La conjecture abc

Abderrahmane Nitaj

1. INTRODUCTION

En 1637, Pierre de Fermat écrivait dans la marge des œuvres de Diophante qu'il avait trouvé une belle démonstration du théorème suivant:

Théorème 1.1. *Pour tout entier $n \geq 3$, les seules solutions entières (x, y, z) de l'équation*

$$x^n + y^n = z^n,$$

sont telles que $xyz = 0$.

Non seulement cette démonstration ne fut jamais retrouvée, mais depuis cette date, personne n'a réussi à démontrer ce théorème dans sa généralité. Les travaux récents de A. Wiles y sont finalement parvenus. Le théorème de Fermat se distingue donc particulièrement par la simplicité de son énoncé et par la difficulté de sa résolution. Il a illustré l'évolution de certaines branches des mathématiques (théorie des nombres, géométrie algébrique, ...). Pourtant, isolé, le théorème de Fermat n'a pas une grande importance. Il a repris de l'interêt dès qu'on l'a relié à d'autres problèmes de mathématiques et notamment à la conjecture de Shimura-Taniyama-Weil. La conjecture abc de J. Oesterlé et D. W. Masser est née dans ce contexte: rompre l'isolement du théorème de Fermat. Même si cette conjecture n'implique que la version asymptotique du théorème de Fermat, son importance en théorie des nombres est grande. Sa démonstration permet en effet de résoudre plusieurs autres problèmes ouverts.

Le but de cet article est de donner une description de la conjecture abc (partie 2) et d'enumérer la plupart de ses conséquences (partie 3). La partie 4 est consacrée à l'étude de certaines méthodes permettant de tester numériquement la conjecture abc et d'en prévoir une forme effective. Enfin, la partie 5 présente quelques généralisations possibles de la conjecture abc.

2. LA CONJECTURE abc

Dans cette partie, nous allons rappeler la conjecture abc, ainsi que les quelques tentatives qui ont été faites pour essayer de la démontrer. La définition suivante est étroitement liée à la conjecture abc.

Définition 2.1. *Soit n un entier non nul. On appelle radical de n et on écrit $r(n)$ le produit*

$$r(n) = \prod_{p|n} p \quad (p \textit{ premier}),$$

des facteurs premiers distincts divisant n, avec par convention $r(1) = 1$.

Le radical est quelquefois appelé support, conducteur ou noyau et vérifie $r(n)|n$.

Motivés par un théorème de Mason ([10], [20]) sur les polynômes et par certaines conjectures de Szpiro [31], J. Oesterlé et D.W. Masser ont formulé en 1985 la conjecture suivante, plus connue sous le nom de conjecture abc [20]:

Conjecture 2.2. (abc). *Soit $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout triplet (a, b, c) d'entiers positifs, vérifiant $a + b = c$ et $(a, b) = 1$ on ait:*

$$c \leq c(\varepsilon) \left(r(abc)\right)^{1+\varepsilon}.$$

Une première analyse de l'inégalté de la conjecture abc montre que si un triplet (a, b, c) d'entiers positifs vérifie $a + b = c$ et $(a, b) = 1$, alors le produit abc est composé de nombres premiers distincts avec pour la plupart un exposant relativement petit. On peut constater ce fait dans les tables de factorisation de nombres de la forme $a^n - b^n$, données à la fin du livre de H. Riesel (voir [24], pp 388-437).
Pour $\varepsilon > 0$ fixé, la constante $c(\varepsilon)$ qui lui correspond dans la conjecture abc peut être unique, en prenant:

$$c(\varepsilon) = \inf_{(a,b,c)\in I} \frac{c}{(r(abc))^{1+\varepsilon}}, \tag{2.3}$$

avec $I = \{(a, b, c) \in \mathbb{N}^3,\ (a, b) = 1,\ a + b = c\}$. Quand à la possibilité de prendre $\varepsilon = 0$ dans la conjecture abc, la proposition suivante montre que ce choix n'est pas possible.

Proposition 2.4. *Pour $\varepsilon > 0$, soit $c(\varepsilon)$ la constante définie par (2.3) vérifiant l'inégalité de la conjecture abc. Alors*

$$\lim_{\varepsilon \to 0} c(\varepsilon) = +\infty.$$

Preuve. On définit les entiers x_n et y_n par la relation:

$$x_n + y_n\sqrt{2} = \left(3 + 2\sqrt{2}\right)^n.$$

Alors pour tout $n \geq 1$, $1 + 2y_n^2 = x_n^2$. Si $n = 2^m$, on vérifie facilement par récurrence que $2^{m+1}|y_n$. Appliquons la conjecture abc à la relation $x_n^2 = 1 + 2y_n^2$. On obtient pour $n = 2^m$:

$$x_n^2 \leq c(\varepsilon) \left(r\left(x_n y_n\right)\right)^{1+\varepsilon} \leq c(\varepsilon) \left(x_n y_n / 2^m\right)^{1+\varepsilon} \leq c(\varepsilon) x_n^{2(1+\varepsilon)} / 2^{m(1+\varepsilon)}.$$

Alors $c(\varepsilon) \geq 2^{m(1+\varepsilon)}/x_n^{2\varepsilon}$ et donc

$$\varliminf_{\varepsilon \to 0} c(\varepsilon) \geq 2^m,$$

ce qui montre que $\lim\limits_{\varepsilon \to 0} c(\varepsilon) = +\infty$. ■

Des démonstrations différentes de la proposition 2.4. se trouvent dans [10] et [20].

Depuis sa formulation en 1985, peu de résultats théoriques ont été découverts sur la conjecture *abc*. Il n'existe actuellement que deux théorèmes la concernant. Les démonstrations de ces deux théorèmes s'appuyent sur des méthodes utilisant des formes linéaires de logarithmes complexes et p-adiques. Nous donnons ici ces deux théorèmes. Leurs démonstrations se trouvent dans [29] et [30] respectivement.

Théorème 2.5. (Stewart, Tijdeman, 1986**).** *Il existe une constante effectivement calculable $k > 0$ telle que, pour tout triplet (a, b, c) d'entiers positifs, vérifiant $a + b = c$ et $(a, b) = 1$ on ait:*

$$c < \exp\left\{k\,(r(abc))^{15}\right\}.$$

Théorème 2.6. (Stewart, Yu, 1990**).** *Il existe une constante effectivement calculable $k > 0$ telle que, pour tout triplet (a, b, c) d'entiers positifs, vérifiant $a + b = c$ et $(a, b) = 1$ on ait:*

$$c < \exp\left\{(r(abc))^{2/3+k/\log\log r(abc)}\right\}.$$

Remarquons que les inégalités des deux théorèmes ci-dessus sont exponentielles en $r(abc)$, alors que l'inégalité de la conjecture *abc* est seulement polynômiale.

