Butlletí de la Societat Catalana de Matemàtiques
Vol. 11, núm. 1, 1996. Pàgs. 0–0.

La conjectura de Catalan*

Paulo Ribenboim

1 El problema

Consideraré successions de nombres enters i formularé algunes preguntes. Primer considereu la successió de tots els quadrats i els cubs:

$$4, 8, 9, 16, 25, 27, 36, 49, 64, 81, 100, \ldots$$

Es pot observar que 8 i 9 són nombres consecutius dins d'aquesta successió. El primer problema és:

Hi ha altres enters consecutius en la successió anterior? Quantes parelles d'enters consecutius? Un nombre finit? Un nombre infinit?

També puc considerar la successió de totes les potències pròpies, que inclogui també les potències cinquenes, les potències setenes, les potències onzenes, etc. (noteu que les potències d'exponent parell són quadrats, les potències d'exponent múltiple de 3 són cubs).

Es pot plantejar el mateix problema. Hi ha altres potències consecutives fora de 8 i 9?

Però per a la successió de totes les potències té sentit plantejar un nou problema: hi ha tres enters consecutius que siguin potències pròpies?

Com que les potències creixen molt ràpidament, les taules de potències són necessàriament molt limitades i, a part de 8 i 9, no s'han observat potències consecutives. Això és un indici que cal tenir present, però s'ha d'anar amb compte abans de treure'n cap conclusió.

Penseu, per exemple, que fins a 100, el 10 % dels nombres són quadrats, fins a 10.000, l'1 % són quadrats, fins a 1.000.000, un de cada 1.000 és un quadrat, i així anar fent. Amb tot, Lagrange va provar que malgrat la creixent escassetat dels quadrats, tot nombre natural és suma de quatre o menys quadrats. Com si els quadrats ocupessin llocs estratègics. Naturalment, el nostre problema és diferent.

Es poden formular problemes semblants amb la següent successió. Siguin a, b nombres enters, $1 < a < b$ i considereu la successió de totes les potències de a i de b. Per exemple,

*Conferència donada en el seminari *Philosophie et Mathématique* de l'École Normale Supérieure de París, el 28 de novembre de 1994.

si $a = 2$, $b = 3$, és la successió:

$$4, 8, 9, 16, 27, 32, 64, 81, \ldots$$

Quantes parelles de nombres enters consecutius s'hi poden trobar en aquestes successions?

Sigui ara E un conjunt finit (no buit) de nombres primers i sigui $E^\times$ el conjunt de tots els nombres naturals, els factors primers dels quals pertanyen a E. Quantes parelles de nombres enters consecutius pertanyen a $E^\times$?

Tots els problemes anteriors es poden expressar fàcilment en termes d'equacions diofàntiques. El primer problema equival a trobar els nombres naturals que són solució de les equacions

$$X^2 - Y^3 = 1, \qquad X^3 - Y^2 = 1.$$

El problema de les potències arbitràries s'expressa per mitjà de l'equació diofàntica exponencial de quatre incògnites

$$X^U - Y^V = 1,$$

on se cerquen solucions enteres més grans que 1.

Si $1 < a < b$, el tercer problema és el mateix que cercar solucions enteres més grans que 1, de les equacions

$$a^U - b^V = 1, \qquad b^V - a^U = 1.$$

Finalment, el problema per a la successió $E^\times$ es correspon amb la simple equació

$$X - Y = 1,$$

les solucions de la qual, però, han de pertànyer a $E^\times$.

En el 1844, Catalan conjecturà que 8 i 9 són els únics nombres enters consecutius que són potències.

Malgrat els molts avenços que s'han fet —dels quals en parlaré aviat— la conjectura de Catalan encara no s'ha pogut provar.

2 Relació amb altres problemes

En aquesta xerrada donaré més importància a entendre la naturalesa dels problemes, el seu lloc dins de la teoria, que no pas a entrar en detalls tècnics.

Sigui P un conjunt de nombres naturals; si convé es pot suposar que $0 \in P$.

