6th World Conference on 21st Century Mathematics
Abdus Salam School of Mathematical Sciences (ASSMS)
Lahore (Pakistan) http://www.sms.edu.pk/

On the abc Conjecture and some of its consequences

by

Michel Waldschmidt

http://www.math.jussieu.fr/∼miw/

March 6–9, 2013 *Thursday, March 7, 2013*

International Congress of Mathematicians
Seoul, Korea
August 13 - 21, 2014

Travel Grants for 1,000 Mathematicians
ICM 2014 Invitation Program : "NANUM 2014"
http://www.icm2014.org/

Tentative schedule for the application and review process :
- Call for application : June 1, 2013
- Deadline to submit all the application documents : August 31, 2013
- Selection of the travel grant recipient : September 2013 December 2013
- Notification to applicants of acceptance : January 2014

Abstract

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 Œsterlé 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.

Abstract (continued)

This talk will be at an elementary level, giving a collection of consequences of the abc Conjecture. It will not include an introduction to the Inter-universal Teichmüller Theory of Shinichi Mochizuki.

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

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* or *square free part* $\mathrm{Rad}(n)$ of n is the product of the distinct primes dividing n :

$$n = p_1 p_2 \cdots p_t.$$

Examples :

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

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

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

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:`

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

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

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

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

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

But for $a \geq 1$,

$$(2^a, 2^{a+3}, 2^a \cdot 3^2)$$

is not an abc–hit since these three numbers are not coprime.

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

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

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

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

`Proof` : Induction on k.

`Consequence` :

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

Hence

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

is an abc–hit.

Infinitely many abc–hits

This argument, due to F. Beukers, 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 $c > \mathrm{Rad}(abc)^2$?*

`Answer`: this is unknown.

Examples

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

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

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
$11^2 + 3^2 5^6 7^3$	$=$	$2^{21} \cdot 23$	$1.625990\ldots$	B.M. de Weger

There are 140 known values of $\lambda(a, b, c)$ which are ≥ 1.4.

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 : $23/9$

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

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

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

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

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

Explicit abc Conjecture



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

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

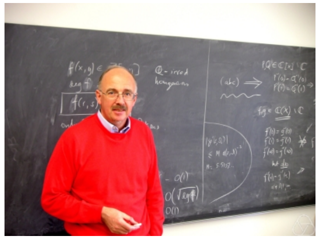
for any abc–triple (a, b, c).

The abc Conjecture

Recall that for a positive integer n, the *radical* or *square free part* of n is
$$\mathrm{Rad}(n) = \prod_{p|n} p.$$

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

The abc Conjecture of Œsterlé and Masser



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

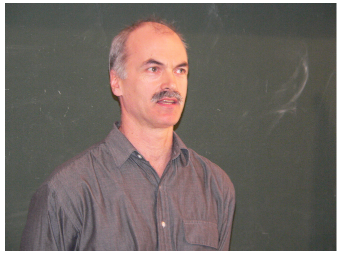
C.L. Stewart and Yu Kunrui

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

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

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

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



Lucien Szpiro

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

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

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

Further examples

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

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

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

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

There are 47 known triples (a,b,c) with $0 < a < b < c$, $a + b = c$ and $\gcd(a,b) = 1$ satisfying $\varrho(a,b,c) > 4$.

Abderrahmane Nitaj عبدالرحمان نتاج

http://www.math.unicaen.fr/~nitaj/abc.html

THE ABC CONJECTURE HOME PAGE

ABC

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

The abc conjecture is the most important unsolved problem in diophantine 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

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

Pierre de Fermat
1601 – 1665

Andrew Wiles
1953 –

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 $n \leq 5$.

Square, cubes...

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

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

- Cubes :

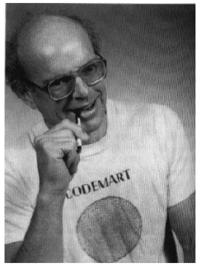
$$1,\ 8,\ 27,\ 64,\ 125,\ 216,\ 343,\ 512,\ 729,\ 1\,000,\ 1\,331, \ldots$$

- Fifth powers :

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

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

Consecutive elements in the sequence of perfect powers

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

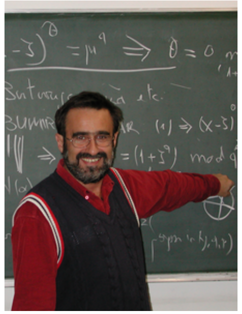
$$x^p - y^q = k,$$

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

Preliminary results :
J.W.S. Cassels, Rob Tijdeman

Also 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

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

Not a consequence of the abc Conjecture

$p = 3$, $q = 2$

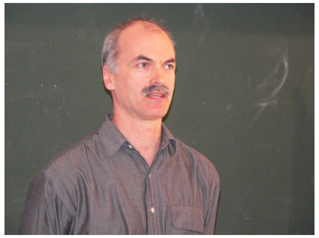
Hall's Conjecture (1971) :

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

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

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 there are infinitely many solutions (x, y, z).

