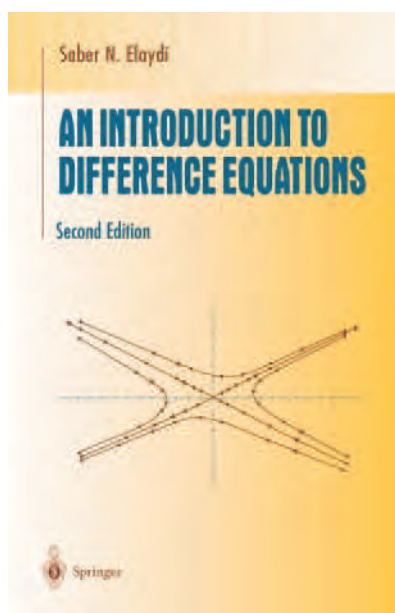


An introduction to difference equations

Autor: SABER N. ELAYDI

«Undergraduate Texts in Mathematics», Springer-Verlag, 1999 (2a ed.).

Les equacions en diferències (EeD) apareixen de manera natural en problemes d'aritmètica, anàlisi clàssica, anàlisi numèrica, sistemes dinàmics, teoria de control, processos estocàstics i, evidentment, en qualsevol disciplina científica on la modelització discreta de fenòmens que evolucionen en el temps tingui un paper rellevant. Potser aquesta diversitat fa que no sigui fàcil trobar fonts que presentin un discurs sistemàtic d'estudi de les EeD. No és aquest el cas del llibre que ressenyem, i la nostra opinió és que aquesta és la seva principal virtut.



Aconsellem la consulta del llibre al lector que desitgi introduir-se en l'àmbit de les EeD. Però com que l'obra es presenta com un manual d'EeD per a un curs de llicenciatura, o com a font complementària d'un curs de teoria de control, creiem que serà de gran utilitat al professor que vulgui preparar un curs sobre la matèria. En aquest sentit, un curs bàsic quadrimestral per a llicenciats en matemàtiques o en física es podria preparar a partir dels capítols 1 al 4, amb algunes de les aplicacions del capítol 6. D'especial interès per a aquells que hagin de preparar cursos avançats de matemàtiques en

carreres o programes de doctorat d'enginyeria, són els capítols 5 i 6, dedicats a la transformada Z —la versió discreta de la transformada de Laplace— i a la teoria de control, respectivament. Recomanem, doncs, que estigui present a les biblioteques de les nostres universitats. Pensant en els estudiants, el nostre parer és que per seguir el llibre cal haver consolidat els coneixements elementals de l'anàlisi i de l'àlgebra lineal. Per l'estructura del llibre, els serà molt més còmoda la lectura a aquells que hagin seguit un curs estàndard d'equacions diferencials ordinàries (EDO). Això és per què els continguts dels capítols 1 a 4 es presenten d'una manera anàloga a com es presenten els continguts en els manuals usuals d'EDO.

El capítol 1 conté una recopilació de la terminologia pròpia de les EeD (punt d'equilibri, punt periòdic, cicles, atractors, diferents tipus d'estabilitat, diagrames de *teranyina* i de bifurcació), presentada a través de l'estudi de diferents exemples d'EeD de primer ordre que provenen de camps diversos.

En el capítol 2 s'examinen les tècniques de resolució d'EeD lineals: es presenta el mètode dels coeficients indeterminats i els mètode de variació de les constants. El capítol 3 està dedicat a l'estudi dels sistemes lineals. S'introdueix la notació matricial, s'obté la fórmula de variació de les constants, i es presenta la teoria de Floquet per a sistemes d'EeD lineals periòdics. El capítol acaba presentant aplicacions dels continguts a l'estudi de cadenes de Markov, de l'equació de la calor discreta i d'un model que explica l'evolució del comerç entre dos països. El capítol 4 conté una exposició clàssica de teoria d'estabilitat per a EeD. En primer lloc es fa una anàlisi dels retrats de fase i s'estudia l'estabilitat per sistemes lineals. També es presenta el segon mètode de Liapunov (o mètode de les funcions de Liapunov), i s'enuncia el teorema de Hartman-Grobman.