3. APPLICATIONS DE LA CONJECTURE *abc*

Dans cette partie, nous décrivons la plupart des conséquences de la conjecture *abc* montrant ainsi son importance en théorie des nombres.

3.1. Les conjectures de Szpiro.

Les conjectures de Szpiro sont antérieures (1983) à la conjecture *abc* et certaines d'entre elles ont les mêmes conséquences. Nous donnons deux de ces conjectures. La conjecture suivante est une conséquence de la conjecture *abc* et à été très étudiée ([13], [15], [17], [31]).

Conjecture 3.1.1. (Szpiro, forme forte). *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour toute courbe elliptique semi-stable E sur $\mathbb{Q}$, de discriminant minimal Δ_E et de conducteur N_E on ait:*

$$|\Delta_E| \leq c(\varepsilon) N_E^{6+\varepsilon}.$$

Le conducteur d'une courbe elliptique semi-stable est le radical de son discriminant minimal. Pour une définition exacte du conducteur, on peut consulter [27].

La conjecture suivante est connue aussi sous le nom de conjecture de Lang-Szpiro.

Conjecture 3.1.2. *Pour tout $\varepsilon > 0$ et pour tout couple (A, B) d'entiers premiers entre eux, il existe une constante $c(\varepsilon, A, B) > 0$ telle que pour tous les entiers u, v, k vérifiant $(Au, Bv) = 1$ et $k = Au^3 + Bv^2$, on ait:*

$$|u| \leq c(\varepsilon, A, B) r(k)^{2+\varepsilon} \qquad \text{et} \qquad |v| \leq c(\varepsilon, A, B) r(k)^{3+\varepsilon}.$$

Proposition 3.1.3. *La conjecture abc est équivalente à la conjecture* 3.1.2.

Preuve. Admettons d'abord la conjecture abc. Soient A, B, u, v et k des entiers tels que $(Au, Bv) = 1$ et $k = Au^3 + Bv^2$. La conjecture abc donne:

$$|v|^2 \leq \frac{c_1(\varepsilon)}{|B|} \left(r(ABuvk)\right)^{1+\varepsilon} \leq c_2(\varepsilon, A, B)|uv|^{1+\varepsilon} \left(r(k)\right)^{1+\varepsilon}.$$

Supposons que $|Au^3| \leq |Bv^2|$ (le cas inverse se fait de la même manière), alors $|u| \leq c_3(A, B)|v|^{2/3}$. En reportant cette majoration dans l'inégalité ci-dessus, on obtient:

$$|v|^2 \leq c_4(\varepsilon, A, B)|v|^{5(1+\varepsilon)/3} \left(r(k)\right)^{1+\varepsilon},$$

et par suite:

$$|v|^{(1-5\varepsilon)/3} \leq c_4(\varepsilon, A, B) r(k)^{1+\varepsilon}.$$

Prenons ε tel que $1 - 5\varepsilon > 0$ et posons $\varepsilon' = 18\varepsilon/(1 - 5\varepsilon)$, alors:

$$|v| \leq c_5(\varepsilon, A, B) \left(r(k)\right)^{3(1+\varepsilon)/(1-5\varepsilon)} \leq c_6(\varepsilon', A, B) \left(r(k)\right)^{3+\varepsilon'}.$$

On obtient alors pour $|u|$:

$$|u| \leq c_6^{2/3}(\varepsilon', A, B) c_3(A, B) r(k)^{2(3+\varepsilon')/3} \leq c_7(\varepsilon', A, B) \left(r(k)\right)^{2+\varepsilon'}.$$

Ceci prouve la conjecture 3.1.2.
Inversement, admettons la conjecture 3.1.2. Soient a, b et c des entiers positifs vérifiant $a < b$, $a + b = c$ et $(a, b) = 1$. Alors:

$$(a^2 + ab + b^2)^3 - \left((b - a)(a + 2b)(2a + b)/2\right)^2 = 3^3 \left(ab(a + b)/2\right)^2.$$

Cette relation peut être éventuellement simplifiée par 3^3 si $a \equiv b \pmod 3$. En appliquant la conjecture 3.1.2, on obtient:

$$a^2 \leq b^2 \leq a^2 + ab + b^2 \leq c_1(\varepsilon) \left(r(abc)\right)^{2+\varepsilon},$$

et donc:

$$a \leq b \leq \left(c_1(\varepsilon)\right)^{1/2} \left(r(abc)\right)^{1+\varepsilon/2},$$

et finalement:
$$c \leq c(\varepsilon')\,(r(abc))^{1+\varepsilon'}.$$
Ceci prouve la conjecture *abc*. ■

3.2. Conséquences sur les triplets d'entiers.

Les propositions suivantes montrent l'influence de la conjecture *abc* sur l'architecture des triplets d'entiers.

Proposition 3.2.1. *Si la conjecture abc est vraie, alors pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon)$ telle que pour tout triplet (x_1, x_2, x_3) d'entiers positifs, vérifiant $x_1 + x_2 = x_3$ et $(x_1, x_2) = 1$, un des x_i, $i \in \{1, 2, 3\}$, vérifie:*
$$x_i \leq c(\varepsilon)\,(r(x_i))^{3+\varepsilon}.$$

Cette proposition fait apparaitre un lien entre la conjecture *abc* et le théorème de Fermat. Nous avons aussi le résultat suivant:

Théorème 3.2.2. *Si la conjecture abc est vraie, alors pour tout $\varepsilon > 0$ et tout entier $a \geq 1$, il existe une constante $c_1(\varepsilon, a) > 0$ telle que pour tout entier $n \geq 2$ et tout entier $x \geq 2$ vérifiant $(a, x) = 1$ on ait:*
$$x^{n-1} \leq c_1(\varepsilon, a)\,(r(x^n - a^n))^{1+\varepsilon}.$$

Preuve. Soit ε fixé tel que $0 < \varepsilon < 1/2$. Appliquons la conjecture *abc* à la relation $(x^n - a^n) + a^n = x^n$ avec $(a, x) = 1$. On obtient:
$$x^n \leq c(\varepsilon, a)\,(r(x^n - a^n))^{1+\varepsilon}\,x^{1+\varepsilon},$$