Descriuré problemes d'addició i de subtracció.

Problemes d'addició. Sigui $P + P = \{p + p' \mid p, p' \in P\}$. Si $n \geq 1$, sigui

$$nP = \{p_1 + p_2 + \cdots + p_n \mid \text{cada } p_i \in P\}.$$

Sigui $\langle P \rangle = \bigcup_n \geq 1 nP$.

Hom desitja estudiar els conjunts nP, $\langle P \rangle$ i comparar-los amb el conjunt $\mathbb{N}$ de tots els nombres naturals o bé amb algun subconjunt apropiat de $\mathbb{N}$.

Per exemple, aquestes són les preguntes habituals: existeix n tal que $nP = \mathbb{N}$? És $\langle P \rangle = \mathbb{N}$?

Hi ha també les corresponents preguntes asimptòtiques. Existeix un k_0 tal que

$$\{k \in \mathbb{N} \mid k \geq k_0\} \subseteq nP \qquad \text{o} \qquad \{k \in \mathbb{N} \mid k \geq k_0\} \subseteq \langle P \rangle?$$

En aquestes situacions, es pot trobar k_0 de manera efectiva?

Problemes de subtracció. El problema és ara identificar el conjunt $P - P$. Més concretament, si $n \in P - P$ determinar el conjunt

$$\{(p, p') \in P \times P \mid n = p - p'\}$$

o, com a mínim, trobar fites per al nombre d'elements del conjunt.

La resposta, en alguns casos, només es coneix asimptòticament i pot ser molt complicada.

Aquestes idees s'il·lustren tot seguit.

2.1 Nombres primers

Sigui P el conjunt de tots els nombres primers. Més generalment, si $k \geq 1$ sigui P_k el conjunt de tots els nombres enters de la forma $p_1^{e_1} \cdots p_n^{e_n}$ amb $0 < e_1 + \cdots + e_n \leq k$, els quals s'anomenen k-quasi primers.

Així doncs, $P_1 = P$.

Problema d'addició: El problema de Goldbach. La famosa conjectura de Goldbach afirma que

$$\{2n \mid n \geq 2\} \subset P + P,$$

o equivalentment,

$$\{n \mid n \geq 6\} = P + P + P.$$

En el meu llibre sobre nombres primers (citat a les referències) explico els resultats principals obtinguts en l'estudi de la conjectura de Goldbach. Per exemple, Vinogradov demostrà:

$$\{n \mid n \,\text{senar}, \, n > 3^{3^{15}}\} \subset P + P + P.$$

Schnirelmann provà que existeix un S_0 tal que

$$\{n \mid n \geq 4\} = \bigcup_{k}^{S_0} = 1kP.$$

Riesel i Vaughan calcularen que S_0 es pot prendre igual a 19.

Faig notar, quan s'hi permeten quasi primers, el resultat pioner de Brun:

$$\{n \mid n \geq 4\} = P_9 + P_9.$$

El millor resultat conegut fins avui és degut a Chen:

$$\{n \mid n \geq 4\} = P + P_2.$$

Problemes de subtracció: la conjectura de Polignac i la conjectura dels nombres primers bessons. Polignac va conjecturar que tot nombre parell és la diferència de dos primers; en altres paraules:

$$\{2k \mid k \geq 1\} \cup \{1\} = P - P.$$

Aquesta conjectura no s'ha demostrat.

La conjectura dels nombres primers bessons afirma que existeixen infinits nombres primers p tals que $p + 2$ és també primer. En altres paraules, 2 es pot representar d'infinites maneres com $2 = p' - p$, on p, p' són nombres primers. Aquesta afirmació també està esperant ser demostrada.

Per a cada $N > 1$, $\pi_2(N)$ denota el nombre de primers $p \leq N$ tals que $p+2$ també és primer. Heus aquí una versió quantitativa de la conjectura dels nombres primers bessons:

$$\pi_2(N) \sim \frac{N}{(\log N)^2},$$

és a dir, el quocient de les dues expressions té límit 1 (quan $N \to \infty$).

