On the abc Conjecture and some of its consequences

by

Michel Waldschmidt

Sorbonne University
Institut Mathématique de Jussieu

http://www.imj-prg.fr/~michel.waldschmidt/

Abstract

We explain the statement of the abc Conjecture proposed by Oesterlé and Masser in the mid 80's and we give a collection of easy to state consequences of this conjecture. It will not include an introduction to the Inter-universal Teichmüller Theory of Shinichi Mochizuki.

Abstract (continued)

According to *Nature News*, 10 September 2012, quoting Dorian Goldfeld, the abc Conjecture is "the most important unsolved problem in Diophantine analysis". It is a kind of grand unified theory of Diophantine curves : "The remarkable thing about the abc Conjecture is that it provides a way of reformulating an infinite number of Diophantine problems," says Goldfeld, "and, if it is true, of solving them." Proposed independently in the mid-80s by David Masser of the University of Basel and Joseph Oesterlé of Pierre et Marie Curie University (Paris 6), the abc Conjecture describes a kind of balance or tension between addition and multiplication, formalizing the observation that when two numbers a and b are divisible by large powers of small primes, $a + b$ tends to be divisible by small powers of large primes. The abc Conjecture implies – in a few lines – the proofs of many difficult theorems and outstanding conjectures in Diophantine equations– including Fermat's Last Theorem.

As simple as abc

American Broadcasting Company

http://fr.wikipedia.org/wiki/American_Broadcasting_Company

Annapurna Base Camp, October 22, 2014

Mt. Annapurna (8091m) is the 10th highest mountain in the world and the journey to its base camp is one of the most popular treks on earth.

http://www.himalayanglacier.com/trekking-in-nepal/160/annapurna-base-camp-trek.htm

The radical of a positive integer

According to the fundamental theorem of arithmetic, any integer $n \geq 2$ can be written as a product of prime numbers :

$$n = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_t}^{a_t}.$$

The *radical* (also called *kernel*) $\mathrm{Rad}(n)$ of n is the product of the distinct primes dividing n :

$$\mathrm{Rad}(n) = p_1 p_2 \cdots p_t.$$

$$\mathrm{Rad}(n) \leq n.$$

Examples : $\mathrm{Rad}(2^a) = 2$,

$$\mathrm{Rad}(60\,500) = \mathrm{Rad}(2^2 \cdot 5^3 \cdot 11^2) = 2 \cdot 5 \cdot 11 = 110,$$

$$\mathrm{Rad}(82\,852\,996\,681\,926) = 2 \cdot 3 \cdot 23 \cdot 109 = 15\,042.$$

abc–triples

An abc–triple is a triple of three positive integers a, b, c which are coprime, $a < b$ and that $a + b = c$.

Examples:

$$1 + 2 = 3, \quad 1 + 8 = 9,$$

$$1 + 80 = 81, \quad 4 + 121 = 125,$$

$$2 + 3^{10} \cdot 109 = 23^5, \qquad 11^2 + 3^2 5^6 7^3 = 2^{21} \cdot 23.$$

13 abc–triples with $c < 10$

a, b, c are coprime, $1 \leq a < b$, $a + b = c$ and $c \leq 9$.

$1+2=3$			
$1+3=4$			
$1+4=5$	$2+3=5$		
$1+5=6$			
$1+6=7$	$2+5=7$	$3+4=7$	
$1+7=8$		$3+5=8$	
$1+8=9$	$2+7=9$		$4+5=9$

Radical of the abc–triples with $c < 10$

$\mathrm{Rad}(1\cdot 2\cdot 3) = 6$		
$\mathrm{Rad}(1\cdot 3\cdot 4) = 6$		
$\mathrm{Rad}(1\cdot 4\cdot 5) = 10$	$\mathrm{Rad}(2\cdot 3\cdot 5) = 30$	
$\mathrm{Rad}(1\cdot 5\cdot 6) = 30$		
$\mathrm{Rad}(1\cdot 6\cdot 7) = 42$	$\mathrm{Rad}(2\cdot 5\cdot 7) = 70$	$\mathrm{Rad}(3\cdot 4\cdot 7) = 42$
$\mathrm{Rad}(1\cdot 7\cdot 8) = 14$		$\mathrm{Rad}(3\cdot 5\cdot 8) = 30$
$\boxed{\mathrm{Rad}(1\cdot 8\cdot 9) = 6}$	$\mathrm{Rad}(2\cdot 7\cdot 9) = 54$	$\mathrm{Rad}(4\cdot 5\cdot 9) = 30$

$a = 1$, $b = 8$, $c = 9$, $a + b = c$, $\gcd = 1$, $\mathrm{Rad}(abc) < c$.

abc–hits

Following F. Beukers, an abc–hit is an abc–triple such that $\mathrm{Rad}(abc) < c$.

http://www.staff.science.uu.nl/~beuke106/ABCpresentation.pdf

Example: $(1, 8, 9)$ is an abc–hit since $1 + 8 = 9$, $\gcd(1, 8, 9) = 1$ and

$$\mathrm{Rad}(1 \cdot 8 \cdot 9) = \mathrm{Rad}(2^3 \cdot 3^2) = 2 \cdot 3 = 6 < 9.$$

On the condition that a, b, c are relatively prime

Starting with $a + b = c$, multiply by a power of a divisor $d > 1$ of abc and get

$$ad^\ell + bd^\ell = cd^\ell.$$

The radical did not increase : the radical of the product of the three numbers ad^ℓ, bd^ℓ and cd^ℓ is nothing else than $\mathrm{Rad}(abc)$; but c is replaced by cd^ℓ.

For ℓ sufficiently large, cd^ℓ is larger than $\mathrm{Rad}(abc)$.

But $(ad^\ell, bd^\ell, cd^\ell)$ is not an abc–hit.

It would be too easy to get examples without the condition that a, b, c are relatively prime.

