Butlletí de la Societat Catalana de Matemàtiques
Vol. 20, núm. 1, 2005. Pàg. 53–66

L'ABC de l'aritmètica*

Xavier Xarles

Resum

Bona part dels últims resultats més importants en teoria de nombres, com l'últim teorema de Fermat i la conjectura de Catalan, tenen aspectes comuns que els unifica. Aquests últims anys s'ha arribat a la formulació d'una conjectura que en certa manera explicaria i generalitzaria aquests resultats, l'anomenada conjectura ABC. En aquesta exposició presentem alguns d'aquests resultats i introduïm aquesta conjectura de manera gradual.

Paraules clau: conjectura ABC, Fermat, Mordell, Catalan, radical, equació diofàntica.

Classificació AMS: 11D61 (11D41, 11G30, 14G05, 14H25).

1 Sumes de potències

Aquests últims deu anys la gent que treballem en teoria de nombres hem vist la demostració de varis resultats que fa uns anys ens semblaven encara inabastables. Començarem per recordar potser el més famós de tots ells, demostrat per Andrew Wiles [Wi] (amb l'ajuda de Pierre de Fermat i de Richard Taylor [T-W]) l'any 1994.

* Aquest article és una versió escrita de la conferència inaugural del curs 2004-2005 de la Secció de Matemàtiques de la UAB, feta el dia 10 de novembre de 2004. Donat que la conferència anava dirigida principalment a alumnes de la llicenciatura, he intentat que tingués un nivell comprensible i que no fos gaire tècnica. M'he basat en part en l'article d'Andrew Granville i Thomas J. Tucker [G-T], que us recomano molt especialment.

1 TEOREMA (L'ÚLTIM TEOREMA DE FERMAT) *Sigui $n \geq 3$. Si tenim enters x, y i z tals que*

$$x^n + y^n = z^n$$

aleshores $xyz = 0$.

De fet, tots sabeu que Fermat va demostrar el cas $n = 4$, i que Wiles va demostrar un resultat molt més fort del qual es dedueix, gràcies a una idea de Gerhard Frey i a un resultat de Ken Ribet, el cas que n és un nombre primer senar qualsevol; d'aquests dos casos es demostra el resultat per a tot $n \geq 3$.

Després d'aquest resultat s'han aplicat les mateixes tècniques per a demostrar resultats semblants a aquest, com per exemple el següent, de Ken Ribet [Ri], Henri Darmon i Loïc Merel [D-M]: si $n \geq 3$, i tenim enters x, y i z tals que $x^n + y^n = 2z^n$, aleshores $xyz = 0$ o bé $x = \pm y = \pm z$.

Una altra conjectura famosa que s'ha resolt últimament ha estat l'anomenada conjectura de Catalan (vegeu l'article de Paulo Ribenboim [R]). El seu nom no té res a veure amb cap català, sinó amb qui primer la va formular, el matemàtic belga Eugène Charles Catalan, en una carta a l'editor de la revista de Crelle l'any 1844, publicada en el volum 27 d'aquesta revista.

2 CONJECTURA (LA CONJECTURA DE CATALAN) *Siguin a, b, c i d nombres enters més grans que 1. Si*

$$a^b = c^d + 1$$

aleshores $a = 3$, $b = 2$, $c = 2$ i $d = 3$.

L'any 1976, Robert Tijdeman, [Ti], va demostrar que la conjectura era certa si a, b, c i d eren prou grans (de fet va donar una fita superior per a una hipotètica solució de l'equació, però la fita era massa gran per a poder ser comprovada fins i tot amb ordinador). Finalment, el 18 d'abril de 2002, Preda Mihăilescu, [Mi], va anunciar que havia trobat una demostració d'aquesta conjectura; la qual s'ha publicat en la mateixa revista on es va anunciar, 545 volums més endavant.

Observeu que aquestes conjectures (ara teoremes) semblen dir que si sumem dues potències prou grans de dos nombres enters, aleshores el nombre que obtenim no pot ser una potència d'un nombre enter (observeu que 1 sempre és una potència d'ell mateix). Això és el que diu (aproximadament) la següent conjectura, formulada per primer cop, sembla ser, per Viggo Brun l'any 1914, [Br], i reformulada diverses vegades més, entre aquestes l'any 1996 per Andrew Beal, un multimilionari texà i matemàtic amateur, el qual oferí un premi de 75.000 $ per al primer que la resolgui (he de dir que no estic segur si aquesta oferta encara és vàlida). És coneguda popularment com la conjectura de Catalan-Fermat, [Ma].