Segons Brun, els nombres primers bessons són escassos ja que

$$\sum \frac{1}{p} = B < \infty$$

(la suma s'estén a tots els primers p tals que $p+2$ és també primer). Noteu que $\sum 1/p = \infty$ (suma estesa a tots els primers).

2.2 Potències i nombres potents

Sigui P el conjunt de totes les potències pròpies. Sigui Q el conjunt de tots els nombres potents (aquests són els nombres N tals que si p divideix N, aleshores p^2 divideix N).

És immediat veure que $Q = \{a^2b^3 \mid a, b \geq 1\}$.

Problemes d'addició. El problema interessant en el conjunt $P + P$ és el de la descripció de $(P + P) \cap P$; o sigui, l'estudi de les solucions de $X^l + Y^m = Z^n$ per a l, m, n fixats o fins i tot arbitraris. En particular, l'estudi de l'equació $X^n + Y^n = Z^n$ (equació de Fermat) ha estat vigent durant més de tres segles. El problema de Fermat s'acaba de resoldre per A. Wiles (amb la col·laboració de R. Taylor):

Si $n \geq 3$ i x, y, z són nombres naturals tals que $x^n + y^n = z^n$, aleshores $xyz = 0$.

La situació és molt diferent quan $n = 2$. Des de fa molt temps se sap que existeixen infinites tripletes de nombres enters, dos a dos coprimers (x, y, z) tals que $x^2 + y^2 = z^2$ (són les tripletes pitagòriques).

Recentment, Elkies ha obtingut un resultat semblant: existeixen infinites potències quartes que són sumes de tres potències quartes.

Un altre problema d'addició famós es deu a Waring. Donat $k \geq 2$, existeix un nombre enter $G(k) > 1$ tal que tot nombre natural prou gran és suma de $G(k)$ o menys potències k-èsimes? Igualment, existeix un nombre enter $g(k) > 1$ tal que tot nombre natural és suma de $g(k)$ o menys potències k-èsimes?

Així Lagrange —com ja n'he fet esment— provà que pels quadrats $g(2) = 4$, mentre Gauss vegé que $G(2) = 4$.

Hilbert demostrà l'existència de $g(k)$ per a tot $k \geq 2$. El problema esdevení, doncs, com calcular exactament $G(k)$, $g(k)$. Així, Davenport vegé que $g(4) = 19$. La solució completa per a potències quartes fou donada recentment per Balasubramanian, Deshouillers i Dress: $G(4) = 16$. És a dir, tots els nombres naturals prou grans són suma de 16 potències quartes; n'hi ha infinits que no són sumes de 15 potències quartes; tots són sumes de 19 potències quartes.

Més resultats sobre el problema de Waring es poden trobar al meu llibre sobre els nombres primers.

Quant als nombres potents cal notar que no tot nombre natural és suma de dos nombres potents. Ben al contrari

$$\lim_N \to \infty \frac{\sharp\{n \in Q + Q \mid n \leq N\}}{N} = 0.$$

Heath-Brown ha provat, però, que tot nombre natural prou gran és suma de tres o menys nombres potents.

Problemes de substracció. Ara considero en primer lloc els nombres potents. La notació $1 \underset{\infty}{\in} Q-Q$ vol dir que 1 s'escriu d'infinites maneres com a diferència de nombres potents; o sigui, existeixen infinites parelles de nombres potents consecutius. En efecte, existeixen infinites parelles (x, y) amb $x^2 - 8y^2 = 1$ i, per tant, x^2, $8y^2$ són nombres potents consecutius.

Amb la mateixa notació, Mollin i McDaniel demostraren que $n \underset{\infty}{\in} Q - Q$, per a tot $n \geq 2$.

Per a tres nombres potents consecutius, Erdös conjecturà: no hi ha tres nombres potents que siguin consecutius.

