Miscelánea Matemática **47** (2008) 1–10 SMM

El *abc* de una conjetura

Felipe Zaldívar

Departamento de Matemáticas

Universidad Autónoma Metropolitana-I

09340, México, D. F.

México.

fzc@oso.izt.uam.mx

Introducción. En años relativamente recientes, en teoría de números, se han obtenido algunos resultados espectaculares: la demostración de la *conjetura de Mordell* por Faltings en 1983, la *conjetura de Fermat* por Wiles (y Ribet, Serre, Frey) en 1995, la *conjetura de Catalan* por Mihăilescu en 2002, y siguiendo una tendencia hacia la unión o convergencia de ciertas líneas en la matemática, se ha encontrado un hilo común que aparentemente motiva y muestra los aspectos comunes de las conjeturas anteriores y de muchas otras, de tal forma que estos resultados ya no aparecen como aislados o dispersos y la conjetura *abc* que discutiremos en este artículo es un resultado que unifica varias de estas conjeturas.

El abc de polinomios. Si $f(t)$ es un polinomio con coeficientes complejos, pongamos

$$n_0(f) := \text{ número de ceros distintos de } f(t).$$

A principios de la década de 1980, Mason [7] probó el resultado siguiente:

Teorema 1 (Mason)**.** *Sean $a(t), b(t), c(t)$ polinomios en $\mathbb{C}[t]$ coprimos por pares y tales que $a + b = c$. Entonces,*

$$\max\{\operatorname{gr} a, \operatorname{gr} b, \operatorname{gr} c\} \leq n_0(abc) - 1,$$

donde $\operatorname{gr} p$ denota el grado del polinomio $p(t)$.

Demostración. Dividiendo entre c y poniendo $f = a/c$, $g = b/c$, se obtiene que $f + g = 1$, con $f(t)$ y $g(t)$ funciones racionales (cocientes de

polinomios) con coeficientes complejos. Derivando la ecuación anterior obtenemos $f' + g' = 0$, que podemos escribir como

$$\frac{f'}{f} f + \frac{g'}{g} g = 0$$

de tal forma que

$$\frac{b}{a} = \frac{g}{f} = -\frac{f'/f}{g'/g}$$

donde observamos que en el lado derecho las derivadas logarítmicas involucradas hacen que las multiplicidades de los ceros de las funciones racionales correspondientes desaparezcan, ya que si $R(t)$ es una función racional con ceros y polos τ_i de multiplicidades m_i, escribiendo

$$R(t) = R_0 \prod (t - \tau_i)^{m_i},$$

con $m_i \in \mathbb{Z}$ y R_0 una constante, su derivada logarítmica es

$$\frac{R'}{R} = \sum_i \frac{m_i}{t - \tau_i}$$

con polos de multiplicidad 1. Escribamos ahora los polinomios $a(t)$, $b(t)$, $c(t)$ como

$$a(t) = a_0 \prod (t - \alpha_i)^{m_i}, \quad b(t) = b_0 \prod (t - \beta_j)^{n_j}, \quad c(t) = c_0 \prod (t - \gamma_k)^{r_k},$$

con a_0, b_0, c_0 constantes no nulas. Entonces, para las funciones racionales $f(t) = a/c$ y $g = b/c$, sus derivadas logarítmicas son

$$\frac{f'}{f} = \sum \frac{m_i}{t - \alpha_i} - \sum \frac{r_k}{t - \gamma_k}$$

y

$$\frac{g'}{g} = \sum \frac{n_j}{t - \beta_j} - \sum \frac{r_k}{t - \gamma_k}$$

por lo que

$$\frac{b}{a} = -\frac{f'/f}{g'/g} = -\frac{\sum \frac{m_i}{t-\alpha_i} - \sum \frac{r_k}{t-\gamma_k}}{\sum \frac{n_j}{t-\beta_j} - \sum \frac{r_k}{t-\gamma_k}}$$

donde observamos que un denominador común de f'/f y g'/g está dado por el producto

$$N_0 = \prod (t - \alpha_i) \prod (t - \beta_j) \prod (t - \gamma_k)$$

cuyo grado es $n_0(abc)$.

