El ABC de la Aritmética

por

Xavier Xarles*

Este artículo es una versión revisada, actualizada y (espero) mejorada del publicado en catalán en [Xa], que a su vez fue una versión por escrito de la lección inaugural del curso 2004/05 de la *Secció de Matemàtiques de la Universitat Autònoma de Barcelona*. Esta charla iba dirigida a alumnos de la licenciatura, y he intentado mantener el nivel suficientemente comprensible para no expertos en la materia, aunque sin intención de engañar al lector. De todos modos me guiaré por la máxima de que «las ideas predominen sobre las demostraciones».

Aunque está claro que no se pueden hacer Matemáticas con medias verdades o engaños, es aún más cierto que no se pueden hacer sin ideas (aunque pueda parecerlo para un foráneo). El objetivo de esta nota es explicar una intuición que, por decirlo de algún modo, justificaría la verdad de muchos de los últimos teoremas aritméticos. Por el camino haremos un repaso de algunos de los resultados recientes más importantes de la teoría de números algebraica y la geometría aritmética, intentando enfatizar las ideas comunes subyacentes y sus interrelaciones. De todos modos, animo al lector a profundizar en los resultados que considere más interesantes en los numerosos *surveys* o directamente en los artículos originales.

Los problemas más difíciles y conocidos de la Aritmética son casi siempre cuestiones que relacionan las dos operaciones básicas de los números enteros: la suma y la multiplicación. Así, por un lado, tenemos las conjeturas que relacionan los números primos (un concepto multiplicativo) y la suma, como la conjetura de Goldbach, o la conjetura de los primos gemelos, que involucra los primos y la resta (su versión más general, llamada a veces conjetura de Polignac[1], afirma que cada número par es resta de dos números primos de infinitas maneras). Otras relacionan suma y divisores, como la conjetura sobre la no existencia de números perfectos impares. Y otras, sumas y potencias. En este artículo nos centraremos en estas últimas.

1. Sumas de potencias

Empecemos por recordar el problema más famoso del siglo pasado (o sea, el XX), resuelto en la última década del siglo: el (mal) llamado último teorema de Fermat, verificado por Andrew Wiles en 1994 [Wi], con la ayuda de Pierre de Fermat, Leonhard Euler, Gerhard Frey, Ken Ribet y Richard Taylor, entre otros.

*Subvencionado parcialmente por el proyecto MTM2006-11391 del Ministerio de Educación y Ciencia.

[1]En realidad, la conjetura de Polignac afirma algo más fuerte, y es que cada número par es la diferencia de dos números primos consecutivos de infinitas maneras.

El último Teorema de Fermat (Wiles, 1994). *Sea $n \geq 3$. Si tenemos enteros a, b y c tales que*

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

entonces alguno de ellos es cero, o sea $abc = 0$.

Concretamente, el resultado para $n = 4$ es de Fermat, para $n = 3$ es esencialmente debido a Euler, y Wiles lo demuestra para $n = p > 3$ primo siguiendo una idea de Frey y un resultado de Ribet.

Después de este resultado, se han usado las mismas técnicas para probar otros parecidos, como por ejemplo el siguiente, debido a Ken Ribet [Ri], Henri Darmon y Loïc Merel [D-M]: si $n \geq 3$, y tenemos enteros a, b y c tales que $a^n + b^n = 2c^n$, entonces $abc = 0$ o bien $a = \pm b = \pm c$.

Otra conjetura famosa relacionada con la suma de potencias es la llamada conjetura de Catalan (véase por ejemplo el artículo de Paulo Ribenboim [R1] o [R2]). Esta conjetura no es llamada así, aunque lo parezca, por su relación con ningún catalán, sino por el primero que la formuló, el matemático belga Eugène Charles Catalan, en una carta del año 1844 al editor de la revista de Crelle[2], publicada en el volumen 27 de dicha revista.

La conjetura de Catalan (Mihailescu, 2002). *Sean a, b, c y d números enteros mayores que 1. Si*

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

entonces $a = 3$, $b = 2$, $c = 2$ y $d = 3$.

Esta conjetura fue casi demostrada por Robert Tidjdeman en 1976 [Ti], quien probó que para números enteros a, b, c y d suficientemente grandes la ecuación no tenía solución (dando incluso una cota explícita a partir de la cual la conjetura era cierta, aunque demasiado grande para ser comprobada con un ordenador). Finalmente, el 18 de abril de 2002, Preda Mihailescu anunció que había encontrado una demostración de la conjetura [Mi]. Puede verse un resumen de la demostración en [Me], o bien en el seminario Bourbaki en [Bi].

Estos dos teoremas vienen a decir que la suma de potencias de números enteros suficientemente grandes no puede ser una potencia de un número entero. Esto es lo que afirma la siguiente conjetura, aún no demostrada, llamada por algunos conjetura de Catalan-Fermat (aunque en esto no hay consenso: también es llamada conjetura de Beal y conjetura de Tijdeman-Zagier).

La conjetura de Catalan-Fermat. *Si n, m y r son enteros mayores o iguales que 3, entonces*

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

no tiene ninguna solución con a, b y c enteros primos entre sí y diferentes de cero.

La historia de esta conjetura es bastante curiosa, ya que ha sido propuesta diversas veces en la historia de forma independiente. Parece ser que el primero en formularla fue Vigo Brun el año 1914 [Br]. Según Frits Beukers, Robert Tijdeman

[2] *Journal für die reine und angewandte Mathematik.*

y Don Zagier la redescubrieron en 1994. Pero seguramente quien más la popularizó fue Andrew Beal (véase [Ma]), un multimillonario tejano y matemático amateur[3] que, según él mismo, también la redescubrió en 1994, y la bautizó con su nombre, claro. Además ha ofrecido un premio de 100 000 dólares[4] para el primero que logre resolverla. En cualquier caso, el estudio de las ecuaciones de este tipo tiene una larga historia que después trataremos brevemente.

Antes de seguir, comentaremos la nueva condición que aparece en esta conjetura: la necesidad de que a, b y c sean primos entre sí. Sin esta condición es fácil obtener soluciones, como por ejemplo

$$27^4 + 162^3 = 9^7.$$

Esto no es un caso aislado, dado que de hecho podemos encontrar infinitas soluciones no coprimas para cada elección n y m, sin más que tomar $r = n \cdot m + 1$.

Ejemplo 1. Dados a, b, n y m, si llamamos $c := a^n + b^m$, y d es múltiplo de n y m, entonces, multiplicando por c^d a los dos lados de la igualdad, tenemos que

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

Obsérvese que esta condición no aparecía en los resultados anteriores porque, de hecho, estaba implícita en el enunciado. Por ejemplo, para el teorema de Fermat, si a, b y c verifican la ecuación y no son coprimos, podemos dividir toda la ecuación por su máximo común divisor elevado a n, obteniendo ahora una solución que ya verifica la condición. Esto no es posible hacerlo si los exponentes no son todos iguales.

