



HAL
open science

Poster summarizing "The abc conjecture and some of its consequences"

Razvan Barbulescu, Michel Waldschmidt

► **To cite this version:**

Razvan Barbulescu, Michel Waldschmidt. Poster summarizing "The abc conjecture and some of its consequences". 6th World Conference on 21st Century Mathematics 2013, Oct 2017, Lahore, India. hal-01626155v1

HAL Id: hal-01626155

<https://hal.science/hal-01626155v1>

Submitted on 31 Oct 2017 (v1), last revised 8 Jan 2018 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The *abc* conjecture and some of its consequences

The *abc* conjecture Esterlé and Masser (1985)

For any $\epsilon > 0$, there exists $\kappa(\epsilon)$ such that, if a, b and c are relatively prime positive integers which satisfy $a + b = c$, then

$$\text{Rad}(abc) > \kappa(\epsilon)c^{1-\epsilon},$$

where for any positive integer n , $\text{Rad}(n)$ is the product of its distinct prime factors.

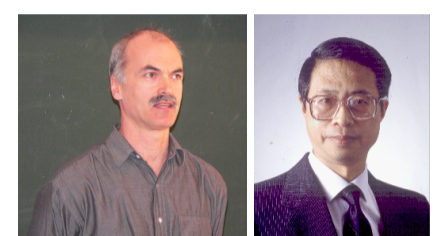


Best unconditional result Stewart and Kunrui Yu (1991, 2001)

For all a, b, c triplet of coprime positive integers such that $a + b = c$ we have

$$c^{R(\log R)^2} \geq c,$$

where $R = \text{Rad}(abc)$ and κ is an absolute constant.



Pillai's conjecture (1945)

Let k be a positive integer. The equation

$$x^p - y^q = k,$$

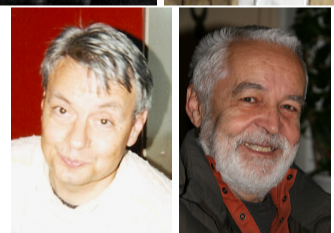
where the unknowns x, y, p and q take integer values, all ≥ 2 , has only finitely many solutions (x, y, p, q) .



The case $k = 1$ Cassels, Tijdeman, Langevin, Mignotte



The equation $|x^p - y^q| = 1$ has no integer solution (x, y, p, q) with $p, q > 1$ and $\max(x^p, y^q) > \exp(\exp(\exp(700)))$.

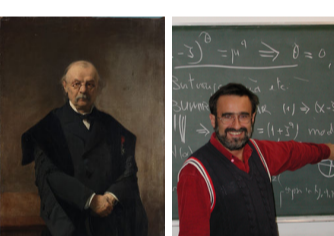


The Catalan-Mihăilescu theorem (1844, 2002)

The only solution to the equation

$$x^p - y^q = 1$$

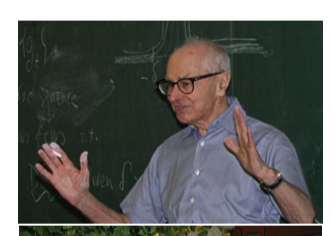
with $x, y > 0$ and $p, q > 1$ is $3^2 - 2^3 = 1$.



The Lang-Waldschmidt conjecture (1978)

Let $\epsilon > 0$. There exists a constant $c(\epsilon) > 0$ with the following property. If $x^p \neq y^q$, then

$$|x^p - y^q| \geq c(\epsilon) \max\{x^p, y^q\}^{\kappa-\epsilon}$$



$$\text{with } \kappa = 1 - \frac{1}{p} - \frac{1}{q}.$$

The *abc* conjecture implies Lang-Waldschmidt and therefore Pillai's conjecture

Hall's conjecture (1971)

The case $p = 3, q = 2$: If $x^3 \neq y^2$, then

$$|x^3 - y^2| \geq c \max\{x^3, y^2\}^{1/6}.$$

To deduce Hall's conjecture from the *abc* conjecture, one would need to take $\epsilon = 0$, which is not allowed.

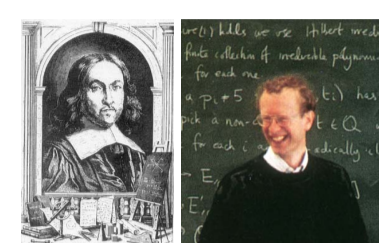


The Fermat-Wiles theorem (1621, 1994)

The equation

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

has no integer solutions x, y, z, n with $x, y, z > 0$ and $n > 2$.



