On the abc Conjecture and some of its consequences

by

Michel Waldschmidt

Université P. et M. Curie (Paris VI)

http://www.imj-prg.fr/~michel.waldschmidt/
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 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.
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 abc conjecture and some of its consequences

https://hal.archives-ouvertes.fr/hal-01626155
As simple as abc
American Broadcasting Company

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.

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 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*) \( \text{Rad}(n) \) of \( n \) is the product of the distinct primes dividing \( n \):

\[
\text{Rad}(n) = p_1p_2 \cdots p_t.
\]
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*) $\text{Rad}(n)$ of $n$ is the product of the distinct primes dividing $n$:

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

$$\text{Rad}(n) \leq n.$$
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*) $\text{Rad}(n)$ of $n$ is the product of the distinct primes dividing $n$:

$$\text{Rad}(n) = p_1p_2 \cdots p_t.$$

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

*Examples*: $\text{Rad}(2^a) = 2$, 
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 \textit{radical} (also called \textit{kernel}) \( \text{Rad}(n) \) of \( n \) is the product of the distinct primes dividing \( n \):

\[
\text{Rad}(n) = p_1 p_2 \cdots p_t.
\]

\[
\text{Rad}(n) \leq n.
\]

\textit{Examples} : \( \text{Rad}(2^a) = 2, \)

\[
\text{Rad}(60\ 500) = \text{Rad}(2^2 \cdot 5^3 \cdot 11^2) = 2 \cdot 5 \cdot 11 = 110,
\]

\[
\text{Rad}(82\ 852\ 996\ 681\ 926) = 2 \cdot 3 \cdot 23 \cdot 109 = 15\ 042.
\]
$abc$–triples

An $abc$–triple is a triple of three positive integers $a$, $b$, $c$ which are coprime, $a < b$ and that $a + b = c$. 
An \textit{abc–triple} is a triple of three positive integers \(a, b, c\) which are coprime, \(a < b\) and that \(a + b = c\).

Examples:

\[
1 + 2 = 3, \quad 1 + 8 = 9, \\
1 + 80 = 81, \quad 4 + 121 = 125, \\
2 + 3^{10} \cdot 109 = 23^5, \quad 11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23.
\]
13 abc-triples with $c < 10$

$a, b, c$ are coprime, $1 \leq a < b$, $a + b = c$ and $c \leq 9$. 
13 $abc$-triples with $c < 10$

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

\begin{align*}
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
\end{align*}
Radical of the $abc$–triples with $c < 10$

- $\text{Rad}(1 \cdot 2 \cdot 3) = 6$
- $\text{Rad}(1 \cdot 3 \cdot 4) = 6$
- $\text{Rad}(1 \cdot 4 \cdot 5) = 10$  $\text{Rad}(2 \cdot 3 \cdot 5) = 30$
- $\text{Rad}(1 \cdot 5 \cdot 6) = 30$
- $\text{Rad}(1 \cdot 6 \cdot 7) = 42$  $\text{Rad}(2 \cdot 5 \cdot 7) = 70$  $\text{Rad}(3 \cdot 4 \cdot 7) = 42$
- $\text{Rad}(1 \cdot 7 \cdot 8) = 14$  $\text{Rad}(3 \cdot 5 \cdot 8) = 30$
- $\text{Rad}(1 \cdot 8 \cdot 9) = 6$  $\text{Rad}(2 \cdot 7 \cdot 9) = 54$  $\text{Rad}(4 \cdot 5 \cdot 9) = 30$
Radical of the $abc$–triples with $c < 10$

\[
\begin{align*}
\text{Rad}(1 \cdot 2 \cdot 3) &= 6 \\
\text{Rad}(1 \cdot 3 \cdot 4) &= 6 \\
\text{Rad}(1 \cdot 4 \cdot 5) &= 10 & \text{Rad}(2 \cdot 3 \cdot 5) &= 30 \\
\text{Rad}(1 \cdot 5 \cdot 6) &= 30 \\
\text{Rad}(1 \cdot 6 \cdot 7) &= 42 & \text{Rad}(2 \cdot 5 \cdot 7) &= 70 & \text{Rad}(3 \cdot 4 \cdot 7) &= 42 \\
\text{Rad}(1 \cdot 7 \cdot 8) &= 14 & \text{Rad}(3 \cdot 5 \cdot 8) &= 30 \\
\text{Rad}(1 \cdot 8 \cdot 9) &= 6 & \text{Rad}(2 \cdot 7 \cdot 9) &= 54 & \text{Rad}(4 \cdot 5 \cdot 9) &= 30 \\
\end{align*}
\]

\[a = 1, \ b = 8, \ c = 9, \ a + b = c, \ \gcd = 1, \ \text{Rad}(abc) < c.\]
Following F. Beukers, an \( abc \)–hit is an \( abc \)–triple such that \( \text{Rad}(abc) < c \).
Following F. Beukers, an $abc$–hit is an $abc$–triple such that $\text{Rad}(abc) < c$.

