Lecturas Matemáticas
Volumen **34** *(1) (2013), páginas 11–75*
ISSN 0120–1980

La conjetura abc

The abc conjecture

Víctor S. Albis
Universidad Nacional de Colombia, Bogotá, Colombia
Nelly Y. Villamizar
Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria

Resumen. Este es un trabajo de tipo expositivo. El matemático japonés Shinichi Mochizuki anunció en agosto de 2012 una demostración, en más de quinientas páginas, de la famosa conjetura *abc*, cuyas repercusiones en el mundo matemático son inmensas, si ella es correcta. A pesar de la seriedad del trabajo anterior de Mochizuki esta demostración requiere aún del escrutinio de la comunidad matemática, lo cual tomará aún un buen tiempo, mucho más que lo necesitó la verificación de la demostración de Andrew Wiles del último teorema de Fermat. Mientras esto ocurre, hemos creído conveniente hacer una introducción de esta conjetura destinada a los lectores hispanoamericanos y mostrar cómo ella implica el último teorema de Fermat, la conjetura de Catalan (que ya ha sido probada; véase [32]) y otros resultados como el teorema de Roth, el teorema de Faltings y otras conjeturas aún no probadas.

Key words and phrases. The *abc* conjecture, number theory, Shinichi Mochizuki.

Abstract. This is an expository paper. The Japanese mathematician Shinichi Mochizuki announced in August 2012 a proof, in more than 500 pages, of the celebrated *abc* conjecture, whose repercussions in the world of mathematics are enormous, if true. Despite the quality and

seriousness of MOCHIZUKI's previous mathematical work, it seems that his alleged proof requires the mathematical community scrutiny. This will take a good amount of time, maybe more than the one needed to verify the proof of Fermat's Last Theorem by ANDREW WILES.Waiting for the results of this scrutiny, we believe that an introduction to this conjecture, aimed to Spanish Americans readers, would be very convenient for its understanding and implications such as FERMAT's Last Theorem, CATALAN's conjecture (already proved; see [32]), ROTH's theorem, FALTINGS's theorem and some other unproven conjectures.

2010 AMS Mathematics Subject Classification. 11D72

1. **Introducción**

En teoría de números es frecuente encontrar problemas que se pueden formular en términos comprensibles, y que son relativamente fáciles de entender. Sin embargo, muchas de estas preguntas son sorpresivamente difíciles, o en un momento determinado imposibles de responder.

El último teorema de Fermat, por ejemplo, involucra una ecuación de la forma $x^n + y^n = z^n$. Hace más de 300 años, PIERRE DE FERMAT (1601–1665), conjeturó que la ecuación no tiene solución si x, y y z son enteros positivos y n es cualquier entero más grande que dos. ANDREW WILES de la Universidad de Princeton finalmente probó la conjetura en 1994.[1]

Con el objeto de probar el teorema, WILES tuvo que intentar extender varias ideas del núcleo de las matemáticas modernas. Él no probó el último teorema de Fermat directamente. En su lugar, atacó una vieja y famosa conjetura sobre curvas elípticas (que provee enlaces entre diversas ramas de las matemáticas como geometría algebraica y análisis complejo) llamada la "conjetura de Taniyama"[2], y probó lo suficiente para poder deducir el teorema de Fermat. La fecha de esta última conjetura se remonta a 1955, cuando fue publicada en japonés como un problema de investigación por YUTAKA TANIYAMA. Los célebres matemáticos GORO SHIMURA y ANDRÉ WEIL proporcionaron conocimientos claves en la formulación de la conjetura, los cuales proponían un tipo especial de equivalencia entre los objetos matemáticos llamados curvas elípticas y las matemáticas de ciertos movimientos en el espacio [40].

[1] WILES, ANDREW. *Modular elliptic curves and Fermat's Last Theorem.* Ann. of Math. **141** (1995), 443–551.

[2] El primer enunciado de esta conjetura fue hecho por TANIYAMA. Posteriormente, se hizo más preciso con SHIMURA, quien probó que había infinitos ejemplos en los que la conjetura era verdadera. La conjetura sólo se dio a conocer ampliamente con los trabajos y la influencia de WEIL. Por esta razón, ha sido acreditada confusamente a varios subconjuntos de estos tres nombres.

La ecuación del último teorema de Fermat es un ejemplo de *ecuación diofántica*, una expresión algebraica en varias variables cuyas soluciones se requiere que sean números racionales (números enteros o fracciones).

Resulta interesante que la prueba de Wiles del último teorema de Fermat haya sido producto de su profunda incursión en la prueba de la conjetura de Taniyama. El esfuerzo de Wiles podría ayudar a conducir a una teoría general de ecuaciones diofánticas en tres variables. Históricamente los matemáticos han enunciado y resuelto problemas diofánticos sobre la base caso–por–caso, una teoría que abarque todo representaría un gran avance. El elemento clave para construir tal teoría parece ser un problema llamado la *conjetura abc*, que fue formulado a mediados de los años 80 del siglo pasado por Joseph Oesterlé de la Universidad de París VI y David W. Masser del Instituto de Matemáticas de la Universidad de Basilea en Suiza.[3] La conjetura *abc* ofrece un nuevo camino para expresar problemas diofánticos. De hecho, traduce un número finito de ecuaciones diofánticas (incluyendo la ecuación del último teorema de Fermat) a una única sentencia matemática.

La conjetura *abc* es uno de esos problemas que pueden enunciarse de manera relativamente simple, en términos comprensibles. Incorpora el concepto de *entero libre de cuadrados*, también llamado *primitivo*: un entero es libre de cuadrados o primitivo cuando no es divisible por el cuadrado de ningún número. O también, cuando $n = p_1 \cdots p_k$, donde los p_i son todos primos distintos entre sí. Por ejemplo, 15 y 17 son libres de cuadrados pero 16 y 18 no lo son.

La *parte libre de cuadrados de un entero* n se define como el número más grande libre de cuadrados que puede formarse multiplicando los factores primos de n. Tal número se denota con $\mathrm{rad}\,(n)$. Así, para $n = 15$, los factores primos son 3 y 5 y $3 \cdot 5 = 15$ es un número libre de cuadrados, y por lo tanto, $\mathrm{rad}\,(15) = 15$. Por otro lado, para $n = 16$, los factores primos son todos 2, lo cual significa que $\mathrm{rad}\,(16) = 2$. Similarmente, $\mathrm{rad}\,(17) = 17$ y $\mathrm{rad}\,(18) = 6$.

Es claro que si n es libre de cuadrados, la parte libre de cuadrados de n es justamente n. De otra manera, $\mathrm{rad}\,(n)$ representa lo que queda después de que todos los factores que crean un cuadrado han sido eliminados, es decir, $\mathrm{rad}\,(n)$ es el producto de los distintos primos que dividen a n.

Con estos preliminares, el matemático Dorian Goldfeld de la Universidad de Columbia [13, 14], describió la conjetura *abc* en los siguientes términos: El problema trata de parejas de números que no tienen factores en común. Suponga que a y b son dos de tales números y que c es su suma. Por ejemplo, si $a = 3$ y $b = 7$, entonces, $c = 3 + 7 = 10$. Ahora, considere la parte libre de cuadrados del producto *abc*: $\mathrm{rad}\,(3 \cdot 7 \cdot 10) = 210$.

Para la mayoría de las elecciones de a y b, $\mathrm{rad}\,(abc)$ es más grande que c, como en el ejemplo anterior. Es decir, para la mayoría de los casos, $\mathrm{rad}\,(abc)/c$ es más grande que 1.

[3]Según Oesterlé la conjetura la discutieron Masser y él en Basilea en 1985 [38].

De vez en cuando, sin embargo, esto no es verdad. Por ejemplo, si $a = 1$ y $b = 8$, entonces $c = 1 + 8 = 9$, $\operatorname{rad}(abc) = \operatorname{rad}(1 \cdot 8 \cdot 9) = 6$ y $\operatorname{rad}(abc)/c = 6/9 = 2/3$. Similarmente, si $a = 3$, $b = 125$, la proporción es $15/64$, y si $a = 1$ y $b = 512$ la proporción es $2/9$.

Masser probó que $\operatorname{rad}(abc)/c$ puede ser arbitrariamente pequeño. Con otras palabras, él probó que si tomamos un número cualquiera más grande que 0, no importa que tan pequeño, podemos encontrar enteros a y b para los cuales $\operatorname{rad}(abc)/c$ sea más pequeño que ese número.

En contraste, la conjetura *abc* afirma que $\big(\operatorname{rad}(abc)\big)^{1+1/n}/c$ alcanza un valor mínimo siendo n cualquier entero mayor que 1.

Sorprendentemente, una demostración de la conjetura *abc* proveería un camino para establecer el último teorema de Fermat en menos de una página de razonamiento matemático. Realmente, muchas conjeturas y teoremas famosos en teoría de números se seguirían inmediatamente de la conjetura *abc*, algunas veces, en pocas líneas.

"La conjetura *abc* es sorprendentemente simple comparada con las preguntas profundas en teoría de números que puede resolver", dice Andrew J. Granville de la Universidad de Montreal, en Canadá [15] "Esta extraña conjetura resulta equivalente a todos lo problemas principales en teoría de números, y éste es el centro de todo lo que a ella se refiere", y añade:

> *La conjetura abc es el problema más importante no resuelto en análisis diofántico, escribe* Goldfeld *en Math Horizons (*[13], [14]*). Aparte de ser muy útil, es para los matemáticos también una cuestión de belleza. Ver muchos problemas diofánticos inesperadamente encapsulados en una única ecuación, y cómo todas las subdisciplinas de las matemáticas son aspectos de una única unidad fundamental que en el fondo es expresable en lenguaje simple, es emocionante.*

No debe pues sorprendernos que los matemáticos hayan estado trabajando duramente para conquistar la fascinante conjetura *abc*.

Cabe anotar que si los enteros a, b, c son reemplazados por polinomios en una variable con coeficientes en un cuerpo de característica cero, una proposición análoga a la conjetura *abc* es verdadera. Este resultado es conocido como el *teorema de Mason* (véase la sección 2).

El presente trabajo lo hemos dividido en cuatro secciones de la siguiente manera.

La sección 2, **De las ecuaciones diofánticas a la conjetura abc**, es una breve exposición del interés original de la conjetura *abc*. Presentamos ahí la conjetura *abc* en su forma más conocida y la demostración de su análogo en polinomios de coeficientes en un cuerpo algebraicamente cerrado de característica 0.

La sección 3, **Aplicaciones de la conjetura** *abc*, contiene algunas de las más importantes consecuencias que se obtienen al asumir que la conjetura *abc* es verdadera. Al comienzo de cada una de las aplicaciones hemos incluido las nociones necesarias para reconstruir cada una de las demostraciones. Otras aplicaciones de conjetura *abc*, no menos importantes se encuentran el los artículos citados en la bibliografía.

En la sección 4, **Conjeturas equivalentes a la conjetura abc**, presentamos el enunciado que originalmente Oesterlé hizo de la conjetura *abc* motivado por las consideraciones de la conjetura de Szpiro en curvas elípticas, y su respectiva equivalencia con la conjetura enunciada por Masser. También incluimos la equivalencia entre la conjetura *abc* y la conjetura *abc* en congruencias, que en principio pareciera ser más débil.

Finalmente, en la sección 5, **Evidencia de la conjetura abc**, exponemos los resultados a los que llegaron Cameron L. Stewart y Robert Tijdeman en 1986, que fueron mejorados posteriormente por Stewart y Kunrui Yu en 1991, y en el 2001. Ellos obtuvieron una cota superior para c (siguiendo la notación del comienzo de este trabajo), en función del radical $\operatorname{rad}(abc)$, basados en estimaciones de Yu para formas lineales $p-$ádicas en logaritmos de números algebraicos. Definimos además lo que se conoce como *buenas triplas*, y listamos las que se conocían hasta enero del año 2002.

El propósito de este trabajo no es presentar todo lo que tiene que ver con la conjetura *abc*, pues, de hecho, un trabajo con tales aspiraciones resultaría bastante extenso. Lo que queremos es dar una idea lo más clara posible de lo poderosa y a la vez sencilla de expresar que resulta ser la conjetura *abc*.

2. De las ecuaciones diofánticas a la conjetura abc

2.1. El último teorema de Fermat. Muchos problemas en teoría de números tienen la forma: si $f = f(x_1, x_2, x_3, \ldots, x_n)$ es un polinomio con coeficientes enteros, ¿tiene la ecuación $f = 0$ soluciones enteras? Tal tipo de preguntas fueron consideradas hace mucho tiempo por el matemático griego Diofanto y en su honor son llamadas *problemas diofánticos*.

Por una *ecuación diofántica* se entenderá, pues, una ecuación polinomia

$$f(x_1, x_2, x_3, \ldots, x_n) = b \tag{1}$$

con coeficientes racionales o enteros. Si esta ecuación tiene una solución en los enteros $x_1, x_2, x_3, \ldots, x_n$ entonces diremos que $(x_1, x_2, x_3, \ldots, x_n)$ es una *solución entera*. Si (1) es homogénea entonces una solución distinta de $(0, \ldots, 0)$ se llama *una solución no trivial*. Una solución a (1) con racionales $x_1, x_2, x_3, \ldots, x_n$ se llama una *solución racional*. Es claro que en el caso de una ecuación homogénea el problema de encontrar las soluciones enteras es equivalente al de encontrar las soluciones racionales.

Un ecuación diofántica muy conocida es la *ecuación pitagórica*

$$x^2 + y^2 = z^2. \tag{2}$$

Las soluciones enteras de esta ecuación son conocidas como *triplas pitagóricas*. Se les llama así pues PITÁGORAS creía tener demostrado que las longitudes a, b, c de los lados de un triángulo rectángulo satisfacen la relación

$$a^2 + b^2 = c^2\,;$$

es así como la existencia de soluciones de la ecuación diofántica (2) justifica principalmente la existencia de tales triángulos con lados medibles mediante números enteros. Para determinar todas las soluciones no triviales de (2) es suficiente determinar las *soluciones primitivas*, es decir, las soluciones en las que x, y, z son positivos y $1 = \text{m. c. d.}(x, y, z)$.[4]

Si (x, y, z) es una solución primitiva de (2), entonces

$$\text{m. c. d. }(x, y) = \text{m. c. d. }(x, z) = \text{m. c. d. }(y, z)$$

y además x y y no son ambos impares, pues si $x = 2k + 1$ y $y = 2k' + 1$ con k y k' enteros, entonces

$$\begin{aligned} x^2 + y^2 &= (2k+1)^2 + (2k'+1)^2 \\ &= 4(k^2 + k'^2 + k + k') + 2 \\ &= 2(2k'+1) \qquad (k' \in \mathbb{Z}) \\ &= z^2 \end{aligned}$$

lo cual contradice que z sea un entero. Podemos entonces asumir sin pérdida de generalidad que x es par, y que y y z son impares. El siguiente resultado se puede remontar hasta la época de DIOFANTO aunque es posible que, al menos en parte, se haya conocido un poco antes.

Sean a, b enteros primos relativos entre sí, no ambos impares, $a > b \geq 1$, y sea

$$\begin{cases} x = a^2 - b^2 \\ y = 2ab \\ z = a^2 - b^2. \end{cases} \tag{3}$$

Entonces (x, y, z) es una solución primitiva de la ecuación pitagórica, y toda solución de (2) *puede obtenerse de una única pareja (a, b) del tipo indicado por las relaciones* (3).

En particular, de acuerdo con este resultado, la ecuación (2) tiene infinitas soluciones. El lector puede encontrar más información sobre la ecuación pitagórica e incluso la prueba del hecho que aquí hemos mencionado en [42, pág. 31–53].

[4] $\text{m. c. d.}(x, y, z)$ denota el máximo común divisor de los enteros x, y, z.

Si consideramos ahora la ecuación diofántica que generaliza la ecuación pitagórica,

$$x^n + y^n = z^n \qquad (n > 2), \tag{4}$$

el problema de encontrar sus soluciones es un poco más desafiante, pues la situación, con respecto a la ecuación pitagórica, es ya muy diferente para cubos, bicuadrados, y de ahí en adelante.

Esta ecuación se conoce como la *ecuación de Fermat*. Se conoce con este nombre, pues en el margen de su copia de la edición de Bachet de los trabajos completos de Diofanto, Fermat escribió:

> *Es imposible separar un cubo en dos cubos, o un bicuadrado en dos bicuadrados, o en general, cualquier potencia más grande que la segunda en potencias de igual grado; he descubierto una prueba realmente extraordinaria pero este margen es demasiado pequeño para contenerla.*[5]

La copia original se extravió, pero la nota apareció en la edición de 1670 de los trabajos de Fermat editada en Toulouse por (su hijo) Samuel de Fermat. En su *History of the Theory of Numbers*, volumen II, Leonard E. Dickson, afirma que Fermat la escribió por el año 1637. Paul Tannery (1883) mencionó una carta que Fermat había escrito a Marin Mersenne en la cual él deseaba encontrar dos cubos cuya suma fuera un cubo, y dos bicuadrados cuya suma fuera un bicuadrado, esta carta aparece con la fecha de junio de 1638, en el volumen 7 de *Correspondance du Père Marin Mersenne* (1962); el mismo problema fue propuesto a Frénicle de Bessy (1640) en una carta a Mersenne, y a John Wallis y William Brouncker en una carta a Kenelm Digby, escrita en 1657, pero no hay mención alguna de la extraordinaria prueba que supuestamente Fermat había encontrado. Para más información véanse [1] y [41, Lectura 1].

En el lenguaje moderno, la afirmación diría:

La ecuación $x^n + y^n = z^n$ no tiene solución con x, y y z enteros positivos y n un número natural mayor que 2.

Ninguna prueba de esta afirmación fue encontrada nunca entre los papeles de Fermat. Tan solo conocemos una prueba que escribió para el caso particular en que $n = 4$ que, de hecho, es una de las dos pruebas hechas por Fermat en teoría de números que aún se preservan. La prueba de Fermat es muy ingeniosa, la realizó por el método que él mismo denominó *descenso infinito*, mediante el cual también se pueden resolver otras ecuaciones diofánticas importantes; para el lector que esté interesado, en [1], [17, pág. 14–15] y [41, pág. 37–38] se ilustra la manera de emplear este método.

[5]En el original latino: *Cubum in duos cubos, aut quadrato–quadratum in duos quadrato–quadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fast est dividere. Cujus rei demostrationem mirabile sane detexi: hanc marginis exiguitas no caperet.*

Con pocas excepciones, todas las otras afirmaciones que hizo FERMAT habían sido probadas hacia la mitad del siglo XIX, razón por la cual usualmente a este problema se le conoce como *el último teorema de Fermat*, a pesar que aún no se conocía ninguna demostración. El problema de Fermat fue capturando el interés de los matemáticos y muchas de las mejores mentes se ocuparon de él. EULER consideró el caso de los cubos, y la primera prueba esencialmente fue hecha por él; GAUSS dio otra prueba, para el mismo caso, empleando números complejos. Ambas pruebas pueden ser vistas en [1] y [41, pág. 39–45].

Alrededor del año 1820 distinguidos matemáticos franceses y alemanes intentaron intensamente probar el último teorema de Fermat, pero por más de tres siglos y medio, desde el momento en que FERMAT escribió esa inocente afirmación, nadie lo logró. Sin embargo, se obtuvieron varias demostraciones de casos particulares, y en lugar de que el ánimo de los matemáticos se desvaneciera, las demostraciones de estos casos particulares hacían fortalecer la idea de que FERMAT tenía razón y que en realidad el caso general era un teorema. Entre los casos particulares que se demostraron, podemos mencionar, por ejemplo, el caso $n = 5$ que fue demostrado independientemente por DIRICHLET y LEGENDRE [41]; el caso $n = 14$ establecido también por DIRICHLET, en 1832; el caso $n = 7$ probado por GABRIEL LAMÉ [22], en 1839, prueba que fue simplificada poco tiempo después, en 1840, por VICTOR LEBESGUE [27]; y el caso en que $n = p$ es un primo impar tal que $2p + 1$ es también un número primo, demostrado por SOPHIE GERMAINE, una matemática francesa. Además, grandes avances en la teoría moderna de números surgieron de intentos fallidos por demostrar el último teorema de Fermat, tal como es el caso de la teoría de números algebraicos que se desarrolló a partir del trabajo de KUMMER. Para más información el lector puede dirigirse a [41].

Este capítulo de la historia de las matemáticas llegó a su cierre en 1994 con el trabajo de WILES [59].

2.2. El teorema de Fermat en anillos de polinomios. Consideremos ahora la ecuación (4) y supongamos que tiene soluciones x, y, z no constantes en $\mathbb{C}[t]$. Sin pérdida de la generalidad podemos suponer que x, y, z no tienen divisores en común. Al derivar la ecuación $x^n + y^n = z^n$ obtenemos:

$$nx'x^{n-1} + ny'y^{n-1} = nz'z^{n-1},$$

dividiendo por el factor común n, obtenemos

$$x'x^{n-1} + y'y^{n-1} = z'z^{n-1}\,. \tag{5}$$

Multiplicando (4) por y' y (5) por y

$$y'x^n + y'y^n = y'z^n$$
$$yx'x^{n-1} + y'y^n = yz'z^{n-1}$$

y restando una de otra obtenemos

$$y'x^n - yx'x^{n-1} = y'z^n - yz'z^{n-1}$$
$$x^{n-1}(y'x - x'y) = z^{n-1}(y'z - z'y)\,.$$

De acuerdo con la última igualdad, x^{n-1} divide al producto $z^{n-1}(y'z - z'y)$; pero como $\text{m. c. d.}\,(x, z) = 1$ entonces

$$x^{n-1} \quad \text{divide a} \quad y'z - z'y.$$

Si $y'z - z'y = 0$ entonces $y'z = z'y$ y como $\text{m. c. d.}(z, y) = 1$ resulta que $y \mid y'$, lo cual no es posible por razones de grado. Por lo tanto, $y'z - z'y \neq 0$ y como x^{n-1} divide a $y'z - z'y$ entonces

$$\operatorname{grad}(x^{n-1}) \leqq \operatorname{grad}(y'z - z'y)\,.$$

Por otro lado, $\operatorname{grad}(y') = \operatorname{grad}(y) - 1$, $\operatorname{grad}(z') = \operatorname{grad}(z) - 1$ y $\operatorname{grad}(x^{n-1}) = (n-1)\cdot\operatorname{grad}(x)$; tenemos entonces que

$$\begin{aligned}\operatorname{grad}(x^{n-1}) &\leqq \operatorname{grad}(y'z - z'y)\\ &= \operatorname{máx}\big(\operatorname{grad}(y'z), \operatorname{grad}(z'y)\big)\\ &= \operatorname{grad}(y) + \operatorname{grad}(z) - 1\,. \end{aligned} \tag{6}$$

Adicionando $\operatorname{grad}(x)$ en ambos lados de (6) obtenemos

$$\begin{aligned} n\operatorname{grad}(x) &\leqq \operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z) - 1\\ &< \operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)\,. \end{aligned} \tag{7}$$

De forma similar a como obtuvimos (7) podemos llegar a las siguientes desigualdades valiéndonos de las simetrías entre x, y y z

$$n\operatorname{grad}(y) < \operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)$$
$$n\operatorname{grad}(z) < \operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)\,;$$

sumando las tres, obtenemos

$$n\big(\operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)\big) < 3\big(\operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)\big)$$

y finalmente, dividiendo por el factor común $\operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)$ llegamos a que $n < 3$, lo cual es evidentemente una contradicción, pues en la ecuación de Fermat el entero n es ≥ 3. Así queda probado el último teorema de Fermat para el anillo $\mathbb{C}[t]$. Más precisamente, tenemos

Proposición 2.1 (Último teorema de Fermat en polinomios)**.** *No existen polinomios $x(t), y(t), z(t) \in \mathbb{C}[t]$ no triviales, primos relativos entre sí y no todos constantes tales que $\big(x(t)\big)^n + \big(y(t)\big)^n = \big(z(t)\big)^n$ siendo n un entero ≥ 3.*

Que el teorema de Fermat sea fácil de probar para polinomios, no es un resultado reciente. La prueba que hemos presentado data del siglo XIX y es debida a Alexander Korkine [19]. Una prueba un poco más complicada fue hecha por R. Liouville ([28], [37]) utilizando integración. La Proposición 2.1

sigue siendo válida si reemplazamos $\mathbb{C}$ por un cuerpo de característica 0 o por un cuerpo de característica $p > 0$ si suponemos en este último caso que $p \nmid n$ [2]. En caso contrario el teorema falla. Por ejemplo, si $f(t) = t + 1$, $g(x) = t$, and $h(t) = 1$ son polinomios de coeficientes en cuerpo de característica $p > 0$, entonces $f(t)^p = g(t)^p + h(x)^p$.