Por otra parte, observe ahora que los productos

$$N_0 f'/f \qquad \text{y} \qquad N_0 g'/g$$

son polinomios de grados $\leq n_0(abc) - 1$, y como

$$\frac{b}{a} = -\frac{N_0 f'/f}{N_0 g'/g}$$

entonces

$$bN_0 g'/g = -aN_0 f'/f$$

con $a(t)$ y $b(t)$ coprimos por lo que a divide a $N_0 g'/g$ y b divide a $N_0 f'/f$ y así

$$\text{gr}(a) \leq \text{gr}\, N_0 g'/g \leq n_0(abc) - 1 \quad \text{y} \quad \text{gr}(b) \leq \text{gr}\, N_0 f'/f \leq n_0(abc) - 1$$

y el teorema se sigue ya que $c = a+b$ implica que $\text{gr}(c) \leq \text{máx}\{\text{gr}\, a, \text{gr}\, b\}$. □

Una consecuencia inmediata del teorema anterior es:

Corolario 2 (El teorema de Fermat para polinomios)**.** *Si $x(t), y(t), z(t)$ son polinomios en $\mathbb{C}[t]$ coprimos por pares, con alguno de ellos de grado ≥ 1 y además $x(t)^n + y(t)^n = z(t)^n$, entonces $n \leq 2$.*

Demostración. Para comenzar nótese que $n_0(x^n y^n z^n) \leq \text{gr}(x) + \text{gr}(y) + \text{gr}(z)$, y así, por el teorema anterior

$$\text{máx}\{\text{gr}\, x^n, \text{gr}\, y^n, \text{gr}\, z^n\} \leq \text{gr}(x) + \text{gr}(y) + \text{gr}(z) - 1,$$

en particular,

$$\text{gr}(x^n), \text{gr}(y^n), \text{gr}(z^n) \leq \text{gr}(x) + \text{gr}(y) + \text{gr}(z) - 1$$

y sumando estas tres desigualdades se obtiene que

$$n(\text{gr}(x) + \text{gr}(y) + \text{gr}(z)) \leq 3(\text{gr}(x) + \text{gr}(y) + \text{gr}(z)) - 3$$

de donde se sigue que $n \leq 2$. □

La versión aritmética. Masser [8] y Oesterlé [9], siguiendo ideas de Szpiro [10] y Frey [3], [4], [5], relacionadas con la conjetura de Fermat y curvas elípticas, e inspirados por el teorema de Mason que describimos anteriormente, formulan una versión aritmética del teorema de Mason como una conjetura, la cual siguiendo la analogía clásica entre los enteros de $\mathbb{Z}$ y los polinomios con coeficientes en un campo, donde el grado de

un polinomio corresponde al (logaritmo del) valor absoluto de un entero, observan que la desigualdad aditiva para los grados de polinomios debe corresponder a una desigualdad multiplicativa y luego observan también que el número de ceros distintos de $f(t)$, $n_0(f)$, corresponde al número de factores primos de $f(t)$ en $\mathbb{C}[t]$, sin contar sus multiplicidades (ya que $\mathbb{C}$ es algebraicamente cerrado). De aquí, siguiendo a Serre definen el *radical* $N_0(m)$ de un entero $m \in \mathbb{Z}$ como el producto de los primos distintos que dividen a m,

$$N_0(m) := \prod_{p|m} p.$$

Note entonces que si m y n son coprimos, se tiene que $N_0(mn) = N_0(m)\, N_0(n)$. Así, la formulación aritmética, en $\mathbb{Z}$, del teorema de Mason sería la siguiente:

Si a, b, c son enteros coprimos por pares tales que $a+b=c$, entonces (ignorando el sumando favorable -1 en el teorema de Mason) se debe tener que

$$\text{máx}\{|a|, |b|, |c|\} \leq N_0(abc).$$

Sin embargo, tienen que hacerse correcciones inmediatas a esta primera formulación conjetural, ya que, siendo a, b coprimos que satisfacen la igualdad $a + b = c$, podemos asumir que $a < b$ y también podemos asumir, para facilitar el argumento, que a, b, c son positivos y por lo tanto $\text{máx}\{a, b, c\} = c$ y se tiene por tanto que:

Proposición 3. *Existe una infinidad de ternas de enteros a, b, c, coprimos y positivos tales que $a < b$, $a + b = c$ y además $N_0(abc) < c$.*