Granville vegé com d'aquesta conjectura se'n pot deduir el teorema de Adleman, Heath-Brown i Fouvry: hi ha infinits primers p tals que si x, y, z són nombres naturals i $x^p + y^p = z^p$, llavors p divideix xyz (primer cas de l'últim teorema de Fermat).

Malgrat la demostració recent de l'últim teorema de Fermat, la connexió entre aquest teorema i els nombres potents segueix essent intrigant.

La corresponent pregunta per a les potències és justament la conjectura de Catalan: si $1 = p' - p$ (amb $p, p' \in P$) aleshores $p' = 9$, $p = 8$.

Pillai conjecturà: per a tot $k > 1$ només hi ha un nombre finit de parelles de potències (p, p') amb $p, p' \in P$ i $k = p' - p$.

La conjectura de Pillai es pot expressar en termes de la successió

$$z_1 < z_2 < z_3 < \cdots$$

de totes les potències, de la manera següent :

$$\lim_i \to \infty (z_i + 1 - z_i) = \infty.$$

En el seu moment tractaré de tres potències consecutives.

3 Casos especials

El primer resultat documentat que té relació amb el problema de Catalan i problemes anàlegs se situa al voltant de l'any 1320 i es deu a Levi Ben Gerson (Leo Hebraeus), un famós astrònom d'aquell temps. Va demostrar que si potències de 2 i de 3 són consecutives hem de tenir $9 - 8 = 1$. Avui això és res més que un senzill exercici de congruències.

Euler provà que si $X^2 - Y^3 = \pm 1$ ha d'ésser $9 - 8 = 1$. La idea de la demostració que $X^2 - Y^3 = -1$ no té solucions enteres x, $y > 0$ és la següent. Si $x^2 - y^3 = -1$ llavors $y^3 = x^2 + 1 = (x + i)(x - i)$, on $i^2 = -1$. Per l'aritmètica dels enters de Gauss (propietats senzilles ja conegudes per Euler), $x+i = \alpha(a+bi)^3$, on a, b són nombres enters i $\alpha = \pm 1$ o $\pm i$. Aleshores $x - i = \bar{\alpha}(a - bi)^3$ amb $\bar{\alpha} = \pm 1$ o $\mp i$ (respectivament). D'aquí $2i = \alpha(a+bi)^3 - \bar{\alpha}(a-bi)^3$ i és fàcil veure que això és impossible. Cal notar el fet d'haver recorregut als enters de Gauss. Aquesta idea, degudament modificada, es troba també en l'estudi dels altres casos especials i es concretitza en el següent lema precedit per una observació òbvia. Si m, $n \geq 2$ i $x^m - y^n = 1$, siguin p, q primers amb $m = pm', n = qn'$, aleshores $(x^{m'})^p - (y^{n'})^q = 1$. Així doncs, per a provar que $X^m - Y^n = 1$ no té solucions, només cal considerar la mateixa equació quan els exponents són nombres primers p, q.

Ara bé, si p, q són primers senars i $x,\ y \neq 0,\ x^p - y^q = 1$, llavors $y^q = x^p - 1 = (x-1)\,((x^p-1)(x-1))$.

Com que $\mathrm{mcd}(x-1, (x^p-1)(x-1)) = 1$ o p, hi ha dos casos possibles:

$$\begin{cases} x - 1 = r^q \\ \dfrac{x^p - 1}{x - 1} = r'^q \end{cases}$$

amb $\mathrm{mcd}(r, r') = 1$ i $rr' = y$, o bé

$$\begin{cases} x - 1 = p^{q-1} r^q \\ \dfrac{x^p - 1}{x - 1} = p r'^q \end{cases}$$

amb $\mathrm{mcd}(r, r') = 1$ i $prr' = y$ (ja que p^2 no divideix $(x^p-1)(x-1)$.

De $x^p = y^q + 1 = (y+1)\,((y^q+1)(y+1))$ s'obtenen expressions anàlogues per a $y+1$, $(y^q+1)(y+1)$ seguint també dos casos.