Alors:
$$x^{n-1} \leq (c(\varepsilon, a))^{(n-1)/(n-1-\varepsilon)}\,(r(x^n - a^n))^{(n-1)(1+\varepsilon)/(n-1-\varepsilon)}.$$
Si ε est assez petit et si $n \geq 2$, on a d'une part $(n-1)/(n-1-\varepsilon) < 2$ et d'autre part:
$$\frac{(n-1)(1+\varepsilon)}{n-1-\varepsilon} \leq \frac{1+\varepsilon}{1-\varepsilon} = 1 + \varepsilon',$$
avec $\varepsilon' = 2\varepsilon/(1-\varepsilon)$. On obtient finalement la conclusion du théorème. ■

3.3. Les nombres de Wieferich.

Un nombre premier p vérifiant la congruence
$$a^{p-1} \equiv 1 \pmod{p^2},$$
avec $a = 2$ est appelé nombre de Wieferich. En 1909, celui-ci a montré que si un nombre premier p ne vérifie pas la congruence ci-dessus, alors il n'existe pas d'entiers $x > 0$, $y > 0$

et $z > 0$, premiers entre eux tels que $xyz \not\equiv 0 \pmod p$ et $x^p + y^p = z^p$ (premier cas du théorème de Fermat). En 1910, Mirimanoff a prouvé la même chose avec $a = 3$. Les nombres premiers vérifiant cette congruence sont très rares. Par exemple, les seuls nombres premiers p vérifiant cette congruence avec $a = 2$ et $p \leq 3 \times 10^{10}$ sont 1093 et 3511. De même, les seuls vérifiant cette congruence avec $a = 3$ et $p \leq 2^{30}$ sont 11 et 1006003 (voir [14] ou [22]). Un problème encore ouvert est la conjecture suivante:

Conjecture 3.3.1. *Soit $a \geq 2$. Il existe une infinité de nombres premiers p tels que $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

J. H. Silverman [28] a montré que cette conjecture est une conséquence de la conjecture *abc*.

3.4. La conjecture de Mordell.

Une des conséquences les plus étonnantes de la conjecture *abc* est le fait que celle-ci implique tout simplement la conjecture de Mordell, devenue théorème de Faltings :

Toute courbe de genre $g \geq 2$ définie sur $\mathbb{Q}$ n'admet qu'un nombre fini de points rationnels.

Cette conjecture à été redémontrée par la suite par P. Vojta [34] et E. Bombieri [1]. En 1991, N.D. Elkies a déterminé son lien avec la conjecture *abc* (voir [4]).

Théorème 3.4.1. (Elkies). *La conjecture abc implique la conjecture de Mordell.*

A la fin de son article, Elkies donne le corollaire suivant:

Corollaire 3.4.2. (Elkies). *La conjecture abc implique que pour tout $\varepsilon > 0$ et tout polynôme $P \in \mathbb{Z}[X, Y]$, homogène, de degré d et sans facteurs carrés, il existe une constante $c(\varepsilon, P)$ telle que pour tout couple (a, b) d'entiers premiers entre eux, vérifiant $P(a, b) \neq 0$ on ait:*

$$\sup\left(|a|, |b|\right)^{d-2} \leq c(\varepsilon, P) r\left(P(a, b)\right)^{1+\varepsilon}.$$

3.5. La conjecture d'Erdős-Woods.

La conjecture suivante a été formulée par P. Erdős, puis par Woods en 1981.

Conjecture 3.5.1. (Erdős-Woods). *Il existe une constante $k > 0$ telle que pour tous les entiers positifs x et y, si $r(x + i) = r(y + i)$ pour tout i, $i = 1, 2, \ldots, k$, alors $x = y$.*

Cette conjecture est fausse pour $k = 2$ ($x = 2^n - 3$, $y = 2^{2n} - 2^{n+1} - 1$ conviennent). Par contre pour $k \geq 3$, aucun exemple d'entiers différents vérifiant les égalités de la conjecture d'Erdős-Woods n'est connu. M. Langevin a montré le résultat suivant (voir [11, 12]).

Proposition 3.5.2. (Langevin) *La conjecture abc implique que la conjecture d'Erdős -Woods est vraie avec $k = 3$, sauf peut être pour un nombre fini d'exceptions pour x et y.*

3.6. La conjecture de Hall.

En 1971, M. Hall Jr. a énoncé la conjecture suivante [7]:

Conjecture 3.6.1. (Hall). *Il existe une constante $c > 0$ telle que pour tous entiers $x > 1$ et $y > 0$ vérifiant $x^3 \neq y^2$ on ait:*

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

On sait par exemple depuis 1738 (Euler), que les seules solutions non triviales de l'équation $|x^3 - y^2| = 1$ sont $(x, y) = (2, \pm 3)$. La relation $28187351^3 - 149651610621^2 = -1090$, montre que dans la conjecture de Hall, la constante c vérifie $c \leq 0,205305$. La conjecture abc n'admet pour conséquence que la forme faible suivante de la conjecture de Hall (voir [17], [25]).

Conjecture 3.6.2. *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tous les entiers $x > 1$ et $y > 0$ on ait:*

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

3.7. L' équation de Fermat généralisée.

La conjecture abc s'applique particulièrement aux équations diophantiennes à trois termes, dont l'équation de Fermat généralisée.

Théorème 3.7.1. *Si la conjecture abc est vraie et si A, B, C sont des entiers strictement positifs, alors l'équation:*

$$Ax^l + By^m = Cz^n,$$

n'admet qu'un nombre fini de solutions en entiers positifs x, y, z, l, m, n vérifiant $l^{-1} + m^{-1} + n^{-1} < 1$ et $(x, y, z) = 1$.

Preuve. Si $z = 1$, alors le théorème est clair, même sans admettre la conjecture abc. Supposons donc que $z \geq 2$ et que $(x, y, z) = 1$. Soit $d = (Ax^l, By^m, Cz^n)$. Alors d est borné. En appliquant la conjecture abc au triplet $(Ax^l/d, By^m/d, Cz^n/d)$, on obtient:

$$Cz^n/d \leq c_1(\varepsilon) \left(r(ABCx^l y^m z^n/d^3) \right)^{1+\varepsilon},$$

d'où l'on tire:

$$z^n \leq c_2(\varepsilon, C) \left(dr \left(\frac{ABCx^l y^m z^n}{d^3} \right) \right)^{1+\varepsilon} \leq c_3(\varepsilon, A, B, C) \, (xyz)^{1+\varepsilon}.$$

Puisque $Ax^l < Cz^n$ et $By^m \leq Cz^n$, alors $x < c_4(A, C) z^{n/l}$ et $y < c_5(B, C) z^{n/m}$. Ainsi

$$z^n \leq c_6(\varepsilon, A, B, C) \, (z^n)^{(1+\varepsilon)(l^{-1}+m^{-1}+n^{-1})},$$

ce qui donne :
$$(z^n)^{1-(1+\varepsilon)(l^{-1}+m^{-1}+n^{-1})} \leq c_6(\varepsilon, A, B, C).$$
Si $l^{-1}+m^{-1}+n^{-1}<1$ et si ε est assez petit, alors $1-(1+\varepsilon)\left(l^{-1}+m^{-1}+n^{-1}\right)>0$ et donc z^n est borné. Ainsi z, x, y, l, m, n sont bornés. ■

