Advanced Studies in Contemporary Mathematics
35 (2025), No. 4, pp. 355 – 363

www.jangjeon.or.kr
http://dx.doi.org/10.17777/ascm2025.35.4.007

ON THE *abc*-CONJECTURE AND SOME OF ITS RESULTS

HYUN SEOK LEE

ABSTRACT. By the Nature News, 10 September 2012, quoting Dorain Goldfeld, "The *abc* conjecture, if proved true, at one stroke solves many famous Diophantine problems, including Fermat's Last Theorem" This is grand unified theory of Diophantine Curves. The marvelous thing on the *abc*-conjecture is that gives a way of reformulating an infinite number of Diophantine Problems. In this article will be at an elementary level, giving a collection of consequences of the *abc*-conjecture. It will not include Inter-universal Teichmüller Theory of Shinichi Mochizuki.

1. INTRODUCTION

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

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

Definition 1.1. *The* **radical** *(also called* **kernel***)* $\mathrm{Rad}(n)$ *of n is the product of the distinct primes dividing n :*

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

Example 1.

$$\mathrm{Rad}(60\,500) = \mathrm{Rad}(2^2 \cdot 5^3 \cdot 11^2) = 2 \cdot 5 \cdot 11 = 110,$$
$$\mathrm{Rad}(82\,852\,996\,681\,926) = 2 \cdot 3 \cdot 3 \cdot 23 \cdot 109 = 15\,042.$$

Definition 1.2. *An abc-***triple** *of three positive integers a, b, c which are coprime, $a < b$ and that $a + b = c$.*

Example 2.

$$1 + 2 = 3, \qquad 1 + 8 = 9,$$
$$1 + 80 = 81, \qquad 4 + 121 = 125,$$
$$2 + 3^{10} \cdot 109 = 23^5, \quad 11^2 + 3^2 5^6 7^3 = 2^{21} \cdot 23.$$

Definition 1.3. *An abc-***hit** *is an abc-***triple** *such that* $\mathrm{Rad}(abc) < c$.

Example 3. *(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

$$(2, 16, 18)$$

is not an abc-hit these three numbers are not coprime.

2010 *Mathematics Subject Classification.* 11D; 11D41; 11J97.

Key words and phrases. abc conjecture, radical of integers, abc-triples, Szpiro's conjecture, Diophantine equations, Waring's problem, Wieferich primes, Erdos–Woods conjecture, Mason's theorem, Diophantine geometry, height inequalities.

$a+b=c$	$\lambda(a,b,c)$	authors
$2+3^{10}\cdot 109=23^5$	$1.629912\cdots$	É. Reyssat
$11^2+3^25^77^6=2^{21}\cdot 23$	$1.6259990\cdots$	B.M. de Weger

- 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.

Proposition 1.4. *There are infinitely many abc-hits. Take* $k\geq 1$, $a=1$, $c=3^{2^k}$, $b=c-1$.

Lemma 1.5. 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. □

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 1. *Are there abc-triples for which* $c>\mathrm{Rad}(abc)^2$*?*

Ans. We do not know the answer! When a, b and c are there 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 $\lambda(abc)$ At the date of September 11, 2008, 217 *abc* triples with $\lambda(a,b,c)\geq 1.4$ were know. Since August 1, 2015, 238 are known.

2. *abc* CONJECTURE

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

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

Conjecture 2.1. *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 $\mathbb{Z}_{>0}$ are relatively prime and satisfy $a+b=c$, then

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

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

Conjecture 2.2. (Explicit *abc*-Conjecture) *According to* S. Lishram *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).

Best known non conditional result:

Theorem 2.3. (C.K. Stewart and Yu Kunrui (1991, 2001))

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

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

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

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

Conjecture 2.4. *Given any* $\varepsilon>0$*, there exists a constant* $C(\varepsilon)>0$ *such that for every elliptic curve with minimal discriminant* Δ *and conductor* N

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

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

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

Here are the two largest known values for $\rho(abc)$, found by A. Nitaj On March 19, 2003 47 *abc* triples were know with $0<a<b<c$, $a+b=c$ and $\gcd(a,b)=1$ satisfying $\rho(a,b,c)>4$.