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

$$\text{Rad}(1 \cdot 8 \cdot 9) = \text{Rad}(2^3 \cdot 3^2) = 2 \cdot 3 = 6 < 9.$$
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 $ad^\ell$, $bd^\ell$ and $cd^\ell$ is nothing else than $\text{Rad}(abc)$; but $c$ is replaced by $cd^\ell$. 
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 $ad^\ell$, $bd^\ell$ and $cd^\ell$ is nothing else than $\text{Rad}(abc)$; but $c$ is replaced by $cd^\ell$.

For $\ell$ sufficiently large, $cd^\ell$ is larger than $\text{Rad}(abc)$. 
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 $ad^\ell, bd^\ell$ and $cd^\ell$ is nothing else than $\text{Rad}(abc)$; but $c$ is replaced by $cd^\ell$.

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

But $(ad^\ell, bd^\ell, cd^\ell)$ is not an $abc$–hit.
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 $ad^\ell$, $bd^\ell$ and $cd^\ell$ is nothing else than $\text{Rad}(abc)$; but $c$ is replaced by $cd^\ell$.

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

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

$$\text{Rad}(1 \cdot 80 \cdot 81) = \text{Rad}(2^4 \cdot 5 \cdot 3^4) = 2 \cdot 5 \cdot 3 = 30 < 81.$$
Some $abc$–hits

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

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

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

$$\text{Rad}(4 \cdot 121 \cdot 125) = \text{Rad}(2^2 \cdot 5^3 \cdot 11^2) = 2 \cdot 5 \cdot 11 = 110 < 125.$$
Further $abc$–hits

- $(2, 3^{10} \cdot 109, 23^5) = (2, 6436341, 6436343)$

is an $abc$–hit since $2 + 3^{10} \cdot 109 = 23^5$ and

$\text{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 15042 < 23^5 = 6436343$. 
Further $abc$–hits

- $(2, 3^{10} \cdot 109, 23^5) = (2, 6436341, 6436343)$ is an $abc$–hit since $2 + 3^{10} \cdot 109 = 23^5$ and $\text{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 15042 < 23^5 = 6436343$.

- $(11^2, 3^2 \cdot 5^6 \cdot 7^3, 2^{21} \cdot 23) = (121, 48234275, 48234496)$ is an $abc$–hit since $11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$ and $\text{Rad}(2^{21} \cdot 3^2 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 23) = 53130 < 2^{21} \cdot 23 = 48234496$. 
Further $abc$–hits

- $(2, 3^{10} \cdot 109, 23^5) = (2, 6436341, 6436343)$ is an $abc$–hit since $2 + 3^{10} \cdot 109 = 23^5$ and $\text{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 15\,042 < 23^5 = 6\,436\,343$.

- $(11^2, 3^2 \cdot 5^6 \cdot 7^3, 2^{21} \cdot 23) = (121, 48\,234\,275, 48\,234\,496)$ is an $abc$–hit since $11^2 + 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$ and $\text{Rad}(2^{21} \cdot 3^2 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 23) = 53\,130 < 2^{21} \cdot 23 = 48\,234\,496$.

- $(1, 5 \cdot 127 \cdot (2 \cdot 3 \cdot 7)^3, 19^6) = (1, 47\,045\,880, 47\,045\,881)$ is an $abc$–hit since $1 + 5 \cdot 127 \cdot (2 \cdot 3 \cdot 7)^3 = 19^6$ and $\text{Rad}(5 \cdot 127 \cdot (2 \cdot 3 \cdot 7)^3 \cdot 19^6) = 5 \cdot 127 \cdot 2 \cdot 3 \cdot 7 \cdot 19 = 506\,730$. 
abc–triples and abc–hits

Among $15 \cdot 10^6$ abc–triples with $c < 10^4$, we have 120 abc–hits.
$abc$–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 $81 = 3^4$. 
More \textit{abc}–hits

Recall the \textit{abc}–hit \((1, 80, 81)\), where \(81 = 3^4\).

\[(1, 3^{16} - 1, 3^{16}) = (1, 43046720, 43046721)\]

is an \textit{abc}–hit.
More \(abc\)-hits

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

\[
(1, 3^{16} - 1, 3^{16}) = (1, 43046720, 43046721)
\]
is an \(abc\)-hit.