3 CONJECTURA (LA CONJECTURA DE CATALAN-FERMAT) *Si n, m i r són enters més grans o iguals que 3, aleshores*

$$a^n + b^m = c^r$$

no té cap solució amb a, b i c enters primers entre si i diferents de zero.

És clar que aquesta conjectura implica l'últim teorema de Fermat. També implica la conjectura de Catalan posant $b = 1$, tot i que cal estudiar els casos amb alguna potència menor que 3, que no són difícils de fer.

1 OBSERVACIÓ *La condició de ser primers entre si és necessària.*

Per exemple, suposem que donats a, b, n i m tenim

$$a^n + b^m = c\,,$$

multiplicant per c^{n+m} tenim, per tant,

$$(c^m a)^n + (c^n b)^m = c^{n+m+1}.$$

De fet, podem trobar molts exemples amb a, b i c no primers entre si.

Observeu també que aquesta condició no apareixia en els enunciats dels resultats anteriors perquè en aquells casos no és necessària. En efecte, pel teorema de Fermat, si a i b tenen algun factor en comú, també el té c, i si dividim tot plegat per aquest factor elevat a n tenim la mateixa equació però ara sense el factor en comú. El cas de la conjectura de Catalan encara és més clar, ja que, a i c són necessàriament primers entre sí.

De fet, encara és pot afinar una mica més el possible resultat, estudiant què pot passar quan sumem potències de nombres enters.

Suposem que tenim n, m i r enters més grans o iguals que 2, i volem estudiar l'equació $a^n + b^m = c^r$, amb a, b i c primers entre si, $abc \neq 0$.

Primer cas: Si $1/n + 1/m + 1/r > 1$, aleshores hi ha infinites solucions. En cadascun dels casos es coneixen a més parametritzacions per a totes les solucions:

- $n = m = 2$, $r \geq 2$, ben conegut (treballeu a $\mathbb{Z}[i]$ o mireu [Mo, pàg. 122]).
- $n = m = 3$, $r = 2$, resolt per Louis J. Mordell el 1969 [Mo, pàg. 235].
- $n = 5$, $m = 3$ i $r = 2$, resolt en part per Frits Beukers, Steve Thiboutot i Don Zagier el 1998 [Be], i definitivament per Harold Edwards el 2001.
- $n = 4$, $m = 3$ i $r = 2$, resolt parcialment per Don Zagier el 1998, i Johnny Edwards el 2004, [Ed].

Segon cas: Si $1/n + 1/m + 1/r = 1$, aleshores no hi ha solucions. Tenim els casos:

- $n = m = 4$, $r = 2$, resolt per Pierre de Fermat.
- $n = m = r = 3$, resolt per Leonard Euler.

Tercer cas: Si $1/n + 1/m + 1/r < 1$, aleshores hi ha un nombre finit de solucions. Els únics casos coneguts en què hi ha solució són:

- Si $m > 6$, la solució general $2^3 + 1^m = 3^2$.
- Si $\{n, m, r\} = \{2, 3, 7\}$, i totes les solucions són (Bjorn Poonen, Ed Schaefer, Michael Stoll, 2005, [PSS]):
  1. $1414^3 + 2213459^2 = 65^7$
  2. $9262^3 + 15312283^2 = 113^7$
  3. $2^7 + 17^3 = 71^2$
  4. $17^7 + 76271^3 = 21063928^2$.
- Si $\{n, m, r\} = \{2, 3, 8\}$, i totes les solucions són (Nils Bruin, 1999, [B1]):
  1. $33^8 + 1549034^2 = 15613^3$
  2. $43^8 + 96222^3 = 30042907^2$.
- Si $\{n, m, r\} = \{2, 3, 9\}$, i totes les solucions són (Nils Bruin, 2003, [B2]):
  1. $7^3 + 13^2 = 2^9$.
- Si $\{n, m, r\} = \{2, 4, 5\}$, i totes les solucions són (Nils Bruin, 1999, [B1]):
  1. $2^5 + 7^2 = 3^4$
  2. $3^5 + 11^4 = 122^2$.

Els únics casos en què es coneix alguna solució són així:

$$\{n, m, r\} = \{2, 3, 7\}, \{2, 3, 8\}, \{2, 3, 9\}, \{2, 4, 5\}.$$

Es conjectura que no hi ha altres solucions.

Aquesta conjectura es pot inscriure dins d'una conjectura encara molt més general, formulada per primer cop per Henry Darmon i Andrew Granville l'any 1993, [D-M].