La conjetura de Catalan-Fermat ha sido explicitada aún más para incluir otros casos. De hecho se sabe, como veremos más adelante, que las soluciones coprimas de la ecuación

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

se comportan de forma diferente dependiendo del valor de su característica

$$\xi(n, m, r) := \frac{1}{n} + \frac{1}{m} + \frac{1}{r}.$$

Caso esférico: Si $\frac{1}{n} + \frac{1}{m} + \frac{1}{r} > 1$, entonces la ecuación tiene, o bien infinitas soluciones coprimas entre sí, o bien ninguna; de hecho se pueden parametrizar, con parametrizaciones conocidas (algunas resueltas recientemente). En concreto, se tiene lo siguiente:

- $\{n, m, r\} = \{2, 2, s\}$, con $s \geq 2$ es bien conocido (por ejemplo [Mo, p. 122]).
- $\{n, m, r\} = \{3, 3, 2\}$ fue resuelto por Louis J. Mordell en 1969 ([Mo, p. 235]).
- $\{n, m, r\} = \{2, 3, 5\}$ fue resuelto en parte por Frits Beukers, Steve Thiboutot y Don Zagier en 1998 [Be], y definitivamente por Johnny Edwards el 2001 [Ed].
- $\{n, m, r\} = \{2, 3, 4\}$ fue resuelto casi totalmente por Don Zagier en 1998, y definitivamente por Johnny Edwards en 2001 [Ed].

[3] También conocido por ser la persona que más dinero ha ganado al póker en un solo día.
[4] Véase la página `www.bealconjecture.com`.

Caso Euclídeo: Si $\frac{1}{n}+\frac{1}{m}+\frac{1}{r}=1$, entonces no hay soluciones aparte de las triviales. Tenemos los casos

- $\{n,m,r\}=\{2,4,4\}$, resuelto por Pierre de Fermat.
- $n=m=r=3$, resuelto por Leonhard Euler.
- $\{n,m,r\}=\{2,3,6\}$, la única solución es la trivial $1^6+2^3=3^2$, y fue resuelto por Leonhard Euler.

Caso Hiperbólico: Si $\frac{1}{n}+\frac{1}{m}+\frac{1}{r}<1$ (y por lo tanto $\frac{1}{n}+\frac{1}{m}+\frac{1}{r}\leq\frac{41}{42}$), entonces hay un número finito de soluciones. Los únicos casos con soluciones conocidas son:

- Si $n>6$, la solución general $2^3+1^n=3^2$.
- Si $\{n,m,r\}=\{2,3,7\}$ (único caso en que $\frac{1}{n}+\frac{1}{m}+\frac{1}{r}=\frac{41}{42}$, el valor máximo), todas las soluciones son (Bjorn Poonen, Ed Schaefer y Michael Stoll, 2004, [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 $\{n,m,r\}=\{2,3,8\}$, todas las soluciones son (Nils Bruin, 1999, [B1]):
  1. $33^8+1549034^2=15613^3$,
  2. $43^8+96222^3=30042907^2$.
- Si $\{n,m,r\}=\{2,3,9\}$, todas las soluciones son (Nils Bruin, 2003, [B2]):
  1. $7^3+13^2=2^9$.
- Si $\{n,m,r\}=\{2,4,5\}$, todas las soluciones son (Nils Bruin, 1999, [B1]):
  1. $2^5+7^2=3^4$,
  2. $3^5+11^4=122^2$.

Todos estos casos hiperbólicos se han resuelto gracias a las últimas herramientas desarrolladas para el cálculo efectivo de soluciones racionales de curvas algebraicas. Estas técnicas muy recientes, concretamente las llamadas Chabauty-Coleman y Chabauty elíptico, permiten certificar que las únicas soluciones de una cierta ecuación son las de una lista previamente calculada, pero sólo funcionan para determinado tipo de curvas y después de cálculos muy arduos con ordenador. Veremos un poco más sobre ellas en la sección 6.

Los únicos exponentes para los que se conoce alguna solución son

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

y se conjetura que no hay otras soluciones. Esto se sabe para algunos casos, por ejemplo:

- Para los valores $\{n,m,r\}$ en que se conoce alguna solución, se sabe que no hay más, tal como se indicó arriba.

- Para $n = m > 3$ y $r = 2$, se sabe que no hay soluciones, por Darmon y Merel [D-M] y Björn Poonen [Po], después del resultado de modularidad de Andrew Wiles [Wi] completado por Christophe Breuil, Brian Conrad, Fred Diamond y Richard Taylor [BCDT].
- Para $n = m > 2$ y $r = 3$, se sabe que no hay soluciones, por Darmon y Merel [D-M] y Björn Poonen [Po].

Esta conjetura se puede inscribir en una conjetura aún más general que fue formulada por Henry Darmon y Andrew Granville el año 1993 [D-G].

La conjetura de Fermat Generalizada. *Sean A, B y C tres números enteros diferentes de cero y primos entre sí. Entonces hay un número finito de enteros x^n, y^m y z^r, donde n, m y r son naturales con $1/n+1/m+1/r < 1$ y x, y, z son enteros con $xyz \neq 0$ y primos entre sí, tales que*

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

Darmon y Granville demuestran que, si fijamos los exponentes n, m y r, hay un número finito de soluciones primitivas.

Teorema 1 (Darmon-Granville [D-G]). *Sean A, B y C tres números enteros diferentes de cero y primos entre sí, y sean n, m y r números naturales con $1/n+1/m+1/r < 1$. Entonces existe un número finito de enteros x, y, z, con $xyz \neq 0$ y primos entre sí, tales que*

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

La demostración se basa en el teorema de Faltings [Fa] (antes llamado conjetura de Mordell). Más adelante comentaremos algo sobre este resultado de Gerd Faltings, y concretamente el hecho que sea un resultado sólo de finitud de soluciones, sin ninguna indicación de cómo encontrarlas todas.

La idea común a todas estas conjeturas (y principalmente la última) es la siguiente máxima aritmética: si sumas dos números divisibles por potencias elevadas de enteros no puedes obtener un número divisible por una potencia elevada de un entero. Veremos que aún se puede afinar mucho más esta máxima en una inecuación conjetural que resume la intuición actual que tenemos de estos problemas.