Frits Beukers and *Don Zagier*

For

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

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

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

are known.


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 :

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

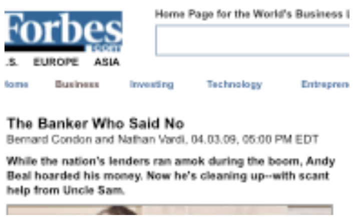
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1\,549\,034^2 = 15\,613^3,$$

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

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

Andrew Beal

Find another solution, or prove that there is no further solution.



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

Beal's Prize : $50,000$\$ US

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.

Conjecture of R. Tijdeman and D. 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.

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* $(1/p) + (1/q) + (1/r) < 1$ *is finite.*

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

1995 (H. Darmon and A. Granville) : for fixed (p, q, r), only finitely many (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 $2^{p-1} - 1$.

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

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

Not too many Wieferich primes 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 $a^{p-1} - 1$.

Consecutive integers with the same radical

Notice that

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

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

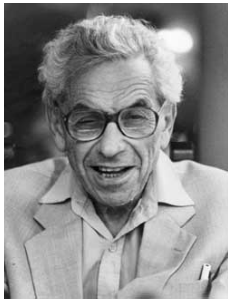
$$\mathrm{Rad}(x) = \mathrm{Rad}(y),$$

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

and

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

Erdős – Woods Conjecture



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 $x = y$.

Erdős Conjecture on $2^p - 1$

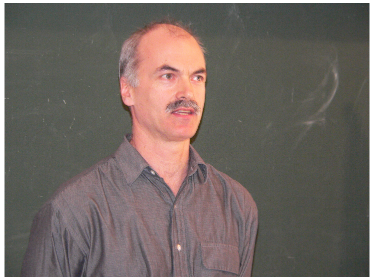
In 1965, P. Erdős conjectured that the greatest prime factor $P(2^n - 1)$ satisfies

$$\frac{P(2^n - 1)}{n} \to \infty \quad \text{when} \quad n \to \infty.$$

In 2002, R. Murty and S. Wong proved that this is a consequence of the *abc* Conjecture.
In 2012, C.L. Stewart proved Erdős Conjecture (in a wider context of Lucas and Lehmer sequences) :

$$P(2^n - 1) > n \exp\bigl(\log n / 104 \log\log n\bigr).$$

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 $c > R \log R$.

C.L. Stewart 's Conjectures

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

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

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 :

"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 $x_1^k + \cdots + x_s^k$.*

The ideal Waring's Theorem

For each integer $k \geq 2$, define $I(k) = 2^k + [(3/2)^k] - 2$. It is easy to show that $g(k) \geq I(k)$. Indeed, write

$$3^k = 2^k q + r \quad \text{with} \quad 0 < r < 2^k, \quad q = [(3/2)^k],$$

and consider the integer

$$N = 2^k q - 1 = (q-1)2^k + (2^k - 1)1^k.$$

Since $N < 3^k$, writing N as a sum of k-th powers can involve no term 3^k, and since $N < 2^k q$, it involves at most $(q-1)$ terms 2^k, all others being 1^k; hence it requires a total number of at least $(q-1) + (2^k - 1) = I(k)$ terms.

The ideal Waring's Theorem

L.E. Dickson and S.S. Pillai proved independently in 1936 that $g(k) = I(k)$, provided that $r = 3^k - 2^k q$ satisfies

$$r \leq 2^k - q - 2.$$

The condition $r \leq 2^k - q - 2$ is satisfied for $3 \leq k \leq 471\ 600\ 000$.
The conjecture, dating back to 1853, is $g(k) = I(k) = 2^k + [(3/2)^k] - 2$ for any $k \geq 2$. This is true as soon as

$$\left\| \left(\frac{3}{2}\right)^k \right\| \geq \left(\frac{3}{4}\right)^k,$$

where $\| \cdot \|$ denote the distance to the nearest integer.

Mahler's contribution

- The estimate

$$\left\| \left(\frac{3}{2}\right)^k \right\| \geq \left(\frac{3}{4}\right)^k$$

is valid for all sufficiently large k.

