
La Preuve De La Conjecture Abc

M. Sghiar

9 allée capitaine Jean Bernard Bossu, 21240, Talant, France.

Abstract : The purpose of this article is to demonstrate the abc conjecture and to deduce among other things a simple proof of the Fermat-Wiles theorem and a proof of the Pillai conjecture.

Résumé : Le but de cet article est de démontrer la conjecture abc et d'en déduire entre autres une preuve simple du théorème de Fermat-Wiles et une preuve de la conjecture de Pillai.

Keywords : la conjecture abc, le théorème de Fermat-Wiles, la conjecture de Pillai, la théorie des nombres, le théorème de Roth, le théorème de Baker, le théorème de Bombieri-Vinogradov, le théorème de Faltings, conjecture de Mordell, équation de Brocard, les premiers de Wieferich, la conjecture d'Erdős-Woods.

Date of Submission: 26-06-2018

Date of acceptance: 10-07-2018

I. Introduction

La **conjecture abc** ou **conjecture d'Oesterlé-Masser** ([3] [9] [10]) est une conjecture en théorie des nombres. Elle a été formulée pour la première fois par Joseph Oesterlé (1988) et David Masser (1985). Elle est formulée en termes de trois nombres entiers positifs, a , b et c (d'où son nom), qui n'ont aucun facteur commun et satisfont à $a + b = c$. Si d est le produit des facteurs premiers distincts de abc , alors la conjecture affirme à peu

près que d ne peut pas être beaucoup plus petit que c . Plus précisément, le rapport $\frac{c}{d}$ peut prendre des valeurs

très grandes mais le rapport $\frac{c}{d^{1+\epsilon}}$ est lui borné pour tout $\epsilon > 0$.

Dorian Goldfeld [2] l'a qualifiée en 2006 de « problème non résolu le plus important en analyse diophantienne » car, si elle était vérifiée, la conjecture permettrait de démontrer aisément entre autres : le théorème de Fermat-Wiles, le théorème de Roth, le théorème de Baker, le théorème de Bombieri-Vinogradov, le théorème de Faltings (ou conjecture de Mordell), la conjecture de Pillai, la quantité finie de solutions de l'équation $n! + 1 = m^2$ (Brocard), la quantité infinie de premiers de Wieferich, la conjecture d'Erdős-Woods s'en déduirait également, à un ensemble fini près de contre-exemples [5].

En août 2012, le mathématicien japonais Shinichi Mochizuki a publié un article sur sa page personnelle où il annonce avoir démontré cette conjecture [1] et [8]. Mais cette démonstration – de 500 pages – n'a pas été validée par les autres spécialistes de la question [4].

Le but de cet article est de démontrer la conjecture abc et d'en déduire entre autres une preuve simple du théorème de Fermat-Wiles et une preuve de la conjecture de Pillai.

Il est à rappeler que dans [7], j'ai donné par des techniques relativistes une preuve du théorème de Fermat-Wiles. Et que ces derniers techniques m'ont également permis de prouver de nombreuses conjectures : l'Hypothèse de Riemann (voir aussi [6]), la conjecture de Goldbach, la conjecture de De Polignac, la conjecture de Legendre, la conjecture de Syracuse, les problèmes sur les nombres de Fermat et de Mersenne, et le dernier théorème de Fermat.

II- Notations, définitions et l'énoncé de la conjecture ABC

Soit a un entier (non nul). Le produit des facteurs premiers de a est appelé le **radical** de a et noté $r(a)$.

Conjecture ABC (Oesterlé-Masser) :

Soit $\epsilon > 0$. Alors, il existe $K = K(\epsilon)$ tel que, pour tous nombres a, b, c (positifs) premiers entre eux et vérifiant $a + b = c$, on a $r(abc)^{1+\epsilon}/c \geq 1/K$ [que l'on voit plus souvent écrit $c \leq Kr(abc)^{1+\epsilon}$].

III- la preuve de la conjecture abc

Théorème (Conjecture ABC d'Oesterlé-Masser) :

Soit $\epsilon > 0$. Alors, il existe $K = K(\epsilon)$ tel que, pour tous nombres a, b, c (positifs) premiers entre eux et vérifiant $a + b = c$, on a $r(abc)^{1+\epsilon}/c \geq 1/K$.