La transformada Z és una eina d'anàlisi d'EeD lineals molt emprada al món de l'enginyeria de control, les telecomunicacions i el pro-

cessament de senyal. De fet, és l'anàleg discret al que representa la transformada de Laplace per a les EDO lineals. La transformada Z es presenta i s'estudia en el capítol 5. Cal advertir als estudiants que per llegir aquest capítol és necessari tenir una mica frescos els coneixements bàsics de nombres complexos. Com a continuació natural d'aquest capítol, en el capítol 6 es presenta una interessant introducció a la teoria de control en temps discret.

Els capítols 7 i 8 tenen un caràcter més específic. El capítol 7 es dedica a l'estudi de les solucions que oscil·len al voltant d'un punt d'equilibri (teoria d'oscil·lacions) i el capítol 8 es

dedica a l'estudi del comportament asimptòtic de les solucions de les EeD. El capítol 9 té un cert caràcter miscel·lani: es presenten algunes aplicacions de les EeD per a l'estudi de les fraccions contínues i per a l'estudi dels polinomis ortogonals.

Saber N. Elaydi és professor de la Universitat de San Antonio, Texas. És també autor d'una llarga llista d'articles de recerca, i editor de la revista *Journal of Difference Equations and Applications*, de la qual recomanem especialment la seva secció «Open problems and conjectures», que coordina G. Ladas.

Víctor Mañosa,
UPC

Stamping through mathematics

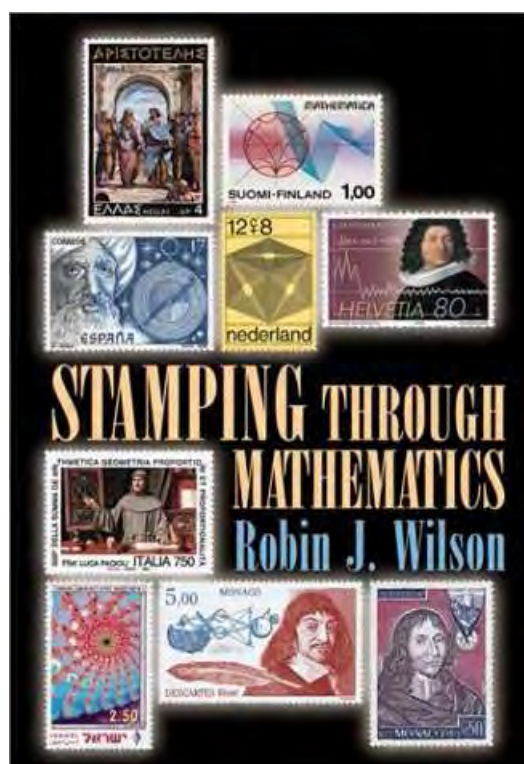
Autor: R. J. WILSON
Springer-Verlag, 2001.

Robin J. Wilson és professor del Keble College d'Oxford i de l'Open University, interessat per la popularització de les matemàtiques. Des del 1984 col·labora a l'«Stamp Corner» de la revista *The Mathematical Intelligencer*.

Per l'autor, els segells de correus constitueixen una manera atractiva per ensenyar les matemàtiques i el seu desenvolupament. Per això el subtítol, «Una història il·lustrada de les matemàtiques al voltant dels segells», ja ens diu que el llibre no és un catàleg sobre filatèlia matemàtica. Es tracta de fer un recorregut, explícitament no convencional, per la història de les matemàtiques, mostrant com aquesta ha quedat reflectida en els segells de correus de tot el món. La idea és molt bonica: penseu que aquests segells ens donen algunes indicacions per entendre què ha transcendit de la nostra ciència a la societat, i quins són els matemàtics que la gent coneix i reconeix. En certa manera, i al meu entendre, l'autor ens presenta una «històriapop» de les matemàtiques.

El llibre és una bonica *delicatessen*. Hi abunden les fotografies a tot color (d'uns quatre-cents segells en total), a on trobareu matemàtics insignes, segells d'homenatge a certs resultats, segells a on apareixen objectes matemàtics de gran bellesa plàstica. Tot això ex-

posat seguint un ordre històric, i acompanyant les fotografies dels segells amb comentaris explicatius sobre els continguts dels segells i el seu context.