Remarque 3.7.2. On peut trouver d'autres démonstrations de cette proposition dans [25] et [33]. Dans le cas $A=B=C=1$, seules 10 solutions sont conues avec $l^{-1}+m^{-1}+n^{-1}<1$:

$$1+2^3=3^2, \quad 13^2+7^3=2^9, \quad 17^3+2^7=71^2, \quad 2^5+7^2=3^4, \quad 3^5+11^4=2^2.61^2,$$

ainsi que les solutions suivantes, découvertes par Beukers et Zagier (voir [3]):

$$17^7+76271^3=21063928^2, \quad 1414^3+2213459^2=65^7, \quad 9262^3+15312283^2=113^7,$$

$$43^8+96222^3=30042907^2, \quad 33^8+1549034^2=15613^3.$$

3.8. Quelques conjectures sur les nombres puissants.

Définition 3.8.1. *Un entier n est un nombre puissant s'il possède la propriété suivante: si p divise n et si p est premier, alors p^2 divise n.*

Si n est un nombre puissant, alors il s'écrit de façon unique sous la forme $n=a^2b^3$, où b est sans facteurs carrés et son radical $r(n)$ vérifie donc $r(n)\leq n^{1/2}$.
Les conjectures citées dans cette partie proviennent de [22] et de [6] (B16).

Conjecture 3.8.2. (Erdős-Mollin-Walsh). *Il n'y a aucun triplet de nombres puissants consécutifs.*

Cette conjecture est vérifiée pour tous les triplets d'entiers inférieurs à 2^{60} [18] et implique en particulier qu'il existe une infinité de nombres premiers p tels que

$$2^{p-1} \not\equiv 1 \pmod{p^2}.$$

Ceci fait apparaître un lien avec le premier cas du théorème de Fermat (voir [20]).
La conjecture *abc* ne permet pas de répondre totalement à la conjecture 3.8.2, mais permet d'avoir ceci (voir [17]):

Proposition 3.8.3. *La conjecture abc implique qu'il n'y a qu'un nombre fini de triplets de nombres puissants consécutifs.*

Les conjectures suivantes concernent les nombres de Fermat et de Mersenne et il est facile de montrer qu'elles sont des conséquences de la conjecture *abc* ([17]).

Conjecture 3.8.4. *Pour tout entier $k \geq 2$, soit n_k le nombre puissant le plus proche de 2^k avec $n_k \neq 2^k$. Alors $\lim_{k\to\infty} |2^k - n_k| = +\infty$.*

Conjecture 3.8.5. *Il existe une infinité de nombres de Fermat et de Mersenne qui ne sont pas des nombres puissants.*

Pour terminer cette partie, citons la conjecture suivante sur les nombres 4-*puissants* et qui sont des entiers n tels que $r(n)^4|n$ (voir problème B16 de [6], édition 1981). Cette conjecture est aussi une conséquence de la conjecture *abc*.

Conjecture 3.8.6. (Erdős) *L'équation $x + y = z$ n'admet qu'un nombre fini de solutions en entiers positifs 4-puissants, premiers entre eux.*

3.9. La conjecture de Richard.

La conjecture suivante est tirée de [23]:

Conjecture 3.9.1. (Richard). *Si deux entiers x et y vérifient pour tout entier $n \geq 0$:*

$$r\left(x^{2^n} - 1\right) = r\left(y^{2^n} - 1\right),$$

alors ils sont égaux.

A. Schinzel a montré de façon élégante que cette conjecture est une conséquence de la conjecture *abc* (voir [17], [23]).

3.10. Le problème de Croft.

Le problème de savoir dans quelle mesure la différence $|n! - 2^m|$ peut être petite par rapport à 2^m s'appelle le problème de Croft (voir [6], F23). Des résultats expérimentaux nous ont motivé pour proposer la conjecture suivante (voir [17]).

Conjecture 3.10.2.Ê *Il existe une constante $c > 0$ telle que pour tous les entiers m et n avec $(m, n) \neq (0, 0), (1, 0), (2, 1)$ on ait:*

$$n \leq c\,(r\,|n! - 2^m|)^{1/n}.$$

La conjecture *abc* implique cependant une forme faible de cette conjecture (voir [17]).

Proposition 3.10.3. *La conjecture abc implique que pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tous les entiers m et n avec $(m, n) \neq (0, 0), (1, 0), (2, 1)$, on ait:*

$$n \leq c(\varepsilon)\,(r\,|n! - 2^m|)^{(1+\varepsilon)/n}.$$

3.11. Autres conséquences.

Nous regroupons dans cette partie plusieurs conséquences de la conjecture *abc*. Cela concerne en particulier des équations diophantiennes liées à des problèmes ouverts.

Proposition 3.11.1. *Soient $A > 0$, $B > 0$ et k des entiers. La conjecture abc implique que l'équation*

$$Ax^m - By^n = k$$

n'a qu'un nombre fini de solutions en entiers $x > 1, y > 1, m > 1, n > 1$ avec $mn > 4$.

Cette proposition est liée à une conjecture de Pillai. Lorsque $A = 1, B = 1$ et $k = 1$, cette conjecture porte le nom de conjecture de Catalan, qui affirme en plus que $(x, y, m, n) = (3, 2, 2, 3)$ est l'unique solution. En 1976, R. Tijdeman [32] a montré que l'équation de Catalan n'admet qu'un nombre fini de solutions.

Proposition 3.11.2. *La conjecture abc implique que l'équation*

$$\left(\frac{x}{v}\right)^m - \left(\frac{y}{w}\right)^n = 1,$$

n'admet qu'un nombre fini de solutions en entiers positifs v, w, x, y, $m > 1$ et $n > 1$ vérifiant $(x, v) = 1$, $(y, w) = 1$ et $mn > 4$.

Cette proposition est liée à une conjecture de Shorey et Tijdeman (voir [26], p. 202). Cette conjecture est vraie en particulier si l'une des variables v, w, x ou y est composée de nombres premiers fixé.

Proposition 3.11.3. *La conjecture abc implique que l'équation*

$$(x!)^n + 1 = y^m,$$

n'admet qu'un nombre fini de solutions en entiers $x > 0$, $y > 0$, $n \geq 1$ et $m \geq 2$.