Proof.

\[
3^{16} - 1 = (3^8 - 1)(3^8 + 1)
\]
\[
= (3^4 - 1)(3^4 + 1)(3^8 + 1)
\]
\[
= (3^2 - 1)(3^2 + 1)(3^4 + 1)(3^8 + 1)
\]
\[
= (3 - 1)(3 + 1)(3^2 + 1)(3^4 + 1)(3^8 + 1)
\]
is divisible by \(2^6\).
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.

$$3^{16} - 1 = (3^8 - 1)(3^8 + 1)$$
$$= (3^4 - 1)(3^4 + 1)(3^8 + 1)$$
$$= (3^2 - 1)(3^2 + 1)(3^4 + 1)(3^8 + 1)$$
$$= (3 - 1)(3 + 1)(3^2 + 1)(3^4 + 1)(3^8 + 1)$$

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

\[
3^{16} - 1 = (3^8 - 1)(3^8 + 1)
= (3^4 - 1)(3^4 + 1)(3^8 + 1)
= (3^2 - 1)(3^2 + 1)(3^4 + 1)(3^8 + 1)
= (3 - 1)(3 + 1)(3^2 + 1)(3^4 + 1)(3^8 + 1)
\]

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

Hence

\[
\text{Rad}((3^{16} - 1) \cdot 3^{16}) \leq \frac{3^{16} - 1}{2^6} \cdot 2 \cdot 3 < 3^{16}.
\]
Infinitely many $abc$–hits

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

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

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

\[
3^{2^k} - 1 = (3^{2^{k-1}} - 1)(3^{2^{k-1}} + 1).
\]
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:**

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

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

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

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

We do not know the answer.
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 $R = \text{Rad}(abc)$.

Question: Are there $abc$–triples for which $c > \text{Rad}(abc)^2$?
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 $R = \text{Rad}(abc)$.

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

We do not know the answer.
Examples

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>$a + b$</th>
<th>$c$</th>
<th>$\lambda(a, b, c)$</th>
<th>authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2 + 3^{10} \cdot 109$</td>
<td>$23^5$</td>
<td>1.629912...</td>
<td>É. Reyssat</td>
</tr>
<tr>
<td>$11^2 + 3^2 5^6 7^3$</td>
<td>$2^{21} \cdot 23$</td>
<td>1.625990...</td>
<td>B.M. de Weger</td>
</tr>
</tbody>
</table>
Examples

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

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

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

<table>
<thead>
<tr>
<th>$a + b$</th>
<th>$c$</th>
<th>$\lambda(a, b, c)$</th>
<th>authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2 + 3^{10} \cdot 109$</td>
<td>$23^5$</td>
<td>1.629912...</td>
<td>É. Reyssat</td>
</tr>
<tr>
<td>$11^2 + 3^2 5^6 7^3$</td>
<td>$2^{21} \cdot 23$</td>
<td>1.625990...</td>
<td>B.M. de Weger</td>
</tr>
</tbody>
</table>
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. 

At the date of August 1, 2015, 238 were known. On May 15, 2017, the total is 240.


The list up to 20 digits is complete.
Eric Reyssat: $2 + 3^{10} \cdot 109 = 23^5$
Example of Reyssat $2 + 3^{10} \cdot 109 = 23^5$

$$a + b = c$$

$$a = 2, \quad b = 3^{10} \cdot 109, \quad c = 23^5 = 6436343,$$
Example of Reyssat $2 + 3^{10} \cdot 109 = 23^5$

$$a + b = c$$

$$a = 2, \quad b = 3^{10} \cdot 109, \quad c = 23^5 = 6436343,$$

$$\text{Rad}(abc) = \text{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 2 \cdot 3 \cdot 109 \cdot 23 = 15042,$$
Example of Reyssat $2 + 3^{10} \cdot 109 = 23^5$

$a + b = c$

$a = 2, \quad b = 3^{10} \cdot 109, \quad c = 23^5 = 6436343,$

$\text{Rad}(abc) = \text{Rad}(2 \cdot 3^{10} \cdot 109 \cdot 23^5) = 2 \cdot 3 \cdot 109 \cdot 23 = 15042,$

$\lambda(a, b, c) = \frac{\log c}{\log \text{Rad}(abc)} = \frac{5 \log 23}{\log 15042} \approx 1.62991.$
Continued fraction

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

Continued fraction of \( 109^{1/5} \): \([2; 1, 1, 4, 77733, \ldots ]\),

approximation: \([2; 1, 1, 4] = 23/9\)

\[ 109^{1/5} = 2.555\,555\,39 \ldots \]

\[ \frac{23}{9} = 2.555\,555\,55 \ldots \]

N. A. Carella. *Note on the ABC Conjecture*

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

$$\text{Rad}(2^{21} \cdot 3^2 \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 23) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 53130.$$  

$2^{21} \cdot 23 = 48234496 = (53130)^{1.625990...}$
Explicit $abc$ Conjecture

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

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

for any $abc$–triple $(a, b, c)$. 
The $abc$ Conjecture

Recall that for a positive integer $n$, the $\textit{radical}$ of $n$ is

$$\text{Rad}(n) = \prod_{p|n} p.$$
The *abc* Conjecture

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

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

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

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

is finite.
The *abc* Conjecture

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

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

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

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

is finite.