Així doncs, com a qualsevol manual d'història, hi trobarem apartats dedicats a la matemàtica grega, xinesa, inca, maia, la matemàtica islàmica, l'edat mitjana d'Occident, el Renaixement, el segle XVII a França, l'emergència de l'àlgebra i la geometria al segle XIX, fins arribar a la matemàtica i la física del segle XX. Hi trobarem també apartats dedicats als calendaris, a l'*astronomia nova* de la revolució científica, a la matemàtica i l'art del Renaixement, els jocs del go i els escacs, la naturalesa

i la matemàtica. . . , això i més.

L'obra és imprescindible per als aficionats a la filatèlia matemàtica (o científica en general), però és també un bon complement (lúdic si voleu) per a aquells que estiguin interessats en la història de les matemàtiques. En definitiva, ens trobem al davant d'una llaunadura, que potser no alimenti gaire, però que innegablement dóna plaer. En la mesura que els pressupostos ho permetin, seria bo que estigués present a les nostres biblioteques.

Víctor Mañosa
UPC

Chance rules: An informal guide to probability, risk, and statistics

Autor: BRIAN S. EVERITT
Springer-Verlag, Nova York, 1999.

L'autor és cap del Departament de Bioestadística i Informàtica de l'Institut de Psiquiatria, del King's College de Londres. És autor de trenta llibres d'estadística; aquí en tenim alguns exemples:

- *Cluster analysis*. Halsted Press, Nova York (diverses edicions).
- *The analysis of contingency tables*. Chapman and Hall, Londres (diverses edicions).
- *The Cambridge dictionary of statistics in the medical sciences*. Cambridge University Press, Cambridge, 1995.
- *The Cambridge dictionary of statistics*. Cambridge University Press, Cambridge, 1998.

En tot cas, quan un té a les mans un llibre i dubta si el vol comprar, normalment en llegeix el resum que surt a la contracoberta. Em permeto citar una part d'aquest resum, traduïda de l'anglès:

«... *Chance rules* explica la història de la nostra apreciació de l'atzar al llarg dels segles i les diverses maneres que aquest afecta les nostres vides. Llegireu sobre els primers jugadors que pensaven que la caiguda d'un dau estava controlada pels déus, així com sobre un genètic modern o un investigador de la teoria quàntica que intenten integrar alguns aspectes de la probabilitat a les àrees que han escollit. Sobre la

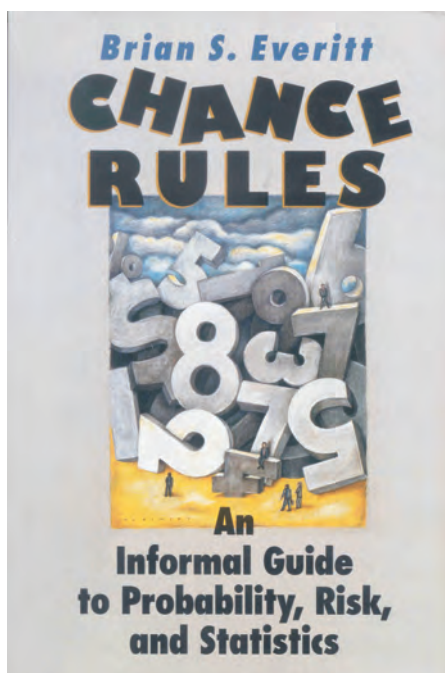
marxa, l'autor utilitza molts exemples interessants per il·lustrar diversos aspectes de l'atzar, com ara el problema desconegut de Monty Hall, tirada de monedes, coincidències, curses de cavalls, aniversaris i fills, descripció de DNA, riscos relacionats amb la salut, assaigs clínics, teràpies alternatives.

