui comprimir les dades en una forma més curta.

Per exemple, una tirallonga regular de zeros i uns que descrigui algunes dades com per exemple 0101010101 ... que tingui mil dígits, es pot comprimir en una instrucció més curta: «repeteix cinc-cents cops 01». Una tirallonga completament aleatòria no es pot reduir de cap manera a un programa més curt. Es diu que és algorísmicament incompressible.

La meva anàlisi demostra que la probabilitat d'aturada és algorísmicament aleatòria. No es pot comprimir en un programa més curt. Per treure d'un ordinador N bits del número, cal donar-li un programa que tingui almenys N bits de llarg. Cadascun dels N bits d'Ω és un fet matemàtic independent i irreduïble, tan aleatori com llençar una moneda. Per exemple, hi han tants zeros a Ω com uns. I conèixer tots els bits parells no ens ajuda a conèixer cap dels senars.

El meu resultat, que la probabilitat d'aturada és aleatòria, correspon a l'afirmació de Turing que el problema d'aturada és indecidible, i resulta que se'n pot treure una bona manera de donar un exemple d'aleatorietat en teoria de nombres, la pedra angular de les matemàtiques. Això va sortir d'uns resultats de fa uns cinc anys: James Jones de la universitat de Calgary al Canadà i Yuri Matijasevic de l'institut de matemàtiques Steklov de Leningrad van descobrir un teorema demostrat per Edouard Lucas a França fa un segle. El teorema dóna una manera força natural de convertir una màquina de Turing universal en una equació diofàntica universal que és equivalent a un ordinador de propòsit general.

Se'm va acudir que tindria gràcia escriure-la explícitament, així que amb l'ajut d'un ordinador gran vaig escriure una equació de màquina de Turing universal. Tenia 17000 variables i ocupava 200 pàgines.

L'equació és d'un tipus anomenat «diofàntiques exponencials». Totes les seves variables i constants són sencers no negatius, 0, 1, 2, 3, 4, 5, etc. En diuen «exponencial» perquè conté nombres elevats a potències senceres. En les equacions diofàntiques normals, l'exponent ha d'ésser una constant, però en aquesta, pot ésser una variable, així que a més a més de tenir X^3, també hi ha X^Y.

Per a convertir l'afirmació que la probabilitat d'aturada és aleatòria en una afirmació sobre l'aleatorietat de les solucions en aritmètica, només em va caldre fer uns petits canvis en aquesta equació diofàntica de màquina de Turing universal. El resultat, la meva equació que presenta exemples d'aleatorietat, també té 200 pàgines de llarg. Té un sol paràmetre, la variable N. Per cada valor particular d'aquest paràmetre, faig la següent pregunta: «la meva equació, té un nombre finit o infinit de solucions?». Respondre aquesta pregunta resulta ésser tan aleatori com calcular la probabilitat d'aturada. La resposta «codifica» en llenguatge matemàtic si el N-èssim bit de Ω és zero o u. Si és zero, la meva equació, per aquest valor de la N, té un nombre finit de solucions. Si és u, aleshores l'equació per aquest valor particular del paràmetre N té un nombre infinit de solucions. I com que el N-èssim bit d'Ω és aleatori (un fet independent i irreduïble com un llençament de moneda) també ho és el que la meva equació tingui un nombre finit o infinit de solucions. Mai no se sap.

Per trobar si el nombre de solucions és finit o infinit en casos particulars, per exemple, per k valors del paràmetre N, hauríem de postular les k respostes com k axiomes addicionals independents. Hauríem d'afegir k bits d'informació al nostre

sistema d'axiomes, així que no hi guanyaríem res. Aquesta és una altra manera de dir que els k bits d'informació són fets matemàtics irreduïbles.

He trobat una forma extrema d'aleatorietat, o irreduïbilitat, a les matemàtiques pures, en una part de la teoria de nombres elementals associada al nom de Diofant i que té dos mil anys d'antiguitat. Hilbert creia que la veritat en matemàtiques era blanc o negre, que les coses eren o vertaderes o falses.Crec que el meu treball fa que les coses semblin grises, i que els matemàtics aniran a fer companyia als seus col·legues de física teòrica. No em sembla que això hagi d'ésser necessàriament dolent. Hem vist que en la física clàssica i en la quàntica, l'aleatorietat i la impredictibilitat són fonamentals. Crec que aquests conceptes també es troben al bell mig de les matemàtiques pures.

Bibliografia

G. J. Chaitin, «*Information, Randomness and Incompleteness*». Second Edition, World Scientific, Singapore, 1990.
G. J. Chaitin, «*Algorithmic Information Theory*». Third printing, Cambridge University Press, Chicago, 1990.