4 CONJECTURA (FERMAT GENERALITZAT) *Siguin A, B i C tres nombres enters diferents de zero. Aleshores hi ha un nombre finit d'enters n, m i r amb $1/n + 1/m + 1/r < 1$ i enters x, y i z amb $xyz \neq 0$ i primers entre si tals que*

$$Ax^n + By^m = Cz^r.$$

De fet, Darmon i Granville demostren que, si fixem n, m i r, hi ha un nombre finit d'enters x, y i z primers entre si i solució de l'equació. La demostració es basa en el teorema de Faltings [Fa] (també anomenada conjectura de Mordell). Més endavant comentarem una mica més aquest resultat de Gerd Faltings.

Per poder entendre què podria estar passant, el que farem és estudiar el cas dels polinomis. Aquesta és una idea molt usual en aritmètica: hi ha moltes

i molt profundes analogies entre els polinomis (sobre $\mathbb{Q}$, sobre $\mathbb{C}$, sobre un cos finit) i els enters. Aquestes analogies han estat una guia constant en la teoria de nombres els últims cent anys, començant per Richard Dedekind, David Hilbert i André Weil (vegeu per exemple la carta publicada a [Kr]), i acabant en molts dels resultats que porten entre d'altres a la geometria d'Arakelov.

2 L'ABC dels polinomis

El següent resultat va ser demostrat per primer cop per Joseph Liouville el 1851, tot i que la demostració que presentem aquí és posterior.

5 TEOREMA (FERMAT POLINÒMIC) *Sigui $n \geq 3$. Aleshores no existeixen polinomis $X(t)$, $Y(t)$ i $Z(t)$ amb coeficients a $\mathbb{C}$, primers entre sí, de grau més gran que 0, tals que*

$$X^n + Y^n = Z^n. \tag{1}$$

DEMOSTRACIÓ: Derivem l'equació $X^n + Y^n = Z^n$ respecte a t:

$$nX^{n-1}X' + nY^{n-1}Y' = nZ^{n-1}Z',$$

dividim per n:

$$X^{n-1}X' + Y^{n-1}Y' = Z^{n-1}Z'. \tag{2}$$

Multipliquem (1) per Y', (2) per Y i restem:

$$X^{n-1}(XY' - YX') = Z^{n-1}(ZY' - YZ').$$

Com que X i Z són coprimers, tenim

$$X^{n-1} \text{ divideix } ZY' - YZ'.$$

El polinomi $ZY' - YZ'$ no pot ser el polinomi zero, ja que si no $(Z/Y)' = 0$, i, per tant, Z i Y són múltiples un de l'altre.

Prenem graus i tenim

$$(n-1)\operatorname{grau}(X) \leq \operatorname{grau}(ZY' - YZ') \leq \operatorname{grau}(Y) + \operatorname{grau}(Z) - 1.$$

O sigui,

$$n\operatorname{grau}(X) < \operatorname{grau}(X) + \operatorname{grau}(Y) + \operatorname{grau}(Z).$$

Podem fer el mateix amb Y i amb Z (l'equació (1) és simètrica). Obtenim tres equacions que al sumar-les ens donen:

$$n(\operatorname{grau}(X) + \operatorname{grau}(Y) + \operatorname{grau}(Z)) < 3(\operatorname{grau}(X) + \operatorname{grau}(Y) + \operatorname{grau}(Z)).$$

O sigui,

$$n < 3.$$

□

L'any 1983, Richard C. Mason va descobrir una desigualtat (que ell anomena la desigualtat fonamental, i ara s'anomena el teorema ABC polinòmic) que generalitza enormement aquest resultat i amb el qual va demostrar de manera elemental tot de resultats respecte a solucions polinòmiques d'equacions.

6 TEOREMA (MASON 1983) *Si tenim tres polinomis $A(t)$, $B(t)$ i $C(t)$ de $\mathbb{C}[t]$, primers entre si, tals que*

$$A + B = C\,,$$

aleshores

$$\max(\text{grau}(A), \text{grau}(B), \text{grau}(C)) < \sharp\{\alpha \in \mathbb{C} \mid \alpha \textit{ arrel de } ABC\}\,.$$

DEMOSTRACIÓ:

Prenem

$$\Delta := \begin{vmatrix} A & B \\ A' & B' \end{vmatrix} = \begin{vmatrix} A & C \\ A' & C' \end{vmatrix} = \begin{vmatrix} C & B \\ C' & B' \end{vmatrix}.$$

Podeu comprovar fàcilment (per exemple fent canvis elementals) que es verifiquen les igualtats. Observem que $\Delta \neq 0$, ja que, seguint el mateix argument que a la demostració anterior, si fos zero aleshores A i B serien múltiples un de l'altre.