Some abc–hits

$(1, 80, 81)$ is an abc–hit since $1 + 80 = 81$, $\gcd(1, 80, 81) = 1$ and

$$\mathrm{Rad}(1 \cdot 80 \cdot 81) = \mathrm{Rad}(2^4 \cdot 5 \cdot 3^4) = 2 \cdot 5 \cdot 3 = 30 < 81.$$

$(4, 121, 125)$ is an abc–hit since $4 + 121 = 125$, $\gcd(4, 121, 125) = 1$ and

$$\mathrm{Rad}(4 \cdot 121 \cdot 125) = \mathrm{Rad}(2^2 \cdot 5^3 \cdot 11^2) = 2 \cdot 5 \cdot 11 = 110 < 125.$$

Further abc–hits

- $$(2, 3^{10} \cdot 109, 23^5) = (2, 6\,436\,341, 6\,436\,343)$$

is an abc–hit since $2 + 3^{10} \cdot 109 = 23^5$ and
$\mathrm{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 15\,042 < 23^5 = 6\,436\,343.$

- $$(11^2, 3^2 \cdot 5^6 \cdot 7^3, 2^{21} \cdot 23) = (121, 48\,234\,275, 48\,234\,496)$$

is an abc–hit since $11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$ and
$\mathrm{Rad}(2^{21} \cdot 3^2 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 23) = 53\,130 < 2^{21} \cdot 23 = 48\,234\,496.$

- $$(1, 5 \cdot 127 \cdot (2 \cdot 3 \cdot 7)^3, 19^6) = (1, 47\,045\,880, 47\,045\,881)$$

is an abc–hit since $1 + 5 \cdot 127 \cdot (2 \cdot 3 \cdot 7)^3 = 19^6$ and
$\mathrm{Rad}(5 \cdot 127 \cdot (2 \cdot 3 \cdot 7)^3 \cdot 19^6) = 5 \cdot 127 \cdot 2 \cdot 3 \cdot 7 \cdot 19 = 506\,730.$

abc–triples and abc–hits

Among $15 \cdot 10^6$ abc–triples with $c < 10^4$, we have 120 abc–hits.

Among $380 \cdot 10^6$ abc–triples with $c < 5 \cdot 10^4$, we have 276 abc–hits.

More abc–hits

Recall the abc–hit $(1, 80, 81)$, where $81 = 3^4$.

$$(1, 3^{16} - 1, 3^{16}) = (1, 43\,046\,720, 43\,046\,721)$$

is an abc–hit.

Proof.

$$\begin{aligned} 3^{16} - 1 &= (3^8 - 1)(3^8 + 1) \\ &= (3^4 - 1)(3^4 + 1)(3^8 + 1) \\ &= (3^2 - 1)(3^2 + 1)(3^4 + 1)(3^8 + 1) \\ &= (3 - 1)(3 + 1)(3^2 + 1)(3^4 + 1)(3^8 + 1) \end{aligned}$$

is divisible by 2^6. (Quotient : $672\,605$).

Hence

$$\mathrm{Rad}((3^{16} - 1) \cdot 3^{16}) \le \frac{3^{16} - 1}{2^6} \cdot 2 \cdot 3 < 3^{16}.$$

Infinitely many abc–hits

Proposition. *There are infinitely many abc–hits.*

Take $k \geq 1$, $a = 1$, $c = 3^{2^k}$, $b = c - 1$.

Lemma. 2^{k+2} *divides* $3^{2^k} - 1$.

Proof : Induction on k using

$$3^{2^k} - 1 = (3^{2^{k-1}} - 1)(3^{2^{k-1}} + 1).$$

Consequence :

$$\mathrm{Rad}((3^{2^k} - 1) \cdot 3^{2^k}) \leq \frac{3^{2^k} - 1}{2^{k+1}} \cdot 3 < 3^{2^k}.$$

Hence

$$(1, 3^{2^k} - 1, 3^{2^k})$$

is an abc–hit.

Infinitely many abc–hits

This argument shows that there exist infinitely many abc–triples such that

$$c > \frac{1}{6 \log 3} R \log R$$

with $R = \mathrm{Rad}(abc)$.

`Question` : *Are there abc–triples for which $c > \mathrm{Rad}(abc)^2$?*

`We do not know the answer.`

Examples

When a, b and c are three positive relatively prime integers satisfying $a+b=c$, define

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

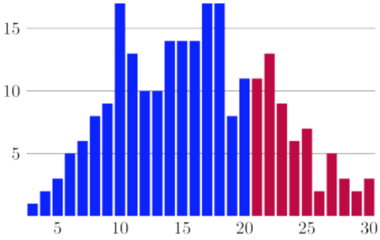
Here are the two largest known values for $\lambda(abc)$

$a+b$	$=$	c	$\lambda(a,b,c)$	authors
$2+3^{10}\cdot 109$	$=$	23^5	$1.629912\ldots$	É. Reyssat
$11^2+3^25^67^3$	$=$	$2^{21}\cdot 23$	$1.625990\ldots$	B.M. de Weger

Number of digits of the good abc–triples

At the date of September 11, 2008, 217 abc triples with $\lambda(a,b,c) \geq 1.4$ were known. https://nitaj.users.lmno.cnrs.fr/tableabc.pdf

At the date of August 1, 2015, 238 were known. On May 15, 2017, the total is 240. http://www.math.leidenuniv.nl/~desmit/abc/index.php?sort=1



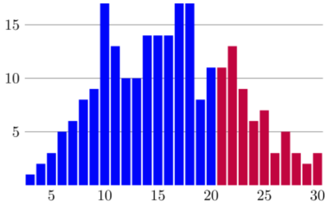
Contributions by A. Nitaj, T. Dokchitser, J. Browkin, J. Brzezinski, F. Rubin, T. Schulmeiss, B. de Weger, J. Demeyer, K. Visser, P. Montgomery, H. Te Riele, A. Rosenheinrich, J. Calvo, M. Hegner, J. Wrobenski...

The list up to 20 digits is complete.

Bart De Smit February 2022

Bart de Smit / ABC triples intro | by size | by quality | by merit | unbeaten

There are currently 241 known ABC triples of quality at least 1.4, which are often called *good* ABC triples. The next plot counts them by their number of digits. For instance, the graph says that there are 11 good triples where *c* has 20 digits.



The method of ABC@home finds all ABC triples for a given lower bound on the quality and an upper bound on the size. By a run of an early implementation of **Jeroen Demeyer** from Gent in June 2007 we know that the list of good triples up to 20 digits is now complete. So when new good triples are discovered, only the red part in the plot above will grow. Demeyer's search turned up nine new triples with *c* of at most 20 digits.