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

$$c < \kappa(\varepsilon)\text{Rad}(abc)^{1+\varepsilon}.$$
The \textit{abc} Conjecture is a \textbf{lower bound} for the radical of the product \textit{abc}:

\textbf{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

\[ \text{Rad}(abc) > \kappa(\varepsilon)c^{1-\varepsilon}. \]
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


\[ \log c \leq \kappa R^{1/3} (\log R)^3. \]

with \( R = \text{Rad}(abc) \):

\[ c \leq e^{\kappa R^{1/3} (\log R)^3}. \]
J. Oesterlé and A. Nitaj proved that the \textit{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 $\Delta$ 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 $(5/6) - \epsilon$. 
Further examples

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

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

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

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

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

<table>
<thead>
<tr>
<th>$a + b$</th>
<th>$c$</th>
<th>$g(a, b, c)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$13 \cdot 19^6 + 2^{30} \cdot 5$</td>
<td>$3^{13} \cdot 11^2 \cdot 31$</td>
<td>4.41901…</td>
</tr>
<tr>
<td>$2^5 \cdot 11^2 \cdot 19^9 + 5^{15} \cdot 37^2 \cdot 47$</td>
<td>$3^7 \cdot 7^{11} \cdot 743$</td>
<td>4.26801…</td>
</tr>
</tbody>
</table>
Further examples

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

\[
\varrho(a, b, c) = \frac{\log abc}{\log \text{Rad}(abc)}.
\]

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

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

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

La conjecture abc est aussi difficile que la conjecture ... xyc. (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, 2000

Index

- The abc conjecture
- Generalizations
- Consequences
- Tables
  - The top ten good abc examples
  - The top ten good abc-Square examples
  - The top ten good algebraic abc examples
  - New good abc examples
  - New hunters of abc examples
  - Largest good abc examples
  - The list of good triples up to 20 digits is now complete

- Bibliography
Bart de Smit

http://www.math.leidenuniv.nl/~desmit/abc/
Escher and the Droste effect

http://escherdroste.math.leidenuniv.nl/
ABC@home is an educational and non-profit distributed computing project finding abc-triples related to the ABC conjecture.
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
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 $x < y$. 
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

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

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

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

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

$$\text{Rad}(x^ny^nz^n) \leq xyz < z^3.$$ 

If the explicit $abc$ Conjecture $c < \text{Rad}(abc)^2$ 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**:

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

- **Cubes**:

  $1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331, \ldots$

- **Fifth powers**:

  $1, 32, 243, 1024, 3125, 7776, 16807, 32768, \ldots$
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, ...
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, ...

Neil J. A. Sloane’s encyclopaedia
http://oeis.org/A001597
Nearly equal perfect powers

- Difference 1 : (8, 9)

- Difference 2 : (25, 27), ...

- Difference 3 : (1, 4), (125, 128), ...

- Difference 4 : (4, 8), (32, 36), (121, 125), ...

- Difference 5 : (4, 9), (27, 32), ...
Two conjectures

Eugène Charles Catalan (1814 – 1894)

Subbayya Sivasankaranarayana Pillai (1901-1950)

- 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 $\geq 2$, has only finitely many solutions $(x, y, p, q)$. 
Results


Catalan was right: the equation \( x^p - y^q = 1 \) where the unknowns \( x, y, p \) and \( q \) take integer values, all \( \geq 2 \), has only one solution \( (x, y, p, q) = (3, 2, 2, 3) \).
Previous work on Catalan’s Conjecture

J.W.S. Cassels, Rob Tijdeman

\[ x^p < y^q < \exp \exp \exp \exp(730) \]

Michel Langevin
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 and the \textit{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 \textit{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_

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

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

Condition: $x, y, z$ are relatively prime

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

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

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

\[ 1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \]
\[ 3^5 + 11^4 = 122^2, \quad 33^8 + 1549034^2 = 15613^3, \]
\[ 1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7, \]
\[ 17^7 + 76271^3 = 21063928^2, \quad 43^8 + 96222^3 = 30042907^2. \]
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.*

Beal’s Prize


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.
Beal’s Prize: $1,000,000 USD

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
"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 $(x, y, z)$. 
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 $2^{p-1} - 1$.

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

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 $75 = 3 \cdot 5^2$ and $1215 = 3^5 \cdot 5$ hence $\text{Rad}(75) = \text{Rad}(1215) = 3 \cdot 5^2 = 15$.

