Gener 2015

Facultat de Matemàtiques i Estadística - C. de Pau Gargallo, 5. - 08028 Barcelona Tel. 93 401 58 80 www.fme.upc.edu Núm. 136

DL. B-37340-2005 - Edició impresa: ISSN 1885-0790 - Edició en Internet: ISSN 1885-1371

• Llibres

La ressenya d'aquest llibre ens ha estat tramesa amablement per un professor del Departament de Matemàtica Aplicada I. Des de la redacció convidem als lectors del Full a escriure ressenyes de llibres o pel·lícules de tema relacionat amb les matemàtiques o amb la ciència en general i les publicarem.



Matt Haig
Els Humans, Editorial Empúries, 2014.

"Els humans" és una d'aquelles novel·les sobre la qual us interpel·laran ben aviat, si encara no han fet. Així la vaig descobrir jo ara fa un mes, i en faig una ressenya per tenir-vos preparats. Us en parlaran perquè es tracta d'una història que pren les matemàtiques com a eix central d'una civilització *avançada*. En realitat, però, i tal com diu el seu autor, és una novel.la sobre l'esfereïdora bellesa de ser humà o, dit d'una altra manera, és un relat que va al cor de les virtuts i inconvenients de la imperfecció humana. Està escrita en un registre irònic que en fa una lectura divertida i ens explica la missió d'un alienígena que vol impedir el desenvolupament tecnològic de l'espècie humana, amb l'argument que massa coneixement en mans dels maldestres humans seria com regalar una arma a un assassí en sèrie. I resulta ser que el perill més gran per a aquest desenvolupament és la conjectura de Riemann, que acaba de ser demostrada (al llibre, és clar!) per un matemàtic britànic. Substituir el matemàtic en qüestió, eliminar la demostració i aturar el progrés consegüent immergiran el nostre alienígena, inesperadament, en un procés d'humanització. Desafortunadament, el llibre no ens explica el perquè d'aquesta relació causa-efecte entre la conjectura de Riemann i el progrés, ni fa un al·legat racional del fet que les matemàtiques siguin el motor d'una civilització *avançada*. No obstant, el sol fet que les situï en el cor de la novel.la és com obrir una finestra d'aire fresc (interestel·lar, és clar) en l'entorn en què vivim, on la difusió de la ciència té un impacte tan baix. A més, col·loca les matemàtiques al centre del coneixement; ho fa amb frases enginyoses com "Els telenotícies haurien de començar parlant de matemàtiques, després de poesia i a continuació de la resta de coses", "La història i la literatura són branques de la matemàtica",... L'Editorial Empúries ha tingut cura de l'edició en català, amb una traducció d'Esther Roig que fa molt plaent la lectura. Molt recomanable, no només per als del *gremi*, sinó per al públic en general, que potser així valorarà una mica més les matemàtiques, encara que només sigui per temor!

• Pel·lícules

The Imitation Game
Director: Morten Tyldum

La pel·lícula és un *biopic* de l'Alan Turing, el matemàtic anglès conegut per haver definit el que ara anomenem màquines de Turing, haver contribuït decisivament a desxifrar els missatges de l'exèrcit alemany codificats amb la màquina Enigma durant la segona guerra mundial i haver estar el primer a parlar d'intel·ligència artificial. El personatge de Turing està interpretat per Benedict Cumberbatch, protagonista també de la sèrie de televisió *Sherlock*, de gran èxit al Regne Unit. La pel·lícula està nominada per 8 òscars, entre ells el propi Cumberbatch com a millor actor. El guió (també nominat) està basat en la biografia d'Andrew Hodges *Alan Turing: The Enigma,* i la segueix de manera força fidel, si

bé alguns detalls històricament correctes estan molt dramatitzats. Algunes escenes no històricament certes semblen tretes de la novel·la *Enigma*, de Robert Harris. Però si fem un capmàs de tot, és una pel·lícula molt recomanable.