By a completely independent method, **Frank Rubin** has found a number of new good ABC triples in the last few years, including most of the good triples with more than 20 digits, and all of the good triples with 30 digits.

Eric Reyssat : $2 + 3^{10} \cdot 109 = 23^5$

Example of Reyssat $2 + 3^{10} \cdot 109 = 23^5$

$a + b = c$

$$a = 2, \qquad b = 3^{10} \cdot 109, \qquad c = 23^5 = 6\,436\,343,$$

$$\mathrm{Rad}(abc) = \mathrm{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 2 \cdot 3 \cdot 109 \cdot 23 = 15\,042,$$

$$\lambda(a,b,c) = \frac{\log c}{\log \mathrm{Rad}(abc)} = \frac{5 \log 23}{\log 15\,042} \simeq 1.62991.$$

Continued fraction

$$2 + 109 \cdot 3^{10} = 23^5$$

Continued fraction of $109^{1/5}$: $[2; 1, 1, 4, 77733, \dots]$,
approximation : $[2; 1, 1, 4] = 23/9$

$$109^{1/5} = 2.555\,555\,39\dots$$
$$\frac{23}{9} = 2.555\,555\,55\dots$$

N. A. Carella. *Note on the ABC Conjecture*
http://arXiv.org/abs/math/0606221

Benne de Weger : $11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$

$$\mathrm{Rad}(2^{21} \cdot 3^2 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 23) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 53\,130.$$

$$2^{21} \cdot 23 = 48\,234\,496 = (53\,130)^{1.625990\ldots}$$

Explicit abc Conjecture

According to S. Laishram and T. N. Shorey, an explicit version, due to A. Baker, of the abc Conjecture, yields

$$c < \mathrm{Rad}(abc)^{7/4}$$

for any abc–triple (a, b, c).

The abc Conjecture

Recall that for a positive integer n, the *radical* of n is

$$\mathrm{Rad}(n) = \prod_{p|n} p.$$

abc **Conjecture**. *Let $\varepsilon > 0$. Then the set of abc triples for which*

$$c > \mathrm{Rad}(abc)^{1+\varepsilon}$$

is finite.

Equivalent statement : *For each $\varepsilon > 0$ there exists $\kappa(\varepsilon)$ such that, if a, b and c in $\mathbf{Z}_{>0}$ are relatively prime and satisfy $a + b = c$, then*

$$c < \kappa(\varepsilon)\mathrm{Rad}(abc)^{1+\varepsilon}.$$

Lower bound for the radical of abc

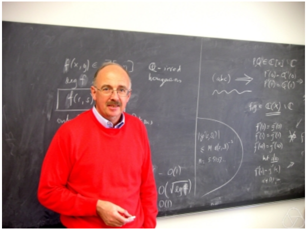
The abc Conjecture is a **lower bound** for the radical of the product abc :

abc **Conjecture**. *For any* $\varepsilon > 0$, *there exist* $\kappa(\varepsilon)$ *such that, if* a, b *and* c *are relatively prime positive integers which satisfy* $a + b = c$, *then*

$$\mathrm{Rad}(abc) > \kappa(\varepsilon) c^{1-\varepsilon}.$$

The *abc* Conjecture of Oesterlé and Masser

Joseph Oesterlé



David Masser

The *abc* Conjecture resulted from a discussion between J. Oesterlé and D. W. Masser in the mid 1980's.

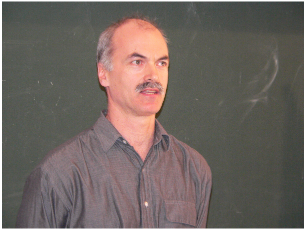
C.L. Stewart and Yu Kunrui

Best known non conditional result : C.L. Stewart and Yu Kunrui (1991, 2001) :

$$\log c \le \kappa R^{1/3}(\log R)^3$$

with $R = \mathrm{Rad}(abc)$:

$$c \le e^{\kappa R^{1/3}(\log R)^3}.$$



Cam. L. Stewart

Yu Kunrui

Szpiro's Conjecture

J. Oesterlé and A. Nitaj proved that the abc Conjecture implies a previous conjecture by L. Szpiro on the conductor of elliptic curves.

Lucien Szpiro
1941 - 2020

Given any $\varepsilon > 0$, there exists a constant $C(\varepsilon) > 0$ such that, for every elliptic curve with minimal discriminant Δ and conductor N,

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

Szpiro's Conjecture

Conversely, J. Oesterlé proved in 1988 that the conjecture of L. Szpiro implies a weak form of the abc conjecture with $1 - \epsilon$ replaced by $(5/6) - \epsilon$.

Joseph Oesterlé

Further examples

When a, b and c are three positive relatively prime integers satisfying $a+b=c$, define

$$\varrho(a,b,c)=\frac{\log abc}{\log \operatorname{Rad}(abc)}\cdot$$

Here are the two largest known values for $\varrho(abc)$, found by A. Nitaj.

$a+b$	$=$	c	$\varrho(a,b,c)$
$13\cdot 19^6+2^{30}\cdot 5$	$=$	$3^{13}\cdot 11^2\cdot 31$	$4.41901\ldots$
$2^5\cdot 11^2\cdot 19^9+5^{15}\cdot 37^2\cdot 47$	$=$	$3^7\cdot 7^{11}\cdot 743$	$4.26801\ldots$

On March 19, 2003, 47 abc triples were known with $0<a<b<c$, $a+b=c$ and $\gcd(a,b)=1$ satisfying $\varrho(a,b,c)>4$.

https://nitaj.users.lmno.cnrs.fr/tableszpiro.pdf

Abderrahmane Nitaj عبدالرحمان نتاج

https://nitaj.users.lmno.cnrs.fr/abc.html

THE ABC CONJECTURE HOME PAGE

ABC

La conjecture abc est aussi difficile que la conjecture ... xyz. (P. Ribenboin
(read the story)

The abc conjecture is the most important unsolved problem in diophantin
analysis. (D. Goldfeld)