But also $76 = 2^2 \cdot 19$ and $1216 = 2^6 \cdot 19$ have the same radical $\text{Rad}(76) = \text{Rad}(1216) = 2^2 \cdot 19 = 38$. 
Consecutive integers with the same radical

Notice that

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

hence

\[ \text{Rad}(75) = \text{Rad}(1215) = 3 \cdot 5 = 15. \]
Consecutive integers with the same radical

Notice that

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

hence

\[ \text{Rad}(75) = \text{Rad}(1215) = 3 \cdot 5 = 15. \]

But also

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

have the same radical

\[ \text{Rad}(76) = \text{Rad}(1216) = 2 \cdot 19 = 38. \]
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.
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

$$\text{Rad}(x) = \text{Rad}(y) \quad \text{and} \quad \text{Rad}(x + 1) = \text{Rad}(y + 1)?$$
Consecutive integers with the same radical

Are there further examples of \( x \neq y \) with

\[
\text{Rad}(x) = \text{Rad}(y) \quad \text{and} \quad \text{Rad}(x + 1) = \text{Rad}(y + 1)\?
\]

Is it possible to find two distinct integers \( x, y \) such that

\[
\text{Rad}(x) = \text{Rad}(y),
\]

\[
\text{Rad}(x + 1) = \text{Rad}(y + 1)
\]

and

\[
\text{Rad}(x + 2) = \text{Rad}(y + 2)\?
Erdős – Woods Conjecture

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

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

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

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:
\[ 7!3!22! = 9!, \quad 7!6! = 10!, \quad 7!5!3! = 10!, \quad 14!5!2! = 16!. \]

Saranya Nair and Tarlok Shorey : The effective abc conjecture implies Hickerson’s conjecture that the largest non-trivial solution is given by \( n = 16 \).
Erdős Conjecture on $2^n - 1$

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

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

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.
**Erdős Conjecture on $2^n - 1$**

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):

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

\[ c > R \exp \left( (4 - \delta) \frac{\log R}{\log \log R} \right). \]
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 $c > R \log R$. 

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

$$c < \kappa(\varepsilon) R \exp \left( (4\sqrt{3} + \varepsilon) \left( \frac{\log R}{\log \log R} \right)^{1/2} \right).$$
Conjectures by Machiel van Frankenhuijisen, Olivier Robert, Cam Stewart and Gérald Tenenbaum

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

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

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 $R(b)$.


http://blms.oxfordjournals.org/content/46/6/1156.full.pdf

Waring’s Problem

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 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 : \( g(2) = 4. \)

\( g(2) \leq 4 \) : any positive number is a sum of at most 4 squares:
\[ n = x_1^2 + x_2^2 + x_3^2 + x_4^2. \]

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

Lower bounds are easy, not upper bounds.


\[ g(4) \geq 19. \]

We want to write 79 as sum \( a_1^4 + a_2^4 + \cdots + a_s^4 \) with \( s \) as small as possible.
$g(4) \geq 19$.

We want to write $79$ as sum $a_1^4 + a_2^4 + \cdots + a_s^4$ with $s$ as small as possible.

Since $79 < 81$, we cannot use $3^4$. Hence we can use only $2^4 = 16$ and $1^4 = 1$. 
$g(4) \geq 19$.

We want to write $79$ as sum $a_1^4 + a_2^4 + \cdots + a_s^4$ with $s$ as small as possible.

Since $79 < 81$, we cannot use $3^4$. Hence we can use only $2^4 = 16$ and $1^4 = 1$.

Since $79 < 5 \times 16$, we can use at most 4 terms $2^4$. 

We want to write $79$ as sum $a_1^4 + a_2^4 + \cdots + a_s^4$ with $s$ as small as possible.

Since $79 < 81$, we cannot use $3^4$. Hence we can use only $2^4 = 16$ and $1^4 = 1$.

Since $79 < 5 \times 16$, we can use at most $4$ terms $2^4$.

Now

$$79 = 64 + 15 = 4 \times 2^4 + 15 \times 1^4$$

with $4 + 15$ terms $a^4$ (namely $4$ with $2^4$ and $15$ with $1^4$).
We want to write 79 as sum $a_1^4 + a_2^4 + \cdots + a_s^4$ with $s$ as small as possible.

Since 79 < 81, we cannot use $3^4$. Hence we can use only $2^4 = 16$ and $1^4 = 1$.

Since 79 < $5 \times 16$, we can use at most 4 terms $2^4$.

Now

$$79 = 64 + 15 = 4 \times 2^4 + 15 \times 1^4$$

with 4 + 15 terms $a^4$ (namely 4 with $2^4$ and 15 with $1^4$).

The number of terms is 19.
\[ n = x_1^4 + \cdots + x_{19}^4 : g(4) = 19 \]

Any positive integer is the sum of at most 19 biquadrates

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
Lower bound for $g(k)$

Let $k \geq 2$. Select $N < 3^k$ of the form $N = 2^k q - 1$. 
Lower bound for $g(k)$

Let $k \geq 2$. Select $N < 3^k$ of the form $N = 2^k q - 1$. Since $N < 3^k$, writing $N$ as a sum of $k$-th powers can involve no term $3^k$. 
Lower bound for \( g(k) \)

Let \( k \geq 2 \). Select \( N < 3^k \) of the form \( N = 2^k q - 1 \). 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 \( 1^k \);
Lower bound for $g(k)$

Let $k \geq 2$. Select $N < 3^k$ of the form $N = 2^k q - 1$. 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 $1^k$; so the most economical way of writing $N$ as a sum of $k$-th powers is