Para llegar a esta formulación razonaremos por analogía con los polinomios. Éste es de hecho un truco habitual en teoría de números: los enteros y los polinomios se parecen tanto que muchos de los teoremas son idénticos en los dos casos, y, si no son idénticos, son muy similares. Estas analogías han sido una guía constante en teoría de números los últimos 100 años, empezando por Richard Dedekind, David Hilbert y André Weil (véase por ejemplo la carta publicada en [Kr]), y acabando por las ideas que llevaron a la geometría de Arakelov.

2. El ABC de los polinomios

Vamos a ver primero cómo muchos de los resultados que tanto costó demostrar para los enteros son mucho más fáciles para los polinomios. Consideraremos en esta

sección polinomios en una variable con coeficientes reales o complejos, aunque los mismos resultados (¡con las mismas demostraciones!) son igualmente válidos con coeficientes en cualquier cuerpo de característica 0 (e, incluso, de característica positiva, con pequeñas modificaciones).

El primer resultado se debe a Joseph Liouville en 1851 (aunque la demostración que damos es posterior).

Teorema 2 (Fermat Polinómico). *Sea $n \geq 3$ un entero. Entonces no existen polinomios $X(t)$, $Y(t)$ y $Z(t)$ con coeficientes en un cuerpo de característica cero, primos entre sí y de grado mayor que 0, tales que $X(t)^n + Y(t)^n = Z(t)^n$.*

Demostración. Supongamos que existan tales soluciones. Derivamos respecto a t en la ecuación $X(t)^n + Y(t)^n = Z(t)^n$, dividimos por n (aquí es el único sitio donde se usa la característica cero), y obtenemos

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

Multiplicamos la primera ecuación por Y' y la segunda por Y, y restamos, para obtener

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

Puesto que X y Z son primos entre sí, obtenemos de esta ecuación que X^{n-1} divide a $ZY' - YZ'$. Dado que Y y Z son primos entre sí, $ZY' - YZ' = Y^2(Z/Y)' \neq 0$.

Consideremos ahora los grados de los polinomios. Tenemos que

$$(n-1)\deg(X) \leq \deg(ZY' - YZ') \leq \deg(Y) + \deg(Z) - 1,$$

o sea

$$n\deg(X) < \deg(X) + \deg(Y) + \deg(Z).$$

Repitiendo el argumento para Y y para Z, tenemos tres inecuaciones que al sumarlas nos dan

$$n(\deg(X) + \deg(Y) + \deg(Z)) < 3(\deg(X) + \deg(Y) + \deg(Z))$$

y por lo tanto $n < 3$. □

Observación 1. Además, la misma demostración prueba que no tenemos soluciones en polinomios de grado mayor que 1 y primos entre sí de la ecuación $X(t)^n + Y(t)^m = Z(t)^r$ si n, m y r son mayores o iguales que 3.

El año 1983, Richard C. Mason [Mas] descubrió una desigualdad, que él llamó «desigualdad fundamental», y que ahora denominamos teorema ABC polinómico, que generaliza este resultado y que de alguna forma descubre una propiedad fundamental de la suma respecto del producto en el caso de los polinomios. De hecho, W. W. Stothers ya había publicado este resultado en 1981 [St], aunque nadie cayó en la cuenta de su importancia.

Antes de enunciar el teorema vamos a introducir una notación usual. Llamamos *radical* de un polinomio $P(t)$, y lo denotamos mediante $\mathrm{rad}(P(t))$, al producto de sus factores irreducibles sin repetición. Así,

$$\mathrm{rad}(P(t)) := \prod_{\alpha \text{ raíz de } P(t)} (t-\alpha)$$

donde las raíces son en una clausura algebraica y sin repetición.

Teorema 3 (Mason, Stothers). *Sean $A(t)$, $B(t)$ y $C(t)$ tres polinomios no constantes con coeficientes en un cuerpo K de característica 0, primos entre sí, y tales que $A+B=C$. Entonces*

$$\max(\deg(A),\deg(B),\deg(C)) < \deg(\mathrm{rad}(ABC)) = \sharp\{\alpha \in \overline{K} \mid \alpha \text{ raíz de } ABC\},$$

donde $\overline{K}$ denota una clausura algebraica de K (y estamos usando $\sharp$ para indicar el cardinal de un conjunto).

Daremos la demostración casi elemental de Joseph Oesterlé en [Oe].

Demostración. Consideremos el polinomio

$$\Delta(t) := \begin{vmatrix} A & B \\ A' & B' \end{vmatrix} = \begin{vmatrix} A & C \\ A' & C' \end{vmatrix} = \begin{vmatrix} C & B \\ C' & B' \end{vmatrix};$$

estas igualdades son fáciles de comprobar usando, por ejemplo, operaciones elementales de matrices. El hecho de que A y B son primos entre sí nos da que $\Delta \neq 0$.

Vamos a ver que A, B y C dividen al polinomio $\Delta(t)\,\mathrm{rad}(ABC)$. Por simetría sólo tenemos que verlo para A. Supongamos que α es una raíz de A con multiplicidad e. Entonces $(t-\alpha)^e$ divide a $A(t)$ y $(t-\alpha)^{e-1}$ divide a $A'(t)$; por lo tanto $(t-\alpha)^e$ divide a

$$\Delta(t)(t-\alpha) = (AB' - BA')(t-\alpha),$$

lo que demuestra la afirmación.

Dado que A, B y C son primos entre sí, obtenemos que ABC divide al polinomio $\Delta(t)\prod(t-\alpha)$. Para concluir sólo es necesario observar que

$$\deg(\Delta) \leq \deg(A) + \deg(B) - 1$$

y que

$$\deg(A) + \deg(B) + \deg(C) \leq \deg(\Delta) + \deg(\mathrm{rad}(ABC)).$$

Combinando las dos desigualdades nos da la desigualdad buscada para $\deg(C)$. Por simetría, lo mismo ocurre con A y B. □

Vamos a ver que la conjetura de Catalan-Fermat para polinomios se deduce inmediatamente de este resultado. De hecho se deduce un resultado aún más fuerte.