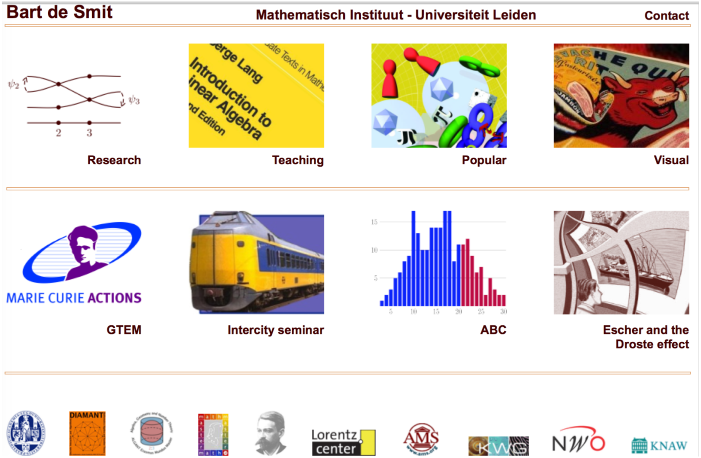
Created and maintained by Abderrahmane Nitaj

Last updated May 27, 2010

Index

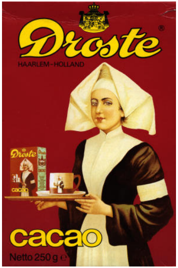
- **The *abc* conjecture**
- **Generalizations**
- **Consequences**
- **Tables**
  - The top ten good *abc* examples
  - The top ten good *abc*-Szpiro examples
  - The top ten good algebraic *abc* examples
  - New good *abc* examples **new**
  - New hunters of *abc* examples **rekenmeemetabc, abc@home** **new**
  - Largest good *abc* examples **new**
  - The list of good triples up to 20 digits is now complete **new**
- **Bibliography**

Bart de Smit



http://www.math.leidenuniv.nl/~desmit/abc/

Escher and the Droste effect



http://escherdroste.math.leidenuniv.nl/

www.abcathome.com

ABC@home is an educational and non-profit distributed computing project finding abc-triples related to the ABC conjecture.

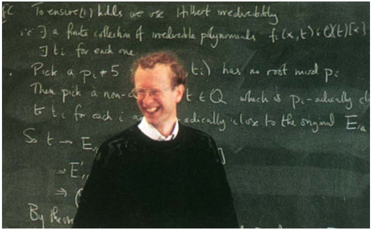
The ABC conjecture is currently one of the greatest open problems in mathematics. If it is proven to be true, a lot of other open problems can be answered directly from it.

The ABC conjecture is one of the greatest open mathematical questions, one of the holy grails of mathematics. It will teach us something about our very own numbers.

Fermat's Last Theorem $x^n + y^n = z^n$ for $n \geq 6$

Pierre de Fermat

1601 – 1665



Andrew Wiles

Solution in 1994

Fermat's last Theorem for $n \geq 6$ as a consequence of the abc Conjecture

Assume $x^n + y^n = z^n$ with $\gcd(x, y, z) = 1$ and $x < y$. Then (x^n, y^n, z^n) is an abc–triple with

$$\mathrm{Rad}(x^n y^n z^n) \leq xyz < z^3.$$

If the explicit abc Conjecture $c < \mathrm{Rad}(abc)^2$ is true, then one deduces

$$z^n < z^6,$$

hence $n \leq 5$ (and therefore $n \leq 2$).

Square, cubes. . .

- A perfect power is an integer of the form a^b where $a \geq 1$ and $b > 1$ are positive integers.
- Squares :

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 144,\ 169,\ 196, \dots$$

- Cubes :

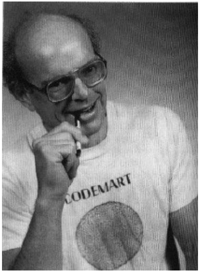
$$1,\ 8,\ 27,\ 64,\ 125,\ 216,\ 343,\ 512,\ 729,\ 1\,000,\ 1\,331, \dots$$

- Fifth powers :

$$1,\ 32,\ 243,\ 1\,024,\ 3\,125,\ 7\,776,\ 16\,807,\ 32\,768, \dots$$

Perfect powers

$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125,$
$128, 144, 169, 196, 216, 225, 243, 256, 289, 324, 343,$
$361, 400, 441, 484, 512, 529, 576, 625, 676, 729, 784, \ldots$



Neil J. A. Sloane's encyclopaedia
http://oeis.org/A001597

Nearly equal perfect powers

- Difference 1 : $(8, 9)$
- Difference 2 : $(25, 27), \dots$
- Difference 3 : $(1, 4)$, $(125, 128), \dots$
- Difference 4 : $(4, 8)$, $(32, 36)$, $(121, 125), \dots$
- Difference 5 : $(4, 9)$, $(27, 32)$,...

Two conjectures

Subbayya Sivasankaranarayana Pillai (1901-1950)

Eugène Charles Catalan (1814 – 1894)

• Catalan's Conjecture : In the sequence of perfect powers, $8, 9$ is the only example of consecutive integers.

• Pillai's Conjecture : In the sequence of perfect powers, the difference between two consecutive terms tends to infinity.

Pillai's Conjecture :

- Pillai's Conjecture : In the sequence of perfect powers, the difference between two consecutive terms tends to infinity.

- Alternatively : Let k be a positive integer. The equation

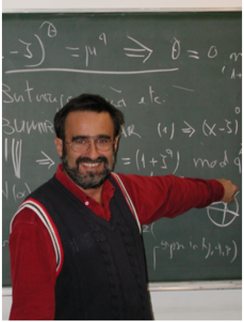
$$x^p - y^q = k,$$

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

Results

P. Mihăilescu, 2002.

Catalan was right : *the equation* $x^p - y^q = 1$ *where the unknowns* x, y, p *and* q *take integer values, all* ≥ 2, *has only one solution* $(x, y, p, q) = (3, 2, 2, 3)$.



Previous work on Catalan's Conjecture

J.W.S. Cassels

1922 - 2015

Rob Tijdeman

Michel Langevin

$$x^p < y^q < \exp\exp\exp\exp(730)$$

Previous work on Catalan's Conjecture

Maurice Mignotte

Yuri Bilu

Pillai's conjecture and the abc Conjecture

There is no value of $k \geq 2$ for which one knows that Pillai's equation $x^p - y^q = k$ has only finitely many solutions.