Hi ha també expressions semblants que es deriven de $x^2 - y^q = 1$ (on q és un primer senar).

Els següents casos especials a tractar foren $X^2 - Y^q = 1$, respectivament $X^p - Y^2 = 1$ (on p, q són nombres primers més grans que 3).

Va resultar que una d'aquestes equacions es pogué tractar sense dificultat i fou resolta tan sols al cap de sis anys d'haver anunciat Catalan la seva conjectura (1844), o sigui en el 1850, per Lebesgue. Mentre l'altra equació, malgrat els múltiples intents, ha necessitat 120 anys, per a ésser finalment resolta, per Ko en el 1964.

Quina és quina?

Aquesta és una pregunta molt *à-propos* per a remarcar que a vegades dues equacions diofàntiques poden tenir un aspecte molt semblant però en canvi la seva resolució requereix mètodes de nivells de dificultat ben diferents.

Lebesgue emprà una variant del mètode d'Euler per a provar que $X^p - Y^2 = 1$ (amb p primer, $p \geq 5$) té només solució trivial.

La demostració de Ko (en el 1964) que $X^2 - Y^q = 1$ (q primer, $q \geq 5$) només té solució trivial, fou molt més difícil. Més endavant, Chein utilitzà resultats de Størmer i Nagell de començament de segle, per a donar una demostració enginyosa i força més curta del teorema de Ko. Només calgueren tres pàgines!

Els matemàtics, repeteixo, no haurien d'abandonar mai la tasca de substituir les demostracions difícils i tortuoses (les quals poden reflectir una manca global de comprensió) per demostracions netes, clares i enginyoses (no feu extensible el que acabo de dir a la demostració de l'últim teorema de Fermat ni tampoc interpreteu que jo penso que se'n podria trobar una demostració de tres pàgines, o una que cabés a un marge).

L'estudi de les equacions $X^3 - Y^q = 1$, $X^p - Y^3 = 1$ (per a p, q nombres primers més grans que 3) conduí a les equacions

$$X^2 + X + 1 = Y^q$$
$$X^2 + X + 1 = 3Y^q.$$

Nagell tractà aquestes equacions i afirmà que només tenien solucions trivials si s'admetia que les solucions de l'equació

$$X^3 - 3XY + Y^3 = 1$$

eren les ja conegudes: $(x, y) = (1, 0)$, $(0, 1)$, $(-1, -1)$, $(2, -1)$, $(1, 3)$ i $(-3, -2)$.

Això no fou pas senzill de demostrar. Ljunggren (1942) va reeixir gràcies a una anàlisi precisa del grup de les unitats d'un cert cos cúbic.

Vull subratllar que ningú es veié amb cor d'atacar l'equació $X^p - Y^q = 1$, on $\min\{p, q\} \geq 5$, fent servir mètodes especials *ad hoc*.

4 Mètodes algebraics

El propòsit d'aquests mètodes, els quals es basen fortament en l'aritmètica dels cossos de nombres algebraics, és el d'estudiar simultàniament grans famílies d'exponents. Les congruències, unitats, classes d'ideals, abunden en aquests raonaments.

Primer, però, vull fer una llista d'algunes condicions addicionals que impliquen que l'única solució no trivial de $X^U - Y^V = 1$ (amb exponents com a mínim 2) és $x = 3$, $y = 2$, $u = 2$, $v = 3$, la qual dóna $9 - 8 = 1$.

a) Si p, q són nombres primers i l és un nombre primer tal que $l^p - y^q = \pm 1$, aleshores necessàriament $l = 3$, $p = 2$, $y = 2$, $q = 3$.

b) Si $x, y \geq 2$ i $x^y - y^x = 1$, aleshores $x = 3, y = 2$.

c) Les úniques potències consecutives de nombres enters consecutius són 9, 8, en altres paraules $x^m - y^n = 1$ i $|x - y| = 1$ implica que $x = 3$, $y = 2$, $m = 2$, $n = 3$.