Kurt Mahler
(1903 - 1988)

Hence the ideal Waring's Theorem

$$g(k) = 2^k + [(3/2)^k] - 2$$

holds for all sufficiently large k.

Waring's Problem and the *abc* Conjecture

S. David : the estimate

$$\left\| \left(\frac{3}{2}\right)^k \right\| \geq \left(\frac{3}{4}\right)^k$$

for sufficiently large k follows from the abc Conjecture.

S. Laishram : the ideal Waring's Theorem $g(k) = 2^k + [(3/2)^k] - 2$ follows from the explicit abc Conjecture.

Alan Baker (1996)

Let (a, b, c) be an abc–triple and let $\epsilon > 0$. Then

$$c \leq \kappa\left(\epsilon^{-\omega} R\right)^{1+\epsilon}$$

where κ is an absolute constant, $R = \mathrm{Rad}(abc)$ and $\omega = \omega(abc)$ is the number of distinct prime factors of abc.

Remark of Andrew Granville : the minimum of the function on the right over $\epsilon > 0$ occurs essentially with $\epsilon = \omega/\log R$. This yields a slightly sharper form of the conjecture :

$$c \leq \kappa R \frac{(\log R)^\omega}{\omega!}.$$

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.

Shanta Laishram and Tarlok Shorey

The Nagell–Ljunggren equation is the equation

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

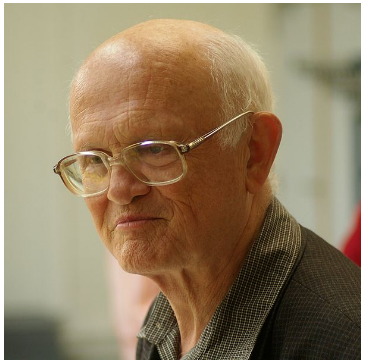
in integers $x > 1$, $y > 1$, $n > 2$, $q > 1$.

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

Kálmán Győry
http://www.math.klte.hu/algebra/gyorya.htm

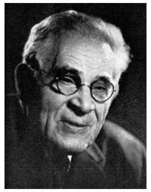


Jerzy Browkin

Mordell's Conjecture (Faltings's Theorem)

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

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



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

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

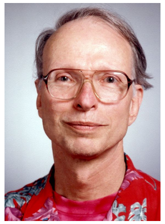
where he replaces ε by

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

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.



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.
- 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 Conjecture for curves.
- Greenberg's Conjecture on Iwasawa invariants λ and μ in cyclotomic extensions.
- Exponents of class groups of quadratic fields.
- Fundamental units in quadratic and biquadratic fields.

abc and meromorphic function fields

Nevanlinna value distribution theory.

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

abc and Vojta's height Conjecture

Paul Vojta

Vojta's Conjecture on algebraic points of bounded degree on a smooth complete variety over a global field of characteristic zero implies the abc Conjecture.

ABC Theorem for polynomials

Let K be an algebraically closed field. The *radical* or *square free part* 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.

The radical of a polynomial as a gcd

The common zeroes of

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

and P' are the α_i with $a_i \geq 2$. They are zeroes of P' with multiplicity $a_i - 1$. Hence

$$\mathrm{Rad}(P) = \frac{P}{\gcd(P, P')}.$$

Proof of the ABC Theorem for polynomials

Now suppose $A + B = C$ with A, B, C relatively prime.

Notice that

$$\mathrm{Rad}(ABC) = \mathrm{Rad}(A)\mathrm{Rad}(B)\mathrm{Rad}(C).$$

We may suppose A, B, C to be monic and, say, $\deg(A) \leq \deg(B) \leq \deg(C)$.

Write

$$A + B = C, \qquad A' + B' = C',$$

and

$$AB' - A'B = AC' - A'C.$$

Proof of the ABC Theorem for polynomials

Recall $\gcd(A, B, C) = 1$. Since $\gcd(C, C')$ divides $AC' - A'C = AB' - A'B$, it divides also

$$\frac{AB' - A'B}{\gcd(A, A')\gcd(B'B')}$$

which is a polynomial of degree

$$< \deg\big(\mathrm{Rad}(A)\big) + \deg\big(\mathrm{Rad}(B)\big) = \deg\big(\mathrm{Rad}(AB)\big).$$

Hence

$$\deg\big(\gcd(C, C')\big) < \deg\big(\mathrm{Rad}(AB)\big)$$

and

$$\deg(C) < \deg\big(\mathrm{Rad}(C)\big) + \deg\big(\mathrm{Rad}(AB)\big) = \deg\big(\mathrm{Rad}(ABC)\big).$$

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/

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