Pillai's conjecture as a consequence of the abc Conjecture : *if* $x^p \neq y^q$, *then*

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

with

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

Lower bounds for linear forms in logarithms

- A special case of my conjectures with S. Lang for

$$|q \log y - p \log x|$$

yields

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

with

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

Serge Lang
(1927 - 2005)

Not a consequence of the abc Conjecture

$p = 3$, $q = 2$

Hall's Conjecture (1971) :

if $x^3 \neq y^2$, *then*

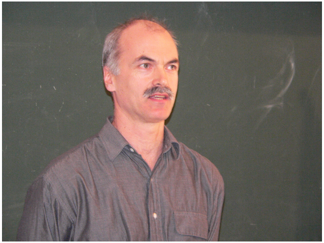
$$|x^3 - y^2| \geq c \max\{x^3, y^2\}^{1/6}.$$

Marshall Hall

1910 - 1990

http://en.wikipedia.org/wiki/Marshall_Hall,_Jr

Conjecture of F. Beukers and C.L. Stewart (2010)



Let p, q *be coprime integers with* $p > q \geq 2$. *Then, for any* $c > 0$, *there exist infinitely many positive integers* x, y *such that*

$$0 < |x^p - y^q| < c \max\{x^p, y^q\}^\kappa$$

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

Generalized Fermat's equation $x^p + y^q = z^r$

Consider the equation $x^p + y^q = z^r$ in positive integers (x, y, z, p, q, r) such that x, y, z relatively prime and p, q, r are ≥ 2.

If

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \geq 1,$$

then (p, q, r) is a permutation of one of

$$(2, 2, k), \quad (2, 3, 3), \quad (2, 3, 4), \quad (2, 3, 5),$$

$$(2, 4, 4), \quad (2, 3, 6), \quad (3, 3, 3)$$

and in each case the set of solutions (x, y, z) is known (for some of these values there are infinitely many solutions).

Frits Beukers and Don Zagier

For

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

10 primitive solutions (x, y, z, p, q, r) (up to obvious symmetries) to the equation

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

are known.

Primitive solutions to $x^p + y^q = z^r$

Condition : x, y, z are relatively prime

Trivial example of a non primitive solution : $2^p + 2^p = 2^{p+1}$.

`Exercise` (Henri Darmon, Claude Levesque) : for any pairwise relatively prime (p, q, r), there exist positive integers x, y, z with $x^p + y^q = z^r$.

`Hint` :

$$\left(17 \times 71^{21}\right)^3 + \left(2 \times 71^9\right)^7 = \left(71^{13}\right)^5.$$

Generalized Fermat's equation

For

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

the equation

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

has the following 10 solutions with x, y, z relatively prime :

$$1+2^3=3^2, \quad 2^5+7^2=3^4, \quad 7^3+13^2=2^9, \quad 2^7+17^3=71^2,$$

$$3^5+11^4=122^2, \quad 33^8+1\,549\,034^2=15\,613^3,$$

$$1\,414^3+2\,213\,459^2=65^7, \quad 9\,262^3+15\,312\,283^2=113^7,$$

$$17^7+76\,271^3=21\,063\,928^2, \quad 43^8+96\,222^3=30\,042\,907^2.$$

Conjecture of Beal, Granville and Tijdeman–Zagier



The equation $x^p + y^q = z^r$ has no solution in positive integers (x, y, z, p, q, r) with each of p, q and r at least 3 and with x, y, z relatively prime.

http://mathoverflow.net/

Andrew Beal

Find a solution with all exponents at least 3, or prove that there is no such solution.

http://www.forbes.com/2009/04/03/banking-andy-beal-business-wall-street-beal.html

Beal's Prize

Mauldin, R. D. – *A generalization of Fermat's last theorem : the Beal Conjecture and prize problem.* Notices Amer. Math. Soc. **44** N°11 (1997), 1436–1437.

> **The prize**. Andrew Beal is very generously offering a prize of $5,000 for the solution of this problem. The value of the prize will increase by $5,000 per year up to $50,000 until it is solved. The prize committee consists of Charles Fefferman, Ron Graham, and R. Daniel Mauldin, who will act as the chair of the committee. All proposed solutions and inquiries about the prize should be sent to Mauldin.

Beal's Prize : $1,000,000\$$ US

An AMS-appointed committee will award this prize for either a proof of, or a counterexample to, the Beal Conjecture published in a refereed and respected mathematics publication. The prize money – currently US$1,000,000 – is being held in trust by the AMS until it is awarded. Income from the prize fund is used to support the annual Erdős Memorial Lecture and other activities of the Society.

One of Andrew Beal's goals is to inspire young people to think about the equation, think about winning the offered prize, and in the process become more interested in the field of mathematics.

http://www.ams.org/profession/prizes-awards/ams-supported/beal-prize

Henri Darmon, Andrew Granville

"Fermat-Catalan" Conjecture (H. Darmon and A. Granville), consequence of the abc Conjecture : *the set of solutions* (x, y, z, p, q, r) *to* $x^p + y^q = z^r$ *with* x, y, z *relatively prime and* $(1/p) + (1/q) + (1/r) < 1$ *is finite.*

Hint: $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ implies $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq \frac{41}{42}$.

1995 (H. Darmon and A. Granville) : unconditionally, for fixed (p, q, r), only finitely many (x, y, z).

Henri Darmon, Loïc Merel : $(p, p, 2)$ and $(p, p, 3)$

Unconditional results by H. Darmon and L. Merel (1997) :
For $p \geq 4$, the equation $x^p + y^p = z^2$ has no solution in relatively prime positive integers x, y, z.
For $p \geq 3$, the equation $x^p + y^p = z^3$ has no solution in relatively prime positive integers x, y, z.

Fermat's Little Theorem

For $a > 1$, any prime p not dividing a divides $a^{p-1} - 1$.

Hence if p is an odd prime, then p divides $2^{p-1} - 1$.

Pierre de Fermat

1601 – 1665

Wieferich primes (1909) : p^2 divides $2^{p-1} - 1$

The only known *Wieferich primes* are 1093 and 3511. These are the only ones below $4 \cdot 10^{12}$.