Corolario 1. *Sean $A(t)$, $B(t)$ y $C(t)$ tres polinomios no constantes, con coeficientes en un cuerpo de característica 0, primos entre sí, y tales que $A+B=C$. Entonces*

$$\frac{\deg(\mathrm{rad}(A))}{\deg(A)} + \frac{\deg(\mathrm{rad}(B))}{\deg(B)} + \frac{\deg(\mathrm{rad}(C))}{\deg(C)} > 1.$$

Demostración. Podemos suponer que $\max(\deg(A), \deg(B), \deg(C)) = \deg(C)$. Entonces el teorema ABC polinómico nos dice que

$$\deg(C) < \deg(\mathrm{rad}(ABC)) = \deg(\mathrm{rad}(A)) + \deg(\mathrm{rad}(B)) + \deg(\mathrm{rad}(C)).$$

Dividiendo por $\deg(C)$ obtenemos

$$\begin{aligned} 1 &< \frac{\deg(\mathrm{rad}(A))}{\deg(C)} + \frac{\deg(\mathrm{rad}(B))}{\deg(C)} + \frac{\deg(\mathrm{rad}(C))}{\deg(C)} \\ &\leq \frac{\deg(\mathrm{rad}(A))}{\deg(A)} + \frac{\deg(\mathrm{rad}(B))}{\deg(B)} + \frac{\deg(\mathrm{rad}(C))}{\deg(C)}. \end{aligned}$$

□

Obsérvese que $\frac{\deg(C)}{\deg(\mathrm{rad}(C))}$ es la media aritmética de las multiplicidades de los ceros de C. Este corolario nos dice así que la media armónica de las medias aritméticas de las multiplicidades de los ceros es menor que 3. La demostración del siguiente resultado es inmediata a partir de aquí.

Corolario 2 (Catalan-Fermat polinómico). *Sea n, m y r enteros positivos tales que $\frac{1}{n} + \frac{1}{m} + \frac{1}{r} < 1$. Entonces no existen polinomios $X(t)$, $Y(t)$ y $Z(t)$, primos entre sí y de grado mayor que 0, tales que $X(t)^n + Y(t)^m = Z(t)^r$.*

Vamos a ver en la siguiente sección cómo podemos traducir este resultado a una conjetura plausible para números enteros.

3. En busca del ABC perdido

El primer concepto que necesitamos traducir de polinomios a enteros es el de radical de un número. Esto está claro: dado que lo análogo de los factores irreducibles de un polinomio es, para enteros, los factores primos, el *radical* de un número entero diferente de 0 (también llamado *conductor* del número) es el producto de los números primos diferentes que dividen al número dado. Así, si

$$n = p_1^{e_1} \cdots p_r^{e_r} \quad \text{con } p_i \neq p_j \text{ si } i \neq j, \quad p_i \text{ números primos},$$

entonces

$$\mathrm{rad}(n) := p_1 \cdots p_r.$$

Llamaremos *triple ABC* a una terna de números enteros diferentes de 0 y primos entre sí dos a dos tales que $A + B = C$.

Así, podríamos pensar, de forma muy naïf, que el análogo del teorema ABC para enteros podría ser que, dado un triple ABC, el número de factores primos de C contados con multiplicidad (llamado habitualmente $\Omega(C)$) es menor que el número de factores primos del radical de ABC (llamado también $\omega(ABC)$). O sea

Conjetura muy naïf:

$$\text{Si } A + B = C, \quad \text{con } (A, B) = 1, \quad \text{entonces } \Omega(C) \leq \omega(ABC).$$

¡Pero esta «conjetura» es claramente falsa! Por ejemplo, si tenemos un primo de Mersenne, o sea un primo $q := 2^p - 1$, con p primo, entonces tenemos el triple ABC $q + 1 = 2^p$, y se cumple que $\Omega(C) = \Omega(2^p) = p$, y $\omega(ABC) = \omega(q2^p) = 2$. Obsérvese que se conjetura la existencia de infinitos primos de Mersenne, y se conocen primos de Mersenne muy grandes, así que no es posible esperar este resultado ni tan siquiera modificando la conjetura naïf con una constante:

Conjetura muy naïf modificada: Existe $K > 1$ constante tal que

$$\text{si } A + B = C, \quad \text{con } (A, B) = 1, \quad \text{entonces } \Omega(C) \leq K\omega(ABC).$$

El punto clave está en pensar que el grado de un polinomio irreducible no es igual a uno si el cuerpo no es algebraicamente cerrado, y que los enteros se parecen más a los polinomios sobre (por ejemplo) el cuerpo de los racionales que sobre el cuerpo de los complejos.

Por lo tanto primero tenemos que encontrar cuál puede ser el análogo del grado para un entero. Observemos que el grado es una función que asigna a cada polinomio un número, y que el grado del producto es la suma de los grados. Si queremos una función que cumpla esto último para los enteros positivos, y queremos que se extienda a los reales positivos de forma continua, entonces la función tiene que ser un logaritmo. Este hecho es bien conocido para los expertos en teoría analítica de números, que dicen que los primos p se cuentan mejor con peso $\log(p)$.

Así podríamos conjeturar que se cumple

Conjetura naïf:

$$\text{Si } A + B = C, \quad \text{con } (A, B) = 1, \quad \text{entonces } \log(|C|) \leq \log(\text{rad}(ABC)),$$

o, equivalentemente, que

$$\text{si } A + B = C, \quad \text{con } (A, B) = 1, \quad \text{entonces } \max(|A|, |B|, |C|) \leq \text{rad}(ABC).$$

Ahora bien, esta última conjetura aún no es cierta, aunque parece un poco más cierta que la anterior. Por ejemplo, tenemos que $1+8 = 9$, de donde debería seguirse que $9 < 2 \cdot 3 = 6$, y también que $1 + 63 = 2^6$, de donde tendríamos que $2^6 = 64 < 2 \cdot 3 \cdot 7 = 42$.

Podemos pensar que tenemos que modificar ligeramente la conjetura incluyendo una constante K, diciendo que

Conjetura naïf modificada: Existe $K > 1$ constante tal que

$$\text{si } A + B = C, \quad \text{con } (A, B) = 1, \quad \text{entonces } \max(|A|, |B|, |C|) \leq K\,\text{rad}(ABC).$$

Pero incluso esta conjetura es también falsa, como prueba el ejemplo siguiente.

Contraejemplo 1. Sea p un número primo, y consideremos

$$A = 2^{p^{r-1}(p-1)},\ B = -1 \text{ y } C = 2^{p^{r-1}(p-1)} - 1.$$

Entonces p^r divide a c, por el teorema de Fermat-Euler, ya que

$$\phi(p^r) = p^{r-1}(p-1) \quad \text{y} \quad 2^{p^{r-1}(p-1)} \equiv 1 \pmod{p^r}.$$

Por lo tanto tenemos que $\text{rad}(ABC) \leq 2c/p^{r-1}$. Así, si la desigualdad fuera cierta tendríamos que $K \geq p^{r-1}/2$ para todo número primo p y todo $r \geq 2$.

Antes de darnos por vencidos, observemos que, si hubiéramos puesto la constante K en la primera versión de la conjetura naïf, habríamos obtenido otra posible modificación.