Suposem ara que $\alpha \in \mathbb{C}$ és una arrel de $A(t)$ amb multiplicitat e. Per tant $(t-\alpha)^e$ divideix A i $(t-\alpha)^{e-1}$ divideix A', d'on $(t-\alpha)^{e-1}$ divideix Δ. Així, $A(t)$ divideix $\Delta\prod(t-\alpha)$, on el producte és respecte a totes les arrels diferents de $A(t)$ (sense multiplicitat).

Fent el mateix amb B i C obtenim finalment

$$ABC \text{ divideix } \Delta \prod_{ABC(\alpha)=0} (t-\alpha)\,.$$

Prenem ara graus. El grau de Δ compleix

$$\text{grau}(\Delta) \leq \text{grau}(A) + \text{grau}(B) - 1$$

$$\text{grau}(\Delta) \leq \text{grau}(A) + \text{grau}(C) - 1$$

$$\text{grau}(\Delta) \leq \text{grau}(C) + \text{grau}(B) - 1\,,$$

i es clar que

$$\text{grau}\Big(\prod_{ABC(\alpha)=0} (t-\alpha)\Big) = \sharp\{\alpha \in \mathbb{C} \ \alpha \text{ arrel de } ABC\}\,.$$

Tot junt ens dóna el resultat. □

Observem que el teorema de Fermat polinòmic es dedueix fàcilment d'aquest resultat. De la mateixa manera podem veure l'equivalent a la conjectura

de Catalan-Fermat per polinomis: si n, m i r són enters més grans que 2, i X, Y i Z són polinomis de $\mathbb{C}[t]$ coprimers que compleixen

$$X^n + Y^m = Z^r,$$

aleshores algun dels polinomis és constant (o sigui de grau zero).

Anem a veure com podríem traduir aquest resultat a una conjectura per als nombres enters.

3 A la recerca de l'ABC

Donat que els nombres primers són l'analogia natural pels factors irreductibles dels polinomis, potser l'anàleg que estem buscant és:

Primer intent: *Si $a + b = c$ amb a, b i c enters primers entre si, aleshores el nombre de factors primers de c comptats amb multiplicitat és menor que el nombre de factors primers diferents de a b c.*

Dit d'una altra manera, si denotem com és usual

$$\Omega(n) := \sharp\{p^r \text{ amb } p \text{ primer } \mid p^r \text{ divideix } n\},$$

aleshores,

$$\Omega(c) < \omega(abc) := \sharp\{p \text{ primer } \mid p \text{ divideix } abc\}.$$

Però aquest resultat és clarament fals! Per exemple, tenim $1+3=4$, i, per tant, $\Omega(4) = 2$ i $\omega(3 \cdot 4) = 2$, o $1 + 7 = 8$, amb $\Omega(8) = 3$ i $\omega(7 \cdot 8) = 2$. Més en general, si $2^p - 1$ és primer (un primer de Mersenne), tenim $1 + (2^p - 1) = 2^p$ amb $\Omega(2^p) = p$ i $\omega(2^p(2^p - 1)) = 2$, i, per tant, si la conjectura fos certa, tindríem $p < 2$.

El problema és que hem fet una mala analogia: hem considerat que l'equivalent en els enters del grau d'un polinomi és el nombre de factors primers, i aquesta analogia és massa simple. Per a comprendre millor l'analogia adequada, observarem primer el resultat següent que es dedueix fàcilment del teorema de Manson.

Anem a veure com podem escriure l'ABC polinòmic per a polinomis sobre $\mathbb{Q}$ (de fet, sobre qualsevol cos K de característica zero segueix essent vàlid).

7 TEOREMA (ABC POLINÒMIC) *Si tenim tres polinomis $A(t)$, $B(t)$ i $C(t)$ de $\mathbb{Q}[t]$, primers entre si, tals que*

$$A + B = C,$$

aleshores

$$\max(\text{grau}(A), \text{grau}(B), \text{grau}(C)) < \sum_{P(t)|ABC} \text{grau}(P(t)),$$

on la suma és sobre tots els polinomis irreductibles *que divideixen ABC.*

D'aquí podem veure que potser el nostre problema ha estat pensar que tots els nombres primers tenien grau 1. Però, quin és l'anàleg del grau en els nombres enters? Doncs la resposta és fàcil quan un recorda que el grau del producte és la suma dels graus; i, per tant, la nostra funció s'ha de comportar com un logaritme.