Infinitely many primes are not Wieferich assuming abc

Joseph H. Silverman

J.H. Silverman : if the abc Conjecture is true, given a positive integer $a > 1$, there exist infinitely many primes p such that p^2 does not divide $a^{p-1} - 1$.

Nothing is known about the finiteness of the set of Wieferich primes.

Consecutive integers with the same radical

Notice that

$$75 = 3 \cdot 5^2 \quad \text{and} \quad 1215 = 3^5 \cdot 5, s$$

hence

$$\mathrm{Rad}(75) = \mathrm{Rad}(1215) = 3 \cdot 5 = 15.$$

But also

$$76 = 2^2 \cdot 19 \quad \text{and} \quad 1216 = 2^6 \cdot 19$$

have the same radical

$$\mathrm{Rad}(76) = \mathrm{Rad}(1216) = 2 \cdot 19 = 38.$$

Consecutive integers with the same radical

For $k \geq 1$, the two numbers

$$x = 2^k - 2 = 2(2^{k-1} - 1)$$

and

$$y = (2^k - 1)^2 - 1 = 2^{k+1}(2^{k-1} - 1)$$

have the same radical, and also

$$x + 1 = 2^k - 1 \quad \text{and} \quad y + 1 = (2^k - 1)^2$$

have the same radical.

Consecutive integers with the same radical

Are there further examples of $x \neq y$ with

$$\mathrm{Rad}(x) = \mathrm{Rad}(y) \quad \text{and} \quad \mathrm{Rad}(x+1) = \mathrm{Rad}(y+1)?$$

Is–it possible to find two distinct integers x, y such that

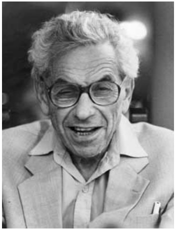
$$\mathrm{Rad}(x) = \mathrm{Rad}(y),$$

$$\mathrm{Rad}(x+1) = \mathrm{Rad}(y+1)$$

and

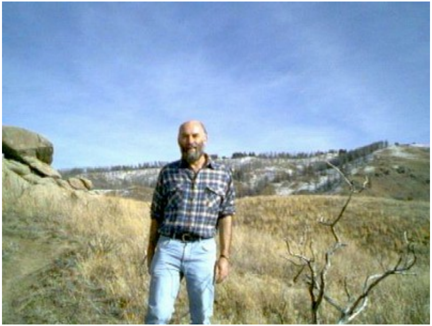
$$\mathrm{Rad}(x+2) = \mathrm{Rad}(y+2)?$$

Erdős – Woods Conjecture



Paul Erdős

1913 - 1996



http://school.maths.uwa.edu.au/~woods/

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

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

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

Erdős – Woods as a consequence of abc

M. Langevin : The abc Conjecture implies that there exists an absolute constant k such that, if x and y are positive integers satisfying

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

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

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

A factorial as a product of factorials

For $n > a_1 \geq a_2 \geq \cdots \geq a_t > 1$, $t > 1$, consider

$$a_1!a_2!\cdots a_t! = n!$$

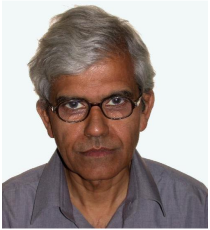
Trivial solutions :

$2^r! = (2^r - 1)!2!^r$ with $r \geq 2$.

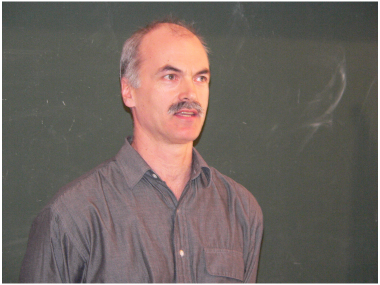
Non trivial solutions :

$7!3!22! = 9!$, $7!6! = 10!$, $7!5!3! = 10!$, $14!5!2! = 16!$.

Saranya Nair and Tarlok Shorey : The effective abc conjecture implies Hickerson's conjecture that the largest non-trivial solution is given by $n = 16$.



Is abc Conjecture optimal ?



Let $\delta > 0$. In 1986, C.L. Stewart and R. Tijdeman proved that there are infinitely many abc–triples for which

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

Better than $c > R \log R$.

Conjectures by Machiel van Frankenhuijsen, Olivier Robert, Cam Stewart and Gérald Tenenbaum

Let $\varepsilon > 0$. There exists $\kappa(\varepsilon) > 0$ such that for any abc triple with $R = \mathrm{Rad}(abc) > 8$,

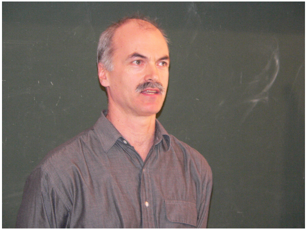
$$c < \kappa(\varepsilon) R \exp\left((4\sqrt{3} + \varepsilon) \left(\frac{\log R}{\log\log R} \right)^{1/2} \right).$$

Further, there exist infinitely many abc–triples for which

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

Machiel van Frankenhuijsen, Olivier Robert, Cam Stewart and Gérald Tenenbaum





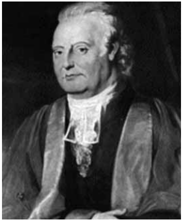

Heuristic assumption

Whenever a and b are coprime positive integers, $R(a+b)$ is independent of $R(a)$ and $R(b)$.

O. Robert, C.L. Stewart and G. Tenenbaum, *A refinement of the abc conjecture*, Bull. London Math. Soc., Bull. London Math. Soc. (2014) **46** (6) : 1156-1166.
http://blms.oxfordjournals.org/content/46/6/1156.full.pdf

http://iecl.univ-lorraine.fr/~Gerald.Tenenbaum/PUBLIC/Prepublications_et_publications/abc.pdf

Waring's Problem



Edward Waring
(1736 - 1798)

In 1770, a few months before J.L. Lagrange solved a conjecture of Bachet (1621) and Fermat (1640) by proving that every positive integer is the sum of at most four squares of integers, E. Waring wrote :

"Omnis integer numerus vel est cubus, vel e duobus, tribus, 4, 5, 6, 7, 8, vel novem cubis compositus, est etiam quadrato-quadratus vel e duobus, tribus, &, usque ad novemdecim compositus, & sic deinceps"

"Every integer is a cube or the sum of two, three, ...nine cubes ; every integer is also the square of a square, or the sum of up to nineteen such ; and so forth. Similar laws may be affirmed for the correspondingly defined numbers of quantities of any like degree."