Conjetura naïf modificada de otra forma: Existe $K > 1$ constante tal que

$$\text{si } A + B = C, \quad \text{con } (A, B) = 1, \quad \text{entonces } \log(|C|) \leq K \log(\text{rad}(ABC)),$$

o, equivalentemente, que

$$\text{si } A + B = C, \quad \text{con } (A, B) = 1, \quad \text{entonces } \max(|A|, |B|, |C|) \leq \text{rad}(ABC)^K.$$

Finalmente hemos llegado a una conjetura que parece plausible. De hecho la conjetura ABC es una conjetura un poco más fuerte que esta conjetura, poniendo la constante $K = 1 + \epsilon$, y diciendo que la desigualdad es válida para todo $\epsilon > 0$ si multiplicamos el radical por una constante que sólo depende de ϵ.

La conjetura ABC (Masser y Oesterlé). *Para todo $\epsilon > 0$, existe una constante K_ϵ tal que, si $A + B = C$ con A, B y C enteros primos entre sí, entonces*

$$\max\{|A|, |B|, |C|\} \leq K_\epsilon \, \text{rad}(ABC)^{1+\epsilon}.$$

Una versión un poco más débil de la conjetura fue la que formuló Oesterlé originariamente en [Oe]. Dado un triple ABC, definamos

$$L(A, B, C) := \frac{\log \max(|A|, |B|, |C|)}{\log \text{rad}(ABC)}.$$

La conjetura afirma que, para todo $K > 1$, existe sólo un número finito de triples ABC tales que

$$L(A, B, C) > K.$$

Aún hay otra versión mucho más débil de la conjetura, pero de la cual se decidirían aún la validez de conjeturas como la de Catalan-Fermat de modo asintótico.

La conjetura ABC débil (Masser y Oesterlé). *Para todo $\epsilon > 0$, existe una constante K_ϵ tal que, si $A + B = C$ con A, B y C enteros primos entre sí, entonces*

$$|ABC|^{\frac{1}{3}} \leq K_\epsilon \, \text{rad}(ABC)^{1+\epsilon}.$$

Y hay además una serie de conjeturas más específicas y/o más fuertes, dos de las cuales detallamos a continuación (véase la página de Abderrahmane Nitaj [Ni] para muchas otras):

- $K_1 = 1$, o sea
$$\text{máx}\{|A|, |B|, |C|\} \leq \text{rad}(ABC)^2.$$
- (Granville) Si $\Theta(N)$ es el número de enteros menores o iguales que N tales que todos sus factores primos son factores primos de N, entonces existe una constante absoluta K tal que
$$\text{máx}\{|A|, |B|, |C|\} \leq K\Theta(\text{rad}(ABC))\,\text{rad}(ABC).$$

4. Algunas consecuencias de la conjetura ABC

Vamos a empezar por ver cómo todas las conjeturas de la primera sección, en concreto la conjetura de Catalan-Fermat y la conjetura de Fermat Generalizada, se pueden deducir (en algunos casos de forma débil) de la conjetura ABC.

Supongamos que tenemos n, m y r enteros positivos y a, b y c enteros primos entre sí y positivos, tales que
$$a^n + b^m = c^r,$$
con $0 < a^n \leq b^m < c^r$.

La conjetura ABC implica que
$$c^r \leq K_\epsilon\,\text{rad}(abc)^{1+\epsilon} \leq K_\epsilon(abc)^{1+\epsilon}.$$
Dado que $a < c^{r/n}$ y que $b < c^{r/m}$, tenemos
$$c^r \leq K_\epsilon(c^{1+\frac{r}{n}+\frac{r}{m}})^{1+\epsilon}.$$
De este modo
$$c^{1-(\frac{1}{r}+\frac{1}{n}+\frac{1}{m})(1+\epsilon)} \leq K_\epsilon^{\frac{1}{r}}.$$
De aquí obtenemos, por ejemplo, que, si $\frac{1}{r} + \frac{1}{n} + \frac{1}{m} \leq 1 - \epsilon$, entonces
$$0 < a^n < b^m < c^r \leq K_\epsilon^{\epsilon^2}$$
y por lo tanto sólo puede haber un número finito de soluciones. Además, si conocemos la constante K_ϵ, podemos calcular todas las soluciones explícitamente. Dado que $\frac{1}{r} + \frac{1}{n} + \frac{1}{m} < 1$ implica $\frac{1}{r} + \frac{1}{n} + \frac{1}{m} \leq \frac{42}{41}$, sería suficiente conocer la conjetura para algún $\epsilon < \frac{1}{41}$.

En caso de que supiésemos que $K_1 = 1$, obtendríamos también que, si
$$a^n + b^m = c^r,$$
con $(a, b) = 1$, entonces $\frac{1}{r} + \frac{1}{n} + \frac{1}{m} \geq \frac{1}{2}$. Por lo tanto lo reduciríamos a probar unas cuantas familias de ecuaciones en las que $\frac{1}{r} + \frac{1}{n} \geq \frac{1}{2}$ (por ejemplo, $n = m = 3$, r cualquiera), y una lista finita de casos excepcionales (por ejemplo $n = 3$, $m = 7$ y $7 \leq r \leq 42$).

De la misma forma se puede analizar la conjetura de Fermat Generalizada. Fijamos A, B y C enteros positivos diferentes de cero y primos entre sí, n, m y r enteros

positivos con $1/n+1/m+1/r<1$, y enteros positivos x, y, z con $xyz\neq 0$ y primos entre sí, tales que $Ax^n+By^m=Cz^r$. Vamos a demostrar que hay un número finito de x^n, y^m y z^r verificando estas condiciones.

Primero, podemos suponer $z>1$, ya que con $z=1$ hay claramente un número finito de soluciones x^n e y^m. Sea d el máximo común divisor de Ax^n, By^m y Cz^r (está claro que hay sólo un número finito de posibles valores para d). Aplicando la conjetura ABC al triple $(Ax^n/d, By^m/d, Cz^r/d)$, tenemos que

$$Cz^r/d \leq K_\epsilon \operatorname{rad}(ABCx^ny^mz^r/d^3)^{1+\epsilon}.$$

Por tanto, tenemos una constante $L_\epsilon(A,B,C)$, que depende de ϵ, A, B y C, tal que

$$z^r \leq L_\epsilon(A,B,C)(xyz)^{1+\epsilon}.$$

Puesto que $Ax^n<Cz^r$, se cumple $x<C/Az^{r/n}$, e igualmente $y<C/Bz^{r/m}$. Así tenemos otra constante $L'_\epsilon(A,B,C)$ que depende de ϵ, A, B y C tal que

$$z^r \leq L'_\epsilon(A,B,C)z^{r(1+\epsilon)(1/n+1/m+1/r)}.$$

En consecuencia,

$$(z^r)^{1-(1+\epsilon)(1/n+1/m+1/r)} \leq L'_\epsilon(A,B,C).$$

Dado que $1/n+1/m+1/r\leq 41/42$, tomando $\epsilon>0$ suficientemente pequeño (menor que $1/41$), podemos asegurar que $1-(1+\epsilon)(1/n+1/m+1/r)>0$, y por lo tanto z^r está acotado en función de A, B y C, de donde se deduce que x^n y y^m también lo están.