En la demostració de l'apartat *c* intervé un interessant resultat aritmètic clàssic sobre els divisors primers de les expressions de la forma $x^m - 1$.

Cassels donà una demostració remarcable del resultat següent:

Si $x^p - y^q = 1$ (amb p, q nombres primers), aleshores p divideix y i q divideix x.

Com a conseqüència d'això només es pot donar el segon cas en el vell lema d'Euler. Per tant, $x - 1 = p^{q-1}r^q$, $\frac{x^p-1}{x-1} = pr'^q$ i també $y + 1 = q^{p-1}s^p$, $\frac{y^q+1}{y+1} = qs'^p$.

Un es pregunta quina importància podria tenir el resultat de Cassels. Sense conèixer l'existència de x, y tals que $x^p - y^q = 1$, com es pot utilitzar la propietat que $p|y$, $q|x$?

Sorpresa! Tant Hyyrö (en finès) com Mąkowski van demostrar:

No hi ha tres potències consecutives.

Sembla haver-hi la regla no escrita que tota conferència ha d'incloure almenys una demostració. Així jo escullo aquesta per la seva impressionant simplicitat:

Prova: Si $x^p < y^q < z^r$ són potències pròpies, els exponents de les quals els podem prendre primers, si $y^q - x^p = 1$, $z^r - y^q = 1$, aleshores pel resultat de Cassels $q|x$ i $q|z$. Per tant, $q|x^p$, $q|z^r$, de manera que q divideix la seva diferència $z^r - x^p = 2$. Així $q = 2$ i es té $z^r - y^2 = 1$. Però això és impossible pel resultat de Lebesgue. Contradicció i fi de la demostració. □

El teorema de Cassels implica que si $x^p - y^q = 1$, llavors x, y són d'una forma especial: $x = 1 + p^{q-1}r^q$, $y = -1 + q^{p-1}s^p$ i també $\frac{x^p-1}{x-1}$, $\frac{y^q+1}{y+1}$ són d'una forma especial.

Hyyrö va explorar aquesta idea, tot imposant més restriccions a x, y.

Però, sobretot, va seguir els passos de Wieferich i Inkeri en relacionar el problema amb les congruències obtingudes per Wieferich per a l'últim teorema de Fermat. Ara explico els resultats tan útils d'Inkeri, que continuà la línia d'investigació de Hyyrö.

Sigui p un primer senar i $H(-p)$ el nombre de classes del cos $\mathbb{Q}(\sqrt{-p})$.

Heus aquí un dels resultats d'Inkeri:

Sigui $p > 3$, $p \equiv 3 \pmod 4$. Si q és un nombre primer, $q > 3$ i

$$q \nmid H(-p) \quad \text{i} \quad p^{q-1} \not\equiv 1 \pmod{q^2}$$

aleshores $X^p - Y^q = 1$ només té solució trivial.

Inkeri donà un criteri semblant quan $q \equiv 3 \pmod 4$ i també un criteri més fort quan $p \equiv 3 \pmod 4$ i $q \equiv 3 \pmod 4$, tot això complementat amb l'estudi detallat de casos especials.

L'interès pràctic d'aquests resultats és doble. En primer lloc, és relativament senzill calcular el nombre de classes d'un cos quadràtic imaginari i comprovar si un primer donat el divideix. En segon lloc, s'ha observat que l'anomenada congruència de Wieferich (amb base p) $p^{q-1} \equiv 1 \pmod{q^2}$ se satisfà molt rarament. Això i la similitud dels criteris permeten, després de fer càlculs, decidir que per a moltes parelles d'exponents (p, q) l'equació corresponent només té solució trivial.

Però fins i tot a una parella petita, com $(5, 7)$ no se li pot aplicar aquest criteri. En efecte, $q = 7 \equiv 3 \pmod 4$, $H(-7) = 1$, 5 no divideix $H(-7)$, però $7^4 \equiv 1 \pmod{5^2}$.