Potser és interessant recordar el context històric i tècnic. La màquina Enigma és una patent de 1918 que al llarg dels anys vint va esdevenir el producte de referència per a l'encriptació de correspondència comercial. En començar la segona guerra mundial era la màquina estàndard per encriptar comunicacions de les forces armades del Tercer Reich. El xifrat Enigma estava basat en el principi de substitució polialfabètica a partir de la configuració inicial. El nombre de configuracions inicials de la màquina era molt gran i això la feia pràcticament inatacable. La màquina era reversible en el sentit que, amb la mateixa configuració inicial, entrar el text xifrat donava directament el text en clar. El problema era, naturalment, conèixer la configuració inicial o deduir-la a partir d'un missatge en clar i la seva versió xifrada. La intel·ligència britànica va centrar els esforços per desxifrar l'Enigma a Bletchley Park, una mansió victoriana situada uns 80 km al nord de Londres.
Entre 1938 i 1939 els serveis secrets polonesos havien desenvolupat diversos mètodes per atacar el problema i havien dissenyat unes màquines electromecàniques que provaven un seguit de configuracions inicials fins a trobar la que convertia el text en clar en el text xifrat. Aquestes màquines van ser adaptades a Bletchley Park (amb alguna diferència de disseny) i van ser decisives per a la intel·ligència aliada: amb el seu ajut es desxifraven de manera quasi rutinària les comunicacions de l'exèrcit de terra i de la força aèria. L'anomenada Enigma naval, utilitzada pels submarins que operaven a l'Atlàntic, era més complicada i es van patir períodes llargs sense poder desxifrar cap missatge.
Tema a part eren les comunicacions entre l'Alt Comandament alemany a Berlin i els diversos caps militars a tota Europa. Aquestes comunicacions es feien a través de la màquina Lorenz i oferien molta més seguretat. Per tal de desxifrar els missatges Lorenz, es van dissenyar els primers ordinadors electrònics (Turing, Flowers i d'altres) anomenats Colossus, els circuits dels quals utilitzaven unes 1500 vàlvules electròniques. A principis de 1944 un Mark Colossus I ja era operacional a Bletchley Park i a mitjan 1944 se n'hi va afegir un segon.
Visitar aquest centre, avui museu, és una opció interessant des del punt de vist del turisme històric-científic. Cal comptar tot un dia entre el viatge d'anada i tornada: els trens que surten de London Euston triguen entre 30 i 60 minuts i la casa està a 10 minuts a peu de l'estació Bletchley Park, però la visita és llarga si es vol fer amb deteniment. Es poden trobar detalls i horaris al web http://www.bletchleypark.org.uk/.
Proposem tot seguit una bibliografia bàsica imprescindible. A [2] i [4] hi ha molts detalls tècnics dels mètodes utilitzats a Bletchley Park.

[1] David Kahn, *Seizing the Enigma*, Houghton Mifflin, 1991.
[2] F. H. Hinsley, A. Stripp (eds.), *Codebreakers: The Inside Story of Bletchley Park*, OUP 2001.
[3] Michael Smith, *Action This Day*, Transworld Distribution, 2003.
[4] Gordon Welchman, *The Hut Six Story*, Classic Crypto Books, 1997.

• Divertiments

Es fan tirades amb un dau estàndard fins que surt un sis, llavors s'atura l'experiència. A cada tirada del dau llencem a l'aire una moneda i anem portant el recompte del nombre de cares menys el nombre de creus que han sortit. Es demana la probabilitat que el valor absolut d'aquest recompte no hagi pres mai el valor 3. Per exemple, si el dau ha sortit 5, 1, 4, 6, i la moneda 0, 0 ,1, aleshores el recompte és 1, 2, 1 i mai ha valgut 3.

Envieu les vostres respostes argumentades abans del 20 de febrer a elfull.fme@upc.edu, o bé per correu a «El Full. FME. Edifici U. Campus Sud.»
Premi al guanyador: un exemplar del llibre ressenyat en aquest Full.
Solució al problema d'octubre: Observem primer que podem estendre la successió de Fibonacci cap enrere, amb $F_0 = 0$, $F_{-1} = 1$, $F_{-2} = -1, \cdots$. Considerem els termes de la successió mòdul 10^9, que seguim anomenant F_n. Considerem el conjunt de parelles de la forma (F_n, F_{n+1}), amb $1 \leq n \leq 10^{18} + 1$. Com a molt hi ha 10^{18} parelles diferents (F_i, F_j), per tant existeixen n i m tals que $(F_n, F_{n+1}) = (F_m, F_{m+1})$. D'on resulta $F_{n-1} = F_{m-1}$ i, tirant enrera, $F_{-2} = F_{m-n-2}$. Aquest darrer terme acaba en nou nous.
Solucions rebudes: s'ha rebut una solució correcta del divertiment de novembre tramesa per Josep Bonet, que per tant és el guanyador.