Cette proposition est liée à un problème de Brocard (voir [6], D25) et sa démonstration (voir [17] et [21]) est basée sur l'utilisation des inégalités suivantes, déduites des formules de Stirling et de Chebyshev (voir [19], p. 374), valables pour $x \geq 2$:

$$\begin{cases} (x/e)^x < x!, \\ \prod_{p \leq x} p < 4^x, \ p \text{ premier.} \end{cases} \tag{3.11.4}$$

Proposition 3.11.5. *La conjecture abc implique que l'équation*

$$n! + 1 = p_k^a p_{k+1}^b,$$

n'admet qu'un nombre fini de solutions en entiers $n \geq 1$, $a \geq 0$, $b \geq 0$ et $p_{k-1} \leq n < p_k$ où (p_i), $i \geq 1$ est la suite des nombres premiers.

Cette proposition est liée à une conjecture d'Erdős-Stewart (voir [6], A2). Sa démonstration est basée aussi sur les inégalités (3.11.4).

Proposition 3.11.6. *La conjecture abc implique que l'équation*

$$x^n + y^n = n!z^n$$

n'a qu'un nombre fini de solutions en entiers $x > 0$, $y > 0$, $z > 0$ *et* $n \geq 4$.

Cette proposition est liée à un problème ouvert sur les équations diophantiennes (voir [6], D2).

Proposition 3.11.7. *La conjecture abc implique que pour tout entier* $a \geq 1$, *l'équation*

$$\frac{x^n - y^n}{x - y} = az^m$$

n'a qu'un nombre fini de solutions en entiers $x > y > 0$, $z > 0$, $n > 3$, $m > 1$ *avec* $(x, y) = 1$, $3n^{-1} + m^{-1} < 1$.

Cette proposition est une réponse générale à un problème de H. Edgar ([6], D10) et de Shorey-Tijdeman ([26], pp. 202,203).

Proposition 3.11.8. *La conjecture abc implique que l'équation*

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

n'a qu'un nombre fini de solutions en entiers $x > y > 1$ *et* $m > n > 3$.

La recherche de solutions pour l'équation ci-dessus est appelée problème de Goormaghtigh (voir [6], B25). Avec $n = 3$, (x, y, m, n)=$(2, 5, 5, 3)$, $(2, 90, 13, 3)$ sont les seules solutions connues.

Proposition 3.11.9. *La conjecture abc implique que pour tout entier* $d \geq 1$, *l'équation*

$$x(x + d) \ldots (x + kd) = y^n$$

n'a qu'un nombre fini de solutions en entiers $x > 0$, $k \geq 2$, $y > 0$ *et* $n \geq 2$.

Cette proposition montre le lien entre la conjecture *abc* et les progressions arithmétiques. P. Erdős et J.L. Selfridge ont montré en 1975 que l'équation ci-dessus n'a pas de solution dans le cas particulier $d = 1$ (voir [33] pour plus de détailles).

4. A LA RECHERCHE DE FORMES EFFECTIVES

Soient a, b et c trois entiers positifs, premiers entre eux et vérifiant $a+b=c$. Soit $r=r(abc)$, le radical de abc. On définit le rapport de Oesterlé-Masser pour le triplet (a,b,c) par:

$$\alpha=\alpha(a,b,c)=\frac{\log c}{\log r}.$$

On définit de même le rapport de Szpiro pour le même triplet par:

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

Ce dernier rapport est lié à la conjecture de Szpiro (voir conjecture 3.1.1) par les courbes elliptiques $E_{a,b,c}$ que Y. Hellegouarch [9] a mis au point en 1972 pour étudier le théorème de Fermat. C'est en utilisant ces mêmes courbes que K. Ribet a établit le lien entre la conjecture de Shimura-Taniyama-Weil et le théorème de Fermat. Pour un triplet (a,b,c) d'entiers positifs vérifiant $a+b=c$ et $(a,b)=1$, la courbe $E_{a,b,c}$ est définie par:

$$E_{a,b,c}: \quad y^2=x(x-a)(x+b).$$

Si le triplet (a,b,c) vérifie, par exemple, $a\equiv 0 \pmod{16}$ et $b\equiv -1 \pmod 4$, alors $E_{a,b,c}$ est semi-stable et dans ce cas son équation minimale est donnée par:

$$y^2+xy=x^3+\frac{a-b-1}{4}x^2-\frac{ab}{16}x.$$

Toujours avec les mêmes hypothèses, le discriminant minimal de la courbe $E_{a,b,c}$ est égal à $(abc/16)^2$ et la conjecture 3.1.1 donne donc la même conclusion que la conjecture abc:

Pour tout $\varepsilon>0$, il existe une constante $c(\varepsilon)>0$ telle que l'on ait:

$$abc\leq c(\varepsilon)(r(abc))^{3+\varepsilon}.$$

L'inégalité de la conjecture abc implique que les rapports de Oesterlé-Masser et de Szpiro vérifient:

$$\overline{\lim_{r\to\infty}}\,\alpha(a,b,c)=1 \quad \text{et} \quad \overline{\lim_{r\to\infty}}\,\rho(a,b,c)=3.$$

Ceci implique en particulier qu'il n'y a qu'un nombre fini de triplets (a,b,c) d'entiers positifs vérifiant $a+b=c$, $(a,b)=1$ et $\alpha(a,b,c)>1+k$ ou $\rho(a,b,c)>3+k$, où $k>0$ est fixé. On peut voir facilement que ceci devient faux pour $k\leq 0$. En effet, définissons les suites (x_n), (y_n) et (z_n) par $x_0=37, y_0=17, z_0=21$, et pour tout $n\geq 0$,

$$\begin{cases} x_{n+1}=x_n(x_n^3+2y_n^3),\\ y_{n+1}=-y^n(2x_n^3+y_n^3),\\ z_{n+1}=z_n(x_n^3-y_n^3).\end{cases}$$

Alors pour tout $n\geq 1$, $x_n^3+y_n^3=6z_n^3$, $(x_n,y_n)=1$ et $z_n\equiv 0 \pmod{3\times 2^n}$. Posons $a_n=\min(|x_n|^3,|y_n|^3,|6z_n^3|)$, $c_n=\max(|x_n|^3,|y_n|^3,|6z_n^3|)$ et $b_n=c_n-a_n$. Alors pour $n\geq 1$,

$$r(a_nb_nc_n)=r\left(6\frac{|x_ny_nz_n|^3}{2^{3n}}\right)<(a_nb_nc_n)^{1/3}<c_n,$$

et donc $\alpha(a_n, b_n, c_n) > 1$ et $\rho(a_n, b_n, c_n) > 3$.