3. Results

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

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

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

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 $n\leq 2$).

Conjecture 3.1. (Pialli'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).

Conjecture 3.2. (Lang-Waldschmidt) *Let* $\varepsilon > 0$. *There exists a constant* $c(\varepsilon) > 0$ *with the following property. If* $x^p \neq y^q$, *then*

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

with

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

Conjecture 3.3. (M. Hall, Jr) *There exists an absolute constant* $c > 0$ *such that if* $x^3 \neq y^2$ *then*

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

Conjecture 3.4. (Beukers-Stewart) *Let* p, q *be coprime integers with* $p > q \geq 2$, *Then, for any* $c > 0$, *there exists 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

$$(2,2,k),\ (2,3,3),\ (2,3,4),\ (2,3,5),$$
$$(2,4,4),\ (2,3,6),\ (3,3,3)$$

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

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

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

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

are known.

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 primes :

$$1 + 2^3 = 3^2,\ 2^5 + 7^2 = 3^4,\ 7^3 + 13^2 = 2^9,\ 2^7 + 17^3 = 71^2$$
$$3^5 + 11^4 = 122^2, \quad 33^8 + 1\,549\,033^2 = 15\,163^2,$$
$$1\,414^3 + 2\,213\,459^2 = 65^7, \quad 9262^3 + 15\,312\,28362 = 113^7$$
$$17^7 + 76\,271^3 = 21\,063\,928^2, \quad 43^8 + 96\,222^3 = 30\,042\,907^2,$$

Definition 3.5. (Wieferich Primes (1909)) p^2 *divides* $2^{p-1} - 1$.

• The only known **Wieferich primes** below $4 \cdot 10^{12}$ are 1039 and 3511.

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

Erdös -Woods Conjecture

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

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

have the same radical.

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

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

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

$$\begin{aligned} \mathrm{Rad}(x) &= \mathrm{Rad}(y) \\ \mathrm{Rad}(x+1) &= \mathrm{Rad}(y+1) \end{aligned}$$

and

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

Conjecture 3.6. (Erdös -Woods Conjecture) *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 $i = 0, 1, \cdots, k-1$, then $x = y$.

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

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

For each integer $k \geq 2$, define $I(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$. It is easy to show that $g(k) \geq I(k)$ (J.A. Euler, son of Leonhard Euler). Indeed, write

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

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 the others being 1^k ; hence it requires a total number of at least $(q-1)+(2^k-1) = I(k)$ terms.

Conjecture 3.7. (C.A. Bretschneider, 1853) $g(k) = I(k)$ *for any* $k \geq 2$, *with*

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

We know that 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

$$r \leq 2^k - q - 2 \qquad \text{and} \qquad q = \lfloor (3/2)^k \rfloor \cdots$$

The condition $r \leq 2^k - q - 2$ is satisfied for $4 \leq k \leq 471\ 600\ 000$. According to K. Mahler, the upper bound is valid for all sufficiently large k. Hence the ideal Warings Theorem

$$g(k) = I(k)$$

holds also for all sufficiently large k. However, Mahlers proof uses a $p$adic Diophantine argument related to the ThueSiegelRoth Theorem which does not yield effective results. S. David noticed that the estimate for sufficiently large k follows from the abc Conjecture. S. Laishram checked that the ideal Warings Theorem $g(k) = I(k)$ follows from the explicit abc Conjecture.

A problem of P. Erdös solved by C.L. Stewart

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

$$\frac{P(2^n-1)}{n} \to \infty \qquad \text{and} \qquad n \to \infty$$

In 2002, R. Murty and S. Wong proved that this is a consequence of the *abc* Conjecture.

In 2012, C.L. Stewart proved Erdös Conjecture (in a wider context of Lucas and Lehmer sequences) :

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

Stronger than *abc*: best possible estimate

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 $c > R \log R$.