5. ¿Qué sabemos de la conjetura ABC?

Obsérvese que de la conjetura ABC podemos deducir lo siguiente: Fijemos un conjunto finito de números primos S, y consideremos el subconjunto de los enteros $S_\mathbb{Z}$ formado por los enteros con factores primos sólo en S. Entonces sólo hay un número finito de triples ABC con $A+B=C$ y primos entre sí con A, B y C en S.

Este resultado es bien conocido, y su demostración se remonta a Siegel y a Mahler. De hecho el problema es equivalente a la resolución de la llamada ecuación de S-unidades (o *S-unit equation*). Se trata de resolver la ecuación $a+b=1$ con a y b números racionales (tomando $(a,b)=(A/C,B/C)$) que son unidades en el anillo $\mathbb{Z}[1/S]$ obtenido de $\mathbb{Z}$ invirtiendo todos los primos en S. Las técnicas de aproximación diofántica han permitido durante el siglo XX estudiar con detalle este tipo de ecuaciones.

De hecho se conocen cotas para el número de soluciones de la ecuación que sólo dependen del número de primos escogidos, y no de los primos en sí. Concretamente, Jan-Hendrik Evertse [Ev] demostró que el número de soluciones está acotado superiormente por $\exp(4s+6)$, donde s es el número de elementos en S. También se sabe que, para cada $\epsilon>0$, hay conjuntos S de s primos, con s arbitrariamente grande, que tienen más de $\exp(s^{2-\sqrt{2}-\epsilon})$ soluciones [K-S].

También se conocen métodos para encontrar, dado S, todas las soluciones de algunas de estas ecuaciones. Por ejemplo, y sólo por citar un caso bien conocido, tenemos el teorema clásico de Carl Størmer [Sto], que analiza el caso en que $A = 1$, dando un algoritmo para encontrar todas las soluciones. En general, se pueden dar cotas específicas para el tamaño de las soluciones, dependiendo de los primos que aparecen en S, como veremos a continuación.

Usando el mismo tipo de técnicas salidas de la teoría de trascendencia, esencialmente el estudio de las formas logarítmicas, se conoce un resultado, debido a Cameron L. Stewart y Kun Rui Yu [S-Y1], [S-Y2], mucho más cercano a la conjetura ABC. Concretamente Stewart y Yu demostraron que el valor absoluto de c en la conjetura ABC está acotado en función del radical de abc, aunque la cota que obtuvieron depende exponencialmente del radical (y no «polinomialmente» tal y como predice la conjetura).

Teorema 4 (Stewart y Yu, 2002). *Existe una constante efectivamente calculable C tal que, si $a + b = c$ con a, b y c enteros primos entre sí, entonces*

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

Finalmente, sabemos que la conjetura ABC se puede deducir de algunas conjeturas que son versiones efectivas (o más efectivas) de teoremas conocidos. En la siguiente sección veremos en detalle uno de estos resultados fundamentales y cómo se relaciona directamente con la conjetura ABC.

6. ABC y Mordell efectivo

Aunque ya hemos visto en la sección 3 que la conjetura ABC resolvería afirmativamente las conjeturas de la primera sección, esto aún no es suficiente para afirmar que sea una panacea de la aritmética (o cura universal para múltiples problemas aritméticos). A pesar de ello, vamos a ver que, tal como probó Noam Elkies en 1991, la conjetura ABC (o una versión efectiva de ella) resolvería mucho más de lo que aparentemente hace.

Para ello consideraremos el siguiente problema fundamental de la aritmética (y de la geometría aritmética): dado un polinomio $f(x, y) \in \mathbb{Q}[x, y]$ con coeficientes racionales, se trata de determinar si tiene o no soluciones, si tiene un número finito o infinito de ellas, y, en el caso que haya un número finito, calcular efectivamente todas las soluciones.

Una idea fundamental en aritmética, desarrollada durante el siglo XX, es que el comportamiento aritmético de la ecuación $f(x, y) = 0$ (por ejemplo, que tenga o no un número finito de soluciones) está determinado por la geometría (en $\mathbb{C}$) de la curva asociada, y concretamente por su género (que es un invariante topológico de la curva proyectiva definida por $f(x, y) = 0$ sobre $\mathbb{C}$).

El género es un número natural asociado a toda curva algebraica, que coincide con el género topológico de la superficie dada por los puntos en $\mathbb{C}$ en el caso no singular. Por ejemplo, si consideramos un polinomio $g(x) \in \mathbb{Q}[x]$ en una variable de grado d y sin raíces múltiples en $\mathbb{C}$, entonces el polinomio $f(x, y) = y^2 - g(x)$

tiene género g igual a la parte entera de $(d-1)/2$ (si $d=3$, esto da lugar a las denominadas curvas elípticas y, si $d>4$, a las curvas hiperelípticas). Y si tomamos $f(x,y) := y^d g(x/y) - a$, donde $a \neq 0$ es un número racional (así se obtienen las curvas de Thue[5]), entonces el género es igual a $(d-1)(d-2)/2$.

En el caso en que el género es 0, la ecuación o bien no tiene soluciones o bien tiene un número infinito de ellas (y de hecho parametrizables por funciones racionales). Si el género es 1, entonces la determinación de si tiene o no un número finito o infinito de soluciones depende, según la famosa conjetura de Birch y Swinnerton-Dyer[6], de otro invariante (que esencialmente cuenta cuántas soluciones tiene la ecuación módulo p al variar los primos p).

Y finalmente, si el género es 2 o superior, entonces el número de soluciones es finito. Este resultado, debido a Gerd Faltings [Fa] y por el que se le concedió la medalla Fields, es uno de los grandes logros de la geometría aritmética. Pero tiene un hándicap importante para los que quieren resolver ecuaciones concretas: que aparte de decirnos que sólo hay un número finito de soluciones, no nos dice (casi) nada más.