Preuve : On se demande pour quelles valeurs a , b , et c on a l'inégalité :

$$r(abc)^{1+\epsilon} \geq c \quad (1)$$

Comme $r(ab)r(a+b) \neq 1$, alors :

$$1+\epsilon \geq \frac{\ln(a+b)}{\ln(r(ab)r(a+b))} \Leftrightarrow r(abc)^{1+\epsilon}/c \geq 1 \quad (2)$$

1^{er} cas : Si $r(ab) \geq a+b$:

Alors on l'équation (1). Et le problème se pose pour $r(ab) < a+b$.

2^{ème} cas : Si $r(ab) < a+b$:

Lemme 1 : Pour tous nombres a , b , c (positifs) premiers entre eux et vérifiant $a+b=c$ avec $r(ab) < (a+b)$

on a : $\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} \notin \mathbb{Q}$.

Preuve : Pour $c > 2$, on ne peut pas avoir simultanément $r(a)=1$ et $r(b)=1$. Supposons que $r(a) \neq 1$.

Si $\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = \frac{p}{q} \in \mathbb{Q}$ avec $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ alors on doit avoir :

$$(a+b)^q = (r(ab)r(a+b))^p.$$

On en déduit, **puisque dans notre cas** $r(ab) < (a+b)$, que $r(ab)|(a+b)$ et comme $r(a)|r(ab)$ et $r(a)|a$, alors $r(a)|b$ et $r(a)|c$ ($c = a+b$), et a , b et c ne seront pas premiers entre eux (car $r(a) \neq 1$), ce qui est absurde.

Lemme 2 : Pour tous nombres a , b , c (positifs) premiers entre eux et vérifiant $a+b=c$ avec $r(ab) < (a+b)$,

on a : $\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = p+i$, $p \in \mathbb{N}$, $i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0, 1[$. Et si

$$\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = \frac{p}{q} + i, \frac{p}{q} \in \mathbb{Q}, i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0, 1+\epsilon[\text{ alors } q=1.$$

Preuve :

Comme pour $c > 2$ on ne peut pas avoir simultanément $r(a)=1$ et $r(b)=1$, supposons que $r(a) \neq 1$.

Si $\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = \frac{p}{q} + i$ avec $\frac{p}{q} \in \mathbb{Q} \setminus \mathbb{N}$, $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ et $p \wedge q = 1$ et $i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0, 1[$ (ceci

est possible car \mathbb{Q} est dense dans \mathbb{R}), alors on doit avoir :

$$\frac{a+b}{(r(ab)r(a+b))^{\frac{p}{q}}} = (r(ab)r(a+b))^i \in \mathbb{Q}^{\frac{1}{q}} \quad (3)$$

Soit $(a+b)^q = K(r(ab)r(a+b))^p$ avec $K = \frac{\alpha}{\beta} \in \mathbb{Q}$, $(\alpha, \beta) \in \mathbb{N}^* \times \mathbb{N}^*$ et $\alpha \wedge \beta = 1$.

Donc : $\beta(a+b)^q = \alpha(r(ab)r(a+b))^p$.

Comme $r(ab) \nmid (a+b)$ - car sinon a, b et c ne seront pas premiers entre eux -, et **comme dans notre cas** $r(ab) < (a+b)$, alors $r(ab) \mid \beta$, et $r(ab)^p \mid \beta$. Et comme $r(ab) \nmid \alpha$ (car α et β sont premiers entre eux) et $r(ab) \nmid r(a+b)$ (car a, b et c sont premiers entre eux), alors : $\beta = r(ab)^p \beta'$.

On a donc : $\beta'(a+b)^q = \alpha r(a+b)^p$

- Si $\beta' \neq 1$ et $r(\alpha) \neq r(a+b)$ alors il existe $x (x \neq 1)$ un diviseur de $r(a+b)$ tel que : $x^{r\alpha} = x^p$ et par suite $q=1$ car p et q premiers entre eux.

- Si $\beta' \neq 1$ et $r(\alpha) = r(a+b)$ alors $r(\beta') \mid r(a+b) = r(\alpha)$ et β et α ne seront pas premiers entre eux, ce qui est absurde.

- Si $\beta' = 1$ alors $(a+b)^q = \alpha r(a+b)^p$ et il existe $x (x \neq 1)$ un diviseur de $r(a+b)$ tel que : $x^{r\alpha} = x^p$ et par suite $q=1$ car p et q premiers entre eux.

Ce qui démontre le **lemme 2**.

Lemme 3 : Pour tous nombres a, b, c (positifs) premiers entre eux et vérifiant $a+b=c$ avec $r(ab) < (a+b)$,

on a : $\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = \mu + i, \mu \in [0,1], i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[$.