The *abc* conjecture implies asymptotic Fermat-Wiles

Assume $x^n + y^n = z^n$ with $\gcd(x, y, z) = 1$. Then *abc* applied to (x^n, y^n, z^n) implies

$$z^3 > xyz = \text{Rad}(x^n y^n z^n) > \kappa(\epsilon) z^{n(1-\epsilon)}.$$

When $n \geq 4$ we set $\epsilon = \frac{1}{n}$ and obtain a bound on z^n .

The Fermat-Catalan conjecture Brun (1914)

The equation

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

has a finite set of solutions (x, y, z, p, q, r) in positive integers such that

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

The Beal's Prize (IMS) supported by the AMS will be given for a proof or a disproof of this conjecture.



The *abc* conjecture implies asymptotic Fermat-Catalan conjecture Tijdeman (1988)

An elementary study shows that the condition on (p, q, r) actually implies

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{41}{12}.$$

The *abc* conjecture applied to $\epsilon = \frac{1}{12}$ and $(a, b, c) = (x^p, y^q, z^r)$ implies

$$z^{r(1-2\epsilon)} > xyz \geq \text{Rad}(x^p y^q z^r) > \kappa(\epsilon) z^{r(1-\epsilon)}.$$

The case of fixed (p, q, r) Darmon and Granville (1995)

For each triplet (p, q, r) with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ there exist only finitely many coprime solutions (x, y, z) to the Fermat-Catalan equation.



The case $(p, p, 3)$ Darmon and Merel (1997)

The Fermat-Catalan equation has no solution for $p = q \geq 3$ and $r = 3$.



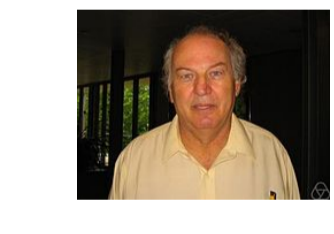
Szpiro's conjecture (1983)

Given any $\epsilon > 0$, there exists a constant $C(\epsilon) > 0$ such that, for any elliptic curve over \mathbb{Q} with minimal discriminant Δ and conductor N ,

$$|\Delta| < C(\epsilon) N^{6+\epsilon}.$$

The *abc* conjecture implies Szpiro's conjecture (Esterlé (1988))

Conversely, Szpiro's conjecture implies a weak form of the *abc* conjecture, with $1 - \epsilon$ replaced by $5/6 - \epsilon$.



Wieferich's theorem (1909)

Let p be a prime and x, y, z positive integers such that $x^p + y^p = z^p$ and p doesn't divide xyz . Then p has the property that

$$p^2 \text{ divides } 2^{p-1} - 1.$$

Such a prime is called a Wieferich prime. An effective bound on the set of Wieferich primes would yield a new proof to the Fermat-Wiles theorem in the first case (p does not divide xyz).

Infinitely many non-Wieferich primes Silverman (1988)

The *abc* conjecture implies that there are infinitely many non-Wieferich primes.



Nothing is known about the finiteness of the set of Wieferich primes, the only two known examples being 1093 and 3511.

The Erdős-Woods conjecture (1981)

There exists an absolute constant k such that, if x and y are positive integers satisfying

$$\text{Rad}(x+i) = \text{Rad}(y+i)$$

for $i = 0, 1, \dots, k-1$, then $x = y$.



The *abc* conjecture implies Erdős-Woods Langevin (1996)

Already in 1975, Langevin studied the radical of $n(n+k)$ (with $\gcd(n, k) = 1$) using lower bounds for linear forms in logarithms of algebraic numbers (Baker's method)



Dirichlet's approximation theorem (≈ 1830)

For any irrational α there exist infinitely many relatively prime pairs (p, q) such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

This theorem implies that the Pell-Fermat equation

$$x^2 - dy^2 = 1$$

has non-trivial solutions for any squarefree $d > 1$, a result which was previously proved by Lagrange (1766) and extended in a work on quadratic forms by Gauss (1801).



The Thue-Siegel-Roth's theorem (1909, 1921, 1955)

For any irrational algebraic number α and any positive ϵ the set of relatively prime integers p, q such that

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

is finite.



The number fields *abc* conjecture implies a refinement Bombieri (1994)

In the inequality

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

of the Thue-Siegel-Roth theorem, Bombieri shows that the *abc* conjecture allows to replace the exponent ϵ with

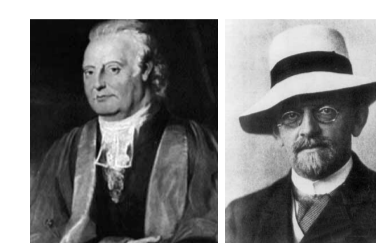
$$\kappa(\log q)^{-1/2} (\log \log q)^{-1}$$

where κ depends only on α .