Cuando $n = 2$ sucede algo similar al caso de los enteros: existen soluciones polinomias de la ecuación $x^2+y^2 = z^2$; por ejemplo, $(1-t^2)^2+(2t)^2 = (1+t^2)^2$.

2.3. El teorema de Mason. Richard C. Mason (1983) se propuso buscar las soluciones a la ecuación

$$a(t) + b(t) = c(t)\,,$$

donde $a(t), b(t), c(t) \in \mathbb{C}[t]$ ([29]). El resultado de esta búsqueda le condujo al siguiente resultado

Proposición 2.2 (Teorema de Mason)**.** *Si $a(t), b(t), c(t) \in \mathbb{C}[t]$ son polinomios no nulos tales que* $\mathrm{m.\,c.\,d.}(a(t), b(t), c(t)) = 1$ *y $a(t) + b(t) = c(t)$, entonces*

$$\text{máx}\{\operatorname{grad} a(t), \operatorname{grad} b(t), \operatorname{grad} c(t)\} \leq N_0(a(t)b(t)c(t)) - 1,$$

donde $N_0(a(t)b(t)c(t))$ denota el número de raíces distintas del polinomio $a(t)b(t)c(t)$.

Si $f(t) = \alpha p_1(t)^{e_1} \cdots p_k(t)^{e_k}$, donde $\alpha \in \mathbb{C}^* := \mathbb{C} \setminus \{0\}$, es la descomposición canónica de $f(t)$ en factores irreducibles en el anillo factorial $\mathbb{C}[t]$, definimos el radical de $f(t)$ como $\operatorname{rad} f(t) := p_1(t) \cdots p_k(t)$.

Los polinomios distintos del polinomio 0 tienen grado ≥ 0. Al polinomio 0 le asignamos, como es costumbre, el grado $\operatorname{grad} 0 = -\infty$. Es decir, un polinomio es distinto del polinomio 0 si y sólo si su grado es un número entero ≥ 0.

Lema 2.1. *Si $f(t) = p_1(t)^{e_1} \cdots p_k(t)^{e_k}$, se tiene* $\dfrac{f(t)}{\operatorname{rad} f(t)} \mid f'(t)\,.$

Demostración. Es claro que

$$\frac{f(t)}{\operatorname{rad} f(t)} = p_1(t)^{e_1-1} \cdots p_k(t)^{e_k-1}\,.$$

Por otro lado,

$$f'(t) = e_1 p_1(t)^{e_1-1} p_2(t)^{e_2} \cdots p_k(t) + p_1(t)^{e_1} \frac{d}{dt} p_2(t)^{e_2} \cdots p_k(t)^{e_k}\,.$$

Es claro ahora que $p_1(t)^{e_1-1} \mid f'(t)$. De la misma manera se demuestra que $p_i(t)^{e_i-1} \mid f'(t)$, para $i = 1, \ldots, k$. Como los $p_i(t)$ son primos entre sí, tenemos el resultado. ☑

Lema 2.2. *Si $f(t), g(t) \in \mathbb{C}[t]$ y se tiene que $f(t) \mid g(t)$ y $\operatorname{grad} f(t) > \operatorname{grad} g(t)$, entonces $g = 0$.*

Demostración. Tenemos $g(t) = f(t)h(t)$ para algún $h(t) \in \mathbb{C}[t]$, de modo que $\operatorname{grad} g(t) = \operatorname{grad} f(t) + \operatorname{grad} h(t)$. Pero esto es imposible si queremos que $\operatorname{grad} g(t)$ sea un entero, pues $\operatorname{grad} f(t) > \operatorname{grad} g(t)$. Luego $\operatorname{grad} g(t) = -\infty$, es decir, $g(t) = 0$. ☑

Proposición 2.3. *Sean $a(t)$, $b(t)$ y $c(t) \in \mathbb{C}[t]$ tales que $a(t) + b(t) + c(t) = 0$ y $\text{m. c. d.}(a(t), b(t), c(t)) = 1$. Si $\operatorname{grad} a(t) \geq \operatorname{grad}\operatorname{rad}[a(t)b(t)c(t)]$, entonces $a'(t) = b'(t) = c'(t) = 0$.*

Demostración. En primer lugar observemos que

$$\text{m. c. d.}(a(t), b(t)) = \text{m. c. d.}(b(t), c(t)) = \text{m. c. d.}(c(t), a(t)) = 1\,.$$

Por otro lado,

$$a(t)b'(t) - a'(t)b(t) = c'(t)b(t) - c(t)b'(t) = a(t)c'(t) - a'(t)c(t)\,, \qquad (8)$$

como es fácil verificar. Por el lema 3.1, $\dfrac{c(t)}{\operatorname{rad} c(t)}$ divide tanto a $c(t)$ como a $c'(t)$ y, por lo tanto, a $c'(t)b(t) + c(t)b'(t)$. De manera semejante, $\dfrac{b(t)}{\operatorname{rad} b(t)}$ divide a $c'(t)b(t) + c(t)b'(t)$. Finalmente, (9) muestra $\dfrac{a(t)}{\operatorname{rad} a(t)}$ divide a

$$a(t)b'(t) - a'(t)b(t) = c'(t)b(t) - c(t)b'(t)\,.$$

Como $a(t)$, $b(t)$ y $c(t)$ son primos entre sí de dos en dos, también lo son los cocientes

$$\frac{a(t)}{\operatorname{rad} a(t)},\ \frac{b(t)}{\operatorname{rad} b(t)} \quad \text{y} \quad \frac{c(t)}{\operatorname{rad} c(t)}\,.$$

Luego

$$\frac{a(t)}{\operatorname{rad} a(t)}\frac{b(t)}{\operatorname{rad} b(t)}\frac{c(t)}{\operatorname{rad} c(t)} \mid c'(t)b(t) - c(t)b'(t)\,.$$

Pero, también por coprimalidad, $(\operatorname{rad} a(t))(\operatorname{rad} b(t))(\operatorname{rad} c(t)) = \operatorname{rad}(a(t)b(t)c(t))$. Por consiguiente,

$$\frac{a(t)b(t)c(t)}{\operatorname{rad} a(t)b(t)c(t)} \mid c'(t)b(t) - c(t)b'(t)\,.$$

Ahora bien, nuestra hipótesis $\operatorname{grad} a(t) \geq \operatorname{grad}\operatorname{rad}[a(t)b(t)c(t)]$ implica que

$$\begin{aligned}\operatorname{grad}\frac{a(t)b(t)c(t)}{\operatorname{rad}(a(t)b(t)c(t))} &= \operatorname{grad} a(t)b(t)c(t) - \operatorname{grad}\operatorname{rad} a(t)b(t)c(t)\\ &\geq \operatorname{grad} a(t)b(t)c(t) - \operatorname{grad} a(t) = \operatorname{grad} b(t)c(t)\\ &> \operatorname{grad}(c'(t)b(t) - c(t)b'(t))\,.\end{aligned}$$

Por el lema 3.2, tenemos $0 = c'(t)b(t) - c(t)b'(t) = a(t)b'(t) - a'(t)b(t)$, o sea, $a(t)b'(t) = a'(t)b(t)$, lo que implica que $a(t) \mid a'(t)$, pues $\text{m. c. d.}(a(t), b(t)) = 1$. Como $\operatorname{grad} a(t) > \operatorname{grad} a'(t)$, tenemos finalmente $a'(t) = 0$. De manera semejante se demuestra que $b'(t) = 0$ y, en consecuencia, $c'(t) = 0$. ☑

Lo que esta proposición dice es que si $a(t) + b(t) + c(t) = 0$, el número de factores irreducibles (o lo que es lo mismo, de primos) de $a(t)b(t)c(t)$ no puede ser muy pequeño (a menos que las derivadas de los factores $a(t)$, $b(t)$ y $c(t)$ sean 0).

El teorema de Mason es ahora una consecuencia de la anterior proposición.

Demostración del teorema de Mason. Como estamos en característica 0, $a'(t) = 0$ implica que $a(t)$ es constante. Luego si ninguno de entre $a(t)$, $b(t)$ y $c(t)$ es constante, entonces $\operatorname{grad} a(t) \leq \operatorname{grad}\operatorname{rad}(a(t)b(t)c(t)) - 1$. Simétricamente,

$$\operatorname{grad} b(t) \leq \operatorname{grad}\operatorname{rad}(a(t)b(t)c(t)) - 1\,,$$
$$\operatorname{grad} c(t) \leq \operatorname{grad}\operatorname{rad}(a(t)b(t)c(t)) - 1\,.$$

Por consiguiente,

$$\text{máx}\{\operatorname{grad} a(t), \operatorname{grad} b(t), \operatorname{grad} c(t)\} \leq \operatorname{grad}(\operatorname{rad} a(t)b(t)c(t)) - 1\,.$$

Finalmente, es fácil verificar que $\operatorname{grad}\operatorname{rad}(a(t)b(t)c(t)) = N_0(a(t)b(t)c(t))$. ☑

La desigualdad del teorema de Mason es la "mejor posible", en el sentido de que podemos encontrar infinitos ejemplos en los que el número de raíces de la ecuación $abc(t) = 0$ es exactamente igual al grado más alto de los polinomios $a(t), b(t), c(t)$ más uno. Por ejemplo, en la identidad que consideramos antes

$$(2t)^2 + (t^2 - 1)^2 = (t^2 + 1)^2,$$

o si se quiere una un poco más interesante

$$t^n + 1 = (t^n + 1).$$

Observación 2.1. La anterior demostración sigue los lineamentos de la del entonces estudiante de secundaria Noah Snyder publicada en [45]. Los argumentos anteriores siguen siendo válidos cuando reemplazamos $\mathbb{C}$ por un cuerpo algebraicamente cerrado de característica cero.

Con la versión del teorema de Mason en cuerpos algebraicamente cerrados de característica cero se puede probar la siguiente proposición, un poco más general que el último teorema de Fermat en polinomios (2.1).

Proposición 2.1′. *Sean $x(t)$, $y(t)$, $z(t)$ polinomios primos relativos, cuyos coeficientes pertenecen a un cuerpo algebraicamente cerrado de característica cero, y por lo menos uno de ellos tiene grado > 0. Entonces*

$$x(t)^n + y(t)^n = z(t)^n$$

no tiene solución para $n > 3$.

Demostración. Sea $n \geq 3$ y supongamos que x, y, z son polinomios no nulos, primos relativos entre sí, no todos constantes, tales que $x^n + y^n = z^n$. Aplicamos el teorema de Mason con $a = x^n$, $b = y^n$, y $c = z^n$. Entonces

$$\operatorname{rad}(abc) = \operatorname{rad}(x^n y^n z^n) = \operatorname{rad}(xyz).$$

Dado que $\operatorname{grad}(x^n) = n \operatorname{grad}(x)$,

$$\begin{aligned} n \operatorname{grad}(x) &\leq n \operatorname{máx}\big(\operatorname{grad}(x), \operatorname{grad}(y), \operatorname{grad}(z)\big) \\ &= \operatorname{máx}\big(\operatorname{grad}(x^n), \operatorname{grad}(y^n), \operatorname{grad}(z^n)\big) \\ &= \operatorname{máx}\big(\operatorname{grad}(a), \operatorname{grad}(b), \operatorname{grad}(c)\big) \\ &\leq \operatorname{grad}\big(\operatorname{rad}(abc)\big) - 1 = \operatorname{grad}\big(\operatorname{rad}(xyz)\big) - 1 \\ &\leq \operatorname{grad}(xyz) - 1 = \operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z) - 1. \end{aligned}$$

Debido a que la anterior desigualdad se puede obtener también para $n \operatorname{grad}(y)$ y $n \operatorname{grad}(z)$, sumando las tres obtenemos

$$\begin{aligned} n\big(\operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)\big) &\leq 3\big(\operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)\big) - 3 \\ &\leq n\big(\operatorname{grad}(x) + \operatorname{grad}(y) + \operatorname{grad}(z)\big) - 3\,, \end{aligned}$$

es decir, $3 \leq 0$, lo cual es imposible. ☑

2.4. Dos mundos paralelos y el teorema de Mason. Es bien conocido el paralelismo entre la aritmética de $\mathbb{Z}$ y la de $K[t]$, donde K es un cuerpo: ambos son *dominios factoriales* o como se dice también *dominios de factorización única*. Por esta razón cada vez que se tiene un resultado en $\mathbb{Z}$ los matemáticos se preguntan si existe un análogo de este en $K[t]$, y recíprocamente.

En particular, dada una ecuación diofántica o un sistema de ecuaciones diofánticas, nos preguntamos si sus análogos en $K[t]$ tienen sentido e intentamos entonces estudiar sus soluciones en $K[t]$. Resulta, en general, que demostrar entonces estos análogos en $K[t]$ es más sencillo que en $\mathbb{Z}$, sobre todo si K es un cuerpo finito, o recíprocamente. Este el caso del teorema de Mason en $K[t]$ cuando K es un cuerpo algebraicamente cerrado y de característica 0. Es decir, nos atreveríamos a conjeturar que análogo de la Proposición 2.2 fuese algo así:

Si $a + b = c$ con a, b, c enteros primos relativos, entonces el número total de factores primos de a (b o c) contando multiplicidades, es menor que el número total de factores primos distintos de abc.

Pero al revisar el enunciado anterior, uno encuentra contraejemplos rápidamente: $1 + 1 = 2$, $1 + 3 = 4$ o $1 + 7 = 8$. Más generalmente, si $2^n - 1 = p$, $n > 2$, es primo, la afirmación muestra que $n \leq 2$ (tomando $a = 2^n$, $b = -1$ y $c = p$, entonces n es el número de factores primos de a y 2 el número de factores primos distintos de abc), lo cual es contradictorio.

Quizá si modificáramos un poco la anterior conjetura obtendríamos un mejor resultado.

Por mucho tiempo en teoría analítica de números se ha establecido la importancia de la función logaritmo cuando se trata de contar primos. Quizá entonces, la medida apropiada para un entero $a = \prod_p p^{e_p}$ análoga al grado en el caso de los polinomios, no es $\sum_p e_p$, si no $\sum_p e_p \log p = \log a$. Reemplazando el número

total de factores distintos de abc por $\sum_{p|abc} \log p$ y aplicando exponencial a ambos lados, tendríamos la siguiente conjetura:

Si $a+b=c$ con a,b,c enteros primos relativos, entonces $\text{máx}\{a,b,c\} \leq \prod_{p|abc} p$.

Desafortunadamente de nuevo encontramos contraejemplos rápidamente: $1+8=9$, $5+27=32$, $1+48=49$, $1+63=64$ $1+80=81$, $32+49=81\ldots$ Sin embargo, en todos estos ejemplos el cociente $\text{máx}\{a,b,c\}/\prod_{p|abc} p$ nunca es demasiado grande. En realidad, cuando $1 \leq a,b,c < 1000$ la proporción más grande encontrada es $9/2$ que ocurre cuando $a=1$, $b=2^9$ y $c=3^3\cdot 19$, $\text{máx}\{a,b,c\}/\prod_{p|abc} p = 3^3\cdot 19/3\cdot 2\cdot 19$.

Lo anterior nos sugiere que, posiblemente, si multiplicáramos el lado derecho de la desigualdad $\text{máx}\{a,b,c\} \leq \prod_{p|abc} p$ por una constante convenientemente grande (tal vez 5), podríamos obtener una desigualdad válida.

Pero aún así, igual es falso para $a=1$ y $c=2^{p(p-1)}$ donde p es algún primo grande, pues tenemos que $b=2^{p(p-1)}-1$ es divisible por p^2 (ya que por el teorema de Euler $2^{p-1}\equiv 1 \pmod{p^2} \Rightarrow 2^{p(p-1)}\equiv 1 \pmod{p^2}$); si suponemos que existe tal constante k tal que $\text{máx}\{a,b,c\} = 2^{p(p-1)} \leq (2b/p)k$, como $2(2^{p(p-1)}-1)k - 2^{p(p-1)}p = 2^{p(p-1)}(2k-p)-2k$ y p puede ser tan grande como se quiera, la diferencia anterior no necesariamente es mayor que cero.

Aún cuando los cálculos numéricos actuales indican que estamos muy cerca de llegar a algo que sea válido, todo parece indicar que esto se va ha lograr haciendo solamente pequeñas modificaciones.

Conjetura 1 (Conjetura *abc*)**.** *Para todo $\epsilon > 0$ existe una constante k_ϵ tal que, si a,b,c son enteros positivos primos relativos, para los cuales $a+b=c$ entonces:*

$$c \leq k_\epsilon \left(\prod_{p|abc} p \right)^{1+\epsilon}.$$

Una de las metas en la formulación del análogo al teorema de Mason era que pudiéramos deducir el último teorema de Fermat sobre los enteros. Veamos a qué resultado llegamos con la conjetura anterior.

Sea (x,y,z) una solución entera a la ecuación de Fermat (4) donde x y y son ambos positivos. Ponemos $a=x^n$, $b=y^n$ y $c=z^n$. Según la conjetura anterior debemos saber exactamente cuáles son los primos que dividen al producto xyz. Esta información no la tenemos, pero dado que x y y son positivos entonces los dos son más pequeños que z, de modo que $xyz < z^3$. Por lo tanto, según la conjetura, dado ϵ existe una constante k_ϵ para la cual

$$z^n < k_\epsilon \left(\prod_{p|xyz} p \right)^{1+\epsilon} \leq k_\epsilon (z^3)^{1+\epsilon},$$

si tomamos $\epsilon = 1/6$ y $n \geq 4$ tenemos que $z^{n-3(1+(1/6))} \leq k_{1/6}$. Como $n \geq 4$ entonces $n - 3(1 + (1/6)) \geq n/8$ y de la conjetura *abc* deducimos

$$z^n \leq k_{1/6}^8;$$

hemos probado entonces que para cualquier solución de $x^n + y^n = z^n$ con $n \geq 4$ los números x^n, y^n, z^n están por debajo de alguna cota, por lo tanto, existen sólo un número finito de tales soluciones.

Esta versión del teorema que Fermat es conocida como el *teorema asintótico de Fermat*.

Si tuviéramos una versión explícita de la conjetura *abc*, esto es, con los valores de k_ϵ explícitos, podríamos dar una cota explícita sobre todas las soluciones de la ecuación de Fermat y calcular hasta dicha cota si existen o no soluciones. Ésta no sería la prueba más elegante del último teorema de Fermat, pero habríamos conseguido el objetivo.

La conjetura *abc* fue enunciada por Oesterlé y Masser en 1985 [38]. Masser estaba motivado por las proposiciones análogas sobre $\mathbb{Z}$ del teorema de Mason, mientras que Oesterlé lo estaba por consideraciones de la conjetura de Szpiro en curvas elípticas.

Originalmente Oesterlé enunció la conjetura en la siguiente forma:

Si a, b, c son enteros primos relativos, que satisfacen $a + b = c$ entonces,

$$L = L(a, b, c) = \frac{\log \max(|a|, |b|, |c|)}{\log \operatorname{rad}(abc)}$$

es acotado.

Masser [30] refinó el enunciado , y le dio la forma más común que es la que presentamos anteriormente.

Consideremos las triplas del cuadro 1. Nótese que

$$\sum_{p|abc} \log p$$

es mayor que $\log c$. La conjetura *abc* lo que afirma es que $\sum_{p|abc} \log p$ no puede ser mucho más grande que $\log c$.

Si escribimos la desigualdad de la conjetura *abc* como

$$\log c \leq k + (1 + \epsilon) \cdot \sum_{p|abc} \log p\,,$$

donde $k = \log k_\epsilon$, en particular, podemos decir que la conjetura *abc* afirma que si se fija el radical, esto es, si consideramos sumas en las que *abc* tienen los mismos factores primos, entonces hay sólo un número finito de tales sumas.

La importancia del ϵ que aparece en la versión de Masser se puede apreciar en el siguiente ejemplo desarrollado por Wojtek Jastrzebowski y Dan Spielman.

$a+b=c$	$\log c$	$\sum_{p\mid abc}\log p$
$2+3=5$	$\log 5$	$\log 30$
$9+16=25$	$\log 25$	$\log 30$
$3+125=128$	$\log 128$	$\log 30$
$19\cdot 1307+7\cdot 29^2\cdot 31^8=2^8\cdot 3^{22}\cdot 5^4$	$36{,}1523\cdots$	$22{,}2683\cdots$

CUADRO 1. Ejemplos de triplas (a,b,c)

Mostraremos que no existe k tal que $c\leq k\,\mathrm{rad}\,(abc)$, para triplas (a,b,c) que cumplan las condiciones de la hipótesis. Si $n\in\mathbb{Z}^+$, tomemos $a_n=3^{2^n}-1,\ b_n=1,\ c_n=3^{2^n}$. Entonces para cada entero positivo n, $\mathrm{m.c.d.}\,(a_n,b_n,c_n)=1$ y $a_n+b_n=c_n$, por lo tanto, (a_n,b_n,c_n) satisface las hipótesis de la conjetura *abc*. Supongamos que existe una constante k tal que

$$3^{2^n}\leq k\,\mathrm{rad}\,(a_nb_nc_n);$$

como $2^n|(3^{2^n}-1)$ y

$$\mathrm{rad}\,(a_nb_nc_n)=3\,\mathrm{rad}\,(3^{2^n}-1)=3\,\mathrm{rad}\left(2^n\cdot\frac{3^{2^n}-1}{2^n}\right)\leq 3\cdot 2\cdot\frac{3^{2^n}-1}{2^n},$$

tenemos que $3^{2^n}\leq 6k\cdot\frac{3^{2^n}-1}{2^n}$. Multiplicando ambos lados de la desigualdad por 2^n y dividiendo por 3^{2^n} obtenemos: $2^n\leq 6k\cdot\frac{3^{2^n}-1}{3^{2^n}}$, lo cual implica que para cada $n\in\mathbb{Z}^+$, $2^{n-1}\leq 6k$, y esto es evidentemente una contradicción. Este ejemplo fue presentado por SERGE LANG (véase [24]).

3. Aplicaciones de la conjetura *abc*

La conjetura *abc* parece estar siempre situada sobre la frontera entre lo conocido y lo desconocido. Es una simple, pero poderosa afirmación, entre las propiedades aditivas y multiplicativas de los enteros, con la cual es posible probar muchos teoremas en teoría de números que se ven muy difíciles sin ella, por ejemplo, el último teorema de Fermat para exponentes suficientemente grandes, tal como fue mostrado en la sección anterior. En esta sección presentaremos algunas de estas consecuencias bajo la hipótesis de que la conjetura *abc* sea verdadera.

3.1. Conjetura de Catalan. La *conjetura de Catalan* asegura que 8 y 9 son las únicas potencias consecutivas. Con otras palabras, que la única solución de la *ecuación de Catalan*

$$x^m-y^n=1 \tag{9}$$

con x,y,m,n enteros mayores que 1 es $3^2-2^3=1$.

Veamos algo de la historia de este problema. El enunciado de esta conjetura apareció en una carta que escribió Catalan en 1884 [5]. En 1850 Victor Lebesgue, usando enteros gaussianos, probó que la ecuación $x^m - y^2 = 1$ no tiene solución en enteros positivos x, y cuando $m > 2$ [25]. En 1964, Chao Ko [18] probó que $x^2 - y^n = 1$ no tiene soluciones en enteros positivos cuando $n > 2$ (después del resultado de Lebesgue se necesitaron casi 120 años para establecer este caso especial). Tijdeman, en 1976, demostró que hay a lo sumo un número finito de potencias consecutivas [50]. Finalmente, en 2004, Preda Mihăilescu [32] logró una demostración completa de este resultado. El lector que esté interesado en conocer detalles anteriores a esta demostración bien puede puede consultar [42] y [43].

De acuerdo con lo anterior, será suficiente considerar la ecuación de Catalan cuando mín $(m, n) \geq 3$.