Segon intent: *Si $a+b=c$ amb a, b i c enters primers entre si, aleshores*

$$\max\{\log|a|,\log|b|,\log|c|\} \leq \sum_{\substack{p \text{ primer}\\ p|abc}} \log(p)\,,$$

o, equivalentment,

$$\max\{|a|,|b|,|c|\} \leq \prod_{\substack{p \text{ primer}\\ p|abc}} p\,.$$

Ara bé, aquest resultat no és cert, com podem veure de $1+8=9$, d'on tindríem $9<2\cdot 3=6$, i de $1+63=2^6$, d'on tindríem $2^6=64<2\cdot 3\cdot 7=42$.

Abans de donar-nos per vençuts, intentem ser una mica menys estrictes i comprovem si, multiplicant la part dreta de la desigualtat per una constant (independent de a, b, i c), la conjectura podria ser certa. Abans de fer-ho introduirem una notació que ens serà útil.

Definim el radical d'un nombre enter com la part lliure de quadrats:

$$\mathrm{rad}(a) := \prod_{\substack{p \text{ primer}\\ p|a}} p\,.$$

Segon intent (bis): *Existeix una constant K tal que, si $a+b=c$ amb a, b i c enters primers entre si, aleshores*

$$\max\{|a|,|b|,|c|\} \leq K\,\mathrm{rad}(abc)\,. \tag{3}$$

Però fins i tot aquesta desigualtat no és certa. Per a veure-ho anem a fer servir el petit teorema de Fermat (de fet, el teorema de Fermat-Euler):

8 TEOREMA (TEOREMA DE FERMANT-EULER) *Si p és un nombre primer, i n es un nombre no divisible per p, aleshores per a tot $r\geq 1$ tenim*

$$n^{p^{r-1}(p-1)} \equiv 1 \mod p^r.$$

1 CONTRAEXEMPLE *Prenem*

$$a = 2^{p^{r-1}(p-1)}\,,\quad b=-1 \quad i \quad c = 2^{p^{r-1}(p-1)}-1\,.$$

Així tenim p^r divideix c. Per tant,

$$\mathrm{rad}(abc) \leq 2c/p^{r-1},$$

i la desigualtat (3) *implicaria*

$$K \geq p^{r-1}/2$$

per a tot nombre primer $p > 2$ i per a tot $r > 1$.

En aquest moment podríem llançar la tovallola, o bé fer el que els matemàtics fem a vegades quan creiem que un resultat és *aproximadament* cert: introduir un nombre $\epsilon > 0$ i fer la conjectura depenent de manera adequada de ϵ. Això és el que varen fer, simultàniament, David Masser i Joseph Oesterlé, [Oe], l'any 1985.

9 CONJECTURA (LA CONJECTURA ABC (MASSER I OESTERLÉ)) *Per a tot $\epsilon > 0$, existeix una constant K_ϵ tal que, si $a + b = c$ amb a, b i c enters primers entre si, aleshores*

$$\max\{|a|, |b|, |c|\} \leq K_\epsilon \,\mathrm{rad}(abc)^{1+\epsilon}.$$

S'ha de dir que els motius que tenien per a fer aquesta conjectura no eren únicament els que nosaltres hem presentat aquí. De fet, un dels objectius d'aquest escrit és explicar com aquesta conjectura està relacionada directament amb multitud de conjectures i de resultats de la teoria de nombres i la geometria aritmètica.

A part d'aquesta conjectura, hi ha també versions més explícites. Per exemple, es conjectura que si prenem $\epsilon = 1$, aleshores podem prendre $K_1 = 1$. Així tindríem

$$\max\{|a|, |b|, |c|\} \leq \mathrm{rad}(abc)^2.$$

A més hi ha una versió més forta de la conjectura per Alan Baker de l'any 1996 que explicaria la procedència de l'exponent ϵ de la conjectura *ABC*:

10 CONJECTURA (ALAN BAKER) *Existeixen dues constants absolutes K i L tals que*

$$\max\{|a|, |b|, |c|\} \leq K \,\mathrm{rad}(abc) L^{\omega(\mathrm{rad}(abc))}$$

on $\omega(N)$ és el nombre de primers que divideixen N sense multiplicitat (per tant, $\omega(\mathrm{rad}(abc)) = \omega(a) + \omega(b) + \omega(c)$ ja que a, b i c no tenen factors en comú).