On peut se poser maintenant naturellement la question s'il existe un triplet pour lequel l'un des deux rapports α ou ρ est maximal. Nous avons en fait la réponse suivante.

Proposition 4.1. *La conjecture abc implique qu'il existe un triplet d'entiers positifs (a, b, c) vérifiant $(a, b) = 1$ et $a + b = c$, pour lequel le rapport $\alpha(a, b, c)$ (resp. $\rho(a, b, c)$) est maximal.*

Preuve. Admettons la conjecture *abc*. Supposons qu'il n'existe pas de triplet (a, b, c) admettant un rapport α maximal. Soit (a_0, b_0, c_0) un triplet d'entiers positifs vérifiant $(a_0, b_0) = 1$ et $a_0 + b_0 = c_0$, avec $\alpha(a_0, b_0, c_0) > 1$. On peut donc construire une infinité de relations (a_n, b_n, c_n) telles que pour tout $n \geq 1$, $\alpha(a_n, b_n, c_n) > \alpha(a_{n-1}, b_{n-1}, c_{n-1})$. D'autre part, la conjecture *abc* implique que pour tout réel $\varepsilon > 0$, il existe une constante positive $c(\varepsilon)$ telle que pour tout $n \geq 0$, on ait:

$$\alpha(a_n, b_n, c_n) \leq 1 + \varepsilon + \frac{c(\varepsilon)}{\log r(a_n b_n c_n)}.$$

Choisissons ε tel que $1 + \varepsilon < \alpha(a_0, b_0, c_0)$. Comme les tiplets (a_n, b_n, c_n) sont différents deux à deux, alors d'après le théorème de Mahler (voir [26]), $\lim_{n \to \infty} r(a_n b_n c_n) = \infty$ et donc:

$$\lim_{n \to \infty} \alpha(a_n, b_n, c_n) \leq 1 + \varepsilon < \alpha(a_0, b_0, c_0),$$

ce qui contredit la définition de la suite. ■

Les triplets (a, b, c) d'entiers positifs vérifiant $a + b = c$, $(a, b) = 1$ pour lesquels les rapports $\alpha(a, b, c)$ ou $\rho(a, b, c)$ sont proches des valeurs conjecturales 1 et 3 sont nombreux. Nous convenons de dire qu'un triplet (a, b, c) est *bon* pour la conjecture *abc* si $\alpha(a, b, c) > 1.4$ ou si $\rho(a, b, c) > 3.3$. Dans la suite, on se propose de décrire une méthode de recherche de bons triplets pour la conjecture *abc*. Cette méthode est basée sur la résolution de l'équation diophantienne:

$$Ax^n - By^n = Cz \tag{4.2}$$

en entiers x, y, z où les entiers A, B, C et n sont donnés et vérifient $A > 0$, $B \neq 0$, $C > 0$, $n \geq 2$ et $(A, B) = 1$. Pour chaque solution (x, y, z) de (4.2), nous prenons les entiers a, b et c parmis Ax^n, By^n et Cz de telle sorte que le triplet (a, b, c) vérifie $0 < a < b$, $a + b = c$ et $(a, b) = 1$. On calcule enfin les rapports $\alpha(a, b, c)$ et $\rho(a, b, c)$ en espérant qu'ils soient bons pour la conjecture *abc*. Pour cela, on doit bien choisir les données A, B et C et on cherche les solutions de (4.2) dans lesquelles $|z|$ est petit par rapport à C. La description détaillée de cette méthode se trouve dans [15, 16, 17].
Nous avons ainsi déterminé 86 exemples de tiplets (a, b, c) d'entiers positifs vérifiant $a + b = c$, $(a, b) = 1$ et $\alpha(a, b, c) \geq 1.4$ et 103 autres exemples vérifiant $\rho(a, b, c) \geq 3.8$. Nous listons dans les tables 4.3 et 4.4 les 11 meilleurs triplets connus actuellement relativement au

rapport α et au rapport ρ. L'auteur peut fournir, sous demande, la totalité des triplets dont il dispose. Certains exemples ont été déterminés en même temps par une méthode différente par J. Browkin et J. Brzeziński et sont notés B-B (voir [2]). De manière exhaustive, N. Elkies et J. Kanapka ont déterminé tous les triplets d'entiers positifs (a, b, c) vérifiant $a + b = c \leq 2^{32}$, $(a, b) = 1$ et $\alpha(a, b, c) \geq 1.2$ (communication privée). Récemment, H. te Riele et P. Montgomery ont déterminé 5 nouveaux exemples en utilisant l'algorithme LLL de Lenstra, Lenstra et Lovász (communication privée). D'autre part, nous avons continué la recherche de bons exemples pour la conjecture abc avec une méthode basée sur les approximations p-adiques. Cette méthode à permis de découvrir 21 nouveaux exemples avec $\alpha > 1.4$ et 20 autres avec $\rho > 4.0$.

$N.$	a	b	c	α	Auteur
1.	2	$3^{10}.109$	23^5	1.62991	Reyssat (1987)
2.	11^2	$3^2.5^6.7^3$	$2^{21}.23$	1.62599	de Weger (1987)
3.	19.1307	$7.29^2.31^8$	$2^8.3^{22}.5^4$	1.62349	B-B (1992)
4.	283	$5^{11}.13^2$	$2^8.3^8.17^3$	1.58076	B-B, Nitaj (1992)
5.	1	2.3^7	$5^4.7$	1.56789	de Weger (1987)
6.	7^3	3^{10}	$2^{11}.29$	1.54708	de Weger (1987)
7.	$7^2.41^2.311^3$	$11^{16}.13^2.79$	$2.3^3.5^{23}.953$	1.54443	Nitaj (1994)
8.	5^3	$2^9.3^{17}.13^2$	$11^5.17.31^3.137$	1.53671	te Riel-Montgomery (1994)
9.	13.19^6	$2^{30}.5$	$3^{13}.11^2.31$	1.52700	Nitaj (1992)
10.	$3^{18}.23.2269$	$17^3.29.31^8$	$2^{10}.5^2.7^{15}$	1.52216	Nitaj (1994)
11.	239	$5^8.17^3$	$2^{10}.37^4$	1.50284	B-B, Nitaj (1992)