Teorema 3.1 (Teorema asintótico de Catalan o teorema de Tidjeman)**.** *La conjetura abc implica que la ecuación de Catalan tiene solo un número finito de soluciones.*

Demostración. Sea (x, y, m, n) una solución a la ecuación de Catalan (9). Entonces x, y son primos relativos (ya que si $p|x$ y $p|y$, $p|(x^m - y^n)$ lo cual implicaría que $p|1$). Aplicando la conjetura *abc* con $a = x^m$, $b = -y^n$, $c = 1$ y $\epsilon = 1/4$, existe una constante $k_{1/4}$ tal que

$$y^n < x^m = \text{máx}\,(x^m, y^n, 1) \leq k_{1/4}\big(\text{rad}\,(x^m y^n)\big)^{5/4} = k_{1/4}\big(\text{rad}\,(xy)\big)^{5/4}.$$

Entonces,

$$n \log y < m \log x \leq \log k_{1/4} + \frac{5}{4} \cdot \log xy = \log k_{1/4} + \frac{5}{4}(\log x + \log y),$$

y sumando las desigualdades correspondientes a $\log x$ y $\log y$ obtenemos

$$m \log x + n \log y < 2 \log k_{1/4} + \frac{5}{2}(\log x + \log y),$$

lo cual implica que

$$\left(m - \frac{5}{2}\right) \log x + \left(n - \frac{5}{2}\right) \log y < 2 \log k_{1/4}. \tag{10}$$

Como $x, y \geq 2$, se sigue que

$$(m + n - 5) \log 2 < 2 \log k_{1/4} m + n < \frac{2 \log k_{1/4}}{\log 2} + 5.$$

De acuerdo con esta última desigualdad, tenemos que hay sólo un número finito de parejas (m, n) de enteros para los cuales la ecuación de Catalan es soluble. Además, para exponentes fijos $m \geq 3$ y $n \geq 3$ la ecuación (10) tiene solo un número finito de soluciones en enteros positivos x y y. Por lo tanto, el conjunto de soluciones (x, y, m, n) es finito, y ésto completa la demostración. ☑

3.2. Primos de Wieferich. Sean $n \in \mathbb{Z}$ y p un primo. Entonces si $n \neq 0$ existe un entero no negativo d tal que $p^d | n$ pero $p^{d+1} \nmid n$. El número d es llamado el orden de n en p y se denota por $\operatorname{ord}_p n$. Por convención, si $n = 0$, $\operatorname{ord}_p 0 = \infty$.

Diremos entonces que un entero positivo v es un *número poderoso* si para cada primo p que divide a v, $\operatorname{ord}_p v \geq 2$.

Por el *pequeño teorema de Fermat* sabemos que para todo primo impar p, $2^{p-1} \equiv 1 \pmod{p}$, es decir, p divide $2^{p-1} - 1$. Un primo impar p tal que

$$2^{p-1} \not\equiv 1 \pmod{p^2}$$

se llama un *primo de Wieferich*.

Por ejemplo, 3, 5 y 7 son primos de Wieferich dado que $2^2 \not\equiv 1 \pmod{9}$, $2^4 \not\equiv 1 \pmod{25}$, y $2^6 \not\equiv 1 \pmod{49}$.

Wieferich [58] probó que si p es un número primo impar para el cual la ecuación de Fermat

$$x^p + y^p = z^p$$

tiene una solución en enteros x, y, z con $\text{m. c. d.}\,(p, xyz) = 1$, entonces

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Los cálculos que se han hecho sugieren que tales primos son muy raros pero que también hay "muchos" primos que son primos de Wieferich. Aún no se conoce si existen infinitos primos que sean primos de Wieferich ni tampoco si existen infinitos primos que no lo sean. Ahora bien, asumiendo la conjetura *abc* podemos dar una demostración de que el conjunto W de primos de Wieferich es infinito. Esta prueba se debe a Joseph H. Silverman [44]. Empezamos este demostración con el siguiente lema:

Lema 3.1. *Sea p un primo impar. Si existe un entero n tal que $2^n \equiv 1 \pmod{p}$ pero $2^n \not\equiv 1 \pmod{p^2}$, entonces p es un primo de Wieferich.*

Demostración. Sea d el orden de 2 módulo p (es decir, d es el menor entero positivo tal que $2^d \equiv 1 \pmod{p}$), entonces $d|n$. Dado que $2^n \not\equiv 1 \pmod{p^2}$, se sigue que $2^d \not\equiv 1 \pmod{p^2}$, de modo que $2^d = 1 + kp$ donde $\text{m. c. d.}\,(k, p) = 1$. Además, como $2^{p-1} \equiv 1 \pmod{p}$, entonces $d|(p-1)$, es decir, $p - 1 = de$ donde e es un entero tal que $1 \leq e \leq p - 1$. Tenemos entonces que $\text{m. c. d.}\,(ek, p) = 1$ y

$$2^{p-1} = 2^{de} = (2^d)^e = (1 + kp)^e.$$

Como

$$(1 + kp)^e = \sum_{t=0}^{e} \binom{e}{t} (kp)^t \equiv \binom{e}{0} + \binom{e}{1} kp \pmod{p^2}$$

entonces,

$$2^{p-1} \equiv 1 + ekp \pmod{p^2}, \quad 2^{p-1} \not\equiv 1 \pmod{p^2},$$

y por lo tanto p es un primo de Wieferich. ☑

Teorema 3.2. *La conjetura abc implica que existen infinitos primos de Wieferich.*

Demostración. Para cada entero positivo n escribimos

$$2^n - 1 = u_n v_n$$

donde v_n es el número poderoso maximal que divide a $2^n - 1$. Es decir,

$$v_n = \prod_{p|2^n-1, \mathrm{ord}_p(2^n-1)\geq 2} p^{\mathrm{ord}_p(2^n-1)} \quad \text{y} \quad u_n = \prod_{p|2^n-1, \mathrm{ord}_p(2^n-1)=1} p.$$

Tenemos entonces que u_n es libre de cuadrados, y como para cada primo p que divide a u_n se cumple

$$2^n \equiv 1 \pmod{p}, \quad 2^n \not\equiv 1 \pmod{p^2},$$

se sigue, del Lema 3.1, que $p \in W$, de modo que u_n es un entero libre de cuadrados divisible únicamente por primos de Wieferich.

Supongamos ahora que W es finito. Entonces existe solo un número finito de enteros sin factores cuadráticos cuyos únicos divisores son primos de Wieferich. En consecuencia, el conjunto $\{u_n : n = 1, 2, \dots\}$ es finito, y como $\{2^n - 1 : n = 1, 2, \dots\}$ es infinito, esto implica que $\{v_n : n = 1, 2, \dots\}$ es también infinito. Por otra parte, por ser v_n un número poderoso,

$$\mathrm{rad}\,(v_n) \leq v_n^{1/2}.$$

Sea $0 < \epsilon < 1$. Aplicando la conjetura *abc* a la identidad

$$(2^n - 1) + 1 = 2^n,$$

como $v_n \leq 2^n - 1$ obtenemos,

$$\begin{aligned} v_n < 2^n &= \max(2^n - 1, 1, 2^n) \leq k_\epsilon \,\mathrm{rad}\left(2^n(2^n-1)\right)^{1+\epsilon} \\ &= k_\epsilon \,\mathrm{rad}\,(2u_n v_n)^{1+\epsilon} \leq k_\epsilon (2u_n)^{1+\epsilon} \,\mathrm{rad}\,(v_n)^{1+\epsilon} \leq k'_\epsilon \cdot v_n^{(1+\epsilon)/2} \end{aligned}$$

donde $k'_\epsilon = k_\epsilon \cdot s$, siendo s una constante tal que $u_n \leq s$ para cada n. La última desigualdad que obtuvimos implica que los v_n están acotados, lo cual, por supuesto, es una contradicción. Por lo tanto, W no puede ser finito. ☑

3.3. Conjetura original de Hall. Esta conjetura la formuló Marshall Hall, Jr. en 1970 [16].[6]

Conjetura 2 (Conjetura original de Hall)**.** *Sean u y v números enteros, primos relativos*[7] *tales que $u^3 - v^2 \neq 0$. Entonces*

$$|u^3 - v^2| \gg |u|^{1/2-\epsilon}.$$

[6] Para ella existe una versión polinomia demostrada, en 1965, por Harold Davenport [7].

[7] Originalmente la hipótesis de que u y v son primos relativos no fue hecha, pero dado cualquier par de enteros no nulos podemos eliminar los factores que tienen en común y continuar como se hace en la demostración de Lang.

Teorema 3.3. *La conjetura abc implica la conjetura original de Hall.*

Demostración. La siguiente prueba se debe a Lang [23]. Nótese que equivalentemente se podría afirmar que si $v^2 = u^3 + t$ para algún $t \in \mathbb{Z}$, entonces t está acotado. En particular, la conjetura *abc* implicaría que

$$|u| \ll |t|^{2+\epsilon}. \tag{11}$$

A continuación, probaremos una afirmación un poco más general. Fijamos $a, b \in \mathbb{Z}$ no nulos, y $m, n \in \mathbb{Z}^+$ tales que $mn > m + n$. Pongamos

$$a \cdot u^m + b \cdot v^n = k.$$

Para $\epsilon' > 0$ fijo, aplicamos la conjetura *abc* a la anterior igualdad y obtenemos

$$|u|^m \ll \left|u \cdot v \cdot \operatorname{rad}(k)\right|^{1+\epsilon'}$$

y

$$|v|^n \ll \left|u \cdot v \cdot \operatorname{rad}(k)\right|^{1+\epsilon'}. \tag{12}$$

Sin pérdida de la generalidad, supongamos que $|a \cdot u^m| \leq |b \cdot v^n|$. Entonces

$$|u| \ll |v|^{n/m}. \tag{13}$$

Por (12) y (13):

$$|v|^n \ll \left|v^{\frac{n}{m}+1} \cdot \operatorname{rad}(k)\right|^{1+\epsilon'} = |v|^{\left(\frac{n}{m}+1\right)(1+\epsilon')} \cdot (\operatorname{rad} k)^{1+\epsilon'},$$

por lo tanto,

$$|v|^{n-\left(\frac{n}{m}+1\right)(1+\epsilon')} \ll (\operatorname{rad} k)^{1+\epsilon'},$$

y en consecuencia:

$$|v| \ll (\operatorname{rad} k)^{\frac{(1+\epsilon')m}{nm\cdot(n+m)(1+\epsilon')}} \leq k^{\frac{(1+\epsilon')m}{nm\cdot(n+m)(1+\epsilon')}}.$$

Entonces, por (13)

$$|u| \ll k^{\frac{(1+\epsilon')\cdot n}{nm\cdot(m+n)(1+\epsilon')}}. \tag{14}$$

Teniendo establecido el caso general, podemos ahora, establecer la implicación de la conjetura de Hall. Tomamos $\epsilon = \frac{12\epsilon'}{1-5\epsilon'}$. Entonces $\epsilon' = \frac{\epsilon}{12+5\epsilon}$. Escogemos $m = 3$, $n = 2$, $a = 1$ y $b = -1$, de esta manera la ecuación

$$a \cdot u^m + b \cdot v^n = k$$

que vamos a considerar es

$$u^3 - v^2 = k.$$

Por (14):[8]

$$|u| \ll k^{\frac{2+2\epsilon'}{1-5\epsilon'}} = k^{2+\frac{12\epsilon'}{1-5\epsilon'}},$$

y entonces

$$|u|^{\frac{1}{2}-\frac{12\epsilon'}{1-5\epsilon'}} \ll k^{2+\left(\frac{12\epsilon'}{1-5\epsilon'}\right)\left(\frac{1}{2}-\frac{12\epsilon'}{1-5\epsilon'}\right)} = k^{1-\frac{3}{2}\cdot\frac{12\epsilon'}{1-5\epsilon'}-\left(\frac{12\epsilon'}{1-5\epsilon'}\right)^2}.$$

[8] Nótese que de la desigualdad que obtenemos se puede llegar a (11) escrita anteriormente.

Sustituyendo por ϵ obtenemos

$$|u|^{\frac{1}{2}-\epsilon} \ll k^{1-\frac{3}{2}\cdot\epsilon-\epsilon^2} < k,$$

que finalmente nos conduce a

$$|u|^{\frac{1}{2}-\epsilon} \ll |u^3 - v^2|. \quad \boxtimes$$

3.4. Una forma efectiva de la conjetura abc. Todd Cochrane y Robert E. Dressler [6] se preguntaron si la distancia entre dos enteros positivos A, C tales que $C - A < A < C$ y con los mismos factores primos podría ser pequeña. A partir de la conjetura *abc*, ellos lograron demostrar que para todo $\epsilon > 0$, la desigualdad $C - A < A^{1/2-\epsilon}$ tiene sólo un número finito de soluciones (A, C).

En esta sección, asumiendo una forma débil, pero efectiva, de la conjetura *abc*, demostraremos que $C - A > A^{0,4}$ siempre, excepto en dos casos dados explícitamente.

Consideremos las triplas (a, b, c) de enteros positivos que satisfacen:

$$\begin{cases} a + b = c \\ a < b \\ \text{m. c. d. } (a, b, c) = 1. \end{cases} \tag{15}$$

Para cada tripla (a, b, c), sea

$$L = L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)}.$$

Consideremos, además, las parejas (A, C) de enteros positivos que satisfacen:

$$C - A < A < C \qquad \text{y}$$
$$\operatorname{rad}(A) = \operatorname{rad}(C),$$

las cuales se llaman *parejas admisibles*.

Para cada pareja admisible (A, C) definimos

$$\alpha = \alpha(A, C) = \frac{\log(C - A)}{\log A},$$

de modo que $A^\alpha = C - A$.

Si p es un número primo, escribimos $p^r \| n$ si $p^r | n$ pero $p^{r+1} \nmid n$.

Lema 3.2. *Si (A, C) es una pareja admisible, entonces para todo entero positivo d la pareja (Ad, Cd) es también admisible, $\alpha(A, C) < \alpha(Ad, Cd)$ para todo $d > 1$ y $\lim_{d\to\infty} \alpha(Ad, Cd) = 1$.*

Demostración. Veamos, en primer lugar, que si $d \geq 1$ entonces (Ad, Cd) es una pareja admisible. Dado que $C - A < A < C$, por ser d un entero positivo tenemos que $(C-A)d < Ad < Cd$ y además $\operatorname{rad}(Ad) = \operatorname{rad}(Cd)$ pues, si p es un primo tal que $p | \operatorname{rad}(Ad)$ entonces $p|d$ o $p|A$, y sabemos que $\operatorname{rad}(A) = \operatorname{rad}(C)$,

luego, en cualquiera de los dos casos $p|\operatorname{rad}(Cd)$; así que $\operatorname{rad}(Ad)|\operatorname{rad}(Cd)$, y similarmente, $\operatorname{rad}(Cd)|\operatorname{rad}(Ad)$. Por lo tanto, $\operatorname{rad}(Ad)=\operatorname{rad}(Cd)$, y con ésto, (Ad, Cd) es una pareja admisible. Ahora veamos que $\alpha(A,C)\leq\alpha(Ad,Cd)$ para cada entero $d>1$. Tenemos lo siguiente:

$$\alpha(A,C)=\frac{\log(C-A)}{\log A},\quad \text{y}$$
$$\alpha\ (Ad,Cd)=\frac{\log(Cd-Ad)}{\log Ad}.$$

Como $C-A<A$, entonces $\log(C-A)<\log A$. Así que

$$\begin{aligned}\log(C-A)\log d &< \log A\log d,\\ \log(C-A)\big(\log d+\log A\big) &< \log A\big(\log d+\log(C-A)\big),\\ \frac{\log(C-A)}{\log A} &< \frac{\log d+\log(C-A)}{\log d+\log A}\\ &= \frac{\log\big((C-A)d\big)}{\log Ad},\end{aligned}$$

que era lo que se quería.

Faltaría ver que $\lim_{d\to\infty}\alpha(Ad,Cd)=1$.

$$\lim_{d\to\infty}\alpha(Ad,Cd)=\lim_{d\to\infty}\frac{\log d+\log(C-A)}{\log d+\log A}=\lim_{d\to\infty}\frac{1+\frac{\log(C-A)}{\log d}}{1+\frac{\log A}{\log d}}=1.\quad ☑$$

Decimos que la pareja admisible (A,C) es una *pareja reducida* si para cada primo p que divida a A, la pareja $\big(A/p, C/p\big)$ no es admisible.

Lema 3.3. *(I) La pareja admisible (A,C) es reducida si y sólo si, para todo primo p que divida a A se tiene $p\|A$ y $p^2|C$ o $p\|C$ y $p^2|A$.*

(II) Para cada pareja admisible (A,C) existe un único entero d tal que

$$d|\operatorname{m.c.d.}(A,C),$$

y la pareja (Ad,Cd) es admisible y reducida.

Demostración. ($\Rightarrow$) Sean (A,C) una pareja reducida y p un número primo. Si $p\|A$ y $p\|C$ entonces $\operatorname{rad}(A/p)=\operatorname{rad}(C/p)$, es decir, $(A/p, C/p)$ es una pareja admisible. Ahora bien, si suponemos que $p^2|A$ y $p^2|C$ para algún primo p, dado que $\operatorname{rad}(A)=\operatorname{rad}(C)$, también en este caso tenemos que $(A/p, C/p)$ es una pareja admisible. Pero esto contradice que (A,C) sea una pareja reducida, por lo tanto, para cada primo p se tiene que: $p\|A$ y $p^2|C$ o $p\|C$ y $p^2|A$.

($\Leftarrow$) Supongamos ahora que para cada primo p tal que $p|A$ se tiene $p\|A$ y $p^2|C$, o $p\|C$ y $p^2|A$. Si existiera un primo p para el cual la pareja $(A/p, C/p)$ fuese admisible entonces, $\mathrm{rad}\big(A/p\big) = \mathrm{rad}\big(C/p\big)$, pero esto no posible pues:

- Si $p\|A$ y $p^2|C$, $p\big|\,\mathrm{rad}\,\big(C/p\big)$ pero $p\nmid \mathrm{rad}\,\big(A/p\big)$.
- Si $p\|C$ y $p^2|A$, $p\big|\,\mathrm{rad}\,\big(A/p\big)$ pero $p\nmid \mathrm{rad}\,\big(C/p\big)$.

Por lo tanto, la pareja (A, C) es una pareja reducida. Para cada primo p que divida a A, sea

$$S_p = \begin{cases} \text{mín}\,\big(\mathrm{ord}_p(A), \mathrm{ord}_p(C)\big) - 1; & \text{si } \mathrm{ord}_p(A) \neq \mathrm{ord}_p(C) \\ \mathrm{ord}_p(A); & \text{si } \mathrm{ord}_p(A) = \mathrm{ord}_p(C). \end{cases}$$

Tomemos d de manera que

$$\mathrm{ord}_p(d) = S_p \leq \text{mín}\,\big(\mathrm{ord}_p(A), \mathrm{ord}_p(C)\big).$$

Entonces

$$d|\,\mathrm{m.\,c.\,d.}\,(A, C).$$

Por construcción,

$$\mathrm{ord}_p(A) < \mathrm{ord}_p(C) \Rightarrow \mathrm{ord}_p(d) = \mathrm{ord}_p(A) - 1;$$

y en este caso

$$\mathrm{ord}_p\left(\frac{A}{d}\right) = 1$$

y

$$\mathrm{ord}_p\left(\frac{C}{d}\right) = \mathrm{ord}_p(C) - \big(\mathrm{ord}_p(A) - 1\big) \geq 2.$$

Similarmente, en el caso en que $\mathrm{ord}_p(A) > \mathrm{ord}_p(C)$ tenemos

$$\mathrm{ord}_p\left(\frac{C}{d}\right) = 1 \qquad \text{y} \qquad \mathrm{ord}_p\left(\frac{A}{d}\right) \geq 2.$$

Si $\mathrm{ord}_p(A) = \mathrm{ord}_p(C)$, tenemos $\mathrm{ord}_p(d) = \mathrm{ord}_p(A) = \mathrm{ord}_p(C)$ y en este caso

$$\mathrm{ord}_p\left(\frac{A}{d}\right) = \mathrm{ord}_p\left(\frac{C}{d}\right) = 0.$$

Se sigue, que $\mathrm{rad}\,(A/d) = \mathrm{rad}\,(C/d)$. Como (A, C) es una pareja admisible entonces, $C - A < A < C$, y por lo tanto $C/d - A/d < A/d < C/d$. Nótese que $d \neq 0$ pues A y C no son 0. De esta manera, $(A/d, C/d)$ es también una pareja admisible, y aplicando la parte (I), $(A/d, C/d)$ que es reducida. Además d, por construcción, es única. ☑

Para una pareja admisible (A, C) definimos la tripla (a, b, c) de la siguiente manera

$$a = \frac{C - A}{\mathrm{rad}\,(A)}, \quad b = \frac{A}{\mathrm{rad}\,(A),} \quad c = \frac{C}{\mathrm{rad}\,(a)}.$$

Y para una tripla de enteros positivos (a, b, c) que satisface (15), definimos la pareja (A, C) como sigue

$$A = b \cdot \operatorname{rad}(bc), \quad C = c \cdot \operatorname{rad}(bc).$$

Entonces $C - A = a \cdot \operatorname{rad}(bc)$.

Lema 3.4. *(I) La tripla (a, b, c) definida por la pareja admisible (A, C) satisface (15).*
(II) La pareja (A, C) definida por la tripla (a, b, c) es admisible y reducida.
(III) Las fórmulas de (a, b, c) y (A, C) corresponden a las triplas que satisfacen (15) y las parejas admisibles reducidas, respectivamente.

Demostración. (I) Sea (A, C) una pareja admisible reducida, y (a, b, c) la tripla definida por ella. Entonces, dado que $C - A < A < C$, tenemos que a, b y c son enteros positivos, $a < c$ y además

$$a + b = \frac{C - A}{\operatorname{rad}(A)} + \frac{A}{\operatorname{rad}(A)} = \frac{C}{\operatorname{rad}(A)} = c. \tag{16}$$

Si p es un primo tal que $p \mid (A/\operatorname{rad}(A))$, $p \mid (C/\operatorname{rad}(A))$ entonces, $p^2|A$ y $p^2|C$. Pero, esto contradice que (A, C) sea reducida (Lema 3.3. (i)). Por lo tanto,

$$\text{m. c. d.}\left(\frac{A}{\operatorname{rad}(A)}, \frac{C}{\operatorname{rad}(A)}\right) = 1\,,$$

y esto termina la prueba, ya que lo anterior implica que $\text{m. c. d.}(a, b, c) = 1$.

(II) Veamos que la pareja (A, C) definida por la tripla (a, b, c) es admisible y reducida.

$$C - A = a \cdot \operatorname{rad}(bc) < b \cdot \operatorname{rad}(bc) = A < (a + b) \cdot \operatorname{rad}(bc) = C.$$

Además, $\operatorname{rad}(A) = \operatorname{rad}\big(b \cdot \operatorname{rad}(bc)\big) = \operatorname{rad}(bc) = \operatorname{rad}\big(c \cdot \operatorname{rad}(bc)\big) = \operatorname{rad}(C)$. Por lo tanto, (A, C) es una pareja admisible.

Ahora bien, usando el Lema 3.3. (i), veamos que (A, C) es reducida. Si p es un primo tal que $p^2 \big| \big(b \cdot \operatorname{rad}(bc)\big)$, dado que $\text{m. c. d.}(a, b, c) = 1$ entonces, $p|b$ y por lo tanto, $p \nmid c$ y $p^2 \nmid \big(c \cdot \operatorname{rad}(bc)\big)$. Es decir, $p \| C$. Similarmente ocurre cuando tomamos un primo p tal que $p^2 \big| \big(c \cdot \operatorname{rad}(bc)\big)$. De esta manera, para cada primo p que divide a A tenemos que $p^2|A$ y $p \| C$ o $p^2|C$ y $p \| A$.

(III) Sea (A, C) una pareja admisible y reducida. Veamos que existe una tripla (a, b, c) que la define.

