Quins nombres depassen el miler de trilions?

Els resultats de la teoria de nombres són d'aquells resultats matemàtics dels quals, per la seva espectacularitat, els diaris parlen arreu. L'exemple més recent és l'anunci, fet per Andrew Wiles el 23 de juny del 1993 al Newton Institut de Cambridge, de la demostració de la conjectura de Fermat. Des de fa més de tres-cents cinquanta anys, aquest problema porta enfeinats un gran nombre de matemàtics. Què se cerca en teoria de nombres i a quin tipus de conclusions s'espera arribar? Els seus resultats, profunds o no, es troben únicament en referències especialitzades?

ANDREAS BENDER

Hauríem de començar per la primera matèria d'aquests problemes: d'entrada, acceptem solament el conjunt dels nombres naturals $1, 2, 3, \ldots$ i les seves operacions d'addició i de multiplicació. Malgrat que fem ara ampliacions més o menys temeràries d'aquest conjunt, les nostres reflexions sempre ens hi retornaran.

El primer problema se'ns presenta quan volem invertir l'addició: $3 - 5$ no és cap *nombre natural*. Per tal de resoldre'l, ampliem el nostre conjunt cap als nombres negatius $-1, -2, -3, \ldots$. Iterarem processos d'aquesta mena; és a dir, ampliarem un conjunt de nombres a fi de poder portar a terme una operació, sense restriccions, amb tots els seus elements.

La divisió de tots els nombres enters, llevat del zero, ens condueix al conjunt dels *nombres racionals*. Però en l'antiguitat ja se sabia que, per exemple, la longitud de la diagonal d'un quadrat de costat 1 no és cap nombre racional. Per tant, si sobre una recta assenyalem un punt com a origen, tenim que els nombres racionals no descriuen tots els seus punts.

El pas següent se'ns imposa quan volem extreure arrels quadrades de *nombres reals* negatius: $\sqrt{-1}$ no és cap nombre real. Podem interpretar els nombres complexos, indispensables per a tal fi, com a parells ordenats de nombres reals. Però fóra feixuc explicar aquí com s'hi opera. Aquestes dues darreres ampliacions permeten, per primera vegada, poder portar a terme sèries infinites d'operacions. D'altra banda, tots els intents d'ordenar els nombres complexos porten a contradicció; en conseqüència, no són cap conjunt ordenable.

L'algorisme d'Euclides

Si volem prosseguir en aquesta direcció, tot mantenint el sentit de les definicions, només podem fer dos passos més: els de les extensions quaterniòniques i octaniòniques. Aquest és un resultat difícil, que amb prou feines fa cinquanta anys que es coneix. A partir de la teoria de nombres ens hem anat endinsant en l'àlgebra i hem trobat un dels molts exemples que fan palesa l'estreta relació existent entre aquesta teoria i altres dominis de la matemàtica.

Tornem a la segona de les nostres ampliacions: la divisió. Considerem les dues equacions: $3x = 12$ y $3x = 13$. Ambdues són resolubles en el conjunt dels nombres racionals mitjançant una divisió. Però si volem, de fet, solucions enteres, derivem cap al concepte de divisibilitat. La primera equació té la solució $x = 4$, mentre que la segona manca de solucions en els enters, car 13 no és divisible per 3. Prenguem una altra indeterminada y i considerem una equació com $2x + 6y = 22$. Podem donar a x un valor arbitrari en el conjunt dels nombres racionals i calcular y per mitjà d'una resta i una divisió. Per raons de divisibilitat, no sempre obtenim solucions enteres en aquests tipus d'equacions. Aquest és el cas de $2x + 6y = 23$; siguin quins siguin els valors que donem a x i a y, $2x + 6y$ és divisible per 2, mentre que 23 no ho és. Per tant, l'equació no és resoluble en els

enters. Si no volem temptejar per trobar les solucions de la primera de les equacions, podem fer ús d'un algoritme: l'algoritme d'Euclides, una de les conquestes de l'antiguitat en teoria de nombres.

Les equacions que hem considerat són de grau 1. Quan es troben indeterminades elevades al quadrat, com per exemple $2x^2 + 6y^2 = 22$, parlem d'equacions de grau 2. Si ampliem els nombres racionals amb totes les arrels quadrades tant de nombres positius com de nombres negatius, la resolució d'aquestes equacions és, de fet, trivial. Certament, la pregunta sobre la seva resolubilitat esdevé interessant quan només admetem solucions racionals. La teoria necessària per a tal fi es conformà a principis d'aquest segle; permet, per exemple, decidir en tots els casos la resolubilitat d'una equació donada.

L'equació de Fermat

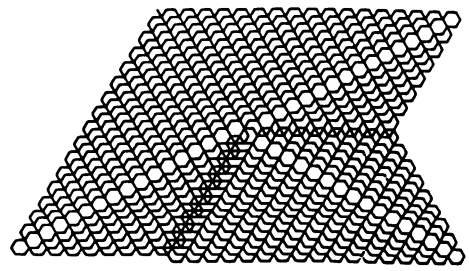
Considererem les equacions de tercer grau en dues indeterminades $y^2 = x^3 + ax + b$, on a i b són nombres enters. Aquí ens trobem a les portes de la recerca. La teoria d'aquestes equacions resta força lluny de ser compresa. Per exemple, encara no es disposa d'un mètode general per decidir si són o no resolubles en els racionals.