No és difícil veure que aquesta conjectura implica la conjectura *ABC* utilitzant resultats ben coneguts de la teoria de nombres analítica.

4 Què sabem de la conjectura ABC?

El resultat més proper a la conjectura ABC que es coneix és de Cameron L. Stewart i Kun Rui Yu, [S-Y], [S-Y2], que varen demostrar que efectivament el valor absolut de c en la conjectura ABC està fitat per una funció del radical de abc, tot i que la fita depèn exponencialment del radical (i no *polinomialment* tal com prediu la conjectura).

11 TEOREMA (STEWART I YU, 1991-2002) *Existeix una constant efectivament calculable C tal que, si $a+b=c$ amb a, b i c enters primers entre si, aleshores*

$$\max\{|a|,|b|,|c|\} \leq \exp(C\,\mathrm{rad}(abc)^{1/3}(\log \mathrm{rad}(abc))^3)\,.$$

Podem deduir d'aquest resultat que si fixem un conjunt finit de nombres primers S, només hi ha un nombre finit de tripletes (a,b,c) amb a, b i c primers en si amb tots els factors primers a S tals que $a+b=c$.

1 EXERCICI *Busqueu totes aquestes tripletes, i demostreu que efectivament són totes, en el cas que $S=\{2,3\}$, $\{2,5\}$ i $\{2,3,5\}$ (aquest últim és més difícil).*

També se sap que la conjectura ABC es conseqüència de diverses generalitzacions naturals de resultats de teoria de nombres i de geometria aritmètica, com per exemple el teorema de Roth, el teorema de Baker i, molt especialment, el teorema de Faltings (vegeu l'última secció d'aquest article o bé l'article [G-T]).

5 Primeres conseqüències de la conjectura ABC

Anem a veure algunes implicacions de la conjectura ABC en la conjectura de Catalan-Fermat:

Suposem que tenim n, m i r enters positius i a, b i c enters primers entre si i diferents de zero tals que

$$a^n+b^m=c^r,$$

amb $|a|<|b|<|c|$.

La conjectura ABC implica que

$$|c|^r \leq K_\epsilon\,\mathrm{rad}(abc)^{1+\epsilon} \leq K_\epsilon |c|^{3+3\epsilon}\,.$$

Per tant,

$$|c|^{r-3-3\epsilon} \leq K_\epsilon\,.$$

Si $r \geq 4+3\epsilon$, això ens diria que

$$|a| \leq |b| \leq |c| \leq K_\epsilon$$

i, per tant, que sols hi pot haver un nombre finit de solucions de l'equació.

Treballant amb la versió explícita que ens diu que $K_1 = 1$, ens diria que si

$$a^n + b^m = c^r,$$

amb $|a| < |b| < |c|$, aleshores $r \leq 6$.

De la mateixa manera es pot veure que la conjectura ABC implica la conjectura de Fermat generalitzada, i una llista molt llarga d'altres conjectures; vegeu per exemple la pàgina web de Abderrahmane Nitaj, [Ni].

Per posar un altre exemple elemental, no és difícil veure que la conjectura ABC implica que només hi ha un nombre finit de parelles (n, m) de nombres enters positius tals que $n! + 1 = m^2$. El problema de calcular totes aquestes parelles s'anomena el problema de Brocard, i va ser formulat l'any 1876. Ha estat estudiat entre d'altres per Srinivasa Ramanujan i per Paul Erdös, qui va conjecturar que les úniques parelles són $(4, 5)$, $(5, 11)$ i $(7, 71)$.

Anem a veure una conseqüència molt més interessant de la conjectura ABC.

6 ABC i Mordell efectiu

Un dels problemes fonamentals de la teoria de nombres és trobar totes les solucions racionals d'una equació amb coeficients racionals.

Considerem $f(x, y) \in \mathbb{Q}[x, y]$ un polinomi amb coeficients racionals i dues variables. Aquest polinomi ens determina una corba *algebraica* si mirem les seves solucions en els nombres reals, o millor en els nombres complexos. Un resultat fonamental, que dóna origen a la geometria aritmètica, és que la geometria de la corba determina l'aritmètica de les seves solucions racionals.

El primer que podem observar és que, gràcies que existeix una teoria de la desingularització, podem reduir-nos a estudiar les corbes projectives i no singulars (per tant, corbes donades per sistemes d'equacions polinòmiques homogènies, i on la recta tangent en un punt està sempre ben definida).