Aquest llibre, ben escrit i fàcil de comprendre, us enganxarà a aquest camp interessant i aviat sereu vosaltres els que contareu els vostres propis acudits sobre l'atzar. . . »

Després d'haver llegit un resum com aquest, és lògic que un comenci a mirar els continguts i en trobarà els apartats següents: «Breu història de l'atzar». «Tirar monedes i tenir fills». «Dau». «Apostar per divertir-se: loteries i travesses de futbol». «Jocs "seriosos": ruleta, naips, curses de cavalls». «Boles, aniversaris i coincidències». «Probabilitat condicionada i l'Honorable Thomas Bayes». «Probabilitats que desconcerten». «Prendre riscos». «Estadístics, estadística i medecina». «Teràpies alternatives: panacees o placebo?». «Atzar, caos i cromosomes.» A més, fullejant el llibre hi veureu dibuixos divertits, fotos i gravats, de manera que segurament en demanareu preu al llibreter. Us emportareu el llibre i, sens dubte, no ho lamentareu, ja que el llibre s'ho mereix.

Per començar, es dóna un repàs no gaire llarg, però molt interessant, dels jocs de l'atzar que, segons l'autor, van esdevenir, com a

mínim, 3.000 anys abans de Jesucrist. Es fa referència al primer objecte, l'anomenat *astragalus*, l'os lleugerament retocat de turmell d'ovella o qualsevol altre dels artiodàctils, que s'utilitzava com a element de l'atzar. Es reproduïx una pintura mural d'una tomba egípcia que representa una persona noble en la seva vida postmortal utilitzant l'astràgal en un joc de taulell. Entre els exemples de jocs d'atzar en les èpoques i pobles diferents, crida l'atenció el que diu que en la comunitat jueva els rabins sovint veïen aquests jocs amb mals ulls, i els jugadors es consideraven lladres. Curiosament, el problema no era el joc per si mateix, sinó el fet que el guanyador s'emportava tot el guany sense pagar una recompensa justa! Així, de forma distesa i entenedora, l'autor porta el lector pel món de les probabilitats i estadístiques, sense deixar al marge les probabilitats freqüentista i subjectiva. No abusa de fórmules, però se'n donen algunes, com diu l'autor al prefaci, «ignorant la precaució de Stephen Hawking que cada equació inclosa en un llibre redueix a la meitat les seves vendes».



El que sí augmenta les vendes és la inclusió de fets interessants i poc coneguts. Per exemple, durant set generacions de la família Pitofsky, als Estats Units, més d'un segle, segons el diari *New York Times*, naixien només nens. L'any 1959 va néixer el quaranta-setè (!) nen consecutiu, tot i que l'autor expressa certes reserves respecte de la veracitat d'aquesta informació.

El capítol dedicat a coincidències presenta una comparació molt curiosa sobre Abraham Lincoln i John Fitzgerald Kennedy, dos presidents nord-americans víctimes dels dos assassinats més tràgics en la història dels EUA. En reproduïm només alguns fets:

1. Lincoln va ser elegit al Congrés l'any 1846 i Kennedy, l'any 1946.
2. Lincoln va ser elegit president l'any 1860 i Kennedy, l'any 1960.
3. Tots dos van ser assassinats en divendres, en presència de les seves dones.
4. Tots dos van ser rellevats per un president que es deia Johnson de cognom, ambdós demòcrates del sud i senadors amb anterioritat.
5. Pel que fa als presidents successors, Andrew Johnson va néixer l'any 1808 i Lyndon Johnson, l'any 1908.
6. L'assassí de Lincoln, John Wilkes Booth, va néixer l'any 1839 i el de Kennedy, Lee Harvey Oswald, l'any 1939.

En aquest capítol se cita un dels estadístics més importants del segle XX, R. A. Fisher, que ha dit que allò que tingui «una possibilitat sobre un milió sens dubte passarà, amb ni més ni menys que la seva freqüència adient, la nostra sorpresa és, però, que ens hagi passat *a nosaltres*». Per tant, s'ha de distingir entre esdeveniments rars i impossibles (a més, tenint en compte que el fet que un esdeveniment és impossible, és a dir, té probabilitat zero, no significa que sigui *buit!*).

Alguns capítols del llibre estan dedicats a aplicacions mèdiques de probabilitat i estadística, la qual cosa no sorprèn si recordem el càrrec que ocupa l'autor. S'hi arriba a parlar de teràpies alternatives, homeopatia, DNA i genoma, mantenint sempre la manera informal d'exposició, la qual cosa ajuda molt que el lector s'enriqueixi amb fets i problemes reals. Per acabar, vull proposar tres problemes del capítol «Probabilitats que desconcerten».