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

which requires a total number of $(q - 1) + (2^k - 1)$ terms.
Let \( k \geq 2 \). Select \( N < 3^k \) of the form \( N = 2^k q - 1 \). 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 \( 1^k \); so the most economical way of writing \( N \) as a sum of \( k \)-th powers is

\[
N = (q - 1)2^k + (2^k - 1)1^k
\]

which requires a total number of \((q - 1) + (2^k - 1)\) terms. The largest value is obtained by taking for \( q \) the largest integer with \( 2^k q < 3^k \). Since \((3/2)^k\) is not an integer, this integer \( q \) is \( \lfloor (3/2)^k \rfloor \).
Let $k \geq 2$. Select $N < 3^k$ of the form $N = 2^k q - 1$. 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 $1^k$; so the most economical way of writing $N$ as a sum of $k$-th powers is

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

which requires a total number of $(q - 1) + (2^k - 1)$ terms. The largest value is obtained by taking for $q$ the largest integer with $2^k q < 3^k$. Since $(3/2)^k$ is not an integer, this integer $q$ is $\lceil (3/2)^k \rceil$ (quotient of the division of $3^k$ by $2^k$).
For each integer $k \geq 2$, define $I(k) = 2^k + \lceil (3/2)^k \rceil - 2$. Then $g(k) \geq I(k)$.

(J. A. Euler, son of Leonhard Euler).
The ideal Waring’s “Theorem” : $g(k) = I(k)$

Recall

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

Conjecture (C.A. Bretschneider, 1853) : $g(k) = I(k)$ for any $k \geq 2$. 

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 $r < 2^k q^2$ with $q = b(3/2)^k c$. 

The ideal Waring’s “Theorem” : $g(k) = I(k)$

Recall

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

Conjecture (C.A. Bretschneider, 1853) : $g(k) = I(k)$ for any $k \geq 2$.

Divide $3^k$ by $2^k$ :

$$3^k = 2^k q + r \quad \text{with} \quad 0 < r < 2^k, \quad q = \lfloor (3/2)^k \rfloor$$
The ideal Waring’s “Theorem” : $g(k) = I(k)$

Recall

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

Conjecture (C.A. Bretschneider, 1853) : $g(k) = I(k)$ for any $k \geq 2$.

Divide $3^k$ by $2^k$:

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

The remainder $r = 3^k - 2^k q$ satisfies $r < 2^k$. A slight improvement of this upper bound would yield the desired result. 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

$$r \leq 2^k - q - 2 \quad \text{with} \quad q = \lfloor (3/2)^k \rfloor.$$
The condition \( r \leq 2^k - q - 2 \)

The condition \( r \leq 2^k - q - 2 \) is satisfied for \( 4 \leq k \leq 471\,600\,000 \).
The condition \( r \leq 2^k - q - 2 \)

The condition \( r \leq 2^k - q - 2 \) is satisfied for \( 4 \leq k \leq 471 \, 600 \, 000 \).

If, for some \( k \), the condition \( r \leq 2^k - q - 2 \) is not satisfied, then \( (3/2)^k \) is extremely close to an integer:

\[
q + 1 - \frac{q - 2}{2^k} < \left(\frac{3}{2}\right)^k < q + 1,
\]

which is unlikely.
The condition \( r \leq 2^k - q - 2 \)

The condition \( r \leq 2^k - q - 2 \) is satisfied for \( 4 \leq k \leq 471\,600\,000 \).

If, for some \( k \), the condition \( r \leq 2^k - q - 2 \) is not satisfied, then \( (3/2)^k \) is extremely close to an integer:

\[
q + 1 - \frac{q - 2}{2^k} < \left(\frac{3}{2}\right)^k < q + 1,
\]

which is unlikely: one expects that the numbers \( (3/2)^k \) are well distributed modulo 1.
Mahler’s contribution

- The estimate

\[ r \leq 2^k - q - 2 \]

is valid for all sufficiently large \( k \).

Hence the ideal Waring’s Theorem

\[ g(k) = 2^k + \left\lfloor (3/2)^k \right\rfloor - 2 \]

holds for all sufficiently large \( k \).
Waring’s Problem and the $abc$ Conjecture

S. David: the estimate

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

for sufficiently large $k$ follows from the $abc$ Conjecture.