Preuve : Du **lemme 2** si, $\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = p+i, p \in \mathbb{N}, i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[$ avec $p > 1$, comme on peut

écrire $p+i = (p - \frac{m}{n}) + (i + \frac{m}{n})$ avec $\frac{m}{n}$ petit, alors $(p - \frac{m}{n})$ doit être un entier plus petit que p, ce qui montre le résultat.

Corollaire 1 : Pour tous nombres a, b, c (positifs) premiers entre eux et vérifiant $a+b=c$, on a : $r(abc)^2/c \geq 1$.

Preuve : Il suffit de prendre $\epsilon = 1$, et d'utiliser le **lemme 3** et l'équation (2).

Remarque 1 : de l'équation (3), on déduit que : $\frac{a+b}{(r(ab)r(a+b))^{\frac{p}{q}}} = (r(ab)r(a+b))^i > 1$, donc :

$\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} > 1$ (car $q=1$ d'après le **lemme 2**), et par suite on ne peut pas avoir

$1 + \epsilon \geq \frac{\ln(a+b)}{\ln(r(ab)r(a+b))}$ pour $\epsilon = 0$, ce qui justifiera le fait de supposer $\epsilon > 0$ dans la suite. Et du

corollaire 1, on peut même se restreindre au cas où $0 < \epsilon < 1$.

Remarque 2 : Pour $\epsilon = 0$ on a des contre-exemples : a=1 et b=80 donnent $r(abc)/c=0.38$; a=1 et b=512 donnent $r(abc)/c=0.22...$ On peut en fait montrer (**voir [9]**) que ce rapport peut être arbitrairement proche de zéro (en prenant par exemple $a=32^{n-1}$ et $b=1$).

Corollaire 2 :

Soit $\epsilon > 0$. Alors $\text{card}\left\{\frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = \mu + i > (1+\epsilon), \mu \in [0,1], i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[\right\} < \infty$ où a, b, c

sont des nombres (positifs) premiers entre eux et vérifiant $a+b=c$ avec $r(ab) < (a+b)$.

Preuve : Résulte du fait que $\left\{ \frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = \mu+i > (1+\epsilon), \mu \in [0,1], i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[\right\}$ est

discret : En effet de la preuve des lemmes 2 et 3 on a : $\mu \in [0,1]$ et $i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[$.

Soit d un réel **positif tout petit** et non nul.

- Si $d \in \mathbb{Q}$: $\mu+i+d = \mu+d+i$, et de ce qui précède $\mu+d \in \mathbb{N}$ avec $\mu+d \geq \mu+1$, donc $\mu+i+d \geq \mu+i+1$. Et $\mu+i-d = \mu-d+i$, donc $\mu+i-d = \mu+i-1$

(une petite variation entraîne donc un grand **saut** !).

- Si $d \in \mathbb{R} \setminus \mathbb{Q}$: $\mu+i+d = \mu+y+d-y+i$ avec $y \in \mathbb{Q}$ proche de 0, et $\mu+y \in \mathbb{N}$ avec $\mu+y \geq \mu+1$ et par suite $\mu+d+i \geq \mu+d+i-y+1$. Et $\mu+i-d = \mu+y-d-y+i$ donc

$$\mu+i-d = \mu+y-d-1+i = \mu+i+(-1+y-d)$$

Ce **saut** montre bien que le dit ensemble est **discret** donc de cardinal fini dans le compact $[1+\epsilon, 2]$.

Et par suite $\text{card} \left\{ \frac{\ln(a+b)}{\ln(r(ab)r(a+b))} = \mu+i > (1+\epsilon), i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[\right\} < \infty$

Corollaire 3 : Si $\epsilon > 0$. Alors il existe K ($K = K(\epsilon)$) tel que, pour tous nombres a, b, c (positifs) premiers entre eux et vérifiant $a+b=c$ avec $r(ab) < (a+b)$ on a : $r(abc)^{1+\epsilon}/c \geq 1/K$.

Preuve : résulte du **corollaire 2**

D'où le **théorème**.

Corollaire 4 : L'application $K : \mathbb{R}^{**} \rightarrow \mathbb{R}^+ : \epsilon \rightarrow K(\epsilon)$ est **décroissante**.