Table 4.3

$N.$	a	b	c	ρ	Auteur
1.	13.19^6	$2^{30}.5$	$3^{13}.11^2.31$	4.41901	Nitaj (1992)
2.	$2^5.11^2.19^9$	$5^{15}.37^2.47$	$3^7.7^{11}.743$	4.26801	Nitaj (1994)
3.	$2^{19}.13.103$	7^{11}	$3^{11}.5^3.11^2$	4.24789	de Weger (1987)
4.	$2^{35}.7^2.17^2.19$	$3^{27}.107^2$	$5^{15}.37^2.2311$	4.23069	Nitaj (1994)
5.	$3^{18}.23.2269$	$17^3.29.31^8$	$2^{10}.5^2.7^{15}$	4.22979	Nitaj (1994)
6.	$17^4.79^3.211$	$2^{29}.23.29^2$	5^{19}	4.22960	Nitaj (1994)
7.	$5^{14}.19$	$2^5.3.7^{13}$	$11^7.37^2.353$	4.22532	Nitaj (1994)
8.	3^{21}	$7^2.11^6.199$	$2.13^8.17$	4.20094	Nitaj (1992)
9.	$5^{18}.6359$	$3^2.47^6.73^3$	$2^7.19^{10}.79$	4.14883	Nitaj (1994)
10.	$11^3.31^5.101.479$	107^8	$2^{31}.3^4.5^6.7$	4.13000	Nitaj (1994)
11.	$7.11^6.43$	$3^{11}.5^4$	$2^{17}.17^3$	4.10757	G. Xiao (1986)

Table 4.4

Les tables 4.3 et 4.4 nous permettent de donner la forme effective suivante de la conjecture abc:

Conjecture 4.5. *Si (a,b,c) est un triplet d'entiers positifs vérifiant $a+b=c$ et $(a,b)=1$, alors $c < r(abc)^{1.63}$ et $abc < r(abc)^{4.42}$.*

Cette conjecture est bien entendu plus faible que la conjecture abc. Elle permet de déterminer des bornes explicites pour les solutions de certaines équations diophantiennes. A titre d'exemple, elle implique le théorème de Fermat pour les exposants $n \geq 5$.

La recherche d'une formule de la constante $c(\varepsilon)$ de la conjecture abc en fonction de ε est un problème différent. Il faut tenir compte du fait que $\lim_{\varepsilon \to \infty} c(\varepsilon) = +\infty$, (Proposition 2.3) et du théorème suivant, démontré dans [13] et [29]:

Théorème 4.6. *Soit $\delta > 0$. Il existe une infinité de triplets (a,b,c) d'entiers positifs vérifiant $a+b=c$, $(a,b)=1$ et tels que*

$$c > r(abc) \exp\left((4-\delta) \frac{\sqrt{\log r(abc)}}{\log\log r(abc)} \right).$$

Ce théorème admet la conséquence suivante:

Proposition 4.7. *Pour tout $k > 0$ et tout $k_1 > 0$, il existe un triplet (a,b,c) d'entiers positifs vérifiant $a+b=c$, $(a,b)=1$ et tels que $c > kr(abc)(\log r(abc))^{k_1}$.*

Preuve. Soient $k > 0$ et $k_1 > 0$. Supposons que tous les triplets (a,b,c) d'entiers positifs avec $a+b=c$ et $(a,b)=1$ vérifient $c \leq kr(abc)(\log r(abc))^{k_1}$. Soit (a,b,c) un triplet vérifiant l'inégalité du théorème (4.6). Alors:

$$r(abc) \exp\left((4-\delta) \frac{\sqrt{\log r(abc)}}{\log\log r(abc)} \right) < c \leq kr(abc)(\log r(abc))^{k_1},$$

ce qui donne:

$$(4-\delta)\sqrt{\log r(abc)} < (\log k + k_1 \log\log r(abc)) \log\log r(abc),$$

et donc $r(abc)$ est borné, ce qui est impossible par le théorème (4.6) et par le théorème de Mahler. ∎

La proposition 4.7 nous donne maintenant le résultat suivant:

Proposition 4.8. *Pour tout $k > 0$. Il existe un réel $\varepsilon > 0$ et un triplet (a,b,c) d'entiers positifs, vérifiant $a+b=c$ et $(a,b)=1$, tels que*

$$c > \frac{1}{\varepsilon^k}(r(abc))^{1+\varepsilon}.$$

Preuve. Soit $k > 0$. Supposons que pour tout $\varepsilon > 0$, et tout triplet (a,b,c) d'entiers positifs vérifiant $a+b=c$, $(a,b)=1$ on ait:

$$c \leq \frac{1}{\varepsilon^k}(r(abc))^{1+\varepsilon}.$$

Le minimum du second membre de cette inégalité est atteint pour $\varepsilon = k/\log r(abc)$. Alors, on doit avoir:

$$c \leq \left(\frac{e}{k}\right)^k r(abc)\,(\log r(abc))^k\,,$$

ce qui contredit la proposition 4.7. $\blacksquare$

5. GENERALISATIONS

La conjecture *abc* est aussi simple par son énoncé que le théorème de Fermat, mais certainement beaucoup plus difficile, et en tout cas sa résolution aura beaucoup de conséquences en théorie des nombres. L'interêt de cette conjecture nous ramène à envisager la possiblité d'une généralisation dans différentes directions.

5.1. n-conjecture *abc*

La conjecture *abc* peut être étendue à un nombre de paramètres supérieur à trois de la façon suivante.

Soit $n \geq 3$. Soient $a_1, a_2, \cdots, a_n$ des entiers vérifiant les conditions:

$$(5.1.1) \qquad \begin{cases} a_1 + a_2 + \ldots a_n = 0, \\ (a_1, a_2, \cdots, a_n) = 1, \\ \text{Aucune sous-somme n'est nulle.} \end{cases}$$

Soit $r(a_1 a_2 \cdots a_n)$ le radical du produit $a_1 a_2 \cdots a_n$. La n-conjecture *abc* s'énonce ainsi (voir [2]):

Conjecture 5.1.2. (n-conjecture *abc*) *Pour tout entier $n \geq 3$ et tout $\varepsilon > 0$, il existe une constante $c(\varepsilon, n) > 0$ telle que pour tout n-uplet $(a_1, a_2, \cdots, a_n)$ d'entiers vérifiant les conditions* (5.1.1) *on ait:*

$$\max(|a_1|, \cdots, |a_n|) \leq c(\varepsilon, n)\,(r(a_1 a_2 \cdots a_n))^{2n-5+\varepsilon}\,.$$

5.2. L'anneau des polynômes.

L'analogue de la conjecture *abc* dans l'anneau des polynômes $K[X]$ d'un corps K de caractéristique nulle est en fait un théorème. On peut trouver sa démonstration dans [10], [17] ou [20].