S. Laishram: the ideal Waring’s Theorem

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

follows from the explicit $abc$ Conjecture.
Conjecture of Alan Baker (1996)

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

\[
c \leq \kappa (\epsilon^{-\omega R})^{1+\epsilon}
\]

where \(\kappa\) is an absolute constant, \(R = \text{Rad}(abc)\) and \(\omega = \omega(abc)\) is the number of distinct prime factors of \(abc\).
Conjecture of Alan Baker (1996)

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

\[ c \leq \kappa (e^{-\omega R})^{1+\epsilon} \]

where \(\kappa\) is an absolute constant, \(R = \text{Rad}(abc)\) 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 hand side over \(\epsilon > 0\) occurs essentially with \(\epsilon = \omega / \log R\). This yields a slightly sharper form of the conjecture:

\[ c \leq \kappa R \frac{(\log R)^\omega}{\omega!}. \]
Let \((a, b, c)\) be an \(abc\)–triple. Then

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

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

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

Jerzy Browkin
(1934 – 2015)

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 $\geq 2$ over the same number field.


http://www.math.harvard.edu/~elkies/
The abc conjecture for number fields

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

Andrea Surroca

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

\[
|\alpha - \frac{p}{q}| > \frac{1}{q^{2+\epsilon}}
\]

where he replaces \( \epsilon \) by

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

where \( \kappa \) depends only on the algebraic number \( \alpha \).
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.
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 \textit{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 Dressler 1999).
- Squarefree and powerfree values of polynomials (Browkin, Filaseta, Greaves and Schinzel, 1995).
- Bounds for the order of the Tate–Shafarevich group (Goldfeld and Szpiro 1995).
- Greenberg’s Conjecture on Iwasawa invariants $\lambda$ and $\mu$ 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)
Let $n \geq 3$. There exists a positive constant $\kappa_n$ 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

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

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
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):

$$59^4 + 158^4 = 133^4 + 134^4 = 635318657$$

A parametric family of solutions of $x_1^4 + x_2^4 = x_3^4 + x_4^4$ is known.
and meromorphic function fields

Nevanlinna value distribution theory.

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

Let $K$ be an algebraically closed field. The \textit{radical} of a monic polynomial

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

with $\alpha_i$ pairwise distinct is defined as

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

Let \( A, B, C \) be three relatively prime polynomials in \( K[X] \) with \( A + B = C \) and let \( R = \text{Rad}(ABC) \). 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 \( \alpha_i \) with \( a_i \geq 2 \). They are zeroes of \( P' \) with multiplicity \( a_i - 1 \). Hence

\[ \text{Rad}(P) = \frac{P}{\gcd(P, P')} . \]
Proof of the \textit{ABC} Theorem for polynomials

Now suppose $A + B = C$ with $A, B, C$ relatively prime.
Proof of the $ABC$ Theorem for polynomials

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

Notice that

$$\text{Rad}(ABC) = \text{Rad}(A)\text{Rad}(B)\text{Rad}(C).$$
Proof of the $ABC$ Theorem for polynomials

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

Notice that

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

We may suppose $A, B, C$ to be monic and, say, $\deg(A) \leq \deg(B) \leq \deg(C)$. 
Proof of the $ABC$ Theorem for polynomials

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

Notice that

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

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

Write

$$A + B = C,$$
Proof of the \textit{ABC} Theorem for polynomials

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

Notice that

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

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

Write

$$A + B = C, \quad A' + B' = C', $$
Proof of the *ABC* Theorem for polynomials

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

Notice that

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

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

Write

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

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

\[
< \deg(\text{Rad}(A)) + \deg(\text{Rad}(B)) = \deg(\text{Rad}(AB)).
\]

Hence

\[
\deg(\gcd(C, C')) < \deg(\text{Rad}(AB))
\]

and

\[
\deg(C') < \deg(\text{Rad}(C')) + \deg(\text{Rad}(AB)) = \deg(\text{Rad}(ABC')).
\]
Shinichi Mochizuki

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

E-mail: motizuki@kurims.kyoto-u.ac.jp

Shinichi Mochizuki
Professor
Research Institute for Mathematical Sciences
Kyoto University
Kyoto 606-8502, JAPAN

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


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

In August 2012, Shinichi Mochizuki released a series of four preprints announcing a proof of the abc Conjecture. When an error in one of the articles was pointed out by Vesselin Dimitrov and Akshay Venkatesh in October 2012, Mochizuki posted a comment on his website acknowledging the mistake, stating that it would not affect the result, and promising a corrected version in the near future. He proceeded to post a series of corrected papers of which the latest dated November 2017.
http://www.kurims.kyoto-u.ac.jp/~motizuki/top-english.html

Inter-universal Teichmuller Theory

[1] Inter-universal Teichmuller Theory I: Construction of Hodge Theaters. PDF NEW !! (2017-08-18)


Workshop on IUT Theory of 
Shinichi Mochizuki, December 
7-11 2015

CMI Workshop supported by 
Clay Math Institute and 
Symmetries and 
Correspondences

Organisers: Ivan Fesenko, Minhyong Kim, Kobi Kremnitzer
Finding the speakers and the program of the workshop: Ivan Fesenko
CMI Workshop supported by Clay Math Institute and Symmetries and Correspondences

The work (currently being refereed) of SHINICHI MOCHIZUKI on inter-universal Teichmüller theory (also known as arithmetic deformation theory) and its application to famous conjectures in diophantine geometry became publicly available in August 2012. This theory, developed over 20 years, introduces a vast collection of novel ideas, methods and objects. Aspects of the theory extend arithmetic geometry to a non-scheme-theoretic setting and, more generally, have the potential to open new fundamental areas of mathematics.