Waring's functions $g(k)$ and $G(k)$

• Waring's function g is defined as follows : *For any integer* $k \geq 2$, $g(k)$ *is the least positive integer* s *such that any positive integer* N *can be written* ${x_1}^k + \cdots + {x_s}^k$.

• Waring's function G is defined as follows : *For any integer* $k \geq 2$, $G(k)$ *is the least positive integer* s *such that any sufficiently large positive integer* N *can be written* ${x_1}^k + \cdots + {x_s}^k$.

J.L. Lagrange : $g(2) = 4$.

$g(2) \le 4$: any positive number is a sum of at most 4 squares :
$n = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2$.

$g(2) \ge 4$: there are positive numbers (for instance 7) which are not sum of 3 squares.

Joseph-Louis Lagrange
(1736 – 1813)

Lower bounds are easy, not upper bounds.

$n = {x_1}^4 + \cdots + x_{19}^4 : g(4) = 19$

Any positive integer is the sum of at most 19 *biquadrates*
R. Balasubramanian, J-M. Deshouillers, F. Dress (1986).

François Dress, R. Balasubramanian, Jean-Marc Deshouillers

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

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

$g(k) \geq I(k)$

For each integer $k \geq 2$, define
$I(k) = 2^k + \lfloor (3/2)^k \rfloor - 2.$
Then $g(k) \geq I(k)$.

(J. A. Euler, son of Leonhard Euler).

Johann Albrecht Euler
1734 - 1800

Conjecture (C.A. Bretschneider, 1853) : $g(k) = I(k)$ for any $k \geq 2$.
True for $4 \leq k \leq 471\ 600\ 000$.

Mahler's contribution

- The ideal Waring's Theorem

$$g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$$

holds for all sufficiently large k.

Kurt Mahler
(1903 - 1988)

Waring's Problem and the abc Conjecture

S. David :
The ideal Waring's Theorem $g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$ for large k follows from the abc Conjecture.

S. Laishram : the ideal Waring's Theorem for all k follows from the explicit abc Conjecture.

Alan Baker : explicit abc Conjecture (2004)

Let (a, b, c) be an abc–triple. Then

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

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

Alan Baker

1939 - 2018

Shanta Laishram and Tarlok Shorey

The Nagell–Ljunggren equation is the equation

$$y^q = \frac{x^n - 1}{x - 1}$$

in integers $x > 1$, $y > 1$, $n > 2$, $q > 1$.

This means that in basis x, all the digits of the perfect power y^q are 1.

If the explicit abc–conjecture of Baker is true, then the only solutions are

$$11^2 = \frac{3^5 - 1}{3 - 1}, \quad 20^2 = \frac{7^4 - 1}{7 - 1}, \quad 7^3 = \frac{18^3 - 1}{18 - 1}.$$

The abc conjecture for number fields

P. Vojta (1987) - variants due to D.W. Masser and K. Győry



The abc conjecture for number fields (continued)

Survey by J. Browkin.

Jerzy Browkin
(1934 – 2015)

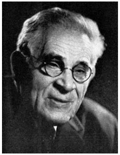
The abc– conjecture for
Algebraic Numbers
Acta Mathematica Sinica,
Jan., 2006, Vol. 22, No. 1,
pp. 211–222

http://dx.doi.org/10.1007/s10114-005-0624-3

Mordell's Conjecture (Faltings's Theorem)

Using an effective extension of the abc Conjecture for a number field, N. Elkies deduces an effective version of Faltings's Theorem on the finiteness of the set of rational points on an algebraic curve of genus ≥ 2 over the same number field.

L.J. Mordell (1922) G. Faltings (1984) N. Elkies (1991)



http://www.math.harvard.edu/~elkies/

Mordell : 1888 - 1972

The abc conjecture for number fields

Andrea Surroca

1973 - 2022

The effective abc Conjecture implies an effective version of Siegel's Theorem on the finiteness of the set of integer points on a curve.

A. Surroca, *Méthodes de transcendance et géométrie diophantienne*, Thèse, Université de Paris 6, 2003.

Thue–Siegel–Roth Theorem (Bombieri)

Using the abc Conjecture for number fields, E. Bombieri (1994) deduces a refinement of the Thue–Siegel–Roth Theorem on the rational approximation of algebraic numbers

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

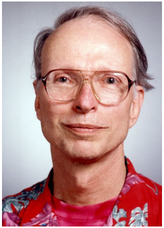
where he replaces ε by

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

where κ depends only on the algebraic number α.

Siegel's zeroes (A. Granville and H.M. Stark)

The uniform abc Conjecture for number fields implies a lower bound for the class number of an imaginary quadratic number field, and K. Mahler has shown that this implies that the associated L–function has no Siegel zero.



abc and Vojta's height Conjecture

Paul Vojta

Vojta stated a conjectural inequality on the height of algebraic points of bounded degree on a smooth complete variety over a global field of characteristic zero which implies the *abc* Conjecture.

Further consequences of the abc Conjecture

• Erdős's Conjecture on consecutive powerful numbers.

• Dressler's Conjecture : between two positive integers having the same prime factors, there is always a prime (Cochrane and textcolormacouleurDressler 1999).

• Squarefree and powerfree values of polynomials (Browkin, Filaseta, Greaves and Schinzel, 1995).

• Lang's conjectures : lower bounds for heights, number of integral points on elliptic curves (Frey 1987, Hindry Silverman 1988).

• Bounds for the order of the Tate–Shafarevich group (Goldfeld and Szpiro 1995).

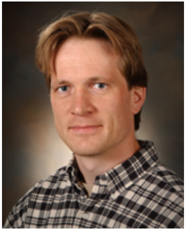
• Greenberg's Conjecture on Iwasawa invariants λ and μ in cyclotomic extensions (Ichimura 1998).