Per a cobrir més casos, Inkeri considerà també cossos ciclotòmics. Sigui h_p el nombre de classes del cos ciclotòmic $\mathbb{Q}(\zeta_p)$ on ζ_p és una arrel primitiva p-èsima de 1.

Inkeri provà:

Suposem que $X^p - Y^q = 1$ té una solució no trivial.

1. Si p no divideix h_q, aleshores $q^{p-1} \equiv 1 \pmod{p^2}$.
2. Si q no divideix h_p, aleshores $p^{q-1} \equiv 1 \pmod{q^2}$.

En particular, les equacions $X^5 - Y^7 = \pm 1$ tenen només solucions trivials. En efecte, $5 \nmid h_7$, $7 \nmid h_5$ però$5^6 \not\equiv 1 \pmod{7^2}$.

En un article posterior amb Aaltonen es cobriren moltes més parelles d'exponents amb aquest mètode, després de calcular nombres de classes i congruències de Wieferich.

Mignotte ha continuat aquests càlculs. El darrer resultat és que (amb un lema de W. Schwarz encara no publicat) si $\min\{p, q\} \leq 10640$, aleshores $X^p - Y^q = 1$ té només solució trivial.

5 Mètodes analítics

En aquest moment vull remarcar el que és obvi i s'ha dit implícitament: hem estat considerant tres tipus diferents d'equacions

1. $a^U - b^V = 1$, on a, b són nombres enters fixats, diferents i més grans que 1.
2. $X^m - Y^n = 1$, on m, n són nombres enters fixats, diferents i més grans que 1.
3. $X^U - Y^V = 1$.

S'escau, doncs, de parlar per separat de cadascuna d'aquestes equacions.

5.1 Equació $a^U - b^V = 1$

El principal resultat és de LeVecque, que vegé que hi ha com a màxim una parella (u, v) amb $u \geq 2, v \geq 2$ tal que $a^u - b^v = 1$.

Cassels donà un algoritme que permet trobar la hipotètica solució (si existeix). Per a $(a, b) \neq (3, 2)$ l'algoritme —fins ara— no ha pogut trobar cap solució!

Vull considerar també la variant d'aquesta equació, ja esmentada a l'inici d'aquesta conferència. Sigui $E = \{p_1, \dots, p_s\}$ (amb $s \geq 1$), un conjunt finit de nombres primers. Sigui $k \geq 1$.

Thue va demostrar que existeix una constant efectivament calculable $C > 0$ tal que si

$$p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} - p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} = k$$

(amb enters $n_i, m_i \geq 0$), aleshores $n_i, m_i < C$ (per a tot $i = 1, \dots, s$).

Els casos especials quan $k = 1$ o 2 havien estat demostrats anteriorment per Størmer amb un mètode molt interessant que utilitzava propietats de divisibilitat de termes de successions recurrents lineals d'ordre 2 (és a dir, anàlogues a les successions de nombres de Fibonacci i de nombres de Lucas).

5.2 Equació $X^m - Y^n = 1$

Siegel tractà una equació més general. Del seu principal resultat s'obté:

> Si $m, n \geq 2$ amb $\max\{m, n\} \geq 3$, si a, b, k són nombres enters no nuls donats, aleshores l'equació $aX^m - bY^n = k$ només té un nombre finit de solucions enteres.

El resultat de Siegel no incloïa cap fita sobre el nombre o, *a fortiori*, sobre la magnitud de les possibles solucions.

El gran aconseguiment de Baker, que el féu mereixedor d'una Medalla Fields, fou l'invent d'un nou mètode que portés a fites efectives per a les possibles solucions de molts tipus d'equacions diofàntiques.

En el nostre cas, les estimacions de Baker donaren:

Si $m, n \geq 2$, $k \geq 1$ i $x^m - y^n = k$, llavors

$$|x|, |y| < \exp\exp\left((3m)^{10} n^{10n^3} |k|^{n^2}\right)$$

(i una fita semblant si es permuta m i n). La fita depèn de les fortes estimacions de les fites inferiors de certes formes lineals en logaritmes. El que cal recordar de tot això és que, ara per ara, la fita conté una doble exponenciació i, per tant, és molt i molt gran.