Para atacar el problema del cómputo explícito de todas las soluciones de una ecuación dada, se han desarrollado últimamente varias técnicas que permiten estar seguros de tener todas las soluciones después de largos cálculos con la ayuda del ordenador. Estas técnicas, salidas de un método debido a Claude Chabauty y refinado por Robert Coleman, pasan por calcular el grupo de puntos racionales de la jacobiana de la curva, cálculo que en principio es posible[7], pero que en la práctica puede ser muy largo. El método original, además, sólo podía aplicarse bajo ciertas condiciones restrictivas, aunque se ha modificado para, en principio, poder aplicarse iterativamente a curvas obtenidas a partir de la original (y esperar que siempre lleguemos a una que verifique las condiciones). Puede consultarse el artículo [PSS] para ver ejemplos de cómo usar estos métodos.

Por otra parte, dado que el número de soluciones racionales es finito, debería ser posible dar una cota para el tamaño de las soluciones en función de los coeficientes de f. El problema, llamado de Mordell efectivo (o Faltings efectivo), consiste precisamente en esto: encontrar una fórmula en términos de los coeficientes de f de la llamada *altura* de una solución. Si $(a,b) \in \mathbb{Q}$, y escribimos $a = A/C$ y $b = B/C$ con A, B y C enteros primos entre sí, entonces la altura de (a,b) es, por definición, $H(a,b) := \max(|A|,|B|,|C|)$. Obsérvese que sólo hay un número finito de puntos racionales con altura acotada superiormente por una constante, y además es fácil dar la lista completa. Por lo tanto, si tuviéramos Mordell efectivo, podríamos calcular la lista de todas las soluciones racionales simplemente probando para cada punto de la lista si es o no solución.

Teorema 5 (Elkies, 1991). *Si la conjetura ABC es cierta para todo ϵ, entonces Mordell efectivo es cierto. Además la cota efectiva depende de conocer los valores K_ϵ.*

[5]Por Axel Thue, quien demostró que, si $d>2$ y $g(x)$ tiene coeficientes enteros, entonces $f(x,y)=0$ tiene un número finito de soluciones enteras.

[6]Famosa principalmente por ser uno de los siete problemas del milenio.

[7]Aunque la demostración de que los métodos conocidos siempre funcionan pasaría por la resolución de una conjetura de Tate y Shafarevich.

La demostración de este teorema usa un resultado sorprendente de G. V. Belyĭ[8] [B]: para toda curva dada por un polinomio con coeficientes en $\mathbb{Q}$ existe una función racional F de la curva ramificada sólo en 0, 1 e ∞[9]. La construcción de esta función es totalmente efectiva, y está relacionada directamente con la teoría de dibujos de niños (o *dessins d'enfants*[10]). Por ejemplo, para la curva de Fermat $x^n + y^n = 1$, la función $F(x, y) = x^n$ cumple las condiciones: salvo para los valores $x = 0$ y para $x^n = 1$ (y $x = \infty$), la antiimagen de x respecto a F (en la curva) tiene exactamente n^2 puntos (sin multiplicidad) en $\mathbb{C}$ (esto nos dice que la función F tiene grado n^2 como función de la curva).

La idea de la demostración es usar esta función F para ver que cualquier solución racional de la curva que no sea ramificada para F nos da un triple ABC con radical «pequeño» respecto a C (véanse los detalles en [E]).

Para ver el resultado es útil considerar la siguiente conjetura equivalente a la conjetura ABC: dados dos números racionales a y b con $a + b = 1$, la altura de (a, b) está acotada por el producto de los primos p en los que $a \equiv 0, 1$ o ∞ (mód p) elevado a $1 + \epsilon$ por una constante que depende de ϵ. Esta versión de la conjetura permite, además, generalizar la conjetura ABC a otro tipo de números: si K es un cuerpo de números (una extensión finita de $\mathbb{Q}$), entonces tenemos nociones análogas de altura de un punto de K^2 y radical (o conductor) de un número, y la conjetura ABC uniforme de Andrew Granville y H. M. Stark [G-S] predice lo siguiente:

La conjetura ABC uniforme (Granville y Stark). *Dado $\epsilon > 0$, existe una constante K_ϵ tal que, para todo par $(a, b) \in K^2$ con $a + b = 1$ se tiene*

$$H_K(a, b) < K_\epsilon^{[K:\mathbb{Q}]}(|D_K| \operatorname{rad}_K(a, b))^{1+\epsilon},$$

donde D_K denota el discriminante de $K/\mathbb{Q}$.

Otras conjeturas menos ambiciosas proponen que existe una constante dependiente del cuerpo K, sin especificar cómo depende, para la cual se cumple la conjectura. Esta conjetura uniforme está en parte justificada por una conjetura de Vojta [Vo] y por la «gran» conjetura de Mordell, llamada conjetura de Lang, que generalizan el teorema de Faltings a cualquier dimensión. Esta última última conjetura implica, tal como demostraron Lucia Caporaso, Joe Harris y Barry Mazur (véase [CHM]) que existe una cota absoluta (o uniforme) dependiente sólo del género de la curva, para el número de soluciones racionales de una curva definida en $\mathbb{Q}$. Por ejemplo, esto implicaría que existe un número N tal que toda ecuación de la forma $y^2 = p(x)$, con $p(x)$ un polinomio con coeficientes en $\mathbb{Q}$, de grado 5 y sin raíces repetidas en $\mathbb{C}$, tiene a lo sumo N soluciones racionales[11].

[8] Gennadii Vladimirovich Belyĭ.

[9] De hecho, el teorema es mucho más fuerte: una curva definida sobre $\mathbb{C}$ es isomorfa a una curva definida sobre la clausura algebraica de $\mathbb{Q}$ si y sólo si existe una función racional de la curva que sólo ramifica en 0, 1 e ∞.

[10] Una idea introducida por Alexander Grothendieck después de saber del resultado de Belyĭ en su famoso *Esquisse d'un programme*, y que permitiría estudiar la aritmética de las curvas combinatoriamente.

[11] Este resultado es visto de hecho por algunos como un indicio en contra de la conjetura de Lang.

Por otro lado, una cierta versión de la conjetura efectiva de Mordell implicaría la conjetura ABC, o por lo menos la versión débil. De hecho, Laurent Moret-Bailly [MB] demostró que si tenemos buenas cotas para la altura de las soluciones de la ecuación $y^2 + y = x^5$ en los cuerpos de la forma $K := \mathbb{Q}(\sqrt[5]{m})$, con m un entero, en función del discriminante del cuerpo de una forma concreta (lo que él llama «hipótesis ME»), entonces la conjetura ABC es cierta para un cierto ϵ. El hecho de que sea específicamente esta ecuación no es importante: lo importante es que sólo necesitamos Mordell efectivo para una curva concreta pero, esto sí, en una familia infinita de cuerpos.