Demostración. Tomando $a = 1$, $c = 3^{2^k}$ y $b = 3^{2^k} - 1$, con $k \geq 0$, se tiene que a, b, c son coprimos, satisfacen $a + b = c$, y por inducción se demuestra fácilmente que b es divisible por 2^{k+1}, de tal forma que

$$N_0(b) = N_0(3^{2^k} - 1) \leq (3^{2^k} - 1)/2^{k+1} < c/2^{k+1}$$

y por lo tanto, ya que $N_0(c) = 3$,

$$N_0(abc) = N_0(bc) = 3N_0(b) < 3c/2^{k+1}$$

de donde se sigue que

$$c > N_0(abc)2^{k+1}/3$$

y consecuentemente $c > N_0(abc)$ si $k \geq 1$. □

Así, la desigualdad aritmética, análoga a la del teorema de Mason, debe ser corregida, y como en la versión aritmética la analogía exige una formulación multiplicativa, lo natural es considerar exponentes > 1 en $N_0(abc)$. La conjetura *abc* es:

Conjetura 4 (D. W. Masser y J. Oesterlé, 1985)**.** *Si a, b, c son enteros coprimos tales que $a + b = c$, entonces para todo $\varepsilon > 0$ existe una constante $C(\varepsilon)$ tal que*

$$\text{máx}\{|a|, |b|, |c|\} \leq C(\varepsilon) N_0(abc)^{1+\varepsilon}.$$

Antes de comentar algunos progresos recientes hacia la demostración de esta conjetura, veamos algunas de sus consecuencias para aquilatar su importancia:

Supongamos primero que $\varepsilon = 1$ para fijar ideas y que $C(\varepsilon) = C(1) = 1$ también; podemos asumir también que a, b, c son enteros positivos. Entonces, la conjetura *abc* dice que si $a + b = c$, se debe tener que

$$c < N_0(abc)^2. \tag{1}$$

Supongamos ahora que x, y, z, n son enteros positivos con x, y, z coprimos y tales que

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

Poniendo $a = x^n$, $b = y^n$, $c = z^n$, notamos que

$$N_0(abc) = N_0((xyz)^n) = N_0(xyz) \leq xyz < z^3 \tag{2}$$

y de (1) y (2) se sigue que

$$z^n = c < N_0(abc)^2 < (z^3)^2 = z^6$$

lo cual sólo es posible si $n < 6$. Así, la conjetura de Fermat es cierta para todo exponente $n \geq 6$, como una consecuencia de la conjetura *abc* en la forma (1). Nótese sin embargo que, en la forma (1), a la conjetura *abc* de Masser y Oesterlé se añadió la hipótesis de que $C(\varepsilon) = C(1) = 1$, pero en general no se sabe el valor de la constante $C(\varepsilon)$, por lo que la hipótesis de que $C(1) = 1$ no tiene apoyo. Lo que sí se tiene es que, poniendo de nuevo $a = x^n$, $b = y^n$, $c = z^n$, como $N_0(abc) \leq xyz$, la conjetura *abc* de Masser-Oesterlé implica que

$$\begin{aligned} x^n &\leq C(\varepsilon)(xyz)^{1+\varepsilon} \\ y^n &\leq C(\varepsilon)(xyz)^{1+\varepsilon} \\ z^n &\leq C(\varepsilon)(xyz)^{1+\varepsilon} \end{aligned}$$

y multiplicando estas tres desigualdades se obtiene que

$$(xyz)^n \leq C(\varepsilon)^3 (xyz)^{3+3\varepsilon}$$

y así, para $xyz > 1$, tomando logaritmos se sigue que

$$n \leq (3 + 3\varepsilon) + 3 \log C(\varepsilon)$$

es decir, n está acotado, o dicho en otras palabras, la conjetura de Fermat (ahora teorema por Wiles) es cierta para todo exponente mayor que la cota anterior. Decimos entonces que se ha demostrado una versión asintótica de la conjetura de Fermat y lo ideal sería tener una forma explícita de la cota $C(\varepsilon)$ involucrada.

La consecuencia anterior debe ser suficiente para ver de qué calibre es la conjetura *abc* de Masser-Oesterlé, sin embargo a continuación enumeraremos algunas otras consecuencias de la conjetura *abc* de formulación aparentemente tan simple.