Si tomamos $a = \dfrac{C - A}{\operatorname{rad}(A)}$, $b = \dfrac{A}{\operatorname{rad}(A)}$ y $c = \dfrac{C}{\operatorname{rad}(A)}$, la pareja que define la tripla (a, b, c) es precisamente la pareja (A, C) pues

$$\operatorname{rad}\left(\frac{AC}{(\operatorname{rad} A)^2}\right) = \operatorname{rad}(AC),$$

ya que para cada primo p, si $p \big| (AC/(\operatorname{rad} A)^2)$ entonces $p|AC$ y, si suponemos que existe un primo q tal que, $q \big| \operatorname{rad}(AC) = \operatorname{rad}(A)$ y $q \nmid (AC/(\operatorname{rad} A)^2)$, dado

que (A, C) es reducida entonces $q \| A$ y $q^2 | C$ o, $q^2 | A$ y $q \| C$. Pero en cualquiera de los dos casos tendremos que $q^3 | AC$, y esto implica que $q \big| (AC/(\operatorname{rad} A)^2)$, lo cual es una contradicción. Por lo tanto,

$$\operatorname{rad}(bc) = \operatorname{rad}\left(\frac{AC}{(\operatorname{rad} A)^2}\right) = \operatorname{rad}(AC) = \operatorname{rad}(A)$$

entonces,

$$b \cdot \operatorname{rad}(bc) = \frac{A}{\operatorname{rad}(A)} \cdot \operatorname{rad}(A) = A$$

y

$$c \cdot \operatorname{rad}(bc) = \frac{C}{\operatorname{rad}(A)} \cdot \operatorname{rad}(A) = C.$$

Finalmente, veamos que para cada tripla (a, b, c) existe una pareja admisible y reducida (A, C) que la define. Sea $A = b \cdot \operatorname{rad}(bc)$ y $C = c \cdot \operatorname{rad}(bc)$. La tripla definida por la pareja $b \cdot \operatorname{rad}(bc), c \cdot \operatorname{rad}(bc)$ es precisamente la tripla (a, b, c) pues,

$$\frac{C - A}{\operatorname{rad}(A)} = \frac{(c-b) \cdot \operatorname{rad}(bc)}{\operatorname{rad}\big(b \cdot \operatorname{rad}(bc)\big)} = \frac{(c-b) \cdot \operatorname{rad}(bc)}{\operatorname{rad}(bc)} = a,$$

$$\frac{A}{\operatorname{rad}(A)} = \frac{b \cdot \operatorname{rad}(bc)}{\operatorname{rad}\big(b \cdot \operatorname{rad}(bc)\big)} = \frac{b \cdot \operatorname{rad}(bc)}{\operatorname{rad}(bc)} = b,$$

$$\frac{C}{\operatorname{rad}(A)} = \frac{c \cdot \operatorname{rad}(bc)}{\operatorname{rad}\big(b \cdot \operatorname{rad}(bc)\big)} = \frac{c \cdot \operatorname{rad}(bc)}{\operatorname{rad}(bc)} = c. \quad \boxtimes$$

Podemos ahora enunciar una versión de la conjetura *abc* de la siguiente manera:

Conjetura 1′. *Para todo número real $q > 1$ existe solo un número finito de triplas (a, b, c) que satisfacen las condiciones (15) y $L(a, b, c) > q$.*

(Recordemos que la anterior fue la forma en la que originalmente Oesterlé enunció la conjetura *abc*.)

Conjetura 3. *Sólo hay 11 triplas (a, b, c) que satisfacen $L(a, b, c) > 1{,}5$.*

Las 11 triplas a las que se refiere la Conjetura 3 se encuentran en el Cuadro 2.

Observación 3.1. La Conjetura $(1')$ sólo garantiza que existe un número finito de triplas (a, b, c) para las cuales $L(a, b, c) > 1{,}5$, pero no nos asegura que ese número sea 11, por lo tanto, no implica la Conjetura 3. Tampoco esta última implica la primera, pues podría existir un número real q_0, $0 < q_0 < 1{,}5$ para el cual infinitas triplas (a, b, c) satisfagan $1{,}5 > L(a, b, c) > q_0$. Decimos entonces, simplemente, que la Conjetura 3 es una versión débil de la Conjetura $(1')$.

Teorema 3.4. *Para una pareja (A, C) admisible y reducida, sea (a, b, c) la tripla que ella define. Si $\alpha = \alpha(A, C) < t < 1/2$ entonces, $L = L(a, b, c) > \dfrac{1-t}{t} > 1$.*

N_0	a	b	c	$L(a,b,c)$
1.	2	$3^{10}\cdot 109$	23^5	1,629912
2.	11^2	$3^2\cdot 5^6\cdot 7^3$	$2^{21}\cdot 23$	1,625991
3.	$19\cdot 1307$	$7\cdot 29^2\cdot 31^8$	$2^8\cdot 3^{22}\cdot 5^4$	1,623490
4.	283	$5^{11}\cdot 13^2$	$2^8\cdot 3^8\cdot 17^3$	1,580756
5.	1	$2\cdot 3^7$	$5^4\cdot 7$	1,567887
6.	7^3	3^{10}	$2^{11}\cdot 29$	1,547075
7.	$7^2\cdot 41^2\cdot 311^3$	$11^{16}\cdot 13^2\cdot 79$	$2\cdot 3^3\cdot 5^{23}\cdot 953$	1,54434
8.	5^3	$2^9\cdot 3^{17}\cdot 13^2$	$11^5\cdot 17\cdot 31^3\cdot 137$	1,536714
9.	$13\cdot 19^6$	$20^{30}\cdot 5$	$3^{13}\cdot 11^2\cdot 31$	1,526999
10.	$3^{18}\cdot 23\cdot 2269$	$17^3\cdot 29\cdot 31^8$	$2^{10}\cdot 5^2\cdot 17^{15}$	1,522160
11.	239	$5^8\cdot 17^3$	$2^{10}\cdot 37^4$	1,502839

CUADRO 2. Triplas conocidas para las cuales $L(a,b,c)>1{,}5$.

Demostración. Recordemos que

$$\alpha(A,C)=\frac{\log(C-A)}{\log A}\quad \text{y}\quad L(a,b,c)=\frac{\log c}{\log \operatorname{rad}(abc)}.$$

Como $a=\dfrac{C-A}{\operatorname{rad}(A)}$ entonces, $C-A=a\cdot\operatorname{rad}(A)=A^\alpha$. Y de acuerdo con la demostración del Lema 3.4. (iii), $\operatorname{rad}(bc)=\operatorname{rad}\left(\frac{AC}{(\operatorname{rad}A)^2}\right)=\operatorname{rad}(AC)=\operatorname{rad}(A)$ y, $A=b\cdot\operatorname{rad}(bc)$. Tenemos que

$$a\cdot\operatorname{rad}(A)=\big(b\cdot\operatorname{rad}(A)\big)^\alpha,$$

lo cual implica

$$a^{1-\alpha}\cdot\big(\operatorname{rad}(A)\big)^{1-\alpha}\le a\cdot\big(\operatorname{rad}(A)\big)^{1-\alpha}=b^\alpha.$$

Entonces

$$a\cdot\operatorname{rad}(A)\le b^{\frac{\alpha}{1-\alpha}},$$

y por lo tanto

$$\begin{aligned}c^{1/L}&=\operatorname{rad}(abc)=\operatorname{rad}(a)\cdot\operatorname{rad}(bc)=\operatorname{rad}(a)\cdot\operatorname{rad}(A)\\&\le a\cdot\operatorname{rad}(A)\le b^{\frac{\alpha}{1-\alpha}}<c^{\frac{\alpha}{1-\alpha}}.\end{aligned}$$

Así, obtenemos que

$$\frac{1}{L}<\frac{\alpha}{1-\alpha}.$$

Dado que $0 < \alpha < 1$, pues C y A son enteros positivos y $C - A < A < C$, la anterior desigualdad nos conduce finalmente a

$$L > \frac{1-\alpha}{\alpha} > \frac{1-t}{t} = 1 + \frac{2}{t}\left(\frac{1}{2} - t\right) > 1. \quad \text{☑}$$

Si ponemos $t = \frac{1}{2} - \epsilon$ obtenemos $L > 1 + \frac{2}{t}\epsilon$. Aplicando la conjetura *abc* tenemos que, para cada $q = 1 + \frac{2}{t}\epsilon$ existe sólo un número finito de triplas (a, b, c) para las cuales $L > 1 + \frac{2}{t}\epsilon$. Ahora bien, si recordamos la correspondencia entre las triplas (a, b, c) y las parejas admisible y reducidas (A, C) (Lema 3.4. (iii)), esto nos conduce a que para cada $\epsilon > 0$ existe sólo un número finito de parejas admisibles y reducidas (A, C) para las cuales $\alpha(A, B) < \frac{1}{2} - \epsilon$.

Además, el número de parejas admisibles (A, C) (no necesariamente reducidas) que satisfacen la desigualdad $\alpha(A, C) < \frac{1}{2} - \epsilon$ también es finito pues, por el Lema 3.2, si (A, C) es una pareja admisible y d es entero positivo, $\lim_{d\to\infty} \alpha(Ad, Cd) = 1$. La sucesión

$$\{(Ad, Cd)\}_{d=1}^{\infty} \tag{17}$$

es estrictamente creciente ya que $C - A < A$ implica que para cada d,

$$\log(C - A) \cdot \big(\log(d + 1) - \log(d)\big) < \log(A) \cdot \big(\log(d + 1) - \log(d)\big);$$

lo cual, haciendo un cálculo simple nos conduce a

$$\frac{\log(C - A)d}{\log Ad} < \frac{\log(C - A)(d + 1)}{\log A(d + 1)}.$$

Tenemos con esto, que sólo para un número finito de enteros d, $\alpha(Ad, Cd) < 1/2 - \epsilon$ (ya que 1 es el único punto de acumulación de la sucesión (17)), y como a cada pareja admisible (A, C) corresponde una única pareja reducida (Lema 3.3. (ii)) según lo anterior, si la pareja admisible (A, C) satisface $\alpha(A, C) < 1/2 - \epsilon$ entonces necesariamente su pareja reducida debe satisfacer la misma desigualdad, lo cual nos conduce directamente al resultado.

En resumen, para cada ϵ $(0 < \epsilon < 1/2)$ existe sólo un número finito de parejas admisibles (A, C), tales que $C - A > A^{1/2-\epsilon}$.

Este resultado se debe a T. Crochrane y R. E. Dressler (véase [6]).

Colorario 1. *Si existen exactamente 11 triplas que satisfacen $L(a, b, c) > 1{,}5$ entonces, salvo dos casos, para todas las parejas (A, C) admisibles y reducidas se cumple $C - A > A^{0,4}$.*

Demostración. Sea $t = 0{,}4$, según el Teorema 3.4 y el Lema 3.4. (iii) las parejas admisibles y reducidas que satisfacen $\alpha(A, C) < 0{,}4$ son precisamente las que corresponden a las triplas (a, b, c) tales que $L(a, b, c) > 1{,}5$. La prueba se concluye haciendo los cálculos de acuerdo con el cuadro 2. ☑

Colorario 2. *Si existe una pareja admisible (A', C') para la cual $\alpha(A', C') < \frac{1}{3}$, se puede encontrar una tripla (a, b, c) que satisfaga las condiciones (15) y $L(a, b, c) > 2$.*

Demostración. Por el Lema 3.3. (ii) sabemos que para la pareja (A', C') existe un entero positivo d para el cual la pareja $(A'/d, C'/d) = (A, C)$ es admisible y reducida. Además, por el Lema 3.2, $\alpha(A, C) < 1/3$. Finalmente, aplicando el Teorema 3.4 a la pareja (A, C), sabemos que para la tripla (a, b, c) que ella define se tiene que $L(a, b, c) > 2$. ☑

3.5. Soluciones a la ecuación diofántica $\alpha x^r + \beta y^s + \gamma z^t = 0$.

Teorema 3.5. *Asumiendo la conjetura abc, fijamos $0 < \epsilon < 1$ y enteros α, β, γ. Entonces la ecuación diofántica $\alpha x^r + \beta y^s + \gamma z^t = 0$ tiene sólo un número finito de soluciones en enteros x, y, z, r, s, t que satisfacen*

$$xyz \neq 0,$$
$$\text{m. c. d. } (x, y) = \text{m. c. d. } (x, z) = \text{m. c. d. } (y, z) = 1,$$
$$r, s, t > 0,$$
$$\frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1 - \epsilon.$$

Además, el número de tales soluciones puede ser efectivamente calculable si la constante k_ϵ de la conjetura abc es efectiva.

Demostración. Consideremos x, y, z, r, s, t una de las soluciones descritas en el teorema. Sin pérdida de generalidad, podemos suponer $\text{m. c. d. } (x, y, z) = 1$. La conjetura *abc* implica que existe una constante k_ϵ para la cual

$$\text{máx}\{|\alpha x^r|, |\beta y^s|, |\gamma z^t|\} < k_\epsilon \big(\text{rad}\,(\alpha\beta\gamma xyz)\big)^{1+\epsilon} \leq k_\epsilon |\alpha\beta\gamma xyz|^{1+\epsilon}. \tag{18}$$

Supongamos que $|\alpha x^r| < |\beta y^s| < |\gamma z^t|$, así que

$$|x| < \left|\frac{\gamma}{\alpha}\right|^{1/r} \cdot |z|^{t/r} \quad \text{y} \quad |y| < \left|\frac{\gamma}{\beta}\right|^{1/s} \cdot |z|^{t/s}.$$

Por (18) tenemos entonces que

$$|z| \ll k_\epsilon \cdot \left|z^{1/t+1/s+1/r}\right|^{1+\epsilon} \ll k_\epsilon \cdot |z|^{1-\epsilon^2}.$$

Por lo tanto, z está acotado. Ahora bien, como $|\alpha x^r| < |\beta y^s|$ entonces,

$$|x| < \left|\frac{\beta}{\alpha}\right|^{1/r} \cdot |y|^{s/r},$$

y por (18),

$$|y| \ll k_\epsilon |y|^{(1/s+1/r)(1+\epsilon)} \cdot |z|^{(1+\epsilon)/s}.$$

Dado que z está acotado, y

$$\frac{1}{s} + \frac{1}{r} < (1 - \epsilon) - \frac{1}{t} < 1 - \epsilon,$$

entonces

$$|y| \ll k_\epsilon \cdot |y|^{1+\epsilon^2},$$

lo cual implica que y está acotado. Similarmente, obtenemos que x también está acotado. Lo anterior implica que

$$\text{máx}\left(|\alpha x^r|, |\beta y^s|, |\gamma z^t|\right) < k_\epsilon \cdot |\alpha\beta\gamma xyz|^{1+\epsilon} \ll 1.$$

Es decir, r, s y t están acotados. Se sigue entonces que el número de soluciones de la ecuación diofántica $\alpha x^r + \beta y^s + \gamma z^t = 0$ que satisfacen las condiciones dadas el enunciado del teorema, es finito. ☑

3.6. Teorema de Roth y conjetura de Mordell. En 1991, Noam D. Elkies mostró que la conjetura *abc* implica la conjetura de Mordell [8]. Y en 1994 Enrico Bombieri mostró que la conjetura *abc* implica el teorema de Roth [4]. Las demostraciones de estas dos implicaciones son muy similares, incluso hay un teorema que implica a ambos, el teorema de Roth y la conjetura de Mordell (véase [52, pág. 69–70]). En realidad, hoy tanto el teorema de Roth como la conjetura de Mordell son teoremas, y desde este punto de vista no parece interesante tener pruebas condicionales de ellos que dependan de la conjetura *abc* cuya validez está aún en entredicho. Sin embargo, los pruebas de estos teoremas a partir de la conjetura *abc* son mucho más simples y transparentes. Aún más importante, usando la conjetura *abc* se pueden demostrar versiones considerablemente fuertes de los dos teoremas. Específicamente, *abc* implica *Mordell eficaz* y una forma fuerte de la conjetura *abc* implica un cierto refinamiento del teorema de Roth.

En esta sección hemos restringido nuestra exposición a los números racionales, pero la conjetura *abc*, la conjetura de Mordell y el teorema de Roth pueden ser formulados en cualquier extensión finita de $\mathbb{Q}$, y *abc* también implica Roth y Mordell en estas situaciones más generales.

Presentaremos primero algunas nociones preliminares necesarias y, a continuación, la demostración del teorema de Roth a partir de una forma fuerte de la conjetura *abc*. Enunciaremos la conjetura de Mordell pero su demostración no la haremos aquí, remitiendo al lector a la bibliografía correspondiente donde la puede encontrar.

En adelante, C denotará una curva elíptica (véase subsección 4.3), $C(\mathbb{Q})$ los puntos en C con coordenadas racionales, P^1 la línea proyectiva y $\overline{\mathbb{Q}}$ la clausura algebraica de $\mathbb{Q}$.

Pensamos en C como el conjunto de puntos $(x_0 : \cdots : x_n) \in P^n$ que satisfacen las ecuaciones homogéneas

$$p_1(x_0, \ldots, x_n) = 0, \ldots, p_k(x_0, \ldots, x_n) = 0$$

con k un entero $\geq n - 1$ y p_i irreducible.

El conjunto de soluciones complejas de estas ecuaciones se conoce como la *superficie de Riemann* $C(\mathbb{C})$.

Si los coeficientes de $p_1, \ldots, p_k$ están en $\mathbb{Q}$ decimos que *C está definida sobre* $\mathbb{Q}$.

Una transformación $f : C \longrightarrow P^m$ está definida por $m+1$ polinomios homogéneos del mismo grado:

$$f : (x_0 : \cdots : x_n) \longmapsto \big(f_0(x_0, \ldots, x_n) : \cdots : f_m(x_0, \ldots, x_n)\big). \tag{19}$$

Si los coeficientes de $f_0, \ldots, f_m$ están en $\mathbb{Q}$ decimos que *f está definida sobre* $\mathbb{Q}$.

Sea $a+b=c$ con $a, b, c \in \mathbb{Z}$ primos relativos, definimos la *altura* y el *radical*[9] de esta suma por:

$$\begin{aligned} h(a,b,c) &= \text{máx}\,(\log|a|, \log|b|, \log|c|), \\ r(a,b,c) &= \sum_{p|abc} \log p, \end{aligned} \tag{20}$$

donde p recorre todos los divisores primos de a, b y c. En estos términos, enunciamos la conjetura *abc* de la siguiente manera:

Para cada $\epsilon > 0$ existe una constante k_ϵ tal que

$$h(a,b,c) \leq r(a,b,c) + \epsilon h(a,b,c) + k_\epsilon$$

para toda suma $a+b=c$ de enteros primos relativos entre sí.

La desigualdad anterior la podemos escribir (de forma equivalente) como:

$$h(a,b,c) \leq \frac{1}{1-\epsilon} r(a,b,c) + \frac{k(\epsilon)}{1-\epsilon}. \tag{21}$$

Una *valuación* de $\mathbb{Q}$ es una función $\nu : \mathbb{Q} \longrightarrow \mathbb{R} \cup \{-\infty\}$ que para alguna constante k satisface:

$$\begin{aligned} &\nu(x) = -\infty, \text{ sólo para } x = 0\ , \\ &\nu(xy) = \nu(x) + \nu(y), \text{ para todo } x, y \in \mathbb{Q}^*\ , \\ &\nu(x+y) \leq k + \text{máx}\,(\nu(x), \nu(y)), \text{ para todo } x, y \in \mathbb{Q}. \end{aligned}$$

Dado un número primo p, denotamos el número de factores p del número racional x por $\text{ord}_p(x)$ (en el caso en que x es un entero esta definición coincide con la que dimos en la subsección 3.2).

Ahora bien, definimos la *valuación p–ádica de* $\mathbb{Q}$ como:

$$\nu_p = -\,\text{ord}_p(x) \log p$$

y la *valuación* ∞ como:

$$\nu_\infty(x) = \log|x|.$$

Por ejemplo, $\nu_2(4/3) = -2\log 2$, $\nu_3(4/3) = \log 3$, $\nu_p(4/3) = 0$ para cualquier otra valuación p–ádica, y $\nu_\infty(4/3) = \log(4/3)$.

[9]El lector no debe confundir $r(a,b,c)$ con $\text{rad}\,(abc)$ definido en la sección 2.

Para todo primo p la valuación p–ádica de $\mathbb{Q}$ es no–arquimediana, pues:

$$\nu_p(x+y) \leq \max\big(\nu_p(x), \nu_p(y)\big) \quad \text{para todo } x, y \in \mathbb{Q}.$$

La valuación ∞ satisface

$$\nu_\infty(x+y) \leq \log 2 + \max\big(\nu_\infty(x), \nu_\infty(y)\big) \quad \text{para todo } x, y \in \mathbb{Q},$$

y la llamamos arquimediana.

Sabemos que las anteriores son las únicas valuaciones sobre $\mathbb{Q}$, excepto por la *valuación trivial*:

$$\nu(0) = -\infty \qquad \text{y,} \qquad \nu(x) = 0 \qquad \text{para } x \neq 0\ .$$

Todo número racional x distinto de 0 tiene una descomposición en factores primos

$$|x| = \prod_p p^{\mathrm{ord}_p(x)}\,;$$

tomando logaritmos, obtenemos la siguiente relación entre las valuaciones de $\mathbb{Q}$.

Proposición 3.1. *Para todo $x \in \mathbb{Q}^*$,*

$$\sum_\nu \nu(x) = 0$$

donde la sumatoria recorre todas las valuaciones sobre $\mathbb{Q}$.

Con otras palabras, la anterior proposición dice que la suma de todas las valuaciones sobre $\mathbb{Q}$ es precisamente la valuación trivial.

La valuación ν_∞ puede extenderse a una valuación de $\mathbb{Q}(\alpha)$ valiéndonos del hecho que un número algebraico α es usualmente visto como una raíz compleja de su polinomio minimal y $|\alpha|$ es justamente el módulo de este número complejo. En el caso de una valuación finita ν_p, toda función $\sigma : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}_p$ da una extensión de ν_p definida por $\nu_p(\beta) = \nu_p\big(\sigma(\beta)\big)$, para $\beta \in \mathbb{Q}(\alpha)$.

Denotamos con $P^2(\mathbb{Q})$ al *plano proyectivo* sobre $\mathbb{Q}$, es decir, el conjunto de triplas $(x : y : z)$ tales que x, y, z son racionales no todos nulos, y para cada $\lambda \in \mathbb{Q}^*$ las triplas $(x : y : z)$ y $(\lambda x : \lambda y : \lambda z)$ denotan el mismo punto de $P^2(\mathbb{Q})$. Tenemos entonces, varios caminos para denotar cada punto en $P^2(\mathbb{Q})$, por ejemplo, dado un punto $(x : y : z)$ podemos escoger λ de tal manera que $\lambda x, \lambda y, \lambda z$ sean enteros primos relativos entre sí, o en el caso en que $z \neq 0$ podemos dividir por z para obtener $(f : g : 1)$ donde $f = x/z$ y $g = y/z$.

La punto $(0 : 0 : 0)$ que llamaremos *indeterminado*, no es un punto de $P^2(\mathbb{Q})$.

La altura del punto $P = (a : b : c) \in P^2(\mathbb{Q})$ está definida por

$$h(P) = h(a : b : c) = \sum_\nu \max\big(\nu(a), \nu(b), \nu(c)\big),$$

donde, como siempre, ν recorre todos las valuaciones sobre $\mathbb{Q}$; si a, b y c no son cero, el radical de P se define como

$$r(P) = r(a:b:c) = \sum_{p:\#\{\nu_p(a),\nu_p(b),\nu_p(c)\}\geq 2} \log p.$$

Se puede chequear fácilmente que las dos definiciones son independientes de la elección de coordenadas de P (en el caso de la altura usamos la Proposición 3.1), y que además, coinciden con las definiciones (20)

Definimos el *término error* de P como

$$e(P) = e(a:b:c) = \text{máx}\big(h(P) - r(P), 0\big).$$

Conjetura 4 (Reformulación de la conjetura *abc*)**.**
Para todo $\epsilon > 0$ existe una constante k_ϵ tal que

$$e(P) \leq \epsilon \cdot h(p) + k_\epsilon, \tag{22}$$

para todo punto $P = (a:b:c) \in P^2(\mathbb{Q})$ sobre la recta $a+b=c$ con $abc \neq 0$.

Si suponemos que en (22) conocemos k_ϵ explícitamente como una función de ϵ entonces, para cada valor de h podemos determinar el mínimo $\psi(h)$ de $\epsilon h + k_\epsilon$:

$$\psi(h) = \min_{\epsilon>0} (\epsilon h + k_\epsilon).$$

En estas condiciones, la desigualdad de la Conjetura 4 se puede escribir como

$$e(P) \leq \psi\big(h(P)\big). \tag{23}$$

Por ejemplo, si $k_\epsilon = \dfrac{k}{\epsilon}$,

$$\psi(\epsilon) = \min_{\epsilon>0} \left(\epsilon h + \frac{k}{\epsilon}\right),$$

$\dfrac{d}{d\epsilon}\left(\epsilon h + \dfrac{k}{\epsilon}\right) = h - \dfrac{k}{\epsilon^2}$, igualando a cero obtenemos que $\left(\epsilon h + \dfrac{k}{\epsilon}\right)$ tiene un valor mínimo cuando $h = \dfrac{k}{\epsilon^2}$ es decir, cuando

$$\epsilon = \left(\frac{k}{h}\right)^{1/2},$$

entonces

$$\psi(h) = \left(\frac{k}{h}\right)^{1/2} \cdot h + k \cdot \left(\frac{h}{k}\right)^{1/2} = 2\sqrt{hk}.$$

Para $x = (x_0 : x_1 : \cdots : x_n) \in P^n(\mathbb{Q})$, la *altura* de x está definida por:

$$h(x) = \sum_{\nu} \text{máx}\,(\nu(x_0), \ldots, \nu(x_n)).$$

El primero, y más importante hecho sobre las alturas, es que para todo $B > 0$ el número de puntos x tales que $x \in P^1(\mathbb{Q})$ y $h(x) \leq B$, es finito.