Entre aquestes equacions i la conjectura de Fermat esmentada al començament existeix una estreta relació. L'any 1637, el jurista i matemàtic francès Pierre de Fermat anotà la següent sospita: l'equació $x^n + y^n = 1$ no té solucions racionals per a cap exponent n més gran que 2 (recordem que x^n representa el producte de n vegades el nombre x). Tocant a això, cal que x i y siguin diferents de zero. Per a molts valors de n particulars s'ha pogut demostrar que l'equació no té cap solució. Així, per exemple, Leonhard Euler provà que no existeixen parelles de racionals (x, y) de manera que $x^3 + y^3 = 1$. El problema de Fermat motivà l'aprofundiment i l'evolució de teories senceres. Tot just el fet de poder reconèixer els casos on la «solució» és relativament senzilla, ja donà un impuls decisiu al desenvolupament de la teoria algebraica de nombres.

El 1986, Gerhard Frey d'Alemanya i Ken Ribet dels EUA mostraren com aquest problema es pot reduir a una qüestió sobre unes equacions de grau 3. El seu treball posa de manifest com, a partir d'una solució de l'equació de Fermat, es podria construir una equació no modular de grau 3. Aquest fet entra en contradicció amb la hipòtesi que totes les equacions de grau 3 són modulars. Si es pogués provar aquesta conjectura, el problema de Fermat quedaria resolt. El manuscrit, inèdit, d'Andrew Wiles versa precisament sobre aquest fet. Quan cloem la nostra redacció, encara no s'ha fet públic si la llacuna de la demostració es deixarà cloure aviat.

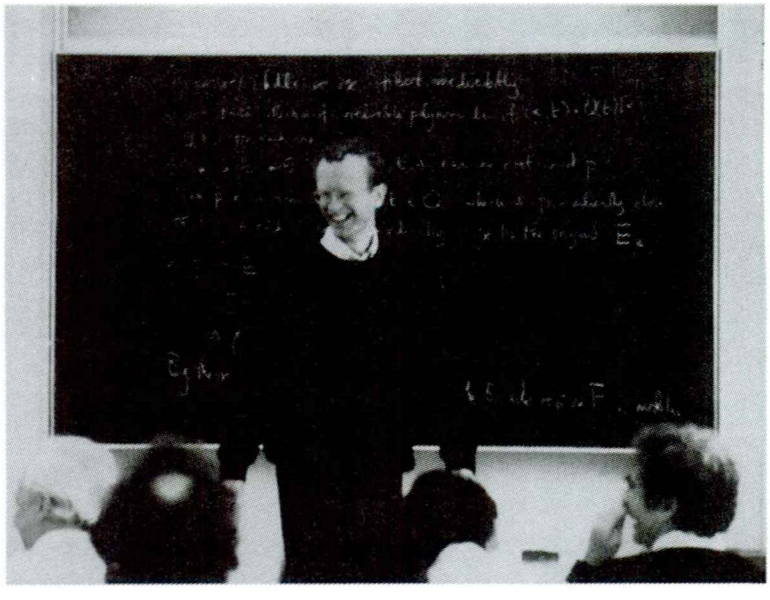
Els ordinadors són molt útils en teoria de nombres

Diofant d'Alexandria va ser un dels primers en cercar sistemàticament solucions racionals i solucions enteres d'equacions. D'ell prenen el nom les equacions de les quals únicament se cerquen aquest tipus de solucions. Encara que aquest sigui un dels temes centrals de la teoria de nombres, ara volem considerar quelcom completament diferent, a fi de donar una idea de la diversitat de preguntes interessants que s'hi plantegen. Prenguem un nombre natural x arbitrari i apliquem-li la regla següent: si és parell li assignem $x/2$; si és senar li fem correspondre $3x+1$. Atès que ambdós resultats són novament nombres naturals, podem iterar el procés i obtenir, per a cada x, una successió de longitud tan gran com vulguem. Basta una calculadora de butxaca per intuir ràpidament, a partir d'uns quants exemples, preguntes centrals sobre aquesta successió que encara avui



resten obertes. Tocant a això, s'aprèn de pressa a apreciar els avantatges d'una calculadora programable. De fet, foren els primers llistats de resultats d'ordinador els que feren plausibles les conjectures. Els ordinadors són molt útils en teoria de nombres a l'hora de calcular dades de manera sistemàtica. Però, només amb el problema $3x+1$, ja ens adonem que els coneixements obtinguts d'aquesta manera tenen les seves limitacions. Els ordinadors poden verificar solament per a un nombre finit de valors inicials que la successió sempre assoleix el valor 1. Això no ens lliura de la incertesa de si el següent valor inicial satisfà la propietat i, en conseqüència, no poden proporcionar mai una demostració general.

Per què s'investiguen qüestions de teoria de nombres? Per què se cerquen solucions enteres o racionals d'equacions quan una ampliació senzilla del domini dels nombres basta per a conduir-nos a una solució també senzilla? La resposta dels filòsofs podria ser: «I per què no?» La resposta dels experts es decantaria per dir que en moltes disciplines, i també en la quotidianitat, únicament s'hi valen els enters i que a ells s'han de referir els càlculs, encara que els estadístics ens parlin de famílies que tenen, de mitjana, dues criatures i mitja. La teoria de nombres troba aplicacions en disciplines com la física, la teoria de la informació i els gràfics per ordinadors. A fi d'entendre'n les motivacions, potser ens ajudaria escoltar alguna vegada un grup de sexagenaris discutint animadament sobre quins nombres són més grans que un miler de trilions. Hi ha persones sensibles a la fascinació dels nombres. Es queden bocabadades davant de l'obra dels seus avantpassats i, d'una manera especial, davant del munt de misteris arcans que encara resten per comprendre. Espero no perdre mai aquesta capacitat d'embadalir-me.



Sembla que el matemàtic britànic Andrew Wiles ha desenvolupat una demostració formal del darrer teorema de Fermat.

Andreas Bender és un enginyer diplomat per l'ETH. Estudià matemàtiques primerament a la Universitat de Zuric. Actualment treballa en una tesi en teoria de nombres a la Universitat de Cambridge, Anglaterra.