La ecuación de Fermat-Catalan. La conjetura de Catalan, en teoría de números, afirma que 8 y 9 son las únicas potencias perfectas consecutivas, es decir, que para la ecuación diofantina

$$x^m - y^n = 1 \tag{3}$$

las únicas soluciones enteras positivas son $x = 3^2$, $y = 2^3$. Esta conjetura fue demostrada en 2002 por Preda Mihăilescu usando resultados teóricos muy profundos de la teoría de campos ciclotómicos. Veremos a continuación cómo la conjetura *abc* implica que la ecuación de Catalan sólo tiene un número finito de soluciones. Para comenzar, observe que la ecuación de Catalan (3) es un caso especial (para $x = 1$) de la ecuación de Catalan-Fermat

$$x^p + y^q = z^r \tag{4}$$

de la cual interesan sus soluciones enteras positivas coprimas y con $p, q, r > 1$ dados. Tres casos se distinguen inmediatamente:

(I). Si $1/p + 1/q + 1/r > 1$. Es fácil ver que entonces se debe tener que (p, q, r) es una permutación de las ternas $(2, 2, k)$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$ y en cada uno de estos casos el número de soluciones de (4) es infinito.

(II). Si $1/p + 1/q + 1/r = 1$. Se muestra directamente que (p, q, r) es una permutación de las ternas $(2, 4, 4)$, $(2, 3, 6)$, $(3, 3, 3)$ y que en cada

uno de estos casos el número de soluciones de (4) es finito.

(III). Si $1/p + 1/q + 1/r < 1$, se tiene un número infinito de ternas (p, q, r) con la propiedad anterior y Darmon y Granville [1] mostraron en 1995 que en estos casos el número de soluciones de (4) es finito.

A continuación veremos cómo el caso (III) anterior es una consecuencia sencilla de la conjetura *abc*. Para comenzar notese que, por los casos (I) y (II), la terna más chica que puede tenerse en el caso (III) es $(2, 3, 7)$ para la cual $1/2 + 1/3 + 1/7 = 41/42$ por lo que $1/p + 1/q + 1/r < 1$ implica que $1/p + 1/q + 1/r \leq 1 - 1/42$. Ahora aplicamos la conjetura *abc* a los enteros $a = x^p$, $b = y^q$, $c = z^r$ con $\varepsilon = 0.01$ notando que

$$N_0(abc) = N_0(x^p y^q z^r) \leq xyz < z^{r/p} z^{r/q} z$$

y $\max\{|a|, |b|, |c|\} = z^r$ por lo que, salvo un número finito de excepciones (dadas por la cota inducida por la constante $C(\varepsilon)$ de la conjetura *abc*) se tiene que

$$z^r < \Big(z^{(r/p+r/q+1)}\Big)^{1+\varepsilon} = \Big(z^{(r/p+r/q+1)}\Big)^{1.01}$$

donde tomando logaritmos se obtiene que

$$r < 1.01\big(r/p + r/q + 1\big)$$

que al dividir entre r implica que

$$1 < 1.01\big(1/p + 1/q + 1/r\big)$$

lo cual es imposible porque

$$1/p + 1/q + 1/r \leq 1 - 1/42 \quad \text{y} \quad 1.01(1 - 1/42) < 1.$$

El resultado de Darmon y Granville (el caso (III)) se sigue. Como observamos previamente, lo anterior implica que $x^p - y^q = 1$ tiene sólo un número finito de soluciones.

Una observación importante. Al deducir la conjetura de Fermat (al menos, en una versión asintótica) usando la conjetura *abc*, es de notarse que todo se ve *muy fácil*, de hecho, *demasiado fácil*. Esto puede estarnos diciendo una de dos cosas: que la conjetura *abc* es muy profunda o que la conjetura *abc* puede ser falsa.

A continuación recordaremos algunas otras consecuencias de la conjetura *abc* que son teoremas muy importantes en geometría diofantina

y cuyas demostraciones usan resultados muy profundos de la geometría algebraica y de la teoría de números y que, sin embargo, son consecuencias en cierto modo sencillas, de la conjetura *abc*. De nuevo, lo anterior tiene la misma interpretación acerca de *abc*, de que o es muy profunda o es falsa.