Théorème 5.2.1. (Mason). *Soient A, B et C trois polynômes non tous constants de $K[X]$, vérifiant $A + B + C = 0$ et $(A, B) = 1$. Soit $r(ABC)$ la somme des degrés des différents facteurs irréductibles de ABC. Alors*

$$\max\,(\deg(A), \deg(B), \deg(C)) \leq r(ABC) - 1.$$

L'inégalité du théorème ci-dessus ne peut pas être améliorée (voir [12]). D'autre part, ce théorème est très utile pour l'étude des équations polynômiales. En particulier il implique le théorème de Fermat dans $K[X]$ et explique pourquoi on ne peut pas espérer trouver des formules polynômiales donnant un grand nombre de bons exemples pour la conjecture *abc*.

La n-conjecture *abc* dans $K[X]$, où K est un corps de caractéristique nulle, peut être formulée aussi de la façon suivante (voir [2]).

Conjecture 5.2.2. *Soient $n \geq 3$ un entier et a_i, $1 \leq i \leq n$ des polynômes non tous constants de $K[X]$ vérifiant des conditions analogues aux conditions* (5.1.1). *Alors*

$$\max_{1 \leq i \leq n} \deg(a_i) \leq (2n-5)(r(a_1 \cdots a_n) - 1),$$

où $r(a_1 \cdots a_n)$ désigne la somme des degrés des différents facteurs irréductibles de $a_1 \cdots a_n$.

5.3. Corps de nombres

La conjecture *abc* existe aussi dans les corps de nombres. Le lecteur intéressé peut trouver sa formulation par exemple dans [4], [5] ou [35].

REFERENCES

[1] E. Bombieri, *The Mordell Conjecture Revisited,* Annali Scuola Normale Sup. Pisa, Cl. Sci., S. IV, **17** (1990), 615 – 640.

[2] J. Browkin and J. Brzeziński, *Some remarks on the abc-conjecture,* Math. Comp. **62**, no. 206 (1994), 931 – 939.

[3] H. Darmon and A. Granville, *On the equation $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$,* à paraître dans Bull. London Math. Soc.

[4] N.D. Elkies, *ABC implies Mordell,* Intern. Math. Res. Notices **7** (1991), 99 – 109, in: Duke Math. Journ. **64** (1991).

[5] G. Frey, *Links between solutions of $A - B = C$ and elliptic curves*, Number Theory, Ulm 1987, H.P. Schlickewei, E. Wirsing, eds., Lecture Notes in Math. **1380**, pp. 31 – 62.

[6] R.K. Guy, *Unsolved Problems in Number Theory,* second edition Springer Verlag, 1994.

[7] M. Hall Jr, *The diophantine equation $x^3 - y^2 = k$,* Computers in Number Theory, A.O.L. Atkin, B.J. Birch, eds., Academic Press, London 1971, pp. 173 – 198.

[8] K. Hardy, J.B. Muskat and K. S. Williams, *A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v,* Math. Comp. **55**, no. 191 (1990), 327 – 343.

[9] Y. Hellegouarch, *Courbes elliptiques et équation de Fermat,* Thèse (1972), Université de Besançon.

[10] S. Lang, *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. **23** (1990), 37 – 75.

[11] M. Langevin, *Partie sans facteur carré d'un produit d'entiers voisins* , Approximations Diophantiennes et Nombres Transcendants, Luminy 1990, P. Philippon, eds., Walter de Druyter, Berlin 1992, pp. 203 – 214.

[12] M. Langevin, *Cas d'égalité pour le théorème de Mason et applications de la conjecture* (*abc*), C. R. Acad. Sci. Paris, t. 317 (1993), Série I, 441 – 444.

[13] D.W. Masser, *Note on a conjecture of Szpiro*, Astérisque **183** (1990), 19 – 23.

[14] P.L. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp. **61**, no. 203 (1993), 361 – 363.

[15] A. Nitaj, *Algorithms for finding good examples for the abc and the Szpiro conjectures*, Experimental Math. **2** (1993), 223 – 230 .

[16] A. Nitaj, *An algorithm for finding good abc-examples*, C. R. Acad. Sci. Paris, t. 317 (1993), Série I, 811 – 815.

[17] A. Nitaj, *Conséquences et aspects expérimentaux des conjectures abc et de Szpiro*, Thèse (1994), Université de Caen.

[18] A. Nitaj, *Consecutive powerful numbers to* 2^{60}, Preprint (1994).

[19] I. Niven, H.S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley and Sons, (New York) 1991.

[20] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki, 1987-88, no. 694. (Astérisque, vols. 161-162, pp. 165-186) Paris, Soc. Math. Fr. 1988.

[21] M. Overholt, *The diophantine equation* $n! + 1 = m^2$, Bull. London Math. Soc. **25** (1993), 104.

[22] P. Ribenboim, *Remarks on exponential congruences and powerful numbers,* J. Number Theory, **29** (1988), 251 – 263.

[23] D. Richard, *Equivalence of some questions in mathematical logic with some conjectures in Number Theory,* Number Theory and Applications, R.A. Mollin ed., NATO ASI Series, Ser. C, vol. 265 (1989), Kluwer, 529 – 545.

[24] H. Riesel, *Prime Numbers and Computer Methods for Factorization,* Prog. in Math., **126**, second edition, Birkhäuser, Basel and New York, 1994.

[25] W.M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. **1467**, Springer-Verlag 1991.

[26] T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge (1986).

[27] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[28] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), 226-237.

[29] C.L. Stewart and R. Tijdeman, *On the Oesterlé-Masser conjecture,* Monatsh. Math. **102** (1986), 251 − 257.

[30] C.L. Stewart and Kunrui Yu, *On the abc-conjecture,* Math Ann. **291** (1991), 225 − 230.

[31] L. Szpiro, *Discriminant et conducteur des courbes elliptiques,* Astérisque **183** (1990), 7 − 18.

[32] R. Tijdeman, *On the equation of Catalan,* Acta Arith. **29** (1976), 197 − 209.

[33] R. Tijdeman, *Diophantine equations and diophantine approximations,* Number Theory and Applications, R.A. Mollin ed., NATO ASI Series, Ser. C, vol. 265 (1989), Kluwer, 215 − 243.

[34] P. Vojta, *Siegel's Theorem in the compact case,* Annals of Math. **133** (1991), 509 − 548.

[35] P. Vojta, *Diophantine Approximation and Value Distribution Theory,* Lecture Notes in Math. **1239**, Springer-Verlag 1987.

[36] B.M.M. de Weger, *Algorithms for diophantine equations*, CWI Tract, Centr. Math. Comput. Sci. , Amsterdam 1989.

[37] K.S. Williams and K. Hardy, *A refinement of H.C. Williams'qth root algorithm,* Math. Comp. **61**, no. 203 (1993), 475 − 483.

Abderrahmane Nitaj,
Université de Caen,
Département de Mathématiques,
14000 Caen Cedex
(email nitaj@math.unicaen.fr)