Además de estos resultados, se sabe que la conjetura ABC es equivalente a varias versiones más explícitas de teoremas famosos, como por ejemplo el Teorema de Roth de aproximación diofántica, o el teorema de Siegel sobre soluciones enteras de ecuaciones en dos variables, e implica algunas otras conjeturas como la conjetura de Schinzel-Tijdeman sobre cuándo un polinomio toma valores que son poderosos[12], e incluso la finitud de soluciones de la ecuación $n! + 1 = m^2$ (Paul Erdős conjeturó que las únicas soluciones son $n = 4, m = 5$; $n = 5, m = 11$; y $n = 7, m = 71$). En el artículo de Andrew Granville y Thomas J. Tucker [G-T] se comentan con más detalle algunas de estas relaciones, y en la página de Abderrahmane Nitaj [Ni] se puede ver una lista bastante exhaustiva de todas ellas.

El resumen final podría ser que la conjetura ABC no es sólo otra conjetura más de las muchas que hay en la aritmética; es una conjetura clave cuyo principal mérito es, además de tener un enunciado muy elemental, el hecho de situarse de forma central en numerosos resultados y conjeturas del final del siglo XX y principios del XXI. Con mucha seguridad podemos predecir que servirá de guía, por lo menos implícitamente, de muchos de los resultados futuros, y tanto si resulta ser cierta como falsa, nos proporcionará una mayor comprensión de la relación, aún tan incomprendida, entre la suma y las propiedades multiplicativas de los números enteros.

Referencias

[B] G. V. Belyĭ, Galois extensions of a maximal cyclotomic field, *Izv. Akad. Nauk SSSR Ser. Mat.* **43** (1979), no. 2, 267–276.

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

[Bi] Y. Bilu, Catalan's conjecture (after Mihailescu), *Astérisque* **294** (2004), 1–26.

[BCDT] C. Breuil, B. Conrad, F. Diamond y R. Taylor, On the modularity of elliptic curves over **Q**: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), no. 4, 843–939.

[B1] N. Bruin, The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, *Compositio Math.* **118** (1999), no. 3, 305–321.

[12]Un número entero n se llama poderoso (*powerful* en inglés) si cumple que, para todo primo p que divide n, p^2 también divide a n. O, equivalentemente, si n se puede expresar como el producto de un cuadrado y un cubo.

[B2] N. Bruin, The primitive solutions to $x^3 + y^9 = z^2$, *J. Number Theory* **111** (2005), no. 1, 179–189.

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

[CHM] L. Caporaso, J. Harris y B. Mazur, Uniformity of rational points, *J. Amer. Math. Soc.* **10** (1997), no. 1, 1–35.

[D-G] H. Darmon y A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = cZ^r$, *Bull. London Math. Soc.* **27** (1995), 513–543.

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

[E] N. D. Elkies, *ABC* implies Mordell, *Internat. Math. Res. Notices* **1991**, no. 7, 99–109.

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

[Ev] J.-H. Evertse, On equations in S-units and the Thue-Mahler equation, *Invent. Math.* **75** (1984), 561–584.

[Fa] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), no. 3, 349–366.

[G-S] A. Granville y H. M. Stark, *abc* implies no "Siegel zeros" for L-functions of characters with negative discriminant, *Invent. Math.* **139** (2000), no. 3, 509–523.

[G-T] A. Granville y T. J. Tucker, It's as easy as *abc*, *Notices Amer. Math. Soc.* **49** (2002), no. 10, 1224–1231.

[K-S] S. Konyagin y K. Soundararajan, Two S-unit equations with many solutions, *J. Number Theory* **124** (2007), 193–199.

[Kr] M. H. Krieger, A 1940 letter of André Weil on analogy in mathematics, *Notices Amer. Math. Soc.* **52** (2005), no. 3, 334–341.

[Mas] R. C. Mason, *Diophantine Equations over Function Fields*, London Mathematical Society Lecture Note Series **96**, Cambridge University Press, Cambridge, 1984.

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

[Ma] R. D. Mauldin, A generalization of Fermat's last theorem: the Beal conjecture and prize problem, *Notices Amer. Math. Soc.* **44** (1997), no. 11, 1436–1437.

[Me] T. Metsänkylä, Catalan's conjecture: another old Diophantine problem solved, *Bulletin of the AMS* **41** (2004), no. 1, 43–57.

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

[Mo] L. J. Mordell, *Diophantine equations*, Academic Press, London y New York, 1969.

[MB] L. Moret-Bailly, Hauteurs et classes de Chern sur les surfaces arithmétiques, *Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988)*, *Astérisque* **183** (1990), 37–58.

[Ni] A. Nitaj, The ABC Conjecture home page, `http://www.math.unicaen.fr/~nitaj/abc.html`

[Oe] J. Oesterlé, Nouvelles approches du "théorème" de Fermat, *Séminaire Bourbaki, Vol. 1987/88*, *Astérisque* **161-162** (1988), Exp. No. 694, 4, 165–186 (1989).

[Po] B. Poonen, Some Diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* **86** (1998), no. 3, 193–205.

[PSS] B. Poonen, E. F. Schaefer y M. Stoll, Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$, *Duke Math. J.* **137** (2007), no. 1, 103–158.

[R1] P. Ribenboim, La conjectura de Catalan, *Butlletí de la SCM* **11** (1996), no. 1, 5–105.

[R2] P. Ribenboim, Catalan's Conjecture, *Amer. Math. Monthly* **103** (1996), 529–538.

[Ri] K. A. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.* **79** (1997), no. 1, 7–16.

[S-Y1] C. L. Stewart y K. R. Yu, On the *abc* conjecture, *Math. Ann.* **291** (1991), no. 2, 225–230.

[S-Y2] C. L. Stewart y K. R. Yu, On the *abc* conjecture. II, *Duke Math. J.* **108** (2001), no. 1, 169–181.

[Sto] C. Størmer, Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications, *Skrifter Videnskabs-selskabet (Christiania), Mat.-Naturv. Kl. I* **2** (1897).

[St] W. W. Stothers, Polynomial identities and Hauptmoduln, *Quart. J. Math. Oxford Ser. (2)* **32** (1981), no. 127, 349–370.

[T-W] R. Taylor y A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math. (2)* **141** (1995), no. 3, 553–572.

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

[Vo] P. Vojta, Diophantine Approximations and Value Distribution Theory, *Lecture Notes in Math.* **1239**, Springer-Verlag, Berlin y Heidelberg, 1987.

[Wi] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), no. 3, 443–551.

[Xa] X. Xarles, L'ABC de l'Aritmètica, *Butlletí de la SCM* **20** (2005), no. 1, 53–66.

Xavier Xarles, Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra, Barcelona

Correo electrónico: `xarles@mat.uab.es`

Página web: `http://mat.uab.cat/~xarles/`