The Waring-Hilbert theorem (1770, 1909)

For any k there exists $g(k)$ such that each positive integer is a sum of at most $g(k)$ k th powers.



A conjecture on $g(k)$

J. A. Euler (1772): For all $k \geq 1$, $g(k) \geq I(k)$ where $I(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$. Indeed, the integer $2 \lfloor (3/2)^k \rfloor - 1$ is less than 3^k so it must be written so that only powers of 2 and 1 occur, and the most economic expression uses $I(k)$ terms.

Bretschneider's conjecture (1853): $g(k) = I(k)$ for any $k \geq 2$.



Evaluations of $g(k)$ for $k = 2, 3, 4, \dots$

$g(2)=4$	Lagrange	1770
$g(3)=9$	Kempner	1912
$g(4)=19$	Balushbraminian, Dress, Deshouillers	1986
$g(5)=37$	Chen Jingrun	1964
$g(6)=73$	Pillai	1940
$g(7)=143$	Dickson	1936

A sufficient condition Dickson, Pillai (1936)

If k is such that $2^k \{ (3/2)^k \} + \lfloor (3/2)^k \rfloor \leq 2^k - 2$ then Bretschneider's conjecture holds for k .



Mahler's theorem (1957)

The condition of Dickson and Pillai is true for all but a finite set of integers k .



Kubina and Wunderlich (1990) created a fast algorithm to test the conjecture up to large values of k .

Effective bound assuming *abc* (2011)

A discussion between David and Waldschmidt lead to a proof of Mahler's result as a consequence of *abc*. Laisant proved that Bretschneider's conjecture follows from the explicit version of *abc* due to Baker. The same author proved a series of explicit results in a joint work with Shorey.



Baker's explicit version of the *abc* conjecture (2004)

Let (a, b, c) be three integers such that $\gcd(a, b) = 1$ and $c = a + b$. Then

$$c \leq \frac{6}{5} R \frac{(\log R)^2}{\omega!}$$

with $R = \text{Rad}(abc)$ the radical of *abc* and $\omega = \omega(abc)$ the number of distinct prime factors of *abc*.



Siegel's theorem (1929)

Let g be the genus of a smooth algebraic curve in a given coordinate system, with coefficients in a number field K . If $g \geq 2$, then the curve has only finitely many integer points.



The effective *abc* conjecture implies effective Siegel Surroca (2004)

In the proof she uses a theorem of Belyi.



Further consequences of the *abc* conjecture

- The uniform *abc* conjecture for number fields implies a lower bound for the class number of imaginary quadratic fields (Granville and Stark), and Mahler has shown that this implies that the associated L -function has no Siegel zeros.
- Erdős's conjecture on consecutive powerful numbers.
- Dressler's conjecture: between two positive integers having the same prime factors, there is always a prime.
- Squarefree and powerfree values of polynomials.
- Lang's conjectures: lower bounds for heights, number of integral points on elliptic curves.
- Bounds for the order of the Tate-Shafarevich group.
- Vojta's height conjecture for curves.
- Greenberg's conjecture on Iwasawa invariants λ and μ in cyclotomic extensions.
- Frey proved that when the product *abc* is divisible by 16 the degree conjecture and the *abc* conjecture are equivalent.

Vojta's height conjecture (1987)

Vojta stated a conjectural inequality on the height which implies the *abc* conjecture. Another consequence of this inequality is the following. Let K be a number field and S a finite set of absolute values of K . If X is a variety with trivial canonical bundle and D is an effective ample normal crossing divisor, then the S -integral points on the affine variety $X \setminus D$ are not Zariski dense.



The Lang-Faltings theorem (1991)

If X is an abelian variety then the above statement holds.

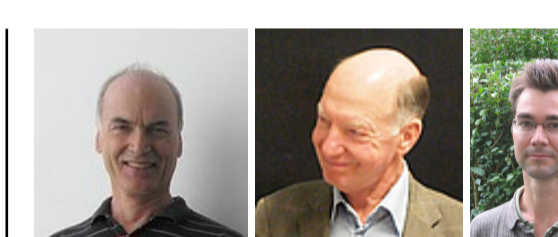
Is the *abc* conjecture optimal? Theorems by Stewart and Tijdeman and later by van Frankenhuijsen (1986, 2012)

Stewart-Tijdeman (1986): For any $\delta > 0$ there are infinitely many triplets (a, b, c) with $\gcd(a, b) = 1$ and $c = a + b$ for which

$$c > R \exp \left((4 - \delta) \frac{(\log R)^{1/2}}{\log \log R} \right),$$

where $R = \text{Rad}(abc)$.