The coefficient $4 - \delta$ has been improved by M. van Frankenhuijsen into 6.068 in 2000. In the same paper, M. van Frankenhuijsen suggested that there may exist two positive absolute constants κ_1 and κ_2 such that, for any *abc*triples (a, b, c), Let $\varepsilon > 0$. There exists $\kappa(\varepsilon)$ such that for any *abc* triple with $R = \mathrm{Rad}(abc) > 8$,

$$c < \kappa(\varepsilon) R \exp\left(\kappa_1 \left(\frac{\log R}{\log\log R} \right)^{1/2} \right).$$

Further, there exist infinitely many *abc*-triples for which

$$c > R\exp\left(\kappa_2\left(\frac{\log R}{\log\log R}\right)^{1/2}\right).$$

O. Robert, C.L. Stewart and G. Tenenbaum suggest the following more precise limit for the abc Conjecture, which would yield these statements with $\kappa_1 = 4\sqrt{3}+\varepsilon$ for c sufficiently large in terms of ε and $\kappa_2 = 4\sqrt{3}-\varepsilon$ for any $\varepsilon > 0$.

Conjecture 3.8. (Robert-Stewart-Tenenbaum) *There exist positive constants* κ_1, κ_2, κ_3 *such that, for any abctriple* (a,b,c) *with* $R = \mathrm{Rad}(abc)$,

$$c < \kappa_1 R\exp\left(4\sqrt{3}\left(\frac{\log R}{\log\log R}\right)^{1/2}\left(1+\frac{\log\log\log R}{2\log\log R}+\frac{\kappa_2}{\log\log R}\right)\right)$$

and there exist infinitely many abctriples (a,b,c) *for which*

$$c > R\exp\left(4\sqrt{3}\left(\frac{\log R}{\log\log R}\right)^{1/2}\left(1+\frac{\log\log\log R}{2\log\log R}+\frac{\kappa_3}{\log\log R}\right)\right)$$

Explicit *abc* Conjecture

In 1996, A. Baker suggested the following statement. Let (a,b,c) be an *abc*-triple let $\varepsilon > 0$. Then

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

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

Remark of Anderw Granville : the minimum of the function on the right hand side over $\varepsilon > 0$ occurs essentially with $\varepsilon = \omega/\log R$. This yields sharper form of the conjecture :

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

Conjecture 3.9. (Explicit abc Conjecture (Alan Baker, 2004)).
Let (a,b,c) *be an abc-triple. Then*

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

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

The *Nagell-Ljunggre equations* 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

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

The *abc* Conjecture for number fields

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

Using the *abc* Conjecture for number fields, **E. Bombieri** (1994) deduces a refinement of the **Thué-Sigel-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.

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 Results of the *abc* Conjecture

- Erdös'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-Shafraevich 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* 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

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

Theorem 3.10. (*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*

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

Proof. The common zeroes of

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

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

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

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 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

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

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

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

□

References

[1] Cartier, Pierre, A. D. R. Choud Ary, and Michel Waldschmidt. *Mathematics in the 21st Century. 6th World Conference, Lahore, March.* Vol. 2015. 2013.

[2] Bombieri, Enrico, and Walter Gubler. *Heights in Diophantine geometry. Vol. 4*. Cambridge University Press, 2007.

[3] A. Baker, *Transcendental Number Theory*. Cambridge University Press, 1990.

[4] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups: Transcendence Properties of the Exponential Function in Several Variables (Grundlehren der mathematischen Wissenschaften)*. Springer, 2000.

[5] J. P. Serre, *Travaux de Baker. Sem. Bourbaki1969170, N 368. Lecture Notes in Mathematics, 180, 73-86.* Springer-Verlag, Berlin, 1971.

[6] Baker, Alan, and Gisbert Wüstholz. *Logarithmic forms and Diophantine geometry*. Vol. 9. Cambridge University Press, 2008.

Department of Mathematics, Kwangwoon University, Seoul 139-701, Republic of Korea

Email address: `luciasconstant@kw.ac.kr`