Sea m un polinomio en dos variables con grado total d ; entonces existe una constante k tal que:

$$\log|\,\mathrm{m.\,c.\,d.}\,(s,t)| \leq d\cdot h(s:t)+k \tag{24}$$

para $s,t\in\mathbb{Z}$ primos relativos.

Una transformación $f : P^1(\mathbb{Q}) \longrightarrow P^m(\mathbb{Q})$ de grado d se define como en (19), tomando $n=1$ y $f_i\in\mathbb{Q}[x_0,x_1]$ de grado d.

Como podemos denotar el punto $f(x)\in P^2$ por

$$\big(\lambda f_0(x_0,x_1),\ldots,\lambda f_m(x_0,x_1)\big)\,,$$

de tal manera que sus coordenadas sean enteros primos relativos, entonces para cada primo p

$$\text{máx}\,\big(\nu_p(\lambda f_0(x_0,x_1)),\ldots,\nu_p(\lambda f_m(x_0,x_1))\big)=0$$

y

$$\begin{aligned}\text{máx}\big(\nu_\infty(\lambda f_0(x_0,x_1)),\ldots,\nu_\infty(\lambda f_m(x_0,x_1))\big)&\\ =\text{máx}\,(\log|\lambda f_0(x_0,x_1)|,\ldots,\log|\lambda f_m(x_0,x_1)|),&\end{aligned}$$

por lo tanto

$$\begin{aligned}h\big(f(x_0:x_1)\big)&=\sum_\nu \text{máx}\,\big(\nu(\lambda f_0(x_0,x_1)),\ldots,\lambda f_m(x_0,x_1)\big)\\ &=\text{máx}\,\big(\log|\lambda f_0(x_0,x_1)|,\ldots,\log|\lambda f_m(x_0,x_1)|\big);\end{aligned}$$

aplicando (24)

$$h(f(x_0:x_1)\leq dh(x_0,x_1)+k.$$

La desigualdad $-k+dh(x)\leq h\big(f(x)\big)$ también es cierta, pero no es tan fácil de demostrar. A continuación veremos las dos desigualdades para una transformación particular, es decir, mostraremos que

$$\big|h\big(f(x)\big)-dh(x)\big|\leq k \tag{25}$$

para una transformación particular.

Consideremos $P:(a:b)\longmapsto(a:b:a+b)$, entonces

$$h(x)\leq h\big(P(x)\big)\leq h(x)+\log 2, \tag{26}$$

la primera desigualdad resulta obvia por la definición de h, veamos la segunda: Tomando x_0 y x_1 primos relativos, por lo que se dijo antes,

$$h\big(P(x)\big)=\text{máx}\,\big(\nu_\infty(x_0),\nu_\infty(x_1),\nu_\infty(x_0+x_1)\big),$$

y aplicando la desigualdad $\nu_\infty(x_0+x_1)\leq\log 2+\text{máx}\,\big(\nu_\infty(x_0),\nu_\infty(x_1)\big)$ obtenemos,

$$\begin{aligned}h\big(P(x)\big)&\leq\text{máx}\,(\nu_\infty(x_0),\nu_\infty(x_1),\log 2+\text{máx}\,\big(\nu_\infty(x_0),(x_1)\big)\\ &=\log 2+\text{máx}\,\big(\nu_\infty(x_0),\nu_\infty(x_1)\big)\\ &=\log 2+h(x_0:x_1)=\log 2+h(x).\end{aligned}$$

Para definir una función de altura sobre $C(\mathbb{Q})$, primero, escogemos una transformación $f : C \longrightarrow P^1$. Si f tiene grado d definimos la altura $h(x) = h_f(x)$ de $x \in C(\mathbb{Q})$ por

$$h(x) = h_f = \frac{1}{d} \cdot h\big(f(x)\big).$$

Si $g : C \longrightarrow P^1$ es otra transformación, existe una constante k tal que

$$\big|h_f(x) - h_g(x)\big| \leq k \cdot \sqrt{h_f(x)}$$

para todo $x \in C(\bar{\mathbb{Q}})$, los puntos con coordenadas algebraicas sobre C.

Consideremos una transformación $f : C \longrightarrow C'$ entre curvas algebraicas no singulares. Permitiendo valores complejos para las coordenadas conseguimos una transformación entre superficies de Riemann, $f : C(\mathbb{C}) \longrightarrow C'(\mathbb{C})$. Para el punto $y \in C'(\mathbb{C})$ la preimagen $f^{-1}\{y\}$ contiene, en general, un cierto número de puntos, digamos d. Sólo para un número finito de puntos y, la preimagen contiene un número diferente de puntos, y en este caso, ese número es menor que d. El número d con esa propiedad es llamado el *grado de* f y lo denotamos con $\operatorname{grad}(f)$.

Cuando $\#f^{-1}\{y\} < \operatorname{grad}(f)$ decimos que f es *ramificada sobre* y.

En general, para un punto $x \in C(\mathbb{C})$, f transforma una vecindad bastante pequeña de x, en $C(\mathbb{C})$, en una pequeña vecindad de $f(x)$, en $C'(\mathbb{C})$, en forma inyectiva.

Sólo para un número finito de puntos x la transformación f no es uno–a–uno en ninguna vecindad de x, para tales puntos x decimos que *f es ramificado en x*. En este caso, existe un número $e \geq 2$ y una vecindad pequeña U de x en $C(\mathbb{C})$ tal que, la restricción de f a $U\backslash\{x\}$ es e–a–uno; e se llama la *multiplicidad de f en x*, y se denota por $e_x(f)$.

Decimos que *f no es ramificada en x* si y sólo si $e_x(f) = 1$.

Una forma de chequear si f es ramificada en un punto x es por medio de la derivada. Sea $\Delta \subset \mathbb{C}$ el disco unidad y $\varphi : \Delta \longrightarrow U$ una biyección analítica, con U como la tomamos anteriormente y $\varphi(0) = x$. Así mismo, sea $\psi : f(U) \longrightarrow \mathbb{C}$ analítica e inyectiva. Entonces $g = \psi \circ f \circ \varphi : \Delta \longrightarrow \mathbb{C}$ es analítica y e–a–uno cerca de 0. Así, $g(z) = g(0) + g_e \cdot z^e + \cdots$ y por lo tanto, f es ramificada sobre y si y sólo si $g'(0) = 0$.

Sabemos que f es ramificada sobre y si y sólo si f es ramificada en algún punto x tal que $f(x) = y$. Sea $g : C' \longrightarrow C''$ otra transformación. Entonces $\operatorname{grad}(g \circ f) = \operatorname{grad} f \cdot \operatorname{grad} g$, y $g \circ f$ es ramificada exactamente sobre cada punto sobre el cual g es ramificada y, sobre cada punto $z \in C''$ tal que f es ramificado en algún elemento de $g^{-1}\{z\}$.

Si contamos los puntos en $f^{-1}\{y\}$ teniendo en cuenta multiplicidades, este número siempre es grad (f), es decir, para cada $y \in C'(\mathbb{C})$:

$$\sum_{x:f(x)=y} e_x(f) = \operatorname{grad}(f). \tag{27}$$

Más adelante aplicaremos la llamada *fórmula de Hurwitz*, la cual relaciona la ramificación de f con el género de C y el género de C'. Esta fórmula es la siguiente,

$$2\,\mathrm{g}(C) - 2 = \big(2\,\mathrm{g}(C') - 2\big)\operatorname{grad}(f) + \sum_{x\in C(\mathbb{C})} \big(e_x(f) - 1\big) \tag{28}$$

donde $\mathrm{g}(C)$ y $\mathrm{g}(C')$ denotan los géneros de las curvas C y C', respectivamente.

Nótese que la suma de la derecha es finita, ya que sólo para un número finito de $x \in C(\mathbb{C})$, se tiene $e_x(f) \neq 1$.

La fórmula de Hurwitz es muy útil para hallar el género de ciertas curvas. Hallemos, por ejemplo, el género de P^1.

Consideremos la transformación $z \longmapsto z^2$ de P^1 en P^1.

El grado de esta transformación es 2, ya que para cada $(x_0 : x_1) \in P^1$ hay, a lo sumo, dos elementos en su preimagen: $(z_0 : z_1)$ y $(z_0 : -z_1)$, y como los únicos elementos en P^1 para los cuales $e_x \neq 1$ (es decir, para los cuales su preimagen está conformada por un sólo elemento) son $(0 : z_1)$ y $(z_0 : 0)$, entonces, $\sum_{x\in C(\mathbb{C})}\big(e_x(f) - 1\big) = 2 \cdot (2 - 1) = 2$.

Aplicando la fórmula de Hurwitz obtenemos

$$2\,\mathrm{g}(P^1) - 2 = \big(2\,\mathrm{g}(P^1) - 2\big) \cdot 2 + \sum_{x\in C(\mathbb{C})} \big(e_x(f) - 1\big),$$

y esto implica que

$$2 \cdot \mathrm{g}\,(P^1) = 0,$$

es decir, el género de P^1 es 0.

Ahora bien, para una transformación que solamente es ramificada sobre 0, 1 y ∞ tenemos que

$$\begin{aligned} 2\,\mathrm{g}\,(C) - 2 &= \big(2\,\mathrm{g}\,(C') - 2\big)\operatorname{grad}(f) + \sum_{x:f(x)=0,1,\infty} \big(e_x(f) - 1\big) \\ &= 2\,\mathrm{g}\,(C')\operatorname{grad}(f) + \operatorname{grad}(f) + \sum_{x:f(x)=0,1,\infty} e_x(f) - \#f^{-1}\{0,1,\infty\}. \end{aligned}$$

Tomando $C' = P^1$, por el resultado anterior y por (27), sabemos que

$$\sum_{x:f(x)=0,1,\infty} e_x(f) = 3 \cdot \operatorname{grad}(f),$$

por lo tanto:

$$2\,\mathrm{g}(C) - 2 = 2\,\mathrm{g}(C')\operatorname{grad}(f) + \operatorname{grad}(f) + \operatorname{grad}(f) - \#f^{-1}\{0,1,\infty\}. \tag{29}$$

Sea C una curva algebraica de género g. El cuerpo de transformaciones $f : C(\mathbb{C}) \longrightarrow P^1(\mathbb{C})$ tiene las valuaciones $\nu_x(f) = -\operatorname{ord}_x(f)$ para cada punto $x \in C(\mathbb{C})$. La proposición análoga a la Proposición 3.1 es $\sum_x \nu_x(f) = 0$.

Para una transformación no constante $f : C(\mathbb{C}) \longrightarrow P^1(\mathbb{C})$, definimos la altura y el radical de $P = (f : 1 - f : 1) \in P^2\big(\mathbb{C}(C)\big)$ por

$$h(P) = \operatorname{grad}(f) \qquad \text{y}$$
$$r(P) = \#f^{-1}\{0,1,\infty\},$$

respectivamente. Por (27) y (28), obtenemos

$$\begin{aligned} 2\,\mathrm{g}(C) - 2 &\geq -2\operatorname{grad}(f) + \sum_{x:f(x)=0,1,\infty} \big(e_x(f) - 1\big) \\ &= \operatorname{grad}(f) - \sum_{x:f(x)=0,1,\infty} 1, \end{aligned}$$

de esta manera,

$$2\,\mathrm{g} - 2 \geq h(P) - r(P),$$

es decir,

$$h(P) \leq 2g - 2 + r(P),$$

que es precisamente el análogo de la conjetura *abc* para funciones algebraicas.

La pregunta que queda, es si esta desigualdad es la mejor posible. Con otras palabras, si existe una transformación $f : C \longrightarrow P^1$ que sea solamente ramificada sobre 0, 1 y ∞.

El siguiente teorema responde esta pregunta.

Teorema 3.6 (Belyĭ)**.** *Dada una curva algebraica C definida sobre $\mathbb{Q}$ y un subconjunto finito Σ de puntos algebraicos sobre C, existe una transformación (llamada de Belyĭ) $f : C \longrightarrow P^1$ definida sobre $\mathbb{Q}$ únicamente ramificada sobre 0, 1 y ∞ y tal que $f(\Sigma) \subseteq \{0,1,\infty\}$.*

Demostración. La demostración está dada en tres pasos:

1) *Reducción a $C = P^1$.*
   Sea $g : C \longrightarrow P^1$ una transformación definida sobre $\mathbb{Q}$, y consideremos el subconjunto finito de P^1 :

$$\Sigma' = g(\Sigma) \cup \{x \in P^1 : g \text{ es ramificado sobre } x\}.$$

Sea $f' : P^1 \longrightarrow P^1$ la transformación que resulta al aplicar el teorema a P^1 y Σ'.

La transformación $f = f' \circ g$ es precisamente la que se requiere para demostrar el teorema. Por esta razón, en adelante, nos dedicaremos a encontrar f'.

Supongamos entonces, que $C = P^1$ y $\Sigma \subset P^1$ es un conjunto finito de puntos algebraicos.

2) *Reducción del grado de* $\alpha \in \Sigma$.

Sea d el grado maximal sobre $\mathbb{Q}$ de los elementos de Σ, escogemos $\alpha \in \Sigma$ de grado d. El número algebraico α es raíz de un polinomio $m(x)$ de grado d con coeficientes racionales.

Definimos la transformación

$$m : P^1 \longrightarrow P^1$$
$$m : (x_0, x_1) \longmapsto \Big(x_1^d \cdot m\Big(\frac{x_0}{x_1}\Big) : x_1^d\Big),$$

la cual es ramificada en ∞ y en todo punto x en el cual la derivada $m'(x)$ se anula.

Consideremos el conjunto

$$\Sigma' = m(\sigma) \cup \{m(x) : m'(x) = 0\} \cup \{\infty\}.$$

Ahora bien, $m(\alpha) = 0$, y para todo $\beta \in \Sigma$, el grado de $m(\beta)$ es a lo más el grado de β ; además, dado que m' tiene grado $d-1$, $m(x)$ tiene grado a lo más $d-1$ sobre $\mathbb{Q}$ para una raíz x de m'.

Por lo tanto, Σ' contiene menos elementos de grado d que Σ.

Repitiendo este paso, eventualmente Σ contendrá sólo puntos racionales. Podemos entonces asumir que $\{0, 1, \infty\} \subseteq \Sigma$. A saber, si $a \in \Sigma$ entonces la transformación $z \longmapsto z/a$ es ramificada y transforma a en ∞ ; luego, si $\{a, 0, \infty\} \subseteq \Sigma$, $z \longmapsto z/a$ es ramificado y transforma a, 0, ∞ en 1, 0, ∞.

3) *Reducción del número de elementos de* Σ.

Supongamos que Σ contiene a 0, 1 y ∞, y a un cuarto punto a/c tal que $a, c \neq 0$ y $a \neq c$. Consideremos la función

$$\varphi(x) = \lambda x^a (1-x)^{c-a}.$$

Esta transformación es posiblemente ramificada en 0, 1, ∞ y en puntos x en los cuales $\varphi'(x) = 0$.

Además, $\varphi(x) = 0$ o ∞ sólo cuando $x = 0, 1$ o ∞. De manera que, para $x \neq 0, 1, \infty$, $\varphi'(x) = 0$ si y sólo si $\frac{\varphi'(x)}{\varphi(x)} = 0$.

Por otro lado,

$$\frac{\varphi'(x)}{\varphi(x)} = \frac{a}{x} - \frac{c-a}{1-x},$$

entonces, $\varphi'(x) = 0$ si $x = a/c$.

Escogiendo λ de tal manera que $\varphi(c/a) = 1$, φ solamente es ramificada en 0, 1 y ∞, y dado que $\varphi\big(\{0, 1, \infty\}\big) = \{0, \infty\}$ entonces, $\varphi(\Sigma)$ contiene

menos elementos que Σ. Repitiendo este último paso, eventualmente, Σ sólo contendrá a 0, 1 y ∞.

3.7. Teorema de Roth. En 1955, KLAUS F. ROTH probó el siguiente teorema:

Teorema 3.7 (Teorema de Roth)**.** *Sea α algebraico sobre $\mathbb{Q}$ y $\epsilon > 0$. Entonces*

$$\left|\alpha - \frac{s}{t}\right| < \frac{1}{t^{2+\epsilon}}$$

solamente para un número finito de números racionales s/t.

Definamos la altura de $x = s/t$ donde $s, t \in \mathbb{Z}$ son primos relativos, como:

$$h(x) = \text{máx}\{\log|s|, \log|t|\}.$$

Dada una valuación ω de $\mathbb{Q}$ y un número algebraico α, extendemos ω a una valuación de $\mathbb{Q}(\alpha)$, y consideramos la función

$$\lambda_\omega(x, \alpha) = \text{máx}\big(0, -\omega(x-\alpha)\big)$$
$$\lambda_\omega(x, \infty) = \text{máx}\big(0, \omega(x)\big),$$

con ella formulamos la siguiente generalización del teorema de Roth:

Teorema 3.8 (Generalización del teorema de Roth)**.** *Sean $\epsilon > 0$ y S un conjunto de valuaciones de $\mathbb{Q}$. Para cada $\omega \in S$ definimos α_ω como un número algebraico o ∞, y extendemos ω a una valuación de $\mathbb{Q}(\alpha\omega)$. Entonces existe una constante k tal que:*

$$\sum_{\omega \in S} \lambda_\omega(x, \alpha_\omega) \leq 2h(x) + \epsilon h(x) + k \tag{30}$$

para todo $x \in \mathbb{Q}$.

En los años sesenta LANG conjeturó que el teorema de Roth podía ser mejorado a $-\log|\alpha - p/q| - 2\log q \leq (1+\epsilon)\log\log q$, ver [23, pág. 214]. Sin embargo, la forma más fuerte posible de la conjetura *abc* solo conduce a

$$-\log\left|\alpha - \frac{p}{q}\right| - 2\log q \leq k \cdot \frac{\sqrt{\log q}}{\log\log q},$$

para alguna constante k que depende sólo de α.

Teorema 3.9. *La conjetura abc en la forma (23) implica que existen constantes k y d tales que (30) es satisfecha por todo $x \in \mathbb{Q}$, reemplazando $\epsilon\big(h(x)\big) + k$ por $\psi\big(d \cdot h(x)\big) + k$.*

Demostración. Sea $f : P^1 \longrightarrow P^1$ la transformación de Belyĭ asociada a $C = P^1$, y $\Sigma = \{(\alpha_\omega : 1) : \omega \in S\}$. Como f es una función racional definida sobre $\mathbb{Q}$, la podemos considerar como un cociente de polinomios homogéneos, primos relativos, y con coeficientes enteros:

$$f(x_0 : x_1) = \big(a(x_0, x_1) : c(x_0, x_1)\big)$$

donde $a, c \in \mathbb{Z}[x_0, x_1]$ son polinomios homogéneos de grado $d = \text{grad}(f)$.

Sea $b(x_0, x_1) = c(x_0, x_1) - a(x_0, x_1)$. Consideramos los polinomios a, b y c como producto de factores homogéneos irreducibles en $\mathbb{Z}[x_0, x_1]$,

$$\begin{aligned} a(x_0, x_1) &= m_1^{e_1}(x_0, x_1) \cdot \cdots \cdot m_i^{e_i}(x_0, x_1), \\ b(x_0, x_1) &= m_{i+1}^{e_{i+1}}(x_0, x_1) \cdot \cdots \cdot m_j^{e_j}(x_0, x_1), \\ c(x_0, x_1) &= m_{j+1}^{e_{j+1}}(x_0, x_1) \cdot \cdots \cdot m_k^{e_k}(x_0, x_1). \end{aligned}$$

Si $d_v = \text{grad}(m_v)$ entonces,

$$\#f^{-1}\{0\} = \sum_{v=1}^{i} d_v, \qquad \#f^{-1}\{1\} = \sum_{v=i+1}^{j} d_v, \qquad \#f^{-1}\{\infty\} = \sum_{v=j+1}^{k} d_v\,;$$

por lo tanto,

$$\sum_{v=1}^{k} d_v = \#f^{-1}\{0, 1, \infty\}.$$

Por (29): $\#f^{-1}\{0, 1, \infty = \text{grad}\,(f) + 2 - 2\,\text{g}\,(C)$, pero dado que C en este caso es P^1 entonces, $\text{g}(C) = 0$, y por lo tanto:

$$\sum_{v=1}^{k} d_v = d + 2. \tag{31}$$

Ahora bien, como para cada $\omega \in S$, $f(\alpha_\omega) = 0$, 1 o ∞ (pues, por f una transformación de Belyĭ $f(\Sigma) \subseteq \{0, 1, \infty\}$), el punto α_ω es una raíz de uno de los factores irreducibles m_v, es decir, para algún μ $(1 \leq \mu \leq k)$ $m_\mu(\alpha_{\omega,1}) = 0$ o, $m_\mu(1, 0) = 0$ si $\alpha_\omega = \infty$.

Dado que los polinomios m_v son primos relativos, este m_μ es único.

En adelante, si $\omega = \nu_p$ o $\omega = \nu_\infty$ es una valuación específica, escribiremos α_p o α_∞ en lugar de α_ω.

Sea $x \in P^1(\mathbb{Q})$ un punto tal que $f(x) \neq 0, 1, \infty$. Tomamos $x = (s : t)$ con $s, t \in \mathbb{Z}$ primos relativos, y aplicamos la conjetura *abc* al punto:

$$P = \big(f(x) : 1 - f(x) : 1\big) = \big(a(s, t) : b(s, t) : c(s, t)\big).$$

De acuerdo con las desigualdades (25) y (26), existe una constante k_0 tal que

$$h(P) > h\big(f(x)\big) \geq dh(x) - k_0; \tag{32}$$

y para el radical de P :

$$r(P) = \sum_{p:\#\{\nu_p(a),\nu_p(b),\nu_p(c)\}\geq 2} \log p,$$

dado que $a(s,t)$, $b(s,t)$ y $c(t)$ son primos relativos, entonces

$$\begin{aligned} r(p) &\leq \sum_{p|a(s,t)\cdot b(s,t)\cdot c(s,t)} \log p \\ &= \sum_{p|m_i(s,t)\cdot\cdots\cdot m_k(s,t)} \log p. \end{aligned} \tag{33}$$

Si S contiene sólo la valuación ν_∞ podemos continuar de la siguiente manera.

Por (33),

$$\begin{aligned} r(P) &\leq \sum_{v=1}^{k} \log |m_v(s,t)| \\ &\leq \sum_{v=1}^{k} d_v h(x) - \lambda_\infty(x,\alpha_\infty) + K \end{aligned} \tag{34}$$

para alguna constante K. Esta última desigualdad es consecuencia del Lema 3.5 (véase la página 51 más adelante).

Por (31), (32) y (34), obtenemos

$$\begin{aligned} \lambda_\infty(x,\alpha_\infty) &\leq \sum_{v=1}^{k} d_v h(x) - r(P) + K \\ &= (d+2)h(x) - r(P) + K \\ &= 2\cdot h(x) + K + \big(dh(x) - r(P)\big) \end{aligned}$$

y por la conjetura *abc* en la forma (23),

$$\text{máx}\,(dh(P) - r(P), 0) \leq \psi\big(dh(x)\big)$$

por lo tanto,

$$\lambda_\infty(x,\alpha_\infty) \leq 2\cdot h(x) + K + \psi\big(dh(x)\big),$$

y esto implica el Teorema 3.7.

Consideremos ahora el caso en que S contenga más valuaciones.

Por (33), si un primo p contribuye con $\log p$ al radical de P entonces, $p|m_\mu(s,t)$ para algún μ entre 1 y k.

Esta contribución está acotada por $-\nu_p\big(m_\mu(s,t)\big)$.

Si $\nu_p \in S$ y α_p es una raíz de m_μ, aplicamos el caso (ii) del Lema 3.5 (página (51)) para conseguir una mejor cota para la contribuciíon de p al radical,

$$\log p \leq -\nu_p\big(m_v(s,t)\big) - \lambda_p(x,\alpha_p) + K_p\,,$$

donde K_p es una constante.