- a) Li truca a la porta una nova veïna per demanar-li una tassa de sucre. Vostè li demana si té fills. Diu que en té dos. «Algun noi?», pregunta vostè. Sí, diu, i se'n va.

- b) Li truca a la porta una nova veïna per demanar-li una tassa de sucre. Vostè li demana si té fills. Sí, diu, un de cinc anys i un altre de nou. «El més gran és un noi?», demana vostè. Sí, diu, i se'n va.
- c) Li truca a la porta una nova veïna per demanar-li una tassa de sucre. Vostè li demana si té fills. Diu que en té dos. «Algun noi?», pregunta vostè. Sí, diu, i se'n va. L'endemà la veu al carrer amb un fill petit. «És seu el nen?», li demana. Sí, contesta.

En cadascun dels tres casos es demana la probabilitat que tots dos fills de la veïna siguin nois, suposant que la probabilitat que neixi un noi és 0,5 i que el sexe d'un nen noutat no depèn del sexe dels fills anteriors de la família. Espero que no us desconcertin aquestes probabilitats, per cert, iguals a $1/2$, $1/3$ i $1/2$, i que els vostres alumnes també perdin la por a les probabilitats i estadístiques que sovint els espanten molt més del que cal!

Vladimir Zaiats
UV i UAB

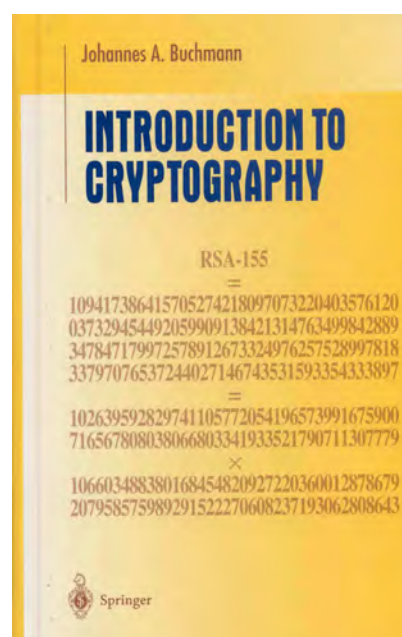
Introduction to cryptography

Autor: JOHANNES A. BUCHMANN
Springer-Verlag, Nova York, 2001.

Aquest és un llibre agradable. L'autor, Johannes A. Buchmann, és editor associat del *Journal of Cryptology* i professor del Departament d'Informàtica i Matemàtiques de la Universitat Tècnica de Darmstadt. En la introducció se'ns diu que «aquest llibre està pensat per als lectors que volen aprendre els algorismes criptogràfics moderns i no tenen una gran preparació matemàtica prèvia». De manera que els dos primers capítols forneixen el lector de tota la maquinària necessària per poder entendre en profunditat aquesta estranya disciplina que s'atreveix a reunir sota un mateix sostre teoria de nombres i tecnologia punta.

En el primer capítol es presenten els fets més elementals de l'aritmètica, des de la divisibilitat d'enters fins a l'algorisme estàndard d'Euclides. S'hi introdueixen les notacions O - i Ω - i s'utilitzen amb especial cura a l'hora d'avaluar el cost computacional de les operacions elementals. Tots els resultats estan escrupolosament demostrats i se segueix l'esquema clàssic definició-teorema. I malgrat tot la lectura és amena, gràcies a una gran quantitat d'exemples (concebuts, sens dubte, per donar suport als lectors amb formacions acadèmiques no estrictament matemàtiques). Amb el mateix esperit, el capítol 2 introdueix les congruències, l'anell de classes residuals, els conceptes de cos, grup i subgrup (ordre d'un element, ciclicitat, generadors), els teoremes petit de Fermat i xinès de la resta, l'anell de polinomis sobre un cos.