Si tenim una corba projectiva no singular, els seus punts complexos formen una superfície (de Riemann) orientable i compacta (aquesta és la raó per la qual hem pres la corba projectiva), i per tant és o bé una esfera ($g = 0$) o bé un tor ($g = 1$) o bé un tor amb diverses nanses ($g > 1$).

Per exemple, si $f(x, y)$ té grau 1 o 2, aleshores ens determinarà un corba amb $g = 0$.

O per exemple, si $F(x)$ és un polinomi de grau tres sense arrels repetides (per tal que la corba que ens determini sigui no singular) aleshores la corba donada per l'equació $y^2 = F(x)$ té $g = 1$.

Si $g = 0$, aleshores les solucions racionals són fàcils de descriure: o bé no n'hi ha (i hi ha un mètode efectiu per a saber si n'hi ha o no) o bé hi ha infinites solucions, i tenim una fórmula que les descriu.

Per exemple, si prenem $f(x, y) = x^2 + y^2 - 1$, aleshores les solucions són exactament

$$x = \frac{2t}{1 + t^2} \text{ i } y = \frac{1 - t^2}{1 + t^2}$$

per a cada $t \in \mathbb{Q}$.

Si $g = 1$, tenim el que s'anomena una corba ell·líptica. Aquest cas és més difícil de descriure, ja que pot ser que hi hagi infinites solucions o bé un nombre finit. De fet, la resolució de l'anomenada conjectura de Birch i Swinnerton-Dyer, que és un dels problemes del mil·leni, ens permetria donar un mètode per a saber distingir els dos casos i a més ens permetria saber com donar una fórmula per a trobar totes les solucions racionals.

Finalment arribem al cas en què $g > 1$. Un dels resultats més importants del segle XX és el teorema de Faltings, [Fa], que va ser conjecturat per Mordell, que diu que en aquest cas només hi ha un nombre finit de solucions.

Per exemple, si prenem qualsevol polinomi $F(x) \in Q[x]$ sense arrels múltiples (a $\mathbb{C}$), de grau $d \geq 5$, aleshores l'equació

$$y^2 = F(x)$$

només té un nombre finit de solucions racionals.

O bé, amb les mateixes hipòtesis, si $d \geq 4$ i prenem $f(x, y) := y^d F(x/y)$, obtenim un polinomi homogeni i l'equació

$$f(x, y) = a$$

té només un nombre finit de solucions racionals per a cada $a \in \mathbb{Q}$, $a \neq 0$ que escollim.

La pregunta fonamental és: donada una equació d'aquestes, podem trobar exactament quines són les seves solucions racionals?

Ara per ara la resposta és que no. Fora d'alguns casos en què es poden arribar a calcular quines són les solucions, en general no podem ni tan sols donar una fita per al nombre de solucions.

Això és perquè el teorema de Faltings no és *efectiu*; només demostra que hi ha un nombre finit de solucions, però no ens diu (gairebé) res més. L'any 1991, Noam Elkies, [E], va demostrar, utilitzant el teorema de Belyĭ, que si es provés la conjectura ABC el problema estaria totalment resolt.

12 TEOREMA (ELKIES, 1991) *La conjectura ABC (per a tot $\epsilon > 0$) implica el teorema de Faltings efectiu.*

Dit d'una altra manera, si sabem que la conjectura ABC és certa i sabem calcular efectivament la constant K_ϵ que hi apareix, aleshores tenim un mètode que ens permetria determinar exactament totes les solucions racionals de qualsevol corba amb $g > 1$.

De fet, una mica abans, Laurent Moret-Bailly, [MB], havia demostrat la implicació contrària: si tenim una certa versió explícita del teorema de Faltings, aleshores la conjectura ABC (de fet, una versió lleugerament més feble de la conjectura) és certa.

Concretament, el que necessitem és una versió efectiva del teorema de Faltings que ens doni bones fites per a la mida de les solucions de certa equació

concreta amb $g = 2$ però ara no només a $\mathbb{Q}$ sinó a tot cos de nombres, és a dir, tota extensió $K/\mathbb{Q}$ finita (com per exemple $\mathbb{Q}(\sqrt{2})$). Moret-Bailly considera la corba donada per l'equació $y^2 + y = x^5$, i estudia els seus punts als cossos de la forma $K := \mathbb{Q}(\sqrt[5]{m})$, on m és un enter. La seva afirmació és que, si és cert que totes les solucions d'aquesta equació en qualsevol cos K com el d'abans tenen mida (el que tècnicament es diu altura) fitada en funció del discriminant del cos d'una manera concreta (el que ell anomena la hipòtesi ME), aleshores la conjectura ABC és certa per a un cert ϵ.