De esta manera, la contribución de ν_p al radical está acotada por

$$\sum_{v=1}^{k} -\nu_p\big(m_v(s,t)\big), \qquad \text{si } \nu_p \notin S$$

y por

$$\left(\sum_{v=1}^{k} -\nu_p\big(m_v(s,t)\big)\right) - \lambda_p(x-\alpha_p) + K_p, \qquad \text{si } \nu_p \in S.$$

Sumando todas las contribuciones, obtenemos, por la Proposición 3.1:

$$r(P) \leq \sum_{v=1}^{k} \log|m_v(s,t)| - \sum_{\omega\in S,\ \text{finito}} \lambda_\omega(x,\alpha_\omega) + \sum_{\omega\in S,\text{finito}} K_\omega,$$

y concluimos (como en (34)) que:

$$r(P) \leq \sum_{v=1}^{k} d_v h(x) - \sum_{\omega\in S} \lambda_\omega(x,\alpha_\omega) + K \tag{35}$$

para alguna constante K.

Finalmente, combinando (35), (31) y (32), por la conjetura *abc* (en la forma (23)) obtenemos:

$$\sum_{\omega\in S} \lambda_\omega(x,\alpha_\omega) \leq 2\cdot h(x) + K + \psi\big(dh(x)\big),$$

y ésto concluye la prueba. ☑

Lema 3.5. *Sea α algebraico sobre $\mathbb{Q}$ de grado d, o $\alpha=\infty$, en cuyo caso $d=1$. Sea $m(x_0,x_1)\in\mathbb{Z}[x_0,x_1]$ el polinomio minimal homogéneo tal que $m(\alpha,1)=0$ (o $m(x_0,x_1)=x_1$, si $\alpha=0$). Sea ω una valuación de $\mathbb{Q}$ que extendemos a una valuación de $\mathbb{Q}(\alpha)$. Entonces, existe una constante K tal que, para todo $x=s/t\in\mathbb{Q}$, con s y t son primos relativos:*

I) *Si $\omega=\nu_\infty$,*

$$\nu_\omega\big(m(s,t)\big) \leq dh(x) - \lambda(x,\alpha) + K.$$

II) *Si $\omega=\nu_p$,*

$$\nu_p\big(m(s,t)\big) \leq -\lambda_p(x,\alpha) + K.$$

Demostración. Si $\alpha=\infty$, el resultado se sigue directamente de la definición de las valuaciones y de λ_ω. La demostración en el caso $\alpha\neq\infty$ se encuentra en [52, pág. 64].

3.8. Conjetura de Mordell. En 1922, Louis J. Mordell hizo la siguiente conjetura, ver [33],

Conjetura 5 (Conjetura de Mordell)**.** *Si C es una curva algebraica definida sobre $\mathbb{Q}$ de género $g \leq 2$, entonces $C(\mathbb{Q})$ es finito.*

La conjetura de Mordell fue probada por Gerd Faltings en 1983 [10]. En 1991, Paul Vojta presentó una prueba usando aproximación diofántica (véase [3, 11, 54]). Pero, tal como Vojta afirmó en [54], las demostraciones conocidas de esta conjetura son ineficaces, en el sentido, que dada una curva algebraica, se puede obtener una cota superior explícita para el número de puntos en $C(\mathbb{Q})$, pero no para su altura. Tal demostración es posible a partir de la conjetura *abc*.

La conjetura *abc* **implica Mordell eficaz**. Usando la conjetura *abc*, obtenemos un algoritmo para encontrar puntos de $C(\mathbb{Q})$ como sigue:

i) Se construye un transformación especial $f : C \longrightarrow P^1$;
ii) Entonces para todo punto $x \in C(\mathbb{Q})$, la altura de $f(x)$ está acotada por una constante explícita o $f(x) = 0$, 1 o ∞.

La demostración y algunas nociones adicionales a las que hemos dado pueden ser consultada en [52, pág. 64–69].

4. Conjeturas equivalentes a la conjetura abc

4.1. Formulación de Oesterlé de la conjetura abc. Bajo hipótesis apropiadas, Oesterlé consideró

$$L = L(a, b, c) = \frac{\log \text{máx}\,(|a|, |b|, |c|)}{\log \text{rad}\,(abc)} = \frac{\log c}{\log \text{rad}\,(abc)}$$

y se preguntó si L tenía una cota.

Teorema 4.1. *La conjetura abc se sigue si y sólo si* $\limsup\{L\} \leq 1$.

Demostración.
($\Rightarrow$) Sea $\epsilon > 0$, y a, b, c enteros positivos tales que $a+b = c$ y m. c. d. $(a, b, c) = 1$. Por la conjetura *abc* tenemos que:

$$\begin{aligned} L(a, b, c) = \frac{\log \text{máx}(|a|, |b|, |c|)}{\log \text{rad}(abc)} &\leq \frac{\log\big(k_\epsilon \cdot (\text{rad}\, abc)^{1+\epsilon}\big)}{\log \text{rad}\,(abc)} \\ &= \frac{\log k_\epsilon}{\log \text{rad}\,(abc)} + (1 + \epsilon). \end{aligned}$$

Fijemos ϵ y pongamos $k = k_\epsilon$. Lo que queremos conseguir es

$$\frac{\log k}{\log \text{rad}\,(abc)} \leq \epsilon$$

para todas excepto un número finito de triplas (a, b, c). Esta desigualdad es equivalente a la siguiente,

$$\log \operatorname{rad}(abc) \geq \frac{\log k}{\epsilon},$$

que a su vez, se tiene si y sólo si

$$\operatorname{rad}(abc) \geq M := e^{\log k/\epsilon}. \tag{36}$$

Y (36) se cumple, dado que por las hipótesis de la conjetura *abc*, existe sólo un número finito de triplas (a, b, c) tales que $\operatorname{rad}(abc) \leq M$.

($\Leftarrow$) Supongamos que $\lim\sup\{L\} \leq 1$. Es decir, supongamos que

$$\lim\sup\left(\frac{\log c_n}{\log \operatorname{rad}(a_n \cdot b_n \cdot c_n)}\right) \leq 1.$$

Tenemos entonces que, dado $\epsilon > 0$,

$$\frac{\log c_n}{\log \operatorname{rad}(a_n \cdot b_n \cdot c_n)} \leq 1 + \epsilon$$

para n suficientemente grande.

Por lo tanto, para $n \geq N$, donde N es un entero fijo:

$$c_n \leq \big(\operatorname{rad}(a_n \cdot b_n \cdot c_n)\big)^{1+\epsilon}.$$

Buscamos constantes $\mu_1(\epsilon), \mu_2(\epsilon), \ldots, \mu_N(\epsilon)$ tales que

$$c_i \leq \mu_i(\epsilon) \cdot \big(\operatorname{rad}(a_i \cdot b_i \cdot c_i)\big)^{1+\epsilon}$$

para todo $i = 1, \ldots, N$.

Sea $\mu(\epsilon) = \text{máx}_{1 \leq i \leq N}\big(\mu_i(\epsilon)\big)$, entonces

$$c_n \leq \mu(\epsilon) \cdot \big(\operatorname{rad}(a_n \cdot b_n \cdot c_n)\big)^{1+\epsilon}$$

para todo n. ☑

Recordemos un ejemplo dado en la sección 2, en el cual pusimos

$$a_n = 3^{2^n} - 1, \qquad b_n = 1 \quad \text{y} \qquad c_n = 3^{2^n};$$

para estos valores:

$$\begin{aligned} L_n &= \frac{\log 3^{2^n}}{\log \mathrm{rad}\big((3^{2^n}-1)\cdot 1\cdot 3^{2^n}\big)}\,\frac{\log 3^{2^n}}{\log 3+\log \mathrm{rad}\,(3^{2^n}-1)} \\ &\geq \frac{\log 3^{2^n}}{\log 3+\log\left(2\cdot \mathrm{rad}\left(\frac{3^{2^n}-1}{2^n}\right)\right)} \\ &\geq \frac{2^n\cdot \log 3}{\log 3+\log 2+\log\,(3^{2^n}-1)-\log 2^n}. \end{aligned}$$

Por lo tanto,

$$L_n \geq \frac{2^n\cdot \log 3}{\log 3+\log(3^{2^n}-1)-(n-1)\log 2}. \tag{37}$$

y para $n=3$

$$L_3 \geq \frac{8\cdot \log 3}{\log 3+\log(3^8-1)-2\log 2}\,;$$

en particular, tenemos $L_3>1$.

Observemos que el cociente de la desigualdad (37) crece cuando n llega a ser suficientemente grande. Por lo tanto, existen infinitas triplas (a_n,b_n,c_n) tales que $L_n>1$. Con esto hemos mostrado:

Teorema 4.2. *La conjetura abc es verdadera si y sólo si* $\lim\sup\{L\}=1$.

4.2. Conjetura abc en Congruencias. Entenderemos por (a,b,c), una tripla de enteros que satisfacen $a+b+c=0$ y $\mathrm{m.\,c.\,d.}\,(a,b,c)=1$.

Oesterlé en [38] observa que si la conjetura *abc* se cumple para toda tripla (a,b,c) para la cual $16|abc$ entonces, la conjetura *abc* es cierta para toda tripla (a,b,c).

Este resultado se puede extender mostrando que si para algún entero N (≥ 2) la conjetura *abc* en congruencias (*vide infra*) es cierta para cada tripla (a,b,c) tal que $N|abc$ entonces la conjetura *abc* se sigue.

La demostración de este hecho se debe a Jordan S. Ellenberg.

Para nuestros propósitos, una *abc–solución* s, es una tripla (a,b,c) de enteros distintos y tal que a y b sean enteros negativos.

Si $n>0$ es un entero, para cada $\epsilon>0$ definimos la siguiente función

$$f(s,\epsilon)=\log(c)-(1+\epsilon)\log \mathrm{rad}\,(abc);$$

entonces la conjetura *abc* puede enunciarse de la siguiente manera:

Conjetura 6. *Para cada* $\epsilon>0$, *existe una constante* C_ϵ *tal que para cada* s, $f(s,\epsilon)<C_\epsilon$.

Esta conjetura es evidentemente equivalente a la Conjetura 1 (la constante k_ϵ sería una constante k'_ϵ que depende de C_ϵ).

Conjetura 7 (Conjetura *abc* en congruencia para N)**.** *Sea N un entero (≥ 2). Para cada $\epsilon > 0$ existe una constante $C_{N,\epsilon}$ para la cual, $f(s,\epsilon) < C_{N,\epsilon}$ para toda solución s tal que $N|abc$.*

Este enunciado es más débil que el de la conjetura *abc*, ya que está restringido por una condición de congruencia ($abc \equiv 0 \pmod N$). Sin embargo, probaremos que si la conjetura en congruencias es cierta para algún N, entonces la conjetura *abc* sin restricciones es también verdadera.

Teorema 4.3. *Sea $N \geq 2$. Si la conjetura abc en congruencia es verdadera para N, entonces la conjetura abc es verdadera.*

Demostración. Para cada entero positivo par n definimos Θ_n sobre las *abc*–soluciones como sigue,

$$\Theta_n(s) = (-2^{-m}(a-b)^n, -2^{-m}\big(c^n - (a-b)^n\big), 2^{-m}c^n),$$

donde

$$\begin{cases} m = n, & \text{si } c \text{ es par,} \\ m = 0, & \text{en otro caso.} \end{cases}$$

Veamos que $\Theta_n(s)$ es nuevamente una *abc*–solución. Sea

$$\begin{aligned} A &= -2^{-m}(a-b)^n, \\ B &= -2^{-m}\big(c^n - (a-b)^n\big) \qquad \text{y} \\ C &= 2^{-m}c^n. \end{aligned}$$

Entonces

$$\begin{aligned} A + B + C &= -2^{-m}\big((a-b)^n + c^n - (a-b)^n - c^n\big) \\ &= 0. \end{aligned}$$

Si c es par,

$$\begin{aligned} A &= -\left(\frac{a-b}{2}\right)^n, \\ B &= -\frac{c^n - (a-b)^n}{2^n}, \\ C &= \left(\frac{c}{2}\right)^n; \end{aligned}$$

por ser c un número par, a y b deben ser impares, puesto que $\text{m. c. d.}\,(a,b,c) = 1$; por lo tanto, $a - b$ es par, luego $A, C \in \mathbb{Z}$ y, por consiguiente, también $B \in \mathbb{Z}$. En este caso $\text{m. c. d.}\,(A,B,C) = 1$, pues si $d\big|(c/2)$ y $d\big|(a-b)/2$ entonces $d\big|\big((a-b)/2 + (a+b)/2\big)$, es decir, d es divisor común para c y a, pero como $\text{m. c. d.}\,(a,b,c) = 1$ y $a + b + c = 0$, entonces $d = 1$.

Ahora bien, si c es impar,

$$\begin{aligned} A &= -(a-b)^n, \\ B &= (a-b)^n - c^n, \\ C &= c^n; \end{aligned}$$

y es obvio que, A, B y C son enteros y $\mathrm{m.\,c.\,d.}\,(A,B,C)=1$.

Lema 4.1. *Existen constantes $c_{n,\epsilon}>0$ y $c'_{n,\epsilon}$ tales que,*

$$f\left(\Theta_n(s), \frac{\epsilon}{n+(n+1)\epsilon}\right) \geq c_{n,\epsilon} f(s,\epsilon) + c'_{n,\epsilon}.$$

Demostración. Como $\Theta_n(s)$ es una *abc*–solución podemos aplicarle f; conservando la notación introducida anteriormente, tenemos que

$$f\left(\Theta_n(s), \frac{\epsilon}{n+(n+1)\epsilon}\right) = \log(2^{-m}\cdot c^n) - \left(1+\frac{\epsilon}{n+(n+1)\epsilon}\right)\cdot \log \mathrm{rad}\,(ABC),$$

$$\log \mathrm{rad}(ABC) \leq \log\left(|a-b|\cdot \mathrm{rad}\,(abc)\cdot \mathrm{rad}\left(\frac{B}{ab}\right)\right),$$

Además

$$\begin{aligned} \frac{B}{ab} &= \frac{(a+b)^n-(a-b)^n}{ab} \\ &= 2b\cdot \frac{(a+b)^{n-1}+(a+b)^{n-2}(a-b)+\cdots+(a-b)^{n-1}}{ab} \\ &= 2\cdot \frac{2a\cdot\left((a+b)^{n-2}+(a+b)^{n-4}(a-b)^2+\cdots+(a-b)^{n-2}\right)}{a} \end{aligned}$$

(nótese que en este último paso hemos usado que n es un número par)

$$\begin{aligned} &= 2\cdot 2\cdot\left((a+b)^{n-2}+(a+b)^{n-4}(a-b)^2+\cdots+(a-b)^{n-2}\right) \\ &\leq 2\cdot 2\cdot \frac{n}{2}\cdot (a+b)^{n-2} \end{aligned}$$

(pues como a y b tienen el mismo signo, entonces, $|a+b|\geq|a-b|$, y por lo tanto $(a+b)^2\geq(a-b)^2$)

$$\begin{aligned} &= 2n\cdot(a+b)^{n-2} \\ &= 2n\cdot c^{n-2}. \end{aligned}$$

De acuerdo con esto tenemos que:

$$\begin{aligned}\log \operatorname{rad}(ABC) &\leq \log|a-b| + \log \operatorname{rad}(abc) + \log(2n \cdot c^{n-2}) \\ &\leq \log c + \log \operatorname{rad}(abc) + (n+2)\cdot \log c + \log 2n \\ &= (n-1)\cdot \log c + \log \operatorname{rad}(abc) + \log 2n \\ &= (n-1)\cdot \log c + \frac{\log c - f(s,\epsilon)}{1+\epsilon} + \log 2n \\ &= (n-1)\cdot \log c + (1+\epsilon)^{-1}\cdot \log c - (1+\epsilon)^{-1} f(s,\epsilon) + \log 2n.\end{aligned}$$

Como $C = c^n/2^m$ entonces, $\log C = n\cdot \log c - m\cdot \log 2$ y, por lo tanto,

$$\begin{aligned}\log \operatorname{rad}(ABC) &\leq \log C + m\cdot \log 2 - \log c + (1+\epsilon)^{-1}\cdot \log c \\ &\qquad -(1+\epsilon)^{-1} f(s,\epsilon) + \log 2n \\ &= \big(1 - \epsilon\big(n(1+\epsilon)\big)^{-1}\big)\cdot (\log C + m\cdot \log 2) - (1+\epsilon)^{-1} f(s,\epsilon) + \log 2n.\end{aligned}$$

Entonces,

$$\frac{\log \operatorname{rad}(ABC) + (1+\epsilon)^{-1} f(s,\epsilon) - \log 2n}{1 - \epsilon\big(n(1+\epsilon)\big)^{-1}} - m\cdot \log 2 \leq \log C$$

y, por lo tanto,

$$\begin{aligned}f\left(\Theta_n(s), \frac{\epsilon}{n+(n-1)\epsilon}\right) &\geq \frac{\log \operatorname{rad}(ABC) + (1+\epsilon)^{-1} f(s,\epsilon) - \log 2n}{1 - \epsilon\big(n(1+\epsilon)\big)^{-1}} \\ &\qquad - m\log 2 - \left(1 + \frac{\epsilon}{n+(n+1)\epsilon}\right)\cdot \log \operatorname{rad}(ABC).\end{aligned}$$

Tomando

$$c_{n,\epsilon} = \frac{(1+\epsilon)^{-1}}{1 - \epsilon\big(n(1+\epsilon)\big)^{-1}} = \frac{n}{n(1+\epsilon) - \epsilon}$$

y

$$\begin{aligned}c'_{n,\epsilon} &= \frac{n(\epsilon+1)}{n+\epsilon n+\epsilon}\cdot \log \operatorname{rad}(ABC) - \frac{n(1+\epsilon)}{n+\epsilon n+1}\cdot \log 2n \\ &\qquad - m\cdot \log 2 - \frac{n(\epsilon+1)}{n+\epsilon n+\epsilon}\cdot \log \operatorname{rad}(ABC) \\ &= -\frac{n(1+\epsilon)}{n+\epsilon n+1}\cdot \log 2n - m\cdot \log 2,\end{aligned}$$

obtenemos el resultado que se buscaba. ☑

Continuando con la demostración del teorema, si la conjetura *abc* en congruencia es verdadera para N, existe una constante $C_{N,\epsilon}$ tal que $f(s,\epsilon) < C_{N,\epsilon}$ para cada *abc*–solución s tal que $N|abc$.

Si aplicamos la función ϕ de Euler a $N = p_1^{a_1} \cdot p_2^{a_2} \cdots p_l^{a_l}$, sea

$$n = \phi(N) = N \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_l}\right).$$

Observemos que si $N = 2$ el teorema es trivial pues, dado que $a + b + c = 0$ al menos uno de los tres es par. Así que en adelante, consideraremos $N > 2$.

Lema 4.2. *Si $N > 2$ y $(A, B, C) = \Theta_n(s)$ entonces $N|ABC$.*

Demostración. Sea p un primo que divide a N tal que $\operatorname{ord}_p N = v$. Entonces $\phi(p^v) = (p-1)p^{v-1}|n$ y, $v < n$ (ya que $v \leq \frac{\log n}{\log p} < n$).

Supongamos inicialmente que p es impar. Siguiendo con la notación establecida al comienzo de la demostración del teorema:

Si $p|c$, dado que p es un primo impar entonces $p^n|C$, y de manera semejante, si $p|(a-b)$ entonces $p^n|A$. Es decir, si p es divisor de alguno de los dos, de c o de $a - b$ entonces,

$$p^n|ABC;$$

y como $v < n$ entonces,

$$p^v|ABC.$$

En el caso en que $p \nmid c$ y $p \nmid (a-b)$ tenemos $(c, p^v) = (a-b, p^v) = 1$. Aplicando el teorema de Euler,

$$c^{\phi(p^v)} \equiv 1 \pmod{p^v} \qquad \text{y} \qquad (a-b)^{\phi(p^v)} \equiv 1 \pmod{p^v},$$

como $\phi(p^v)|n$ entonces,

$$c^n \equiv 1 \pmod{p^v} \qquad \text{y} \qquad (a-b)^n \equiv 1 \pmod{p^v},$$

por lo tanto

$$c^n - (a-b)^n \equiv 0 \pmod{p^v}$$

y dado que p es impar, lo anterior implica que

$$p^v|B$$

y como consecuencia

$$p^v|ABC.$$

Ahora consideremos el caso $p = 2$. Sea $\operatorname{ord}_2(N) = r$. Si c es par, dado que $a+b+c = 0$, entonces $a+b$ y $a-b$ son enteros pares, exactamente uno de ellos múltiplo de 4 (pues si $a+b = 2k$ y $a-b = 2k'$ $(k, k' \in \mathbb{Z})$, $2a = 2(k+k')$ y como $\text{m. c. d.}\,(a, b, c) = 1$ entonces k y k' no pueden tener la misma paridad). Por lo tanto, exactamente uno de los dos c^n o $(a-b)^n$ es múltiplo de 4^n, es decir, sólo uno de los dos $A = -(a-b)^n/2^n$ o $C = c^n/2^n$ es múltiplo de 2^n. Y como $r < n$, aquel que sea múltiplo de 2^n también lo es de 2^r, entonces $2^r|ABC$. Si c es impar, también $a + b$ y $a - b$ son impares, luego, c^n y $(a-b)^n$ son ambos congruentes a 1 módulo 2^n, es decir

$$(a-b)^n \equiv c^n \pmod{2^n},$$

lo que significa que $2^n|B$ y por lo tanto que $2^r|B$. Esto último implica que

$$2^r|ABC.$$

De acuerdo con todo lo anterior tenemos entonces, que todo divisor de N divide al producto ABC, es decir, $N|ABC$.

Sea $\epsilon > 0$ y s una *abc*–solución. Por la conjetura *abc* en congruencia para N, existe una constante $C_{N,\epsilon}$ tal que para cada n

$$f(\Theta_n(s), \epsilon) < C_{N,\epsilon}.$$

De acuerdo con el Lema 4.1, existen constantes $c'_{n,\epsilon}$ y $c_{n,\epsilon}$ para las cuales

$$f(s,\epsilon) \leq \frac{f\left(\Theta_n(s), \frac{\epsilon}{n+(n-1)\epsilon}\right) - c'_{n,\epsilon}}{c_{n,\epsilon}} < \frac{C_{N,\epsilon'} - c'_{n,\epsilon}}{c_{n,\epsilon}}$$

donde $\epsilon' = \dfrac{\epsilon}{n+(n-1)\epsilon}$.

Dado que ninguna de las constantes $C_{N,\epsilon'}$, $c'_{n,\epsilon}$, $c_{n,\epsilon}$ que aparecen en la desigualdad anterior depende de la *abc*–solución, podemos decir entonces que:

Para cada $\epsilon > 0$ existe una constante k_ϵ tal que, para cada *abc*–solución, $f(s,\epsilon) < k_\epsilon$. Y ésta es precisamente la conjetura *abc*.

El recíproco del teorema anterior se cumple trivialmente. Por lo tanto, la conjetura *abc* es equivalente a la conjetura *abc* en congruencia para N ($N \geq 2$).

4.3. Conjetura de Szpiro. Sea K un cuerpo y $F(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ un polinomio homogéneo de grado d. Se dice que la ecuación

$$F(x_0, x_1, x_2) = 0$$

define una curva de grado d sobre K si L es un cuerpo que contiene a K uno puede considerar los ceros de F en $P^2(L)$ (el espacio proyectivo bidimensional) que son precisamente los puntos en la hipersuperficie $\overline{H}_F(L)$ definida por F en $P^2(L)$, esto es, $\overline{H}_F(L) = \{[a] \in P^n(K) : F(a) = 0\}$. Una hipersuperficie en el espacio proyectivo bidimensional es llamada una *curva*.

Un punto $a \in \overline{H}_F(L)$ es un *punto no singular*, si no es solución simultánea a las ecuaciones

$$\frac{\partial F}{\partial x_0} = 0, \qquad \frac{\partial F}{\partial x_1} = 0, \qquad \frac{\partial F}{\partial x_2} = 0.$$

En este caso, la recta

$$0 = \frac{\partial F}{\partial x_o}(a)x_0 + \frac{\partial F}{\partial x_1}(a)x_1 + \frac{\partial F}{\partial x_2}(a)x_2$$

es llamada la *recta tangente a F en a*. Se dice que la curva $F(x_0, x_1, x_2)$ es no singular si, para toda extensión L de K, todos los puntos en $\overline{H}_F(L)$ son no singulares.

Si F está definida sobre K, un cero de F en $P^2(K)$ se dice que es un punto racional sobre K.