• Lower bound for the class number of imaginary quadratic fields (Granville and Stark 2000), hence no Siegel zero for the associated L–function (Mahler).

• Fundamental units of certain quadratic and biquadratic fields (Katayama 1999).

• The height conjecture and the degree conjecture (Frey 1987, Mai and Murty 1996)

The n–Conjecture



Nils Bruin, Generalization of the ABC-conjecture, Master Thesis, Leiden University, 1995.

http://www.cecm.sfu.ca/~nbruin/scriptie.pdf

Let $n \geq 3$. There exists a positive constant κ_n such that, if $x_1, \ldots, x_n$ are relatively prime rational integers satisfying $x_1 + \cdots + x_n = 0$ and if no proper subsum vanishes, then

$$\max\{|x_1|, \ldots, |x_n|\} \leq \mathrm{Rad}(x_1 \cdots x_n)^{\kappa_n}.$$

? Should hold for all but finitely many $(x_1, \ldots, x_n)$ with $\kappa_n = 2n - 5 + \epsilon$?

A consequence of the n–Conjecture

Open problem : for $k \geq 5$, no positive integer can be written in two essentially different ways as sum of two k–th powers.

It is not even known whether such a k exists.

Reference : Hardy and Wright : §21.11

For $k = 4$ (Euler) :

$$59^4 + 158^4 = 133^4 + 134^4 = 635\,318\,657$$

A parametric family of solutions of ${x_1}^4 + {x_2}^4 = {x_3}^4 + {x_4}^4$ is known

Reference : http://mathworld.wolfram.com/DiophantineEquation4thPowers.html

abc and meromorphic function fields

Rolf Nevanlinna

1895 - 1980

Nevanlinna value distribution theory.

Recent work of Hu, Pei–Chu, Yang, Chung-Chun and P. Vojta.

ABC Theorem for polynomials

Let K be an algebraically closed field. The *radical* of a monic polynomial

$$P(X) = \prod_{i=1}^{n} (X - \alpha_i)^{a_i} \in K[X]$$

with α_i pairwise distinct is defined as

$$\mathrm{Rad}(P)(X) = \prod_{i=1}^{n} (X - \alpha_i) \in K[X].$$

ABC Theorem for polynomials

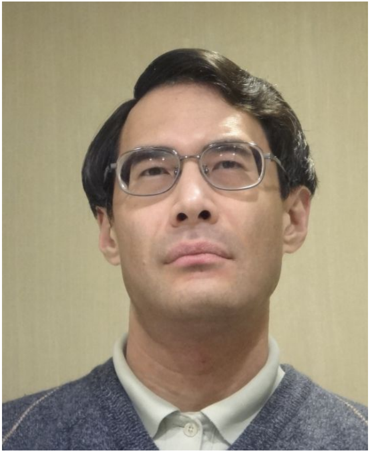
ABC **Theorem** (A. Hurwitz, W.W. Stothers, R. Mason). Let A, B, C be three relatively prime polynomials in $K[X]$ with $A + B = C$ and let $R = \mathrm{Rad}(ABC)$. Then

$$\max\{\deg(A), \deg(B), \deg(C)\} < \deg(R).$$

Adolf Hurwitz (1859–1919)

This result can be compared with the abc Conjecture, where the degree replaces the logarithm.

Shinichi Mochizuki



INTER-UNIVERSAL TEICHMÜLLER THEORY IV : LOG-VOLUME COMPUTATIONS AND SET-THEORETIC FOUNDATIONS
by
Shinichi Mochizuki

http://www.kurims.kyoto-u.ac.jp/~motizuki/top-english.html

Papers of Shinichi Mochizuki

- General Arithmetic Geometry
- Intrinsic Hodge Theory
- p–adic Teichmüller Theory
- Anabelian Geometry, the Geometry of Categories
- The Hodge-Arakelov Theory of Elliptic Curves
- Inter-universal Teichmüller Theory

Shinichi Mochizuki

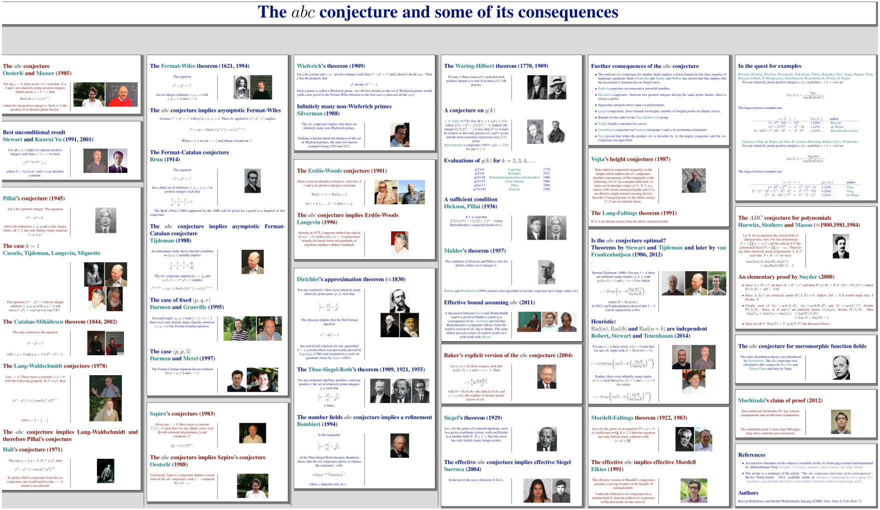
[1] Inter-universal Teichmüller Theory I : Construction of Hodge Theaters. PDF

[2] Inter-universal Teichmüller Theory II : Hodge-Arakelov-theoretic Evaluation. PDF

[3] Inter-universal Teichmüller Theory III : Canonical Splittings of the Log-theta-lattice. PDF

[4] Inter-universal Teichmüller Theory IV : Log-volume Computations and Set-theoretic Foundations. PDF

Poster with Razvan Barbulescu — Archives HAL



https://hal.archives-ouvertes.fr/hal-01626155

On the abc Conjecture and some of its consequences

by

Michel Waldschmidt

Sorbonne University
Institut Mathématique de Jussieu

http://www.imj-prg.fr/~michel.waldschmidt/