Elkies [2] demuestra en 1991 que la conjetura de Mordell, demostrada por Faltings en 1983 usando las más sofisticadas herramientas de la geometría algebraica aritmética, se sigue de la conjetura *abc*. Recordemos que la conjetura de Mordell afirma que si $p(x, y) = 0$ es una ecuación polinomial en dos variables y con coeficientes racionales, y si el género de la curva que define es > 1, entonces el número de soluciones racionales de $p(x, y) = 0$ es finito. Bombieri, en 1994, demostró que el teorema de Roth, sobre la aproximación diofantina de irracionales algebraicos, se sigue también de la conjetura *abc*. M. van Frankenhuysen [6] nota la similitud formal entre el argumento de Elkies y el de Bombieri y en su artículo de 1999 prueba una consecuencia de la conjetura *abc* que implica ambos teoremas, el de Faltings y el de Roth.

Aunque estas consecuencias de la conjetura *abc* requieren argumentos un poco más sofisticados que los recordados arriba, son mucho más simples, por ejemplo, que el argumento de Faltings para demostrar la conjetura de Mordell, y además muestran claramente la relación entre la teoría de aproximación diofantina y la de puntos racionales o enteros en curvas definidas sobre los racionales.

Existen varias otras consecuencias importantes en análisis diofantino de la conjetura *abc*, lo cual resalta su importancia, y la facilidad relativa con la que se deducen (usando la conjetura *abc*) algunos de los resultados más importantes de la teoría de números puede ser una indicación de cuán difícil puede ser una demostración de esta conjetura, aun cuando la demostración sencilla del caso de campos de funciones es algo que debe mantenerse en mente. Por otra parte, y dándole oportunidad al pesimismo, también pudiera pensarse que lo anterior, con todo y su aparente simplicidad, es un argumento en contra de la posible veracidad de esta conjetura, y tal vez valga la pena recordar que originalmente Masser pedía un contraejemplo a lo que ahora llamamos la conjetura *abc*.

Avances hacia la demostración de la conjetura *abc***.** Todavía no se vislumbra una demostración de esta conjetura y algunos avances relativamente recientes son:
En 1986, Stewart y Tijdeman probaron que

$$\log c < C_1 N_0(abc)^{15}$$

y posteriormente Stewart y K. Yu obtuvieron ciertas mejoras en el exponente de N_0, por ejemplo,

$$c < \exp\left(C_1 N_0 (abc)^{1/3+\varepsilon}\right).$$

Agradecimientos. Agradezco a un árbitro anónimo su lectura cuidadosa del manuscrito original.

Referencias

[1] Darmon, H. and Granville, A., *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*. Bull. Lond. Math. Soc. **27**, No.6, 1995, 513-543.

[2] Elkies, N., *ABC implies Mordell*. Int. Math. Res. Not., **7**, 1991, 99-109.

[3] Frey, G., *Links between stable elliptic curves and certain diophantine equations*. Annales Universitatis Saraviensis, Series Mathematicae, **1**, 1986, 1-40.

[4] Frey, G., *Links between elliptic curves and solutions of $A - B = C$*. Journal of the Indian Math. Soc., **51**, 1987, 117-145.

[5] Frey, G., *Links between solutions of $A - B = C$ and elliptic curves*. Number theory, Proc. 15th Journ. Arith., Ulm 1987, Lecture Notes in Mathematics **1380**, 31-62 (1989). Springer Verlag, Berlin.

[6] van Frankenhuysen, M., *The abc conjecture implies Roth's theorem and Mordell's conjecture*. Matematica Contemporanea, **16**, 1999, 45-72.

[7] Mason, R. C., *Equations over function fields*. Lecture Notes in Mathematics **1068**, 1984, 149-157. Springer Verlag, Berlin, New York.

[8] Masser, D. W., *Note on a conjecture of Szpiro*. Séminaire sur les pinceaux de courbes elliptiques, Paris 1988, Astérisque **183**, 1990, 19-23.

[9] Oesterlé, J., *Nouvelles approches du "Thèoréme" de Fermat*. Sémin. Bourbaki, 1987-88, Exposé 694, Astérisque **161/162**, 1988, 165-18.

[10] Szpiro, L., *La conjecture de Mordell*. Sémin. Bourbaki, 1983-84, Exposé 619, Astérisque **121/122**, 1985, 93-103.

[11] Stewart, C.L.; Tijdeman, R. *On the Oesterlé-Masser conjecture*. Monatsh. Math. **102**, 1986, 251-257.

[12] Stewart, C.L.; Yu, K., *On the abc conjecture*. Math. Ann. **291**, No.2, 1991, 225-230.

[13] Stewart, C.L.; Yu, K., *On the abc conjecture II*. Duke Math. J. **108** No. 1, 2001, 169-181.