Preuve : De ce qui précède, $K(\epsilon) = \text{Sup} \left\{ \frac{c}{(r(ab)r(a+b))^{1+\epsilon}} \right\}$ où a, b, c (positifs) premiers entre eux et

vérifiant $a+b=c$ avec $r(ab) < (a+b)$ et

$$\frac{\ln(c)}{\ln(r(ab)r(a+b))} = \mu+i > (1+\epsilon), \mu \in [0,1], i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[$$

Si $\epsilon' \leq \epsilon$ alors $\left\{ \frac{\ln(c)}{\ln(r(ab)r(a+b))} = \mu+i > (1+\epsilon), \mu \in [0,1], i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[\right\} \subset$

$$\left\{ \frac{\ln(c)}{\ln(r(ab)r(a+b))} = \mu+i > (1+\epsilon'), \mu \in [0,1], i \in (\mathbb{R} \setminus \mathbb{Q}) \cap]0,1[\right\} \text{ donc } K(\epsilon') \geq K(\epsilon)$$

Remarque 3 : En utilisant la **remarque 2**, le **corollaire 4** montre donc que $K(\epsilon)$ grandit indéfiniment au fur et à mesure que epsilon diminue.

IV- La preuve du Théorème (de Fermat-Wiles)

Théorème (Fermat-Wiles) : L'équation diophantienne $x^n + y^n = z^n$ n' a aucune solution non triviale si l'entier n est strictement supérieur à 2.

Preuve :

Supposons l'existence de trois entiers x, y et z (sans perte de généralité, on peut supposer qu'ils sont premiers entre eux, que z est le plus grand et que $z \geq 2$) vérifiant $x^n + y^n = z^n$. On pose alors $a = x^n$, $b = y^n$ et $c = z^n$, ce qui donne $r(abc) = r(x^n y^n z^n) = r(xyz)$. Par définition $r(xyz) \leq xyz$, et puisque l'on a supposé $x, y \leq z$, on a $xyz \leq z^3$ et $r(abc) \leq z^3$.

D'après le **corollaire 1**, on a $1 \leq r(abc)^2/c$. D'après l'inégalité ci-dessus, $1 \leq (z^3)^2/z^n = z^{6-n}$. Pour que cette dernière inégalité soit vraie, il faut que $n \leq 6$. Donc l'équation $x^n + y^n = z^n$ n'admet aucune solution entière non triviale pour $n > 6$ et par suite aucune solution entière non triviale pour $n > 2$ (car le autres cas ont déjà été démontré).

V- la preuve de la conjecture de Pillai.

Théorème (conjecture de Pillai) : Tout entier ne s'écrit qu'un nombre fini de fois comme différence de puissances parfaites.

Preuve : Il est connu qu'il se déduit de la conjecture abc. (voir [9, 10])

VI- Conclusion

Cette preuve de la conjecture abc est si simple et si importante puisqu'il a permis de démontrer des conjectures (conjecture de Pillai par exemple) et de redonner des preuves simples pour d'autres théorèmes : le célèbre théorème de **Fermat-Wiles** est ainsi démontré en une **page** au lieu de **150** pages pour sa preuve donnée par A. Wiles.

VII- Remerciements

Je remercie tout ceux qui ont contribué à la réussite de cet article .

Références

- [1]. Pierre Colmez, « $a+b=c?$ » — *Images des Mathématiques*, CNRS, 2012. En ligne, URL : <http://images.math.cnrs.fr/a-b-c.html>
- [2]. Dorian Goldfeld (en), « Beyond the last theorem », *The Sciences (en)*, , 34-40.
- [3]. Gerhard Frey , La conjecture ABC – Pour la Science – Nov. 2012 – pages 24 à 31.
- [4]. Cathu O'Neil, « [La conjecture abc n'a pas encore été prouvée](#) » .
- [5]. M. Langevin, « Cas d'égalité pour le théorème de Mason et applications de la conjecture abc », *CRAS*, 317, o 5, , 441-444
- [6]. M. sghiar, the mertens function and the proof of the riemann's hypothesis , <https://hal.archives-ouvertes.fr/hal-01667383>
- [7]. M Sghiar. Une preuve relativiste du Théorème de Fermat-Wiles. IOSR Journal of Mathematics(IOSR-JM), International Organization Of Scientific Research, 2016, 12 (5) (voir aussi : La relativité et la théorie des nombres : <https://hal.archives-ouvertes.fr/hal-01174146v4>)
- [8]. Mochizuki, Shinichi, « [Inter-Universal Teichmüller Theory IV: Log-Volume Computations and Set-Theoretic Foundations](#) » .
- [9]. M. Waldschmidt, Conjecture abc : quelques conséquence, <https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/abcFrVI.pdf>
- [10]. Wikipedia. : https://fr.wikipedia.org/wiki/Conjecture_abc