El capítol 3 presenta els conceptes i la nomenclatura propis d'aquesta disciplina. Es descriuen alguns sistemes de xifratge de l'era pretecnològica (Vigenère, Hill, transposició) amb llenguatge modern, i alguns exemples de xifratge en bloc, que serveixen de preparació per al capítol 5, on s'explica exhaustivament el criptosistema DES, el més utilitzat durant els darrers vint-i-cinc anys.



El capítol 4 enuncia i prova el famós teorema del secret perfecte de Shannon. Per fer-ho calen alguns conceptes de teoria de probabilitats. L'autor no s'està de res i, en quatre

pàgines, introdueix de manera entenedora la probabilitat condicional, els esdeveniments independents, el teorema de Bayes i la «paradoxa dels aniversaris».

Els capítols 6, 7, 8 i 9 conformen una unitat dedicada als sistemes de clau pública. Els capítols 6 i 8 analitzen la dificultat de factoritzar un enter extremadament gran. Hi apareixen els patològics nombres de Carmichael i els tests de Fermat i Miller-Rabin, que ens permeten afirmar, amb probabilitat alta, que un enter donat és primer. Els capítols 7 i 9 estan dedicats a la descripció dels dos sistemes de clau pública més importants: RSA i ElGamal. I també a la del protocol d'intercanvi de claus de Diffie-Hellman. De tots aquests algorismes, se n'avalua la seguretat i se'n compara l'eficiència. Aquí l'autor també juga fort i ens trobem amb aquesta perla: «it may very well be that someone already knows an efficient fac-

toring algorithm and that RSA is insecure.»

Els capítols 10 i 11 introdueixen les funcions de compressió, la necessitat d'evitar la suplantació de personalitat mitjançant la signatura electrònica, i la implementació de l'algorisme DSA de signatura digital.

Finalment, s'agraeix especialment el contingut dels capítols 12, 13 i 14, que tracten, encara que breument, temes que habitualment es deixen de banda en els textos clàssics de criptografia elemental: construcció de grups finits en els quals és difícil resoldre el problema del logaritme discret, identificació i gestió de *passwords*, autoritats certificadores.

Cada capítol consta d'una extensa llista de problemes de tota mena: fàcils, difícils, divertits, de programació, purament matemàtics. La meitat dels exercicis proposats estan resolts en un apèndix final.

David Juher
Universitat de Girona

Problemes

Abans de parlar dels problemes, permeteu-me que em presenti. Sóc en Carles Romero, i, a partir d'aquest número del *Notícies*, em faig càrrec d'aquesta secció. He rebut tots els protocols, arxius i benediccions d'en Pelegrí Viader, qui se n'encarregava fins ara, i em llenço a l'aventura de seguir oferint-vos aquestes racions de *tapes*, que, espero, trobareu prou saboroses.

Bé, parlem de problemes de matemàtiques: del problema A46, no n'hem rebut cap solució. Un acostament naïf porta a quatre pesades com a mínim, però no és gaire arriscat sospitar (i el proposant ho creu) que es pot fer en tres. Així doncs, el tornem a proposar tot animant-vos a rerumiar-lo.

I, com ja es feia abans, preguem als nostres lectors que, si fan servir $\text{\TeX}$ o $\text{\LaTeX}$ per escriure les seves solucions, les enviïn per correu electrònic a: (cromero@pie.xtec.es) així com qualsevol proposta o suggeriment. (Sí, és clar, *abans* s'enviava a *una altra* adreça!)

Problemes proposats

A46. (Proposat per Jordi Ramoneda, Valldoreix.) Tenim 12 boles iguals i indistingibles en tot llevat del pes, ja que una d'aquestes pesa diferent de les altres, no sabem si més o menys. Disposem d'una balança de dos plats. Quin és el mínim nombre de pesades que ens cal fer per tal de trobar la bola diferent?

A50. (Proposat per Pelegrí Viader, UPF.) Inspirat en l'article de G. Polya «On the Harmonic Mean of Two Numbers», *The American Mathematical Monthly*, vol. 57, núm. 1, gener 1950, p. 26–28.) En Joan fa la següent juguesca amb la Joana: «tria un nombre real qualsevol entre 9 i 11 (extrems inclosos); si t'equivoques en més del 10%