In 2012 van Frankenhuijsen showed that $4 - \delta$ can be replaced by 6.008.



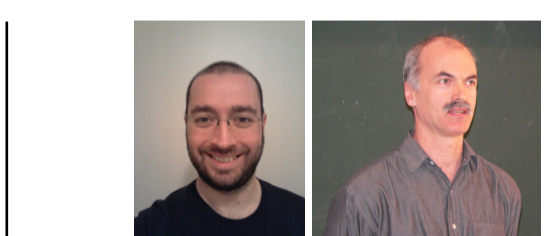
Heuristic: Rad(*a*), Rad(*b*) and Rad(*a* + *b*) are independent Robert, Stewart and Tenenbaum (2014)

For any $\delta > 0$ there exists $\kappa(\delta) > 0$ such that for any *abc* triple with $R = \text{Rad}(abc) > 8$,

$$c < \kappa(\delta) R \exp \left((4\sqrt{3} + \delta) \left(\frac{\log R}{\log \log R} \right)^{1/2} \right).$$

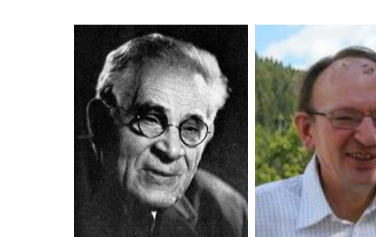
Further, there exist infinitely many triples (a, b, c) such that $\gcd(a, b) = 1$ and $c = a + b$ for which

$$c > R \exp \left((4\sqrt{3} - \delta) \left(\frac{\log R}{\log \log R} \right)^{1/2} \right).$$



Mordell-Faltings theorem (1922, 1983)

Let g be the genus of an equation $P(x, y) = 0$ of coefficients in \mathbb{Q} . If $g \geq 2$ then the equation has only finitely many solutions with $(x, y) \in \mathbb{Q}^2$.



The effective *abc* implies effective Mordell Elkies (1991)

The effective version of Mordell's conjectures amounts to giving bounds on the heights of rational points.

Under the (effective) *abc* conjecture for a number field K then the (effective) conjecture of Mordell holds for the same K .



In the quest for examples

Bosman, Brøberg, Browkin, Brzezinski, Dokchitser, Elkies, Kanapka, Frey, Gang, Hegner, Nitaj, Reysat, de Riele, P. Montgomery, Schulmeister, Rosenheirich, Wisser, de Weger.

For any relatively prime positive integers a, b, c such that $a + b = c$ we set

$$\lambda(a, b, c) = \frac{\log c}{\log(\text{Rad}(abc))}.$$

The largest known examples are:

$a + b = c$	$\lambda(a, b, c)$	author
$2 + 3^{10} \cdot 100 = 23^5$	1.6290...	Reysat
$11^2 + 3^5 5^2 7^3 = 2^4 \cdot 23$	1.6250...	de Weger
$19 \cdot 1307 + 7 \cdot 29^2 \cdot 31^4 = 2^8 \cdot 3^2 \cdot 1.6234...$	1.6234...	Browkin, Brzezinski

Demeyer, Nitaj, de Weger, de Smit, H. Lenstra, Palenstijn, Rubin, Calvo, Wrobenksi, For any relatively prime positive integers a, b, c such that $a + b = c$ we set

$$\rho(a, b, c) = \frac{\log(abc)}{\log(\text{Rad}(abc))}.$$

The largest known examples are:

$a + b = c$	$\rho(a, b, c)$	author
$13 \cdot 19^2 + 2^8 \cdot 5 = 9^{13} \cdot 11^2 \cdot 31$	4.1190...	Nitaj
$2^5 \cdot 11^2 \cdot 19^2 + 5^3 \cdot 37^2 \cdot 47 = 3^7 \cdot 7^{11} \cdot 743$	4.2680...	Nitaj
$2^{19} \cdot 13 \cdot 103 + 7^{11} = 3^{11} \cdot 5^3 \cdot 11^2$	4.2678...	de Weger

The *ABC* conjecture for polynomials Hurwitz, Stothers and Mason ($\approx 1900, 1981, 1984$)

Let K be an algebraically closed field of characteristic zero. For any polynomial $P = \prod_{i=1}^n (x - \alpha_i)$ call the radical of P the polynomial $\text{Rad}(P) = \prod_{i=1}^n (x - \alpha_i)$. Then for any three relatively prime polynomials A, B, C such that $A + B = C$ we have