Referències

[Be] BEUKERS, F. «The Diophantine Equation $Ax^p + By^q = Cz^r$». *Duke Math. J.*, 91 (1998), 61–88.

[B1] BRUIN, N. «The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$». *Compositio Math.*, 118 (1999), núm. 3, 305–321.

[B2] BRUIN, N. «The primitive solutions to $x^3 + y^9 = z^2$». *J. Number Theory*, 111 (2005), núm. 1, 179–189.

[Br] BRUN, V. «Über hypothesenbildung». *Arc. Math. Naturvidenskab*, 34 (1914), 1–14.

[D-M] DARMON, H.; MEREL, L. «Winding quotients and some variants of Fermat's last theorem». *J. Reine Angew. Math.*, 490 (1997), 81–100.

[Ed] EDWARDS, J. «A Complete Solution to $X^2 + Y^3 + Z^5 = 0$». *J. Reine Angew. Math.*, 571 (2004), 213–236.

[E] ELKIES, N. D. «*ABC* implies Mordell». *Internat. Math. Res. Notices*, 7 (1991), 99–109.

[Fa] FALTINGS, G. «Endlichkeitssätze für abelsche Varietäten über Zahlkörpern». *Invent. Math.*, 73 (1983), núm. 3, 349–366.

[G-T] GRANVILLE, A.; TUCKER, T. J. «It's as easy as abc». *Notices Amer. Math. Soc.*, 49 (2002), núm. 10, 1224–1231.

[Kr] KRIEGER, M. H. «A 1940 letter of André Weil on analogy in mathematics». *Notices Amer. Math. Soc.*, 52 (2005), núm. 3, 334–341.

[M] MASSER, D. W. «Note on a conjecture of Szpiro». Séminaire sur les Pinceaux de Courbes Elliptiques (París, 1988). *Astérisque*, 183 (1990), 19–23.

[Ma] MAULDIN, R. D. «A generalization of Fermat's last theorem: the Beal conjecture and prize problem». *Notices Amer. Math. Soc.*, 44 (1997), núm. 11, 1436–1437.

[Mi] MIHĂILESCU, P. «Primary cyclotomic units and a proof of Catalan's conjecture». *J. Reine Angew. Math.*, 572 (2004), 167–195.

[Mo] MORDELL, E. J. *Diophantine equations*. Londres-Nova York: Academic Press, 1969.

[MB] MORET-BAILLY, L. «Hauteurs et classes de Chern sur les surfaces arithmétiques». Séminaire sur les Pinceaux de Courbes Elliptiques (París, 1988). *Astérisque*, 183 (1990), 37–58.

[Ni] NITAJ, A. *The ABC Conjecture* [en línia]. http://www.math.unicaen.fr/~nitaj/abc.html

[Oe] OESTERLÉ, J. «Nouvelles approches du "théorème"de Fermat». Séminaire Bourbaki, Vol. 1987/88. *Astérisque*, 161–162 (1988), Exp. Núm. 694, 4, 165–186.

[PSS] POONEN, B.; SCHAEFER, E.; STOLL, M. *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*. ArXiv, Math.NT/0508174, 2005.

[R] RIBENBOIM, P. «La conjectura de Catalan». *Butlletí de la Societat Catalana de Matemàtiques*, 11 (1) (1996), 95–105.

[Ri] RIBET, K. A. «On the equation $a^p + 2^\alpha b^p + c^p = 0$». *Acta Arith.*, 79 (1997), núm. 1, 7–16.

[S-Y] STEWART, C. L.; YU, K. R. «On the abc conjecture». *Math. Ann.*, 291 (1991), núm. 2, 225–230.

[S-Y2] STEWART, C. L.; YU, K. R. «On the abc conjecture. II». *Duke Math. J.*, 108 (2001), núm. 1, 169–181.

[T-W] TAYLOR, R.; WILES, A. «Ring-theoretic properties of certain Hecke algebras». *Ann. of Math.*, (2) 141 (1995), núm. 3, 553–572.

[Ti] TIJDEMAN, R. «On the Equation of Catalan». *Acta Arith.*, 29 (1976), 197–209.

[Wi] WILES, A. «Modular elliptic curves and Fermat's last theorem». *Ann. of Math.*, (2) 141 (1995), núm. 3, 443–551.

DEPARTAMENT DE MATEMÀTIQUES
UNIVERSITAT AUTÒNOMA DE BARCELONA
08193 BELLATERRA, BARCELONA
xarles@mat.uab.es