Diremos que un polinomio cúbico homogéneo no singular

$$F(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$$

define una *curva elíptica* sobre K si tiene un punto racional sobre K.

La razón por la cual se le da este nombre proviene del hecho de que las coordenadas de sus puntos pueden expresarse en términos de un parámetro elíptico u valiéndose de la función de Weierstrass.

Si $F(x_0, x_1, x_2)$ define una curva elíptica sobre K y L es un cuerpo de extensión de K notamos $\overline{H}_F(L)$ como $E(L)$.

Si la característica del cuerpo K no es 2 ni 3 se puede mostrar que una curva elíptica sobre K puede ser transformada en una de la forma

$$x_0x_2^2 = x_1^3 - Ax_0^2x_1 - Bx_0^3, \quad A, B \in K. \tag{38}$$

Esta curva tiene exactamente un punto en el infinito, a saber $(0, 0, 1)$. Si $x_0 \neq 0$ sea $x = x_1/x_0$ y $y = x_2/x_0$. Entonces, en coordenadas afines la ecuación de la curva es

$$y^2 = x^3 - Ax - B. \tag{39}$$

La no singularidad de

$$F(x_0, x_1, x_2) = x_0x_2^2 - x_1^3 + Ax_0^2x_1 + Bx_0^3$$

es equivalente a que

$$\Delta = 16(4A^3 - 27B^2) \neq 0.$$

Recíprocamente, si $\Delta \neq 0$, entonces F define una curva elíptica.

Por medio de las llamadas *transformaciones birracionales* que consisten en cambios de variables del tipo

$$\begin{aligned} x &= \varphi(z, u), & y &= \psi(z, u); \\ z &= \Phi(x, y), & u &= \Psi(x, y); \end{aligned}$$

donde $\varphi, \psi, \Phi, \Psi$ son funciones racionales, se establece una correspondencia biunívoca entre los puntos de las curvas

$$f(x, y) = 0 \qquad \text{y} \qquad f(z, u) = f\big(\varphi(z, u), \psi(z, u)\big) = 0,$$

salvo un número finito puntos.

Mediante una transformación birracional, de una curva a otra, puede cambiar el grado de la ecuación o su forma, pero hay algo que no varía, el número positivo llamado el género g de la curva. Este hecho es un conocido teorema de Riemann [56, 185-190].

En el caso de las curvas de tercer grado es posible caracterizar aquellas que tienen géneros 0 y 1.

Si la curva $f(x, y) = 0$ tiene un punto singular, la curva es de género 0. En el caso contrario, la curva es de género 1.

Siendo $F(x_0, x_1, x_2)$ un polinomio homogéneo de grado d, consideramos la ecuación correspondiente en coordenadas afines $f(x, y) = F(1, x, y)$. Para encontrar los puntos de intersección de $f(x, y)$ con la recta $y = mx+b$ simplemente sustituimos y y encontramos las soluciones de $f(x, mx + b) = 0$. Dado que F tiene grado d esta última ecuación generalmente tiene grado d, Si estamos en un cuerpo algebraicamente cerrado L habrán d raíces contando multiplicidades. Las únicas excepciones serán las intersecciones en el infinito, en cuyo caso $f(x, mx + b)$ tendrá grado menor que d. En el caso particular de las curvas elípticas, si $P_1, P_2 \in E(L)$ entonces la recta que une P_1 y P_2 intersecta la curva en un tercer punto P_3 unívocamente determinado que también pertenece a $E(L)$. Si $P_1 = P_2$ entonces la recta tangente en P_1 da lugar a un tercer punto P_3. Este procedimiento para encontrar puntos racionales sobre curvas elípticas debido a Bachet, sugiere la posibilidad de que todos los puntos racionales de la cúbica $f(x, y) = y^2 - x^3 + Ax + B$ se obtienen de esta forma.

Supongamos ahora, $K = \mathbb{Q}$. En 1922, intentando demostrar el hecho anterior, Mordell demostró el siguiente teorema, conjeturado por Poincaré en 1901[10].

Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.

Con otras palabras, Mordell demostró que sobre una curva elíptica E definida sobre $\mathbb{Q}$, existen puntos $P_1, \ldots, P_r$ a partir de los cuales se obtienen todos los puntos racionales de la curva mediante el trazado de rectas tangentes y secantes[11].

En 1928 Weil extendió este resultado al caso en que $\mathbb{Q}$ es reemplazado por un cuerpo arbitrario de números algebraicos[12]. El teorema que se obtiene se llama el teorema de Mordell–Weil.

El menor valor posible de r se llama el *rango* de la curva.

Una curva elíptica E sobre un cuerpo K tiene una ecuación de Weierstrass generalizada (o modelo) de la forma

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{40}$$

donde $a_i \in K$ para $i = 1, 2, 3, 4, 6$.

[10] Poincaré, Henri. *Sur les propriétés des courbes algebriques planes.* J. Liouville (v), **7**, 1901, 161–205.

[11] Mordell, Louis J. *Diophantine equations.* Academic Press. New York, 1969, 138–144

[12] Weil, André. *Sur un théoréme de Mordell.* Bull. Sci. Math. **54**, 1930, 182–191. Reproducido en: *Oeuvres Scientifiques*, Collected Papers, vol.1. Springer Verlag, New York, 1980, 11–45.

Siguiendo las formulaciones de TATE (ver [49]), definimos:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4, \end{aligned}$$

el discriminante de E

$$\begin{aligned} \Delta &= -b_2^2b^8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6; \quad \text{y} \\ j &= \frac{a_4^3}{\Delta}. \end{aligned}$$

Para cada primo p consideramos el cuerpo $\mathbb{Q}_p$ de los racionales $p-$ádicos. Sea ν_p la valuación $p-$ádica normalizada de tal manera que $\nu_p(p) = 1$. Entonces, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \nu_p(x) \geq 0\}$.

Sea p un número primo fijo. Entre todos los modelos isomorfos de una curva elíptica dada definida sobre $\mathbb{Q}_p$ podemos encontrar uno donde todos los coeficientes a_i estén en $\mathbb{Z}_p$, y de esta manera, $\nu_p(\Delta) \geq 0$. Esto se hace posible mediante el cambio de coordenadas

$$\begin{aligned} x &\to u^{-2} \cdot x \\ y &\to u^{-3} \cdot y, \end{aligned}$$

el cual conduce cada a_i en $u^i \cdot a_i$, y u se escoge como una potencia de p.

Dado que ν_p es una función discreta, además podemos considerar una ecuación de la curva elíptica para la cual $\nu_p(\Delta)$ sea del menor valor posible.

Si una curva elíptica E sobre $\mathbb{Q}$ con ecuación de Weierstrass (40). Decimos que E es minimal a p si: $a_i \in \mathbb{Z}_p \quad (i = 1, 2, 3, 4, 6)$ y $-\nu_p(\Delta)$ es minimal entre todos los modelos isomorfos de E sobre $\mathbb{Q}_p$.

Decimos que E es un modelo minimal global si E es minimal para todo primo p.

Consideremos entonces, una curva elíptica E definida sobre $\mathbb{Q}$ (modelo minimal global) con ecuación de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

asociamos a E dos invariantes, el discriminante (Δ) y el conductor (N).

- **Discriminante:** $\Delta = -b_2^2b_8 - 8b_4^3 - 27b^6 + 9b_2b_4b_6$
- **Conductor:** $N = \prod_p \Delta_p^{f_p}$ donde

$$f_p = \begin{cases} 0, & \text{si } E(F_p) \text{ es no singular,} \\ 1, & \text{si } E(F_p) \text{ tiene una singularidad nodal,} \\ 2+\delta, & \text{si } E(F_p) \text{ tiene una singularidad de cúspide,} \\ & \text{con } \delta = 0 \text{ si } p \neq 2, 3. \end{cases}$$

Los valores del conductor fueron mostrados por primera vez en 1967 por Ogg [39].

Conjetura 8 (Conjetura de Szpiro (1981))**.** *Sea E una curva elíptica sobre $\mathbb{Q}$ que es modelo minimal con discriminante Δ y conductor N. Entonces, para todo $\epsilon > 0$ existe una constante $K(\epsilon) > 0$ tal que*

$$\Delta < K_\epsilon \cdot N^{6+\epsilon}.$$

Teorema 4.4. *La conjetura abc es equivalente a la conjetura de Szpiro.*

Conjetura *abc* ($\Rightarrow$) Conjetura de Szpiro. *Demostración.* Como $\mathbb{Q}$ es un cuerpo de característica cero, la curva elíptica E puede ser transformada a una de la forma (38) cuya representación en coordenadas afines está dada por (39).

Fijemos $\epsilon > 0$ y sea $\epsilon'' = \frac{1}{2}\epsilon$. Tomemos

$$D = 4u^3 - 27v^2.$$

Por la conjetura *abc*, (en particular por nuestra demostración la conjetura de Hall (sección 3.3),

$$|u| \ll (\operatorname{rad} D)^{\frac{2(1+\epsilon')}{1-5\epsilon'}} \qquad \text{y} \qquad |v| \ll (\operatorname{rad} D)^{\frac{3(1+\epsilon')}{1-5\epsilon'}}$$

para algún ϵ', $0 < \epsilon' \leq \frac{\epsilon''}{(18+5\epsilon'')}$.

Entonces

$$|u| \ll (\operatorname{rad} D)^{2+\epsilon''} \qquad \text{y} \qquad |v| \ll (\operatorname{rad} D)^{3+\epsilon''},$$

y, por lo tanto,

$$|u|^3 \ll (\operatorname{rad} D)^{6+3\epsilon''} = (\operatorname{rad} D)^{6+\epsilon}$$

y

$$|v|^2 \ll (\operatorname{rad} D)^{6+3\epsilon''} = (\operatorname{rad} D)^{6+\epsilon}.$$

Luego,

$$|D| = |4u^3 - 27v^2| \leqq 4|u|^3 + 27|v|^2 \ll (4+27)(\operatorname{rad} D)^{6+\epsilon},$$

con lo cual obtenemos que

$$\Delta \ll (\operatorname{rad} D)^{6+\epsilon} \ll N^{6+\epsilon}.$$

La demostración de la implicación Conjetura de Szpiro ($\Rightarrow$) Conjetura *abc*, se encuentra en [24], aquí presentamos la demostración de algo un poco más débil.

Conjetura 9 (Conjetura *abc* (débil))**.** *Sean a, b, c enteros primos entre sí que satisfacen $a + b = c$. Entonces, para todo $\epsilon > 0$ existe una constante k_ϵ tal que*

$$|abc|^{1/3} < k_\epsilon \operatorname{rad}(abc)^{1+\epsilon}.$$

A partir de la conjetura *abc* se deduce fácilmente la anterior, y decimos que es una versión débil pues no es posible a partir de ella demostrar la conjetura *abc*.

La conjetura *abc* implica la conjetura *abc* (débil), ya que para toda tripla de enteros a, b, c :

$$|a|, |b|, |c| \leq \operatorname{máx}(|a|, |b|, |c|)$$

y dado que a, b, c son distintos, entonces

$$|a| \cdot |b| \cdot |c| < \left(\operatorname{máx}(|a|, |b|, |c|)\right)^3$$

y por lo tanto,

$$\begin{aligned} |abc| &= |a| \cdot |b| \cdot |c| \\ &< \left(\operatorname{máx}(|a|, |b|, |c|)\right)^3. \end{aligned}$$

Conjetura de Szpiro ($\Rightarrow$) Conjetura *abc* (débil). *Demostración.* Sean a, b, c enteros primos relativos tales que $a + b + c = 0$.

Consideremos la curva de Frey–Hellegouarch [12]

$$E_{a,b} : y^2 = x(x - a)(x - b).$$

Un modelo minimal para esta curva tiene discriminante

$$\Delta = (abc)^2 \cdot 2^{-s}$$

y conductor

$$N = \operatorname{rad}(abc) \cdot 2^{-t}$$

donde s y t son enteros acotados. Por la conjetura de Szpiro, para cada $\epsilon > 0$ existe una constante $K_\epsilon > 0$ tal que

$$\Delta = (abc)^2 \cdot 2^{-s} \quad < K_\epsilon \cdot N^{6+\epsilon} \quad = K_\epsilon (\operatorname{rad}(abc) \cdot 2^{-t})^{6+\epsilon},$$

y entonces tenemos que

$$|abc|^{1/3} < \left(K_\epsilon \cdot 2^{-t(6+\epsilon)+s}\right)^{1/6} \cdot \operatorname{rad}(abc)^{(6+\epsilon)/6}.$$

Si ponemos $k_\epsilon = \left(K_\epsilon \cdot 2^{-t(6+\epsilon)+s}\right)^{1/6}$, k_ϵ es entonces una constante que sólo depende de ϵ y para la cual

$$|abc|^{1/3} = k_\epsilon \operatorname{rad}(abc)^{(6+\epsilon)/6} < k_\epsilon \operatorname{rad}(abc)^{1+\epsilon}.$$

De esta manera, dado un $\epsilon > 0$ hemos encontrado una constante k_ϵ tal que

$$|abc|^{1/3} < k_\epsilon \operatorname{rad}(abc)^{1+\epsilon},$$

es decir, a partir de la conjetura de Szpiro se sigue la conjetura *abc* (débil). □ ✓

5. Evidencia de la conjetura abc

5.1. La evidencia. Recordemos el enunciado de la conjetura *abc* presentado en la sección 2: *Para todo* $\epsilon > 0$ *existe una constante* k_ϵ *tal que, si* a, b, c *son enteros positivos primos relativos, para los cuales* $a + b = c$ *entonces:*

$$c \leq k_\epsilon\big(\mathrm{rad}\,(abc)\big)^{1+\epsilon}.$$

En 1986, Stewart y Tijdeman [46] obtuvieron una cota superior para c en función de $\mathrm{rad}\,(abc)$, probando lo siguiente:

Existe una constante positiva c_0 *efectivamente calculable, la cual, para todos los enteros positivos* a, b *y* c *tales que* $a + b = c$ *y* $\mathrm{m.\,c.\,d.}\,(a, b, c) = 1$,

$$c < \exp\big(c_0(\mathrm{rad}\,abc)^{15}\big). \tag{41}$$

La prueba depende de una estimación $p-$ádica para formas lineales en logaritmos de números algebraicos debida a van der Poorten [51]. En 1991, Stewart y Yu [47] reforzaron (41); ellos probaron el siguiente teorema combinando una estimación p–ádica para formas lineales en logaritmos de números algebraicos desarrollada por Yu [60], con una temprana estimación arquimediana debida a Waldshmidt [55],

Teorema 5.1. *Existe una constante* k *efectivamente calculable tal que para todos los enteros positivos* a, b *y* c *con* $a + b = c$, $\mathrm{m.\,c.\,d.}\,(a, b, c) = 1$ *y* $c > 2$,

$$c < \exp\big((\mathrm{rad}\,abc)^{2/3+k/\log\log\mathrm{rad}\,abc}\big). \tag{42}$$

Stewart y Yu en junio del 2001 [48], presentaron dos versiones mejoradas de (42).

Teorema 5.2. *Existe un número positivo efectivamente calculable* k_1 *tal que, para todos los enteros positivos* a, b *y* c *con* $a + b = c$ *y* $\mathrm{m.\,c.\,d.}\,(a, b, c) = 1$,

$$c < \exp\big(k_1(\mathrm{rad}\,abc)^{1/3} \cdot (\log\mathrm{rad}\,abc)^3\big). \tag{43}$$

El nuevo ingrediente clave de la prueba es una estimación de Yu [61] para formas lineales p–ádicas de números algebraicos que tiene una mejor dependencia del número de términos en la forma lineal que la estimación p–ádica previa. Los detalles sobre la medida arquimediana usada por Yu se pueden ver en el trabajo de Matveev [31]. Ellos emplearon esta estimación con el objetivo de controlar el orden p–ádico en los primos p más pequeños que dividen a a, b y c.

Un examen cuidadoso en la prueba del teorema anterior revela que el obstáculo para mejorarlo no es la dependencia sobre el número de términos de la estimación para formas lineales en logaritmos, en lugar de esto, es la dependencia sobre el parámetro p en la estimación p–ádica. Este hecho se resalta en el resultado que enunciamos a continuación, también de Stewart y Yu [48], el cual

muestra que si el factor primo más grande de a, b o c es pequeño en relación con $\operatorname{rad}(abc)$, entonces la estimación para c del Teorema 5.2 puede ser mejorada.

Si p_a, p_b y p_c denotan los factores primos más grandes de a, b y c respectivamente, con la convención de que el factor primo más grande de 1 es 1 ; y $p' = \min(p_a, p_b, p_c)$. El resultado puede ser enunciado de la siguiente manera.

Teorema 5.3. *Existe un número positivo k_2 efectivamente calculable tal que, para todos los enteros positivos a, b y c con $a+b=c$ y $c>2$,*

$$c < \exp\big(p' \cdot (\operatorname{rad} abc)^{k_2 \cdot \log_3(r_*)/\log_2 \operatorname{rad} abc}\big). \tag{44}$$

Donde $r_* = \max\big(\operatorname{rad}(abc), 16\big)$ y $\log_i$ denota la i–ésima iteración de la función logaritmo, esto es, $\log_1 t = \log t$ y $\log_i t = \log(\log_{i-1} t)$ para $i = 2, 3, \ldots$.

Las demostraciones de los teoremas 5.2 y 5.3 se encuentran con todos sus detalles en [48]. Nosotros presentamos aquí la demostración del Teorema 5.1.

A continuación daremos algunas nociones y lemas preliminares que necesitaremos más adelante.

Si p es un número primo, sea

$$q = \begin{cases} 2 & \text{si } p > 2 \\ 3 & \text{si } p = 2, \end{cases} \qquad \text{y} \tag{45}$$

$$\alpha_0 = \begin{cases} \zeta_4 & \text{si } p > 2 \\ \zeta_2 & \text{si } p = 2 \end{cases} \tag{46}$$

donde $\zeta_m = e^{2\pi i/m}$ siendo m un entero positivo.

Sea $K = \mathbb{Q}(\alpha_0)$ y $D = \Omega \cap K$ el anillo de los enteros algebraicos en K.

Para $c = x + iy \in \mathbb{C}$, $|c| = \sqrt{x^2+y^2}$. Entonces, si $\alpha_1, \ldots, \alpha_n \in D$ son tales que $|\alpha_i| \le A_i$ para $1 \le i \le n$ donde cada $A_i \ge 4$, denotamos

$$A = \max_{1 \le i \le n} A_i.$$

Sean $b_1, \ldots, b_n$ enteros racionales (es decir, en $\mathbb{Z}$) tales que $|b_i| \le B$ para $1 \le i \le n$, donde B es un entero fijo ≥ 3.

Para cada $\alpha \in K \setminus \{0\}$, dado que D es un dominio de Dedekind, el ideal $(\alpha)D$ puede ser escrito como un producto de ideales primos en D, es decir, $(\alpha)D = \wp_1^{e_{\wp_1}} \cdots \wp_g^{e_{\wp_g}}$. Definimos $\operatorname{ord}_{\wp_i} \alpha = e_{\wp_i}$, que es el índice de ramificación de $\wp_i$, y $f_\wp$ el grado de la clase residual de $\wp$. Y por último, sea $\Theta = \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1$.

Lema 5.1. *Si $\big[K\big(\alpha_0^{1/q}, \ldots, \alpha_n^{1/q}\big) : K\big] = q^{n+1}$, $\operatorname{ord}_\wp \alpha_j = 0$ para $j = 1, \ldots, n$ y $\Theta \neq 0$, entonces*

$$\operatorname{ord}_\wp \Theta < (c_1 n)^n p^2 \cdot \log B \cdot \log\log A \cdot \log A_1 \cdot \cdots \cdot \log A_n$$

donde c_1 es un número efectivamente calculable.

Lema 5.2. *Para $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^+$, si $\left[\mathbb{Q}\left(\alpha_1^{1/2}, \ldots, \alpha_n^{1/2}\right) : \mathbb{Q}\right] = 2^n$ y $b_1 \cdot \log \alpha_1 + \cdots + b_n \cdot \log \alpha_n \neq 0$, entonces*

$$|b_1 \cdot \log \alpha_1 + \cdots + b_n \cdot \log \alpha_n| > \exp\left((-c_2 n)^n \cdot \log B \cdot (\log\log A)^2 \cdot \log A_1 \cdot \cdots \cdot \log A_n\right).$$

donde c_2 es un número positivo efectivamente calculable.

Lema 5.3. *Sean $\alpha_1, \ldots, \alpha_n$ números primos tales que $\alpha_1 < \alpha_2 < \cdots < \alpha_n$. Entonces*

$$\left[\mathbb{Q}\left(\alpha_1^{1/2}, \alpha_2^{1/2}, \ldots, \alpha_n^{1/2}\right) : \mathbb{Q}\right] = 2^n.$$

Si $q = 2$ y $\alpha_0 = \zeta_4$ o $q = 3$ y $\alpha_0 = \zeta_6$, y $K = \mathbb{Q}(\alpha_0)$. Entonces

$$\left[K\left(\alpha_0^{1/q}, \alpha_1^{1/q}, \ldots, \alpha_n^{1/q}\right) : K\right] = q^{n+1},$$

excepto cuando $q = 2$, $\alpha_0 = \zeta_4$ y $\alpha_1 = 2$, y en este caso,

$$\left[K\left(\alpha_0^{1/2}, (1+i)^{1/2}, \alpha_2^{1/2}, \ldots, \alpha_n^{1/2}\right) : K\right] = 2^{n+1}.$$

Lema 5.4. *Sea $p_1 = 2, p_2, \ldots$ la sucesión de números primos en orden creciente. Entonces, existe una constante efectivamente calculable $c_3 > 0$ tal que para todo entero positivo r,*

$$\prod_{j=1}^{r} \frac{p_j}{\log p_j} > \left(\frac{r+3}{c_3}\right)^{r+3}.$$

El lector que este interesado en las demostraciones de los lemas anteriores las puede encontrar en [47].

La siguiente prueba se debe a Stewart y Yu.

Demostración. [Demostración del Teorema 5.1] Sean $c_4, c_5, \ldots$ constantes positivas efectivamente calculables. Sin pérdida de la generalidad supongamos que $a \leq b$. Dado que $a + b = c$, $\mathrm{m.c.d.}\,(a, b, c) = 1$ y $c \geq 2$, se sigue que $a < b < c$ y $\mathrm{rad}(abc) \geq 6$. Escribimos

$$\begin{aligned} a &= p_1^{e_1} \cdots p_t^{e_t}, \\ b &= q_1^{f_1} \cdots q_u^{f_u}, \\ c &= s_1^{g_1} \cdots s_v^{g_v}, \end{aligned}$$

donde $p_1, \ldots, p_t, q_1, \ldots, q_u, s_1, \ldots, s_v$ son primos distintos, $t \geq 0$, $u \geq 1$, $v \geq 1$ y $e, f, g \in \mathbb{Z}^+$.

De nuevo, denotamos por p_a el primo más grande que divide a a, excepto cuando $a = 1$ en cuya situación simplemente ponemos $p_a = 1$; de manera semejante notamos por p_b y p_c el primo más grande que divide a b y c respectivamente.

Entonces para cualquier primo p

$$\max\left(\mathrm{ord}_p\, a, \mathrm{ord}_p\, b, \mathrm{ord}_p\, c\right) \leq \frac{\log c}{\log 2}. \tag{47}$$

Por otro lado,

$$\log c = \sum_{p|c} (\operatorname{ord}_p c \cdot \log p) \leq \max_{p|c} (\operatorname{ord}_p c) \cdot \log \operatorname{rad}(abc) \tag{48}$$

pues,

$$\begin{aligned}\sum_{p|c} (\operatorname{ord}_p c \cdot \log p) &\leq \sum_{p|c} \big(\max_{p|c} (\operatorname{ord}_p c) \cdot \log p\big) \\ &= \max_{p|c} (\operatorname{ord}_p c) \cdot \sum_{p|c} \log p \\ &= \max_{p|c} (\operatorname{ord}_p c) \cdot \log\Big(\prod_{p|c} p\Big).\end{aligned}$$

Dado que $(a,b) = (a,c) = (b,c) = 1$, para cada primo p que divide a c,

$$\operatorname{ord}_p c = \operatorname{ord}_p \left(\frac{c}{-b}\right) = \operatorname{ord}_p\Big(\frac{a}{-b} - 1\Big) \leq \operatorname{ord}_p\Big(\Big(\frac{a}{b}\Big)^4 - 1\Big).$$

Estimamos ahora

$$\operatorname{ord}_p\Big(\Big(\frac{a}{b}\Big)^4 - 1\Big) = \operatorname{ord}_p(p_1^{4e_1} \cdots p_t^{4e_t} \cdot q_1^{-4f_1} \cdots q_u^{-4f_u} - 1)$$

empleando el Lema 5.1.