També s'hauria de fer esment que per al nombre de parelles (m, n) tals que $X^m - Y^n = 1$ té solució no trivial, Hyyrö trobà la fita superior següent: $\exp(631m^2n^2)$.

Més petita que la de Baker, però més gran que 0 —la fita desitjada!

Un bon suport a la conjectura prové del següent teorema de densitat, que jo vaig demostrar utilitzant un teorema de Schinzel i Tijdeman: donats a, b, k nombres enters no nuls, es considera per a cada $N > 1$ el número $\alpha(N)$ de parelles (m, n) amb $2 \leq m, n \leq N$ tals que l'equació $aX^m - bY^n = k$ no té cap solució en nombres enters positius. Aleshores $\frac{\alpha(N)}{N^2}$ té límit 1 (quan N tendeix a ∞).

5.3 Equació $X^U - Y^V = 1$

Ha arribat el moment d'enunciar el resultat més important en relació amb la conjectura de Catalan obtingut fins ara. Fou provat en el 1976 per Tijdeman, el qual utilitzà dues vegades les desigualtats de Baker, d'una manera innovadora i hàbil:

> Hi ha una constant C tal que si p, q són nombres primers, si x, y són nombres enters positius i $x^p - y^q = 1$, aleshores $p, q < C$.

Si això s'ajunta amb el resultat efectiu de Baker per a l'equació 2, es pot enunciar:

Hi ha una constant $T > 0$ tal que si $x^p - y^q = 1$, amb p, q nombres primers $x, y \geq 1$, aleshores x, y, p, $q < T$.

Langevin va estimar que T es pot prendre igual a $\exp\exp\exp\exp(730)$ —un nombre d'una magnitud que no em puc ni imaginar (només de pensar-hi em ve mal de cap).

Si bé aquest teorema no demostra que la conjectura de Catalan és certa, sí que prova que el problema de Catalan es pot decidir en un nombre finit de passos. Teòricament (si no a la pràctica), només cal provar, una per una, totes les quàdruples (x, y, p, q) i veure si $x^p - y^q = 1$.

La millora de les desigualtats de Baker en relació directa amb l'equació de Catalan ha portat a Mignotte, per una banda, i a Glass (i col·laboradors seus) de l'altra, a una cursa per a rebaixar la fita per als exponents. Ara ja se sap que si $X^p - Y^q = 1$ té una solució no trivial, llavors $\max\{p, q\} \leq 10^{26}$.

Així doncs, sabem que la conjectura de Catalan és decidible, però no se sap quan es decidirà.

Referències

Per a demostracions, observacions i detalls sobre la conjectura de Catalan, podeu consultar el meu propi llibre, que conté una bibliografia gairebé completa sobre el problema:

P. Ribenboim: *Catalan's Conjecture*, Academic Press, Boston, 1994.

Prèviament, en vaig publicar un survey:

P. Ribenboim: *Consecutive powers*, Expositiones Mathematicae, 2 (1984), 193–221.

També hi ha alguns preprints molt recents de A. W. Glass *et al.*, de M. Mignotte i de W. Schwarz, que s'ocupen dels avenços en la línea dels criteris de K. Inkeri i dels càlculs relacionats amb aquests, alguns d'ells encara no publicats.

Els resultats sobre nombres primers es poden trobar, per exemple, al meu llibre:

P. Ribenboim: *The Book of Prime Number Records*, Nova York, Springer-Verlag, (primera edició 1987; segona edició 1989; tercera edició 1995).

Vegeu també la versió abreujada en francès:

P. Ribenboim: *Les nombres premiers: mystères et records*, Presses Universitaires de France, París, 1994.

Departament of Mathematics
Queen's University
Kingston, Ontario K7L 3N6
Canada
mastdept@qucdn.queensu.ca