The workshop aims to present and analyse key principles, concepts, objects and proofs of the theory of Mochizuki and study its relations with existing theories in different areas, to help to increase the number of experts in the theory of Mochizuki and stimulate its further applications.
Speakers

Shinichi Mochizuki will answer questions during skype sessions of the workshop. He also responds directly to emailed questions.

Participants:

Julio Andrade (Univ. Oxford), Federico Bambozzi (Univ. Regensburg), Alexander Beilinson (Univ. Chicago),
Oren Ben-Bassat (Univ. Haifa), Brian Birch (Univ. Oxford), Francis Brown (Univ. Oxford),
Martin Bridson (Univ. Oxford), Olivia Caramello (Univ. Paris 7), Brian Conrad (Stanford Univ.),
Weronika Czerniawska (Univ. Nottingham), Ishai Dan-Cohen (Univ. Duisburg-Essen),
Jamshid Derakhshian (Univ. Oxford), Taylor Dupuy (Univ. California Los Angeles), Gerd Faltings (MPIM, Bonn),
Ivan Fesenko (Univ. Nottingham), Gerhard Frey (Univ. Duisburg-Essen), Adam Gal (Univ. Oxford),
Yuichiro Hoshi (RIMS, Kyoto Univ.), Alexander Ivanov (Techn. Univ. München), Artur Jackson (Purdue Univ.),
Ariyan Javanpeykar (Univ. Mainz), Kiran Kedlaya (Univ. California San Diego), Minhyong Kim (Univ. Oxford),
Kobi Kreminitzer (Univ. Oxford), Robert Kucharzyk (ETH, Zurich), Ulf Kühn (Univ. Hamburg),
Lars Kuehne (MPIM, Bonn), Laurent Lafforgue (IHES, Bures-sur-Yvette), Emmanuel Lepage (Univ. Paris 7),
Junghwan Lim (Univ. Oxford), Angus Macintyre (Univ. Oxford), Nils Matthes (Univ. Hamburg),
Chung Pang Mok (Morningside Center Mathematics Beijing and Purdue Univ.), Alexander Cruz Morales (MPIM, Bonn),
Sergey Olbezin (Univ. Nottingham), Alexander G. Oldenziel (Utrecht Univ.), Thomas Oliver (Univ. Bristol),
Florian Pop (Univ. Pennsylvania at Philadelphia), Damian Rossler (Univ. Oxford),
Thomas Scanlon (Univ. California Berkeley), Francisco Simkiewich (Univ. Oxford), Jakob Stix (Univ. Frankfurt),
Tamás Szamuely (Rényi Inst. Math., Budapest), Fucheng Tan (Shanghai Cent. Math. Sc. & Shanghai Jiao Tong Univ.),
Dinesh Thakur (Rochester Univ.), Ulrike Tillmann (Univ. Oxford), Wester van Urk (Univ. Nottingham),
Felipe Voloch (Univ. Texas Austin), Matthew Waller (Univ. Nottingham), Andrew Wiles (Univ. Oxford),
Bora Yalkinoglu (Univ. Strasbourg), Go Yamashita (RIMS, Kyoto Univ.), Fernando Garcia Yamauti (Univ. Sao Paulo),
Shou-Wu Zhang (Princeton Univ.), Boris Zilber (Univ. Oxford), Lorenzo Lane (Univ. Edinburgh)
The submitted proof is more than 500 pages long and is currently being peer-reviewed.

Ivan Fesenko estimates that the proof has been verified at least 30 times in §3.1 of the most recent updated version https://www.maths.nottingham.ac.uk/personal/ibf/notesonIUT.pdf of his survey.
Not Even Wrong
Latest on abc
Posted on December 16, 2017 by Peter Woit
http://www.math.columbia.edu/~woit/wordpress/?p=9871

The ABC conjecture has (still) not been proved
Posted on December 17, 2017 by Frank Calegari
https://galoisrepresentations.wordpress.com/2017/12/17/the-abc-conjecture-has-still-not-been-proved/

Hector Pasten
Shimura curves and the abc conjecture
https://arxiv.org/abs/1705.09251
Michel Waldschmidt
On the $abc$ conjecture and some of its consequences.
Mathematics in 21st Century, 6th World Conference, Lahore, March 2013,

The abc conjecture and some of its consequences

https://hal.archives-ouvertes.fr/hal-01626155
On the abc Conjecture
and some of its consequences

by

Michel Waldschmidt

Université P. et M. Curie (Paris VI)

http://www.imj-prg.fr/~michel.waldschmidt/
On the abc Conjecture and some of its consequences

by

Michel Waldschmidt

Université P. et M. Curie (Paris VI)

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