Sea $\Theta = \left(\frac{a}{b}\right)^4 - 1$ (claramente $\Theta \neq 0$ ya que $\text{m. c. d.}\,(a,b) = 1$). Si $p = 2$ ponemos $K = \mathbb{Q}(\zeta_6)$, y si $p > 2$, $K = \mathbb{Q}(\zeta_4)$. Definimos q y α_0 como en (45) y (46) respectivamente. Sea $\wp$ un ideal primo del anillo de los enteros algebraicos de K tal que $(p) \subseteq \wp$ (aquí (p) es el ideal principal generado por p en D); entonces,

$$\operatorname{ord}_p \Theta \leq \operatorname{ord}_\wp \Theta.$$

Para el entero n del Lema 5.1, tomamos $n = t + u$ y consideramos $\alpha_1, \ldots, \alpha_n$ como los primos $p_1, \ldots, p_t, q_1, \ldots, q_u$ ordenados en orden creciente, excepto en el caso en que $p > 2$ y $\alpha_1 = 2$. En este caso ponemos en el primer lugar de la sucesión $\alpha_1 = 1 + i$ en lugar de $\alpha_1 = 2$. Para $i = 1 \ldots, n$ tomamos

$$A_i = \begin{cases} \alpha_i, & \text{si } |\alpha_i| \geq 4 \\ 4, & \text{de lo contrario.} \end{cases}$$

Como $p|c$ y $\text{m. c. d.}\,(a,c) = \text{m. c. d.}\,(b,c) = 1$ entonces $\operatorname{ord}_p \alpha_i = 0$ para $i = 1, \ldots, t+u$, además como $(p) \subseteq \wp$ y $\wp$ es un ideal primo entonces $(\alpha_i) \nsubseteq \wp$ es decir, $\operatorname{ord}_\wp \alpha_i = 0$ para $i = 1, \ldots, n$. En el caso en que $p > 2$ y $\alpha_1 = 2$, en el cual hemos puesto $\alpha_1 = 1 + i$ en lugar de $\alpha_1 = 2$, basta observar que $2^4 = (1+i)^8$, en consecuencia, si $1 + i \in \wp$, $2^4 = (1+i)^8 \in \wp$ y esto implica que $2 \in \wp$ (por ser $\wp$ un ideal primo), lo cual es claramente una contradicción.

Por el Lema 5.3,

$$\big[K\big(\alpha_0^{1/q}, \alpha_1^{1/q}, \ldots, \alpha_{t+u}^{1/q}\big) : K\big] = q^{t+u+1},$$

y haciendo $B = \max(4e_1, \ldots, 4e_t, 4f_1, \ldots, 4f_u)$, por (47)

$$B \leq \frac{4 \log c}{\log 2}.$$

Entonces, por el Lema 5.1,

$$\begin{aligned} \operatorname{ord}_p c \leq \operatorname{ord}_p \Theta &\leq \operatorname{ord}_\wp \Theta \\ &< \big(c_4 \cdot (t+u)\big)^{t+u} \cdot p^2 \cdot \log\log c \cdot \log\log \operatorname{rad}(abc) \cdot \prod_{p|abc} \log p, \end{aligned} \tag{49}$$

donde c_1 es una constante efectivamente calculable.

Similarmente, si $p|b$ consideramos $\operatorname{ord}_p \left(\left(\frac{c}{a}\right)^4 - 1\right)$ y tenemos que

$$\operatorname{ord}_p b < \big(c_5 \cdot (t+v)\big)^{t+v} \cdot p^2 \cdot \log\log c \cdot \log\log \operatorname{rad}(abc) \cdot \prod_{p|ac} \log p, \tag{50}$$

donde c_5 es una constante efectivamente calculable.

Y si $p|a$ entonces consideramos $\operatorname{ord}_p \left(\left(\frac{c}{b}\right)^4 - 1\right)$, y obtenemos

$$\operatorname{ord}_p a < \big(c_6 \cdot (u+v)\big)^{u+v} \cdot p^2 \cdot \log\log c \cdot \log\log \operatorname{rad}(abc) \cdot \prod_{p|bc} \log p. \tag{51}$$

Ahora bien, por (48) y (49)

$$\begin{aligned} \frac{\log c}{\log\log c} &\leq \big(\max_{p|c}(\operatorname{ord}_p c)\big) \cdot \frac{\log \operatorname{rad}(abc)}{\log\log c} \\ &< \big(c_4 \cdot (t+u)\big)^{t+u} \cdot p_c^2 \cdot \log\log \operatorname{rad}(abc) \cdot \log \operatorname{rad}(abc) \cdot \prod_{p|abc} \log p \\ &< \big(c_4 \cdot (t+u)\big)^{t+u} \cdot p_c^2 \cdot \big(\log \operatorname{rad}(abc)\big)^2 \cdot \prod_{p|abc} \log p. \end{aligned} \tag{52}$$

Dado que $b > \frac{c}{2}$ y $c \geq 3$,

$$\log b > (\log c) - (\log 2) > \frac{\log c}{4}. \tag{53}$$

Además (48) se cumple si reemplazamos c por b, entonces por (50) y (53),

$$\begin{aligned} \frac{\log c}{4 \log\log c} &< \frac{b}{\log\log c} \\ &\leq \Big(\max_{p|b}(\operatorname{ord}_p b)\Big) \cdot \frac{\log \operatorname{rad}(abc)}{\log\log c} \qquad (54) \\ &< \big(c_5 \cdot (t+v)\big)^{t+v} \cdot p_b^2 \cdot \log\log \operatorname{rad}(abc) \cdot \log \operatorname{rad}(abc) \cdot \prod_{p|ac} \log p \\ &\leq \big(c_5 \cdot (t+v)\big)^{t+v} \cdot p_b^2 \cdot \big(\log \operatorname{rad}(abc)\big)^2 \cdot \prod_{p|ac} \log p. \qquad (55) \end{aligned}$$

Por otro lado,

$$\begin{cases} \text{Si } a > \sqrt{b}, & \log a \geq \frac{1}{2}\log b > \frac{\log c}{8} \qquad \text{(por 53)} \\ \text{Si } a \leq \sqrt{b}, & \log\left(\frac{a+b}{b}\right) = \log\left(1+\frac{a}{b}\right) < \log\left(1+\frac{1}{\sqrt{b}}\right) < \frac{1}{\sqrt{b}} < \frac{\sqrt{2}}{\sqrt{c}}. \end{cases} \quad (56)$$

En el caso en que $a > \sqrt{b}$, por (48) reemplazando c por a, y (51) :

$$\begin{aligned} \frac{\log c}{8\log\log c} &< \frac{\log a}{\log\log c} \\ &\leq \left(\max_{p|a}(\operatorname{ord}_p a)\right) \cdot \frac{\log \operatorname{rad}(abc)}{\log\log c} \\ &< \left(c_6 \cdot (u+v)\right)^{u+v} \cdot p_a^2 \cdot \left(\log \operatorname{rad}(abc)\right)^2 \cdot \prod_{p|bc} \log p; \end{aligned} \quad (57)$$

en el segundo caso,

$$\begin{aligned} 0 < \log\left(\frac{a+b}{b}\right) &= \log\left(\frac{c}{b}\right) \\ &= g_1 \log s_1 + \cdots + g_v \log s_v - f_1 \log q_1 - \cdots - f_u \log q_u. \end{aligned} \quad (58)$$

Por el Lema 5.3 aplicado a los primos $q_1, \ldots, q_u, s_1, \ldots, s_v$, podemos usar el Lema 5.2 para obtener una cota inferior para $\log\left(\frac{c}{b}\right)$.

Entonces, de acuerdo con el Lema 5.2,

$$\begin{aligned} |g_1 \log s_1 + \cdots + g_v \log s_v - f_1 \log q_1 - \cdots - f_u \log q_u| > \\ \exp\left(\left(-c_2 \cdot (u+v)\right)^{u+v} \cdot \log B \cdot (\log\log A)^2 \cdot \prod_{p|cb} \log p\right), \end{aligned} \quad (59)$$

donde $B = \max(4f_1, \ldots, 4f_u, 4g_1, \ldots, 4g_v)$, $\alpha_1, \ldots, \alpha_{u+v}$ los primos que dividen a bc ordenados en orden creciente, $A = \max_{1 \leq i \leq u+v}(\alpha_i)$ y c_2 un número positivo efectivamente calculable.

De (56) y (59) obtenemos

$$\exp\left(\left(-c_2 \cdot (u+v)\right)^{u+v} \cdot \log B \cdot (\log\log A)^2 \cdot \prod_{p|c} \log p\right) < \frac{\sqrt{2}}{\sqrt{c}},$$

y de esta última desigualdad obtenemos nuevamente (57) (con una constante diferente).

Tomando $\rho = t+u+v$, de (52), (55) y (57) deducimos que

$$\begin{aligned}\Big(\frac{\log c}{4\log\log c}\Big)^3 &\le \frac{(\log c)^3}{4\cdot 4\cdot 2\cdot(\log\log c)^3} = \frac{\log c}{\log\log c}\cdot\frac{\log c}{4\log\log c}\cdot\frac{\log c}{8\log\log c}\\ &\le \big(c_4\cdot(t+u)\big)^{t+u}\cdot\big(c_5\cdot(t+v)\big)^{t+v}\cdot\big(c_6\cdot(u+v)\big)^{u+v}\cdot(p_c\cdot p_b\cdot p_a)^2\\ &\quad\cdot\big(\log\operatorname{rad}(abc)\big)^6\cdot\prod_{p\mid ab}\log p\cdot\prod_{p\mid ac}\log p\cdot\prod_{p\mid bc}\log p.\end{aligned}$$

Entonces,

$$\Big(\frac{\log c}{4\log\log c}\Big)^3 \le (c_8\cdot\rho)^{2\rho}\cdot(p_c\cdot p_b\cdot p_a)^2\cdot\Big(\prod_{p\mid abc}\log p\Big)^2\cdot\big(\log\operatorname{rad}(abc)\big)^6. \quad (60)$$

Por el Lema 5.4,

$$\Big(\frac{\rho}{c_9}\Big)^\rho < \prod_{j=1}^{\rho-3}\frac{p_j}{\log p_j} < 2\cdot\prod_{\substack{p\mid abc\\ p\neq p_a,p_b,p_c}}\frac{p}{\log p}, \quad (61)$$

con la convención usual que el producto vacío es 1.

Con la desigualdad anterior y (60) obtenemos

$$\begin{aligned}\Big(\frac{\log c}{4\log\log c}\Big)^3 &\le (c_{10})^\rho\cdot\left(2\cdot\prod_{\substack{p\mid abc\\ p\neq p_a,p_b,p_c}}\frac{p}{\log p}\right)^2\cdot\left(\prod_{p\mid abc}\log p\right)^2\\ &\quad\cdot(p_a\cdot p_b\cdot p_c)^2\cdot\big(\log\operatorname{rad}(abc)\big)^6\\ &= 4\cdot(c_{10})^\rho(\operatorname{rad} abc)^2\cdot(\log p_a\cdot\log p_b\cdot\log p_c)^2\cdot\big(\log\operatorname{rad}(abc)\big)^6\\ &\le (c_{10})^\rho\cdot(\operatorname{rad} abc)^2\cdot\big(\log\operatorname{rad}(abc)\big)^{12}. \quad (62)\end{aligned}$$

De nuevo, por el Lema 5.4 tenemos que

$$c_{10}^p < (\operatorname{rad} abc)^{c_{11}/\log\log\operatorname{rad}(abc)},$$

entonces, por (62),

$$\Big(\frac{\log c}{4\log\log c}\Big)^3 < (\operatorname{rad} abc)^{c_{11}/\log\log\operatorname{rad} abc}\cdot(\operatorname{rad} abc)^2\cdot(\log\operatorname{rad} abc)^{12},$$

lo cual implica que

$$\frac{\log c}{4\log\log c} < (\operatorname{rad} abc)^{c_{11}/3\log\log\operatorname{rad} abc}\cdot(\operatorname{rad} abc)^{2/3}\cdot(\log\operatorname{rad} abc)^4$$

y, en consecuencia,

$$\log c < (\operatorname{rad} abc)^{2/3+k/\log\log\operatorname{rad} abc},$$

donde k es una constante efectivamente calculable.

5.2. Buenas triplas asociadas con la conjetura *abc*. De acuerdo con la formulación de Oesterlé de la conjetura *abc*, y a la equivalencia que demostramos en la sección (4.1), decimos que una tripla (a, b, c) es una *buena tripla* si $L > 1{,}4$ donde

$$L = L(a, b, c) = \frac{\log(|a|, |b|, |c|)}{\log \operatorname{rad}(abc)}.$$

Conjetura 10. *Si la conjetura abc es verdadera, existe sólo un número finito de buenas triplas.*

Hasta enero de 2002, existían 152 buenas triplas conocidas. Una lista de ellas se encuentra en [53].

$a = 1$	$b = 2400$	$L = 1{,}454673$
$a = 1$	$b = 44374$	$L = 1{,}567887$
$a = 1$	$b = 512000$	$L = 1{,}443307$
$a = 3$	$b = 125$	$L = 1{,}426565$
$a = 5$	$b = 177147$	$L = 1{,}412681$
$a = 37$	$b = 32768$	$L = 1{,}482910$
$a = 121$	$b = 255879$	$L = 1{,}488865$
$a = 338$	$b = 390625$	$L = 1{,}445064$
$a = 343$	$b = 59049$	$L = 1{,}547075$
$a = 2197$	$b = 700928$	$L = 405785$
$a = 7168$	$b = 78125$	$L = 1{,}435006$

Cuadro 5. Resultados (Buenas Triplas para $1 \leq a, b \leq 100000$)

Parece que los valores de las buenas triplas en la mencionada lista fueron descubiertos por medio de varios algoritmos. De hecho los valores expuestos fueron tomados de buenas triplas sobre un intervalo particular, tal como lo confirma el programa en C escrito por Jeffrey P. Wheeler con ayuda de Joel Mejeur y Michael Saum (Universidad de Tennessee, Knoxville). Este programa se hizo correr en paralelo (usando MPI) entre 24 y 30 computadores Intel 450 MHz Pentium III durante aproximadamente cuatro días y medio. Inicialmente el programa chequeó las buenas triplas sobre los intervalos $1 \leq a \leq 100000$ y $a \leq b \leq 100000$. Estos resultados aparecen en el cuadro 5.

El lector puede encontrar el código del programa y algunos detalles adicionales en [57, págs. 27–33].

Agradecimientos. Los autores quieren agradecer al revisor anónimo por sus correcciones y valiosas sugerencias que contribuyeron a mejorar el artículo.

Referencias

[1] Albis, Víctor. *El Señor de Fermat y sus Problemas I*. Boletín de Matemáticas **7**, 1973, 219–232.

[2] Albis, Víctor. *Las ecuaciones de Fermat y Catalan en $K[t]$*. Boletín de Matemáticas **9**, 1975, 217–220.

[3] Bombieri, Enrico. *The Mordell Conjecture revisited*. Ann. Scu. Norm. Sup. Pisa Cl. Sci. IV**17, 4**, 1990, 615–640, and *Errata–corrige, ibid IV* **18, 3**, 1991, 473.

[4] Bombieri, Enrico. *Roth's Theorem and the abc Conjecture*. ETH Zürich, 1994.

[5] Catalan, Eugène. *Note extraite d'une lettre adressée à l'éditeur*. J. Reine Angew. Math. **27**, 1844, 192.

[6] Cochrane, Todd & Dressler, Robert E. *Gaps between integers with the same prime factors*. Math. Comp. **68**, 1999, 395–401.

[7] Davenport, Harold. *On $f^3(t) - g^2(t)$*. Norske Vid. Selsk. Forh. (Trondheim) **38**, 1965, 86–87.

[8] Elkies, Noam D. *ABC implies Mordell*. Intern. Math. Research Notices No. **7**, 1991, 99–109 ; Duke Math. J. **64**, 1991.

[9] Ellenberg, Jordan S. *Congruence ABC implies ABC*. Indag. Math. N.S. **11** (2), 2000, 197–200.

[10] Faltings, Gerd. *Endlichkeitssätze fürabelsche Varietäten über Zahlkörpern*. Invent. Math. **73**, 1983, 349–366.

[11] Faltings, Gerd. *Diophantine approximation on Abelian varieties*. Annals of Mathematics **133**, 1991, 549–576.

[12] Frey, Gerhard. *Links between stable elliptic curves and certain diophantine equations*. Annales Universiatis Saraviensis **1** (1), 1986, 1–39.

[13] Goldfeld, Dorian. *Beyond the last theorem*. Math Horizons. September, 1996, 26-34.

[14] Goldfeld, Dorian. *Beyond the last theorem*. The Sciences. March/April, 1996, 34-40.

[15] Granville, Andrew & Tucker, Tomas J. *It's As Easy As abc*. Notices of the AMS. Volume **49**, Number 10, 2002, 1224–1231.

[16] Hall, Jr., Marshall. *The Diophantine equation $x^3 - y^2 = k$*. In Atkin, A.O.L.; Birch, B. J. *Computers in Number Theory*, New York: Academic Press Inc, 1971, 173–198.

[17] Ireland, Kenneth & Rosen, Michael. *A Classical Introduction to Modern Number Theory*. Second ed., Springer–Verlag New York Inc., 1990.

[18] Ko, Chao, *On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$* . Sci. Sinica **14**, 1964, 457.

[19] Korkine, Alexander. *Sur l'impossibilité de la relation algébrique $X^n+Y^n+Z^n = 0$*. C. R. Acad. Sci. Paris **90**, 1880, 303–304.

[20] Lamé, Gabriel. *Étude des binômes cubiques $x^3 \pm y^3$*. C. R. Acad. Sci. Paris **61** (1865), 921–924, 961–965.

[21] Lamé, Gabriel. *Mémoire sur le dernier théorème de Fermat*. C. R. Acad. Sci. Paris **9** (1839), 4–46.

[22] Lamé, Gabriel. *Mémoire d'analyse indéterminée démontrant que l'équation $x^7+y^7 = z^7$ est impossible en nombres entiers*. J. Math. Pures Appl. **5** (1840), 195–211.

[23] Lang, Serge. *Number Theory III*. Encyclopedia of Mathematical Sciences. Vol. **60**. Springer–Verlag. New York, 1991.

[24] Lang, Serge. *Old and New Conjectured Diophantine Equations*.Bulletin of the American Mathematical Society **23**, 1990, 37–75.

[25] Lebesgue, Victor A. *Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$*. Nouvelles annales de mathématiques **9**, 1850, 178–181.

[26] Lebesgue, Victor A. *Résolution des équations biquadratiques* $z^2 = x^4 \pm 2my^4$, $z^2 = 2mx^4 - y^4$, $2mz^2 = x^4 \pm y^4$. J. Math. Pures Appl. **18** (1853). 73–86.
[27] Lebesgue, Victor A. *Démonstration de l'impossibilité de résoudre l'équation* $x^7 + y^7 + z^7 = 0$ *en nombres entiers*. J. Math. Pures Appl. **5** (1840), 276–279, 348–349.
[28] Liouville, R. *Sur l'imposibilité de la relation algébrique* $X^n + Y^n + Z^n = 0$. Comptes Rendus Acad. Sci. Paris, **89**, 1879, 1108–1110.
[29] R. C. Mason. *Diophantine Equations over Function Fields*. London: London Mathematical Society Lecture Note Series, 1984.
[30] Masser, David W. *Open problems*. Contenido en Chen, W. W. L., Proceedings of the Symposium on Analytic Number Theory, London: Imperial College, 1985.
[31] Matveev, Eugene M. *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers*. Izvestiya: Mathematics **62**: 4, 1998, 723–772.
[32] Mihăilescu, Preda V. *Primary cyclotomic units and a proof of Catalan's conjecture* J. Reine Angew. Math. **572** (2004), 167–195.
[33] Mordell, Louis J. *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Math. Proc. Cambridge. Philos. Soc. **21**, 1922, 179–192.
[34] Mordell, Louis J. *Diophantine equations*. Academic Press. New York, 1969.
[35] Mordell, Louis J. *Tres lecciones sobre el último teorema de Fermat*. Lecturas Matemáticas **14** (1-3) (1993).
[36] Moreno, Carlos J. *Fermat's Last Theorem: From Fermat to Wiles*, Revista Colombiana de Matemáticas **29**, 1995, 49–88.
[37] Noguès, Richard. *Théorème de Fermat. Son histoire*. Paris: Librairie Vuibert, 1932.
[38] Oesterlé, Joseph. *Nouvelles approches du Théorème de Fermat*. Sem. Bourbaki **694**, 1987–88, 694–01– 694–21.
[39] Ogg, Andrew P. *Elliptic curves and wild ramification*. Amer. J. Math. **89**, 1967, 1–21.
[40] Peterson, Ivars. *The Amazing ABC Conjecture*, 1997. Disponible en `http://www.maa.org/mathland/mathtrek_12_8.html`.
[41] Ribenboim, Paulo. *13 Lectures on Fermat's Last Theorem*. Springer–Verlag New York Inc., 1979.
[42] Ribenboim, Paulo. *Catalan's Conjecture: are 8 and 9 the only consecutive powers?*. Academic Press Inc., 1994.
[43] Schoof, René. *Catalan's Conjecture* Universitext. Berlin: Springer–Verlag, 2008.
[44] Silverman, Joseph H., *Wieferich's Criterion and the abc–Conjecture*. J. Number Theory **30**, 1988, 226–237.
[45] Snyder, Noah. *An alternative proof of Mason's theorem*. Elem. Math. **53**, 2000, 93–94.
[46] Stewart, Cameron L. & Tijdeman, Robert. *On the Oesterlé–Masser conjecture*. Monatsh. Math. **102**, 1986, 251–257.
[47] Stewart, Cameron L. & Yu, Kunrui. *On the abc Conjecture*, Math. Ann. **291**, 1991, 225–230.
[48] Stewart, Cameron L. & Yu, Kunrui. *On the abc Conjecture II*. Duke Math. J. **108**, 2001, 169–181.
[49] Tate, John. *Algorithm for determining the Type of a Singular Fiber in an Elliptic Pencil*. Modular Functions of One Variable IV. Lecture Notes in Math. **476**, 1975, 33–52.
[50] Tijdeman, Robertf *On the Equation of Catalan*. Acta Arith. **29**, 1976, 197–209.
[51] van der Poorten, Alfred J. *Linear forms in logarithms in the p−adic case*. En A. Baker & D. W. Masser (ed.), *Transcendence Theory: Advances and Applications*, Academic Press, London, 1977, 29–57.
[52] van Frankenhuysen, Machiel, *The ABC conjecture implies Roth's theorem and Mordell's conjecture*. Department of Mathematics, Sproul Hall. University of California, 1991, 45–72.

[53] Villamizar, Nelly. *La conjetura abc*. Universidad Nacional de Colombia, Trabajo de grado, 2005.
[54] Vojta, Paul. *Siegel's theorem in the compact case*. Annals of Mathematics **133**, 1991, 509–548.
[55] Waldschmidt, Michel. *A lower bound for linear forms in logarithms*. Acta Arith. **37**, 1980, 257–283.
[56] Walker, Robert J. *Algebraic curves*. Dover Publications Inc., New York, 1962.
[57] Wheeler, Jeffrey P., *The abc conjecture*. Thesis Presented for the Master of Science Degree The University of Tennessee, Konoxville, 2002.
[58] Wieferich, Arthur. *Zum letzten Fermat'schen Theorem*. J. Reine Angew. Math. **136**, 1909, 29–302.
[59] Wiles, Andrew. *Modular elliptic curves and Fermat's Last Theorem*. Ann. of Math. **141**, 1995, 443–551.
[60] Yu, Kunrui. *Linear forms in p−adic logarithms II*. Compositio Math. **74**, 1990, 15–113.
[61] Yu, Kunrui. *p−adic logarithmic forms and group varieties II*. Acta Arith. **89**, 1999, 337–378.

(Recibido en agosto de 2012. Aceptado para publicación en abril de 2013)

Víctor S. Albis
Departamento de Matemáticas
Universidad Nacional de Colombia, Bogotá, Colombia
e-mail: vsalbisg@unal.edu.co
Nelly Y. Villamizar
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences, Linz, Austria
e-mail: nelly.villamizar@oeaw.ac.at