Els àtoms de l'infinit

DARIO RAMIS
3r ESO - IES Gata de Gorgos

Segell commemoratiu de Gauss.
De la col·lecció de JOSEP PEDRO.

Tots hem hagut d'aprendre la definició de *nombre primer* -"són els nombres que sols tenen dos divisors: ell mateix i l'un", ens fan repetir volta rere volta a classe-, però, més enllà d'aquesta raó i alguna utilitat matemàtica, ningú no aprén res més sobre aquests nombres.

Fa 2300 anys, Euclides va definir què era un nombre primer. Va demostrar que són infinits amb un bell i simple procediment i va demostrar el teorema fonamental de l'aritmètica, pel qual sabem que qualsevol nombre és producte únic d'altres nombres primers més petits. Aquest procés s'anomena *factoritzar*. Però Euclides no va establir l'ordre en la successió d'aquests singulars nombres.

Potser siga aquest problema el que ha despertat més interés en la comunitat matemàtica al llarg de la història. Els nombres primers varen ser motiu de correspondència entre el monjo Marin Mersenne i el jurista Pierre de Fermat, ambdós grans afeccionats a les matemàtiques, els quals van conjecturar algunes afirmacions que encara hui es tenen en consideració, a pesar d'haver resultat errònies.

Al segle XIX, Carl Friedrich Gauss, matemàtic alemany obsessionat amb els nombres primers des de la seua joventut, va desenvolupar un teorema sobre la seua distribució. Tot i que va ser una gran gesta, la teoria de Gauss era bastant imprecisa i no satisfeia ningú. Va ser un alumne seu, Bernhard Riemann, qui va formular un problema matemàtic sense precedents, i que ha estat abordat pels més grans matemàtics, des de la seua època fins l'actualitat. La majoria d'ells van desistir: *la hipòtesi de Riemann*.

Riemann se'n va adonar, quan treballava amb una funció anomenada zeta, Z, que podia crear un camp matemàtic en tres dimensions que tenia relació amb els nombres primers. Al principi, Riemann desconeixia la relació d'aquesta funció i els nombres primers, però acabà per descobrir que les corbes creades per la fórmula de la funció s'hi podien relacionar. Les corbes de la gràfica descrivien uns pics màxims, però el realment important no radicava en aquesta zona de la gràfica, sinó amb les valls creades per les corbes: cada punt de la vall que coincidia amb la altura zero es corresponia amb un nombre primer en la recta numèrica. Aquests punts són anomenats *punts zero*.

Aquesta és la hipòtesi de Riemann, formulada el 1859. És una conjectura sobre la distribució dels zeros de la funció X de Riemann, la qual ens dóna la clau per a saber la distribució dels nombres primers. Riemann va morir prematurament als 40 anys i no la va poder confirmar.

Entre la llarga llista de matemàtics que han intentat resoldre la hipòtesi de Riemann cal destacar-ne un: cal destacar-ne un, Alan Turing, un dels pares de la computació. Per intentar resoldre-la, Turing va construir una gran màquina, màquina que va deixar de tindre fins civils quan va esclatar la Segona Guerra Mundial. Aleshores, Turing va passar a formar part de l'equip encarregat de desencriptar els codis secrets alemanys, cosa que va aturar la seua recerca durant uns quants anys.

En acabar la guerra, Turing va aconseguir mitjançant la seua innovadora màquina ubicar els primers 1104 zeros sobre la recta i tots coincidien amb les posicions dels nombres primers. Actualment, amb els ordinadors millor preparats, s'han aconseguit ubicar molts més punts zero: tots corresponen a un nombre primer.

L'interés pels nombres primers en l'actualitat no és teòric, i és que d'ells depèn la seguretat informàtica. Suposem un nombre tan gran com ara el 1 409 305 684 859, el qual és el resultat de multiplicar els nombres primers 705 967 i 1 996 227; doncs bé, en això consisteix bàsicament la seguretat informàtica actual, en la factorització. Multiplicar dos nombres primers enormes és fàcil, però una vegada realitzat aquest procés el realment complicat és saber els nombres primers que han sigut multiplicats per trobar un nombre enorme, en això consisteix la factorització.

Si bé fins ara no s'ha aconseguit, ni amb els ordinadors més potents, factoritzar nombres tan grans com els introduïts en les claus informàtiques, existeix una esperança per als descodificadors, una esperança que ve donada per la física quàntica: l'ordinador quàntic.